Office of the Minister of State Services

Office of the Minister of Internal Affairs

Cabinet State Sector Reform and Expenditure Control Committee

Information Privacy and Security Programme: Final Report

Proposal

1. This is the final report on the Information Privacy and Security programme (the Programme). The programme was established by Cabinet to carry out the recommendations from the Review of Publicly Accessible Information Systems, undertaken by the Government Chief Information Officer (GCIO) in 2012 at the request of the State Services Commissioner.

2. The programme has reported on progress regularly to the Minister of State Services. This final report sets out overall progress made since 2012 in improving operational practice in privacy and information security across the State services; recommends the programme be formally closed; and sets out how continuous improvement and ongoing assurance will be supported after the programme is closed.

Executive summary

3. Ensuring the security of all publicly accessible information systems was the first priority of the Programme and was addressed early on. The focus shifted from an immediate response to privacy and security breaches; to recognition that good operational practice can enable broader benefits for government and New Zealanders.

4. The programme has resulted in system-wide improvement in operational practice. Good practice in privacy and security underpins government's ability to safely and appropriately use information to deliver citizen-centred services. It also means government security practice can keep pace with a constantly evolving threat environment.

5. Privacy and security risks will never be completely eliminated so an ongoing focus is needed. The Programme has delivered enduring functions through the Government Chief Privacy Officer (GCPO) and the New Zealand Protective Security Requirements (PSR) to support Chief Executives to embed and refine improvements in privacy and protective security.

6. The GCPO and PSR complement and reinforce the GCIO, State Services Commission and the Privacy Commissioner to enable strengthened oversight of privacy and security practice across the State services, sustain continuous improvement and enable agencies to recognise, protect and release the value of the information they hold.

7. The diagram at **Appendix 1** summarises overall progress made as a result of the Programme.

Background

8. Following a number of high profile privacy and information security breaches in 2012, the State Services Commissioner tasked the GCIO with undertaking an urgent review of publicly accessible information systems across the State services (the GCIO Review).

9. The GCIO Review identified that while some good privacy and security practice existed in government agencies, in many cases this was under-developed. The State Services Commissioner and Cabinet directed the GCIO to lead a plan of action to improve privacy and security capability across the State services (Cab Min (13) 6/2D) and report to the Minister of State Services annually on progress.

10. The Information Privacy and Security Governance Group (chaired by the GCIO) was established in 2013 to oversee these actions. The core activities of the Information Privacy and Security programme are:

    - ***Initiatives to lift operational practice within agencies*** through risk and security assessments of publicly accessible information systems; monitoring agency progress in building capability; and providing guidance and access to expertise;
    - ***Enduring, cohesive functions to sustain continuous improvement*** through the establishment of the GCPO and the implementation of the PSR; and
    - ***Strategic information management -*** ensuring the broader settings and practices that underpin information management support appropriate data sharing and use.

Lifting operational practice within agencies

11. All agencies completed risk and security assessments of their publicly accessible information systems early in the programme. In doing so, all Chief Executives also made a formal commitment to lift their capability in privacy and information security.

12. Throughout the Programme, agencies have received tools, support and access to market expertise to assist them in meeting Cabinet directions.

13. The GCIO has overseen system-wide progress in improving practices and capability maturity through regular self-assessment reporting from agencies. This approach has reinforced the accountability of Chief Executives and the need for agencies to tailor their improvement programmes to their level of information risk.

14. The GCIO has overseen this process with the ability to intervene or direct agencies if required. Intervention has not been needed due to the steady progress reported by agencies.

What has changed since 2012?

15. The initial results of the 2012 GCIO Review indicated a need to focus on ensuring the right governance, operational and assurance practices were in place. Governance and oversight of privacy and security had the highest level of improvement early on in the programme[1], which has remained stable throughout.

16. The subsequent focus of the Programme has therefore been on improving operational and assurance practices by formalising security policies; security risk management processes; security certification and accreditation processes; and security assurance processes.

17. **Appendix 1** sets out the progress made in improving operational and assurance practices over the term of the programme.

