Information Security Review Report

Commerce Commission

June 2020

kpmg.com/nz

Contents

Disclaimers

Inherent Limitations

This report has been prepared in accordance with our Contract for Services dated 8 October 2019 as varied by the Information Security Review Addendum dated 4 December 2019 (together our Contract). The services provided under our Contract ('Services') have not been undertaken in accordance with any auditing, review or assurance standards. The term "Audit/Review" used in this report does not relate to an Audit/Review as defined under professional assurance standards.

The information presented in this report is based on that made available to us in the course of our work by the Commerce Commission. We have indicated within this report the sources of the information provided. Unless otherwise stated in this report, we have relied upon the truth, accuracy and completeness of any information provided or made available to us in connection with the Services without independently verifying it.

No warranty of completeness, accuracy or reliability is given in relation to the statements and representations made by, and the information and documentation provided by the Commerce Commission as part of the process.

KPMG is under no obligation in any circumstance to update this report, in either oral or written form, for events occurring after the report has been issued in final form.

Any redistribution of this report requires the prior written approval of KPMG and in any event is to be a complete and unaltered version of the report and accompanied only by such other materials as KPMG may agree. Responsibility for the security of any electronic distribution of this report remains the responsibility of those parties identified in our Contract. KPMG accepts no liability if the report is or has been altered in any way by any person.

Third Party Reliance

This report is solely for the purpose set out in the Description of Services in our Contract and is not to be used for any other purpose or copied, distributed or quoted whether in whole or in part to any other party without KPMG's prior written consent.

Other than our responsibility to the Commerce Commission, neither KPMG nor any member or employee of KPMG assumes any responsibility, or liability of any kind, to any third party in connection with the provision of this Report. Accordingly, any third party choosing to rely on this Report does so at their own risk.

Internal Controls

Due to the inherent limitations of any internal control structure it is possible that errors or irregularities may occur and not be detected. Our procedures were not designed to detect all weaknesses in control procedures and consequently we do not express an opinion on the effectiveness of the internal control structure.

1. Executive summary

Introduction

Commerce Commission (the **Commission**) is entrusted with protecting the information it obtains and creates on behalf of a broad range of stakeholders. Handling this information appropriately and improving the information protection working practices and processes are obligations the Commission takes seriously.

Following a recent information security incident, the Commission requested KPMG to perform an independent assessment of the controls in place across its information asset lifecycle; including but not limited to information held or accessible by its external providers. Based on our independent assessment which was completed during the period December 2019 to February 2020 we summarise below our findings and recommendations.

This report summarises our approach and the results of the work performed in accordance with the Contract for Services agreed between the parties. The specific details of all fieldwork completed that have led to the findings and recommendations has not been included as part of this report.

Our high level approach

Our high-level approach included but was not limited to the following:

- Obtaining and assessing relevant documents: policies (refer appendix 5), procedures and operating manuals.
- Interviewing key staff responsible for staff induction and training and overall information security at the Commission.
- Interviewing key staff responsible for key information security processes and controls, assessing any supporting documentation or evidence to assess design effectiveness.
- Conducting site visits to the Auckland and Wellington offices, interviewing key staff responsible for physical security controls and assessing any visible controls in place.
- Interviewing key staff primarily involved in managing third party relationships including those who provide information to the Commission or recipients of information provided by the Commission.
- Interviewing senior management to understand the expectations of staff in relation to information security and to highlight any known risks.
- Conducting control workshops with key groups of staff identified by management as responsible for managing in-confidence information.
- Completing a staff survey to better understand the level of awareness, culture and working practices in relation to information security.
- Conducting controls testing based on the 33 agreed controls defined within the Protective Security Requirements (PSR).

The outputs from all the above were correlated and baselined against PSR and industry accepted practice to determine the level of organisational maturity, the detailed findings and areas for improvement and any high-level themes and potential systemic issues.

It is important to note that our approach also applied a top down methodology. This means that while many controls were tested, in some cases where there was no formal framework, strategy, policy, or process documentation further testing was not always completed.

In this situation we applied our professional judgement to determine whether controls testing could be performed to sufficient levels to provide management with the confidence that the control or process would be consistently enforced across the organisation and aligned to the risk profile of the organisation. Consequently, our findings and recommendations are both detailed and strategic in nature.

High level summary and recommendations

The Commission have implemented a number of processes and controls that appear fit for purpose and there is a strong culture and awareness among its staff. We have provided further information on the positive aspects and areas for improvement that were identified during this engagement by the following categories below:

- Culture
- Policies and Procedures/Working Practices
- Third party and contractor controls
- Control effectiveness

Based on the controls that were assessed we noted that the Commission has a moderate level of maturity.

However, the Commissions approach to determining the controls to be deployed and the implementation was in many cases largely informal. The control environment has been created in the absence of some key organisational considerations (**Finding 6**):

- The key information security risks and associated risk appetite, including those related to third parties, being defined to an appropriate level of specificity.
- A formalised Information Management Lifecycle that includes both people, process and technology related controls.
- The specific nature and type of information being managed by the Commission that is considered at-risk, where this information resides, who has access and clarity around ownership of controls.

