Deloitte.

Electoral Commission

2023 GE Cyber, Privacy and Resilience readiness - Executive Brief

FINAL

July 2023

CPR Readiness | Introduction

BACKGROUND

The Electoral Commission (EC) is preparing for the 2023 General Election. As part of its preparation, with the ever evolving threat landscape and the experiences of other jurisdictions in their elections, the EC understands that this general election will be taking place in a heightened risk context.

Global Incidents that have Targeted Elections

- **This year** cyber criminals unsuccessfully targeted Estonia's parliamentary elections in an attack which saw a range of threat actor activity.
- **2020** in the lead up to the 2020 U.S. presidential election, two Iranian nationals, operating in a coordinated conspiracy, accessed voter information from at least one state's voter database and disseminated false claims after the election
- **2016** an attack targeting the Philippines Commission on Elections led to the personal information of 1.3 million overseas Filipino voters being leaked in data dumps
- **2016** U.S. presidential election saw systems in all 50 states targeted by Russia in an attack that went largely undetected by the states and federal officials at the time

Additionally, recent cyber breaches in New Zealand and Australia (Mercury IT, Optus, Medicare) has highlighted that our region is not immune to being targeted by cyber attacks.

OBJECTIVE

Therefore, the EC seeks to have confidence that its:

Cyber

Privacy

Resilience

capability and readiness for the election are appropriately robust and that its preparations are targeted to deliver a safe and successful election.

The EC requested Deloitte to support its readiness and preparations so that its capabilities are fit for purpose, and any required risk remediation or capability uplifts can be achieved in an effective and timely manner, at pace.

SCOPE

This Executive Brief sets out our perspectives and advice based on the point in time discovery fieldwork and analysis performed by Deloitte in collaboration with the Electoral Commission in the period 11 May to 13 July 2023.

The scope of this work includes all aspects of cyber, privacy and resilience elements associated with EC's delivery of the 2023 General Election.

The scope excludes any aspect of the EC's business or technology that has no bearing on the delivery of the 2023 General Election. It also excludes Physical Security and Health & Safety.

APPROACH

The analysis undertaken included the following:

- Taking into consideration global and national trends around cyber, privacy and resilience attacks and incidents
- Industry good practices on cyber, privacy and resilience
- Workshops and meetings with EC staff and one of key vendor (Catalyst)
- Review of documentation provided
- Walkthrough of security monitoring tooling

We have structured this deliverable as follows:

- Context
- Executive Summary
- Current State and Capability
- Key Risks
- Action Plan

Supported by a range of Appendices

CPR Readiness | Context

Much has changed since GE 2020: Changes in the external environment and within EC's domain have significantly impacted the context for GE '23 which drives the imperative for EC to have fit-for-purpose cyber, privacy and resilience measures in place and ready for GE '23.

GE '23 objective: Deliver a well-run, risk-mitigated, free and fair 2023 General Election that enables more people to take part in the electoral process, and maintains public and political trust and confidence in the electoral system and in NZ's democracy.

Geo and local political contexts

Geopolitical - Heightened geopolitical tension has seen an increase in nation-state cyber activities influencing democratic processes. Potential exists that NZ and GE '23 is seen as a strategic target for some threat actors.

NZ political context - Shifts in the NZ political climate means that GE '23 will be highly contested and potential exists that local groups/individuals may have sufficient motivation to disrupt the process or influence the outcome.

Increased use of digital channels

NZ voters are more likely to use websites to gain information on GE '23, parties etc. and engage with EC's digital channels, e.g., to enrol or vote internationally. There has been a worldwide increase in the adoption and use of digital channels. People are increasingly using digital channels to find information, engage or transact, mainly due to the pandemic and technological advancements.

EC Staff and Partners

EC has seen a significant change in its staff composition.

Core IT and security team - The core team is constrained and performing multiple roles and some new members filling key roles e.g. Security Analyst. This will likely impact the team's ability to provide an effective and sustained response in the event of one or more significant cybersecurity events in spite of best efforts.

Reliance on 3rd parties - EC is highly reliant on a small set of technology and service providers that host and support the systems and applications that underpin the delivery of GE '23 and their operationalisation of good cyber practices is largely unvalidated, e.g., [redacted] 6(a), 6(c), 9(2)(k)

Cyber vigilance - EC and its 3rd party technology and service providers are subject to advanced cyber threats on an ongoing basis. Computer end-users do not always identify or respond effectively malicious email threats, e.g., 2022 Telnet incident and results from EC phishing exercises.

