

In Confidence

Office of the Minister of State Services
Office of the Minister of Internal Affairs

Chair
Cabinet Committee on State Sector Reform and Expenditure Control

IMPROVING GOVERNMENT INFORMATION AND COMMUNICATIONS TECHNOLOGY (ICT) ASSURANCE

Proposal

1. This paper is a companion paper to the Government ICT Strategy and Action Plan 2017 (*Strategy and Action Plan*). It outlines a strengthened approach to system-wide ICT assurance across the State Services¹ and provides for the mandates required by the Government Chief Information Officer (GCIO) to implement that approach. ICT spans information management, technology infrastructure, and technology-enabled business processes and services.

Executive Summary

2. Ministers have been concerned about a succession of problems with information and technology management, including privacy and security breaches, and ICT-enabled project delays, cost escalations and failures. This has resulted in reduced public trust and confidence in government ICT.
3. The current approach to the provision of ICT assurance is fragmented. For example:
 - there is no systematic assessment of the current risk status of ICT systems within agencies;
 - no agency has responsibility for intervening, where necessary, to help agencies to take corrective action on failing ICT projects or systems; and
 - information from current ICT assurance processes is not widely shared.

The proposed approach

4. Improving system-wide ICT assurance is intended to provide stakeholders with confidence that ICT risks and processes within the State Services are identified and effectively managed. While no assurance model can guarantee there will never be security or privacy breaches or service delivery failures, it can ensure risks are identified and managed.
5. At the project and programme level, work is already underway to build upon and strengthen current ICT assurance processes, such as *Major Projects Monitoring* and the *Gateway* review processes. At an agency level, the recommendations of

¹ The State Services refers to Public Service departments and four non-Public Service departments (the New Zealand Police, Parliamentary Counsel Office, the New Zealand Defence Force and the New Zealand Security Intelligence Service), Crown entities, and organisations subject to the Public Finance Act and the Reserve Bank. The Parliamentary Service, the Office of the Clerk, Tertiary Education Institutions, State-Owned Enterprises and local government are part of the wider State sector.

Proactively Released by the Minister of Internal Affairs

the GCIO Review of Publicly Accessible Systems are being implemented to improve the maturity of security and privacy practices within agencies.

6. However, there is a gap at the system level. We consider the GCIO, as functional leader for all-of-government ICT, is best placed to provide effective system-wide ICT assurance by:
 - providing coordinated oversight and delivery of system-wide ICT assurance;
 - reporting to Ministers on a system-wide view of the status of information management, technology infrastructure, and technology-enabled business processes and services across government;
 - identifying areas where interventions may be needed;
 - taking actions/intervening to support agencies to improve their ICT assurance processes;
 - providing Ministers with advice on whether ICT projects and programmes should proceed, and on the suitability of current ICT systems and processes, as the GCIO sees fit, or at the request of Ministers; and
 - coordinating, developing and mandating common ICT assurance and information management standards.
7. More detailed analysis of the assurance gaps identified and actions that will be taken is set out at **Appendix A**.

Scope

8. The system-wide ICT assurance role will provide assurance on information management (including security and privacy), technology infrastructure, existing ICT-enabled services, and new ICT-enabled projects and programmes.

New mandates required

9. The GCIO will be supported in this role by central agencies (the State Services Commission (SSC), the Treasury and the Department of the Prime Minister and Cabinet (DPMC)), and will require the support and cooperation of all chief executives and board chairs across the State Services.
10. The GCIO does not currently have the required mandates to provide a State Services-wide view of ICT risks, or to intervene with agencies across the State Services.
11. This paper recommends that Cabinet direct departments to provide assurance information to the GCIO and work with the GCIO on ICT issues of concern.
12. In the wider State Services, the State Sector and Public Finance Bill, if passed, will support the GCIO's ICT assurance role by allowing a whole-of-government direction to be issued to Crown entities to provide for the GCIO's information gathering requirements in relation to ICT assurance.
13. The Department of Internal Affairs (DIA) will work with SSC and the Treasury to prepare a direction that helps give effect to the GCIO's new role in Crown entities. The State Services Commissioner will also encourage chief executives

and board chairs in the wider State Services to provide ICT assurance information to the GCIO on request.

Risks

14. Requiring the GCIO to provide system-wide ICT assurance will carry some risks. It may drive unwanted behaviours by agencies, which may seek to offload some or all of their ICT assurance responsibilities to the GCIO, or inundate the GCIO with requests for advice, guidance and intervention actions, that may prove overly onerous and costly for DIA.
15. In addition, there is a risk that the imposition of overly onerous assurance requirements may cause unnecessary and costly delays across the system, instead of enabling the transformative business change being sought through the *Strategy and Action Plan*. The GCIO will work with central agencies to ensure that agencies are aware of the likely pressures on the GCIO and to ensure that the assurance requirements are proportionate and do not impede successful implementation of ICT projects, programmes and services.

