KPMG

Data platform system assurance: Te Kauhangaroa

Electoral Commission

August 2023

Contents

Disclaimers

Inherent limitations

The information presented in this report is based on the information provided by the Electoral Commission. We have indicated within this report the sources of the information provided. This report has been prepared and is delivered by KPMG, a New Zealand partnership (KPMG, we, us, our) subject to the agreed written terms of KPMG's Consultancy Services Order with Electoral Commission (Client, you) dated 27 June 2023 (Engagement Contract).

The services provided under our Engagement 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/Assurance/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. 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. Nothing in this report constitutes legal advice or legal due diligence.

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, Electoral Commission management and personnel / stakeholders consulted as part of the process.

This report was based on information available at the time it was prepared. 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.

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 as they are not performed continuously throughout the period and the tests performed are on a sample basis. As such, except to the extent of sample testing performed, it is not possible to express an opinion on the effectiveness of the internal control structure.

Third party reliance

This report is solely for the purpose set out in the Executive Summary of this report and for Client's information, 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 Client, none of KPMG, any entities directly or indirectly controlled by KPMG, any of their respective employees or any other member firms assume 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.

Executive summary

Overview

This review was initiated due to an incident that occurred within the Electoral Commission data platform Te Kauhangaroa in May 2023. In that incident, the data platform created approximately 5,000 duplicate records over a nine-day period which led to inaccurate data being shared with the media.

KPMG was engaged to examine to what extent the existing system of data integrity related controls are sufficient to prevent a future data integrity issue within Te Kauhangaroa.

The review was undertaken through a combination of:

- A desktop review of the system and associated processes as documented.
- Discussions with key staff and third-party providers on key processes and controls.

The review did not include any testing of the implementation or effectiveness of the existing controls. Note: the source systems, MIKE and EMS, were not in scope.

Key findings

Overall, the controls designed to be in place within Te Kauhangaroa are the types of controls we would expect to see for a data system. If these controls are operating as expected, and the recommended controls are implemented, the Board should be able to have confidence that there should be no material data integrity issues with the system.

However, a range of opportunities were identified to reduce the likelihood of future data integrity issues arising or reduce the impact should they arise.

Two key risk areas exist, which if not addressed, are likely to lead to further data integrity issues:

- **Change management**: The change management processes are not integrated or fully coordinated across the end-to-end system and the different stakeholders involved in managing and supporting the system. As a result, a change made in one aspect of the system may have unintended downstream consequences impacting the integrity, confidentiality or availability of the system and its data.
- **Third-party risk management:** A process is not in place to evaluate and manage the third-party risks posed by suppliers such as Catalyst, Deloitte, and Microsoft at an aggregate level. Ad-hoc activities are undertaken to oversee the third parties; however, these are not consistent throughout the organisation. Moreover, they do not currently cover the full breadth of risks, or the end-to-end lifecycle of a third party.

  The Commission does however take a system risk approach and complete certification and accreditation for key systems, as well as running project risk processes to identify and manage challenges with third party providers like Deloitte and Catalyst.

  As a result, the Electoral Commission is unlikely to have a full understanding of what risks it is exposed to, and therefore unable to fully manage those risks.

A third risk area exists, which if not addressed, can result in a greater impact of a future data integrity issues:

- **Incident response:** The incident response framework that has been developed for the Electoral Commission has not yet been implemented or tested. As a result any future data integrity issues would possibly have a larger impact than necessary.