GE '23 underpinned by technology

While most of the operational processes to conduct the election are human-driven and paper-based, technology underpin and enable how the election will be run.

EC's technology landscape

Evolution of EC's technology foundations - EC's technology landscape has changed significantly since the 2020 general election. EC modernised its end-user workplace technology including productivity tools and its fleet of end-user computing systems. EC's transitioned to Microsoft's evergreen cloud platform and security services.

This enabled EC to implement and benefit from Microsoft's modern identity and access management and interconnected set of cloud-based security tools to prevent and detect cybersecurity threats.

New applications and data platforms - EC also implemented new cloud-based applications and data platforms e.g. SnapHire and Snowflake, new middleware to facilitate integration between recruitment systems , and recently upgraded its FMIS system.

Reliance on bespoke and dated systems - EC will rely on a core set of bespoke and non-standardised systems, most of which were developed before EC formalised its security and privacy risk assessments processes, and as such the risk inherent in these systems are largely unknown. EC has continued to build on and expand the functionality of these systems that will be relied on in the delivery of GE '23, e.g. local and overseas enrolment, international voting, nominations, electoral roll management and verification, and the Election Management System.

Cyber threat landscape

Nation-state entities and organised crime syndicates have increasingly turned to cyber exploitation since 2020, mainly due to the commercialisation of cyber and influencing factors as a result of the pandemic. While attack volumes are generally holding, the extent of disruption and harm caused by these attacks has significantly risen.

Focused Supply Chain and Third Party Compromise Campaigns

Supply chain attacks are rampant in NZ and globally, causing severe harm. Over the last nine months, prominently in NZ, 2 Technology Providers have been compromised impacting 44, and 70+ organisations respectively including several prominent government entities. These campaigns continue to feature with crippling impacts across direct and indirect customers of these technology providers who are targeted.

Cybercriminals are now for hire. This means unskilled people/groups can now buy cyber exploits as-a-service at a relatively small fee to cause digital harm to people or to defraud/disrupt business, government or democratic processes

	EC's Top 5 cyber threats for GE '23	Threat Level
1.	Social engineering attacks against EC or 3rd party personnel e.g. phishing emails as a means to launch more advanced attacks such as Ransomware	Moderate
2.	Supply chain attacks exploiting vulnerabilities of EC's 3rd party technology or service providers	High
3.	Distributed denial of service (DDoS) attacks against EC or 3rd party technology or service partner	Moderate
4.	Configuration mistakes	Moderate
5.	Accidental/intentional insider threats	Moderate

* Threat Levels aligned to Mitre ATT&CK Framework https://www.mitre.org/sites/default/files/pdf/10_2914.pdf

CPR Readiness | Executive Summary

1. Are we exposed to a high degree of risk to delivering GE'23 Elections outcomes?

For GE 2023, EC has made a concerted effort to uplift, remediate and modernise aspects of the supporting technology environment. These efforts have been significant considering the historic underinvestment and inability to dedicate resource and specialist capability towards building a fit for need, modern, secure and resilient General Election enabling technology ecosystem. We acknowledge the effort and commitment in making the progress that has been made. However, considering the low base EC was starting from, even with the significant efforts to date, there is a high degree of risk to delivering the GE 2023 outcomes.

6(a), 6(c), 9(2)(k)

6(a), 6(c), 9(2)(k)

6(a), 6(c), 9(2)(k)

6(a), 6(c), 9(2)(k)

Despite the above, EC has made good progress to mitigate the overall risk through the implementation of a number of good practice measures that have significantly reduced the gross risk, including:

- Identity and access management
- End-point threat detection
- Secure configuration and hardening of user computers and devices
- Phishing simulation exercises and privacy awareness e-learning
- DDOS protection
- Malware protection (Defender)
- Agreement from NCSC to provide support
- High availability configuration of core systems
- Vulnerability detection
- Data security

CPR Readiness | Executive Summary cont.

