IN-CONFIDENCE

Office of the Minister of Internal Affairs

Cabinet Committee on State Sector Reform and Expenditure Control

ACCELERATING THE ADOPTION OF PUBLIC CLOUD SERVICES

Proposal

1. The purpose of this paper is to seek agreement to a range of measures to accelerate the adoption of public cloud computing services.

Executive summary

2. In October 2015, Cabinet directed the Government Chief Information Officer (GCIO) to work with the New Zealand Intelligence Community (NZIC) to review how to accelerate the use of cloud computing within the public sector.

3. The GCIO and the NZIC have worked collaboratively to identify opportunities to accelerate the use of public cloud services in a way that balances opportunity and risk. The review focused on public cloud services – cloud computing services used by multiple organisations from different industries, including private and government sectors – because they have economies of scale that reduce costs and generally improve resilience and security compared with other technology delivery models.

4. Since Cabinet approval of the use of cloud services in 2012, public cloud services have become a mainstream technology choice for private sector enterprises globally. While most agencies recognise the benefits of public cloud services they are not fully exploiting this opportunity, largely because of the risks associated with these services and a lack of capability to systematically adopt public cloud services.

5. The review found that there are a number of complex and inter-related challenges that are inhibiting agencies from accelerating their adoption of public cloud services. A comprehensive twelve-month programme is required to accelerate the adoption of these services in a balanced way (as outlined in **Appendix A**). This programme will complement the existing policies and cloud risk assessment processes that provide checks and balances for agencies' use of public cloud services.

6. I expect to see the following outcomes from this programme:
   - senior leaders increasingly use public cloud services in a balanced way to drive digital transformation;
   - public servants increasingly use public cloud services to deliver new services; and
   - agencies have frameworks and skills to adopt public cloud services securely.

7. Ministers can play an important role in accelerating the adoption of public cloud services by removing the restriction on offshore-hosted office productivity services and requiring agencies to have a plan for how they intend to use these services.

8. The GCIO will continue to work with other agencies to re-allocate existing resources to this programme and will provide progress reports to Cabinet through existing reporting mechanisms used by the GCIO and as part of agency assurance reporting against the Protective Security Requirements (PSR).

Background

9. Public cloud services have now become a mainstream technology choice for private sector enterprises worldwide. It is now widely recognised that security is the core concern of global cloud services providers and that their services are typically more secure than traditional deployments of IT systems.

10. The most well-known public cloud services are provided by global suppliers such as Amazon, Google, Microsoft, and Salesforce.com. These suppliers have leveraged global scale to provide IT services that can be used across multiple industries. This has led to a proliferation of innovative and specialised cloud services that in turn are digitally transforming enterprises.

11. Public cloud services are increasingly being purchased by business units within enterprises. This is often driven by employees seeking to replicate their consumer experience by using public cloud services within their workplaces. The use of these services often bypasses corporate controls such as IT change management, legal, security, and procurement – a phenomenon known as 'shadow cloud'. While this can appear to meet immediate business needs it is often at the cost of a thorough assessment of risks.

Previous Cabinet decisions

12. In response to the opportunity and risks of adopting public cloud services, Cabinet directed agencies in August 2012 to adopt these services in preference to traditional IT systems, with the exception of office productivity public cloud services which, "for the time being", were not permitted to be hosted offshore [CAB Min (12) 29/8A]. In October 2013 Cabinet directed agencies to make adoption decisions on a case-by-case basis following a formal risk assessment. In addition, no data classified above RESTRICTED was permitted to be stored in a public cloud service [CAB Min (13) 37/6B]. Cabinet also agreed to incorporate the cloud risk assessment process into the system-wide ICT assurance framework [CAB Min (13) 20/13].

13. In 2014, the GCIO published guidance (*Cloud Computing Information Security and Privacy Considerations*) to support agencies to systematically identify, analyse and evaluate the information security and privacy risks associated with individual public cloud services. This includes guidance on information classification, data sovereignty, privacy, legal, and security controls.

Cabinet direction to accelerate adoption of public cloud services

14. The October 2015 *Government ICT Strategy* signalled that agencies would outsource their IT functions using common capabilities and public cloud services. To support this Strategy, Cabinet directed the GCIO and the NZIC to work together to review the 2012

cloud services policy and remove any barriers that may inhibit the accelerated adoption of cloud services [CAB-15-MIN-0148.01].