Some aspects of the above may be clearly defined however there is no holistic and integrated view that is part of a broader framework. These factors provide important context when assessing the effectiveness of the controls relative to the Commissions situation and should provide the foundations of how the Commission implements the report recommendations. These factors should also form the basis of the target maturity for the organisation which we would expect to be high for, as a minimum the handling of in-confidence information.

It is also critical that once defined, staff and third parties are also made aware of these to help reinforce and explain why effective information security and management practices are considered critical at the Commission.

The lack of these important factors does not necessarily mean that all controls will be ineffective. It can however create potential control gaps or a control environment that does not align to the organisation's definition of an acceptable level of risk.

Reviewing the information security risks, risk appetite Information management lifecycle, at-risk data and continuous monitoring and reporting on the implementation and effectiveness of the recommended improvements will help ensure that controls continue to remain relevant and effective.

The recommended tactical and strategic improvements to technical, people and process related controls outlined in this report will help increase the overall effectiveness of information handling practices at the Commission.

Culture

The staff survey results and perspectives obtained from senior management interviews indicate there is alignment of expectations and strong culture of openness and accountability in relation to information security. Staff appeared to understand the importance of the information they deal with and were generally taking a cautious approach to the handling and sharing of information.

As would be expected following the information security incident, our survey, interviews and workshops confirmed that there is a low level of confidence that third parties and contractors adhere to information protection working practices and processes.

Policies and procedures / Working practices

We note that the Commission has a comprehensive set of information security policies that align with accepted practice and are generally fit for purpose. No significant policy gaps were identified. The policy requirements however are not consistently translating into staff working practices. The key gaps we noted were:

- Some staff are unclear on the information classifications, what information is included in each category and what controls need to be applied. The implementation of the relevant policies currently lacks sufficient context for staff that "brings them to life" (**Findings 3 and 5**).
- While staff are confident that they will be supported when reporting a potential incident, the escalation process itself is not as visible to allow them to easily do so (**Finding 10**).
- There are some inconsistencies in the requirements across the policies and insufficient levels of specificity of requirements and expectations of staff in some areas (e.g. what are mandatory requirements, what requirements apply depending on the information classification). For example, the Clear Desk policy was consistently raised as being an area that requires further clarity. These issues could result in inconsistent application and interpretation and unintended working practices, which increase the risk of a compromise. (**Finding 15**).
- The Information security policy framework states that all confidential information should be redacted. There is however no detailed process

that outlines how this is to be achieved, the criteria applied and who is responsible for aspects of the process. (Finding 13).

- There is a formal process for the publication of online information and management approval is for any high-risk information which is viewed prior to publication. The process does not allow for the "pre-loading" of information on the website prior to publication. All requests are logged and retained and there are appropriate security controls designed to restrict access to the Content management platform which is third party hosted. [redacted] (**Finding 14**).
- To improve the overall effectiveness of the policies and procedures management should implement a focused formal training and education program for all staff and contractors that is designed to clarify key areas of the policies and help embed the expected behaviours (**Finding 5**). We understand that a formal staff training program is planned but has not yet been implemented. The training programme should be considered both at onboarding and while they remain employees.

Third party and Contractor controls

The Commission frequently uses contractors and third parties who have specialised skillsets. We noted the following that align with accepted practice:

- Contractual obligations have recently been strengthened, in line with All of Government (AoG) and MBIE recommendations. Additional confidentiality requirements have also been mandated over and above AoG and MBIE requirements.
- The approval process appears robust and IT systems access accounts are automatically disabled in line with the agreement terms with further approval required to reactivate.
- Approved third parties are provided with secure connections to remotely access the [redacted].
- Third parties were asked to confirm that they adhere to better practice control frameworks like PSR and NZISM. While largely positive responses were received the level of detail in responses varied widely. From a sample of these responses we noted that the suppliers have affirmatively stated that they use control frameworks ranging from NZISM to ISO 27001 and controls around data retention and destructions were followed.

We noted some areas where improvements are required to reduce the risk of an information security incident:

- There is no mandatory requirement for contractors to attend formal induction training when they are onboarded (**Finding 5**).
- Contractors are now required to use The Commission devices that have encrypted hard drives however this is not codified into policies and contractual obligations (**Finding 13**).
- While the security policy provides guidance to staff and contractors on their responsibilities of handling in-confidence information and the inappropriate use of unauthorised cloud providers [redacted] (**Finding 7**).
- There is no formal third party risk management framework which categorises the level of risk of all third party providers and the associated security requirements and assurance requirements based on the level of criticality (**Finding 1**).
- Data is being shared with external parties like courts and legal counsels on a USB or a hard drive. [redacted] (**Finding 13**).