2. What is the worst case if we do nothing?

Loss of public trust and confidence in the electoral system, the results and/or our democracy	Some eligible people may face challenges that mean they don't participate	Disruption/delays in electoral processes or inability to deliver the election/results within set times

In the event of one/more significant cyberthreats at critical times, in the lead up to, during or post the voting period can:

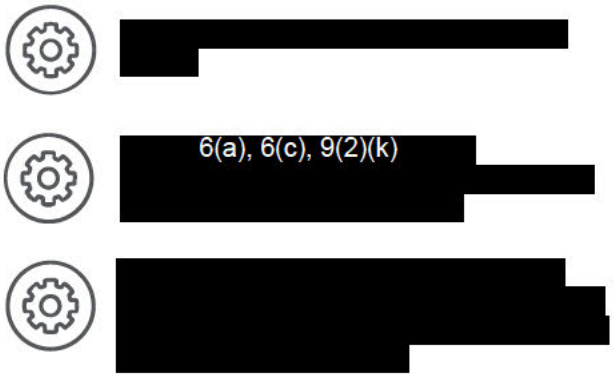
- Disrupt election processes or voting if core systems/critical data become unusable for a prolonged period, and data integrity may be compromised which can also damage public and political trust.
- Compromise or expose sensitive personal information of voters that can damage public and political trust in the electoral system and the results. Such events may also deter some voters from registering or can deter some voters from participating.
- Prevent or impede EC or its third parties from printing or distributing election materials e.g. ballots or rolls in time which would disrupt voting
- Ease of online voter registration can be affected, and in the worst case may deter/prevent some voters from participating, e.g. inability of overseas voters to upload their vote.

3. Are we able to mitigate key risks in time?

Yes, through targeted mitigation efforts the most impactful risks can be mitigated or contained, subject to urgent leadership decision and, actively managed follow through from IT and Security teams with the required specialist support.

4. Are we on track to mitigate key risks in time for GE'23?

Generally, on track for planned work, but some key gaps exist



5. What do we need to do differently?

For the EC Executive and Board to prioritise pragmatic and focused actions to reduce the ease of GE 2023 being targeted by threat actors and potential harm if attacked, and for EC to be in a defensible position if a disruption or compromise were to occur, we strong advise:

- **Allocate funding and support for specialist capability and dedicated resourcing** to be applied to urgently action the Prioritised Mitigation Plan on Slide 7. It is important that the already stretched technology team is not further stretched to try and accommodate what will be a reasonable amount of effort and without highly experienced, specialist capability to accelerate and be impactful in executing the mitigation measures.
- **Immediately appoint and onboard a specialist 24/7 retained Cyber Response Lead Partner** to provide cover from now and throughout the GE 2023 period as a minimum. This organisation must have **specialist Crisis Leadership, Cyber Threat Intelligence and Response – Technical and Forensics, and broader business recovery expertise and experience**. Also, it is important this partner organisation has the appropriate scale and is proven credible and trusted by EC's external stakeholders.
- **Build on-demand additional capacity** for key IT Security and Privacy personnel to augment current capacity.
- 6(a), 6(c), 9(2)(k)
- **Build Cyber response, recovery and leadership muscle memory for the EC Executive and Board** through carefully designed and facilitated simulations in preparation for GE 2023.

