Te Tari Taiwhenua The Department of Internal Affairs

Proactive release of Cabinet material Proposals for refreshing the Cloud First Policy and strengthening cloud adoption across the public service.

16 May 2023

These documents have been proactively released:

4 April 2023, Cabinet Paper: Proposals for refreshing the Cloud First Policy and strengthening cloud adoption across the public service; and

4 April 2023, ERS 23-MIN-0019 Minute.

Some parts of this information release would not be appropriate to release and, if requested, would be withheld under the Official Information Act 1982 (the Act). Where this is the case, the relevant sections of the Act that would apply have been identified. Where information has been withheld, no public interest has been identified that would outweigh the reasons for withholding it.

Key to Redaction Codes:

- **Section 9(2)(f)(iv) – confidentiality of advice tendered by Ministers and officials.**

Where information has been withheld for other reasons consistent with advice, it has been annotated with an asterisk. This information may in some cases be accessible under the Official Information Act 1982.

Office of the Minister Responsible for the Government Communications Security Bureau

Office of the Minister for the Digital Economy and Communications

Cabinet External Relations and Security Committee

Proposals for refreshing the Cloud First Policy and strengthening cloud adoption across the public service

Proposal

1 This paper seeks agreement to a refreshed Cloud First Policy and agreement to carry out further work to increase public sector adoption of cloud computing.

Relation to government priorities

2 Refreshing the Cloud First Policy (the Policy) will make it easier for agencies to deliver on Government priorities. The work is being progressed to ensure public service agencies can effectively utilise changes in technology to provide better public services, help meet emissions targets and better ensure Māori interests are reflected in their use of cloud technology. It supports the Strategy for a Digital Public Service and the Digital Strategy for Aotearoa.

Executive Summary

3 Cloud computing enables new ways of working and can provide improved security, flexibility, resilience, insights and innovation. Cloud will be an important feature of any digital economy and with the arrival of billions of dollars of investment in onshore hyperscale[1] cloud services, there will be opportunities and options not previously available in Aotearoa.

4 The 2012 Cloud First Policy is no longer in sync with either the advancements in technology or changes in societal and Government priorities. A refresh of the Policy is timely. The proposed refresh will provide greater clarity, guidance and support to agencies in their consideration of cloud and cloud adoption.

5 Four changes to the Policy are recommended: reflect societal shifts and commitment to Government priorities (for example, Te Tiriti o Waitangi (Te Tiriti) and sustainability); reflect evolving cloud technology by revoking the Infrastructure-as-a-Service (IaaS) Cabinet directive [CAB Min (12) 23/12 refers]; refresh considerations for security and jurisdictional risk; and strengthen the Government Chief Digital Officer's (GCDO) mandate for cloud digital investment.

6 To enable system-wide transformation and tackling of deeper barriers to adoption of cloud by the public service, a second phase of work is recommended. This phase would seek to identify further Government interventions and potential investments that would enable optimisation of existing and planned new public sector transitions to cloud.

[1] The term "hyperscale" refers to significantly scalable cloud computing systems in which a very large number of servers are networked together. The number of servers used at any one time can increase or decrease to respond to changing requirements. This means the network can efficiently handle both large and small volumes of data traffic.

Background

What is cloud computing?

7 Cloud enables the delivery and management of technology solutions over the Internet. Cloud computing lets an agency access services, such as computing power, storage, and databases, on an as-needed basis from cloud providers rather than owning, buying, or maintaining physical data centres and servers. Compared to legacy and on-premise environments, cloud users can pursue outcomes with speed, insights, and flexibility. A more technical description of cloud, its service and deployment models can be found in **Appendix A**. In this paper, cloud refers to public cloud unless otherwise specified.

Objectives and benefits of the Cloud First Policy

8 On 20 August 2012, Cabinet agreed that an all of government (AoG) cloud first' approach be taken for the government's cloud adoption [CAB-MIN (12) 29/8A refers]. Further additions to the policy in 2013 and 2016 recognised that, to maximise the benefits of public cloud, consistent, secure adoption of cloud was needed [CAB Min (13) 20/13, CAB (13) 37/6B and CAB-16-MIN-0316 refers].

9 There are many potential benefits of a cloud first approach, including increased security and reduced risk, increased continuity, resilience and flexibility for agencies to scale and deliver services as needed, utilise new tools to gather insights andinnovate, and ultimately, accelerate digital transformation of the public service. These advantages could be seen in agency responses to COVID-19. Further information on the benefits of cloud computing and New Zealand case studies can be found in **Appendix B**. Public service transition to cloud also provides an opportunity to support broader economic and sector development, through commercial scale, security, interoperability, workforce development and innovation.

10 The Policy requires agencies[2] to:

10.1 adopt public cloud services in preference to traditional ICT systems;

10.2 make cloud adoption decisions on a case-by-case basis following a risk assessment;

10.3 have a plan for how they intend to use public cloud services; and

10.4 only store data classified as RESTRICTED or below in public cloud services.

A refresh of the Policy is required

11 Since the 2016 refresh, cloud technologies and service offerings have matured significantly. A growing New Zealand based cloud infrastructure sector has developed (for example, Spark, Datacom, Kyndryl and Catalyst Cloud). More recently, three major global cloud providers (Microsoft, Amazon Web Services (AWS), and Google Cloud) and several other specialist hyperscale data centre providers have announced plans to create onshore cloud infrastructure. With billions

[2] The application of the Policy is aligned to DIAs system leadership for digital transformation. Remit of GCDO mandate includes public service agencies as defined in section 10 of the Public Service Act 2020, and entities (Accident Compensation Corporation, Te Whatu Ora, the Earthquake Commission, Kāihga Ora, the New Zealand Qualifications Authority, the New Zealand Transport Agency, New Zealand Trade and Enterprise and the Tertiary Education Commission) covered by the existing ICT direction under section 107 of the Crown Entities Act 2004.

of dollars of announced investments in the New Zealand cloud ecosystem, this new infrastructure will provide options and opportunities not previously available.

12 It is timely to adjust the Policy to align with societal and Government commitments (such as Te Tiriti and sustainability); make it fit for purpose in terms of security in an evolving digital environment, and support agencies to adopt cloud solutions to position the public service to deliver for communities now and in the future.

13 We recommend four changes to the Policy: reflect societal shifts and commitment to government priorities; reflect evolving cloud technology by revoking the IaaS Cabinet directive [CAB Min (12) 23/12 refers]; refresh considerations for security and jurisdictional risk; and strengthen the requirement for agencies to use cloud services under the GCDO's mandate for cloud digital investment.

Further work is required to address inconsistent uptake across the public service

14 The Policy sets the direction for the public service but on its own, will not drive widespread cloud uptake. Despite several attempts to increase cloud adoption across the public service, cloud uptake across the public service remains uneven and lower than expected. For example, only 32.5 percent of public service systems[3] are hosted in the cloud.

