Deloitte.

NSW Electoral Commission

iVote Controls Review

Pre-Election Report

15 November 2021

Inherent limitations

The Services provided are advisory in nature and have not been conducted in accordance with the standards issued by the Australian Auditing and Assurance Standards Board and consequently no opinions or conclusions under these standards are expressed.

Because of the inherent limitations of any internal control structure, it is possible that errors or irregularities may occur and not be detected. The matters raised in this report are only those which came to our attention during the course of performing our procedures and are not necessarily a comprehensive statement of all the weaknesses that exist or improvements that might be made.

Our work is performed on a sample basis; we cannot, in practice, examine every activity and procedure, nor can we be a substitute for management's responsibility to maintain adequate controls over all levels of operations and their responsibility to prevent and detect irregularities, including fraud. Any projection of the evaluation of the control procedures to future periods is subject to the risk that the systems may become inadequate because of changes in conditions, or that the degree of compliance with them may deteriorate. Recommendations and suggestions for improvement should be assessed by management for their overall impact before they are implemented.

We believe that the statements made in this report are accurate, but no warranty of completeness, accuracy, or reliability is given in relation to the statements and representations made by, and the information and documentation provided by NSW Electoral Commission (NSWEC) personnel. We have not attempted to verify these sources independently.

Limitation of use

This report is not intended to and should not be used or relied upon by anyone else and we accept no duty of care to any other person or entity. The report has been prepared for the purpose set out in our contract dated 18 May 2021. You should not refer to or use our name or the advice for any other purpose.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms, and their related entities. DTTL (also referred to as "Deloitte Global") and each of its member firms are legally separate and independent entities. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

The entity named herein is a legally separate and independent entity. In providing this document, the author only acts in the named capacity and does not act in any other capacity. Nothing in this document, nor any related attachments or communications or services, have any capacity to bind any other entity under the 'Deloitte' network of member firms (including those operating in Australia).

Liability limited by a scheme approved under Professional Standards Legislation.

Member of Deloitte Asia Pacific Limited and the Deloitte organisation.

Table of contents

Section I:
Executive Summary

Section I: Executive Summary

Overview

NSW Electoral Commission ('NSWEC') is a statutory authority responsible for conducting, regulating and reporting on general and by-elections for the Parliament of New South Wales. NSWEC's main responsibilities include:

- Running independent, fair and accessible elections;
- Providing guidance to assist political participants in complying with their legal obligations;
- Publishing political donation and expenditure disclosures and registers of political parties;
- Engaging with the public to simplify and increase the participation of the democratic process; and
- Conducting investigations of possible offences (including the enforcement of breaches) of electoral, funding and disclosure and lobbying laws.

As part of NSWEC's effort to simplify and increase the participation in the democratic process, NSWEC introduced a remote electronic voting system, named iVote, in November 2011 to provide technology-assisted voting to eligible electors registered to vote in NSW. As at October 2021, the iVote system has been used as a remote electronic voting system for the following elections:

- 2011 NSW State General Election;
- 2015 NSW State General Election;
- 2019 NSW State General Election; and,
- 11 NSW State by-elections from November 2011 to May 2021.

With each implementation, iVote has constantly been refined to improve the iVote experience for electors, as well as providing electors with assurances by using the latest advances in electronic voting technologies and security.

The iVote voting channel is offered alongside postal and early voting channels to provide a means of voting for electors who do not have the ability to vote independently or have difficulty voting in person at a voting centre on election day. Electors can vote using iVote if they:

- are blind or have low vision;
- are unable to vote without assistance or have difficulty voting at a polling place because they have a disability or have difficulties reading;
- are a silent elector;
- applied for a postal vote but did not receive a postal ballot papers before 5pm on 26 November 2021;
- live more than 20 kilometres from a polling place; or,
- will not be within the council area during election day.

Eligibility criteria to use iVote are defined in the Electoral Act 2017 under Section 152, and are defined in the Local Government (General) Amendment Regulation 2021, under Section 333C, for NSW Local Government elections.

The iVote voting channel will be made available from 9am on Monday, 22 November, until 1pm on Saturday, 4 December.

Purpose

At the request of NSWEC, Deloitte Touche Tohmatsu ('Deloitte') undertook an engagement to provide a pre-election report on the design and operating effectiveness of NSWEC's information technology controls within the iVote system which can be tested pre-election.

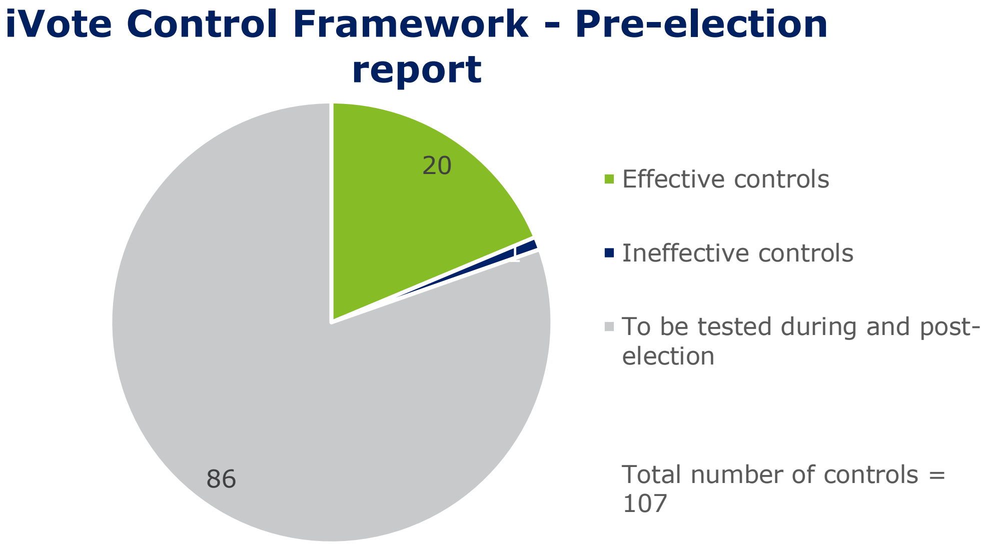
Scope

Independent auditing of technology assisted voting is required by Section 156 of the NSW Electoral Act 2017 and by Section 333G of the Local Government (General) Amendment Regulation 2021.
The NSW Electoral Commissioner has engaged Deloitte as an independent auditor to assist in independently validating the iVote control environment prior to and during the NSW Local Government Elections on 4 December 2021.

The NSW Electoral Commission have developed an iVote control framework. This framework draws on the guidance from industry practices, as listed in Section IV of this document, as well as the Electoral Council of Australia and New Zealand (ECANZ). Testing against this control framework has been conducted for those controls which could be tested prior to the elections. Refer to Section IV for further information.

Summary of results

Below is a summary of the pre-election report results. This summary of results does not provide all details relevant for users of this report and should be read in conjunction with the entire report. The details of the specific controls tested, and the nature, timing and extent of those tests, are listed in Section IV.



Control Reference	Control Activity	Details of Control deviation
10.02	The voter must be made aware of the information collected from them during all phases of election (registration to results).	• Notice of Personally Identifiable Information (PII) retention was not explicitly highlighted for the following iVote stages: - Registration: The privacy policy is included as a link in the website footer; however notice of specific PII retention was not explicitly referenced throughout the registration process. - Voting: The voting process references external webpages, however, notice of specific PII retention was not explicitly referenced throughout the voting process.

The controls which could not be tested pre-election will be tested during and after the system is made available to voters from 9am on Monday, 22 November, until 6pm on Saturday, 4 December. A reasonable assurance report on the design and operating effectiveness of NSWEC's controls throughout the period of the election will be completed by Deloitte post-election.

Acknowledgement

We wish to place on record our appreciation of the assistance and cooperation received from the management and staff of NSWEC in completing this pre-election report.

Duncan Auty
Partner,
Deloitte Touche Tohmatsu

Section II:
iVote Vote Journey Map

iVote

iVote is a technology assisted voting system provided by NSW Electoral Commission (NSWEC).

Eligible voters use iVote from the devices that suit their needs, either online or over the phone.

Who can use iVote?

You can vote using iVote if you:

- are blind or have low vision
- are unable to vote without assistance or have difficulty voting at a poling place because you have a disability or have difficulties reading
- are a silent elector
- applied for a postal vote buy did not receive your postal ballot before 5pm on 26 November 2021
- live more than 20 kilometres from a polling place, or
- will not be within the council area during election day.

Controls at-a-glance

The iVote system has processes that keep iVote secure, reliable and accessible.

Governance

- Processes for iVote reflect the rules used for other voting channels
- iVote platform enforces one vote per person
- Independent assessment from third parties ensure the platform is accessible (WCAG 2.0 compliant)
- Voters can verify that their vote was correctly recorded by NSWEC after voting
- Electoral Commissioner approves the iVote system for use in line with published policies and procedures
- An Independent Auditor is engaged to audit the voting technology used throughout the voting period (from pre-election activities to close of vote processes)
- Scrutineers are invited to observe that the approved procedures are followed

Authentication

- Voters use a password and a unique iVote number sent to them before accessing a voting ballot or verifying their vote

Refer to Section IV for background processes and controls not depicted in this journey map.

Key

- ? Key question
- Purpose
- Process

1 Apply

How does a voter apply for iVote?

Applying to use iVote is simple and voters can do it themselves.

If eligible, a voter applies online on the iVote site or by contacting the Call Centre.

Applying for iVote is a similar process to applying for a postal vote. A voter checks that they're on the roll and that their details are correct. For security, voters can provide additional identification documents for checking (such as a passport or driver license).

Voters create a password when applying. After applying the voter will get their iVote number to access the iVote platform. Voters can choose to get their iVote number by SMS or email.

Voters will receive an iVote number after successfully applying. This allows voters to log into the voting system to cast their vote.

2 Vote

How is a vote cast with iVote?

Vote securely in the way that suits the voter.

Voters use their iVote numbers to vote online or over the phone.

iVote is an accessible online platform that supports assistive technology. Call centre operators can also support voters and help cast votes over the phone.

After voting, voters will get confirmation via a receipt that their vote has been received by NSWEC.

If voters don't get confirmation, or if they have difficulties with voting, they can contact the Call Centre for help.

Voters can choose to verify or check their vote as an optional step.

3 Verify & Check

How can a voter be sure their vote has been received?

Be confident that a vote has been received by checking the vote afterwards.

Voters can choose to check or verify their votes after voting, using the confirmation they got in Step 2. These are optional steps.

QR codes

Online voters will have one hour to use their QR code to verify their vote. The NSW Verification App is used to verify a vote. Users can download the app from the Android or iOS app stores.

