Requirements for a trial of online voting in local elections

A framework to guide Local Government

May 2015

INTERNAL AFFAIRS
Te Tari Taiwhenua

New Zealand Government

Contents

Purpose and status of this document

The Government is looking at enabling a limited number of territorial authorities to trial online voting in local elections in 2016. Territorial authorities would be responsible for procuring independently tested online voting services, and preparing for any trial.

This document provides the proposed operational outcomes for any trial of online voting in local elections. There will be further refinement of the framework to reflect engagement with stakeholders, testing of technology solutions, and amendments required in order to progress proposals for regulations. Additions, deletions and refinements adopted in relation to the framework will be advised as soon as possible to stakeholders, who will include councils, election service providers and developers of online voting services.

Regulations are required in order to authorise councils to participate in the trial, and to regulate its conduct. Participation by authorised councils will remain discretionary. The requirements of the Local Electoral Act 2001 and the final content of the framework, including information gathered from the testing and refinement of the framework, will inform the content of any regulations.

Introduction

In New Zealand, territorial authorities are responsible for the way elections are conducted in their area, including elections to regional councils, district health boards, local boards, community boards, and licensing trusts.[1] In practice, the actual running of local elections is now largely out-sourced. Presently, two New Zealand-based companies provide election services to nearly 90 per cent of local authorities.

The Local Electoral Act 2001 (the Act) and the Local Electoral Regulations 2001 together provide the framework for the running of local elections. Currently, under that framework, local authorities can carry out their elections by booth and/or postal voting. In practice, all authorities choose to solely use postal voting.[2] The Act anticipates other future voting methods and implementation of new technology. It specifies that "voting method" includes "any form of electronic voting"[3], and allows new voting methods to be authorised by regulations.[4]

In recent years, a number of local authorities have asked for online voting to be allowed as a voting method for local elections. In light of this, in 2013, an Online Voting Working Party was established to consider the matter. The Working Party found that online voting has the potential to address some concerns with the current local electoral framework. However, there are significant risks associated with its use.[5] The key risks relate to the security, accuracy, usability and availability of any technology solutions used for voting online. A lack of public confidence in online voting is also a risk to successful implementation and uptake. Further, technology failure as part of an online voting trial could undermine public confidence in local authority capability, any potential for future use of online voting by local government, and public comfort with carrying out other official transactions online.

A staged approach to any use of online voting is considered to be appropriate, as this allows all parties and stakeholders to become familiar with the opportunities and challenges presented by online voting.

What is online voting?

Online voting and e-voting are sometimes used interchangeably. Here, 'online voting' is used to refer to the form of voting where an elector is able to vote using the internet, remotely and unsupervised by officials, on the voter's own device. Use of the term online voting is not intended to include the use of electronic voting kiosks but may include use of publicly provided devices, such as computers in libraries.

[1] Local authorities are responsible for deciding the system of voting used (First Past the Post or Single Transferable Voting); deciding the method of voting used (postal voting, booth voting, or both); appointing electoral officials; and the conduct of local elections and polls, including the option of contracting companies to process and count votes.

[2] Booth voting was last used for local elections in 1992, by Hutt City Council.

[3] Section 5 of the Local Electoral Act 2001.

[4] Section 139 of the Local Electoral Act 2001.

[5] Retrieved 29 October 2014, from http://www.dia.govt.nz/pubforms.nsf/URL/Online-Voting-in-New-Zealand-report.pdf/$file/Online-Voting-in-New-Zealand-report.pdf.

In December 2014, the Government decided that while it did not have an objection in principle to local government trialling online voting, such a trial would not be allowed to proceed until local government had demonstrated that voting technology solutions can be used in a way the meets the requirements of the Act and security expectations.

How will local government demonstrate it is safe to proceed with a trial?

Territorial authorities trialling online voting in their area will be responsible for demonstrating that voting technology solutions can be used in a way the meets the requirements of the Act and security expectations. They will demonstrate this by obtaining independent assurance that the technical specifications for voting technology solutions to be used in their elections meet the Government's requirements contained in this document. They will also obtain independent assurance that the voting technology solution itself is in compliance with the technical specifications that the territorial authority or their election service provider have prepared.

Why is the Government considering enabling a trial of online voting?

Ensuring fair, effective and efficient electoral processes and procedures, for voters and candidates, is a necessary pre-requisite for healthy and vibrant democratic practice. The combination of a highly IT-enabled population[6] and dissatisfaction among some electors with the current voting experience has prompted many local authorities to seek to trial online voting. Some of the ways online voting has the potential to improve future local authority elections are discussed.