15 We are proposing to build upon the Policy to begin to address underlying issues contributing to inconsistent uptake of cloud technologies. These are varied, complex and interlinked, but broadly include:

15.1 Lack of clarity and understanding of cloud and the Policy. Over time, the Policy has become disjointed, and the core focus lost. The Policy does not reflect changes in technology, society or Government priorities;

15.2 Lack of capacity and capability, which combined with the above lack of understanding, can create uncertainty in cloud adoption, resulting in inertia, or ad hoc or inefficient "lift and shift" adoption. Shifting from legacy environments to the cloud often requires significant resources (including scarce cloud skills) and investment for planning, design and execution. This lack of capability and capacity has lead to;

15.2.1 a perception that security risks are significant obstacles to cloud consideration agencies are not equipped to address, or

15.2.2 uncertainty as to how or whether agencies have the ability to approach issues such as Māori data/Māori data sovereignty.

15.3 Constraints on the ability to invest in cloud, including because of legacy systems and technical debt[4] and understanding or incentives of the current funding model. There are opportunities for better system-wide resource utilisation and outcomes.

[3] Based on a count of systems as indicated by agencies in the 2022 investment intentions survey. The percentage by gross value is 13.3%. Responses of "N/A (non-server hardware), "TBC" or nil response are excluded from these calculations.

[4] Technical debt occurs when there is a tendency to prefer short-term solutions when developing and implementing technology and delaying the upgrade of infrastructure. It is often the result of complex requirements with limited capability. The accumulation of technical debt can adversely affect innovation and the ability to employ new technologies (such as cloud). These impacts begin to compound as unsupported hardware and software components become more expensive to maintain and operate.

Phase One: Proposals for refreshing the Cloud First Policy

16 We seek agreement to four proposals that will provide clarity to the Policy, support agency capability and capacity and lay the foundation for further work to support system-wide interventions and investment for transformation. The proposals are not intended to be additional barriers to cloud but provide guidance and support on how to approach issues agencies are facing or need to address.

17 A summary of proposed changes to the Policy and supporting arrangements are provided as **Appendix C**.

Proposal one: reflect societal shifts and commitment to Government priorities

Māori expectations and interests in the Public Service's use of cloud services as it relates to the storage and use, particularly of Māori data

18 There is an opportunity to include Te Ao Māori perspectives in the Policy. The current Policy is silent on the Crown's Te Tiriti obligations and questions around Māori data and Māori data sovereignty. Inclusion would acknowledge Te Tiriti and would represent a world first for incorporating indigenous considerations into national cloud policies. This has the potential to provide mutual benefits to both Iwi and Māori and the public service, including increased trust in public service agencies and their use of cloud, and appropriate protection of Māori data determined by tikanga and kawa (protocols).

19 Under DIA's Mana Ōrite[5] agreement, we directed officials from DIA to work in partnership with Statistics NZ and the Data Iwi Leaders Group (DILG) to consider Māori expectations and interests in the public service's use of cloud. Representatives across Iwi and Māori, Crown agencies and cloud service providers held a series of wānanga to explore a range of issues related to Government use of cloud capabilities, including for Māori data stewarded by Public Service departments.

20 Informed by those discussions, and building on Te Mana Raraunga[6] Māori Data Sovereignty Principles, the call for Tino Rangatiratanga, Wai262, and partnership with the DILG and Te Kāhui Raraunga[7], the following principles for the Policy are proposed:

20.1 accountability: agencies responsible for Māori data have accountabilities to the communities, groups and individuals from whom the data derive;

20.2 ethics: tikanga, kawa (protocols) and mātauranga (knowledge) shall underpin the protection, access, and use of Māori data;

20.3 transparency: security and controls demonstrate care, trust, and due diligence to appropriately protect Māori data; and

20.4 collaboration: Iwi and Māori are involved in agency decisions about the sensitivity of Māori data and storage locations, including opportunities to improve governance for current and future generations.

[5] The agreement was signed by representatives from the DILG and DIA in 2021. It supports partnership in digital public services so that they are more responsive, accessible and enable better outcomes for Māori.
[6] https://www.temanararaunga.maori.nz/
[7] Te Kāhui Raraunga is the operational arm, a Charitable Trust, that works on behalf of Data Iwi Leaders Group.

21 We seek agreement that agencies consider the above principles when making decisions about adopting cloud. Building and strengthening relationships between the public service and iwi/Māori will be critical to supporting agencies' consideration of Māori expectations and interests as part of their cloud adoption.

22 Guidance to support the public service's capability to consider these principles is in development and expected to be completed by March 2023. This guidance has been developed in partnership with DILG and the guidance is expected to align to and be informed by the Māori Data Governance Model in development between Stats NZ and DILG.

23 While defining Māori data and Māori data sovereignty is outside the scope of the Cloud First Policy[8], Te Kāhui Raraunga's definitions and perspectives, such as on jurisdictional risk in relation to Māori data sovereignty, including a preference for storing Māori data onshore where practicable, will be presented as part of the guidance.

24 The linkages and relationships between the role of the GCDO, the Government Chief Data Steward (GCDS), Iwi and Māori and cloud providers is evolving. Digital and data are deeply connected, and it will be critical to ensure consistency with Te Tiriti across both systems, including on issues such as jurisdictional risk.

Sustainable use of cloud

25 In alignment with Government's aim to transition New Zealand to net-zero emissions economy, we recommend Cabinet agree to include consideration of high-level sustainability principles in the refreshed Policy. If utilised well[9], cloud offers the potential to contribute to achieving the carbon reduction aims of the Carbon Neutral Government Programme.

26 There is an opportunity to incorporate mātauranga taiao (environmental knowledge) into the Policy and support digital transformation in a way that promotes sustainability for future generations. To support this, we propose Cabinet direct officials from the Ministry for the Environment (MfE), Ministry of Business, Innovation and Employment (MBIE), and DIA to work with Iwi/Māori to develop high-level principles that would seek to encourage and support sustainable adoption and use of cloud.

27 Agencies have indicated their support to adopt cloud in sustainable ways but acknowledge the lack of guidance in this space. We propose to direct MBIE (Procurement System Lead) and DIA (Digital System Lead) officials to produce updated guidance in line with the high-level principles to support agencies to adopt cloud technologies in sustainable ways through their procurement activities.

Proposal Two: reflect evolving cloud technology by revoking the IaaS directive

28 In 2012, as part of accelerating the functional leadership for better public services, Cabinet directed agencies to use services from the IaaS panel agreement [CAB Min (12) 23/12 refers]. The intent was to encourage agencies to use common cross-government processes, tools or infrastructure and reduce investment in traditional in-house technology in favour of cloud. Much of the technology supplied through the IaaS panel agreements now conflicts with global definitions of public cloud and is creating confusion for agencies who are considering transitioning to cloud. We

[8] The development of a model for Māori data governance (MDG) is a Stats NZ and the DILG workstream.
[9] For example, by using more sustainable data centres or efficient use of cloud resources or applications.

recommend Cabinet revoke the directive to encourage the public sector to refocus on the "cloud first" objectives of the Policy.