Voters can identify in the app if there is any issue with their vote. The call centre can then help them fix it.

Receipts

Voters can use their receipt with the Receipt Check Portal to check their vote is saved in iVote.

Voters can contact the call centre if there are any issues.

Controls at-a-glance

The iVote system has processes that keep iVote secure, reliable and accessible.

Authentication

Restricted access to use and maintain iVote systems limits security threats

Encryption

iVote platform ensures counted votes can't be connected to a voter

NSWEC encrypts and securely stores uncounted votes

Monitoring protects voting information and data

Refer to Section IV for background processes and controls not depicted in this journey map.

4 Secure & Protect

How does iVote making voting safe and secure?

Validation processes protect and anonymise data.

iVote voting closes at the same time as polling place voting and is then ready for vote processing.

Like regular voting, supervisors check the exporting of a 'virtual ballot box', including:

- two Admin board members (ensures all involved follow processes)
- an independent auditor (assesses the use of technology)
- invited scrutineers to observe that the approved procures are followed.

Secure IT hardware stores data and performs key processes to protect from online threats.

NSWEC processes votes to make sure that:

- only one vote per voter is included in the final vote count
- each vote is stripped of any personal information
- each vote is mixed and randomised

This removes any chances of using information to connect votes to people. After decryption and before tally, an independent expert reviews the mixing and decryption process to make sure it is correct.

Then, a quorum of the Electoral Board (3 of the 6 members) must agree to decrypt the votes and then convert the vote data into files that the counting systems can use. Converted files are stored on USB memory, placed in a Tamper Evident Bag and secured by the Electoral Commissioner until tally.

5 Tally

How are votes through iVote counted?

iVotes go through extra security measures before tallying.

The Electoral Commissioner organises locking away all physical devices with iVote data including any offline machines used in decryption. Where possible, Tamper Evident Bags or election seals are used to secure offline machines or devices with data when not in use.

On 'proof checking', an Independent Monitor (an expert in Cryptography) will check the mathematical proofs and comparison of vote receipts. NSWEC immediately investigates any issues raised to determine if there was any fault with the system and votes.

iVote votes are loaded into the count system alongside votes from other channels.

Finally, once all valid votes from the election are in the count system, the count system proceeds to generate the final results.

NSWEC destroys all votes as per legislation, including iVotes.

Trust & Transparency

How can I trust the iVote system?

Controls are defined and implemented to protect the integrity and accuracy of the votes in the iVote system.

NSWEC have defined policies on how the iVote system should be controlled. These include policies on security, data encryption and privacy, the look and usability of the system, and the management of system changes and incidents.

Controls have been implemented to protect data (including personal and voting data), access to the systems, and the physical security of the systems.

Tests are periodically run to check the security of the system and identify any vulnerabilities. If security flaws are identified these are corrected prior to an election.

Tools have been implemented to monitor and detect security events. If a security incident is detected, it is assessed and resolved as a priority.

When developing enhancements to the iVote software, secure development practices are used to make sure software code is developed in a safe way.

Before an election, the electoral management body makes sure that the iVote system is functioning as it should.

During the election, controls are implemented in the system to check that the person voting has been validated before allowing them to vote.

Should any issues occur with the system during an election, such as the system going off-line unexpectedly, procedures have been defined and tested to make sure that the issue is fixed as soon as possible.

Section III:
Overview of the Work Performed

Section III: Overview of the Work Performed

Overview

NSWEC have developed and continually improved their iVote control framework after each Election, most recently after the 2021 Upper Hunter By-election. This framework draws on the guidance from industry practices, listed below, as well as the Electoral Council of Australia and New Zealand (ECANZ).
Industry practices include:

- Voluntary Voting Systems Guidelines (VVSG) published by National Institute of Standards and Technology (NIST), USA;
- ISO27001:2013 Information Security - Appendix A Clauses; and
- Council of Europe recommendations on standards for e-voting.

For further information, please refer to the Control Assessment Framework published on the NSWEC Website (the 'Framework').

Introduction

This report is intended to provide NSWEC with information for their evaluation on the effective design and operating effectiveness of their control framework over the iVote system pre-election.

Deloitte's pre-election work is advisory in nature and has not been conducted in accordance with the standards issued by the Australian Auditing and Assurance Standards Board and consequently no opinions or conclusions under these standards are expressed. Testing of controls was restricted to the control objectives and related control activities listed in Section IV which are operated by NSWEC and was not extended to controls that may be in effect at third party organisations.

Deloitte's work was carried out at both the premises of NSW Electoral Commission in Sydney and remotely. The scope of work was based on the control framework as agreed with management of NSW Electoral Commission prior to the commencement of the election.

Control environment elements

The control environment sets the tone of an organisation, influencing the control consciousness of its people. It is the foundation for other components of internal control, providing discipline and structure. Deloitte Touche Tohmatsu's procedures included tests of design, implementation, and operating effectiveness of controls identified by NSWEC in the following areas:

A. IT Governance
B. Logical Access and Identity Management
C. Data Privacy and Protection
D. Change Management Process
E. Security Monitoring
F. Physical Security Monitoring
G. Business Continuity Management

Such tests included inquiry of the appropriate management, supervisory, and staff personnel; observation of NSWEC's activities and operations, inspection of NSWEC's documents and records, and re-performance of the application of NSWEC's controls. The results of these tests were considered in planning the nature, timing, and extent of testing of the control activities described in Section IV.

Obtaining Evidence Regarding Design of Controls

In determining which of the controls are necessary to achieve the control objectives stated in the control framework, Deloitte assessed whether those controls were suitably designed. This included:

a) Identifying the risks that threaten the achievement of the control objectives in the framework; and
b) Evaluating the linkage of controls identified in the framework with those risks. Some of the considerations Deloitte took into account included:
   - Appropriateness of the purpose of the control and its correlation to the risk/assertion
   - Competence and authority of the person(s) performing the control

- Frequency and consistency with which the control is performed
- Level of aggregation and predictability
- Criteria for investigation (i.e. threshold) and process for follow-up.

Tests of operating effectiveness

Deloitte's tests of the controls were designed to cover a representative number of sample throughout the per-election period. In determining the nature, timing and extent of tests we considered the following:

a) Nature and frequency of the controls being tested
b) Types of available evidential matter
c) Nature of the control objectives to be achieved
d) Assessed level of control risk
e) Expected effectiveness of the test, and
f) Results of tests of the control environment.

Testing the accuracy and completeness of information provided by NSWEC is also part of the testing procedures performed. Information we utilised as evidence may have included, but was not limited to:

a) Standard "out of the box" reports as configured within the system
b) Parameter-driven reports generated by NSWEC systems
c) Custom-developed reports that are not standard to the application such as scripts, report writers, and queries
d) Spreadsheets that include relevant information utilised for the performance or testing of a control
e) NSWEC prepared analyses, schedules, or other evidence manually prepared and utilised by NSWEC.

While these procedures may not be specifically called out in the test procedures listed in Section IV, they may be completed as a component of testing to support the evaluation of whether or not the information is sufficiently precise and detailed for purposes of fully testing the controls identified by NSWEC.

Description of testing procedures performed

Deloitte performed a variety of tests relating to the controls listed in Section IV throughout the pre-election period. The tests were performed on controls as they existed during this period and were applied to those controls relating to control objectives specified by NSWEC.

Tests performed for the purpose of this report may have included, but were not limited to those described below:

Test	Description
Inquiry	Conducted detailed interviews with relevant personnel to obtain evidence that the control was in operation during the report period and is accompanied by other procedures noted below that are necessary to corroborate the information derived from the inquiry.
Observation	Observed the performance of the control multiple times throughout the report period to evidence application of the specific control activity.
Inspection of documentation	If the performance of the control is documented, inspected documents and reports indicating performance of the control.
Reperformance of monitoring activities or manual controls	Obtained documents used in the monitoring activity or manual control activity and independently reperformed the procedures. Compared any deviation items identified with those identified by the responsible control owner.
Reperformance of programmed processing	Input test data, manually calculated expected results, and compared actual results of processing to expectations.

Sampling Methodology

In terms of frequency of the performance of the control by NSWEC, we consider the following guidance when planning the extent of tests of control for specific types of control.

a) The purpose of the procedure and the characteristics of the population from which the sample will be drawn when designing the sample;
b) Determine a sample size sufficient to reduce sampling risk to an appropriately low level;
c) Select items for the sample in such a way that each sampling unit in the population has a chance of selection;
d) If a designed procedure is not applicable to a selected item, perform the procedure on a replacement item; and
e) If unable to apply the designed procedures, or suitable alternative procedures, to a selected item, treat that item as a deviation.

The following guidelines are at a minimum followed in performing the test of controls:

Frequency of control activity	Minimum sample size
Annual	1
Quarterly	2
Monthly	2
Weekly	5
Daily	15
Many times per day	25
Automated Controls	Test one instance of each automated control.
Indirect Controls (e.g., indirect entity-level controls, general IT controls)	For those indirect entity-level controls that do not themselves directly address risks of material misstatement, the above is the suggested minimum sample size for the test of operating effectiveness. In the event that the indirect control is directly responsive to the control objective, the above is the minimum sample size for the test of operating effectiveness.
The table assumes zero deviations.	

The nature and cause of deviations identified (if any), were evaluated to conclude on whether the deviations are material individually or in combination.

Results of testing

The concept of effectiveness of the operation of controls recognises that some deviations in the way controls are applied by NSWEC may occur. Deviations from prescribed controls may be caused by such factors as changes in key personnel, significant seasonal fluctuations volume of transactions and human error.

We use judgement in considering the overall operating effectiveness of the control by considering the number of deviations detected, the potential significance of the financial statement effect, as well as other qualitative aspects of the deviations such as the cause of the deviation.

When we identify a deviation for a periodic or automated control, we consider whether other controls / mitigating controls may provide the evidence we require.

If we find a single deviation in the initial sample for a recurring manual control operating multiple times per day, when we did not expect to find control deviations, we consider whether the deviation is representative of systematic or intentional deviations.

If control deviations are found in tests of controls which operate daily or less frequently, the sample size cannot be extended and we assess such controls as ineffective.

Section IV:
Control Objectives, Control Activities, Testing of Design and Implementation and Operating Effectiveness

Section IV: Control Objectives, Control Activities, Testing of Design and Implementation and Operating Effectiveness

Introduction

This section presents the following information provided by Deloitte:

- A description of the tests performed by Deloitte to determine whether NSWEC controls were designed and operating with sufficient effectiveness to achieve specified control objectives. Deloitte determined the nature, timing, and extent of the testing performed.
- The results of Deloitte Touche Tohmatsu’s tests of controls.

