

<p>Establishing Context</p> <p>What is the risk that the board specifically need to be concerned about?</p>	<p>Failure to recruit will impair trust in EC's capability to deliver elections</p> <ol style="list-style-type: none"> Is the EC appropriately prepared for and responsive to the tight employment market? Is EC staffed to deliver what is needed? How is EC placed for and welcoming to employees representative of the communities they work in? 	<p>Key data</p>	<p>Trend: less available staff. Unemployment: 3.4%; 102,000.</p> <p>Internal requirements: Number roles required to be recruited ~25,000, 16,000 VS, 4,000 processing, 2,000 other.</p> <p>13 electorates of concern for low recruitment from 2020</p> <p>144 permanent staff (39 vacancies) (this informs central capability to support GE and temp staff)</p>	<p>How may this risk or issue impact us?</p>	<p>Low or inappropriate staffing in each electorate reduces ability to run voting efficiently. This could result in insufficient voting places or queues which disincentivises potential voters, reduces turnout, which can undermine EC and electoral system reputation.</p> <p>We need to address decreased worker availability nationally and the gap that historically, election staff and our workforce demographic have not been representative of the NZ population.</p>	<p>Key factors that influence our success in this space (internal and external)</p>	<p>Public awareness of available work.</p> <p>Creating contingency by recruiting more than we need.</p> <p>Timely and appropriate actions at different periods of the election campaign.</p> <p>Reducing attrition</p>
<p>Commission activities</p> <p>Key area 1</p> <p>Reaching potential staff for GE</p> <p>Parts of business / project involved, what they have considered, and the goals they wish to realise. Summarise key activities being undertaken to prepare, address or respond.</p>	<p>Staff involved: P&C, Comms, VSs: regional and electorate managers; community engagement</p> <p>Considered: known challenge areas, and potential staff</p> <p>Goals: reach as many people as possible, and target outreach in electorate areas of concern; increase representative employment</p> <p>Activities:</p> <ul style="list-style-type: none"> Multifaceted advertising approach <ul style="list-style-type: none"> General national comms Targeted areas (plans, regional partners, voting place approach) Targeted groups (plans, regional partners, translations, hui) Working with other organisations including councils, MSD, other government channels. Addressing misconceptions (including that GE work is unpaid) 	<p>Key area 2</p> <p>Monitor/ respond to ensure on track for GE recruitment</p>	<p>Staff involved: P&C, VSs: regional and electorate managers; governance: programme board</p> <p>Considered: known challenge areas, timelines required to mobilise contingencies and train staff</p> <p>Goals: know when to trigger planned proactive interventions, field supported/ responsive to learnings</p> <p>Activities:</p> <ul style="list-style-type: none"> Monitor the progress of recruitment campaigns in real-time, closely tracking application numbers against targets Including number of applicants received/ hires, by roles/ electorate. regular analysis to identify trends, gaps, and areas requiring additional focus. Information sharing so field can get support/share challenges and how best to manage. Deliver planned proactive interventions where needed based on updates (extra support P&C, C&E) Working with other organisations including councils, MSD, other Government agencies 	<p>Key area 3</p> <p>Contingency</p> <p>Targeted and public sector co-ordinated action</p>	<p>Staff involved: P&C, VSs, business enablement and Community Engagement (relationships with partners).</p> <p>Considered: timeframes for successful resourcing and training of appropriate staff</p> <p>Goals: EC is able to take additional actions to ensure needed electorate and VP staff in place</p> <p>Activities:</p> <ul style="list-style-type: none"> Detective controls – monitoring Planning the public sector contingent mobilisation Compensating controls include over recruiting where able to, to transport staff around regions, <p>Next steps:</p> <ul style="list-style-type: none"> Recruitment dashboard live early July Progressing cross government planning on contingency mobilisation – conversation with public sector CEs 		
<p>Monitoring</p> <p>What visibility has the Board had of key programmes and how the risk is being dealt with?</p>	<p>Board visibility of previous relevant items has been through:</p> <ul style="list-style-type: none"> Programme updates Community engagement updates <p>This month's programme update includes the draft recruitment dashboard.</p> <p>Forthcoming items:</p> <ul style="list-style-type: none"> Plan in response to Archives NZ Audit, timing tbc 	<p>How does management monitor and maintain confidence in these areas? How is success monitored? What is the trend?</p>	<p>Programme board govern key risks and are actively managing and monitoring</p> <ul style="list-style-type: none"> recruitment and associated planning Related programmes of work including community engagement and the GE comms strategy contain projects which are part of our wider recruitment push <p>Running a dashboard on GE recruitments against target.</p> <p>Field governance – weekly regional managers recruitment update.</p>	<p>What key information or milestones will trigger action?</p>	<p>July field and numeric monitoring will prompt proactive interventions in low recruitment areas, this will be focused on those tracking lowest on recruitment.</p> <p>Low applications and hiring will be considered.</p> <p>Public sector mobilisation test will be early August – required as training is mid-Sept.</p> <p>Key metrics: 45,000 applications overall considered indicative of meeting overall staff needs.</p>		
<p>Overview, any gaps?</p> <p>Assurance assessment</p>	<p>Overall, this risk is of both high visibility and has a highly developed networked response within the Commission. Staff have approached the challenge in an innovative and connected manner and considered external issues. Some pieces of work require clarity on resourcing (public sector mobilisation plan – this is being actively managed). We will know early in August we are on track, with 45,000 applicants considered a key indicator on if we will get the overall number we need.</p> <p>Gap on clarity at this time if planned proactive interventions resourced, or if support being provided in known challenge areas is adequate/ proactively being resourced (Northland, Whangārei, etc – what extra resource to support those areas?)</p> <p>Present recruitment for customer service and community engagement staff is tracking well, which is a positive indicator. However, Dunedin monocultural response, and Central NI low applications. How Public Sector Chief Execs respond will be key to developing a confident recruitment contingency plan. On 4/7/23 Karl had a very positive conversation to progress the mobilisation work with Justice which increases our overall confidence that the public sector mobilisation failsafe is on track.</p>						