Proposal Three: addressing cloud security concerns to support cloud uptake

29 Cloud services represent an opportunity to increase the digital capabilities of agencies. They can also reduce risk, increase resilience, and enable agencies to improve their security posture, for example through secure configuration, cloud monitoring and data protection. The policy refresh has identified three areas of cloud security that need to be addressed to allay concerns and support the secure uptake of cloud services. We are proposing to update how agencies manage jurisdictional risk, guidance for the cloud risk assessment process and how data centre certification is implemented.

Managing jurisdictional risk

30 Jurisdictional risk is the potential for foreign governments to compel access to, or interfere with, information stored in the cloud through their own legal frameworks. It is seen as a risk associated with the use of public cloud for hosting government data and may have contributed to the low speed of transition to cloud across government. It is important this risk is not overstated.

31 The level of jurisdictional risk can vary depending on:

31.1 the nature of the information being placed in the jurisdiction;

31.2 the type of service;

31.3 the ease with which an agency can bring information back to New Zealand; and

31.4 changes in legal frameworks or political leadership of a nation-State (which could affect their interest in gaining information about New Zealand Government activities).

32 Any jurisdictional risk needs to be considered alongside other risks and benefits relating to cloud. Using cloud services presents productivity, digital and service transformation, cost, and enables cyber security benefits.

33 DIA and Department of Prime Minister and Cabinet (DPMC) promulgated advice to government agencies on jurisdictional risk in 2017. Changes since 2017 have prompted us to review our position on jurisdictional risk, including major hyperscale providers building onshore capabilities in New Zealand, legal changes in some jurisdictions that New Zealand agencies use cloud services from, and a less benign geopolitical environment.

34 The updated advice on jurisdictional risk is the public service can continue to manage jurisdictional risks when using cloud services. Jurisdictional risk will very rarely be a conclusive reason to avoid cloud services.

35 We consider the main impact of jurisdictional risk relates to RESTRICTED information. Therefore, we are proposing to modify the Cloud First policy to include a policy preference that agencies use onshore cloud services for storing and creating RESTRICTED information as suitable onshore services become available. We note

this policy change would require a consequential amendment to the Protective Security Requirements (PSR) policy managed by the NZSIS.

36 This new policy preference will set a clear expectation with agencies that, while they continue to use and adopt cloud services for RESTRICTED and below, over time RESTRICTED information should be hosted in a New Zealand based cloud service, where possible. With the arrival of onshore hyperscale data centres, the balance of benefits and risks for different information may change.

37 Continued change in technology and geopolitics means up-to-date guidance on jurisdictional risk will continue to be needed. Without this guidance, concerns about jurisdictional risk may slow down, or stop cloud uptake. Therefore, we seek direction for DIA supported by the National Cyber Policy Office (NCPO), National Cyber Security Centre (NCSC) and the Ministry of Foreign Affairs and Trade (MFAT) to provide public service agencies with updated jurisdictional risk advice by August 2023, and with new advice being issued as required by changes in the geopolitical or legal environment, and at least every five years after that.

We need to streamline and improve the cloud risk assessment guidance

38 To manage risks and make good, informed decisions, agencies need support and guidance when taking up cloud services. The NCSC updated its advice and security requirements for public cloud in the New Zealand Information Security Manual (the NZISM) in September 2022 with a dedicated chapter for public cloud specific guidance and controls. This chapter supports agencies to understand shared responsibility models, security governance, data protection and security monitoring efforts in cloud.

39 Under the Cloud First policy, agencies are required to complete a risk assessment. We propose DIA and NCSC produce updated guidance to replace the current Cloud Risk Assessment tool (also known as the “105 questions”) to make it easier for agencies to understand and treat cloud risks in a consistent manner, by March 2023. The current tool is complex and we need to make it easier for agencies to understand and address cloud considerations so they can confidently take up cloud services.

Centralising data centre certification to support providers to meet requirements

40 A centralised certification process for new hyperscale[10] cloud data centres in New Zealand is under development. This new system will provide clarity on certification for hosting government data, with standardised requirements and an assessment tool to ensure consistency across providers. This process will help provide confidence in physical and personnel security posture, as well as mitigate against any ownership, control and supply chain risks.[11] We note each agency will still be responsible for accreditation and management of residual and agency-specific risks.

41 Continuing with the current decentralised approach would mean each agency would be required to undertake their own certification process. Although not mandatory, we expect providers and agencies will support the process as centralised certification

[10] Only onshore hyperscale providers i.e., large onshore data centres with public cloud characteristics, hyperscale capabilities, and requiring over 10MW will be covered by the new system. Existing certification with individual providers on a case-by-case basis will continue for others if required.

[11] Data centres can be privately owned and operated. Change to the effective control of the owner, operator or supply chains, may result in security implications. Overseas experience shows ownership and control of data centres are important considerations when assuring cloud data centres.

would enable streamlining of agency certification and accreditation processes, with reduced duplication of work. The costs of the centralised certification are expected to be met by providers (with the fee charged to providers based on the cost of the certification).

Proposal Four: strengthen the GCDO mandate for cloud digital investment

42 Legacy systems, in particular on-premise, can present multiple challenges, such as to security, continuity, resiliency and cost-effectiveness.[12] Maintaining effective and secure on-premise systems is possible but requires active and skilled management. The on-going range of historical and bespoke applications in the public sector, including those critical for service delivery, presents risks that should be surfaced.

43 In line with the "cloud first" default intent of the Policy, we propose an additional requirement that future investment in on-premise ICT infrastructure, whether new or from baseline, be on an exceptions basis. Investment in on-premise IT should be considered only when specified criteria[13] are met or with the approval of the GCDO.

44 The proposed default position of cloud over on-premise investment signals the need to consider and plan for transition from these systems rather than continually invest further for potentially less functionality, higher costs and risks.

45 There will be cases where continued, or new investment in on-premise infrastructure will be appropriate.[14] This proposed default position will support visibility of these issues and proactive consideration of whether there are other more appropriate cloud options.

46 In May 2022, Cabinet expanded GCDO's mandate over digital investment. This mandate, among other things, supports and enables the GCDO to drive strategically aligned decisions within specified categories and thresholds, to direct agencies to follow system investment priorities or adoption of cross-government processes, tools or infrastructure [CAB-22-MIN-0200]. This extension of GCDO's mandate to on-premise investment aligns with this direction, and the current mandate for agencies to have plans for the use of public cloud but provides more specificity as to the content of that plan. Therefore, we propose to extend GCDO's investment mandate to manage the approval of non-cloud technology under the refreshed Cloud First policy.

47 The proposal is not intended to conflict with the requirements and accountabilities of Ministers and chief executives under the Public Finance Act 2020 (PFA). The GCDO will continue to operate within the context of the PFA while providing clearer direction and support to agencies to achieve the aims of the Policy.