Control effectiveness

The Commerce Commission has implemented many of the expected processes and controls required by the Protective Security Requirements (PSR).

Specifically, we noted the following that align with accepted practice:

- A risk management framework is in place with oversight by the Audit and Risk Committee. A three-year assurance program was documented and approved.
- Disaster recovery plans are documented with clear Recovery Time and Recovery Point objectives.
- An incident management procedure exists, and this requires that all incidents reported are logged and responded.
- Employee hiring and termination procedures were in place including the expected background verifications.
- Access to systems requires a formal approval process to be completed.
- Physical security controls for building access at both locations suitably restricted access to authorised staff/contractors and visitors were required to be escorted while on the premises.
- Server rooms have [redacted].
- Appropriate restrictions are in place for staff/contractor work areas and secure destruction bins are in place for disposal of confidential information.
- IT equipment is required to be re-formatted prior to re-deployment or securely destroyed in the event usage is discontinued (e.g. obsolescence).
- Document management systems (e.g. File site and Office 365) are configured to log access to documents and provide the IT team capability to identify any potential breaches.
- Some data loss prevention measures are in place (refer **Finding 3**) to detect potential loss of data and are monitored by the IT team.

There were however some areas where improvements are required in relation to process and technical controls which, if not addressed could undermine the strong risk and security culture and increase the risk of an information security incident. These findings are detailed later in the report however we have summarised the key findings below:

- [redacted] (**Finding 2**).
- Various controls have been implemented to detect or prevent data loss however there is no holistic strategy/approach that is based on a comprehensive risk assessment and understanding of key information flows which could result in potential control gaps (**Finding 3**).
- [redacted] (**Finding 4**).
- User access reviews are not completed on a regular basis to confirm user access and the associated privileges are appropriate (**Finding 8**).
- An information security incident process has been defined in the security policy however it requires a deeper level of detail to be effective (**Finding 10**).

We did not identify any significant issues in relation to the working practices in the different geographic office locations. Our findings were consistent across all locations.

The findings from this assessment also tend to indicate that the following in regards to PSR/NZISM requirements (refer **Finding 6**):

- The approach to determining the controls to be implemented appeared to be informal and not based on a risk assessment from which the level of applicability of PSR and NZISM requirements can be determined. Management should confirm its key information security risks and develop a Statement of Applicability which outlines how it will comply with the PSR and NZISM requirements.
- There is limited monitoring and regular operational reporting of the effectiveness of information security controls, outside of the assurance programme, which has visibility at the senior management and Board level. Developing a consistent set of report metrics, together with the results of the assurance programme will enable management and the Board to proactively manage its information security risks.

Given the recent information security incident it is critical that management also formalise the extent to which the outcomes from the above actions will be applicable to third parties and contractors. In other words:

- Confirm which policies and procedures also apply to third parties and contractors.
- Which aspects of PSR/NZISM should also apply to third parties and contractors.
- The extent of formal reporting required from third party providers to demonstrate their compliance.

Our interviews also highlighted that management's perception is that the majority of information that the Commission manages is publicly available. This should be formally validated and should be used as a valuable input into how the organisation assesses its risk and control requirements.

The scope of this engagement focused on both the culture and working practices along with key technical controls. Consequently, there are potential controls that may not have been tested which may have been implemented and are operating effectively. In addition, the majority of the findings were, in our experience, consistent with many other public and private sector organisations.

2. Summary results

Survey findings

To better understand the current culture and working practices an anonymous staff survey was conducted. There were 158 responses across all The Commission locations.

The survey indicated some positive staff responses:

- All respondents believe that protecting the information is everyone's responsibility.
- **95%** of respondents feel that the Commission has a comprehensive Information Security Policy and clear data protection requirements.
- **92%** of respondents felt that they were confident in reporting any breaches. However, **22%** feel that the culture is not strong enough to encourage the breaches to be reported.
- **90%** of the respondents believed that they would be appropriately supported during an information security breach incident (however **24%** of the respondents felt they do not have appropriate knowledge of the information security incident reporting process).

Some potential areas of focus were also identified some of which management are already aware of:

- **26%** of the respondents feel that they are not aware of the types of in-confidence information that the Commission maintains.
- **18%** of the respondents felt that they do not know the policies around using unapproved software (including cloud).
- **46%** of the respondents believe that their induction did not sufficiently cover the expectations and level of importance of robust information handling practices.
- **44%** of the respondents believe that the clear desk policy is not appropriately implemented at the Commission.
- **29%** felt that staff and third parties do not consistently adhere to the information security policies across the Commission.
- **37%** do not feel adherence to policies is enforced, particularly with third parties.
- **46%** disagree that third parties take information security seriously.
- **64%** of respondents feel that appropriate Information Security Training is not provided on a periodic basis.
- **46%** of the respondents appear to be aware of risks that are not being addressed.

Regarding the last observation, we were unfortunately unable to obtain significant specific examples from the workshop participants in support of this result.