Detailed Design, Implementation and Operating Effectiveness Testing Breakdown

Effectiveness of each assessed control can be found in the tables below. Each assessed controls have also been mapped to the Vote Journey depicted in Section II.

CONTROL OBJECTIVE 1–

Control Objective: A set of policies for information security are defined, reviewed on a periodic basis, published, and communicated to all relevant stakeholders operating and managing technology assisted voting.

Control Reference	Control Activity	2021 Test Procedures	Results of Tests
1.01	NSWEC have a defined, documented, periodically reviewed and approved information security policy for managing security. The policy is communicated to all relevant stakeholders including key suppliers.	1. Enquire with management to determine whether NSWEC have a defined and documented Information Security Policy in place for the iVote system. 2. Obtain and inspect the NSWEC Information Security Policy to determine if it is: - Approved by senior management; - Reviewed on a regular, predefined basis; and, - Covers relevant and key areas of security in line with better practice (i.e. NIST). 3. Obtain and inspect screenshot of intranet or equivalent to determine if policy is communicated to all relevant stakeholders including key subcontractors. 4. Obtain and inspect evidence of employee acknowledgement of policy/procedures, on starting and periodically during employment.	To be tested during and post-election.
1.02	Appropriate standards, guidelines, and procedures are in place to manage information security in accordance with the information security policy.	1. Enquire with management to determine whether NSWEC has defined and documented policies and procedures in place for the iVote system which are aligned to the Information Security Policy. 2. Obtain and inspect Information Technology Service Management (ITSM) policies and procedures to determine whether appropriate standards, guidelines and procedures have been defined for the following areas: - Cryptographic Key Management Standard; - Access Control policy/procedure; - Network Security policy/procedure; - Security Monitoring policy/procedure; and, - Documents listing out security controls for iVote.	To be tested during and post-election.
1.03	A risk register is maintained and regularly reviewed which captures identified risks to technology assisted voting.	1. Enquire with management to determine whether a risk register is maintained which captures identified risk to iVote. 2. Obtain and inspect the risk register to determine whether: - A risk register is maintained which captures identified risk to iVote; - A risk owner and treatment plan is identified; and, - A regular review is performed over this risk register.	No exceptions noted.

Control Reference	Control Activity	2021 Test Procedures	Results of Tests
1.04	A risk mitigation program is established to identify and mitigate the risks identified in the risk register.	1. Enquire with management to determine whether a risk mitigation program is utilised to identify and mitigate risks identified in the risk register. 2. Obtain and inspect the risk register to determine the total number of risks identified as part of the iVote operation. 3. For a sample of risks, perform inspection to determine whether risk mitigation programs are identified and implemented, including risk treatment plans, updates and action owners.	To be tested during and post-election.

CONTROL OBJECTIVE 2–
Control Objective: Controls have been implemented to enable voters to effectively and accurately use technology assisted voting.

Control Reference	Control Activity	2021 Test Procedures	Results of Tests
2.01	The voter is informed about how to accurately use technology assisted voting.	1. Enquire with management to determine whether NSWEC has established help files and FAQs for voters on the iVote website and how these are accessed. 2. Obtain and inspect help files (including instructional videos / media) and FAQs to determine whether help files and FAQs: - Are available for voters on the iVote website; - Provide information to voters about the steps for registration in order to use iVote; - Are made available online to help build awareness of the: o Timelines for using iVote for voting; o Details of the candidates and other available choices; and, o Details on how to register for iVote and use iVote system. - Provides information to voters about the steps for a voter to cancel their selection and re-submit their vote.	No exceptions noted.
2.02	Technology assisted voting provides feedback on the confirmation of valid/invalid options and on successful completion of voting procedure.	1. Obtain and inspect evidence to determine whether the iVote application provides feedback on the selection of valid/invalid options and on successful completion of voting procedure.	To be tested during and post-election.
2.03	Voters are able to test/perform a demonstration to familiarise themselves with the system.	1. Obtain and inspect evidence to determine whether iVote has a test/demonstration version for voting made available to the voters.	To be tested during and post-election.

CONTROL OBJECTIVE 3–

Control Objective: All official voting information is presented in an equivalent way, across various voting channels to ensure that voter's intentions are not affected.

Control Reference	Control Activity	2021 Test Procedures	Results of Tests
3.01	The candidate information on technology assisted voting is equivalent to the physical ballot.	1. Enquire with management to determine whether candidate information on iVote is equivalent to the physical ballot. 2. Observe the logic and accuracy testing to determine whether the candidate information presented on all components of iVote is consistent with the physical ballot (including the presentation of information through screen readers). 3. Where relevant, obtain and inspect that NSWEC have created a guideline that shows where the iVote ballot paper may differentiate from the physical ballot paper in accordance with the Electoral Act.	To be tested during and post-election.
3.02	No influential language is used which may influence voters towards/against a particular candidate.	1. Enquire with management to determine how management ensure no influential language is used which may influence voters towards/against a particular candidate. 2. Obtain and inspect evidence to determine whether any of the information on the registration and voting systems may influence voters towards/against a particular candidate including: - Help documents; - Technology Assisted Voting Approved Procedures; - FAQs; and, - Accessibility information - screen readers, AUSLAN document. 3. Confirm that language used for ballot paper instructions are replicated in iVote voting instructions unless stated otherwise in the Technology Assisted Voting Procedures.	To be tested during and post-election.
3.03	The technology assisted voting platform is designed to prevent influencing voters into making a specific choice when casting a vote.	1. Enquire with management to determine how the iVote platform is designed to prevent influencing voters into making a specific choice when casting a vote. 2. Observe that the candidate information displayed to voters within the voting system is consistent with all channels of voting in terms of candidate order, and with consistent colour, font, and size for each candidate on a ballot.	To be tested during and post-election.

Control Reference	Control Activity	2021 Test Procedures	Results of Tests
3.04	Technology assisted voting allows users to cast their vote without providing a preference.	1. Enquire with management to determine whether iVote allows users to cast their vote without providing a preference. 2. Observe whether iVote allows the voter to cast a vote without providing a preference for any of the listed voters (to align to what can be done in the physical ballot).	No exceptions noted.

CONTROL OBJECTIVE 4–

Control Objective: Technology assisted voting will ensure that only the appropriate number of votes per voter is cast, stored in the electronic ballot box and included in the election result.

Control Reference	Control Activity	2021 Test Procedures	Results of Tests
4.01	Identity of the voter must be authenticated during the registration process.	1. Enquire with management to determine whether the registration process authenticates voters prior to voting. 2. Observe the registration process onscreen to determine whether voters are authenticated against the electoral roll.	To be tested during and post-election.
4.02	Technology assisted voting allows only voters who have successfully completed the registration process for voting to log in and cast a vote.	1. Enquire with management to determine whether iVote allows only voters who have successfully completed the registration process for voting to log in and cast a vote 2. Observe and re-perform the authentication and voting process onscreen to ensure that only users who have authenticated into iVote can cast a vote.	To be tested during and post-election.
4.03	Voters who have changed their vote/re-voted have their previous vote discarded.	1. Enquire with management to determine whether prior votes are discarded when a voter re-votes. 2. Obtain and inspect the iVote voting procedure to determine whether prior votes are discarded when a voter re-votes. 3. Obtain and inspect evidence of daily cleansing during voting period to determine whether prior votes are discarded when a voter re-votes. 4. Obtain and inspect iVote system documentation to determine if prior votes are discarded when a voter re-votes.	To be tested during and post-election.

Control Reference	Control Activity	2021 Test Procedures	Results of Tests
4.04 ✓	Prior to the final result, the voting system identifies votes which are invalid, duplicated or generated due to an error.	1. Enquire with management to understand final vote procedures executed within the iVote system, including the identification of invalid or duplicate votes, as well as votes generated in error. 2. Obtain and inspect documented procedure implemented and confirm whether it is defined to ensure invalid/duplicate votes are removed. 3. Obtain and inspect iVote generated reporting to determine total number of votes that are invalid, duplicated or generated due to error. 4. Obtain and inspect evidence to indicate these votes are not included in the final vote results. 5. Observe during the decryption ceremony to determine whether the iVote system identifies invalid, duplicate, or votes generated due to error. Confirm whether the following information is captured: - Number of voters – registered; - Voters who voted (data from iVote); - Duplicate voters where an additional channel of voting has been used and supports a real time voter roll; - Voters who voted (data from verification system); and, - Votes with errors.	To be tested during and post-election.

Control Reference	Control Activity	2021 Test Procedures	Results of Tests
4.05 🔍 🛡	Prior to the final results, the number of votes from the voting system and the assurance system are compared and validated. The final result of technology assisted voting must be clearly established.	1. Enquire with management to determine whether the number of votes from the voting system and assurance system are compared and validated prior to the final results. 2. Obtain and inspect documented procedure to determine if requirements for assessment of valid, invalid and duplicate votes through different channels are conducted before the final results of the vote is calculated. 3. Observe the decryption ceremony to determine whether the final count takes into account the valid, invalid and duplicate votes through different channels. Further determine if receipts from the voting system and assurance system are compared and the final result of iVote is clearly established. 4. Obtain and inspect a listing of votes from both iVote voting and assurance systems to determine if the number of votes match and votes are validated. 5. Where applicable, obtain and inspect evidence of discarding and/or remediation of votes with errors.	To be tested during and post-election.

CONTROL OBJECTIVE 5–
Control Objective: The voter interface of technology assisted voting is easy to understand and use.

Control Reference	Control Activity	2021 Test Procedures	Results of Tests
5.01 ✓	Technology assisted voting will enable all voters including persons with disabilities to vote.	1. Enquire with management to understand whether iVote enables all voters (including persons with disabilities) to vote. 2. Observe onscreen to determine whether all the components of the iVote system (registration, voting and assurance) provides users with accessibility options (screen readers etc.) 3. Obtain and inspect the Web Content Accessibility Guidelines (WCAG) 2.0 to determine the requirements that iVote is required to meet. 4. Obtain and inspect results and/or reports from the testing organisations (i.e. Vision Australia) to determine that iVote allows voters (including persons with disabilities) to vote. 5. Where applicable, obtain and inspect evidence of remediation of issues identified by the testing organisation to determine if fixes have been implemented to enable voters (including persons with disabilities) to vote.	No exceptions noted.
5.02 ✓ 🔍	Technology assisted voting is designed to be used on various device types (mobile, laptop, tablets etc.) and maintains the uniformity of the information.	1. Enquire with management to understand how iVote operates in a uniformly manner across different types of devices. 2. Re-perform the registration of iVote accounts on various devices and determine if all the components of the iVote system (registration, voting and assurance) operates as designed on various devices (mobile, laptop, tablets etc.). 3. Observe at Ballot Proofing sessions to determine if iVote is checked using various devices. 4. Obtain and inspect results and/or report from testing organisations (i.e. Vision Australia) to ensure iVote operates as designed on various devices (mobile, laptop, tablets etc.) to determine if iVote maintains the uniformity of information on various device types (mobile, laptop, tablets etc.).	To be tested during and post-election.