The refreshed Cloud First Policy

48 Building on existing requirements, the proposed additions to the Policy will require agencies to:

48.1 adopt public cloud services in preference to traditional ICT systems;

[12] While in 2022 the majority of systems were reported by agencies as operating adequately, there are concerns round the future operation for over half of systems, with more than 27% of systems being over 10 years old.
[13] The criteria will consider technical needs and capabilities, as well as operational and financial considerations.
[14] For example, unique environments and/or specialist systems such as at airports, overseas operations.

48.2 not invest in on-premise ICT infrastructure unless specified criteria are met or approved by the GCDO;

48.3 have a plan for how they intend to use public cloud services;

48.4 make adoption decisions on a case-by-case basis following a risk assessment;

48.5 consider Te Tiriti o Waitangi, Te Ao Māori, accountability, ethics, transparency and collaboration with Iwi and Māori, when making decisions about adopting cloud services particularly for Māori data;

48.6 make cloud adoption decisions which consider high-level sustainability principles;

48.7 only store data classified as RESTRICTED or below in a public cloud service; and

48.8 as a preference, over time, host RESTRICTED information in a New Zealand based data centre, where a suitable onshore service is available.

Phase Two: additional interventions to realise the outcomes of the Cloud First Policy

49 The proposals above will provide greater clarity and focus on the policy, as well as provide the guidance and tools to move to cloud appropriately, securely and effectively. However, the Cloud First Policy has been in place for a decade and successive governments have not yet fully realised the benefits from cloud-based digital transformation of the public service. It is our opinion policy alone will not be sufficient to move the dial on cloud uptake.

50 To comprehensively realise the benefits of the Policy, consideration of other possible interventions and investment in cloud is needed. Possible areas of further work include consideration of centralised support (technical and financial) for prioritisation and sequencing of cloud transitions and interventions to support upskilling of the public sector in cloud technologies and operating models.

51 We are seeking Cabinet agreement for the Minister of the Digital Economy and Communications and the Minister Responsible for the Government Communications Security Bureau to carry out further work, informed by Phase One, to assess interventions and investment to address barriers to cloud adoption across the public service.

Implementation

Phase One: The proposals for refreshing the Cloud First Policy

52 For proposals one to three, the GCDO will communicate the changes to agencies and suppliers, provide refreshed guidance and tools and support agencies on a case-by-case basis as they adopt cloud services.

53 For proposal four, the GCDO will communicate the new expectations regarding on-premise infrastructure investment for the next budget/financial year (2023/24). The GCDO will undertake a stocktake of current and proposed on-premise investment. This would build on information already known to the system, such as through the

annual investment intentions survey, and seek additional information from agencies where there are gaps. GCDO will engage with agencies to understand where on the cloud adoption path they are, provide guidance to support planning/transition, and what future support may be required.

Phase Two: additional interventions to realise the outcomes of the Cloud First Policy

54 Subject to Cabinet approval, the Minister for the Digital Economy and Communications and the Minister Responsible for the Government Communications Security Bureau will instruct officials to begin work to develop additional interventions and possible investment to address barriers to cloud uptake. This will include working closely with stakeholders including central government agencies, DILG and other Iwi and Māori representatives and industry.

Financial Implications

Phase One: The proposals for refreshing the Cloud First Policy

55 There are no immediate financial implications associated with this paper. The proposals (e.g. guidance) outlined in the refreshed Policy will be managed out of baseline for each agency involved, except the centralised data centre certification process, which is expected to be implemented based on recovery of costs of certification from providers.

56 However, these proposals will require agencies to apply the Policy to their Digital and ICT strategies and there may be implications to delivery from within existing baselines.

57 A broad range of agencies have noted constraints of the current CAPEX IT investment model slowing transitions to the OPEX cloud consumption model. The cost of migrations, where legacy and cloud systems may need to operate in parallel for a period exerts pressure on baselines and decisions to adopt, or not adopt, cloud. The scarcity of cloud skills within the public and private sector can also impact on an agency's ability to apply the Policy.

58 The consideration of the preference, over time, for RESTRICTED information to be hosted in New Zealand based data centres where a suitable service exists, could have financial implications. Hyperscale cloud providers are not yet operating onshore and when services commence, it is likely to take time before a wide range of services are available. It may be onshore hosting of information will prove to be more costly than offshore services. However, by signalling this preference now, agencies will also have the opportunity to design their systems and contracts in anticipation of possible movement of data onshore.

Phase Two: additional interventions to realise the outcomes of the Cloud First Policy

59 There are no immediate financial implications associated with Phase Two. However, identifying broad outcomes and possible levers for change will outline whether investment is needed to address the challenges affecting public service adoption of cloud technologies. Transformational change is unlikely to occur without some additional investment, even if temporary and there may be financial impacts from the decisions made by agencies.

60 The paper makes assumptions about the availability of new funding in future Budgets. If assumed funding is not included in the Budget package, elements of

Phase Two will need to be funded through reprioritisation of affected agencies' existing baselines or reconsidered.

Legislative Implications

61 The proposals in this paper do not have any legislative implications.

Impact Analysis

Regulatory Impact Statement

62 A Regulatory Impact Analysis is not required for this paper.

Climate Implications of Policy Assessment

63 The Climate Implications of Policy Assessment (CIPA) team has been consulted and confirms the CIPA requirements do not apply at this stage as the threshold for significance is not met. Any emissions impacts will be reassessed and disclosed to Cabinet following the outcome of the investigation.

Population Implications

64 The proposed Policy refresh, and phase two approach have no direct impacts on population groups. However, the benefits it confers to public services are expected to have positive flow on effects to any businesses and individuals who interact with those services. This covers a broad range of demographics but is likely to disproportionately affect Māori, Pacific, and other minority groups, especially individuals from lower socio-economic backgrounds through their interactions with various public services.

65 The benefits to population groups will likely compound over time as agencies learn to better utilise cloud to provide services more efficiently and take advantage of technology developments. More work would need to be done to properly establish the impacts on population groups.

Human Rights

66 There are no human rights implications resulting from the decisions in this Cabinet paper. Work undertaken as a result of decisions made will be designed to be consistent with the New Zealand Bill of Rights Act 1990, Human Rights Act 1993 and Privacy Act 2020.

Consultation

67 The following agencies were consulted on this paper: Accident Compensation Corporation (ACC), DPMC, Inland Revenue (IR), Kāinga Ora, Land Information New Zealand (LINZ), MBIE, Ministry of Education (MoE), MfE, MFAT, Ministry of Justice (MOJ), Ministry for Primary Industry (MPI), Ministry of Social Development (MSD), New Zealand Customs Service (NZCS), New Zealand Defence Force (NZDF), New Zealand Police (NZP), New Zealand Transport Agency (NZTA), Oranga Tamariki, Parliamentary Service, Public Service Commission (PSC), Stats NZ, Te Arawhiti, Te Puni Kokiri (TPK), Te Whatu Ora (HNZ) and The Treasury.