Enhancing accessibility

Online voting has the potential to assist certain groups of electors who currently have issues exercising their right to vote under the postal system. These include those who are living in remote areas or overseas at election time, and those who (because of disability or language issues) cannot vote unassisted.

There are reported instances where those living in remote areas or overseas at election time have not received their documents in time to vote. In the 2013 local elections, about five percent of overseas electors who were issued a voting pack actually voted, which is significantly lower than the average voter turnout of 41 percent. This suggests that voters overseas may find postal voting limits opportunities to vote. Online voting may make it easier for those that wish to vote overseas. It may also assist those living in remote areas with limited postal services.

[6] The World Internet Project 2013 puts New Zealand's penetration of the internet at 92 per cent. *Online voting in New Zealand: feasibility and options for local elections – Report of the Online Voting Working Party*, page 12. Retrieved 29 October 2014, from http://www.dia.govt.nz/pubforms.nsf/URL/Online-Voting-in-New-Zealand-report.pdf/$file/Online-Voting-in-New-Zealand-report.pdf.

Some electors who struggle with postal voting could find it easier to vote. Electors that are visually-impaired,[7] have low proficiency in literacy,[8] or for other reasons may need assistance to fill out their voting documents. Finding assistance can be difficult and, once a voter finds assistance, they are unable to vote in secret. Online voting could allow these groups to be able to vote more easily and privately..

Improving accuracy

Online voting provides opportunities to make the act of voting simpler and more accurate, by notifying voters if they have incorrectly completed a voting document. Under the current postal voting system, inaccuracy can arise where voters submit a voting document that does not properly record their intent. Voters are not notified that their vote qualifies as informal, and there is no formal verification system for people to check how their vote is counted.

Due to the use of the Single Transferable Voting (STV) and the First Past the Post (FPP) systems of voting, voting in local elections can be complex, resulting in greater potential for voter-error. For the 2013 local authority elections, the number of blank and informal votes ranged from 0.4 – 13.9 per cent of the total votes per local authority. For district health board elections (which are all run as STV elections), this number ranged from 9.5 – 22.4 per cent. Although some of these may have been deliberately spoiled voting documents, there are also voters who accidentally spoil their voting document, such as by giving multiple candidates the same ranking in an STV election.

Local election modernisation

New Zealanders conduct many of their activities online and also have a number of devices to access the internet.[9] There is growing public expectation that online voting will become available soon, in line with the many other activities already undertaken online. Being able to offer online voting aligns with broader commitments of some local authorities to service modernisation, efficiency and 'going digital'.

Cost and frequency of postal services

The current reliance on postal voting also presents some potential risks to the viability of local elections in the longer term. Declining use of postal mail and the shift towards digital communication both reflect and reinforce the changing preferences of New Zealanders for how they communicate and conduct their affairs, which links back to matters of accessibility.

---

[7] According to Statistics New Zealand, in 2013, 168,000 people had varying issues with seeing, many of whom could have required assistance to vote. Statistics New Zealand. *The New Zealand Disability Survey 2013*. Wellington: Statistics New Zealand, 2014. http://www.stats.govt.nz/browse_for_stats/health/disabilities/other-versions-disability-survey-2013.aspx [accessed 17 February 2015].

[8] According to the Ministry of Education, 87 percent of New Zealanders achieved above the lowest proficiency for prose literacy. This means 13 percent achieved the lowest level of proficiency in prose literacy. Available at: http://www.educationcounts.govt.nz/indicators/main/education-and-learning-outcomes/26327 [accessed 18 February 2015].

[9] In 2012, 2.8 million New Zealanders connected to the internet, with 90 percent of 15 to 44 years olds being connected. Statistics New Zealand. *New Zealanders' connection with the Internet.* Available at: http://www.stats.govt.nz/browse_for_stats/snapshots-of-nz/yearbook/people/population/7-million.aspx [accessed 19 February 2015].

The current legislative framework for local elections does not offer sufficient flexibility to start shifting away from a paper-based system, thus preventing local decision-making around what may be appropriate for engagement with the local community.

Select Committee support

The Justice and Electoral Committee indicated support for trialling online voting in its inquiries into the 2010 and 2013 local elections.

If a trial proceeds, which councils will take part?