Key insights from Senior Management interviews

From our workshops with senior management, we understand that management is concerned about the following:

- There is a lack of centralised and formal documentation for all key information management processes in particular those associated with in-confidence information.
- There is no consistent location where certain types of information is stored, which can cause considerable delays in resolving a complaint / other issue in addition to unnecessary duplication and potential loss of fidelity.
- Consistent with the survey results management acknowledged that some policies and procedures (e.g. clear desk policy) are open to interpretation.
- Expectations are not clear about sharing information with other agencies / bodies outside The Commission. (e.g. CLAG, Courts).

These insights indicate that a formal information management framework with clear roles and responsibilities would be beneficial.

Controls Assessment Results

We assessed 33 key PSR controls to understand their design effectiveness. These included the following domains:

- Security Governance
- Personnel Security
- Information Security
- Physical Security

A total of 20 requirements were prescribed by PSR through these four areas. We have identified 33 controls at The Commission that addresses the mandatory requirements. We have reviewed these controls through interviewing the control owners, observing the control being performed and inspecting relevant documentation. Apart from these controls tested, we have considered other factors/controls that influence the control environment throughout the

other phases of the engagement - survey, workshops and interviews.

Of the controls tested 16 were considered effective, 11 were ineffective and 6 were partially effective. The summary results are included in Appendix 3.

Detailed Findings Summary

Summarised below are the number of findings and the associated risk ratings.

	High	Medium	Low
Total findings	4	7	4

Our detailed findings and recommendations are included in Section 3 of this report.

3. Detailed Findings and Recommendations

1. A Third party risk management framework has not been implemented	Rating: High

Finding

We note that while The Commission has leveraged relevant All of Government (AoG) and MBIE templates and expertise for specific aspects of third party risk management. This includes:

- GMC contract templates
- Including specific confidentiality clauses
- Leveraging the cloud risk assessment framework
- Confirming the control practices of high-risk third-party organisations via email confirmation.

There is however no formal third party risk management framework which categorises the level of risk of all third party providers and the associated security requirements.

In addition, we noted that while Contractors are now required to use The Commission devices that have encrypted hard drives, this is not codified into policies and contractual obligations.

Impact

- Poor controls at third party organisations that connect to The Commission's network, or that deal with The Commission's in-confidence data, could jeopardise the security and integrity of that data.

Recommendations

- A formal third party risk management framework should be developed that outlines how The Commission intends to manage its third parties. This should also include considerations for contractors - both general and specialist.
- A checklist-based review of the security practices at contractors/third party organisations should also be considered. The checklist can be a self-assessment, but it should ensure all appropriate control areas are covered and the level evidence a third party is required to provide.
- For key high-risk vendors The Commission should seek independent assurance reports or where appropriate exercise the right to audit the third parties' controls.
- Minimum security expectations for contractors should be established, communicated, and included in contracts.

2. [redacted]	Rating: High

Finding

[redacted]

Impact

- [redacted]
- [redacted]

Recommendations

- [redacted]
- [redacted]

3. There is no formal strategy for Data loss detective/preventative controls	Rating: High

Finding

We understand that currently there some appropriate controls in place to specifically detect potential data loss events (e.g. within Filesite and Office 365). This includes tracking large movements/deletion of data and these events are alerted and responded to by members of the IT team.

These controls have been implemented based on functionality available within specific applications. We noted however there is no holistic strategy/approach to ensure that based on the level risk and the data sources and data flows that all potential data loss scenarios have been considered and controls are implemented where appropriate.

In addition, while The Commission has a data classification policy in place requiring documents to be classified, we understand from the workshops and interviews that this is not regularly adhered to by staff and contractors. To be effective most data loss tools require some form of classification at a data or document level to be in place and this tends to rely on users proactively applying the appropriate classification. If users are unclear this could result in potential data loss events not being detected.

From the survey some staff indicated that they are unaware of the defined classifications.

Impact

- Lack of [redacted] document classification could result in inappropriate handling of the document, inappropriate sharing of the document outside the organisation or unauthorised data loss.

Recommendations

- To ensure classification and data loss prevention is effective and that any risk assessment is robust, The Commission should first document the locations of all in-confidence data. Where possible The Commission should consider streamlining the data and document repositories.
- Based on the analysis above a strategy should be developed to ensure controls are in place for all identified high risk scenarios.
- The Commission should ensure that the documents are classified as per the data classification policy/procedure in place by providing appropriate training and education.
- Management should consider other tools that can help detect/prevent intentional or unintentional data loss to enhance existing capabilities.

4. [redacted]

Rating: High

Finding

[redacted]

Impact

— [redacted]

Recommendations

— [redacted]

— [redacted]

5. Lack of periodic security awareness training

Rating: Medium

Finding

The Commission has fit for purpose policies and induction processes and 'during employment' processes to support its staff and to onboard contractors.