Control Reference	Control Activity	2021 Test Procedures	Results of Tests
5.03 ✓	A mechanism is established for voters to speak to person(s) about using technology assisted voting and ask their queries.	1. Enquire with management to determine whether a mechanism has been established for voters to speak with voting staff about iVote queries. 2. Obtain and inspect evidence to determine whether a call centre was operating to help voters with their iVote queries throughout the voting period.	To be tested during and post-election.

CONTROL OBJECTIVE 6–
Control Objective: Technology assisted voting will only grant a user access after authenticating her/him as a person with the right to vote. The voting system will protect authentication data of the voters, to prevent its misuse, interception, or modification by an unauthorised or malicious user.

Control Reference	Control Activity	2021 Test Procedures	Results of Tests
6.01 🔗	Each registered voter is provided with unique credentials to access all components of technology assisted voting and voters are required to setup their own PIN/Passwords during iVote registration to access the voting system.	1. Enquire with management to understand how the registration process authenticates voters prior to voting. Further understand how voters are provisioned unique iVote Numbers. 2. Obtain and inspect process documentation to ensure that iVote numbers generated by the Credential Management System are unique in nature. 3. Re-perform registration in the test environment of the iVote System to ensure that upon application of an iVote number, users are required to setup their own PIN/Password.	To be tested during and post-election.
6.02 🔗	In order to reset the PIN/Password and generate new credentials users must re-verify their identity.	1. Enquire with management to determine whether NSWEC has defined policies and procedures to verify the identity of the voter prior to re-setting the credentials. 2. Obtain and inspect policies and procedures to determine whether users must re-verify their identity in order to reset the PIN/Password and generate new credentials. 3. Observe and re-perform the PIN/Password reset process onscreen to determine whether voters must re-verify their identity before re-setting the iVote PIN/Password.	No exceptions noted.
6.03	The authentication data is securely erased from technology assisted voting when it is no longer required.	1. Enquire with management to determine whether NSWEC has defined policies and procedures to securely erase authentication, security and privacy data when it is no longer required. 2. Obtain and inspect policies and procedures to determine whether they include data disposal processes when iVote is no longer required, including the deletion of authentication, security and privacy data. 3. Observe the data removal process for a prior election to determine whether authentication data is be securely erased from iVote when it is no longer required.	To be tested during and post-election.

CONTROL OBJECTIVE 7–
Control Objective: Procedures on encryption are developed and implemented for the use of cryptography to protect votes and voter data during election.

Control Reference	Control Activity	2021 Test Procedures	Results of Tests
7.01	An encryption policy is formally documented with approved encryption standards to be used.	1. Enquire with management to determine whether NSWEC has a defined and documented Encryption Policy in place for the iVote system. 2. Obtain and inspect the NSWEC Encryption Policy to determine whether the policy is: - Approved by senior management; - Reviewed on a regular, predefined basis; and, - Defines approved encryption and cryptography standards used on iVote systems.	To be tested during and post-election.
7.02	Cryptographic key management life cycle is documented and includes: - Key generation - Storage, distribution and installation - Key usage and rotation - Backup and recovery - Key revocation and suspension - Secure destruction.	1. Enquire with management to determine whether NSWEC has a defined and documented Encryption Policy in place for the iVote system. 2. Obtain and inspect the NSWEC Encryption Policy to determine if the procedures are defined for the following areas: - Key and certificate generation; - Storage, distribution and installation; - Key usage and rotation; - Backup and recovery; - Key revocation and suspension; and, - Secure destruction.	No exceptions noted.
7.03	A quorum of electoral officers is required for the decryption of votes prior to the end of the election. A private key is shared between members to prevent a single electoral officer from decrypting the votes.	1. Enquire with management to understand how private keys for vote decryption are split between chosen NSWEC members. Further understand storage requirements once the private keys are split. 2. Observe the private key splitting process to determine whether: - The key is split between multiple, appropriate members of the Electoral Commission; and - Pins to card are written down and stored in a tamper-proof envelope which is stored within the Commissioner’s safe. 3. During decryption night, observe if a quorum of members are present to input their portion of the split password.	To be tested during and post-election.

Control Reference	Control Activity	2021 Test Procedures	Results of Tests
7.04	Mechanisms are implemented to ensure integrity of the votes captured from the voter.	1. Enquire with management to understand the encryption mechanism in place to ensure integrity of the votes captured from the voter. 2. Obtain and inspect documented procedures to determine whether a voting receipt is captured in a separate system (assurance). 3. Observe Logic and Accuracy testing to verify: - Receipts are sent to all voters after vote submission; and, - voters can verify their vote with the mobile application.	To be tested during and post-election.
7.05	Scrutineers are invited to the decryption process after the end of the elections and votes are only decrypted after the close of voting.	1. Enquire with management to understand the key decryption process. 2. Obtain and inspect documented procedures to determine whether the decryption process (assembly of election board for the purpose of private key) is conducted only after the end of elections and is only invoked after the end of elections. 3. Obtain and inspect documented procedures to determine whether key stakeholders such as scrutineers are present during the decryption ceremony. 4. Observe the decryption process to determine whether scrutineers are present during the decryption ceremony.	To be tested during and post-election.
7.06	iVote numbers and passwords are not stored in the voting or assurance system.	1. Enquire with management to understand the functionality and purpose of the voting and assurance system. Further understand how iVote numbers and passwords are stored. 2. Obtain and inspect evidence to confirm that iVote numbers and passwords are not stored in the voting or assurance system.	No exceptions noted.

Control Reference	Control Activity	2021 Test Procedures	Results of Tests
7.07	End-to-end encryption is implemented to ensure the integrity of the voting process from the system where the vote is cast through to the voting database where the vote is stored.	1. Enquire with management to determine whether NSWEC has a defined and documented Encryption Policy in place for the iVote system. 2. Obtain and inspect the NSWEC Encryption Policy to determine whether the policy defines the end-to-end encryption used to protect voter information and voter preferences. 3. Obtain and inspect evidence of end to end encryption to protect voter information and preferences to determine if voter information and voter preferences are securely transmitted to the voting system. 4. Obtain and inspect configuration screenshots to determine that voter information/voter preference is not transmitted in cleartext inside the NSWEC environment after SSL offload.	No exceptions noted.
7.08	Backups are protected using encryption and are stored in an offsite location.	1. Enquire with management to determine whether NSWEC has a defined and documented Encryption Policy in place for the iVote system backups. 2. Obtain and inspect the NSWEC Encryption Policy to determine whether the policy defines how backups of relevant iVote systems is encrypted and stored. 3. Obtain and inspect vendor reports for Secure Logic, Secure Agility and AC3 to determine if NSWEC actively monitors that backups are performed, encrypted and are stored in an offsite location for the: - Registration system; - Voting system components; - Assurance system; and, - Offline systems.	To be tested during and post-election.
7.09	An encryption mechanism is implemented in the verification system to ensure that voters can decrypt and read only their vote.	1. Enquire with management to determine whether decryption mechanisms are implemented in the verification system to ensure that voters can decrypt and read only their unique vote. 2. Observe and re-perform on-screen to determine whether an encryption mechanism has been implemented in the verification system to ensure that the voter can decrypt and read only their unique vote (i.e. one vote at a time).	To be tested during and post-election.

CONTROL OBJECTIVE 8–
Control Objective: A voter is able to verify that their intention is accurately represented in the vote.

Control Reference	Control Activity	2021 Test Procedures	Results of Tests
8.01 🔍	A voter is able to verify that their vote has been accurately entered into electronic ballot box without any alteration.	1. Enquire with management to understand how a voter can verify that their vote has been accurately entered into electronic ballot box without any alteration. 2. Obtain and inspect NSWEC documentation to determine whether procedures exist for the voter to verify that their vote has been accurately entered into electronic ballot box without any alteration. 3. Perform re-performance of the process to verify that a user's vote has been entered into the electronic ballot box without any alteration.	To be tested during and post-election.
8.02 🔍	A voter is able to verify that their vote has been taken into account for the purpose of deriving results of the election.	1. Enquire with management to understand the process of a voter wanting to verify that their vote has been taken into account for the purpose of deriving results of the election. 2. Obtain and inspect NSWEC documentation to determine if procedures exist for the voter to verify that their vote has been taken into account for the purpose of deriving results of the election. 3. Re-perform the process to verify the user's vote has been taken into account for the purpose of deriving results of the election.	To be tested during and post-election.

CONTROL OBJECTIVE 9–
Control Objective: The voting system ensures votes remain anonymous.

Control Reference	Control Activity	2021 Test Procedures	Results of Tests
9.01	Voter's personal identifiable information (PII) is kept separate from the vote.	1. Enquire with management to understand how personal identifying information (PII) is stored within the iVote system. 2. Obtain and inspect NSWEC documentation to determine whether procedures exist to separate a voter's PII from the vote. 3. Obtain and inspect system configuration documentation to determine whether systems are designed to keep PII separate from the vote. 4. Obtain and inspect a screenshot of the database for a sample of one vote across iVote systems to determine whether PII is stored separately from the vote.	No exceptions noted.
9.02	Procedures are defined to prevent the link between the voter and the voter's preference to be established.	1. Enquire with management to understand the procedures defined to prevent the establishment of a voter and their preference. 2. Obtain and inspect NSWEC documentation to determine whether procedures exist to ensure that before the Ballot Box is decrypted, any metadata that can link that vote to the voter is removed from the vote. 3. Obtain and inspect evidence of daily cleansing during voting period to determine whether prior votes are discarded when a voter re-votes.	No exceptions noted.
9.03	A procedure is defined and executed for a technically competent and independent individual to check proofs of the integrity of the mixing and shuffling of votes and decryption of the votes after the election.	1. Enquire with management to determine whether procedures are defined for an academic to mathematically proof that the mixing and shuffling of votes, and decryption process. 2. Obtain and inspect the check proofs procedure to determine if guidance is provided to check proofs of the integrity of the mixing and shuffling of votes and decryption of the votes after the election. Determine if the procedure is reviewed and approved before proofs are checked. 3. Observe the execution of the procedures to check the proofs of the integrity of the mixing and shuffling of votes and decryption of the votes after the election.	To be tested during and post-election.