[1] In 2013 98% of agencies (compared to 21% in 2012) reported senior level accountability for privacy and security; and 98% reported that clear roles and responsibilities were in place (compared to 50% in 2012).

Security policy

18. Good security policies and standards are a cornerstone to good security practice. In 2012, the GCIO Review found that only 27% of agencies had formal security standards and procedures in place to enable their security policies. **96% of agencies now have a formal security policy supported by standards and procedures.**

19. Formal in this context means the policy is documented and supported by standards.

20. The remaining agencies have reported that they have security policies embedded within wider organisational policies and are in the process of consolidating these into an overarching framework supported by comprehensive standards.

Certification and accreditation

21. The process to "certify and accredit" a system confirms that controls are robust before it goes live. In 2012, the GCIO Review found that only 13% of agencies had formal certification and accreditation processes in place. **84% of agencies now have formal certification and accreditation processes in place.**

22. Formal in this case means the process is documented and consistently followed.

23. The remaining agencies report they have processes to ensure approval is gained before a system goes live, which include security and privacy assessments and formal acceptance of risks and controls. The majority of these agencies are in the process of documenting the processes or, if they have already done so, building awareness within their organisation to embed behaviours.

Security risk management

24. Good risk management practices are the fundamental driver of appropriate security and privacy measures. In 2012, the GCIO Review found that only 27% of agencies had formal security risk management processes in place. In 2015, **74% of agencies now have formal security risk management processes in place**.

25. Formal in this case means the process is documented and consistently followed.

26. The remaining agencies report they have overarching frameworks in place to consider privacy and security risks. Some have documented their processes and are building awareness so that they are consistently followed at all times (requiring behavioural and cultural change). Others are small agencies, with a limited amount of personal or commercially sensitive information, who report that they plan to do so.

Security Assurance

27. In 2012, the GCIO Review found limited evidence of assurance being sought over security practices. The resulting recommendations required agencies to complete security assessments of their publicly accessible information systems, which significantly reduced the potential for a breach as a result of these systems.

28. New indicators were developed in 2013 to measure progress in developing formal, security assurance processes. **90% of agencies report they now have formal security assurance processes in place** (up from 58% in 2013).

29. Formal in this case means that a structured ICT security assurance programme is in place.

30. The remaining agencies are all small agencies with a limited amount of personal or commercially sensitive information. They have reported that measures are in place to ensure the ongoing security of their systems. The GCIO will continue to support ongoing improvement in this area through the ICT Assurance function, which will be facilitating agency operational assurance planning on an annual basis.

What does this tell us?

31. It is clear from these results that a significant shift has taken place. Chief Executives are aware of their accountability and are treating security as a business issue, supported by improved governance.

32. Agencies have strengthened their information security controls and the majority have formal processes and policies in place, improving the overall capability maturity of the system and enabling improved resilience of government ICT systems. Those that have not all report that they are currently developing or implementing formal processes.

33. All Chief Executives have committed to ongoing improvement, commensurate with their level of risk.

Sustaining continuous improvement

34. Agencies have made steady and sustainable progress but the improvement journey is not over. There is a need for ongoing focus to sustain continuous improvement, and for agencies to use this as a platform for realising the broader strategic value of the information they hold. Continued guidance and oversight is also required.

35. Our reliance on technology brings with it an ever increasing threat of malicious actions and the cost of a cyber-incident can be significant. Government agencies can never entirely remove the risk of damage from a cyber-attack or a privacy breach. However, good operational practice in privacy and security can improve our resilience and our ability to recover should such events occur.

36. A combination of clear Chief Executive accountability and enduring functions to provide ongoing guidance and assurance will ensure appropriate attention remains on privacy and security practice and capability.

37. The State Services Commission has strengthened the performance expectations of Chief Executives to make explicit the need to manage privacy, security and information effectively. The Programme has established specific ongoing functions to assist Chief Executives to meet their accountability.