There is no obligation on councils to participate in a trial. The Associate Minister of Local Government is seeking from Local Government New Zealand (LGNZ), confirmation of which territorial authorities believe they can meet the requirements in this document and wish to proceed with a trial of online voting. The Minister will also seek LGNZ's view on the appropriate size for a trial to ensure that any trial will produce evidence of the practicality and value of online voting in local elections across New Zealand. A decision on this will need to be made before the regulations to enable a trial are to be made, at the end of 2015.

Key principles for a trial of online voting

The Local Electoral Act has three core principles underpinning it:

- fair and effective representation for individuals and for communities
- all qualified people have a reasonable and equal opportunity to cast an informed vote to nominate a candidate and to become a candidate
- public confidence in local electoral processes and public understanding of local electoral processes including: protection of the freedom of choice of voters and the secrecy of the vote, transparent electoral systems and voting methods and certainty in electoral outcomes.

These core principles have implications for the way a trial of online voting must work. More specific principles that represent the application of the core principles to a trial of online voting are discussed below. These in turn underpin the policy requirements set out further in this document.

Equivalence with current system

The concept of people having reasonable and equal opportunity to vote supports electors having options as to *how* they vote. As such, in an online voting trial, it is important that online voting is only made available to electors as an additional option to postal voting. Further to this, the principles of equality of opportunity to vote and retaining public confidence require that the rules and requirements for online voting are generally equivalent to those for postal voting i.e. are similar except where features of online voting require different provisions to achieve the same or an equivalent outcome. For example:

- Voter coercion has a similar risk profile under both postal and online voting, as in both cases voting is unsupervised by officials and so more stringent protections are not required in the online voting context; but
- Security risks associated with the interception and manipulation of votes once they leave the voter are greater for online voting than postal voting; therefore higher as well as different sorts of requirements will need to apply to online voting.

The principle of equivalence is also important where some elections (e.g. for regional councils or district health boards) are conducted partly in territorial authorities using online voting and partly where this is not the case.

Secrecy of the vote/voter privacy

Further steps need to be considered to ensure that secrecy of the vote is adequately protected, in light of new risks presented by use of the internet. However, it is acknowledged that there are limited means by which an online voting system can influence whether a secure environment exists. It is also important that security requirements do not detract from the provision of a reasonable opportunity to vote that preserves equivalence with postal voting.

Transparency/verifiability

It is particularly important, given the "invisible" nature of online voting processes and opportunities for tampering with these, that the transparency of the online voting system is demonstrated through audit processes that verify accuracy of the system. Such additional requirements are important for ensuring equivalence of public confidence in election results with those conducted using postal voting.

Local government accountability

The way online voting trials are conducted needs to support the role and accountability of electoral officers under the local electoral framework. At the same time, the territorial authorities that choose to participate in a trial accept responsibility for ensuring there is adequate resourcing for an online voting trial in their area, that they meet security expectations, and that they will maintain the integrity of local elections practice. This is consistent with the concept of local government responsibility for local elections that underlies in the local electoral regulatory framework.

Development of requirement for a trial of online voting

Many of the requirements contained in this document have been developed from the Council of Europe Recommendation *Rec(2004)11 of the Committee of Ministers to member states on legal, operational and technical standards for e-voting*.[10] While derived from that recommendation, those requirements have been adapted for the New Zealand local electoral context. A table of cross-references is provided in the appendix to this document, to assist in the understanding of the development of such requirements.

Requirements contained in the Council of Europe recommendation have formed guidance for online voting systems in many countries. Independent assessments of how these systems achieved compliance with those requirements can inform useful discussion. One such example is an assessment report by the International Foundation for Electoral Systems on the Norwegian E-vote Project.[11]

Matters not anticipated by this document

Where a matter arises for which there is not a requirement in this document, the principle of equivalence with the current postal voting system should be applied.

[10] This recommendation is available on the Council of Europe's website. Retrieved 16 April 2015, from http://www.coe.int/t/DEMOCRACY/ELECTORAL-ASSISTANCE/themes/evoting/default_en.asp.

[11] Retrieved 16 April 2015, from https://www.regjeringen.no/globalassets/upload/krd/prosjekter/e-valg/evaluering/topic7_assessment.pdf.