Resources and funding required

16. For the GCIO to successfully carry out the system-wide ICT assurance role it will need to establish a core ICT assurance capability as soon as possible. The GCIO will concentrate initially on developing an understanding of the risk status of current ICT systems across the State Services, and on developing the necessary capacity and expertise to intervene where there are significant concerns, for example about the successful delivery of a project or the security and privacy of current ICT systems.
17. The GCIO will need to recruit staff with a mix of specialist and generalist skills to carry out this role. The GCIO has estimated that eight new FTEs will be needed in the short to medium-term to carry out this function within DIA. As benefits will be derived across the system, new Crown funding of \$1.500 million per annum for DIA is required to establish a core capability to carry out the GCIO assurance role.
18. As the GCIO becomes more knowledgeable about the status of ICT assurance across the State Services the assurance model will need to evolve. The GCIO may identify further gaps in the ICT assurance system, or resources or areas of expertise that could be better focused on supporting system-wide ICT assurance. This may mean that we will come back to Cabinet with a refined ICT assurance model or to seek additional funding.

Cloud computing

19. The Chair of Cabinet Economic Growth and Infrastructure Committee (EGI) agreed to delay a report back on a cloud computing risk and assurance framework, from December 2012 to May 2013.

20. The risks associated with cloud computing are similar to other ICT-enabled business decisions, whether based onshore or off-shore (acknowledging that there are some specific cloud computing risks). Adopting cloud computing safely requires agencies to follow robust information management processes such as appropriate data classification, risk assessment and mitigation processes. Only after these processes are followed appropriately can an informed decision be made whether or not a cloud service is a safe and viable option.
21. The Minister of Internal Affairs proposes this paper fulfils the requirement to report back on how cloud computing risks will be addressed.
22. The GCIO will work with the Government Communications Security Bureau (GCSB) to produce requirements and guidance for agencies on security and risk considerations for cloud computing, and will report on this to Cabinet by September 2013, together with a report on the viability of an onshore-hosted, cloud-based office productivity suite of services, which Cabinet agreed would be the first all-of-government cloud services [CAB Min (12) 29/8A].

Background

23. Ministers have been concerned about a succession of problems with information and technology management, including privacy and security breaches, and ICT-enabled project delays, cost escalations and failures. This has resulted in decreased public trust and confidence in government ICT practices at a time when ICT is becoming increasingly vital for service delivery and achievement of results.
24. In response to recent security and privacy breaches, the GCIO was directed to review publicly accessible systems. The GCIO's report and subsequent Cabinet decisions on the GCIO Review of Publicly Accessible Systems [SEC Min (13) 2/6] have resulted in a range of actions to improve security and privacy practices within agencies.
25. Subsequently, Ministers asked that the *Strategy and Action Plan* should also include a strong emphasis on assurance. Improving ICT assurance is a critical enabler of the service transformation being sought through the *Strategy and Action Plan*.
26. At present a number of assurance-related programmes and actions are being performed by the GCIO, the SSC, the Treasury, the GCSB, the Crown Ownership Monitoring Unit and others. However, these programmes are limited in scope, and the information collected is not widely shared.
27. This fragmented approach has arisen in the absence of a clear overall framework, which means that there is a gap at the system level, including:
- no individual with responsibility for providing and reporting on a system-wide ICT assurance view;
 - no systematic assessment of the current risk status of ICT systems within agencies;
 - no agency with responsibility for intervening, where necessary, to help agencies to take corrective action on failing ICT projects or systems; and

- current ICT assurance processes focus primarily on projects and programmes and finish at the post-implementation review point.
28. The lack of a coherent system-wide view of ICT risk and assurance means that Ministers do not have a full understanding of system-wide risks and the implications of ICT investment decisions that they are asked to make.

The proposed approach

29. The overarching objective for improving system-wide ICT assurance is to provide stakeholders with confidence that ICT risks and processes within the State Services are identified and effectively managed. No assurance model can guarantee there will never be any information security or privacy breaches or service delivery failures, but it can ensure risks are identified and managed appropriately.
30. The proposed approach involves the provision of enhanced ICT assurance at a project and programme level, at an agency level, and at system level. This means that every part of the ICT assurance system needs to play its part and improve performance.