68 The majority of agencies endorsed the general direction and support for public cloud adoption. There was strong interest and support for guidance in how agencies should approach Māori data, the improved cloud risk assessment guidance as well as the centralised data centre certification process. The proposed additional GCDO mandate was considered useful in providing a clear signal discouraging on-premise investment and the expected shift in mindset. As the position recognised there are unique needs of agencies that will allow for on-premise investment, no agency indicated concern the mandate will create substantial difficulties.

Communications

69 A public launch of the Cloud First Policy Refresh is planned for the second quarter of 2023. This would be an opportunity to refocus the public sector on cloud, engage with providers and the public on the benefits of cloud while also acknowledging potential concerns and tools for mitigation.

70 GCDO, with the support of relevant agencies, will host a public sector focussed event to lift understanding of cloud, the Policy, guidance and tools available. The refreshed policy will also be disseminated via other channels, such as digital.govt.nz and the Cloud Capabilities Network community of practice.

71 Communications will also aim to ensure the Policy remains distinct from other issues it may be linked or confused with, such as data sovereignty, Māori data sovereignty, digital identity, use of data for artificial intelligence or development of algorithms, and questions around the private sector's, including large multinationals, use of data. Frequently asked questions will be prepared and shared with agencies to support engagement with the public and communities.

Proactive Release

72 In accordance with Cabinet Office Circular CO (18) 4 – Proactive Release of Cabinet Material: Updated Requirements, we intend to proactively release this paper on the Department of Internal Affairs' website, subject to any redactions that may be warranted under the Official Information Act 1982, within 30 business days of Cabinet decisions.

Recommendations

73 The Minister for the Digital Economy and Communications, and the Minister Responsible for the Government Communications Security Bureau recommend the Committee:

Background and potential benefits of cloud computing for the New Zealand public service

1 **note** agencies face several interdependent and complex challenges when considering cloud adoption;

2 **note** if the public service is not supported to invest in and adopt cloud services there is a risk the potential benefits of cloud computing will not be realised;

3 **note** the Cloud First Policy has become diluted in focus and policy does not reflect changes in technology, society or government priorities;

Phase One: Proposals for a refreshed Cloud First Policy

4 **note** the refresh of the Cloud First Policy represents a significant opportunity to include Te Ao Māori perspectives and would represent a world first for incorporating indigenous considerations into national cloud policies;

5 **note** if utilised well, cloud offers the potential to contribute to achieving the carbon reduction aims of the Carbon Neutral Government Programme;

6 **note** that the 2012 directive on the use of Infrastructure-as-a-Service is out of step with technological change and policy aims;

7 **note** addressing security, including jurisdictional risk concerns, actual and perceived, would support cloud adoption;

8 **note** legacy, on-premise infrastructure can pose challenges to management of security risks, transformation of service delivery and transition to cloud;

9 **note** that the proposals in the paper are not intended to conflict with the Public Finance Act 1989 requirements related to responsibilities and accountabilities of Ministers and chief executives;

Cloud First Policy

10 **reconfirm** the existing Cloud First Policy, that directs agencies to:

10.1 adopt public cloud services in preference to traditional ICT systems;

10.2 have a plan for how they intend to use public cloud services;

10.3 make adoption decisions on a case-by-case basis following a risk assessment;

10.4 only store data classified as RESTRICTED or below in a public cloud service;

11 **agree** that agencies consider accountability, ethics, transparency, and collaboration in relation to Māori data, when making decisions about adopting cloud services;

12 **agree** that agencies make adoption decisions which consider high-level sustainability principles in the public sector's use of cloud;

13 **agree** to revoke the 2012 Infrastructure-as-a-Service directive to provide greater clarity to the Cloud First Policy;

14 **agree** that over time RESTRICTED information should be hosted in a New Zealand based data centre, where a suitable onshore service exists;

15 **agree** that agencies will not invest in on-premise ICT infrastructure unless specified criteria are met or approved by the Government Chief Digital Officer (GCDO);

Implementation

Reflect societal shifts and commitment to government priorities

16 **note** the Department of Internal Affairs, in partnership with Statistics NZ and the Data Iwi Leaders Group, is working on guidance to support the public service's capability to give effect to Māori interests when making decisions about adopting cloud;

17 **direct** officials from the Ministry for the Environment, Ministry for Business, Innovation and Employment, and Department of Internal Affairs to work in association with Iwi and Māori to develop high level principles to encourage and support sustainable adoption and use of cloud technologies;

18 **direct** officials from the Ministry of Business, Innovation and Employment, and Department of Internal Affairs to produce updated guidance in line with the high-level principles to support agencies to adopt cloud technologies in sustainable ways through their procurement activities;

Addressing cloud security and jurisdictional risk concerns to support cloud uptake

19 **direct** the GCDO, supported by the National Cyber Policy Office, National Cyber Security Centre and Ministry of Foreign Affairs and Trade to produce updated guidance to agencies on jurisdictional risk of cloud by August 2023, and thereafter as needed, and at least every five years;

20 **note** the creation of a centralised certification process for onshore hyperscale data centres to provide confidence to providers and agencies that the facilities have appropriate physical and personnel security, as well as ownership and contractual requirements to host RESTRICTED and below information;

Strengthen GCDO mandate for cloud digital investment

21 **note** that the GCDO will undertake, with agencies, a stocktake of current and planned expenditure within specified criteria regarding on-premise infrastructure, provide regular reporting on progress and support agency transition to cloud;

Phase Two: additional interventions to realise the outcomes of the Cloud First Policy

22 **note** the challenges of limited capacity and capability, financial resourcing and system-wide prioritisation remain;

23 **invite** the Minister for the Digital Economy and Communications and the Minister Responsible for the Government Communications Security Bureau to carry out further work and report back to Cabinet by April 2024 with options to address these challenges;

24 **note** further detailed investigation will seek to address barriers raised by agencies and will include estimating different levels of intervention and investment required;

25 **note** that delivery of some elements of Phase Two of the Cloud First Policy will require funding through future Budgets for affected agencies, and if assumed funding is not included in future Budget packages, elements of Phase Two of the Cloud First Policy will need to be funded through reprioritisation of existing baselines or reconsidered; and

26 **note** officials will undertake targeted engagement with agencies and relevant groups such as the Data Iwi Leaders Group and other Iwi and Māori representatives and industry to inform the work referred to in recommendation 23.

Communication of refreshed policy

27 **note** the GCDO will lead, supported by relevant agencies, engagement with the public sector and providers on the refreshed Cloud First Policy;

28 **note** communication of the refresh will include explaining the benefits of cloud, acknowledging potential concerns and highlighting tools for mitigation while drawing a distinction between the Policy and other issues outside the scope of the refresh.