We noted however there is no formal information security awareness programme across the organisation that provides regular training and education. We understand that currently, on a yearly basis, an email is sent to staff asking them to re-confirm compliance with policies like the Code of Conduct and other mandatory policies and that management has prepared appropriate training modules, but these have not yet been implemented.

We further understand that this training is not mandatory for contract staff. Contractors typically do not go through the induction process intended for staff (including fixed term employees) but in case of some of the branches (e.g. Competition, Consumer, and IS), the importance of confidentiality is reiterated through floor meetings. As contractors often have the same access as other staff, they should be given similar training on expectations.

Impact

- Without periodic reminders of information security risks and responsibilities, staff and contractors will not have an up-to-date understanding of accepted information security practices, threats and risks, which might lead to unintentional behaviour that impacts the organisations information security posture.

Recommendations

- The Commission should implement a formal information security awareness programme that applies to all persons that access The Commission systems and data. In addition to online or classroom-based training, the program could include posters across the office on expected security behaviours, yearly refresher trainings, workshops, etc. It is important that the focus is not solely compliance based (i.e. passing a test) and that educating users is the primary objective.
- Improvements in awareness should be measured appropriately, and the awareness programme adjusted accordingly.
- Further training on broader information processes and procedures could also be incorporated into the process to ensure staff are aware of tools available and how information should flow and be managed within The Commission and with external parties.

6. PSR and NZISM Compliance	Rating: Medium

Finding

Managements approach to determining the controls to be implemented appeared to be informal and not based on a comprehensive risk assessment from which the level of applicability of PSR and NZISM requirements can be determined.

There is limited monitoring and regular operational reporting of the effectiveness of information security controls, outside of the assurance programme, which has visibility at the senior management and Board level.

Impact

- In the absence of a comprehensive understanding of the nature and extent of information managed by The Commission, an understanding of the level of associated risk, formal alignment to NZISM and PSR requirements and regular reporting on control effectiveness, there is increased likelihood of ineffective or missing controls.

Recommendations

- Formally validate the nature and extent of public and in confidence information retained by the Commission and use this as a valuable input into how the organisation assesses its risk and control requirements.
- Confirm the key (and specific) information security risks and develop a Statement of Applicability which outlines how it will comply with the PSR and NZISM requirements.
- Develop a consistent set reported metrics that indicate the effectiveness of information security controls, that together with the results of the assurance programme will enable management and the Board to proactively manage its information security risks.
- With respect to third parties:
  - Confirm which policies and procedures also apply to third parties and contractors.
  - Confirm the aspects of PSR/NZISM should also apply to third parties and contractors.
  - Formalise the extent of formal reporting required from third party providers to demonstrate their compliance.

7. Approved IT services are not clearly defined

Rating: Medium

Finding

There is currently no comprehensive list of approved software and guidance on appropriate use of this software, particularly in relation to cloud based software that staff may subscribe to on a personal basis that could also be used for work purposes (e.g. personal productivity tools such as Evernote).

Staff and contractors have the capability to access general/personal cloud storage and email applications using The Commission devices. While most contractors use The Commission-provided equipment (laptops), the capability of these machines to access other cloud platforms and to redirect mail to home addresses puts The Commission's data at risk.

We further understand that The Commission uses Box.com for bulk information sharing. [redacted] We noted from the survey and workshops that staff are aware that they should not use any other cloud platform to share/store the information, [redacted]

In our survey,18% of the respondents also felt that they did not know policies around using unapproved software.

Impact

- The ability for Staff and contractors to share the data through unapproved methods and channels or to potentially allow malware into the organisation could increase the risk of compromise of The Commission's in-confidence data or systems.
- Personal cloud based services often have terms and conditions which allow the service provider to access or have ownership of data stored on their platforms which increases the risk of loss of control of corporate data.

Recommendations

- [redacted]
- A clearly defined policy should be developed that outlines the approved services and how they are to be used to support any controls and clarify expectations for staff/contractors.

8. User access reviews are not regularly performed

Rating: Medium

Finding

We noted that there is no regular process to review user accounts and access rights on a periodic basis for the network or applications to reduce the risk of dormant users and/or users with inappropriate access. This requirement is not specified in the Information Security Policy.

Impact

- [redacted]
- [redacted]
- [redacted]

Recommendations

- [redacted]
- The HR onboarding and off-boarding process should be reviewed to ensure there is regular notification of new and terminated staff and contractors to IT to action
- The Information Security Policy should be updated to require periodic user access reviews for the network and key applications

9. Roles and responsibilities for information security and management are unclear	Rating: Medium

Finding	Recommendations
There is no formal information security or information management framework which outlines roles and responsibilities for all staff. Key roles and responsibilities have been defined (e.g. CIO, CISO and CPO) however the roles and responsibilities for example of department heads with respect to information security are not formalised. Consequently, roles and responsibilities for some functions such as User Access Reviews are unclear. **Impact** — There is increased risk of gaps in controls if roles and responsibilities are not clearly defined.	— Establish an Information security and/or Information management framework that clearly outlines roles and responsibilities. — Key aspects of this framework should form part of the training and education programme.