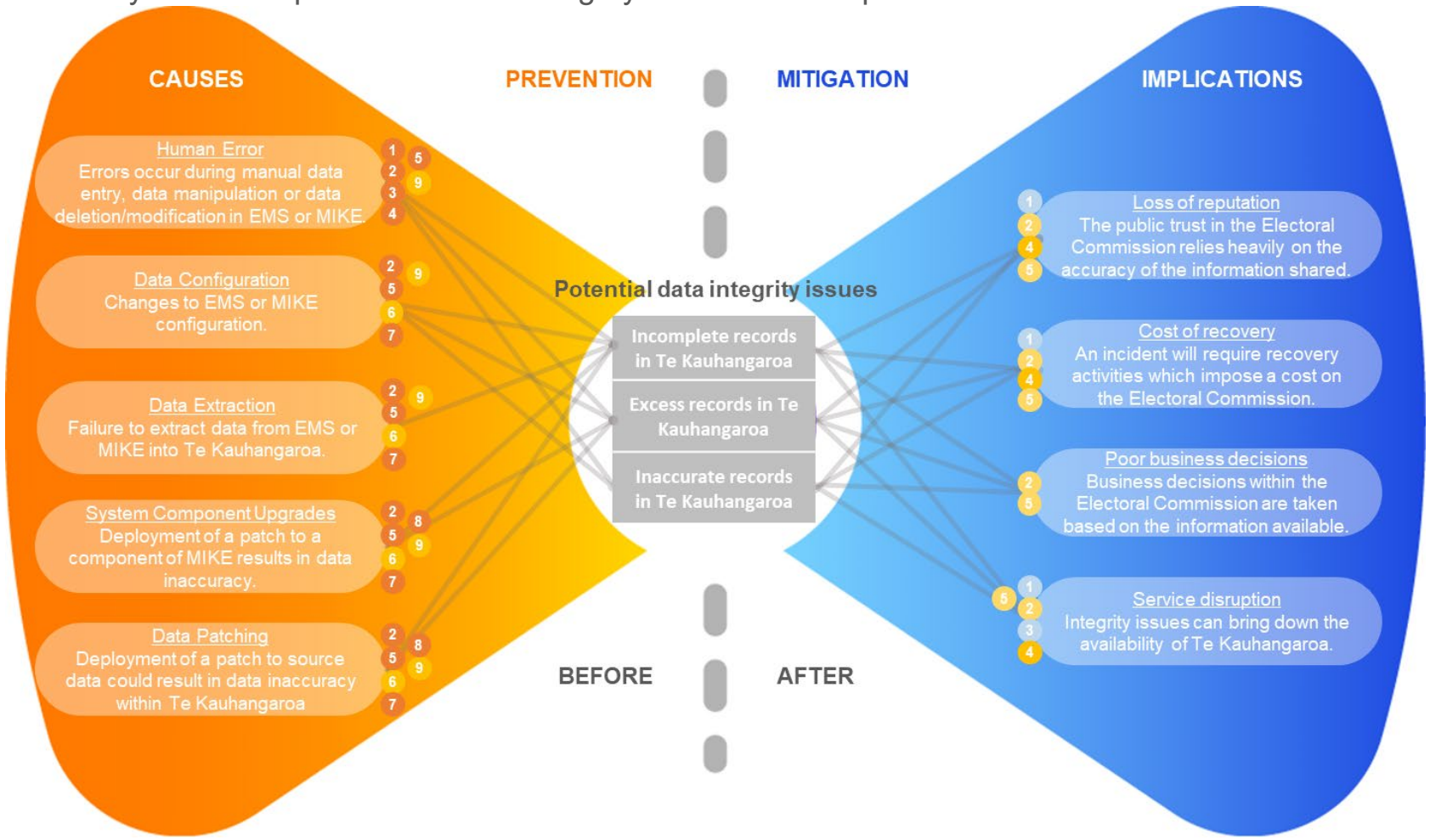
Our recommendations are summarised in the table on the next page and provided in more detail within the body of this report.

Control domain	Priority	Recommendation
Change management	High	The change processes need to be updated to establish clear lines of communication between the various stakeholders including IT, Catalyst, Deloitte, and business owners.
Third-party risk management	High	A standardise third party risk management framework needs to be rolled out across the Electoral Commission. This framework should cover a variety of operational risk domains. It should be designed to manage the risks throughout the supplier lifecycle.
Incident response	High	The newly designed incident response framework should be implemented within the Electoral Commission. This implementation should include training of key staff members and exercises to test the efficacy of the framework.
Data integrity checks	Medium	The newly introduced data duplication checks should be retained, and additional data integrity checks should be implemented.
Errors policy	Medium	The Electoral Commission should implement an errors policy and align this to data management good practices and the incident response framework.

Bow tie analysis

The below bow tie diagram shows the key threats to the integrity of the data in Te Kauhangaroa. Data integrity issues can occur in one of three forms, too many records, inaccurate records, or missing records. On the following page is the table with the relevant preventative and mitigating controls that have been identified.