- ***The Government Chief Privacy Officer*** (GCPO - housed in the Department of Internal Affairs) was appointed in July 2014 to ensure a long-term focus on privacy management and building privacy capability across the State services. The GCPO has issued core expectations of public sector agencies, supported by a Privacy Maturity Assessment Framework. An engagement team is in place to provide ongoing support and assess progress against the core expectations.

- ***The NZ Protective Security Requirements*** (PSR - housed in the NZ Intelligence Community) were implemented in December 2014. It brings together personnel, physical and information security guidance together under one overarching risk-based framework. The PSR has also clarified core requirements of agencies, issued a capability tool and put in place an engagement team to support agencies and assess progress against the requirements.

38. The GCPO and the PSR strengthen the wider system of oversight of privacy and security across the State Services. They complement the work of SSC, the GCIO, who has oversight of system-wide ICT assurance– including ICT security and privacy risks; and the Privacy Commissioner.

39. A new reporting and assessment framework is being put in place to replace the GCIO Review reporting requirements established through the Programme This will seek annual reporting from Chief Executives on progress in meeting the expectations and requirements set by the GCPO and PSR. The framework will also measure each agency's capability maturity uplift on an ongoing basis. The framework will ensure the GCPO and PSR have oversight of continued system-wide improvement.

40. The GCPO and the PSR will build on the improvements agencies have made in response to the GCIO Review (which focussed on information security practices as a priority) to support broader capability uplift. The results of the first agency reports to the GCPO and PSR are due in March 2016 and will re-set the baseline for system-wide capability– considering privacy practice more deeply and a more holistic approach to protective security (encompassing personnel and physical, as well as information security).

41. We recommend that the GCPO, NZ Intelligence community and the GCIO report to the Minister of State Services annually on system-wide capability maturity; and how improvements are being leveraged to enable effective sharing and use of data and information for the broader benefit of government and New Zealanders.

42. We also recommend that the GCPO, the NZ Intelligence Community and the GCIO continue to work together to deliver co-ordinated support to agencies and actively seek opportunities for further alignment where it is of benefit to agencies.

Strategic information management

43. The extent to which information can be used to achieve outcomes is underpinned by public trust and confidence in the government. Maintaining this trust has been a key focus for the programme.

44. Privacy and security are part of a complex data and information eco-system that needs to work in combination to be effective. To ensure this broader context is considered, Cabinet directed that work on strategic information management policy (led by DIA at the time) become a part of the Programme.

45. Information management policy settings, accountabilities and practices have not been considered in a holistic way and, not surprisingly, are fragmented and inconsistent across government. A review of these practices and settings is underway to ensure they are cohesive and fit for purpose in a modern, digital context (action 6.4 from the 2014 update of the Government ICT Strategy and Action Plan). This work, known as the "IM Review" is consistent with a recommendation from the NZ Data Futures Forum to "get the rules of the game right" for data use and re-use (EGI min (15) 1/2).

Withheld under section 9(2)(f)(iv) of the OIA

48. The next steps for the IM Review will be overseen by the Information Group, set up under the GCIO's ICT Partnership Framework (explained below), to ensure findings are considered in the context of other system-wide work on data and information.

Future oversight and co-ordination

49. The Information Privacy and Security programme has come to the end of its Cabinet mandated term. We believe the programme has achieved its intended objectives and recommend the programme be closed.

50. The Programme has resulted in widespread improvement across the agencies in scope of the GCIO Review through the establishment of clear accountabilities and regular agency reporting on practice and capability. It has overseen the implementation of enduring functions to support continuous improvement and provide ongoing assurance over privacy and security. These functions will require ongoing oversight and co-ordination with other system-wide initiatives that intersect with privacy, security and information management.

51. The GCIO has set up a Partnership Framework to drive and accelerate the changes needed for ICT to support radically transformed public services. A Strategic Leadership Group of Chief Executives is supported by four Working Groups, covering Technology, ICT System Investment, Information and Digital Delivery.