Assumptions

31. In designing the assurance model, the following assumptions have been made:
- ICT is an enabler of business transformation;
 - ICT risk and assurance management processes should fit within overall government decision-making, risk management and assurance processes and maintain agency chief executive accountability;
 - the interventions required to address the problems need to leverage existing mechanisms where possible;
 - assurance activities are tailored according to assessed risk levels, within a clear overall framework;
 - the system of assurance will evolve over time as further gaps are identified and new risks emerge; and
 - a successful system of assurance has a number of component parts with clarity about roles, responsibilities, accountabilities, and potential conflicts of interest. The framework will therefore use the '3 lines of defence' good practice model: the first line is staff; the second line is created by oversight functions made up of compliance and risk management controls; and the third line is that of monitoring that the controls are operating effectively.

Scope

32. The system-wide ICT assurance role will provide assurance on information management (including security and privacy), technology infrastructure, existing ICT-enabled services, and new ICT-enabled projects and programmes.
33. The scope of intended system-wide ICT assurance includes the ICT-related activities of agencies of the State Services. The State Services refers to Public

Service departments and four non-Public Service departments (the New Zealand Police, Parliamentary Counsel Office, the New Zealand Defence Force and the New Zealand Security Intelligence Service), Crown entities, organisations subject to the Public Finance Act, and the Reserve Bank. The Parliamentary Service, the Office of the Clerk, Tertiary Education Institutions, State-Owned Enterprises and local government are part of the wider public sectors.

Proposed roles and responsibilities

34. The central agencies, the GCIO, departments and agencies across the State Services all have a role to play in providing a comprehensive ICT assurance model. We propose the following roles and responsibilities:

Table 1 - Roles and responsibilities

GCIO, as mandated functional leader of ICT	<p>Responsible for system-level assurance:</p> <ul style="list-style-type: none"> • Develops and maintains the <i>Strategy and Action Plan</i>. • Maintains a system view of ICT risk across State Services. • Identifies areas where interventions may be needed. • Takes actions to support agencies to improve their ICT assurance processes, and intervenes where necessary. • Reports to Ministers on a system-wide view of the status of information management, technology infrastructure, and technology-enabled business processes and services across government. • Provides Ministers with advice on the suitability of current ICT systems and processes, and on whether ICT projects and programmes should proceed, as the GCIO sees fit, or at the request of Ministers. • Coordinates, develops and mandates common ICT assurance and information management standards.
Other agencies with security functions (eg GCSB)	<p>Responsible for developing standards, policies and procedures that apply to particular areas for which they are responsible, within an overall framework co-ordinated by the GCIO. Contribute to security by managing particular threats.</p>
Agency CEs and Boards	<p>Responsible for ICT management at the agency (or sector) level in support of business objectives:</p> <ul style="list-style-type: none"> • Managing ICT assets, systems, projects and information and technology in accordance with agreed standards, policies, procedures and expectations. • Ensuring internal processes are in place to cost-effectively develop, deliver and operate ICT systems and manage information and technology effectively. • Ensuring ICT systems remain fit for purpose over time. <p>Note: departmental CEs will have an obligation to support the GCIO in the assurance role by providing the GCIO and central agencies with the information needed to provide a system-wide view of ICT risks and performance, and by lifting their own performance.</p>

Corporate Centre (central agencies and GCIO)	Responsible for wider public management system: <ul style="list-style-type: none"> • Advising on whether the whole system remains fit for purpose over time. • Wider decision-making processes and assurance activities that ICT assurance needs to be aligned with: eg Better Business cases, <i>Major Project Monitoring</i> and <i>Gateway</i>. • Co-ordinating the range of central agency assurance processes and activities with GCIO activities to avoid fragmentation and duplication.
-------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

35. The GCIO assurance function will sit within a wider set of assurance activities and use ICT-related information from various processes already in place (such as the *Gateway* and *Major Projects Monitoring* processes run by SSC, and the Treasury's *Four-year Planning* and *Government Project Portfolio* processes and agencies' independent quality reviews), to report to Ministers on the risk status of ICT across the State Services. This information will need to be supplemented by additional information from agencies. These activities, when fully implemented, will provide Ministers with a comprehensive view of risk associated with the government's investment in ICT, and confidence that risks with government ICT-enabled projects and services have been systematically identified and are being proactively managed.
36. For the avoidance of doubt, nothing in the GCIO's proposed role will duplicate or impinge on the GCSB's role relating to information security. We note that GCSB is leading a review of the *New Zealand Information Security Manual*, and the New Zealand Security Intelligence Service (NZSIS) is leading a review of protective security standards.
37. As provided for in the Government's response to the GCIO Review (SEC Min (13) 2/6), the GCIO and central agencies will work closely with the GCSB and the SIS to ensure that roles and responsibilities are clearly defined and that programmes of work are complementary and provide comprehensive coverage of all information security issues.

