KPMG

COMMERCE COMMISSION NEW ZEALAND
Te Komihana Tauhokohoko

Review of information management and security

Terms of Reference

Background

1. In October 2019 computer equipment belonging to an external provider to the Commerce Commission (the **Commission**) was stolen in a burglary (the **incident**). The equipment contained [redacted] across a range of the Commission's work.

2. As a result of this incident the Commission engaged Richard Fowler QC to undertake an independent review of the circumstances that led to the incident.

3. In addition to the Richard Fowler QC review, the Commission has initiated this review of its information management and security.

Objective of the review

4. The Commerce Commission (the **Commission**) is entrusted with, creates, and disseminates information in the course of its operations, and effective, secure information management is important to public confidence in the Commission.

5. The objective of the review into information management and security (the **review**) is to complete an independent assessment of the Commission's information management and security and to report to the Board on the Commission's maturity, culture, control gaps, and improvement opportunities in relation to them.

6. The reviewer will make recommendations on how to address any issues identified in the review.

7. The focus of the review will be forward-looking with a view to building the Commission's capability and maturity in information management and security.

Appointment

8. The Board of the Commission has appointed KPMG (the **reviewer**) to conduct the review.

Nature and scope of the review

9. The reviewer will complete the review using the government's Protective Security Requirements (**PSR**) and industry best practice as frameworks against which to assess the Commission's information management and security.

10. The scope will include all information provided to the Commission by external parties, information generated by the Commission, and information shared or disseminated by the Commission.

11. The reviewer will:

    11.1 complete an independent assessment, and document its understanding, of the Commission's information management throughout the information asset management lifecycle (including storage location details, relevant third-party provider controls, and potential gaps and areas for improvement);

    11.2 identify the Commission's current maturity level at different points in that cycle; and

    11.3 recommend a target maturity level (or levels for different points or types of information) mindful of the work and size of the Commission and the type of information it holds.

12. The reviewer will:

    12.1 identify and review the adequacy of measures in place to safeguard critical information assets;

    12.2 assess the Commission's information management and security policies, practices, and culture as they relate to different Commission roles (staff, contractors, and third-party suppliers) including:

        12.2.1 whether information security policies and procedures are appropriate and fit for purpose;

        12.2.2 the level of awareness of the Commission's information security policies and procedures;

        12.2.3 the level of compliance with the Commission's information security policies and procedures;

        12.2.4 how the Commission's information security policies are communicated and implemented throughout a staff member's time at the Commission (covering the lifecycle from 'on-boarding', to 'on the job', and 'off-boarding'), and the cycle of engagement of a contractor and third-party supplier;

        12.2.5 the appropriateness and effectiveness of staff training and education around information security;

        12.2.6 the effectiveness of the process for staff to report a suspected information or data breach;

        12.2.7 the ways that information is communicated, shared, or disseminated (for example, in public places, over email, or other channels); and

12.3 assess the physical security controls in place for information security at each office and the level of alignment with accepted practice and Commission policies and expectations (including relevant on-site facilities management services);

12.4 assess the Commission's third-party supplier controls over Commission information and the level of appropriateness of those controls based on the nature of the information asset and the size of the provider including:

12.4.1 how information is shared or transmitted;

12.4.2 how it is destroyed;

12.4.3 clarity of procurement and contractual security and confidentiality obligations;

12.4.4 assurance obligations placed on the third-party provider;

12.5 assess the way the Commission handles information received from external parties in the execution of its role including the way the Commission might inform those parties of its information handling procedures;

12.6 seek to understand and advise on the extent of staff awareness of policy settings that restrict the use of external cloud service providers (other than those provided by the Commission) for processing, storage and sending of the Commission's information assets;

12.7 seek to understand and advise on the extent of contractors' use of external cloud service providers for processing, storage and sending of the Commission's information assets;

12.8 assess the design effectiveness of controls in place to detect potential deliberate or accidental data loss or misappropriation by staff or contractors (including, for example, cases where people may be disgruntled or have potential conflicts of interest);

12.9 assess the processes and controls in place for version control and publication of confidential information assets.

13. The reviewer will include in the report:

13.1 findings relating to information security and management maturity against the PSR mandatory requirements and best practice;

13.2 findings relating to information management culture and control gaps; and

13.3 recommendations relating to issues to address, including a prioritised list of recommended controls, processes, or practices that should be considered to address any information security risks.

Process

14. The reviewer will commence their review on 20 November 2019.

15. The Commission and its personnel will provide all reasonable assistance required by the reviewer towards completion of this review.

16. The reviewer will provide a draft report to the Board on or before 12 February 2020.

17. The reviewer will provide a final report to the Board on or before 25 February 2020.

18. The reviewer will, if asked by the Board, produce a summary of their final report at the same time as the final report, as per [25] below.

19. The estimated timeline for the review is set out in the table below and details of engagement on each of the phases (as described by the reviewer) are included in Appendix A:

Stage	Days	Est. Completion
Planning	2	20 November
Employee Survey	4	4 December
Meetings with Senior Management	4	24 January
Workshops	5	24 January
Control Assessment	6	5 February
Draft Report		12 February 2020
Final Report		25 February 2020

Confidentiality of review records

20. The reviewer acknowledges that all review-related material is received in confidence and in the expectation that such confidence shall be strictly respected. The reviewer agrees to hold securely all confidential information received during the review, and to return it to the Commission within 20 working days of completion of the final report, unless otherwise agreed by the Commission. This is subject to the requirement for the reviewer to retain material as required to meet professional practice obligations.

21. The reviewer agrees not to make any public comment in relation to the review, other than to confirm their appointment, unless agreed by the Commission.

22. The reviewer acknowledges that the Official Information Act 1982 applies to all information held by them on behalf of the Commission and will assist the Commission to respond to any request under that Act where requested to do so.

Relevant materials and interviews

23. The Commission will make available all relevant information and any of its members, employees or contactors to provide information to and / or be interviewed by the reviewer.

24. The reviewer will have regard to the findings and recommendations of the Richard Fowler QC independent review into the incident and recognises that the scope of the review may need to be amended in light of the findings of that review. The draft report from the independent review into the incident investigation is expected in early December.

Publication

25. The Board may discuss the review findings publicly and may decide to release the final report or a summary of it (subject to ensuring anonymity, privacy, protection of confidential information, natural justice obligations and suppression orders made by the High Court on 15 October 2019).

Timetable and Terms of Reference

26. The Board may amend the timetable for provision of the report and may amend these terms of reference (in consultation with the reviewer).

Dated: 20 November 2019

Anna Rawlings
Chair