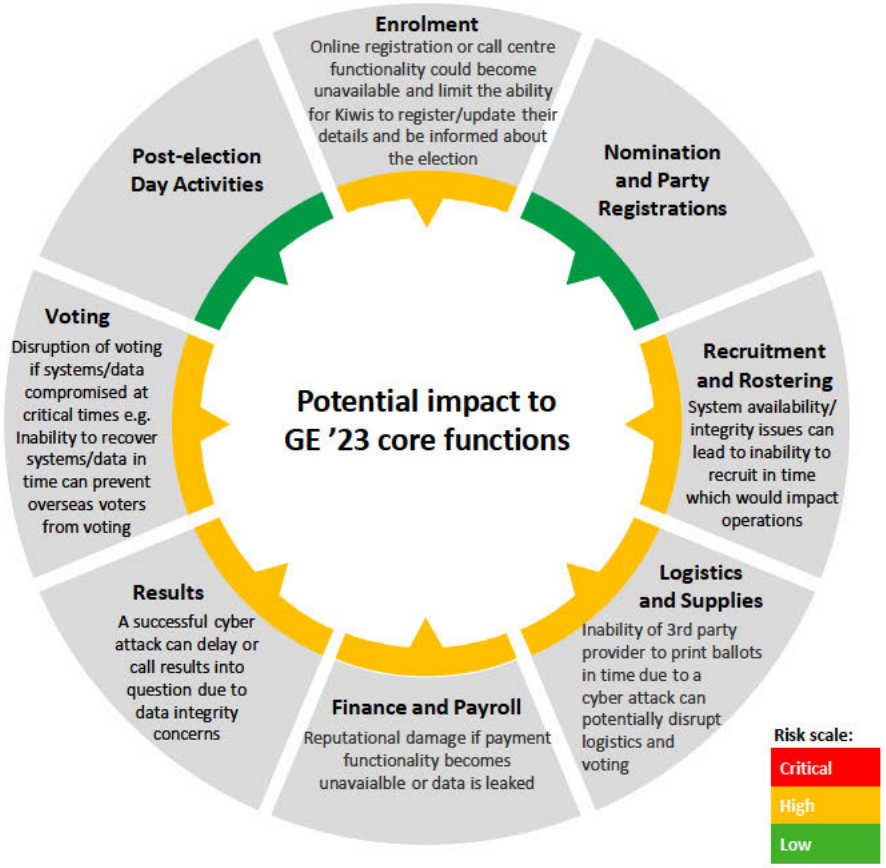
CPR Readiness | Current state and capability

While a lot of good mahi has been done to improve EC's technology and cyber capabilities since the previous election, several areas require prioritised attention to provide confidence that EC and its key technology partners and service providers have fit-for-purpose measures in place and are ready for GE '23 as shown below.

	Cybersecurity	Privacy	Resilience
Technology	• General cybersecurity safeguards • Ability to detect and defend against advanced threats	• Protection of access to unpublished roll • Protection of personal information across key systems	• High Availability for core systems
People & Partners	• People defence against phishing/ social engineering • Supply chain cyber risk mitigated	• Prevent/detect accidental disclosure by insiders	• Resilience measures for key IT Security & Privacy personnel • Ability to deliver an integrated response and recovery
Process	• Cyber Incident response process	• 6(a), 6(c), 9(2)(k) [redacted]	• Validated Systems and Data Recovery processes
Information	• End-to-end systems architecture view	• Personal information footprint minimised	• Current and validated Disaster Recovery plans for all core systems
Governance	• Core systems operated within EC acceptable risk • CIO/CISO role compatibility	• Personal Info. Mngt. in line with Privacy Act • Privacy Officer/Legal/ Party income role compatibility	• Formalisation of DR and BCM business decisions

Key:

- Fit-for-purpose capability in place and ready/adequate uplift in progress and most likely will be ready for GE '23
- Foundational capabilities in place but unlikely to be fit-for-purpose or ready in time for GE '23
- Major capability issues/gaps that will not be remediated in time for GE '23



CPR Readiness | Key risks

6(a), 6(c), 9(2)(k)

Elections unable to be run or are disrupted	H	• [redacted] • 6(a), 6(c), 9(2)(k) [redacted]
Confidence and trust in EC or electoral system is impacted	H	[redacted]
Integrity of the results is in question	L	• While there are various security concerns (i.e. the items list above) that could potentially allow for unauthorised access and thus tampering with data of key systems, due to the paper-based nature of the Elections and manual processes that exist, this risk is assessed at present to be low overall

[redacted]

6(a), 6(c), 9(2)(k) [redacted]

Crisis event leadership muscle memory building simulations for the Exec and Board.

CPR Readiness | Action plan

6(a), 6(c), 9(2)(k)

To Address After Voting Period

Prior to 2026 General Election

- [redacted]
- [redacted]
- [redacted]
- 6(a), 6(c), 9(2)(k)
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

CPR Readiness | Appendix A: GE '23 core functions and key systems

Key Enrolment Activities
- Ensuring eligible voters have an opportunity to enrol to vote and also check and update their enrolment details
- Processing paper enrolments

Key Systems

★ MIKE [redacted]

EOL [redacted]

EnrolMe [redacted]

Vote.nz [redacted]

CallCentre App [redacted]

Key Nominations and Party Registrations Activities
- Registering parties in accordance with the process set out in the Electoral Act 1993
- Ensuring parties have accurate names, logos and candidate details for ballot papers
- Managing and responding to non-compliance