15. The review focused on accelerating the adoption of public cloud services – services designed to be used by multiple enterprises across different industries, including private and government sectors. These services are typically hosted outside New Zealand and provided by suppliers that have global economies of scale. This enables these services to be more innovative, and to have lower costs and improved security compared to on-premises deployment of traditional ICT systems.

16. The GCIO has worked collaboratively with the NZIC to identify potential 'accelerators' – opportunities to appropriately accelerate the adoption of public cloud services. In particular, the GCIO and the NZIC have been mindful of the need to balance the benefits of public cloud services with the need to ensure that agencies appropriately adopt these services so that the risks are understood and managed.

Most agencies are not fully exploiting public cloud services

17. Agencies are clear about the key benefits of public cloud services: reduced costs for IT services, increased agility from quicker deployment times, and improved security for many agencies (particularly from global suppliers). Yet agencies generally adopt cloud in a tactical and opportunistic way, with adoption typically driven by non-core functions, such as human resources, finance, and communications (e.g. e-recruitment and online surveys). Most senior leaders have yet to use public cloud services to drive digital transformation – major business improvements to enhance customer experience, streamline operations, or create new delivery models. The challenges faced by agencies in taking a more strategic approach are described in paragraphs 21-28.

18. Early adopters of public cloud services tend to be small in size, have a single business function, and have few legacy IT systems. For example, Callaghan Innovation and New Zealand Fire Service use public cloud services to support many of their business functions. Other agencies tend to use a mix of onshore IT systems and offshore public cloud services to cater for the different risk profiles of their respective business functions, a mix which is likely to continue for the foreseeable future. For example, while the Department of Internal Affairs supports many of its business functions using traditional IT systems hosted in New Zealand data centres (e.g. passports and citizenship) it also uses public cloud services for an increasing number of business functions (community grants and the National Library's bibliographic database). In contrast, agencies with national security functions tend to limit the use of public cloud services to a small number of corporate services functions.

19. Early adopters recognise that the future IT operating model will be very different from the traditional 'design, build, operate' approach. There is a consensus that the skillsets and focus of IT roles will significantly change and IT frameworks will need to be modernised. The local IT supply market currently has limited capacity to support this.

20. For a variety of reasons, most agencies have used some public cloud services without visibility at the corporate or governance level of the extent and nature of their shadow cloud risks. The GCIO has advised agencies to implement security controls and practices

to mitigate their shadow clouds and it is anticipated that any programme to accelerate public cloud services will reinforce this advice.

Challenges to accelerating adoption are complex and inter-related

21. There are complex and inter-related challenges that inhibit agencies from accelerating adoption of public cloud services.

Public cloud services are perceived to be too risky

22. The Cabinet restriction on agencies' use of office productivity public cloud services that are hosted outside of New Zealand sends a strong signal to agencies that public cloud services are too risky. That is, if one of the most obvious uses for public cloud services (office productivity) cannot be hosted offshore then, by inference, all other offshore-hosted public cloud services are too risky.

23. The risk assessment process for public cloud services emphasises risks rather than benefits and has impeded the take-up of cloud services by agencies. The risk of information disclosure, including jurisdictional issues when data is stored offshore, is in significant tension with cost savings. This creates the perception that public cloud services are not viable and in turn drives a preference for in-house IT systems as a safer option.

24. Agencies must continue to get the balance right and manage the risk appropriately for different classes of information. Agencies can take advantage of the opportunities and innovations offered by public cloud services while ensuring that more-sensitive information remains protected by using a mix of traditional IT systems and on-shore and offshore-hosted public cloud services.

25. In particular, agencies need to evaluate the jurisdictional risks from storing data offshore. If data is stored by the cloud service provider offshore, then that data is subject to the laws of that particular country. In certain circumstances, the government of that particular country may be legally permitted to access New Zealand government data stored offshore (e.g. for the purposes of law enforcement, national security or other reasons).

