The OECD Council adopted on 15 July 2014 the Recommendation on Digital Government Strategies. The Recommendation provides a set of 12 principles structured around 3 pillars. The OECD Secretariat is developing a Digital Government Policy Toolkit to support OECD member countries and non-member adhering countries with the implementation of the Recommendation. This practice was submitted by the government of New Zealand to be considered as a good practice in the implementation of one or more of the principles contained in the Recommendation.

**Description of the practice:**

**Organisation:** Government Chief Technology Officer, Deputy Chief Executive, Service and System Transformation Branch, Department of Internal Affairs

**Name of the practice:** Cross-government programme to improve Privacy and Security across the State Sector

**Principles implemented:** Principle 4 – Reflect a risk management approach to addressing digital security and privacy issues, and include the adoption of effective and appropriate security measures

**Description:** Following a review of publicly accessible information systems by the Government Chief Information Officer (GCIO) in late 2012, the Government directed the GCIO to undertake a range of actions to improve privacy and security capability across the State sector.

A senior level Governance Group was established in April 2013 for a two year term to oversee a work programme of mutually reinforcing initiatives, including:

- Co-ordination and oversight of agency responses to the GCIO Review – confirmation of security assessments of all publicly accessible information systems and regular reporting of ongoing improvement plans in agencies

- The ICT Common Capabilities Panel for Security and Related Services was implemented in 2013 led by the Department of Internal Affairs. The ICT Security and Related Services Panel are an approved cross-government group of 34 industry experts contracted to provide government agencies with services and advice on a range of security and other related matters. For more information, see: [https://www.ict.govt.nz/services/show/SRS-Panel](https://www.ict.govt.nz/services/show/SRS-Panel)
Digital government toolkit

- Provision of tools, advice and guidance to agencies to assist them in building their capability including risk assessment tools, cloud consideration tools and GEA-NZ architecture artefacts. For more information, see: https://www.ict.govt.nz/guidance-and-resources/information-management/privacy-and-security/

- Establishment of the Government Chief Privacy Officer (GCPO) in early 2014. The GCPO leads an all-of-government approach to privacy, and is responsible for four main functions:
  - providing leadership, by setting the vision for privacy across government
  - building capability
  - assurance
  - engaging with the Office of the Privacy Commissioner, and citizens.

- The GCIO is responsible for providing the Government with system-wide assurance that ICT risks are being identified and well managed by agencies and across government as a whole, and that the benefits of ICT investments are being delivered. For more information, see: https://www.ict.govt.nz/ict-system-assurance/

- Development of more integrated and streamlined advice for agencies across privacy and security – providing clear expectations, guidance, advice and tools to support capability building. For example, The Protective Security Requirements (PSR) outlines the Government’s expectations for managing personnel, physical and information security. The PSR helps agencies manage business risks and assure continuity of service delivery, setting out what agencies must and should consider to ensure they are managing security risks effectively. For more information, see: https://www.ict.govt.nz/guidance-and-resources/information-management/privacy-and-security/

Results

Regular progress updates are provided on this work programme to the Minister of State Services. For more information, see: http://www.ssc.govt.nz/search/google_cse_adv/%22information%20privacy%20and%20security%22
**Development**

**Design:** The Information Privacy and Security Governance Group was set up to oversee the plan of action to lift privacy and security practice and capability across the State services.

It comprises senior-level executives from the public service and is chaired by the GCIO. The Privacy Commissioner also attends meetings of the Group.

**Testing:** N/A

**Implementation:** N/A

**Resources:** N/A

**Diffusion and scaling:** N/A

**Partnerships:** Civil Society

Partners: Privacy Commissioner

Nature of the partnership: Ongoing consultation with the Privacy Commissioner

**Lessons learned**

See links above. This is an ongoing policy process.

**Conditions required:** N/A

**Additional information:**