Enterprise Deep Dive: Privacy and Information Management

Environmental driver description

This is a highly regulated area. Core risks/ opportunities to manage include confidentiality of data about persons, integrity of and appropriate availability of data/ information to support business goals.

30 June 23

<p>Establishing Context</p> <p>What is the risk that the board specifically need to be concerned about?</p>	<ol style="list-style-type: none"> How do we know that the data in our systems has integrity, and that our systems will maintain this integrity as it is reshaped as information? Are we appropriately enabling consistent, efficient, well-informed work across the EC? Are our systems protecting the information we hold on individuals? 	<p>Key data</p>	<p>7 reports and 3 public complaints in FY – no significant breaches. Reviews have demonstrated need for work on both privacy and information management. Reviews identify that not all systems which look to require them have had Privacy impact assessments (privacy programme planning being resourced). Plan being developed in reply to Public Records Act audit.</p>	<p>How may this risk or issue impact us?</p>	<p>Potential of election integrity impact if core systems not secure. Inappropriate or unlawful data/information collection or management leads to reputational damage, legal financial penalties. Inaccessibility of data/info leads to loss of institutional knowledge or operational issues. Insufficient security posture (including shadow IT, unmonitored personal device use) leads to a data or privacy breach.</p>	<p>Key factors that influence our success in this space (internal and external)</p>	<p>Key system design Staff behaviours and appropriate preventative, deterrent and directive controls Emerging risk awareness and ability to respond Ability of our data</p>
--	--	-----------------	---	--	---	---	---