1. Functional requirements

This section covers how online voting should work, and how any online voting system should operate. Note that in this document, use of the term 'online voting system' refers to all components that work together to enable an elector to vote online. This includes systems used at the pre-voting stage, such as to generate or hold voter-related information. It includes the core technology solution that provides an internet-based voting platform, electronically stores votes received online, and enables voters to verify their vote. It also includes systems used at the post-voting stage, such as counting software, which may already be in use under the postal voting system. References to 'relevant electoral officer' mean the electoral officer for the relevant territorial authority participating in a trial.

Trial design

1.1 Online voting must only be made available as an additional option alongside postal voting.

1.2 Voters must be able to vote online using their own internet-capable device, and without any need to install additional software (excluding any required browser upgrades).

1.3 Territorial authorities must explicitly define the availability requirements for their online voting system. In doing so they should take into account voter needs, community expectations and how many of their voters may be seeking to vote online from different time zones.

1.4 Electors must be able to vote online without being required to pre-register.

1.5 Voters must be informed, well in advance of the start of voting, of the way in which online voting will be organised, and any steps a voter may have to take in order to participate and vote.

1.6 Online voters must be able to access online, the same degree of information about candidates as postal voters do with hard-copy documents.

1.7 The period in which an electronic vote can be cast must be:

1.7.1 defined and made known to the public well in advance of the start of voting, and

1.7.2 the same as the time allowed for receipt of postal votes, subject to requirement 2.12

1.8 User experience feedback must be enabled and collected to feed into overall trial learnings.

1.9 All electors in an election for which online voting is being used must be provided with an opportunity to sign up to receive confirmation that an online vote has been received and recorded under their name, and must be notified of this opportunity. This opportunity must be provided separately from the casting of a vote online, and provided regardless of whether and how an elector chooses to vote.

Online voting systems

1.10 Before casting a vote online, voters' attention must be explicitly drawn to the fact that the election in which they are submitting their electronic vote is a real election. If opportunities to practice online voting are offered, participants must have their attention drawn explicitly to the fact that they are not participating in a real election and must, when practice opportunities are continued at election times, at the same time be invited to cast their vote in the real election.

1.11 A valid voter ID and access code, enabling an elector to authenticate him or herself online, must be transmitted to electors by way of at least two separate transactions.

1.12 All voting options, and any information about voting options accessible from the online voting site, must be presented in an equal, unbiased manner.

1.13 The way in which voters are guided through the online voting process must discourage their voting without proper opportunity for reflection.

1.14 Voters must be able to alter their choice at any point in the online voting process before casting their vote, or to break off the procedure, without their previous choices being recorded or made available to any other person.

1.15 If the vote capture device requires a response by a voter within a specific period of time, it must provide fair warning, by issuing an alert a reasonable time before this time period has expired and provide a means by which the voter may receive additional time.

1.16 Before submission of a vote, the online voting technology solution must require a voter to confirm their selection and intention to cast the vote.

1.17 The online voting system must provide the voter with an opportunity to deliberately submit a blank or incomplete voting document.

1.18 Where an online voting document has been incorrectly marked, the online voting technology solution must inform the voter of the nature of the error that has been made and give them an opportunity to fix the error before submission of the voting document.

1.19 The online voting system must indicate clearly to the voter when the vote has been submitted successfully and the voting procedure has been completed.

1.20 The voter must be informed about the means to verify that a connection to the official server has been established and that the voting document presented is genuine.

1.21 The voter must be informed of how to delete, where that is possible, traces of the vote from the device used to cast the vote.

1.22 The online voting system must not allow a voter to submit more than one vote for any election.

1.23 The online voting system must prevent the changing of a vote once that vote has been cast.

1.24 The online voting system must not enable the voter to be in possession of a proof of the content of the vote cast.

1.25 Immediately after their votes have been submitted, voters must be provided with a separate opportunity to submit feedback on their experience.

1.26 Online voting must be designed in a way that protects the secrecy of the vote at all stages of the voting process.

1.27 The design of the online voting system must guarantee that votes submitted online are, and will remain, anonymous, and that it is not possible to reconstruct a link between the content of the vote and the voter.

1.28 The online voting system must be so designed that the expected number of votes in any electronic ballot box will not allow the result to be linked to individual voters.

1.29 The online voting system must prevent processing information on submitted votes that could reveal individual voters' choices.

2. Non-functional requirements

This section covers requirements to ensure online voting works well.

Usability and accessibility

2.1 The voter interface of an online voting technology solution must be understandable and easy to use.

2.2 Online voting systems must be designed, as far as it is practicable, to maximise the opportunities that such systems can provide for persons with disabilities.