New mandates required

GCIO mandate with respect to departments

38. Currently the GCIO, as ICT functional lead, has authority to convey expectations of voluntary compliance to Public Service and non-Public Service departments. These expectations can be reinforced by the Head of State Services. However, the GCIO's powers to impose mandatory requirements on departments must currently be specifically agreed by Cabinet.
39. We therefore propose that Public Service and four Executive Branch non-Public Service departments (the New Zealand Police, Parliamentary Counsel Office, the New Zealand Defence Force and the New Zealand Security Intelligence Service) be required to provide information related to ICT assurance to the GCIO upon request. We also propose that these departments be required to work with the GCIO where issues of concern with ICT assurance are identified by the department or the GCIO.

40. The State Services Commissioner will ensure that improving ICT assurance is part of Public Service chief executives' performance plans. The Commissioner will also discuss issues of concern relating to ICT assurance raised by the GCIO with chief executives of departments.
41. We further propose that the GCIO should have the mandate to provide advice to Ministers on whether ICT projects and programmes should progress, and on the suitability of current ICT systems and processes, as the GCIO sees fit, or at the request of Ministers.
42. We also propose that Cabinet invite the Speaker of the House to direct the Office of the Clerk and the Parliamentary Service to provide assurance information to the GCIO upon request.

GCIO mandate with respect to agencies in the wider State Services

43. Currently the GCIO may invite or encourage Crown entity boards and chief executives in charge of State Services agencies to consider how best their agency could participate to give effect to GCIO requirements. Cabinet cannot, however, direct Crown entities to comply with mandatory requirements to provide information, or comply with interventions.
44. The State Sector and Public Finance Reform Bill (the Bill), which is currently before the House, proposes amendments to strengthen the Crown Entities Act 2004 to support functional leadership by expanding the purposes for which whole-of-government directions to Crown entities may be used. The Bill, if passed, may be used to issue a whole-of-government direction for the GCIO's information gathering and intervention requirements relating to system-wide ICT assurance.
45. We propose that the GCIO works with the SSC and the Treasury to prepare a draft whole-of-government direction to Crown entities to give effect to the GCIO assurance role.
46. In addition, the State Services Commissioner will encourage chief executives and board chairs in the wider State Services to provide ICT assurance information to the GCIO on request.

GCIO role development over time

47. The provision of system-wide ICT assurance is a new role for the GCIO. It will develop as the GCIO builds new information networks and develops further 'touch points' to better inform the system-wide ICT assurance view. The GCIO may identify further gaps in the ICT assurance system, or may identify resources or areas of expertise that could be better focused on supporting system-wide ICT assurance. Therefore, it is possible that amendments to the mandates to support the evolving GCIO assurance role will be needed in future.
48. It is an important principle that accountability for ICT assurance within individual agencies remains with agency chief executives and board chairs.

49. It is difficult to predict the size and scale of the GCIO ICT assurance role. However, we believe it is important that in the first year the GCIO concentrates on developing an understanding of the risk status of current ICT systems across the State Services, and on developing the necessary capacity and expertise to intervene with agencies where there are significant concerns about the successful delivery of a project or the effectiveness of current ICT systems. The GCIO will also work closely with GCSB, which has a role in assisting agencies dealing with significant cyber security threats.
50. We will report back to Cabinet if we need to amend the GCIO assurance role or seek further mandates to allow the GCIO role to be better fulfilled.

Immediate actions to strengthen assurance

51. A set of immediate actions to strengthen assurance will be undertaken, including:
- continuing to implement recommendations of the *GCIO Review of Publicly Accessible Systems* e.g. agency risk-based self-assessments of publicly facing systems, and establish a panel of security service providers to support agencies;
 - developing a system-wide view of ICT risk across government, based on best available current information;
 - establishing a centralised process for capturing and disseminating lessons learnt from projects;
 - GCIO regularly reporting to ICT Ministers on a system-wide view of ICT risks and opportunities; and
 - strengthening the independence of Independent Quality Assurance (IQA) and introducing Technical Quality Assurance (TQA), where appropriate, for ICT related projects.
52. Central agencies and GCIO will also ensure that assurance interventions are cost effective. For example, key information from *Gateway* reviews (delivery confidence assessments, recommendations and action plans) will be systematically shared with key stakeholders including GCIO rather than being confidential to the senior agency officials responsible for the projects.
53. Central agencies and GCIO may amend the thresholds for *Gateway* and *Major Project Monitoring* activity. Currently these apply to projects that are inherently high risk, yet the risk profile can and does change over time. Guidance material will also need to be created or updated.
54. While this paper is focused on improving ICT assurance, it is likely that similar consideration will need to be given to non-ICT projects of a capital and operating nature. Any changes to *Gateway* and *Major Project Monitoring* will apply to ICT and non-ICT projects.
55. The GCIO will introduce TQA for appropriate projects and will ensure that the IQA process is truly independent by appointing an independent panel of IQA and TQA providers. We propose that the IQA/TQA panel must be used by departments and that other State Services agencies be encouraged to use the panel.