52. The Minister of State Services has agreed that the Information Privacy and Security Governance Group can be disestablished and the Information Group under the Partnership Framework will provide ongoing oversight of the enduring functions established through the programme (the GCPO and the PSR); and the next steps for the IM Review. This will ensure that the right strategic connections continue to be made across related work.

Consultation

53. The Department of Internal Affairs, Government Chief Information Officer, Government Communications Security Bureau, New Zealand Security Intelligence Service, Statistics New Zealand, Inland Revenue Department, Ministry of Business, Innovation, and Employment, Ministry of Social Development, The Treasury, Ministry of Justice and the Department of Prime Minister and Cabinet were consulted on this paper. The Office of the Privacy Commissioner was informed of this paper.

Financial implications

54. The work required of agencies to meet the ongoing requirements of the GCPO and the PSR will require resources proportionate to their level of risk. The cost will vary across agencies, based on their information holdings and their current and planned capability.

Legislative implications

55. None.

Human rights, gender implications and Disability perspective

56. None.

Publicity

57. To demonstrate progress made as a result of the Programme, we seek Cabinet's agreement to publicly release a copy of this report. The State Services Commission and the GCIO will work together on the process for this release.

Recommendations

58. The Ministers of State Services and Internal Affairs recommend that the Committee:

    1. **Note** that the Information Privacy and Security Programme has resulted in system-wide improvement in operational practice, shifting to a more formalised approach to privacy and information security.
    2. **Note** that the Programme has established enduring functions to sustain continuous improvement through the Government Chief Privacy Officer (GCPO) and the NZ Protective Security Requirements (PSR) which will provide ongoing assurance over privacy and security.
    3. **Note** the GCPO and PSR complement the roles of the GCIO, SSC and the Privacy Commissioner to strengthen system-wide oversight of privacy and security.
    4. **Direct** the GCIO, GCPO and NZ Intelligence Community to report to the Minister of State Services annually on system-wide capability and maturity in privacy, security and the effective use of data and information.
    5. **Direct** the GCIO, GCPO and NZ Intelligence Community to continue to work together to deliver co-ordinated support to agencies and actively seek opportunities for further alignment.
    6. **Agree** that the Information privacy and Security Programme has achieved its objectives and can be closed.
    7. **Note** that ongoing oversight and co-ordination of ongoing activities resulting from the Programme will be provided through the Information Group under the GCIO's ICT Partnership Framework.
    8. **Agree** that this final report can be publicly released.

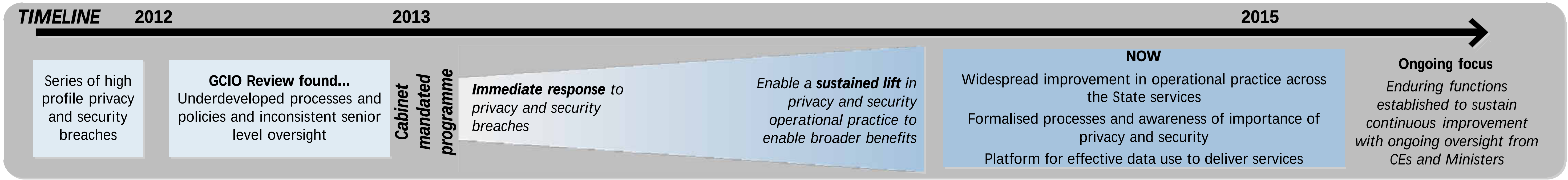
Hon Paula Bennett
Minister of State Services

___/ _/_____

Hon Peter Dunne
Minister of Internal Affairs

___/ _/_____

APPENDIX ONE: INFORMATION PRIVACY AND SECURITY PROGRAMME: OVERVIEW



TIMELINE 2012 2013 2015

Series of high profile privacy and security breaches

GCIO Review found... Underdeveloped processes and policies and inconsistent senior level oversight

Cabinet mandated programme

Immediate response *to privacy and security breaches*

Enable a ***sustained lift*** *in privacy and security operational practice to enable broader benefits*