2.3 Users and/or representative user organisations must be involved in the design of online voting systems, particularly to identify constraints and test ease of use at each main stage of the development process.

2.4 Online voting technology solutions must support and be tested in any browser or device used by more than 1 percent of people accessing sites of the territorial authority in question.

2.5 The voter interface must conform at Level AA to the W3C's Web Content Accessibility Guidelines (WCAG) 2.0.

2.6 Usability and accessibility measures should not detract from the secrecy and integrity of the election.

Systems operation and process

2.7 Online voting systems and processes must preserve the integrity of individual votes and local elections as a whole, and the online voting process must be verifiable end-to-end.

2.8 The authenticity, availability and integrity of all election data must be maintained.

2.9 Measures must be taken to ensure that the information needed during electronic processing cannot be used to breach the secrecy of the vote.

2.10 Decrypting required for the counting of the votes must not be carried out until the voting period has closed.

2.11 No invalid (informal or out of time) votes must enter the electronic ballot box

2.12 In the last hour of voting at least, the voter interface must inform an elector of the time remaining before close of voting.

2.13 The online voting system must allow voters who are logged on when the voting period ends, to complete and submit their votes during a grace period not exceeding five minutes after the close of voting.

2.14 Those responsible for operating the equipment must draw up a contingency procedure. Any backup system must conform to the same standards and requirements as the original system.

2.15 Sufficient backup arrangements must be in place and be available throughout the voting period to ensure that voting proceeds smoothly. Appropriately authorised persons concerned must be ready to intervene rapidly according to a procedure drawn up by the relevant electoral officer.

2.16 Immediately before the election, the equipment must be checked and approved in accordance with a protocol drawn up by the relevant electoral officer. The equipment must be checked to ensure that it complies with technical specifications. The findings must be submitted to the relevant electoral officer.

2.17 All technical operations must be carried out in accordance with an agreed procedure for controlling operations in the online voting system. Any substantial changes to key equipment must be authorised by the relevant electoral officer.

2.18 Key election equipment, such as servers, must be located in a secure area and that area must, throughout the election period, be guarded against interference of any sort and from any person.

2.19 A disaster recovery plan must be in place during the election period.

2.20 Where incidents that could threaten the integrity of the system occur, those responsible for operating the equipment must immediately inform the relevant electoral officer, who will take the necessary steps to mitigate the effects of the incident. The level of incident which must be reported must be specified in advance by the relevant electoral officer.

2.21 In the event of any irregularity affecting the integrity of votes, the affected votes must be recorded as such.

2.22 Except to allow overseas voters the ability to vote online, vote and voter-related information must not be transmitted or held outside New Zealand at any point before, during, or after an election.

2.23 Information on the functioning of an online voting system must be made publicly available.

2.24 Critical election configuration and management processes must require the participation of teams of more than one appropriately authorised person (two-eyes principle). As far as possible, such activities must be carried out outside the election period.

2.25 The online voting system must be accessible only to persons who are eligible to vote. The online voting system must require anonymous authentication of the elector and must ensure that the elector is enabled to vote in all elections for which the elector is qualified and no other election.

2.26 After the end of the voting period, no voter must be allowed to gain access to the voting platform.

2.27 The online voting system must contain measures to preserve the availability of its services during the voting process. It must resist, in particular, malfunction, breakdowns or denial of service attacks, according to the specifications of the territorial authority taking part in the trial of online voting.

2.28 While an electronic ballot box is open, any authorised intervention affecting the online voting technology solutions must be carried out by teams of at least two people, be the subject of a report, and be monitored by representatives of the relevant electoral officer.

2.29 The online voting system must maintain the availability and integrity of the votes. It must also maintain the confidentiality of the votes and keep them sealed until the counting process. If stored or communicated outside controlled environments, the votes must be encrypted.

2.30 Technical and organisational measures must be taken to ensure that no data will be permanently lost in the event of a breakdown or a fault affecting the online voting system.

2.31 The online voting system must maintain the privacy of individual voters, protecting the secrecy of the vote. Confidentiality of voters' registers stored in or communicated by the online voting system must be maintained.

2.32 The online voting system must perform regular checks to ensure that its components operate in accordance with its technical specifications and that its services are available.

2.33 The online voting system must restrict access to its services, depending on the user identity or the user role, to those services explicitly assigned to this user or role. User authentication must be effective before any action can be carried out.

2.34 Identification of voters and candidates in a way that they can unmistakably be distinguished from other persons (unique identification) must be ensured.