Bow tie analysis: desktop review of data integrity controls and implications



Preventative controls			Mitigating controls		
No.	**Control**	**Descriptions**	**No.**	**Control**	**Descriptions**
1	Security testing and reviews	Activities to assess the effectiveness of the Electoral Commission controls' ability to mitigate identified risks.	1	Backup and restore	Ensuring all business-critical information, configuration logs etc are recoverable and prevented from being lost, corrupted or unavailable.
2	Privileged access management	The control of privileged access rights to those who require them.	2	Errors policy	A public statement articulating how the Electoral Commission will manage the accuracy of the data it publishes and how it will handle any inaccuracies.
3	Secure authentication	Process of verifying device and authentication of permissions.	3	Event logging, alerting, and auditing	Processes to log, monitor, detect and alert security events to allow the Electoral Commission to respond to incidents.
4	Role based training and mentoring	Training and mentoring to enable users to competently perform their roles and responsibilities.	4	Incident response management	Processes to enable the Electoral Commission to respond to incidents in an effective and efficient manner that minimises the impact of an incident.
5	Standard operating procedures	Step-by-step documentation detailing how to perform tasks or processes within an organisation.	5	Data integrity checks	Automated and manual verification that the data presented meets the accuracy standards of the Electoral Commission.
6	Change management	The processes and governance structures to control change activities to prevent unintended consequences.			
7	Configuration management	Maintaining configuration of systems to provide comfort that they comply with policies, settings, and standards.			
8	Patch and vulnerability management	The processes and governance structures to control the implementation and prioritisation of patches to software and systems to reduce the risk vulnerabilities.			
9	Third party risk management	Governance and oversight over third parties supporting the Electoral Commission to verify that all required controls are in place and operating as expected within the third-party environment.			

Key

Areas with high priority changes recommended
Areas with medium priority changes recommendation

Recommendations for improvement

1. Change management

Priority: High

Observation

Te Kauhangaroa consists of Azure Data Factory, Azure Data Lake, DBT, Snowflake and Tableau components which extracts data from the MIKE, EMS databases and other sources. As Te Kauhangaroa and the underlying databases are supported by different suppliers, communication is essential to ensure that any changes to one component do not have unintended consequences to another component.

There are existing change management processes in place for both the MIKE and EMS databases as well as Te Kauhangaroa, however, these two change processes are not currently integrated or well-coordinated with one another.

Implication

Gaps in communication regarding changes made to Te Kauhangaroa, EMS and MIKE across business units, suppliers and stakeholders can result in a disruption of services. Without proper communication, changes made can result in errors and confusion.

Recommendation

The change processes need to be updated to establish clear lines of communication between the various stakeholders.

This includes IT, third parties, business owners and functions that rely on the outputs of the various systems. This communication should be consistent, contain the information that the recipient needs and be timely. When changes are made to MIKE and EMS data structures this should be raised to the Te Kauhangaroa business owner.

It would be beneficial to explore what forms of communication are most effective for this. This could be in the form of emails, tickets, or meetings with relevant stakeholders.

2. Third-party risk management

Priority: High

Observation

The Electoral Commission does not have an established processes in place to evaluate and manage the third-party risks posed by suppliers such as Catalyst, Deloitte, and Microsoft.

Ad-hoc activities take place to oversee third parties, but these are not consistent throughout the organisation. Moreover, they do not currently cover the full breadth of risks, or the end-to-end lifecycle of a third party.

There are initiatives underway to improve this led by Procurement.

Implication

When relying on third parties to perform critical business services, it is important to note that the risks associated with that service cannot be outsourced. The Electoral Commission remains ultimately accountable for the performance of its statutory duties. If a third-party causes disruption to a service provided by the Electoral Commission, the Electoral Commission will need to be able to demonstrate that it took all reasonable steps to reduce the likelihood of this issue occurring.

A lack of rigorous third-party risk management means that the Electoral Commission is unlikely to have a full understanding of what risks it is exposed to. Without that understanding, it is not possible to manage the risks.