Section 9(2)(f)(iv)

Section 9(2)(f)(iv)

Authorised for lodgement

Hon Minister Little

Minister Responsible for the Government Communications Security Bureau

Hon Ginny Andersen

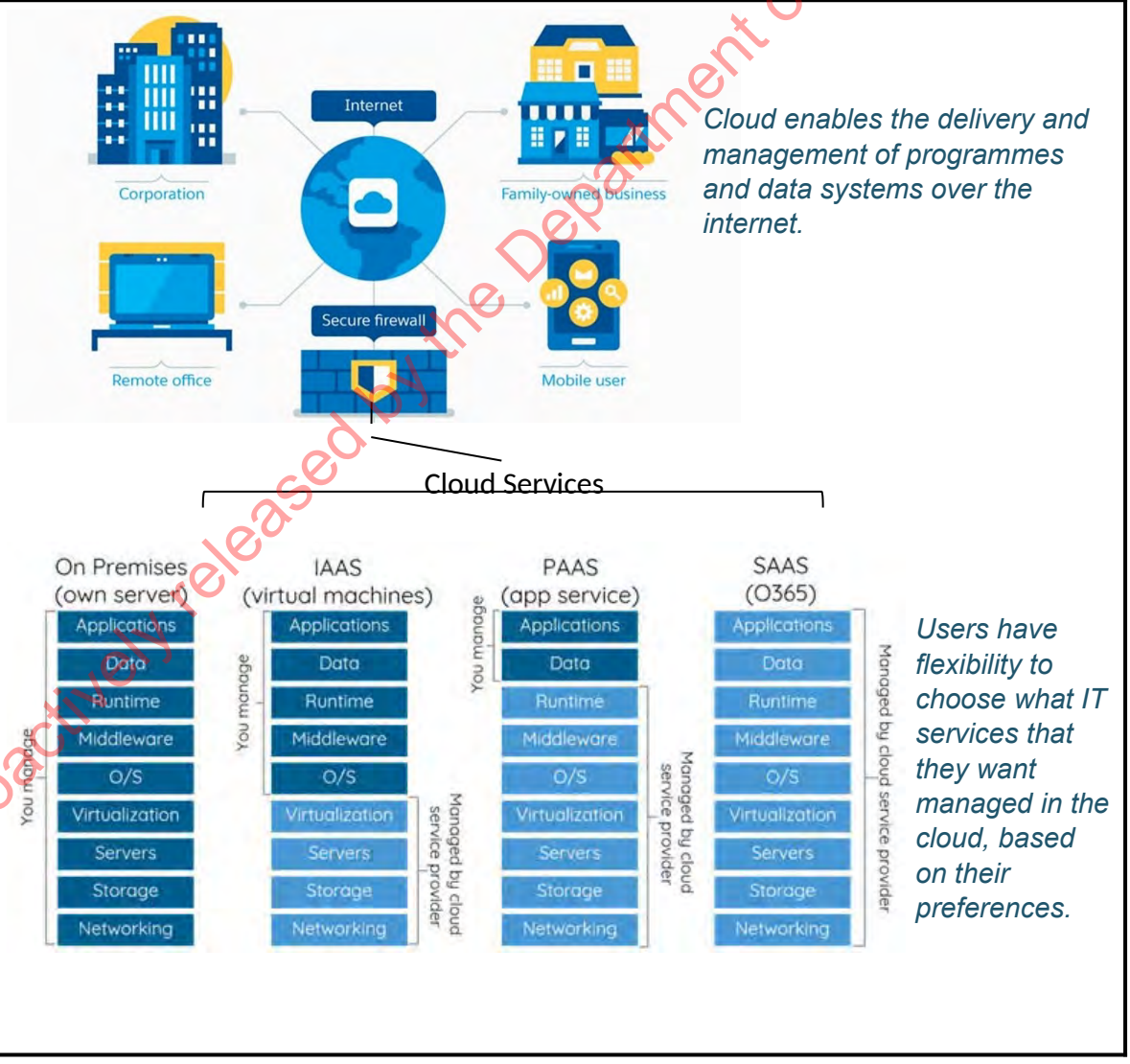
Minister for the Digital Economy and Communications

Appendix A: Defining Cloud Computing

Cloud computing

1 The National Institute of Standards and Technology (NIST), United States Commerce Department, defines cloud computing (cloud) as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable Information Technology (IT) resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction".[1]

2 NIST's definition outlines the cloud model is composed of five characteristics (on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service), three service models (Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) and four deployment models (public, private, community, and hybrid). The image below depicts how cloud works and shows an example of a shared responsibility model:



[1] NIST's Special Publication 800-145 refers: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

Service models[2]

Infrastructure as a Service

3 IaaS is a capability provided to the consumer to provision processing, storage, networks, and other fundamental computing resources where the consumer can deploy and run software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

Platform as a Service

4 PaaS is a capability provided to the consumer to deploy onto the cloud infrastructure, applications (consumer-created or acquired) created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage. However, the consumer has control over the deployed applications and may control configuration settings for the application-hosting environment.

Software as a Service

5 SaaS is a capability provided to the consumer to use the provider's applications running on a cloud infrastructure. The applications are accessible from various devices through either a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, except for limited user-specific application configuration settings. For example, Web-based email and Google Documents or Microsoft Office 365 are all SaaS.

Deployment models

Public

6 The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

7 Public Cloud services are those offered widely through the Internet and available to anyone who wants to purchase them. Typically, these services are made available by large service providers who are offering IaaS, PaaS and SaaS products. Examples: Microsoft Azure / Microsoft 365, AWS, Google Cloud.

Private

8 The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

[2] https://csrc.nist.gov/glossary See also https://www.digital.govt.nz/standards-and-guidance/technology-and-architecture/cloud-services/

9 Private Cloud services are only available to a specific/defined set of users who are on a private, internal network, or a network for their organisation run over the Internet using security controls to separate it from the public Internet environment.

Community

10 The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

Hybrid

11 The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

12 Hybrid Cloud is not simply a mixture of public and private cloud resources to run your workloads, it is about providing a connected cloud experience. Many agencies often use hybrid cloud to build in resilience and Disaster Recovery capability etc.

Other

Multi-cloud

13 Multi-Cloud is the deliberate use of multiple cloud computing and storage services from multiple public cloud providers for the same general class of IT solutions or workloads (e.g., AWS, Azure, GCP) in a single joined-up architecture. This also refers to the distribution of cloud infrastructure assets, software, applications, etc. across several cloud-hosting environments. It is much more common in infrastructure as a service (IaaS) and converged IaaS/platform as a service (PaaS) scenarios than SaaS.