Key Systems

★ EMS [redacted]

Nominations (EMS) 6(a), 6(c), 9(2)(k)

Key Recruitment and Rostering Activities
- Advertising for and recruiting 20,000+ temporary staff members
- Creating user accounts and issuing user access details
- Training new staff members
- Creating rosters and ensuring a contingency workforce is available

Key Systems

ARTS [redacted]

★ EMS [redacted]

ESB [redacted]

Tupu [redacted]

Key Logistics and Supplies Activities
- Dispatching EasyVote and overseas packs to voters
- Securing locations for advanced, overseas and election day voting
- Delivering public information campaign to the voting public
- Equipping electorate HQs and VPs with the supplies and technology
- Delivering ballot papers for advanced and election day voting
- Printing election roll

Key Systems

★ EMS [redacted]

★ MIKE [redacted]

Legend

* Penetration test has been completed in the last 12 months

☆ Critical to delivery of GE '23

Managed by:

6(a), 6(c), 9(2)(k) [redacted]

CPR Readiness | Appendix A: GE '23 core functions CPR lens

Key Finance and Payroll Activities
- Processing and paying invoices
- Processing timesheets for advanced and election day voting staff

Key Systems
- Dynamics 365 [redacted]
- CHRIS21

Key Voting Activities
- Facilitating voting at voting places and overseas

Key Systems
- eRoll
- Reconciliation App 6(a), 6(c), 9(2)(k)
- DVP [redacted]
- UVP [redacted]
- ★ OS App [redacted]

Key Results Activities
- Counting ordinary votes on election day
- Counting special votes, which includes overseas votes
- Publishing results on the Election Results Website
- Feeding election results to the media

Key Systems
- ★ EMS [redacted]
- ★ One NZ Network
- ★ Election Results Website [redacted]

Key Post-election Day Activities
- Scanning rolls, performing roll reconciliation, processing special votes, processing apparent dual votes
- Producing the Marked Master Roll
- Identifying and incorporating data into the Commission's reports for Parliament, the media and public

Key Systems
- ★ ERSA [redacted]
- ★ EMS [redacted]
- ★ OS App [redacted]
- Data Platform [redacted]

Legend

* Penetration test has been completed in the last 12 months

☆ Critical to delivery of GE '23

Managed by:

6(a), 6(c), 9(2)(k) [redacted]

CPR Readiness | Appendix B: Basic Threat Recon

[redacted]

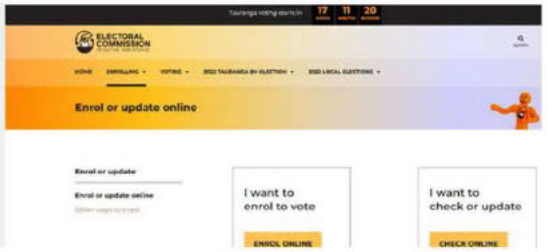
6(a), 6(c), 9(2)(k)

1

Electoral Commission

We designed and developed New Zealand's electoral roll management system for the Electoral Commission. The system stores up-to-date registration details for all New Zealand voters, and information essential to the running of both national and local body elections.

We have also supplied the core election management system for the last four general elections, as well as a number of by-elections. This system performs MMP calculations and provides detailed voting data to all the major media organisations. In addition, we host the public results website, which plays a crucial role on election night.



The Electoral Management System for the Electoral Commission. We have built and managed the EMS for decades, but in 2015-16, we rewrote the system from the ground up. It is now used to manage every aspect of our general elections, by-elections and referenda, from rostering staff, provisioning ballots and polling places to publishing results.

6(a), 6(c), 9(2)(k)

2

6(a), 6(c), 9(2)(k)

3

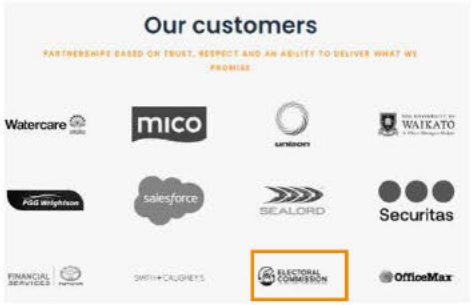
Some of our public sector customers

6(a), 6(c), 9(2)(k)

4

Electoral Commission

The Electoral Commission is an independent Crown entity responsible for the administration of parliamentary elections and referenda. It requires an outsource provider for its contact centre operations that is well versed in security and most importantly, one that can scale operations quickly to support large, highly variable call volumes. They selected Telnet as their provider following an RFP process held in 2012. Telnet's previous work with government agencies and, in particular, our success in managing the call centre for the 2001 and 2006 national Census were among the reasons for our success.