56. As a result of policy decisions relating to the GCIO and functional leadership, more generally, it will be necessary to update Cabinet Office circular CO(10)02 Capital Asset Management in Departments and Crown entities. It may also be desirable to issue further circulars on the GCIO ICT assurance role.
57. We seek delegated authority from Cabinet for the Minister of Finance, the Minister of State Services and the Minister of Internal Affairs, in consultation with the Cabinet Office, to approve any such circulars that may be necessary to clarify Government's intentions relating to the management of information and ICT assets and infrastructure.
58. SSC and Treasury are developing a Portfolio Performance Management approach across a wide range of Capital Investments in the State Sector and this will, when implemented, provide critical information to the GCIO to assist with his assurance role. Portfolio Performance Management will collate information on the group of initiatives being considered, review these against where the Government wants to go within foreseeable constraints, ascertain what will be delivered in the next planning period, and consider what levels of portfolio delivery interventions should be applied. This requires continuous re-assessment of the risk profile of investment and consequent modification of assurance processes accordingly.

Risks and implications

59. Central agency assurance processes offer a sound basis on which to build the new GCIO assurance role. However, requiring the GCIO to provide system-wide ICT assurance will carry some risks. Currently the GCIO role is one of developing and promoting whole-of-government ICT solutions. The assurance role will change the nature of the GCIO and its relationship with agencies, and may have unintended consequences. Assuming the role of providing system-wide ICT assurance means that the GCIO will need to monitor agencies ICT assurance activities, and intervene where necessary to assist agencies, either with urgent remedial action or to improve their assurance capability.
60. Assuming this role runs the risk of driving unwanted behaviours by agencies, which may seek to either offload some or all of their ICT assurance responsibilities to the GCIO, or inundate the GCIO with requests for advice, guidance and intervention actions that may prove overly onerous and costly for DIA.
61. Alternatively, there is a risk that the imposition of overly onerous assurance requirements may cause unnecessary and costly delays instead of enabling the transformative business change being sought through the *Strategy and Action Plan*. The GCIO will work with central agencies to ensure that the assurance requirements are proportionate and do not impede successful implementation of ICT projects, programmes and services.
62. The GCIO is responsible for developing and providing common ICT capabilities and offering whole-of-government ICT solutions. Assurance of these projects will require careful management within DIA of potential conflicts of interest, for example through internal separation of functions.

Cloud computing

63. In August 2012, Cabinet agreed to a 'cloud first' approach and noted that the adoption of cloud computing involves potential risks to the confidentiality, integrity and availability of government-held information. Cabinet directed DIA to develop risk and assurance frameworks and guidance, working collaboratively with other relevant agencies (specifically, the GCSB and the National Cyber Policy Office (NCPO) within DPMC) [CAB Min (12) 29/8A].
64. The Chair of Cabinet Economic Growth and Infrastructure (EGI) Committee agreed to delay the report back on a cloud computing risk and assurance framework, from December 2012 to May 2013.
65. DIA has been working closely with other relevant agencies (specifically, GCSB and the NCPO) to develop a cloud computing risk and assurance framework. The report back to Cabinet on the framework was delayed to ensure that the framework took into consideration the outcome of the GCIO Security Review.
66. The risks associated with cloud computing are similar to any other ICT-enabled business decision, whether based onshore or off-shore. Adopting cloud computing safely requires agencies to follow standard information management processes such as appropriate data classification, risk assessment and mitigation processes. Only after these processes are followed appropriately can an informed decision be made whether or not a cloud service is a safe and viable option. These processes are being developed by the GCIO for system-wide promulgation.
67. The Minister of Internal Affairs proposes that this paper fulfils the requirement to report back on how cloud computing risks will be addressed.
68. The GCIO will work with the GCSB to produce requirements and guidance for agencies on security and risk considerations for cloud computing, and will report on this to Cabinet by September 2013, together with a report on the viability of an onshore-hosted, cloud-based office productivity suite of services, which Cabinet agreed would be the first all-of-government cloud service [CAB Min (12) 29/8A].

Reporting and accountability requirements

69. The GCIO will provide an initial report on system-wide ICT system assurance to Cabinet in September 2013. The GCIO will also provide 6-monthly update reports on progress with improving ICT assurance and issues of concern to the Cabinet and will regularly update the Ministerial Committee on ICT.
70. The GCIO will also report directly on any issues of concern with ICT assurance to relevant chief executives, board chairs, and/or the State Services Commissioner and the responsible Minister.
71. These reporting arrangements are designed to help provide greater visibility of issues of concern at an earlier stage, and will increase the chances of a successful intervention to support agencies.