<p>Commission activities</p> <p>Key area 1</p> <p>Preventions + directions to support IM/privacy</p> <p>Parts of business / project involved, what they have considered, and the goals they wish to realise. Summarise key activities being undertaken to prepare, address or respond.</p>	<p>Staff involved: IT, Data and insights, P&C (compliance/ core training); privacy officer. All staff for institutional knowledge, activities/ training etc. Considered: appropriate systems for business purposes, how to inform staff of behaviours to manage risks, and controls to prevent issues. Goals: Appropriate policies, controls and behaviours to support IM/privacy goals Activities:</p> <ul style="list-style-type: none"> IM and privacy policies and procedures Key systems designed and tested for data integrity, secured access, (Electoral systems, data and enterprise systems, etc) New systems have PIAs done Field and core staff trained (privacy, + security, including security of information) New Te Kauhanganaroa system improves availability of data + privacy protections <p>Next: new IM staff – Plan being developed in response to Public Records Act audit, privacy work programme is under development.</p>	<p>Key area 2</p> <p>Detect / correct controls for privacy and IM</p>	<p>Staff involved: IT, Data and insights, privacy officer. Management responsible for relevant detect information controls in their areas. All staff for being alert to/ reporting privacy/IM issues. Key 3rd parties, IE telnet and IT system providers. Considered: potential identification/ monitoring and reporting and application controls Goals: EC aims to identify risks and issues and take corrective action before harm is caused Activities:</p> <ul style="list-style-type: none"> Assess our systems via annual PSR/Chief Archivist annual record keeping survey/ 5yrly PS Records Act audit *response to 2023 audit being developed. Detect controls for unauthorised access to our information, flagging attempted access Our normal reporting lines/ governance covers privacy/ RM issues, so we have reporting channels for IM and privacy, incl IT service desk, and contact to our privacy officer. Information Systems Strategy for next steps 	<p>Key area 3</p> <p>Ability to respond to, recover from and resolve IM and privacy issues</p>	<p>Staff involved: IT /data/ privacy officer, all staff for implications in their work areas. Considered: potential harm, expectations of the impacted, incl timeliness of response, communications, Māori data sovereignty Goals: EC can appropriately manage and respond to IM and privacy issues. Activities:</p> <ul style="list-style-type: none"> Have in line processes, IE IT issues log system (wording?) May inconsistency in Te Kauhanganaroa data versus MIKE demonstrated system ability to identify and respond <p>Next steps: New issues management approach. Any suggestions as part of work of new IM staff member Potential privacy secondee or provider from AoG panel</p>
--	---	--	--	---	--

<p>Monitoring</p> <p>What visibility has the Board had of key programmes and how the risk is being dealt with?</p>	<p>Board have received verbal updates on privacy as part of GE programme updates. Other relevant updates include: General updates on IT and cybersecurity, and forward planning., including the 22.09-01 - IT strategy update.docx Te Kauhanganaroa updates* 22.08-08 - Legislative compliance & privacy report.docx Items to come: Comply with survey and privacy report for FY 22-23 in line with financial year-end Action plan following Public Records Act audit Continued updates as part of the GE programme</p>	<p>How does management monitor and maintain confidence in these areas? How is success monitored? What is the trend?</p>	<p>Governance: Privacy</p> <ul style="list-style-type: none"> Privacy officer in place with appropriate reactive reporting and PSR annual review and reporting. GE Programme board on PIA applications <p>Information management.</p> <ul style="list-style-type: none"> Data governance group, reports to ELT. Enterprise systems including telnet, monitored by ELT, with very regular updates. <p>Other key controls Te Kauhanganaroa now has data integrity dashboard for monitoring consistency with MIKE. NOTE: Te Kauhanganaroa assurance review also coming in July 2023</p>	<p>What key information or milestones will trigger action?</p>	<p>Action is triggered via a combination of normal business continuous improvement processes and incident response. Note the detection and response controls noted above. Additionally, self-assessment processes and audits, or best practice sector advice may trigger improvement activity i.e. public service records act audit, PSR reviews, etc. Next steps Action plans in response to reviews in presently underway, as is assurance in response to a recent issue.</p>
---	--	---	--	--	--