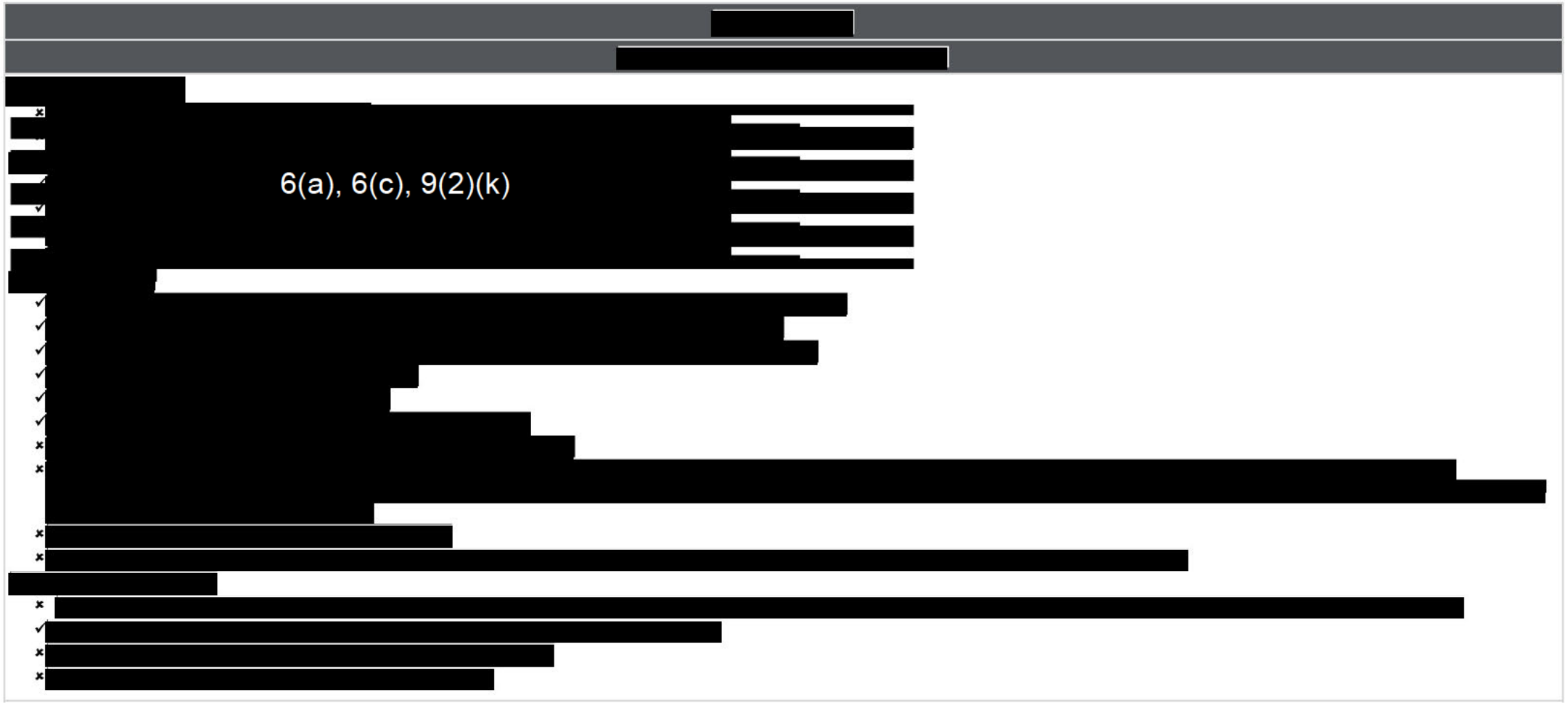
Pikselin quickly built a close and effective relationship with the Commission and have become a trusted provider. We worked closely with senior level business stakeholders to extract and evolve the business vision, website strategy and new brand direction. We continue to contribute to a number of diverse streams of work for the Commission.