CONTROL OBJECTIVE 10–
Control Objective: Personally identifiable information (PII) and privacy of data collected by technology assisted voting is protected.

Control Reference	Control Activity	2021 Test Procedures	Results of Tests
10.01	A Privacy Impact Assessment (PIA) is conducted, capturing a data inventory of all PI data elements (in any form, whether electronic or paper) and their locations across applications, systems, processes, media and data repositories. The PIA also captures the purpose of the data collected and retention period.	1. Enquire with management to determine whether management has conducted a Privacy Impact Assessment (PIA) for the iVote process to capture a data inventory of all PII data elements (in any form, whether electronic or paper) and their locations across applications, systems, processes, media and data repositories. Further understand if the PIA conducted also captures purpose of data collected as well as the retention period. 2. Obtain and inspect the PIA to determine that the following has been captured: - Information required during registration; - Information implicitly and explicitly captured from voters during voting process; - Information implicitly and explicitly captured from voters during verification process; - Purpose of collection and processing each data attribute; and, - Retention period.	No exceptions noted.
10.02	The voter must be made aware of the information collected from them during all phases of election (registration to results).	1. Enquire with management to determine how voters are made aware of the information collected from them during all phases of the election (registration to results). 2. Obtain and inspect the NSWEC Privacy Policy to determine whether it outlines the information collected from the voter during all phases of election (registration to results) and that it is made available to voters. 3. Observe onscreen the privacy notice that is displayed to the voter during the registration process to results and determine if the notice provides information to voters on what personal information and the purpose for which their personal information is being collected, processed, and time period for which it is retained.	**The following deviation was noted:** • Notice of PII retention was not explicitly highlighted for the following iVote stages: - Registration: The privacy policy is included as a link in the website footer; however notice of specific PII retention was not explicitly referenced throughout the registration process. - Voting: The voting process references external webpages, however, notice of specific PII retention was not explicitly referenced throughout the voting process.

Control Reference	Control Activity	2021 Test Procedures	Results of Tests
10.03	Technology assisted voting captures only the information described in the Privacy Impact Assessment.	1. Enquire with management to determine whether iVote only captures only the information described in the Privacy Impact Assessment. 2. Obtain and inspect system documentation to determine whether only the following is captured by the iVote system, in line with the PIA: - Information required during registration; - Information captured from voters during voting process; and, - Information captured from voters during verification process. 3. Observe voting stages (registration, voting and verification) onscreen to confirm that only the following information is captured in line with PIA: - Information required during registration; - Information captured from voters during voting process; and, - Information captured from voters during verification process.	No exceptions noted.
10.04	After the completion of elections, voter identifiable information or voter metadata that is related to elections is securely deleted from the systems, storage systems as well as the backup systems.	1. Enquire with management to determine how, after the completion of elections, voter identifiable information or voter metadata that is related to elections is securely deleted from the systems, storage systems as well as the backup systems. 2. Obtain and inspect NSWEC documentation and observe in-person for a prior election to determine whether procedures are defined and implemented to: - Ensure that the voter information from all the system components of iVote (including storage systems and backup systems) is securely deleted after the elections; - Ensure that voter information from backup tapes is securely deleted after the elections.	To be tested during and post-election.

Control Reference	Control Activity	2021 Test Procedures	Results of Tests
10.05	Only required voter identifiable information data is collected by the technology assisted voting system during and after elections to conduct the election.	1. Enquire with management to understand how the usage of voter identifiable information data collected by iVote during and after elections was limited in line with the PIA. 2. Obtain and inspect NSWEC documentation to determine whether: - Voter information on production instances of iVote was not used in development and test environment; and, - Only information required to conduct the election was collected by the iVote system.	No exceptions noted.
10.06	Access to voter's data is restricted to authorised individuals at NSWEC only. Furthermore, no component of technology assisted voting is deployed on offshore locations (outside Australia)	1. Enquire with management to determine whether access to voter's data is restricted to authorised individuals at NSWEC only and that all components of iVote are deployed onshore in Australia. 2. Obtain and inspect NSWEC documentation to determine whether processes are defined to ensure that access to voter's data at NSWEC is restricted to limited number of authorised individuals. 3. Obtain and inspect a list of all infrastructure for the iVote systems (including backup systems) to determine whether all components of iVote (registration, voting and assurance) are deployed onshore in Australia.	To be tested during and post-election.

CONTROL OBJECTIVE 11–
Control Objective: Open standards are used to enable various technical components or services to inter-operate.

Control Reference	Control Activity	2021 Test Procedures	Results of Tests
11.01	Standard data exchange and data formats are used in the voting and assurance system and avoid the use of proprietary frameworks.	1. Enquire with management to understand standard data exchange and data formats used in the voting and assurance systems. Further understand if there is use of any proprietary frameworks. 2. Obtain and inspect NSWEC documentation/technical specifications to determine whether data exchange formats used in the registration, voting and assurance systems are using standard protocols.	No exceptions noted.
11.02	Standard publicly available encryption algorithms are used and use of proprietary algorithms is avoided.	1. Enquire with management to understand how publicly available encryption algorithms are used. Further understand if there is use of any proprietary encryption algorithms as well as if this has been defined in NSWEC documentation. 2. Obtain and inspect NSWEC documentation to determine whether iVote uses publicly available encryption algorithms.	No exceptions noted.

CONTROL OBJECTIVE 12–
Control Objective: Procedures are implemented for the management and handling of removable media during the election process.

Control Reference	Control Activity	2021 Test Procedures	Results of Tests
12.01	The usage of removable media for elections during the lockdown is documented and restricted.	1. Enquire with management to understand how usage of removable media for elections during the lockdown is documented and restricted. 2. During the election, observe whether the following information was documented and followed: - Type of removable media; - Step in the election process and task for which the removable media was used; - System which were used to transfer information using the device; - Controls implemented to protect sensitive information on removable media; - Name/type of the systems between which information was to be shared using USB/removable media; - Impact on the voting process if the removable media was to be lost/misplaced/stolen; and, - That appropriate removable device has been whitelisted. 3. Obtain and inspect evidence of an Impact Assessment on an election scenario whereby removable media is lost, misplaced and/or stolen.	To be tested during and post-election.

CONTROL OBJECTIVE 13–
Control Objective: Controls are implemented to ensure that only validated personnel are given access to technology assisted voting.

Control Reference	Control Activity	2021 Test Procedures	Results of Tests
13.01	NSWEC perform the relevant background verification checks for employees and contractors of NSWEC who handle technology assisted voting design, architecture, code and access the production environment. As part of their contractual obligation, employees and contractors of NSWEC agree and sign the terms and conditions of their employment contract, which state their and the organisation's responsibilities for information security.	1. Enquire with management to understand how relevant background verification checks for employees and contractors of NSWEC, who handle iVote design, architecture, code and access the production environment are conducted. 2. Obtain and inspect a list of to determine the total number of users that have worked on the iVote system. 3. For a sample of employees and contractors in the following roles, verify the background check documents and verify the Non-Disclosure agreements are signed: - Design and architecture; - Execution/Code; - Testing; - Deployment and maintenance; and, - Security.	To be tested during and post-election.
13.02	Requirements for background verification and contractual obligation are communicated to all third parties who have access to the production environments of technology assisted voting for implementation.	1. Enquire with management to determine whether requirements for background verification and contractual obligations for all third party staff who have access to iVote environments has been communicated to vendors. 2. Obtain and inspect evidence of NSWEC requirements for third party vendors of the requirements for background checks. 3. For each third party with access to the production environment, obtain and inspect NSWEC documentation to determine whether requirements for a background check and contractual obligations are monitored.	To be tested during and post-election.

Control Reference	Control Activity	2021 Test Procedures	Results of Tests
13.03	All employees of the organisation and, where relevant, external party users shall receive security awareness programme, education and training and regular updates in organisational policies and procedures, as relevant for their job function.	1. Enquire with management to determine whether all employees of the organisation and, where relevant, external party users receive awareness programme, education and training and regular updates in NSWEC policies and procedures, as relevant for their job function. 2. Obtain and inspect a list of employees and external party users that are required to undergo regular awareness programs. Compare this with the list of users with access to the iVote systems to ensure appropriate coverage. 3. For the sample selected, determine if the users have received awareness program and training. 4. Obtain and inspect evidence of email requests/reminders sent to employees to notify them that outstanding training is to be completed. 5. Obtain and inspect evidence to ensure where major policy changes are made, employees are notified of revisions via email or other communication channels.	To be tested during and post-election.
13.04	Roles and responsibilities are documented and communicated to members of the election and admin boards.	1. Enquire with management to understand how members of the election and admin boards are selected. Further understand the definition and communication of respective roles and responsibilities to these members. 2. Observe the initiation ceremony to determine: - Processes of creation of election and admin board; and, - Delegation of roles and responsibilities to election and admin board members.	To be tested during and post-election.

Control Reference	Control Activity	2021 Test Procedures	Results of Tests
13.05	NSWEC has formal agreements with all third parties including statements of responsibilities such as; - compliance to all applicable regulatory requirements; - adherence to NSWEC's policies and procedures, including the protection of voter's information.	1. Enquire with management to determine whether NSWEC has formal agreements with all third parties including statements of responsibilities. 2. Obtain and inspect a list of third parties to determine the total number of vendors involved in the operation of the iVote System. 3. Where applicable, obtain security certifications for all vendors (including IS27001 and IRAP reporting). 4. For all vendors, obtain and inspect contracts to determine if the following is monitored: - Compliance to all applicable regulatory requirements; and, - Adherence to NSWEC’s policies and procedures, including the protection of voter’s information (via Non-Disclosure Agreement clauses or other).	To be tested during and post-election.

CONTROL OBJECTIVE 14–
Control Objective: Before an election, the electoral management body will satisfy itself that technology assisted voting operates correctly.

Control Reference	Control Activity	2021 Test Procedures	Results of Tests
14.01	Detailed testing including user acceptance testing (UAT) and Production Readiness Testing (PRT) is performed before deployment of technology assisted voting platforms in production.	1. Enquire with management to understand the change management process, including any relevant testing that is required to be completed prior to migrating changes to a production instance of iVote. 2. For a sample of testing performed, obtain and inspect evidence of UAT and PRT testing across all iVote platforms (registration, voting and assurance) and determine if test cases and results were reviewed and approved by appropriate management before deployment.	To be tested during and post-election.
14.02	Logic & Accuracy (L&A) testing is conducted to confirm the iVote system functions in line with requirements.	1. Enquire with management to understand the requirements for Logic and Accuracy testing (including timelines). 2. Observe Logic and Accuracy testing and inspect supporting documentation to determine whether: - Test votes cast in accordance with the approved procedures were accurately reflected in the corresponding test ballot papers produced; and, - All voting devices are included in L&A testing.	To be tested during and post-election.