Recommendation

The management of third-party risk should be standardised throughout the Electoral Commission through the establishment of a third-party management framework and related processes. These should cover a variety of relevant risk domains including, but not limited to:

- Information and cyber security.
- Business continuity.
- Data privacy.

Third party risk management should be embedded throughout the lifecycle of the third party. The key phases of this are:

- Inherent risk assessment of a service to identify the key controls that should be in place to bring the risks within appetite.
- Inclusion of risk management considerations as part of the tendering process.
- Due diligence on potential suppliers covering all relevant risk domains.
- Inclusion of key risk management clauses in third party agreements including right to audit.
- Ongoing monitoring of compliance to the clauses in the agreement as well as wider risk domain good practices.
- Exit planning for both scheduled and stressed exit scenarios.

Ownership of the third-party risk management framework would traditionally sit with a “second line” risk function, however, this does not currently exist in the Electoral Commission. It is therefore recommended to firstly identify a suitable owner.

3. Incident response

Priority: High

Observation

The Electoral Commission have recently developed an incident response framework to manage and respond to incidents to minimise their impact. This framework has been aligned to New Zealand's official CIMS (Coordinated Incident Management System) framework. Although this has been signed off by the Executive Leadership Team and the Board, it has not yet been embedded or tested.

Implication

The absence of a fully implemented and tested incident response framework increases the risks of incidents, security, or others, being mismanaged. Poorly managed incidents lead to potentially bigger damage to an organisation's operations, assets, and reputation than necessary.

Recommendation

The new incident response framework should be embedded through training of key stakeholders. It should be recognised that this is not an IT specific responsibility even though they are a critical stakeholder in any incident response.

The incident response framework needs to have clear definitions for incident categories including thresholds to determine when the incident response plan needs to be invoked. There need to be clear roles and responsibilities for relevant internal and external stakeholders.

To confirm that the incident response plan is fit for purpose, there should be tabletop exercises to test the plan and the participants. Any lessons learned should be used to improve the framework and plans. It is key that training and testing is repeated regularly to ensure that the framework continues to be embedded. There should be a particular focus to refresh this in the run up to an election.

4. Data integrity checks

Priority: Medium

Observation

After the May 2023 data duplication incident, checks have been introduced to confirm that there are no duplicate entries. However, there are no checks currently in place to confirm if there have been any unexpected deletions or modifications.

Implication

If comprehensive data integrity checks are not performed on a regular basis, the Electoral Commission will be more likely to miss data quality issues. This will lead to delays in the detection of data quality issues and can result in an exacerbation of consequences as mitigating steps cannot be taken in a timely manner.

Recommendation

In addition to the existing data duplication checks, additional data integrity checks should be implemented, such as those that would identify any deletions or alteration to the source data.

As these checks would be more complex and labour intensive, they should therefore be completed on a periodic basis to provide assurance to the accuracy, reliability, and completeness of the Electoral Commission data within Te Kauhangaroa.

5. Errors policy

Priority: Medium

Observation

The Electoral Commission does not have an errors policy.

An errors policy outlines the principles, policy, and procedures for managing errors occurring in data owned by the Electoral Commission. This includes incorrect data entry and processing errors. The policy should identify guidelines for detecting, reporting, and maintaining data and its reliability, while also providing guidance on managing errors that may occur during data management processes.

Implication

As there is manual data entry and manipulation within MIKE and EMS there is a high likelihood that small errors will occur within Te Kauhangaroa reporting in the future. The absence of an errors policy which lays out the principles, policy, and procedures for how the Electoral Commission should manage errors, means that there is a risk that small errors can have disproportionately large consequences.

Against a backdrop of reduced trust in institutions, poorly managed corrections can result in a decrease of trust by the public in the Electoral Commission's ability to produce accurate and reliable data and insights.

Recommendation

The Electoral Commission should implement an errors policy and align this to generally accepted data management good practices and the incident response framework.

The errors policy should guide the Electoral Commission in managing any errors discovered in its data both by internal and external parties. It should outline the principles that are considered when correcting an error including but not limited to:

- **Transparency:** The correction of errors and release of data ensures transparency and accountability in the handling of election data, thereby maintaining visibility and awareness of any changes made to the data.
- **Impact:** Correcting an error, it is important to consider its proportionality and materiality, as well as any potential impact on data users, the data system, and the prevailing political context.
- **Integrity:** The correction of errors is an essential aspect of ensuring the objectivity and professionalism of the Electoral Commission.