6(a), 6(c), 9(2)(k)

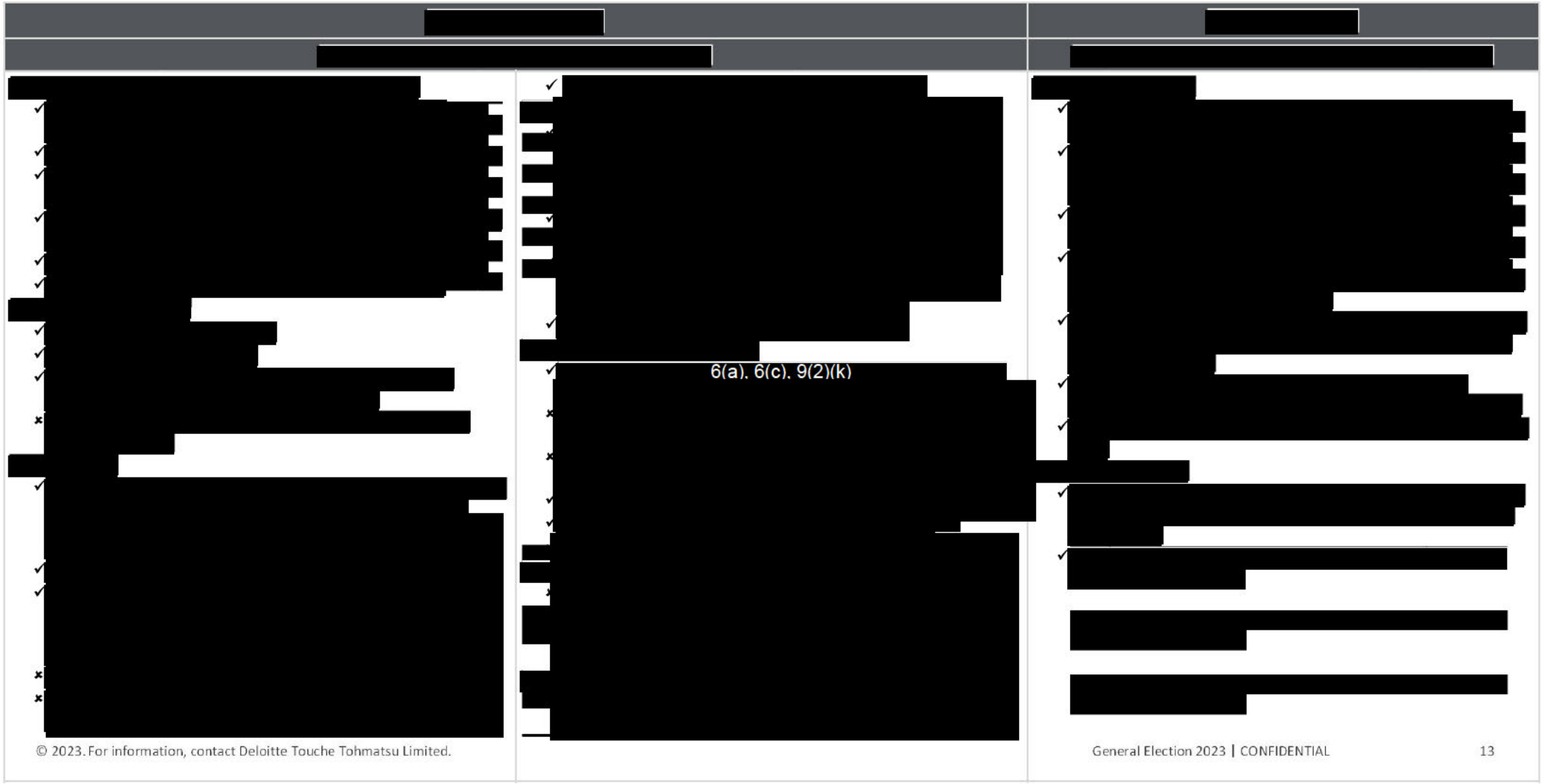
5

CPR Readiness | Appendix C: Controls and Measures

To provide some context around security and privacy coverage, the following tables highlight some of the key controls in place and where there are some deficient controls that need to be addressed. These controls have been mapped at a high level against the NIST cybersecurity and privacy frameworks covering the Identify, Prevent, Detect, Response and Recover domains.