Many agencies do not have the capability to systematically adopt public cloud services

26. New skills and operating models are required to integrate public cloud services with existing IT systems. Significant investment in technologies may also be needed to support the systematic adoption of public cloud services. Transition funding is not readily available to agencies to support a mix of traditional IT systems and public cloud services. This lack of funding is exacerbated by the wide-spread practice of redirecting depreciation funding to other priorities. The near-zero costs of fully-depreciated IT systems make it difficult to justify adoption of public cloud services as these have an on-going impact on operating costs.

Public cloud services require a different approach for security and commercial practices

27. In the context of rapid adoption of public cloud services, traditional IT security practices are costly and time consuming. Many agency procurement practices are not aligned with

the consumption model for public cloud services (i.e. pay for what you use rather than pay for assets), which imposes process-related costs that are disproportionate to the cost of the services. Many contracts from suppliers of traditional on-premises software make it difficult for agencies to make this transition.

Agency practitioners are isolated, and lack guidance and support

28. There is no single community of practitioners that could drive adoption. Practitioners from a wide range of disciplines are involved in any decision to adopt public cloud services, and many operate in a relatively isolated fashion and lack clear guidance.

To drive change a comprehensive programme of accelerators is required

29. Because these challenges are complex and inter-related, there is no 'silver bullet' to accelerate the adoption of public cloud services. Instead, a comprehensive programme of accelerators is required. The proposed accelerators are described below and are summarised in **Appendix A**.

Requiring agencies to have a public cloud services plan

30. I propose that Cabinet requires agencies to have a plan for how they intend to accelerate their adoption of public cloud services as part of their ICT strategy or else as a standalone plan. In addition to its cloud assurance role, the GCIO will benchmark the current state of agency adoption, identify opportunities for acceleration, monitor, and report. Monitoring and reporting will be undertaken through existing mechanisms, e.g. four-year investment planning, six-monthly GCIO functional leadership reporting, and agency capability maturity assessments as part of PSR assurance reporting.

Changing perceptions of the risk profile for public cloud services

31. I propose that Cabinet rescinds its 2012 decision to restrict agencies from using offshore-hosted office productivity public cloud services, provided that agencies comply with new guidance to be jointly-issued by the GCIO and Government Communications Security Bureau (GCSB) for the use of these services. A summary of the guidance and an analysis of the trade-offs involved in removing this restriction is provided in paragraphs 42-54.

32. The GCIO will reshape and reposition the cloud risk assessment process so that it will be easier for agencies to adapt this process to reflect their agency business needs, clarify that sign-off for the cloud risk assessment should be at an appropriately-delegated level within each agency, and collaborate with agencies to improve their capability to undertake cloud risk assessments.

33. The GCIO, in collaboration with the Ministry of Justice, Privacy Commissioner, and the National Cyber Policy Office (NCPO), will provide guidance to assist agencies to manage jurisdictional risks associated with storing data in public cloud services. The GCIO and the NZIC will also support agencies to more-accurately classify information, using the National Security Classification system. This will mean that agencies can take advantage of public cloud services where appropriate, while also separating the relatively small proportion of material classified as CONFIDENTIAL or above for storage on-shore.

Streamlining security certification for public cloud services

34. The GCIO and GCSB will produce joined-up guidance for individual agencies on security certification and accreditation processes for public cloud services. This will streamline current processes and ensure they align with guidance from the NZIC. The NZIC is considering further work to review the effectiveness of the current certification and accreditation processes as articulated in the New Zealand Information Security Manual (NZISM), as part of the PSR. This guidance will be consistent with cloud risk assessment provided by the GCIO.

35. Where public cloud services have significant agency spend and / or are used by many agencies the GCIO will provide centralised security certification. This will reduce duplication of effort and cost, and standardise the quality of certification.

Enabling agencies to transition their ICT operating models

36. I propose that the GCIO provide guidance on target operating models (including policies, frameworks, ICT workforce skills, and architectures) and management of shadow cloud. The GCIO and the GCSB will jointly produce guidance on secure use of public cloud services (including office productivity). The Treasury will provide guidance on funding models that can be used by agencies to support their transition to a hybrid environment (e.g. operating leases and the use of third-party fees to fund operating expenditure).