Consultation

72. The Officials' committee for the Cabinet Committee on State Sector Reform and Expenditure Control (OSEC) were consulted. The following agencies were consulted on this paper: Canterbury Earthquake Recovery Authority, Department of Conservation, Department of Corrections, Ministry of Business, Innovation and Employment, Ministry for Culture and Heritage, Ministry of Defence, Ministry of Education, Education Review Office, Ministry for the Environment, Ministry of Foreign Affairs and Trade, Government Communications Security Bureau, Ministry of Health, Inland Revenue Department, Ministry of Justice, Land Information New Zealand, Ministry of Justice, New Zealand Customs Service, New Zealand Defence Force, New Zealand Police, New Zealand Security Intelligence Service, Office of the Clerk, Parliamentary Counsel Office, Parliamentary Service, Ministry for Primary Industries, Serious Fraud Office, Ministry of Social Development, Statistics New Zealand, Ministry of Transport, The Treasury.

Financial Implications

Funding

73. For the GCIO to successfully carry out the system-wide ICT assurance role it will need to urgently establish a core capability to:
- consolidate relevant existing information from central agencies and gather additional information from agencies across the State Services;
 - work with agencies across the State Services to develop and maintain a comprehensive understanding of the status of current ICT systems;
 - analyse and report on information gathered; and
 - work with agencies where capacity issues are identified relating to ICT assurance understanding or knowledge.
74. Improving ICT system assurance and a new assurance role for the GCIO will require funding. This work is new for the GCIO and will have system-wide benefits by helping all agencies to maintain the public trust and confidence necessary to allow the full benefit realisation of digital technologies and ICT-enabled business transformation. The GCIO will work with central agencies to ensure that the assurance interventions are cost effective and proportionate.
75. The activities referred to in paragraph 73 will require an ongoing core capability within DIA and therefore should be funded from new Crown funding. The GCIO will need to recruit staff with a mix of specialist and generalist skills to carry out this role. The GCIO has estimated that eight new FTE will be needed in the short to medium-term to carry out this function within DIA. As benefits will be derived across the system, new Crown funding of \$1.500 million per annum for DIA is required to establish a core capability to carry out the GCIO assurance role.
76. The GCIO will also need to intervene on failing ICT projects to support agencies to take corrective action; this will be funded through a fee for service charge which will apply to agencies for assurance services provided by the GCIO. In addition, agencies will face additional costs in terms of contracting independent

IQA and TQA, where requested by the GCIO. It is difficult to estimate the cost of additional assurance services provided by either the GCIO or by IQA providers to agencies. Initial estimates indicate that these costs could be in the order of \$400,000 to \$600,000 per annum.

77. As the GCIO becomes more knowledgeable about the status of ICT assurance across the State Services the assurance model will need to evolve. The GCIO may identify further gaps in the ICT assurance system, or resources or areas of expertise that could be better focused on supporting system-wide ICT assurance. This may mean that we will come back to Cabinet with a refined ICT assurance model or to seek additional funding.
78. The increased Crown funding will be applied to a departmental multi-class output expense appropriation within Vote Internal Affairs: "Information and Technology Services"

Regulatory Impact Analysis

79. This paper does not propose any changes to legislation or regulations, therefore a Regulatory Impact Analysis is not required.

Human rights and legislative implications

80. There are no human right issues, or legislative implications.
81. The State Sector and Public Finance Reform Bill provides amendments which are necessary to ensure the extension of the GCIO assurance role beyond core Public Service and non-Public Service departments to Crown entities by providing an enhanced mechanism for whole-of-government directions.

Publicity

82. The Minister of State Services and the Minister of Internal Affairs may proactively release this paper, subject to consideration of any deletions that would be justified if the information had been requested under the Official Information Act 1982 (CO Notice (09) 5).

Recommendations

83. The Minister of State Services and the Minister of Internal Affairs recommend that the Committee:
1. **confirm** that the overarching objective for improving system-wide Information and Communications Technology (ICT) assurance is to provide stakeholders with confidence that ICT risks and processes within the State Services are identified and effectively managed;
 2. **note** that there is currently no single agency with responsibility for providing a system-wide view of government ICT assurance;

3. **note** that improving system-wide ICT assurance is critical for the ICT-led business transformation set out in the *Government ICT Strategy and Action Plan 2017*;