CONTROL OBJECTIVE 15–
Control Objective: Access control is managed and monitored appropriately based on the principle of need to know and need to use.

Control Reference	Control Activity	2021 Test Procedures	Results of Tests
15.01	An access control policy based on the principle of need to know and need to use is documented.	1. Enquire with management to determine whether NSWEC has a defined and documented Access Control Policy in place for the iVote system. 2. Obtain and inspect NSWEC Access Control Policy to determine whether the policy is: - Approved by senior management; - Reviewed on a regular, predefined basis; - Covers access management requirements for user (regular users and privileged users) of iVote systems (including offline systems) and networking/security devices; - Covers access management requirements for suppliers/contractors; and, - Defines the requirement for two factor authentication for privileged access to key iVote components. 3. Obtain and inspect screenshot of intranet or equivalent to determine if policy is communicated to all relevant stakeholders including key subcontractors. 4. Obtain and inspect evidence of policy/procedure acknowledgment, on starting and periodically during employment.	To be tested during and post-election.
15.02	A password policy aligned to the criticality of technology assisted voting is defined and implemented.	1. Enquire with management to determine whether NSWEC has a defined and documented Password Policy in place for the iVote system. 2. Obtain and inspect NSWEC Password Policy to determine if the Password Policy is: - Approved by senior management; - Reviewed on a regular, predefined basis; and, - Mandates the password requirements for all iVote systems. 3. Obtain and inspect screenshot of intranet or equivalent to determine if policy is communicated to all relevant stakeholders including key subcontractors. 4. Obtain and inspect password configuration for all components of iVote system to determine whether each meets the required guidelines as defined in the Password Policy and is in line with industry practices.	To be tested during and post-election.

Control Reference	Control Activity	2021 Test Procedures	Results of Tests
15.03	During lockdown, a list of approved users to be enabled is documented, to ensure that only approved system accounts remain enabled.	1. Enquire with management to understand what user accounts are to be kept enabled during lockdown. 2. Obtain and inspect a list of enabled users during lockdown to determine whether only approved system accounts remain enabled.	To be tested during and post-election.
15.04	Principle of least privilege is adopted and access permissions/privileges are granted based on the need-to-know principle and after receiving proper approval at NSWEC.	1. Enquire with management to determine whether the principle of least privilege is in place and access permissions/privileges are only granted based on the need-to-know principle and after receiving proper approval at NSWEC in line with the access control policy. 2. Obtain and inspect a list of user-IDs in the iVote system prior to the lockdown period (registration, voting and assurance). 3. For a sample of users created in the audit period, inspect evidence of approvals to determine whether approval was granted by authorised NSWEC staff and that the access provisioned matches the access approved.	To be tested during and post-election.
15.05	Users that no longer require physical and/or logical access are removed from systems in a timely manner.	1. Enquire with management to determine whether users that no longer require physical and/or logical access are removed from systems in a timely manner. 2. Obtain and inspect a HR list of employees offboarded from NSWEC. 3. For a sample of offboarded users, obtain and inspect evidence to determine whether: - Physical access components (keys, swipe passes, hard-tokens, etc) were returned to NSWEC where applicable; and, - Logical access to all iVote systems was removed on the individual's last day by performing comparing between active iVote staff user listing and HR leaver listing to determine if former iVote staff maintained access post-termination. 4. Obtain and inspect evidence of monitoring of third party terminations to ensure access to key iVote services are restricted to current staff only.	To be tested during and post-election.

Control Reference	Control Activity	2021 Test Procedures	Results of Tests
15.06	User access is reviewed on a periodic basis to determine whether access is still required and commensurate with the job responsibilities for each user. All identified access changes are corrected as a final step in the review process.	1. Enquire with management to understand the frequency and process of user access reviews for all iVote systems and to determine whether all identified access changes are actioned as a final step in the review process. 2. Obtain and inspect latest user access review for all iVote systems to determine whether a user access review was performed and that all identified access changes were actioned. 3. Obtain and inspect evidence to show that third party access is reviewed and any inappropriate access corrected.	To be tested during and post-election.

CONTROL OBJECTIVE 16–
Control Objective: Development, implementation, and changes to new & existing systems, applications and software are documented, authorised, tested and approved.

Control Reference	Control Activity	2021 Test Procedures	Results of Tests
16.01	Change control procedures are followed for all changes to the production environment.	1. Enquire with management to understand the change management process. 2. Obtain and inspect a list of changes to any component of the iVote production environment (registration, voting and assurance) to determine the total number of changes made. 3. For a sample of changes, inspect evidence to determine whether: - Changes follow the change management process; - Changes are initially approved by management to be developed; - Changes were tested; and, - Changes are approved by management before deployment to production environments.	To be tested during and post-election.

Control Reference	Control Activity	2021 Test Procedures	Results of Tests
16.02	Ensure that a formal process to conduct emergency changes in production is implemented and approved.	1. Enquire with management to determine whether NSWEC has a defined and documented process around emergency changes to the production environment. 2. Obtain and inspect the policy/process to determine whether it: - Is approved by senior management; - Is reviewed on a regular, predefined basis; - Defines emergency change procedures; and, - Defines roles and responsibilities of NSWEC staff able to approve of emergency changes. 3. Obtain and inspect screenshot of intranet or equivalent to determine if policy is communicated to all relevant stakeholders including key subcontractors. 4. Obtain and inspect a list of emergency changes to any component of the iVote production environment (registration, voting and assurance) to determine the total number of emergency changes made. 5. For a sample of emergency changes, inspect evidence to determine whether: - Details of the emergency change; - The change followed the documented process; - Emergency change was approved.	To be tested during and post-election.
16.03	Development, testing and production environment are logically separated.	1. Obtain and inspect evidence to confirm whether the development, testing and production environments are logically segregated.	No exceptions noted.
16.04	Formal software development life cycle management includes maintenance of source code repositories per production environment.	1. Enquire with management to determine whether formal software development life cycle management includes maintenance of source code repositories per production environment. 2. Obtain and inspect the source repositories for production environments (through separation of source code or any other mechanism). Confirm access to source code repositories is appropriately restricted and source code maintenance is controlled.	To be tested during and post-election.

CONTROL OBJECTIVE 17–
Control Objective: Secure development practices, testing, and operating environments are used to ensure the integrity of iVote System.

Control Reference	Control Activity	2021 Test Procedures	Results of Tests
17.01	Developers are trained on secure development practices.	1. Enquire with management to determine whether developers are trained on secure development practices. 2. Obtain and inspect documentation procedures to determine whether it includes the requirements and the processes for developers to be trained on secure development practices. 3. Obtain and inspect a list of developers who have worked on the iVote system to determine the total number of developers involved in the iVote system. 4. For a sample of developers, obtain and inspect evidence to determine developer has conducted training and awareness programs on secure development practices.	To be tested during and post-election.
17.02	Security testing and mitigation is performed for all components of technology assisted voting in production environments prior to go-live.	1. Enquire with management to determine whether security testing and mitigation is performed for all components of iVote in a non-production environment prior to go-live. 2. Obtain and inspect evidence to determine whether all components of iVote systems underwent a security assessment to identify and mitigate vulnerabilities (i.e. OWASP Top 10). 3. Obtain and inspect evidence of penetration testing to determine if security testing has been performed for all components of iVote prior to go-live. 4. Where applicable, obtain and inspect evidence to determine vulnerabilities identified by the security assessment or penetration tests are formally documented and tracked to resolution.	To be tested during and post-election.
17.03	Security testing and mitigation is performed for all infrastructure components of the technology assisted voting platform prior to go-live.	1. Enquire with management to determine whether security testing and mitigation is performed for all infrastructure components of the iVote platform prior to go-live. 2. Obtain and inspect evidence to determine whether a security assessment was performed on all components of the iVote systems prior to go-live to identify infrastructure vulnerabilities and missing patches. 3. Where applicable, obtain and inspect evidence of remediation for security deficiencies to determine whether remediation was performed through configuration changes/patch management procedures.	To be tested during and post-election.

Control Reference	Control Activity	2021 Test Procedures	Results of Tests
17.04	The build/deploy of the system in production is validated.	1. Enquire with management to determine whether build/deployment of the system in production is validated prior to deployment. 2. Obtain and inspect evidence to determine whether all components of iVote (registration, voting and assurance): - Have had the signature of the application build verified to ensure application has not been tampered with; and, - Were deployed from a template in a baseline configuration (golden image).	To be tested during and post-election.
17.05	NSWEC provide mechanisms for review and evaluation of the source code for sensitive parts of the technology assisted voting system.	1. Enquire with management to determine the mechanisms for review and evaluation of source code for sensitive parts of the iVote systems. 2. Obtain and inspect evidence of mechanisms for review and evaluation of source code for sensitive parts of the iVote systems to determine whether: - Specified staff are able to review source code; and, - The public are able to review source code.	To be tested during and post-election.
17.06	Scrutineers are invited to review and observe select iVote processes in accordance with Section 158 of the Electoral Act 2017.	1. Enquire with management to understand how scrutineers are involved in the review of select iVote processes in accordance with Section 158 of the Electoral Act 2017. 2. Observe if NSWEC have made it public for scrutineers to apply to observe specific parts of the election process during the preparation or throughout the voting period.	To be tested during and post-election.

CONTROL OBJECTIVE 18–
Control Objective: A mechanism to protect against malware is implemented and operating.

Control Reference	Control Activity	2021 Test Procedures	Results of Tests
18.01	Antivirus/anti-malware scanning agents are installed on all components of technology assisted voting platforms (both servers and workstations). The signatures are updated on a regular basis and anti-malware is configured to perform regular scans and quarantine upon detection.	1. Enquire with management to determine whether antivirus/anti-malware scanning agents are installed on all components of the iVote platforms (both servers and workstations), that signatures are updated on a regular basis and that anti-malware is configured to perform regular scans and quarantine upon detection. 2. Obtain and inspect evidence of antivirus/anti-malware scanning agents reporting to determine whether: - All components of the iVote platforms (both servers and workstations) are covered; - Virus signatures are scheduled to be updated on a regular basis; and, - Anti-malware is configured to perform regular scans and quarantine threats upon detection.	To be tested during and post-election.