Lifting the capability of cloud practitioners

37. I propose that the GCIO establish a centre of expertise to connect agency practitioners and facilitate sharing of lessons learned and case studies. The GCIO will also educate senior public sector leaders, including business unit managers. This includes supporting agency projects and working with practitioners.

Modernising commercial frameworks

38. The GCIO will enable agencies to consume public cloud infrastructure services (compute and storage) through existing contracts. The GCIO will also negotiate commercial arrangements with cloud providers that have significant agency spend and / or are used by many agencies. Other cloud providers will be offered standard commercial terms.

39. As signalled in the 2015 review of the *Government ICT Strategy*, the GCIO will establish a catalogue of public cloud services (ICT marketplace) that streamlines procurement practices for these services. The GCIO will also establish commercial arrangements with suppliers to provide agencies with expertise and services to enable them to use cloud services (e.g. cloud brokerage services).

What the programme will deliver

40. Successful implementation of this programme will produce the following outcomes:
    - senior leaders increasingly use public cloud services in a balanced way to drive digital transformation;
    - public servants increasingly use public cloud services to deliver new services; and
    - agencies have frameworks and skills to adopt public cloud services securely.

41. I anticipate that the benefits of these outcomes will be:
    - more predictable ICT spending from fewer capital-intensive, ICT-enabled projects;
    - reduced risk as fewer IT systems are operated beyond intended lifespans and large-scale technology refreshes are less likely;
    - increased flexibility as agencies move towards increased standardisation; and
    - accelerated digital transformation as agencies draw on global scale innovation.

Removing the restriction on office productivity services

42. One of the most significant steps to accelerate the adoption of public cloud services is to enable agencies to consume office productivity public cloud services hosted outside of New Zealand. The potential for this step to occur, once agency risk, security and privacy practices had sufficiently matured, was envisaged in 2012 Cabinet policy for cloud computing.

43. I propose that Cabinet now allows agencies to use offshore-hosted office productivity public cloud services provided these comply with guidance to be developed by the GCIO and GCSB for secure use of such services. Until this guidance is developed, agencies will be expected to engage with the GCIO on a case-by-case basis. The guidance will cover a range of security controls, including:

    - a stipulation that no material classified at CONFIDENTIAL and above can be stored in these services;
    - a requirement to ensure that data is encrypted both in transit and at rest, and that agencies have sole control over the associated cryptographic key;
    - multi-factor authentication for access to the cloud service;
    - a requirement to be able to state where any data held in an offshore cloud service might be replicated or backed-up;
    - decommissioning processes as outlined in the NZISM;
    - evidence of security controls over physical access to offshore data centres;
    - assurance checks on cloud service providers in accordance with the NZISM;
    - controls over the interaction between public cloud services and end user devices;
    - assurance that appropriate patching and maintenance of software is undertaken;
    - process controls relating to intrusion detection, investigations and enterprise logging;
    - compatibility with existing government security technology services such as SEEMail and, where appropriate, CORTEX cyber defence capabilities;
    - technical protections to prevent data-mingling on shared storage platforms;
    - where necessary, the re-architecture of agency ICT networks to ensure that cloud services can be used safely and effectively; and
    - revision of agency disaster-recovery plans to cater for cloud-based services.

44. I propose that progress on the development and implementation of this security guidance and the NZIC's work to review the effectiveness of the current certification and accreditation processes as articulated in the NZISM will be reported to Cabinet via

existing reporting mechanisms used by the GCIO and as part of agency assurance reporting for the Protective Security Requirements.

45. This proposal will require Cabinet to rescind its decision to restrict agencies "for the time being" from using offshore-hosted office productivity public cloud services. The restriction was imposed because of "the significant nature and extent of government-held information that is supported by office productivity services, and the nature of the risk for data misuse and loss of control" [CAB Min (12) 29/8A]. Here office productivity means email, word processing, spreadsheets, presentations, and collaboration tools and services.

Agencies are now better able to manage the risks of public cloud services

46. Since 2012, there has been a concerted, government-wide push to improve agency risk, security and privacy practices. This has produced a significant uplift in maturity of these practices, albeit from a relatively low base. Agencies have also had several years' experience using the cloud risk assessment process and it is now appropriate for agencies to carry out case-by-case assessments for these services, relative to the nature of their information, rather than relying on a blanket restriction from Cabinet.