10. Incident Management process lacks detail	Rating: Medium

Finding

We noted that The Commission has a information security incident management process defined as a part of its information system security policy document. However, this process is only at high level and excludes descriptions of various types of incidents, out of office hours contacts, and key templates are not available. The current incident template is also only available to the IS team.

While staff are confident that they will be supported when reporting a potential incident, the escalation process itself is not as visible to allow them to easily do so.

Impact

— The lack of a detailed incident management process could result in inconsistencies in reporting and effectively managing incidents.

Recommendations

— The Incident management process should detail the possible scenarios (including run sheets for common incidents), provide detailed guidance on reporting the incident, have contacts for regular and outside the office hours, escalation mechanisms, and templates like an incident reporting form for users to be able to follow on their own.

— The definition of a security incident and the process for reporting it should be clearly communicated to all staff.

— In our experience a separate incident management process for information security incidents is not required and can be incorporated into the organisations broader incident management process.

11. [redacted]

Rating: Medium

Finding

[redacted]

Impact

- [redacted]

Recommendations

- [redacted]
- [redacted]
- [redacted]

12. Physical security controls on the IT storage room [redacted]

Rating: Low

Finding

Physical security controls over the IT server room aligned with accepted practice with restricted access in place. [redacted]

Physical security controls for building access at both locations suitably restricted access [redacted]

Appropriate restrictions are in place for staff/contractor work areas and secure destruction bins are in place for disposal of confidential information.

Impact

- [redacted]
- [redacted]

Recommendations

- [redacted]
- [redacted]

13. Data sharing processes are informal	Rating: Low

Finding

We understand that currently there some appropriate controls in place to specifically detect potential data loss events (e.g. within Filesite and Office 365). This includes tracking large movements/deletion of data and these events are alerted and responded to by members of the IT team.

Contractors are now required to use Commission approved devices that have encrypted hard drives however this is not codified into policies and contractual obligations.

Through the workshop discussions, we understand that data is being shared with external parties like courts and legal counsels on a USB or a hard drive. [redacted]

The Information security policy framework states that all confidential information should be redacted. There is however no detailed process that outlines how this is to be achieved, the criteria applied and who is responsible for aspects of the process.

Impact

- [redacted]

Recommendations

- The use of removable media for the transfer of data should be reviewed. If this is still required, the policies around the use of any removable media (USB/ external hard drive and laptops) should be clarified [redacted]
- Management should also consider mandating the use of existing or alternative file sharing tools (e.g. Filesite) for more sensitive data.
- Ensure the requirement for all contractors to use Commission approved devices is included in the appropriate contracts and policies.
- Define and implement a formal process for the redaction of confidential information including the criteria applied and roles and responsibilities.

14. [redacted] online publication platform	Rating: Low

Finding

There is a formal process for the publication of online information which includes the following that aligns with accepted practice:

- Communication to all staff of the new formal process and which is published in a centralised location.
- Management approval for any high-risk information which is viewed prior to publication.
- Not allowing for the "pre-loading" of information on the website prior to publication.
- Logging and retention of all change requests.
- Appropriate security controls designed to restrict access to the Content management platform.

[redacted]

- [redacted]
- [redacted]
- [redacted]

Impact

- [redacted]

Recommendations

- [redacted]
- [redacted]
- [redacted]

15. Policy and procedure documents may not be aligned	Rating: Low

Finding

We noted that the Commerce Commission has a comprehensive set of Information management and security policy and procedure documents that were assessed as generally aligning with accepted practice. While each policy and procedure is reviewed on a regular basis there is no holistic formal review across all documents that ensures:

- Consistency of requirements across all of information management/security policies and procedures.
- There are sufficient levels of specificity of requirements and expectations of staff (e.g. what are mandatory requirements, what requirements apply depending on the information classification).

Impact

- In the absence of a holistic review there is increased risk of gaps or inconsistencies in requirements which could result in staff/contractors not applying expected practices.

Recommendations

- The Commission should consider implementing a formal review process of all Information management and security policy and procedure documents. This could occur as part of the current review cycle process.
- The planned training and awareness modules should also be reviewed for consistency and alignment once the holistic review has been completed.