CONTROL OBJECTIVE 19–
Control Objective: Detection and monitoring capabilities have been implemented to detect unauthorised activities.

Control Reference	Control Activity	2021 Test Procedures	Results of Tests
19.01	A log management system (LMS) is implemented for logging of security events.	1. Enquire with management to determine whether a log management system (LMS) is implemented for logging of security events. 2. Obtain and inspect evidence of the LMS to determine whether LMS has been implemented for logging of security events. 3. If not managed by SIEM, obtain and inspect LMS reporting to determine if all web and IVR components of the iVote registration system, voting system and assurance systems are integrated into the LMS.	To be tested during and post-election.
19.02	Log files are immutable for vote casting and cannot be overwritten.	1. Enquire with management to determine how log files are immutable and cannot be overwritten. 2. Obtain and inspect NSWEC documentation to determine whether log files that are required to be immutable are defined. 3. Obtain and inspect LMS configuration to determine whether logs are stored outside the system which generated them. 4. Obtain and inspect a list of log files to determine the total number of logs. 5. For a sample of log files, obtain and inspect evidence to determine the chain of selected log files to ensure that all signatures are valid and that none are missing.	To be tested during and post-election.

Control Reference	Control Activity	2021 Test Procedures	Results of Tests
19.03 ✓	A Security incident and event management (SIEM) is implemented for real time monitoring of events and management of security incidents.	1. Enquire with management to determine whether a SIEM tool is implemented on all components of the iVote system. Further understand how often the SIEM tool is monitored to manage security incidents as they arise. 2. Obtain and inspected documented requirements to determine if SIEM requirements (including what is logged, what events are captured, determining criteria for incidents etc) have been formally defined. 3. Obtain and inspect the configuration of the SIEM tool to determine whether: - SIEM covers all components of iVote system (registration, voting, and assurance systems); - Log sources are integrated with SIEM (e.g. Firewall logs, WAF, access control logs, IDS/IPS, FIM, application level authentication logs, Bridge laptop etc); - Rules are created for identification of events and incidents; and, - All events identified on the web application firewall during lockdown period is logged on SIEM. 4. Obtain and inspect Security Operations Centre reporting to confirm whether the SOC has access to the anti-malware dashboard and are actively monitoring the anti-malware status of the system. 5. Obtain and inspect a list of log files on offline machines to determine the frequency and total number of logs generated on offline machines. 6. For a sample of log files, obtain and inspect logs to confirm: - Detection and monitoring capability is implemented on offline systems as these are not integrated with the SIEM; and, - Logs for offline systems are approved by management to confirm no inappropriate access has been made.	To be tested during and post-election.

Control Reference	Control Activity	2021 Test Procedures	Results of Tests
19.04	Security events logged into the log management and security incident management system must capture the key events and detailed description in the logs.	1. Enquire with management to determine whether audit logging is enabled to capture key events and detailed descriptions of the logs. Further determine if logs are fed through the SIEM tool for analysis. 2. Obtain and inspect a list of security events logged and integrated with the SIEM to determine total number of security incidents. 3. For a sample of logs, obtain and inspect a sample log information from iVote (registration, voting and assurance system) and validate if: - The security events logged into log management and security incident management system contained key information about authentication, authorisation, modification and retrieval of data, network communications, and administrative functions; and, - Logs included information such as timestamp, host details (host name, IP address), identity of the process initiating the event, and a detailed description of the event.	To be tested during and post-election.
19.05	Sensitive information related to voter and votes should not be captured in the logs.	1. Enquire with management to confirm that sensitive information related to voter and votes are not captured in logs. 2. Obtain and inspect a list of log files from the various production systems (registration, voting and assurance systems) to determine the total number of logs 3. For a sample of log files, perform inspection to determine whether logs captured any sensitive voter or voting information (e.g. voter name or PII, voter id, password, voter preference).	To be tested during and post-election.
19.06	All technology assisted voting components is synced with a network time protocol to ensure integrity of logs.	1. Enquire with management to confirm if all technology assisted voting components are synced with a network time protocol to ensure integrity of logs. 2. Obtain and inspect a screenshot of time configuration to determine if all technology assisted voting components are synced with a network time protocol.	To be tested during and post-election.

CONTROL OBJECTIVE 20–
Control Objective: A procedure is established to identify vulnerabilities and regularly install updated versions and corrections of all relevant software.

Control Reference	Control Activity	2021 Test Procedures	Results of Tests
20.01	All the assets utilised in the voting system are identified and an inventory is maintained with relevant details, and is reviewed on a regular basis.	1. Enquire with management to determine whether an inventory of all assets used in the voting system is maintained and reviewed on a periodic basis. 2. Obtain and inspect the asset listing to determine if assets are: - Identified and logged such as asset name, serial or license number, asset owner, asset guardian or custodian, and information classification of data held/processed; and, - All accounted for and no assets are missing. 3. For a sample of assets, obtain and inspect evidence of review to determine whether assets are reviewed periodically.	To be tested during and post-election.
20.02	Vulnerability security assessments are performed to identify vulnerabilities in software and hardware.	1. Enquire with management to determine whether security assessments are performed to identify vulnerabilities in both software and hardware assets on a periodic basis. 2. Obtain and inspect the asset listing to determine all physical and virtual assets used in the iVote system are subject to vulnerability assessments. 3. For a sample of assets, obtain and inspect evidence of vulnerability security assessment to determine if a security assessment has been performed to identify infrastructure vulnerabilities and missing patches. 4. Where applicable, inspect evidence to determine whether remediation was performed to resolve vulnerabilities.	To be tested during and post-election.

Control Reference	Control Activity	2021 Test Procedures	Results of Tests
20.03	The patch management policy is implemented to ensure that all known vulnerabilities are patched.	1. Enquire with management to determine whether NSWEC has a defined and documented Patch Management Policy in place for the iVote system. 2. Obtain and inspect NSWEC Patch Management policy to determine whether the policy is: - Approved by senior management; - Reviewed on a regular, predefined basis; and, - A requirement for known vulnerabilities to be patched is defined and documented. 3. Obtain and inspect vendor reporting or other evidence for all components of iVote (Registration, Voting, Assurance) to determine if NSWEC actively monitors the review and release of patches by third party vendors in line with NSWEC's Patch Management policy.	To be tested during and post-election.
20.04	A mechanism is implemented to ensure only required software is installed on technology assisted voting components.	1. Enquire with management to determine whether a golden source (OS Image) with minimal configuration was used and deployed to all components of the voting system. Further understand how additional packages are deployed and the process for release (including any necessary approvals). 2. Observe onscreen/on-site to determine whether a golden source image is deployed as a baseline to iVote components and that required packages were added after the deployment as required.	To be tested during and post-election.

Control Reference	Control Activity	2021 Test Procedures	Results of Tests
20.05	All updates and patches are reviewed and tested in non-production environments before deployment into the production.	1. Enquire with management to determine how patches are released to the production environment. Further understand: - Where emergency patching is required, the process for approving and deploying changes to the production environment of the iVote system; and, - If a patch release process is documented. 2. Obtain and inspect NSWEC Patch Management policy to determine whether the policy provides governance around patch management processes. 3. Obtain and inspect vendor reporting or other evidence for all components of iVote (Registration, Voting, Assurance) to determine if NSWEC actively monitors the review and release of patches by third party vendors. -	To be tested during and post-election.
20.06	A mechanism is in place to securely deploy updates/patches/config changes during a locked down state.	1. Enquire with management to understand mechanisms in place to securely deploy updates/patches/config changes during a locked down state. 2. Obtain and inspect the NSWEC Patch Management policy to determine whether the policy defines the process for deploying updates/patches/config changes during a locked down state. 3. Obtain and inspect a list of changes made during lock down to determine total number of changes during locked state. 4. For a sample of changes, confirm that: - Changes were conducted in accordance with the Patch Management Policy; and, - Change has been tested and approved for release by appropriate management.	To be tested during and post-election.

Control Reference	Control Activity	2021 Test Procedures	Results of Tests
20.07	Patch update/config correction mechanisms are disabled where required during lockdown of the system.	1. Enquire with management to determine which patch update/config correction mechanisms are disabled where required during lockdown of the system. 2. Obtain and inspect the NSWEC Patch Management policy to determine whether the policy ensures that mechanisms to disable patch update / config correction mechanisms during lockdown of system are documented. 3. Obtain and inspect a list of services/tools to determine the total number of services/tools that require to continue to receive patch updates throughout the election period. 4. For a sample of services requiring to be patched during lockdown, perform inspection to determine whether: - Service has been approved to continue receiving patching during lockdown; and, - Service continues to receive updates during lockdown. 5. Obtain and inspect evidence to indicate all devices (excluding devices that have been approved to remain enabled) have been disabled in accordance with the NSWEC Patch Management policy.	To be tested during and post-election.
20.08	A mechanism is implemented to ensure that latest mobile app/application is used by the voters.	1. Enquire with management to determine how voters are required to install the latest mobile application to verify their submitted vote has been correctly recorded in the iVote System. 2. Obtain and inspect configuration of the iVote mobile application to determine whether voters must have the latest mobile application to verify their submitted vote.	To be tested during and post-election.

CONTROL OBJECTIVE 21–
Control Objective: Technology assisted voting systems’ networks are managed, controlled and segmented to protect information in systems and applications.

Control Reference	Control Activity	2021 Test Procedures	Results of Tests
21.01	Network security policy and procedures are developed and documented to define the controls required for the protection of the voting systems and the voter's information.	1. Enquire with management to determine whether NSWEC has a defined and documented Network Security Policy in place for the iVote system. 2. Obtain and inspect NSWEC Network Security policy to determine whether the policy: - Is approved by senior management; - Is reviewed on a regular, predefined basis; and, - Defines policies and processes to govern the protection of confidential information related to the voting system, detailing network security tools (WAF, Firewalls, NIDS/HIPS, DDoS protection) where applicable. 3. Obtain and inspect screenshot of intranet or equivalent to determine if policy is communicated to all relevant stakeholders including key subcontractors.	No exceptions noted.
21.02	The network hosting technology assisted voting is segregated based on the defined security model to achieve defence in depth.	1. Enquire with management to determine whether the network hosting iVote is segregated based on the defined security model to achieve defence in depth. 2. Obtain and inspect network architecture documentation to determine whether networks hosting the registration, voting and assurance systems are logically segregated in line with NSWEC’s Security Model. 3. Obtain and inspect evidence to determine whether databases are hosted in a secure network zone which is not accessible from untrusted environments.	No exceptions noted.