System-wide ICT assurance

4. **agree** that the Government Chief Information Officer (GCIO) will, as part of the ICT functional leadership role, have responsibility for coordinated oversight and delivery of system-wide ICT assurance;
5. **agree** that the GCIO provision of system-wide ICT assurance will include:
 - providing coordinated oversight and delivery of system-wide ICT assurance;
 - reporting to Ministers on a system-wide view of the status of information management, technology infrastructure, and technology-enabled business processes and services across government;
 - identifying areas where interventions may be needed;
 - taking actions to support agencies to improve their ICT assurance processes and intervening where necessary; and
 - coordinating, developing and mandating common ICT assurance and information management standards;
6. **note** the GCIO will introduce Technical Quality Assessment (TQA) for ICT projects, where appropriate, and will strengthen the Independent Quality Assessment (IQA) of ICT projects by establishing an independent panel of providers for TQA and IQA services;
7. **direct** Public Service departments and the New Zealand Police, New Zealand Defence Force, New Zealand Security Intelligence Service and Parliamentary Counsel Office to use the TQA and IQA panel referred to in recommendation 6 as directed by the GCIO;
8. **note** the State Services Commissioner will encourage chief executives and board chairs in the wider State Services to use the TQA and IQA panel referred to in recommendation 6;
9. **invite** the Speaker of the House to direct the Office of the Clerk and the Parliamentary Service to use the TQA and IQA panel referred to in recommendation 6;
10. **note** that to provide the system-wide ICT assurance referred to in recommendation 4, the GCIO will require the ability to:
 - access ICT assurance information from State Services agencies;
 - compel relevant State Services agencies to work directly with it on ICT assurance issues; and
 - provide independent actionable ICT assurance advice to agency chief executives, board chairs, the Head of State Services and the responsible Minister;

Mandate to ensure application to departments and across the State Services

11. **note** that departmental chief executives will support the GCIO in the assurance role by providing the GCIO and central agencies with the information needed to provide a system-wide view of ICT risks and performance, and by lifting their own ICT risk management and performance;
12. **direct** Public Service departments and the New Zealand Police, New Zealand Defence Force, New Zealand Security Intelligence Service and Parliamentary Counsel Office to provide ICT assurance information to the GCIO upon request;
13. **direct** the departments listed in recommendation 12 above to work with the GCIO where issues of concern related to ICT assurance are raised;
14. **agree** that the GCIO has a mandate to provide Ministers with advice on whether ICT projects and programmes should proceed, and on the suitability of current ICT systems and processes, as the GCIO sees fit or at the request of Ministers;
15. **note** the State Services Commissioner will ensure that improving ICT assurance is part of Public Service chief executives' performance plans;
16. **note** that the State Services Commissioner will discuss issues of concern relating to ICT assurance raised by the GCIO with chief executives of Public Service departments;
17. **note** the State Services Commissioner will encourage chief executives and board chairs in the wider State Services to provide ICT assurance information to the GCIO on request;
18. **invite** the Speaker of the House to direct the Office of the Clerk and the Parliamentary Service to provide assurance information to the GCIO upon request;
19. **invite** Ministers to use all mechanisms available to them to ensure that agency chief executives and board chairs are made aware of government's expectations that ICT assurance information will be provided to the GCIO upon request;
20. **note** that the *State Sector and Public Finance Reform Bill* amends the Crown Entities Act 2004 to support functional leadership, by expanding the purposes for which a whole-of-government direction can be applied (including purposes relating to functional leadership);
21. **direct** the GCIO to work with the State Services Commission to prepare a draft whole-of-government direction to Crown entities, to give effect to the GCIO assurance role, in preparation for the enactment of the *State Sector and Public Finance Reform Bill*, expected in July 2013;

Reporting requirements

22. **direct** the GCIO to provide an initial assessment of the status of system-wide ICT assurance by September 2013 and to report to Cabinet six monthly thereafter;
23. **direct** the GCIO to report significant ICT assurance concerns immediately upon identification to relevant chief executives, board chairs, and/or the State Services Commissioner and the responsible Minister;
24. **direct** the GCIO to provide regular update reports on ICT assurance issues to the Government ICT Ministerial Group;

Updating assurance processes

25. **note** that central agencies and the GCIO will work closely together on ICT assurance, including directly exchanging all relevant information;
26. **direct** central agencies to review Cabinet Office circular CO(10)02 to ensure that it is up-to-date and aligned with the functional leadership role and with requirements to improve system-wide ICT assurance;
27. **delegate** authority to the Minister of Finance, the Minister of State Services and the Minister of Internal Affairs, in consultation with the Cabinet Office to update CO(10)02, and to approve any such circulars as may be necessary to clarify government's intentions relating to the management of information and ICT assets and infrastructure;

Cloud computing

28. **note** that the Minister of Internal Affairs sought and received agreement to delay the report back to Cabinet on a cloud computing risk and assurance framework;
29. **note** that adopting cloud computing safely requires agencies to follow standard information management processes such as appropriate data classification, risk assessment and mitigation processes;
30. **agree** that the cloud computing risk and assurance framework will be included as part of the system-wide ICT assurance framework outlined in this paper;