CPR Readiness | Appendix C: Controls and Measures continued



- [redacted]
- 6(a), 6(c), 9(2)(k)
- [redacted]

CPR Readiness | Appendix C: Controls and Measures continued

CPR Readiness | Appendix D: Workshop attendees

Name	Title	Organisation
Adele 9(2)(a)	Principal Advisor, Voting Services	Electoral Commission
Aidan Kirrane	Manager, Applications	Electoral Commission
Allison 9(2)(a)	Senior Project Leader	Electoral Commission
Anusha Guler	Deputy Chief Executive, Operations	Electoral Commission
Emily Redmond	Programme Director	Electoral Commission
Emma Gillard	Manager, Finance & Administration	Electoral Commission
Erin 9(2)(a)	Principal Advisor, People & Culture	Electoral Commission
Grace Chian	Manager, Business Enablement	Electoral Commission
Ian 9(2)(a)	Senior Manager, IT Services	Electoral Commission
Izak 9(2)(a)	Manager, People & Culture	Electoral Commission
James 9(2)(a)	Chief Information Officer	Electoral Commission
Jeffrey 9(2)(a)	Senior Systems Specialist	Electoral Commission
Joe 9(2)(a)	Technical Specialist	Electoral Commission
Justin 9(2)(a)	Manager, Customer Services	Electoral Commission
Kristin Leslie	Manager, Strategy Risk & Assurance	Electoral Commission
Kristina Temel	Manager, Legal & Policy	Electoral Commission
Leigh Deuchars	Deputy Chief Executive, Strategy, Governance & Development	Electoral Commission
Lisa 9(2)(a)	Senior Project Manager	Electoral Commission

Name	Title	Organisation
Lucy Hickman	Deputy Chief Executive, Enterprise Services	Electoral Commission
Martin Rodgers	Director, Voting Services	Electoral Commission
Maryanne 9(2)(a)	Payroll Advisor	Electoral Commission
Morgan 9(2)(a)	Cyber Security Analyst	Electoral Commission
Natasha 9(2)(a)	Senior Project Leader	Electoral Commission
Rob 9(2)(a)	Senior Project Leader	Electoral Commission
Ross McPherson	Director, Enrolment	Electoral Commission
Sarah 9(2)(a)	Organisational Security & Resilience Senior Advisor	Electoral Commission
Steph 9(2)(a)	Principal Advisor, Enterprise Services	Electoral Commission
Suzanne Knight-Tinirau	Manager, Communications & Education	Electoral Commission
Tracy 9(2)(a)	Finance Business Partner	Electoral Commission
Vincent 9(2)(a)	Manager, IT Infrastructure	Electoral Commission
9(2)(a)	9(2)(a)	6(a)

Statement of Responsibility

Where Deloitte has provided advice or recommendations to the Electoral Commission (EC) we are not responsible for, or the manner in which, suggested improvements, recommendations, or opportunities are implemented. The management of EC, will need to consider carefully the full implications of each of these suggested improvements, recommendations, or opportunities, including any adverse effects and any financing requirements, and make such decisions, as they consider appropriate.

The scope of our work was designed to provide advice in accordance with the Statement of Work. The procedures that we performed did not constitute an assurance engagement in accordance with New Zealand Standards for Assurance engagements, nor did it represent any form of audit under New Zealand Standards on Auditing, and consequently, no assurance conclusion or audit opinion is provided.

We have prepared this deliverable solely for the use of EC. The deliverable is based on the best available information at the time of the discovery and analysis undertaken, and contains the constructive high level suggestions to improve practices which we identified in the course of our work. We would be pleased to discuss any items mentioned in this debrief and to support the corrective action implemented by management.

Our findings are based on observations from our discovery and specific analysis actions defined within scope undertaken in the time allocated (where possible).

This deliverable is not to be used for any other purpose, recited or referred to in any document, copied or made available (in whole or in part) to any other person without prior written express consent. We accept or assume no duty, responsibility or liability to any party in connection with the deliverable or this engagement, including without limitation, liability for negligence in relation to the factual observations expressed or implied in this debrief.

Suggestions for improvement should be assessed by management for their full technical and commercial impact before they are implemented.

Deloitte.