2.35 Online voting systems must generate reliable and sufficiently detailed data so that election observation can be carried out.

2.36 The online voting system must maintain reliable synchronised time sources. The accuracy of the time source must be sufficient to maintain time marks for audit trails and observations data, as well as for maintaining the time limits for voting.

2.37 The online voting system must be able to ascertain that a vote has been cast within the prescribed time limits.

2.38 The online voting system must ensure that the voter's choice is accurately represented in the voting document and that the submitted voting document is securely recorded.

2.39 After the end of the voting period, no voter must be allowed to gain access to the online voting system.

2.40 The integrity of data communicated during the voting stage (e.g. votes, lists of candidates) must be maintained. Data-origin authentication must be carried out.

2.41 The online voting system must maintain the availability and integrity of the electronic ballot box as long as required.

2.42 Voter surveys and their final reports must not compromise directly or indirectly (statistically or by linking information) the secrecy of the vote.

2.43 The online voting system must allow the voter to individually verify that his/her vote is recorded-as-intended.

2.44 The online voting system must allow for an observer or independent auditor to verify that votes are counted as recorded.

2.45 The end-to-end verifiability measures must not compromise the secrecy of the vote.

Interoperability

Between online systems

2.46 All components of the online voting system must be interoperable.

2.47 The online voting system must use open standards and protocols to ensure that the various technical components or services of an online voting system are interoperable with the applicable counting and other local electoral systems.

2.48 A procedure must be established for regularly installing updated versions and corrections of the relevant protection software. It must be possible to check the state of protection of the voting equipment at any time.

2.49 An online voting technology solution must prove its successful interoperability with counting and other local electoral systems by undertaking a test and documenting the results.

With postal voting system

2.50 There must be a secure and reliable method to aggregate electronic and postal votes and to calculate the correct result.

2.51 Aggregated votes must be counted using the counting processes under the existing postal voting system.

2.52 The design of an online voting technology solution must allow for votes to be able to be removed from the electronic ballot box following the processing of special votes.

Security

2.53 Online voting systems must be secure and reliable.

2.54 Online voting systems must comply with New Zealand Government standards and industry best practice for web and applications security, including, at a minimum: the New Zealand Information Security Manual (NZISM), ISO27001, ISO27002 and the OWASP Top 10; and should also meet other web security standards such as the ASD Top 35 mitigations and then SANS Top 25.

2.55 Any online voting system must comply with all mandatory requirements in the NZISM, for government departments regarding security standards for data classified as “In Confidence”.

2.56 Territorial authorities taking part in an online voting trial must assess the broader security risks through the Protective Security Requirements Framework.

Procurement and service provider selection

2.57 Territorial authorities taking part in an online voting trial must employ appropriately skilled personnel to assist with implementation and running of the trial.

2.58 Where a territorial authority does not have appropriately skilled staff, an approved assurance provider (from the public service's ICT Security and Related Services Panel) should be engaged to validate the level of security applied to the online voting system.[12]

2.59 Where territorial authorities seek to use a cloud computing service as a part of participating in an online voting trial, territorial authorities must follow the Government Chief Information Officer's Requirements for Cloud Computing guidance where the online voting system uses a cloud-based service, including endorsement of the solution and acceptance of the residual risks by the head of the territorial authority.[13] In order to inform the solution/tender selection process for cloud-based solutions, territorial authorities must complete the information risk assessment using the All-of-Government 'Cloud Security and Privacy Considerations' questionnaire prior to commencing final contracting negotiations.

2.60 All resulting assurance documentation (endorsement and supporting cloud risk assessment) must be submitted to the Government Chief Information Officer for assurance endorsement purposes.

Risk assessment, assurance, and certification and accreditation

2.61 Territorial authorities taking part in an online voting trial must perform a risk assessment prior to selecting a service provider, in line with the Government Chief Information Officer's All-of-Government information security risk assessment process.[14]

2.62 Any online voting system that is to be selected must be:

2.63.1 assessed to determine its level of security;

2.63.2 certified and accredited through a standardised process, with, at a minimum, the following steps:

2.63.2.1 Risk assessment (RA) – understanding the business and technical context of the information system and identifying the relevant security risks;

2.63.2.2 Privacy Impact Assessment (PIA) – understanding the privacy context and value of the information held in the system;

2.63.2.3 Penetration testing (PT) – to test for vulnerabilities in the system;

2.63.2.4 Statement of applicability (SoA) – identifying the applicable security controls based off leading standard

2.63.2.5 Controls validation plan (CVP) – identifying the documentation and evidence needed to validate the security controls identified in the SoA;

[12] https://www.ict.govt.nz/services/show/SRS-Panel.