Security risks can be managed

47. If the restriction is removed, agencies will have the opportunity to use services that rely on data centres hosted offshore. (Microsoft's 'Office 365 service' is one possible example.) Security risks can be managed, officials assess, assuming that the security guidance GCIO and GCSB is implemented in full. Officials note that some suppliers are capable of offering relatively-high levels of data security in this context – even accepting that the offshore aggregation of agencies' data could create a very attractive target. For some agencies a move to outsourced data centres, even those hosted via an offshore public cloud service, may generate some concrete security benefits.

48. The removal of the restriction will enable agencies to store material classified at RESTRICTED and below in an offshore public cloud service providing that they follow the security guidance to be issued by the GCIO and GCSB when conducting their own risk assessment. However, some agencies may decide to manage this risk by choosing to retain classified (RESTRICTED) and protectively marked (SENSITIVE and IN-CONFIDENCE) data onshore. Agencies seeking to manage this risk by retaining some data onshore will need to ensure that the service they select has the ability to segregate data holdings according to classification or protective marking.

Agencies are able to make decisions about jurisdictional risks

49. As is the case for the offshore-hosted public cloud services currently used by agencies, information stored in offshore-hosted office productivity services will be subject to the jurisdiction and laws of the territory in which it is stored. This poses a risk that legitimate efforts to access this data by other governments (for example, by law enforcement, or by security agencies) or civil litigation in the country where the data is held could be disadvantageous to New Zealand's national interests or inconsistent with New Zealand laws. It is not possible to contract out of the legal framework of another territory.

50. Agencies are currently expected, as part of their existing cloud risk assessment process, to assess the nature and value of their information and the risks of exposure to another country's jurisdiction and, accordingly, make decisions on a case-by-case basis to store certain data on-shore or offshore. Restricting data centre locations to territories with similar legal and policy frameworks [redacted] will reduce the risk of arbitrary access to data, but will not remove the jurisdictional risk. section 6(a) of the Official Information Act 1982

51. Other governments – including New Zealand's closest partners – have sought to manage this risk by retaining critical information in onshore-hosted public cloud services [redacted]. For most of these countries, because of their geographical location and economic scale, global suppliers have been persuaded to deploy their public cloud services in local data centres. These suppliers have indicated that New Zealand's economy is too small and its location too remote to currently justify deploying their public cloud services in New Zealand. section 6(a) of the Official Information Act 1982

52. Where agency risk assessments indicate that office productivity data needs to remain in New Zealand it will be important to ensure that a locally-hosted IT service with comparable functionality is available, even though for most agencies the costs of using these are currently significantly higher than comparable offshore-hosted services.

53. [redacted] section 9(2)(b)(ii) of the Official Information Act 1982

54. Analysis by reputable industry sources suggest that migration from on-premises IT systems to public cloud services could produce savings in the order of 20-25% for some types of services (e.g. IT infrastructure). However, this is dependent on the size and complexity of individual enterprises and their ability to realise these savings.

What the GCIO will do to implement the accelerators

55. The GCIO will establish a twelve month programme to coordinate implementation of the accelerators and transition any on-going activities to business-as-usual functions. The programme will be led by the GCIO and delivered through the Partnership Framework – a group of senior public sector leaders organised into working groups for technology, investment, information, and service innovation to provide advice to a group of Chief Executives and to support the GCIO in the execution of his accountabilities.

56. Implementation will require a significant commitment and the GCIO will work with the Partnership Framework to re-allocate existing resources to this programme. The key agencies that will be involved are GCSB and NZSIS (security guidance, certification and accreditation), Ministry of Business, Innovation and Employment (procurement policy

and practices), Treasury (funding models), and the Ministry of Justice, Privacy Commissioner, and NCPO (jurisdictional risks).

Reporting

57. Progress will be reported to Cabinet as part of the existing reporting mechanisms used by the GCIO and as part of agency assurance reporting for the PSR.

Next steps

58. The GCIO will establish a formal programme to implement the accelerators. It will also communicate the policy changes to agencies and suppliers, and support agencies on a case-by-case basis as they adopt offshore-hosted office productivity public cloud services.