Appendix B – Benefits of cloud computing and New Zealand case studies

The potential benefits of cloud computing (cloud) for the public sector are significant

Security	Cloud enables agencies to more easily improve their security posture, security architecture, and detect and contain threats than traditional (on-premise/in-house) approaches to Information Technology (IT). Cloud also supports responding to volume-based cyber-attacks at scale.
Scalability	Cloud services, particularly hyperscale cloud, can be quickly and easily scaled and reduced to meet changing demands.
Service delivery transformation	Cloud enables digital transformation of delivery models, allowing agencies to focus resources on improved, innovative, and more timely delivery of services to citizens and businesses.
Efficiency and productivity	Users benefit from significant efficiency through economies of scale, freeing up resources to deploy to other priorities.
Managing greenhouse gas (GHG) emissions	Cloud and hyperscale data centres typically have high operational efficiency for energy demand. Global demand for data services has grown exponentially and accounts for 1% of electricity demand. Energy efficiencies, research and development, and demonstration and renewables procurement are essential to curb both energy demand and emissions growth.[1]
Agility and distributed working	Users can securely access systems from wherever there is an internet connection, via an internet-capable device. Users can more easily work across teams and organisations, through multiple means (voice, chat, video-chat, document).
Continuity and resilience	Business continuity is more assured through the ability to back up and quickly recover data systems.
Flexibility	Users can more easily switch between providers and services, depending on their needs.
Insight and intelligence	Through advanced analytics, providers can offer better insight and intelligence at the aggregate user levels, about data use, risk and opportunity.
Innovation	Advanced, effective, and sustainable technology innovations are increasingly being built from the cloud.
Control	Onshore cloud provides stronger control as the data is located within New Zealand's jurisdiction.
Financial	Potential for reduced capital outlay as cloud hardware is maintained by the cloud service provider. This benefit is particularly associated with public cloud deployment models which offer significant economies of scale.

[1] Data Centres and Data Transmission Networks – Analysis - IEA

Why is cloud considered more secure?

1 Cloud does have a number of attributes that can make it less secure than more traditional approaches to IT. These include:

1.1 lack of control over the systems holding and processing your data;

1.2 cloud capabilities being directly accessible over the (insecure and hostile) Internet;

1.3 the rapid rate of change and the complexity of cloud environments can make it hard to maintain and assure security; and

1.4 a false sense of security can arise from an (incorrect) assumption that responsibility for security belongs with the service provider.

Cloud can be more secure…

2 Depending on the cloud provider, cloud services can be more secure than traditional in-house IT. There are two aspects of improved security available from cloud services:

2.1 How well the cloud services are secured – i.e. As Amazon Web Services refers: "security of the cloud".

2.2 The capabilities available to customers to secure their specific cloud environments – i.e. "security in the cloud".

3 Using cloud enables agencies to focus their limited security resources on security in the cloud. Cloud services, particularly cloud provided by large public cloud providers, also have a number of benefits that can offset the 'less secure' attributes. These are set out below.

4 ***Cloud providers use consistent, repeated technology in building their services:*** Concentrating on securing a relatively small amount of different technology components means deeper, consistent security on narrow services, rather than thin security on a wide variety. It also means that expertise about these services can be built up and shared across agencies and projects as staff learn secure approaches and how to replicate them.

5 ***Consistent patching and security management practices:*** keeping systems up to date is both one of the most critically recognised security controls, and widely accepted as difficult to do well in-house. Cloud services homogeneity, and asset management tools make it easier and faster to patch and update systems, and to have good visibility of current software versions being used.

6 ***Incremental security improvements are easier:*** security services are built into the cloud platforms, not added later, and as such are easier to adapt and change over time.

7 ***Talented cyber security professionals are attracted to work in cloud:*** due to the investment being made in security, the focus, and the innovation being used in cloud services, cloud providers can make a compelling case for attracting candidates in the competitive cyber security market.

8 ***Regulatory compliance:*** cloud operators must comply with various regulatory frameworks and laws of countries they operate in. While this brings with it jurisdictional risk, there are also significant benefits to consumers from the investment cloud providers make to meet these standards. The consistent technology used to build a cloud provider's platform ensures that some countries regulatory standards can be met for all customers (not limited sets) and also drives the regulatory bodies towards developing more consistent security standards.

9 ***Increased cyber resilience:*** cloud platforms are highly visible and valuable targets that are constantly tested for vulnerabilities, leading to more refined defensive and detection capabilities rapidly evolving through their services. Threat actors and security teams are in a constant arms race, with the lowest cost (in terms of time and effort) systems typically being compromised first. Cloud providers implement tiered defence strategies across standardised services leading to a consistent security posture without weak points.

And cloud's security should be compared to current state

10 The claim that cloud is "more secure" can seem counter intuitive. However, "more secure than what?" is a key part of assessing cloud security. Overall, the public service has a low cyber security maturity, many agencies have limited IT and cyber security resources, and are undergoing service and digital transformations.

11 When compared to the complexity, costs and expertise required to upgrade security in legacy IT environments, cloud enables agencies to leverage secure-by-design services to more easily improve their security posture, security architecture and detect and contain threats.

12 However, security of the cloud comes down to selecting a good cloud provider, and implementing and maintaining good security controls.

New Zealand case studies from public sector

13 A selection of successful case studies are outlined below, demonstrating the public sector optimising the benefits of cloud. Cloud computing was found to be particularly important during COVID-19 lockdowns. One of the key digital capabilities that were observed in agencies better placed for remote working during COVID-19 lockdowns was a higher level of adoption of cloud services. It is critical that this momentum and key insights on agency resilience are not lost.

Agency	Case study
Inland Revenue • Service Delivery • Scalability • Continuity, and Resilience	Inland Revenue's (IR) previous investment in becoming a digitally enabled workplace positioned them well to keep business running, manage customer demand and support the government's response during COVID-19. At the time of the Kaikōura earthquake in November 2016, IR wasn't set up to respond to disruption — few people had mobile devices and even fewer could connect to systems at any one time. The operating model had been people in a room with a whiteboard. By contrast, during the COVID-19 lockdown, IR held virtual design meetings every day with people in at least 3 agencies, as new services and products were designed and implemented to support the government's response.
Oranga	Oranga Tamariki (OT) was able to take advanta ge of being a new

Tamariki • Efficiency and productivity • Service Delivery • Scalability, continuity, and resilience	agency by starting afresh without legacy technology issues and take advantage of cloud technology as a 'cloud native'. OT was able to benefit from the efficiency and productivity of cloud which allowed them to focus on delivering business value rather than maintaining legacy technology. Cloud enabled a seamless transition without the need for expensive configuration or specialised connectivity to data centres. From day one of the lockdowns, all 6000 OT staff were able to work from home. This meant that staff productivity was not compromised, and OT continued to provide critical services to tamariki and whānau in the communities. OT was able to utilise the on-demand elasticity potential of cloud to scale up the capacity of the Contact Centre cloud platform overnight from 250 to 800/1000 users, providing the Ministry of Business, Innovation and Employment (MBIE) with a channel for the COVID-19 response. Once MBIE had established their own contact centre, the platform was scaled back down to 250 users.
Ministry of Housing and Urban Development • Service Delivery • Scalability, • Continuity, and Resilience • Innovation	The Ministry of Housing and Urban Development (HUD) similarly leveraged its cloud capabilities during COVID-19 and adapted its use of digital tools to continue core business and connect remotely in new ways. As a new organisation, HUD experienced the benefits of being relatively 'cloud native' and were able to adapt quickly during lockdowns due to a modern workplace environment. COVID-19 presented HUD with the opportunity to start using a wider range of functions of the digital tools available to them but not previously used. The experience boosted connection and challenged people's thinking about how they could use their tools differently, rather than just sitting in the office with a device and a headset.
Ministry of Health • Service Delivery • Continuity and Resilience • Innovation	The Ministry of Health is fairly mature in their cloud adoption and is interested in looking at whether a hybrid cloud deployment approach would meet their service needs in the future. The COVID-19 lockdown in particular demonstrated the service delivery benefits of cloud, and allowed MoH to quickly develop solutions, such as the national vaccine booking system, that were oriented around customer service while supporting the government's overall response.