<p>Overview, any gaps?</p> <p>Assurance assessment</p>	<p>Reviews have identified a number of areas where further work is required as relates to understanding our system-based privacy and information management risks. Whilst EC staff create maintain and access information for a variety of business purposes, there isn't uniform understanding and approach to IM and privacy and EC don't have an agreed ongoing assurance approach. There are some known gaps, such as not all systems and processes having current privacy impact assessments, the lack of consistent staff practices around information management policy and the lack of a data retention and disposal plan. These gaps are compliance issues, and a real challenge where they materialise as the EC not being able to access data held for operational purposes. Resourcing and planning is presently in train. An IM specialist has been hired to address key IM gaps. Management is presently considering bringing on privacy resources. Significant improvements can be observed in the accessibility, use, and the privacy of information held and used by the commission in the new-this-year data platform Te Kauhanganaroa and the data and insights programme which is steadily improving access to information held by the EC significantly.</p>
---	--

Enterprise Deep Dive: Disruptive events at voting places

Environmental driver description

Disruptive events range from facility issues (fire or utilities), behaviours which impact on staff or voters, through targeted criminal or violent activities which prevent a voting place from operating efficiently, safely, and with electoral process integrity

30 June 23

<p>Establishing Context</p> <p>What is the risk that the Board specifically need to be concerned about?</p>	<p>Failure to prepare for disruptive events may impair trust in the electoral process. Has the EC (and delivery partners):</p> <ol style="list-style-type: none"> 1. Connected to right external agencies to respond to events? 2. Prepared staff, processes and facilities to minimise likelihood and impact of events? 3. Put appropriate contingencies in place to minimise harm? 	<p>Key data</p>	<p>Similar events (Census) have had increased disruption.</p> <p>Global trend for increased societal division and disruption.</p> <p>Increase / variation in voting place sites (~2370 election day sites planned, without social distancing required, this is less than 2020.</p> <p>Voting places incl alternative channels for voting, IE phone.</p> <p>Uplift in security preparedness incl regional security advisors.</p>	<p>How may this risk or issue impact us?</p>	<p>Lack of appropriate preparedness to identify, prevent, or detect and respond to a variety of potential events, or to prepare so staff and voting places are equipped to reasonably manage disruption, could result in:</p> <ul style="list-style-type: none"> - Health and safety implications. - Potential voters being deterred from voting - The trust of election processes being impacted, potentially also impacting New Zealand's reputation for electoral integrity 	<p>Key factors that influence our success in this space (internal and external)</p>	<p>Understanding the risk environment and appropriate preparations.</p> <p>Public understanding of and voting place rules.</p> <p>Voting place staff knowing & invested in what they need to do.</p> <p>Right connections/ ability to flow information should events occur. Ability to provide/ direct support where needed</p>
--	---	-----------------	---	--	---	---	---