NOW

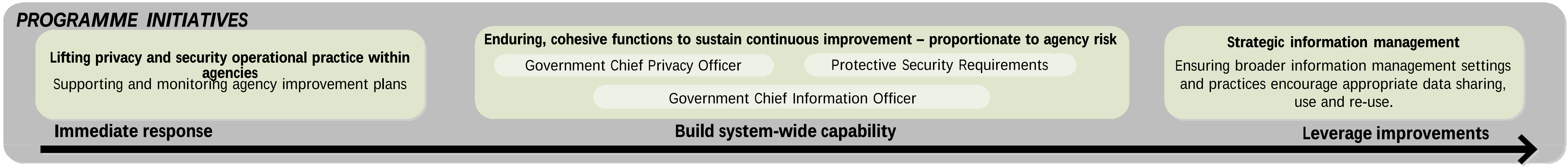
Widespread improvement in operational practice across the State services

Formalised processes and awareness of importance of privacy and security

Platform for effective data use to deliver services

Ongoing focus

Enduring functions established to sustain continuous improvement with ongoing oversight from CEs and Ministers



PROGRAMME INITIATIVES

Lifting privacy and security operational practice within agencies

Supporting and monitoring agency improvement plans

Enduring, cohesive functions to sustain continuous improvement – proportionate to agency risk

Government Chief Privacy Officer

Protective Security Requirements

Government Chief Information Officer

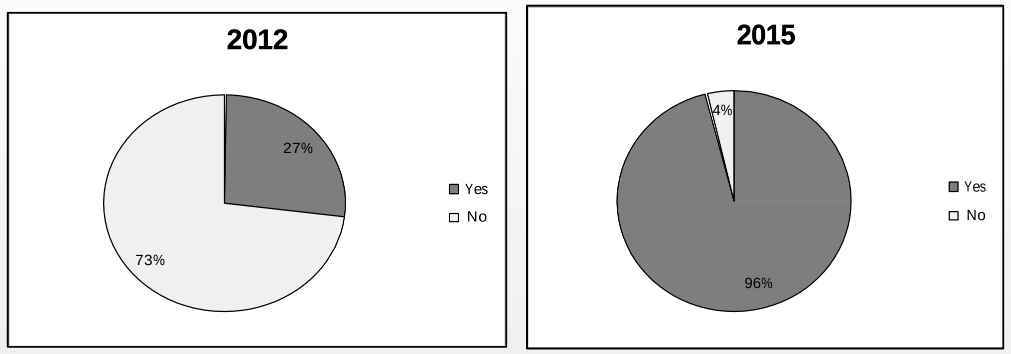
Strategic information management

Ensuring broader information management settings and practices encourage appropriate data sharing, use and re-use.

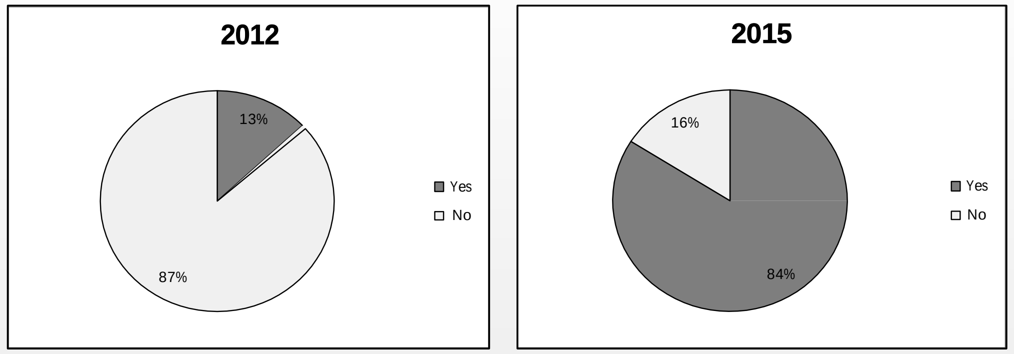
Immediate response **Build system-wide capability** **Leverage improvements**