[13] https://www.ict.govt.nz/guidance-and-resources/information-management/requirements-for-cloud-computing/.

[14] https://www.ict.govt.nz/assets/ICT-System-Assurance/Risk-Assessment-Process-Information-Security.pdf.

2.63.2.6 Controls validation audit (CVA) – using the CVP to audit the relevant security controls;

2.63.2.7 Certification – assessing the completeness and effectiveness of the security controls that were audited; and

2.63.2.8 Accreditation – granting authority to operate the information system.

Technical assessment and testing of the online voting system prior to use

2.63 Territorial authorities must use an approved provider from the public service's ICT Security and Related Service Panel to undertake all security testing, assessment, and certification and accreditation.

2.64 Territorial authorities must undertake appropriate remediation activities following penetration testing and prior to the online voting system being used.

2.65 Additionally, territorial authorities should conduct:

2.67.1 a further penetration test, using a different Panel provider, prior to the system being used in an election; and

2.67.2 a 'red team' exercise to test the service providers' and authorities' security management and incident response capabilities.

Incident detection, response and management

2.66 A service providers' incident detection capability must be considered as a part of the procurement process.

2.67 A service providers' incident response capability must be considered as a part of the procurement process.

2.68 Any service provider selected to operate an online voting system should have their incident management capability and processes validated during the certification and accreditation process.

Security education and awareness

2.69 Territorial authorities should create and disseminate awareness material to educate voters about device security and what steps they can take to improve the security of their devices before they use the online voting system.

2.70 Territorial authorities should consider providing secure facilities to allow voters to access the online voting system and cast their votes.

2.71 Territorial authority business and technology teams undertaking a trial of online voting should establish connections with international counterparts who have successfully implemented online voting systems.

Confidentiality

2.72 Votes and voter information must remain sealed as long as the data is held in a manner where they can be associated. Authentication information must be separated from the voter's decision at a pre-defined stage in the election.

2.73 The online voting system must protect authentication data so that unauthorised entities cannot misuse, intercept, modify, or otherwise gain knowledge of all or some of this data.

Integrity

2.74 Territorial authorities must put in place all appropriate and reasonable security controls to avoid the possibility of fraud or unauthorised intervention affecting the system during the whole voting process.

2.75 Sufficient means must be provided to ensure that the devices that are used by the voters to cast the vote can be protected against influence that could modify the vote.

Availability

2.76 Territorial authorities, or their services providers, must have measures to ensure availability, within defined requirements, in place, and audited, as a part of the certification and accreditation process.

Audit system

2.77 The online voting system must be auditable end-to-end.

2.78 The audit system must be designed and implemented as part of the online voting system. Audit facilities must be present on different levels of the system: logical, technical and application.

2.79 End-to-end auditing of an online voting system must include recording, providing monitoring facilities and providing verification facilities.

2.80 The audit system must be open and comprehensive, and actively report on potential issues and threats.

2.81 The audit system must record times, events and actions, including:

2.84.1 all voting-related information, including the number of eligible voters, the number of votes cast, the number of invalid votes, the counts and recounts, etc.;

2.84.2 any attacks on the operation of the online voting system and its communications infrastructure;

2.84.3 system failures, malfunctions and other threats to the system.

2.82 The audit system must provide the ability to oversee the election and to verify that the results and procedures are in accordance with the applicable policy, procedural and legal requirements.

2.83 Disclosure of the audit information to unauthorised persons must be prevented.

2.84 The audit system must maintain voter anonymity at all times.

2.85 The audit system must provide the ability to cross-check and verify the correct operation of the online voting system and the accuracy of the result, to detect voter fraud and to prove that all counted votes are authentic and that all votes have been counted.

2.86 The audit system must be protected against attacks which may corrupt, alter or lose records in the audit system.

2.87 The conclusions drawn from the audit process must be documented to ensure that the election is true and accurate and to feed into overall trial learnings.