KPMG

Appendices

Appendix 1: Our approach

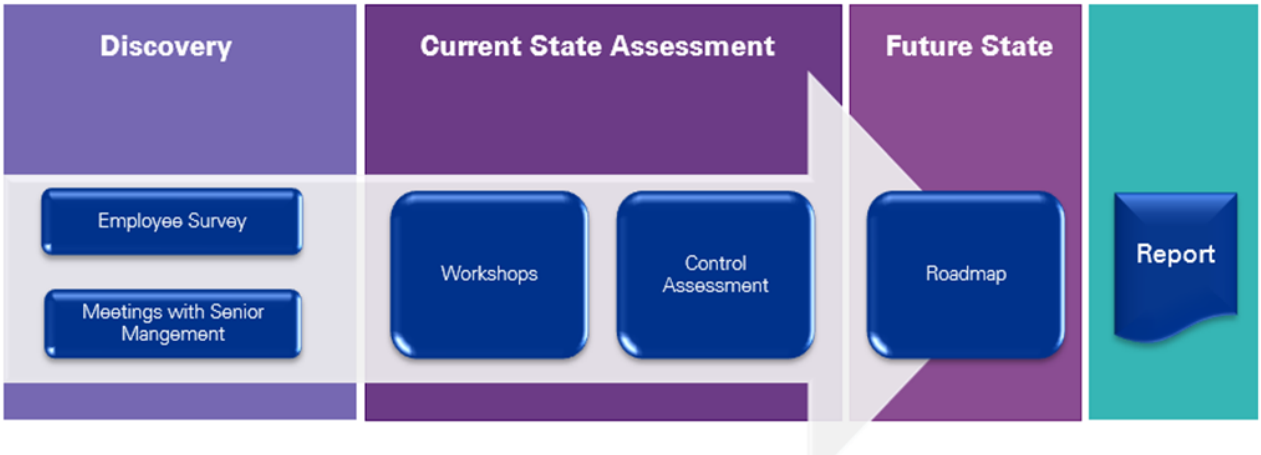
Detailed Engagement approach

The below summarises the detailed approach and estimated timelines for the Information Security Review. The objective is to ensure that an efficient and effective approach is taken to providing management with a forward looking view of potential improvements in information security practices, controls and culture by:

- Documenting our understanding of the various critical information asset lifecycles including storage location details, relevant third party provider controls and potential gaps/areas for improvement.
- Providing management with an understanding of the information management and protection culture and practices across the different Commission roles (staff, contractors and third party suppliers) including:
  - the level of awareness of the Commerce Commission's information security expectations and how these are communicated and enforced throughout the staff members lifecycle (on boarding, on the job and off-boarding)
  - the level of consistency of practices between the different office locations
  - the appropriateness and effectiveness of staff training and education
  - the effectiveness of the process for staff to report a suspected information/information security incident.
- Assessing the physical security controls in place at each office location to understand the level of alignment with accepted practice and Commission policies and standards including relevant on-site facilities management services.
- Assessing consistency of third party / vendor controls and the level of appropriateness based on the nature of the information asset they manage and the size of the provider including:
  - how information is shared / transmitted and destroyed
  - clarity of procurement and contractual security and confidentiality obligations
  - assurance obligations.
- Understanding the extent of staff / contractor use of unauthorised external cloud service providers for processing and storage of critical information assets (Note: This will be limited to understanding the level of awareness of Commerce Commission expectations and will not include a comprehensive list of all cloud services in use).
- Assessing the design effectiveness of controls in place to detect potential deliberate or accidental data loss or misappropriation by staff / contractors on an ongoing basis and in cases where they be disgruntled or have potential conflicts of interest.
- Understanding the processes and controls in place for version control / publication of confidential information assets.

Our high level approach is summarised below:

High level phases:



Employee Survey:

We will conduct a short survey for staff within Commerce Commission to complete. This will provide us with an initial baseline of the information security culture at the Commerce Commission and will be used in conjunction with data from later phases to understand the level of correlation between the security culture and controls that have been implemented.

The survey will focus on:

- Information security guidelines/ requirements at Commerce Commission
- Classification of information
- Requirements of handling sensitive information
- Incident identification and reporting
- Awareness on protection of physical assets.

The intended outcomes of the survey includes:

- Measuring employee awareness of their information security responsibilities
- Providing an indication of come current practices and their alignment to Commerce Commission expectations
- Understand employee perceptions of how well security is working, and highlight where improvements in security culture are required
- Assessing employee understanding of the relevant threats and the level of security consciousness
- Assessing employee understanding of their responsibilities and the process for identification and reporting of information security incidents.

Meetings with Senior Management:

We will hold meetings with relevant senior management to understand the information security policies and expectations along with classification of information at the Commerce Commission. We will also obtain and review available supporting documentation such as policies, procedures. We will also obtain and review any reports relating to previous reviews that may be relevant to the agreed scope.

The objective of this phase is to gain an understanding of the tone at the top and management's expectations of staff and third parties with respect to information security in the most efficient and effective manner.

Workshops:

KPMG will facilitate design-led workshops with staff as an efficient way to gain a high level understanding of key information flows and controls/practices. The objective of these workshops is to discuss and document key information process flows and controls/practices for the handling of both digital and physical information.

We will require management's assistance to select the workshop attendees and to ensure the intent and purpose is clearly communicated to ensure staff openly share their practices and potential areas for improvement.

We propose four workshops with up to ten attendees that deal with key information assets. We would suggest that these workshops include sessions at both your Wellington and Auckland offices.

The key workshop topics include but are not limited to:

- An overview of the information handling processes followed
- Known control exceptions/areas for improvement
- Forward looking discussions on potential improvements
- Other areas of concern.