Appendix C: Summary of proposed changes to the Cloud First Policy

1 Subject to Cabinet agreement to the proposals outlined in the Cabinet paper, the following additions will be made to the existing Cloud First Policy.

Proposed Cloud First Policy

2 The Policy will require public sector agencies to:

2.1 adopt public cloud services in preference to traditional ICT systems;

2.2 not invest in on-premise ICT infrastructure unless specified criteria are met or approved by the GCDO;

2.3 have a plan for how they intend to use public cloud services;

2.4 make adoption decisions on a case-by-case basis following a risk assessment;

2.5 consider Te Tiriti o Waitangi, Te Ao Māori, accountability, ethics, transparency and collaboration with Iwi and Māori, when making decisions about adopting cloud services particularly for Māori data;

2.6 make cloud adoption decisions which consider high-level sustainability principles;

2.7 only store data classified as RESTRICTED or below in a public cloud service; and

2.8 as a preference, over time, host RESTRICTED information in a New Zealand based data centre, where a suitable onshore service is available.

Supporting arrangements

He Aratohu Kapua | Cloud Toolkit

3 Under DIA's Mana Ōrite agreement, officials from DIA and Stats NZ have worked in partnership with Te Kāhui Raraunga (representing the Data Iwi Leaders Group[1]) on the development of guidance for agencies in their consideration of cloud.

4 The toolkit outlines steps agencies can take to build their capability to understand te ao Māori perspectives on cloud, to build their relationships with Iwi and Māori and consider how Māori interests are reflected in decisions related to cloud service adoption or use. It will be a living document that will evolve with the development of the Māori Data Governance model.

High level sustainability principles

5 Subject to further development between agencies and Iwi and Māori, the expectation is the initial principles would be flexible to allow requirements to become more prescriptive as work in this area progresses. Methodologies to measure environmental impacts, critically for emissions, are essential for enabling

[1] Data Iwi Leaders have authority to represent National Iwi Chairs Forum in respect of digital and data kaupapa.

organisations to understand and manage the environmental impact from cloud services and technologies. This is important for Carbon Neutral Government Programme participants, the industry, as well as the wider economy.

Transition from IaaS

6 The IaaS panel agreements will expire in 2026 and 2027. It is recognised it will take several years for some agencies to fully transition to cloud services, and there will be some instances where IaaS services are still required beyond expiry of the current agreement.

7 A project to design a replacement for the IaaS panel agreements that has a more flexible set of arrangements as well as a common approach to support agencies using cloud services has been initiated. This project will provide a pathway to continue IaaS services beyond the current agreements and a managed transition to cloud services, thereby ensuring continuity and reliability in the service. Design of the new service will be completed by June 2023, with implementation to follow.

8 Officials advise replacing the IaaS agreements will not significantly impact agency ability to use cloud services. This is because agencies typically require a wider range of services than those available from the IaaS panel agreements and there are multiple all-of-government commercial options currently available to agencies for this.

Cloud Security Guidance: Cloud Risk Discovery Tool

9 Before agencies move to cloud, they must undertake a risk assessment. Guidance is provided in the Cloud Computing Information Security and Privacy Considerations (2014). Accompanying this document is a Cloud Risk Assessment (CRA) tool in the form of an excel spreadsheet covering the questions used as a prompt for gathering the information needed for agencies to assess their risk. Officials from DIA, in consultation with NCSC will produce an updated and streamlined Cloud Risk Discovery Tool to better support agencies.

10 In addition to security issues and the expected new jurisdictional risk preference, the new tool and accompanying guidance will also support agencies to understand and manage other considerations and risks, including:

10.1 *Privacy Act 2020:* With support from the Office of the Privacy Commissioner (OPC), Government Chief Privacy Officer guidance is expected to be available by March 2023. It should be noted that the Privacy Act 2020 does not reflect the Te Ao Māori concept of collective identity.

10.2 The Privacy Impact Assessment (PIA) toolkit (2015) does not refer to the updated privacy principles from the Privacy Act 2020, including the new Privacy Principle 12 (relating to offshore disclosures of personal information). The PIA includes some references to Cloud and the Office of the Privacy Commissioner (OPC) is planning to make a small update to the toolkit in the near future.

10.3 *Public Records Act 2005:* The refreshed tool will also support agencies to meet their obligations under the Public Records Act, including directing agencies to more detailed guidance where needed.

11 Updated jurisdictional risk guidance for agencies will also be developed by DIA, supported by NCPO, NCSC and MFAT.

Data Centre Certification

12 By March 2023, a finalised certification process, cost model, and standardised legal certification agreement are planned to be ready for implementation. Certification is expected to be funded by fees paid by providers (based on the cost of delivering certification) and could be scaled up in the event providers seek expansion. DIA, supported by subject matter experts from GCSB, NZSIS and OIO, will be the Certification Authority.

13 The design of the system has drawn on the Australian Hosting Certification Framework as well as insights from the UK Centre for the Protection of National Infrastructure. Engagement with key agencies (GCSB, NZSIS, DPMC, DIA, OIO, MBIE, NZDF) and providers was also undertaken.

Establishment of monitoring and reporting

14 The Government Chief Digital Officer's (GCDO) mandate to collect information from all government departments on their digital investment was strengthened in March 2022 [GOV-22-MIN-002].

15 The establishment of the Digital Investment Office (DIO) will support the development of solid baseline data for monitoring and reporting, and ongoing work to form an evidence base for future system-wide prioritisation of investment.

Refreshed definitions of what constitutes cloud services

16 A refresh of definitions has been completed as part of the redesign of the cloud guidance on Digital.govt.nz. These definitions are based on and reference the widely accepted National Institute of Standards and Technology (NIST), United States Commerce Department definitions.

Cloud Capabilities Network (CCN)

17 Public sector capability and capacity to transition to cloud has been identified as a significant barrier. The CCN is a community of practice aimed at supporting and growing public sector cloud knowledge and capability. It is vendor agnostic and hosts case studies, training events and other information sharing events.