The errors policy would help to maintain the integrity, trust, and security of the Commission's data and insights while mitigating the risks associated with data errors.

Management response (draft)

The Electoral Commission are grateful for KPMG's review and recommendations. In response to the recommendations, a group of Electoral Commission staff (Kristin Leslie, James Wilcocks, Iain Henry, Beth Kreitzer and Aidan Kirrane) have reviewed the recommendations. Steph Davidson was consulted on the incident Management recommendation. We propose that ELT take the following actions. Agreed actions will be monitored on a quarterly basis as part of Assurance monitoring and reporting.

Table: Recommendations and management comment

Area	Recommendation	Management comment	Owner
1. Change management (high priority)	The change processes need to be updated to establish clear lines of communication between the various stakeholders. This includes IT, third parties, business owners and functions that rely on the outputs of the various systems. This communication should be consistent, contain the information that the recipient needs and be timely. When changes are made to MIKE and EMS data structures this should be raised to the Te Kauhangaroa business owner. It would be beneficial to explore what forms of communication are most effective for this. This could be in the form of emails, tickets, or meetings with relevant stakeholders.	This finding is consistent with the draft C&A review. We have started to implement a process where changes are notified to stakeholders and will progress this recommendation.	Aidan Kirrane, Applications Manager.
2.Third-party risk management (high priority)	The management of third-party risk should be standardised throughout the Electoral Commission through the establishment of a third-party management framework and related processes. These should cover a variety of relevant risk domains including, but not limited to: • Information and cyber security. • Business continuity. • Data privacy	We note that there is some work underway across the Commission to improve third party risk management – IE Contract management plans and a framework on when these should be done, and project risk management approaches which consider supplier risk and risk to project outcomes. We also note that as an operational risk not a strategic risk, there is no clear owner of a work programme to establish a third party risk management framework and related processes.	Kristin Leslie, Manager Strategy, Risk and Assurance.

		We recommend ELT commission a review of the various pieces of work underway to identify if existing pieces of work could be adapted to incorporate further elements of third party risk management framework, and if not, to identify a lead/home for developing a third party risk management framework. We suggest this review commence after the election, and believe this timing is appropriate as development of a framework and changing these processes would be unlikely to impact short horizon priorities and would take time to implement.	
	Third party risk management should be embedded throughout the lifecycle of the third party. The key phases of this are: • Inherent risk assessment of a service to identify the key controls that should be in place to bring the risks within appetite. • Inclusion of risk management considerations as part of the tendering process. • Due diligence on potential suppliers covering all relevant risk domains. • Inclusion of key risk management clauses in third party agreements including right to audit. • Ongoing monitoring of compliance to the clauses in the agreement as well as wider risk domain good practices. • Exit planning for both scheduled and stressed exit scenarios.	The review would include considering which of these steps are covered in other processes we have underway and how best to implement any gaps.	
3. Incident response (high priority)	The new incident response framework should be embedded through training of key stakeholders. It should be recognised that this is not an IT specific responsibility even though	Work is presently underway to roll out the new incident response approach. We have briefly discussed this recommendation with Steph Davidson, who has been leading	Steph Davidson, Principal Advisor Enterprise Services.