Consultation

59. This paper was developed by the Department of Internal Affairs in collaboration with agencies from the NZIC and socialised with the investment and technology working groups from the Partnership Framework. The following agencies were consulted: Ministry of Social Development, Ministry of Health, Ministry of Justice, Ministry for Primary Industries, Inland Revenue, New Zealand Transport Agency, Ministry of Education, New Zealand Police, Statistics New Zealand, Government Communications Security Bureau, Land Information New Zealand, Department of Conservation, Accident Compensation Corporation, Ministry of Defence, Treasury, Ministry of Business, Innovation and Employment, State Services Commission, Department of Corrections, Customs, Ministry of Transport, Ministry for Women, Ministry of Foreign Affairs and Trade, Ministry for the Environment, Ministry for Culture and Heritage, Tertiary Education Commission, Serious Fraud Office, and Te Puni Kōkiri. The Department of the Prime Minister and Cabinet and the Privacy Commissioner were informed.

Financial implications

60. There are no financial implications. The implementation programme proposed in this paper will be undertaken by reprioritising existing resources from the Department of Internal Affairs and other agencies.

Human Rights, Legislative Implications, and Regulatory Impact Analysis

61. This paper has no human right issues, legislative, or regulatory implications.

Publicity

62. There is considerable interest in the use of public cloud services by the New Zealand public sector, particularly the ICT industry. For this reason I propose to proactively release this paper, subject to consideration of any deletion that would be justified under the Official Information Act 1982 (CO Notice (09) 5).

Recommendations

63. The Minister of Internal Affairs recommends that the Committee:

Cloud acceleration programme

1. **note** that Cabinet directed the Government Chief Information Officer (GCIO) to work with the New Zealand Intelligence Community (NZIC) to review how to accelerate the use of public cloud services [CAB-15-MIN-0148.01];
2. **note** that, because the challenges to accelerating adoption are complex and inter-related, the GCIO and NZIC have developed a comprehensive implementation programme (**Appendix A**) to accelerate the use of public cloud services in a balanced way:
   - requiring agencies to have a public cloud services plan;
   - changing perceptions of the risk profile for public cloud services;
   - streamlining security certification for public cloud services;
   - enabling agencies to transition their ICT operating models;
   - lifting the capability of cloud practitioners; and
   - modernising commercial frameworks;
3. **note** that this programme will complement the existing policies and cloud risk assessment processes that provide checks and balances for agencies' use of public cloud services;

Removing the restriction on using offshore hosted office productivity services

4. **note** that in 2012 Cabinet agreed that agencies would be restricted "for the time being" from using offshore-hosted office productivity public cloud services because of the significant nature and extent of government-held information supported by office productivity services, and the nature of the risk for data misuse and loss of control [CAB Min (12) 29/8A];
5. **note** that agencies are now better able to manage the risks of using these services;
6. **agree** to allow agencies to use offshore-hosted office productivity public cloud services provided that they comply with new guidance for the use of these services that will be issued by the GCIO and Government Communications Security Bureau as summarised in this paper;
7. **agree** that until this new guidance is developed agencies should seek advice from the GCIO on a case-by-case basis;
8. **note** that if agencies choose to manage the risks of using these services by retaining some data onshore then they must ensure that the services they select have the ability to segregate data according to classification or protective marking and therefore retain a particular class of data onshore.

Requiring agencies to have an adoption plan

9. **note** that agencies are not currently required to have a plan for adopting public cloud services, nor is there any requirement to benchmark, monitor, or report on adoption;
10. **agree** that agencies are required to have a plan for how they intend to use public cloud services as part of their ICT strategy or else as a standalone plan;
11. **agree** that the GCIO will benchmark, monitor, and report on adoption;