<p>Commission activities</p> <p>Key area 1</p> <p>Cross security sector connections + information channels</p> <p>Parts of business / project involved, what they have considered, and the goals they wish to realise. Summarise key activities being undertaken to prepare, address or respond.</p>	<p>Staff involved: CEA and security, regional security advisors, security risk group* external partners incl DPMC, Police, security agencies NEMA, and FENZ.</p> <p>Considered: system roles and responsibilities, information channels, and processes to share information, prepare or act.</p> <p>Goals: Enable appropriate preventative, detective corrective and responsive action.</p> <p>Activities: -Cross sector group including relevant system players, enabling co-ordinated and aligned preparation for election security threats.</p> <ul style="list-style-type: none"> - Agreed/ing protocols response to an event. - Information sharing and common operational response support structure during event. - Implementation and testing of controls to include July table-top exercises for weather and disruptive events. 	<p>Key area 2</p> <p>Internally prepared for range of disruption</p>	<p>Staff involved: Voting Services, regional security advisors, CEA and security, ES – BCP and incident management.</p> <p>Considered: full range of potential disruptions, process design in ops manual and protocols to mobilise.</p> <p>Goals: have prepared for disruption and considered disruption risk in the design of election processes.</p> <p>Activities: Incident Management handbook for field</p> <ul style="list-style-type: none"> - Staffed to support regional risk understanding, analysis and implementation of controls which will help minimise potential disruptive events/ impacts. - Range of prevention controls in place including physical protective security, staffing strategy at VPs, HR screening, supplier arrangements, and emergency preparedness. Response guidance in development plans includes voting place safety and security site standards. - Review of election process/ activities to identify and mitigate potential control gaps in design. - Election delivery taskforce to triage issues set up, Incident management planning approach developed. 	<p>Key area 3</p> <p>Election day ability to act/respond appropriately while maintaining trust</p>	<p>Staff involved: VSs, Voting place staff; security, and escalation channels.</p> <p>Considered: safety and electoral integrity .</p> <p>Goals: Ensure we know information will flow appropriately, and staff have access to what they need to respond / trigger system support.</p> <p>Activities: Escalation & comms channels in dev</p> <ul style="list-style-type: none"> - BCP, incident management guidance, and election day information channels presently in development – on track. Includes escalation channel to political parties where acts of parties may result in disruption. - Partner agencies – see key area 1. - Guidance to public on rules once voting starts. - VP staff will have tools to help them identify, act, & escalate should events occur (Training /handbook/ staffing levels controls planned/ in place). - Controls/ steps anticipated to support electoral integrity /safety also include external visibility of key processes, dedicated regional security resources.
--	---	---	--	---	--

<p>Monitoring</p> <p>What visibility has the Board had of key programmes and how the risk is being dealt with?</p>	<p>The Board have received regular verbal security updates and have met with security agency CEs to understand cross sector activity.</p> <p>Forthcoming:</p> <ul style="list-style-type: none"> - August/ Sept security readiness update - August – Business continuity planning, Incident management guidance and scenarios will come to the board. 	<p>How does management monitor and maintain confidence in these areas? How is success monitored? What is the trend?</p>	<p>Overall preparedness is trending upwards against prior EC security and emergency preparedness, but the risks are known to have increased.</p> <p>Risk & security WG govern system protocols</p> <p>ELT / programme board regularly hear about relevant topics including:</p> <ul style="list-style-type: none"> - Trust and Security programme - Guidance, including handbooks for event occurrences, voting place set up, etc - Staff training - Monitoring of security / any incidents are also reported through operational channels, w/ security doing trend monitoring. - Election delivery taskforce daily triage, and IM plan/ team prepped. 	<p>What key information or milestones will trigger action?</p>	<p>Information shared from partners.</p> <p>General escalation management lines, BCP protocols, and to be agreed election event/risk escalation processes will enable appropriate management of disruptive events up to and during GE23, incl where appropriate prompting formal incident management.</p> <p>July tabletop exercises should test our incident/ risk escalation channels including with our partners.</p> <p>Milestones/ information which will trigger action to be confirmed in testing/ simulations.</p>
---	---	---	---	--	--

<p>Overview, any gaps?</p> <p>Assurance assessment</p>	<p>It is inevitable that there will be disruptive events during the election, not just because polarisation, civil and criminal disruption is on the rise globally and domestically.</p> <p>The Commission and key partners have scaled up activity and devoted staff on the analysis, understanding of preparedness, and preventions, plus the ability to detect, prepare for and respond to disruption. It is no longer enough to do a good job; we need to control the narrative about the operation of the electoral event. Our preparedness to respond to disinformation is pivotal.</p> <p>Deep understanding and risk focused prioritisation is indicated by recent exercises reviewing internal controls for disruptive events identifying those in place, in development, and either unknown or not in place status. Whilst some improvement areas have been identified, overall, the increase in BCP, IM, and the reporting and communication lines being implemented look pragmatic and likely effective to respond to most potential incidents. Whilst preparations are wide ranging, sharing solutions to potential challenges, and how efficiently and effectively staff respond in the moment will be key to how our success with anticipated disruptions, including black swan events.</p>
---	--