	they are a critical stakeholder in any incident response. The incident response framework needs to have clear definitions for incident categories including thresholds to determine when the incident response plan needs to be invoked. There need to be clear roles and responsibilities for relevant internal and external stakeholders. To confirm that the incident response plan is fit for purpose, there should be tabletop exercises to test the plan and the participants. Any lessons learned should be used to improve the framework and plans. It is key that training and testing is repeated regularly to ensure that the framework continues to be embedded. There should be a particular focus to refresh this in the run up to an election.	that work who notes that project should address all these recommendations.	
4. Data integrity checks (medium priority)	In addition to the existing data duplication checks, additional data integrity checks should be implemented, such as those that would identify any deletions or alteration to the source data. As these checks would be more complex and labour intense, they should therefore be completed on a periodic basis to provide assurance to the accuracy, reliability, and completeness of the Electoral Commission data within Te Kauhangaroa.	We accept the recommendation and propose that we adopt 2 six monthly data integrity checks to be done in alternate quarters. • A full refresh rebuild of the database • A comprehensive suite of testing against the source databases The next steps to implement these will be completion of some analysis to develop our approach.	Beth Kreitzer, Principal Advisor Data and insights
5. Errors policy (medium priority)	The Electoral Commission should implement an errors policy and align this to generally accepted data management good practices and the incident response framework. The errors policy should guide the Electoral Commission in managing any errors discovered in its data both by internal and external parties. It should outline the principles that are considered when correcting an error including but not limited to:	We accept the recommendation and recommend that the EC should develop an errors policy and associated processes. We propose that the principal advisor data and insights lead the development in consultation with the data and information management committee. We anticipate, allowing for the time required for development and testing, that this would be	Beth Kreitzer, Principal Advisor Data and insights

	• **Transparency:** The correction of errors and release of data ensures transparency and accountability in the handling of election data, thereby maintaining visibility and awareness of any changes made to the data. • **Impact:** Correcting an error, it is important to consider its proportionality and materiality, as well as any potential impact on data users, the data system, and the prevailing political context. • **Integrity:** The correction of errors is an essential aspect of ensuring the objectivity and professionalism of the Electoral Commission. The errors policy would help to maintain the integrity, trust, and security of the Commission's data and insights while mitigating the risks associated with data errors.	completed in the first half of 2024.	

Appendix A Documents reviewed

Documents were provided by the Electoral Commission to assess and review relevant procedures and process documents that discuss the in-scope areas facing the Data within Te Kauhangaroa.

Title	Date	Version
Data Platform – CA Certificate – All Appendices – With Business Owner and Certifying Authority signoffs 09-06-23.pdf	03/06/2023	N/A
Data Ingestion Memo – EMS first changes	13/10/2022	N/A
Data Ingestion Memo – Data Platform – Additional Mike Data Fields	11/04/2023	N/A
Catalyst_ec_msa – (13_12_22)(30671061)250123	25/12/2022	6.0
Data Platform Data Ingestion EMS	31/10/2022	V2.1
Brief-Privacy-Analysis-DataPlatform	22/02/2022	N/A
Userlist_Dataplatform	N/A	N/A
Electoral Commission - Data Platform – Privacy Impact Assessment	12/09/2022	1.1
MIKE -DW Bus Matrix v1.3	N/A	1.3
EC – Data Architectural Design Principals	19/04/2022	0.1
EC Support SOW – Final	12/04/2023	N/A
Deloitte Customer Portal - INC0256393 - Comments Added	20/06/2023	N/A
Data Model process	N/A	N/A
Electoral Commission Data Ingestion Controls	March 2022	N/A
Zendesk 45211	03/05/2023	N/A
Zendesk 45149	N/A	N/A
Userlist dataplatform	N/A	N/A
IT Strategy update	22/09/2022	N/A

Appendix B Interviews conducted

The following table provides details to the interviews/meetings with staff and third-party to gather information and insight to the integrity of data in Te Kauhangaroa.

Date	Title	Attendees
28/06/2023	Kick-Off / Context Stakeholder.	Kristin Leslie – Electoral Commission.
28/06/2023	Overview of Business Context, Engagement and Oversight.	Kristin Leslie – Electoral Commission. Beth Kreitzer – Electoral Commission.
30/06/2023	Overview of Control framework and Governance in place.	Aidan [redacted] – Electoral Commission. James [redacted] – Electoral Commission. Ian [redacted] – Electoral Commission.
30/06/2023	Review of Relationship with Catalyst, Controls in place.	Aidan [redacted] – Electoral Commission. Matthew [redacted] – Electoral Commission.
05/07/2023	Catalyst input into KPMG Te Kauhangaroa Audit.	[redacted] – Catalyst. [redacted] – Catalyst. [redacted] – Catalyst. [redacted] – Catalyst.
06/07/2023	Deloitte input to KPMG audit of EC data system.	[redacted] – Deloitte. [redacted] – Deloitte.
10/07/2023	Te Kauhangaroa Audit – Meeting	Leigh Deuchars – Electoral Commission.