We will agree an appropriate workshop schedule with you.

Control Assessment

The outcomes from previous phases along with the "hot spots" already identified by management will help identify other specific areas that may require further assessment.

Our approach will include but is not limited to:

- One-on-one interviews with identified people
- Walkthrough of identified process/controls as per PSR
- Review of relevant documents as needed

We will not perform any detailed testing to assess operating effectiveness.

Reporting

We will provide report including an overview of the current level of maturity and a prioritised list of recommended controls or processes that should be considered to address information security risks.

The report will include a list of findings and control and/or culture related to gaps in information management/protection along with our assessment of your maturity against PSR mandatory requirements in this domain.

Appendix 2: Ratings and classifications

Risk rating

The risk rating assigned to the findings is determined based on an assessment of the impact of the business and the likelihood of the risk occurring, defined as follows:

Rating	Definition
LOW	Matters which are unlikely to have a significant impact on the system of internal control but should be addressed as part of continuous improvement.
MEDIUM	Matters which are important to the system of internal control and should be addressed as soon as possible.
HIGH	Matters which are fundamental to the system of internal control. The matters observed can seriously compromise the system of internal control and data integrity and should be addressed as a matter of urgency.

Appendix 4: Detailed survey results

Total Respondents	160
Survey Questions	
1. How many direct reports (if any) do you have in your role at the Commission?	Ranges from 0 to 25 - 160 responses
2. Which of the below best describes your role at the Commission? a. Full-time employee b. Part-time employee c. Contractor d. Consultant e. Other (please Specify)	FT-139 PT- 10 Contractor - 2 Other - 7

	In Percentage			
	Strongly Agree	**Agree**	**Disagree**	**Strongly Disagree/ Don't Know**
3. The Commerce Commission takes information security seriously and has a comprehensive Information Systems Security Policy Framework in comparison to other organisations I have worked at.	34	60	6	1
4. The Commerce Commission's data protection requirements are clear, and I know how to apply them within my working environment	18	66	15	1
5. Regular Information security awareness training (either in person or computer based) is provided that helps me understand the risks and my responsibilities.	5	31	60	4
6. It is my responsibility to report any incident involving a potential information security breach that I become aware of.	77	23	0	0
7. I know how and where to report a security or information security incident if I become aware of one.	31	45	11	13
8. I am aware of the different types of "In-Confidence" information we manage and what I am expected to do to protect this information.	18	56	26	0
9. I am expected to use only approved methods to remotely access the Commerce Commission's network	99			1
10. There are clear policies and guidelines provided that help me understand the risks and my responsibilities for installing non-approved software or applications on a work device.	24	58	17	1

11.	It is my responsibility to protect the information I have access to in accordance with our policies and standards.	66	34	0	0
12.	I consistently follow the Commerce Commission's processes for externally sharing information classified as In-Confidence.	57	39	4	0
13.	The Commerce Commission's clear desk policy is effective in managing and protecting In-Confidence information.	8	48	35	9
14.	I consistently follow the Commerce Commission's policy on the disposal of physical assets (e.g. Printed material classified as "In-Confidence", USB drives, computers and mobile devices)	46	49	5	1
15.	Staff and third parties consistently adhere to the Commission's information handling and security requirements.	6	65	25	4
16.	There is a strong culture of encouraging staff to report potential information security policy violations related to other staff or third parties.	23	54	21	1
17.	I feel confident and supported in reporting potential violations of information security to management.	40	52	7	0
18.	My induction adequately covered the expectations for all staff in relation to Information Handling and Security requirements.	10	43	43	3
19.	There is appropriate ongoing training and education in relation to Information Handling and Security requirements and potential threats to our organisation.	4	26	66	3
20.	Information Handling and Security requirements apply to and are consistently enforced for everyone in the Commission, including third parties.	5	57	36	1
21.	Ensuring In-Confidence information is protected is the sole responsibility of IT	2	4	43	51
22.	Our Information Handling and Security practices would be considered as operating at "best practice" levels.	6	55	38	1
23.	Third parties and contractors are equally as concerned about protecting In-Confidence information as we are	4	51	42	4
24.	There are known risks in how we are protecting In-Confidence information which we are not addressing	2	38	57	2
25.	I feel confident that if an accidental information security incident occurred the staff involved would be supported	27	63	9	1

Appendix 5: Policies provided

The Information Systems Security Policy Framework, that consists of:

- Acceptable Usage
- Data Protection
- Guest Wireless network
- Mobile Device usage
- Passwords and pass phrases
- Account management policy (details contractor account management as well)
- Incident Response
- Physical Access
- Risk management
- Secure Acquisitions
- Security Infrastructure
- Change Management
- Systems Configuration
- Systems Maintenance and Monitoring
- Information and Records Management policy
- Information security guidelines and procedures
- Procedure for Handling confidential information.

kpmg.com/nz