Assurance and accountability

Territorial authorities

2.88 Territorial authorities must have in place, a project governance structure to:

- Ensure that the design of the online voting as a service is underpinned by a comprehensive assessment of the risks involved in the successful completion of the particular election. The online voting system must include the appropriate safeguards, based on this risk assessment, to manage the specific risks identified.
- Ensure service failure or service degradation are kept within pre-defined limits.
- Ensure that voters understand and have confidence in the online voting system, and that electors are made aware that all rights and responsibilities existing under the Local Electoral Act 2001 still apply in the online voting context.
- Advise the Chief Executive of the territorial authority in question whether online voting is safe to proceed prior to its use in an election.

2.89 Territorial authorities have overall responsibility for ensuring compliance with these policy requirements. Territorial authorities must also undertake project assurance of the development of online voting systems and services.

2.90 Territorial authorities must appoint an independent assurance provider to provide an impartial and independent assessment of the matters in 2.88. The appointment of the independent assurance provider must be approved by the Secretary for Local Government.

2.91 Before any online voting system is used in an election, and at appropriate intervals thereafter, and in particular after any changes are made to the system, an independent assurance provider appointed by the relevant territorial authority must, in the prescribed manner, verify that the online voting system is working correctly and that all the necessary security measures have been taken.

2.92 Before any online voting system is used in an election, the Chief Executive of the territorial authority in question must advise the Secretary for Local Government in writing that:

- he or she considers that all relevant risks have been identified and mitigated to the extent that it is considered safe to proceed with use of online voting, confirming that the relevant electoral officer is of the same opinion.
- The territorial authority has sought and received endorsement of project assurance from the Government Chief Information Officer.

2.93 Territorial authorities must provide to the Secretary for Local Government, copies of all assessments and other documentation necessary to enable a full independent assessment of their online voting systems and services.

Electoral officers

2.94 The electoral officer for a territorial authority conducting an online voting election must be cognisant of all components of the online voting system, as required for verification and certification purposes.

2.95 Before any online voting election takes place, the electoral officer must be satisfied that the online voting system is legitimate and operates in accordance with these requirements and relevant legislation.

2.96 The electoral officer must ensure that only persons authorised by the electoral officer have access to the central infrastructure, the servers and the election data. There must be clear rules established for such authorisation, and all such persons must be subject to sections 14 and 131 of the Local Electoral Act 2001.

Appendix

This Appendix is only included to assist in the understanding of the development of policy requirements contained in this document. It cross-references the requirements contained in this document with similar requirements contained in the Council of Europe (CoE) Recommendation *Rec(2004)11 of the Committee of Ministers to member states on legal, operational and technical standards for e-voting*. More information on the relevance of those requirements is provided on page 7 of this document.

Requirement no. (NZ)	Requirement no. (CoE)
1.1	4
1.2	
1.3	
1.4	
1.5	38
1.6	
1.7	37
1.8	
1.9	
1.10	50
1.11	
1.12	12, 47,49
1.13	10
1.14	11
1.15	
1.16	
1.17	13
1.18	
1.19	14
1.20	90
1.21	93
1.22	5
1.23	15
1.24	51
1.25	
1.26	16
1.27	17
1.28	18
1.29	54
2.1	1
2.2	3
2.3	62
2.4	
2.5	
2.6	
2.7	26
2.8	83
2.9	19
2.10	55
2.11	
2.12	
2.13	

Requirement no. (NZ)	Requirement no. (CoE)
2.14	70
2.15	71
2.16	73
2.17	74
2.18	75
2.19	75
2.20	76
2.21	58
2.22	
2.23	21
2.24	32
2.25	94
2.26	96
2.27	30
2.28	33
2.29	
2.30	77
2.31	78
2.32	79
2.33	80
2.34	82
2.35	
2.36	84
2.37	91
2.38	95
2.39	96
2.40	97
2.41	99
2.42	
2.43	
2.44	
2.45	
2.46	
2.47	
2.48	69
2.49	
2.50	
2.51	
2.52	
2.53	28
2.54	
2.55	

Requirement no. (NZ)	Requirement no. (CoE)
2.56	
2.57	
2.58	
2.59	
2.60	
2.61	
2.62	
2.63	
2.64	
2.65	
2.66	
2.67	
2.68	
2.69	
2.70	
2.71	
2.72	35
2.73	81
2.74	29
2.75	92
2.76	
2.77	59
2.78	100
2.79	101
2.80	102
2.81	103
2.82	104
2.83	105
2.84	106
2.85	107
2.86	109
2.87	60
2.88	
2.89	85
2.90	85
2.91	25
2.92	
2.93	
2.94	24
2.95	31
2.96	