Financial implications

31. **note** that improving ICT system assurance is a new role for the GCIO;
32. **note** that the GCIO assurance role will have system-wide benefits by helping all agencies to maintain the public trust and confidence necessary to allow the full benefit realisation of digital technologies and ICT-led business transformation;
33. **note** new Crown funding is required for the GCIO to establish the standing capability to successfully carry out the assurance role;

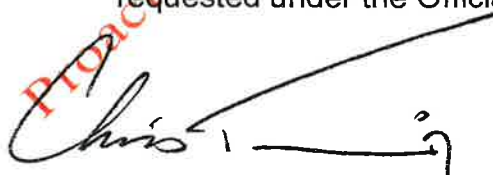
34. **agree** that a fee-for-service funding model will apply for assurance intervention services provided to agencies by the GCIO;
35. **approve** the following changes to appropriations to give effect to the decisions in recommendation 4 and 5 above, with a corresponding impact on the operating balance:

Vote Internal Affairs Minister of Internal Affairs	\$m – increase/(decrease)				
	2013/14	2014/15	2015/16	2016/17	2017/18 and outyears
Departmental Output Expense: Information and Technology Services MCOA: Cross-Government ICT Strategy and Planning, Service Delivery and Investment Proposals (funded by revenue Crown)	1.500	1.500	1.500	1.500	1.500

36. **agree** that the proposed change to appropriations for 2013/14 above be included in the 2013/14 Supplementary Estimates and that, in the interim, the increase be met from Imprest Supply;
37. **agree** that the expenses incurred under recommendation 35 above be a charge against the between-budget operating contingency, established as part of Budget 2013; and

Publicity

38. **invite** the Minister of State Services and the Minister of Internal Affairs to release communications about improvements to ICT assurance, which may include the proactive release of this paper and its associated minute, subject to any deletions that would be justified if the information had been requested under the Official Information Act 1982 (CO Notice (09) 5).



Hon Chris Tremain
Minister of Internal Affairs

5, 6 / 2013



Hon Dr Jonathan Coleman
Minister of State Services

5, 6 / 2013

Appendix A: Assurance matrix

What we need		What we're going to do	
1	Clear strategic direction for a digital and investment plan	Collaborate with the Digital and Investment Plan	Require selected agencies to develop initial SSPs along with Asset Management Plans and provide these to the Corporate Centre
2	Clear standards, policies and processes that ICT-related activities need to comply with	Streamline/clarify and issue ICT standards and guidance within an overall framework	Where multiple agencies undertake security functions, ensure clarity around agencies' roles and responsibilities
3	Portfolio view of all current and future ICT investment intentions	Develop a portfolio view of ICT value and risk across government, based on best available current information	Look for emerging opportunities and risks
4	Clear governance for ICT assurance, clear roles, responsibilities and authorities	Clarify roles, responsibilities, decision rights and escalation processes for ICT assurance and communicate to agencies; evaluate cost-effectiveness of assurance interventions	
5	Systemic reporting on ICT issues	Introduce specific mandate for GCIO to provide independent advice to CEOs, HOSs and Ministers at key gates and undertake independent reviews	
6	Monitoring of compliance with standards, rules and expectations; Monitoring of benefits	A centralised process for capturing and disseminating lessons learnt from projects; GCIO to begin regular reporting to ICT Ministers on portfolio view of ICT risks and opportunities	
7	Assurance of ICT-enabled projects and programmes	Corporate Centre enhances quality of business case analysis, benefits management and performance monitoring; Following development of framework for ICT related standards and guidance, assess best approach to more systematic monitoring	
8	Assurance of existing ICT enabled business services	Strengthen independence of Independent Quality Assurance (IOA) and introduce Technical Quality Assurance (TOA) Strengthen Major Project Monitoring and Gateway, eg. extend Gateway criteria and implement 'Delivery Confidence' reporting; Implement a 'Gateway' for projects/services outside Major Project Monitoring	
9	Assurance of quality of information management processes (including privacy and security)	Develop a portfolio view of ICT value and risk across government, based on best available current information; Based on this information, determine best approach to risk-based assurance of existing services	
10	Management of human resources	Continue to implement recommendations of GCIO review of Publicly Accessible Systems e.g. openly risk based self-assessments of publicly facing systems; establish a panel of security service providers to support agencies	
11	Education and capability development	Invest in capability uplift and make better use of scarce specialist capabilities; Agencies to provide ICT workforce plans that specify current and forecast state of gaps and shortages	
12	Supporting Assurance	Develop and use capability maturity model assessments to target capability building	