SYSTEM-WIDE IMPROVEMENT ACROSS KEY INDICATORS OF OPERATIONAL PRACTICE

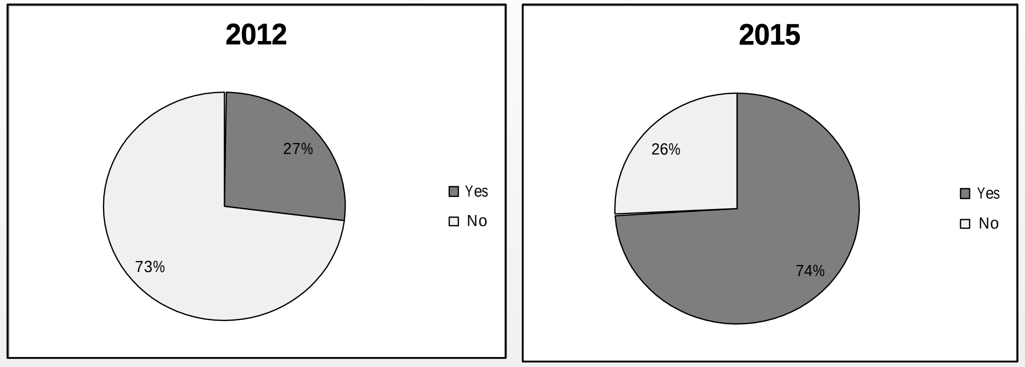
Agencies that have a formal security policy in place, supported by standards



Agencies that have formal certification and accreditation processes in place



Agencies that have formal security risk management processes in place

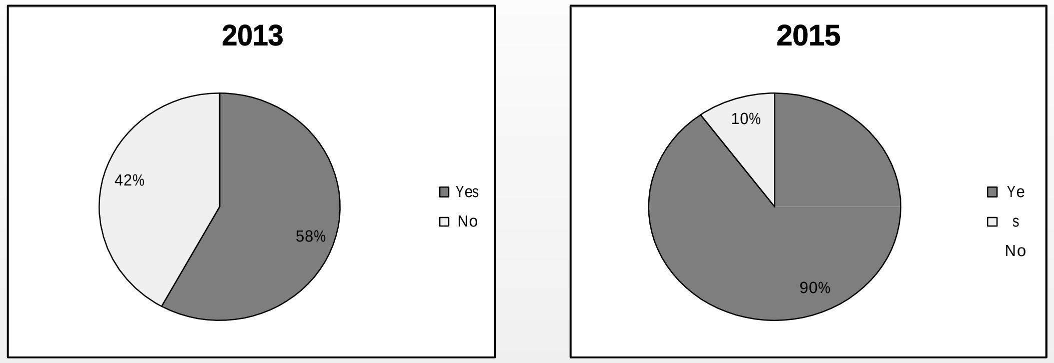


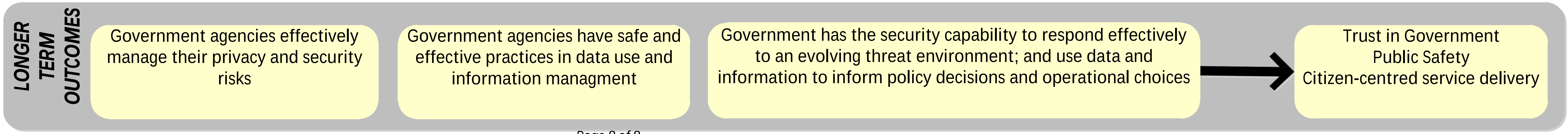
Agencies that have formal security assurance processes in place

2012

In 2012, the GCIO Review found inconsistent assurance over specific security activities and recommended agencies establish security assurance frameworks.

Indicators to measure progress were established from 2013 in response to this recommendation.





LONGER TERM OUTCOMES

Government agencies effectively manage their privacy and security risks

Government agencies have safe and effective practices in data use and information managment

Government has the security capability to respond effectively to an evolving threat environment; and use data and information to inform policy decisions and operational choices

Trust in Government
Public Safety
Citizen-centred service delivery