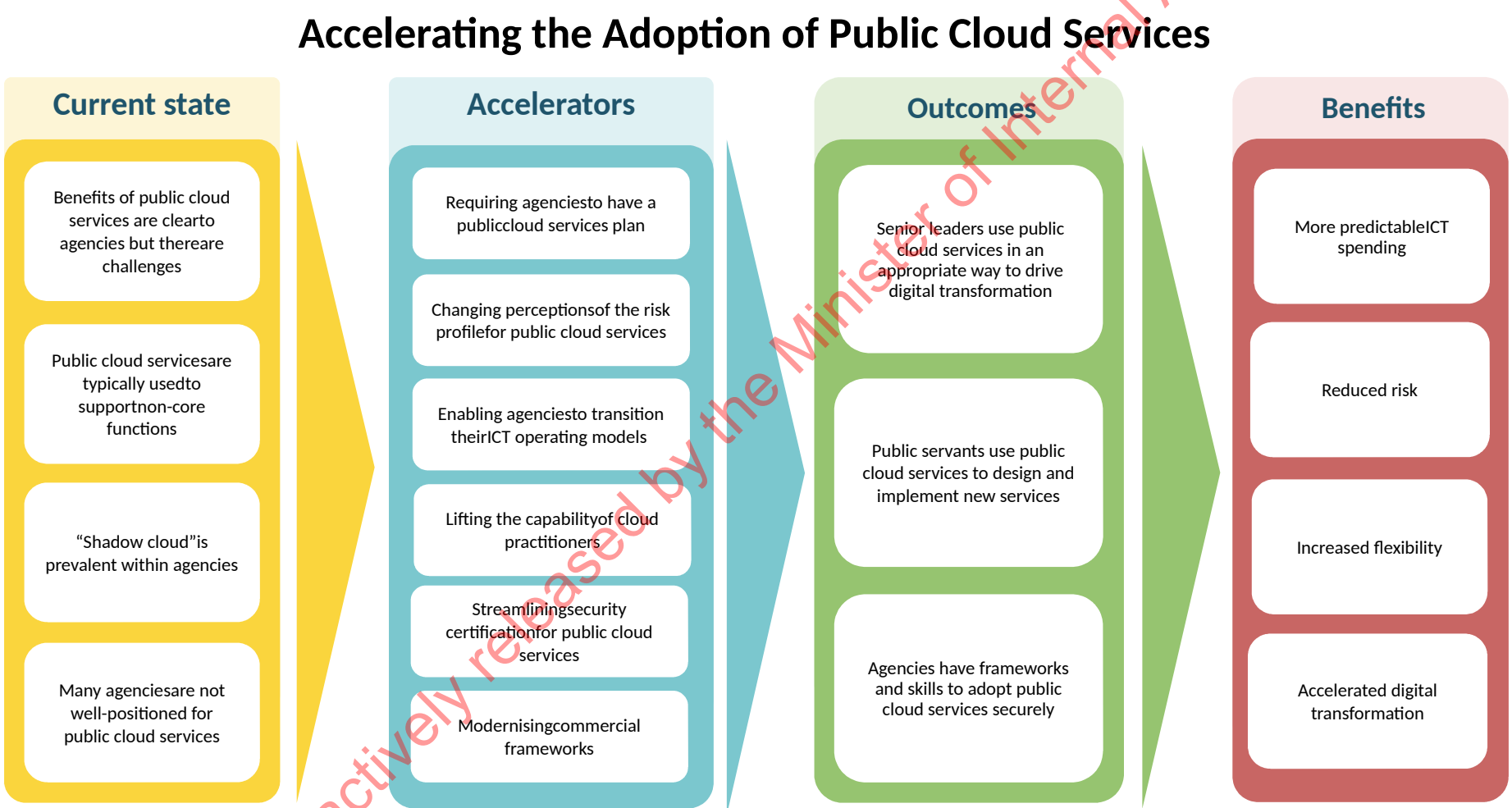
Programme implementation

12. **note** that the GCIO will work with other agencies to re-allocate existing resources to the implement the programme of accelerators;
13. **note** that progress – including the development and implementation of the security guidance and review of certification and accreditation processes – will be reported to Cabinet as part of the existing reporting mechanisms used by the GCIO and as part of agency assurance reporting for the Protective Security Requirements;
14. **note** that joined-up guidance, particularly on the security aspect of public cloud services, will be provided to agencies; and
15. **note** that I will proactively release this paper, subject to consideration of any deletion that would be justified under the Official Information Act 1982 (CO Notice (09) 5).

Hon Peter Dunne
Minister of Internal Affairs

/ /2016

Appendix A: Programme outline



Proposed implementation programme