Control Reference	Control Activity	2021 Test Procedures	Results of Tests
21.03 ✓	Perimeter security controls are defined and implemented to protect technology assisted voting.	1. Enquire with management to determine how perimeter security controls are enforced for the 3 environments of iVote. Further determine the ownership of these controls, as well as any third party monitoring requirements where applicable. 2. Obtain and inspect NSWEC documentation to determine whether an application layer security system such as web application firewall is implemented to protect the voting system from layer 7 attacks (OWASP top 10). 3. Obtain and inspect NSWEC documentation to determine whether a web application firewall is configured to detect and respond to application layer attacks such as SQL Injection, flooding, etc. 3. Obtain and inspect vendor reports for Secure Logic, Secure Agility and AC3 to determine if NSWEC actively monitors the implementation of perimeter security controls.	To be tested during and post-election.
21.04 ✓	Network based Intrusion detection or prevention system are implemented for technology assisted voting.	1. Enquire with management to determine whether intrusion detection and prevention systems are implemented for iVote components. 2. Obtain and inspect the network architecture to determine whether IDS/IPS is implemented. 3. Where applicable, obtain and inspect evidence to determine if IDS/IPS alerts were integrated with the SIEM Platform. 4. Where applicable, obtain and inspect a sample of alerts from the SIEM raised by IDS/IPS to determine if IDS/IPS is capable of raising automatic alerts within the SIEM. 5. Where applicable, obtain and inspect a sample of resolutions where automatic alerts have been raised within the SIEM.	To be tested during and post-election.

Control Reference	Control Activity	2021 Test Procedures	Results of Tests
21.05	Network security controls are tested through a combination of system reviews and red team exercises.	1. Enquire with management to understand how testing of security controls is conducted, as well as frequency and scope of testing. 2. Obtain and inspect evidence of latest security incident response testing to determine: - If security incident response testing produces reports/performance of red team exercises prior to go-live; and, - Security incident response testing covers all the key components of the iVote platform (registration, voting and assurance systems). 3. Where applicable, obtain and inspect documentation to determine security issues identified in the system reviews / exercises are tracked to resolution.	To be tested during and post-election.
21.06	All network security applications and tools (Firewalls/WAF/Load Balancer/Application Servers/Web Servers etc.) have management (administrator) console restricted only to the management network zone for the respective application and have 2FA enabled.	1. Enquire with management to determine whether all network security applications and tools have the administrator console restricted to appropriate staff. 2. Obtain and inspect vendor reports for Secure Logic, Secure Agility and AC3 to determine if NSWEC actively monitors the effective operation of vendor access controls to management (administrator) consoles for all network security applications and tools.	To be tested during and post-election.
21.07	Procedures must define the required network controls and configuration changes for system lockdown.	1. Enquire with management to determine whether procedures define the required network controls and configuration changes for system lockdown. 2. Obtain and inspect NSWEC documentation to ensure that a procedure defines the required network controls and configuration changes for system lockdown.	To be tested during and post-election.

Control Reference	Control Activity	2021 Test Procedures	Results of Tests
21.08	All voting systems are protected during the lockdown using host security system.	1. Enquire with management to determine how the key system of iVote is protected during lockdown stages. Furthermore, understand if requirements for protection of iVote systems is documented and communicated to stakeholders. 2. Obtain and inspect NSWEC documentation to confirm if key systems of iVote is protected by Host Security Systems. 3. Obtain and inspect evidence to show that an Intrusion Prevention System and/or an Intrusion Detection System is implemented.	To be tested during and post-election.
21.09	Procedures and controls are implemented to ensure network performance and availability.	1. Enquire with management to determine what procedures and controls are implemented to ensure network performance and availability. 2. Obtain and inspect NSWEC documentation to determine whether consideration for network performance and availability for iVote Systems have been defined, and that identified issues have been resolved.	To be tested during and post-election.
21.10	The network components and traffic of the technology assisted voting systems are segregated.	1. Enquire with management to understand the ownership of network components and traffic of the iVote system. 2. Obtain and inspect evidence to determine whether the registration system, voting system and assurance systems are provided by three separate providers and routed via three separated infrastructure nodes.	To be tested during and post-election.

CONTROL OBJECTIVE 22–
Control Objective: Physical protection and guidelines for secure areas and equipment are designed and applied.

Control Reference	Control Activity	2021 Test Procedures	Results of Tests
22.01	Management has developed a process to define, monitor, and evaluate third-party physical production environment protection requirements across all third party providers.	1. Enquire with management to determine how physical security controls are enforced for office locations holding voting system components. Further understand if physical access to key iVote systems are managed by vendors or NSWEC staff. 2. Where applicable, obtain and inspect security certifications (ISO, IRAP, etc.) to determine whether physical security controls are operating as intended to protect iVote systems. 3. Obtain and inspect evidence of third party service reporting or third party communications to determine if physical security requirements are reported and monitored.	To be tested during and post-election.
22.02	Access to facilities is aligned with Protective Security Policy Framework (PSPF) zones requirements and restricted to approved NSWEC staff.	1. Enquire with management to determine whether access to facilities is aligned with the Protective Security Policy Framework (PSPF) zones or other security requirements. 2. Where applicable, obtain and inspect vendor certification reports (ISO27001, IRAP, SOC2) to determine if NSWEC actively monitors vendor alignment to Protective Security Policy Framework (PSPF) zones requirements. 3. For NSWEC sites holding critical technology assisted voting assets, obtain and inspect evidence to determine whether the following are implemented: - Access control measures at entrances to restrict and record access of employees; - A visitor management process to ensure that visitors and NSWEC staff are required to sign guest logs, display visitor badges and be escorted by authorised staff at all times within the facility; and, For the NSWEC office and data centre used to host the iVote components, a CCTV mechanism is implemented for 24/7 monitoring of entry and exit points to detect and monitor for physical intrusion, and confirm that CCTV logs are maintained for 90 days.	To be tested during and post-election.

Control Reference	Control Activity	2021 Test Procedures	Results of Tests
22.03	Environmental controls are implemented at data centre and office location for protection of technology assisted voting assets.	1. Enquire with management to determine how NSWEC monitors third party implementation of environmental controls at data centres. Further understand if environmental controls are managed by vendors or NSWEC staff. 2. Where applicable, obtain and inspect vendor certification reports (ISO27001, IRAP, SOC2) to determine if NSWEC actively monitors environmental controls implemented operate effectively for vendor-hosted technology assisted voting assets. 3. Obtain and inspect evidence to determine whether the offline system is stored in a Class B safe with multiple access restrictions. 4. For NSWEC sites holding critical technology assisted voting assets, perform onsite observation to determine whether the environmental controls are in place (including but not limited to fire retardant safes, environmental alarms and sensors, and fire extinguishers).	To be tested during and post-election.

CONTROL OBJECTIVE 23–
Control Objective: Procedures and capabilities related to business continuity and resilience are established to operate effectively during a time of an incident.

Control Reference	Control Activity	2021 Test Procedures	Results of Tests
23.01	A business impact analysis is performed to identify critical processes, technology components and key people. Additionally, RTO & RPO of the critical systems is identified.	1. Enquire with management to determine whether a Business Impact Analysis has been conducted for all critical iVote services. 2. Obtain and inspect evidence of Business Impact Analysis for all key iVote systems and services to determine whether it includes: - Business processes/activities/applications/ key staff; - The period of time operations can continue without each of its critical activities (MAO, RTO, RPOs for at least high risk processes); and, - The impact of a disruption over varying periods of time (e.g. legal, reputational, financial, environmental and regulatory) ○ Recovery requirements; and, ○ Internal and external dependencies.	No exceptions noted.

Control Reference	Control Activity	2021 Test Procedures	Results of Tests
23.02	Business continuity procedures and recovery plans are documented, approved and tested.	1. Enquire with management to determine whether business continuity procedures and recovery plans have been developed, reviewed and approved by appropriate management. 2. Obtain and inspect the Disaster Recovery Plan (DRP) to determine whether: - DRP exists; - DRP is reviewed on a periodic basis; - DRP is signed off by Board/Senior Management; - Version Control is established; - Roles and responsibilities of key stakeholders (including the users who are able to invoke/act the DRP) are defined; - DRP has been aligned to the BIA; and, - DRP establishes scope of coverage (applications, software and hardware). - DR testing is performed. 3. Obtain and inspect Business Continuity Plan (BCP) to determine whether: - BCP exists; - BCP is reviewed on a periodic basis; - BCP is signed off by Board/Senior Management; - Version Control is established; - Roles and responsibilities of key stakeholders (including the users who are able to invoke/act the BCP) are defined; and, - BCP establishes scope of coverage (applications, software and hardware). 4. Obtain and inspect Business Continuity Plan (BCP) testing results to determine whether: - BCP has been tested periodically; - BCP is fit for purpose and provides guidance on how to resume operations in the event of disruption; - Staff are adequately aware of responsibilities when enacting the BCP; and, - NSWEC is able to successfully resume operations in the event of a disruption to all key services and systems.	To be tested during and post-election.

Control Reference	Control Activity	2021 Test Procedures	Results of Tests
23.03	Single point of failure of all components of technology assisted voting has been identified and disaster recovery capabilities established.	1. Enquire with management to determine whether NSWEC has implemented a procedure to identify the single point of failure of all components of the voting system and maintain a record for them. 2. Obtain and inspect Single point of failures listing to determine whether: - Single point of failures have been identified; and, - Disaster recovery capabilities for these failures have been established.	To be tested during and post-election.
23.04	Backup of data and systems is performed during system lockdown in accordance with a formalised backup schedule aligned with defined RPO.	1. Enquire with management to determine whether backup of data and systems is performed during system lockdown in accordance with a formalised backup schedule aligned with defined RPO. 2. Obtain and inspect vendor reports for Secure Logic, Secure Agility and AC3 to determine if NSWEC actively monitors the success of system backups during voting (when systems are locked down). Where applicable, NSWEC follows up on the remediation of backup failures.	To be tested during and post-election.
23.05	Disaster Recovery for technology assisted voting is setup and implemented in a separate geo-redundant data centre.	1. Enquire with management to determine whether DR Setup of iVote is implemented in a separate geo-redundant data centre. 2. Obtain and inspect evidence to ensure that Production and DR data centres are geo-redundant.	No exceptions noted.

Control Reference	Control Activity	2021 Test Procedures	Results of Tests
23.06	DR testing and backup recovery is performed prior to go-live to ensure that controls implemented are operating effectively.	1. Enquire with management to obtain the frequency of testing, exercising and validation of the Disaster Recovery Plan (DRP). 2. Obtain and inspect the DRP to determine whether a formal exercise and training program has been established as part of the Disaster Recovery Plan. 3. Obtain evidence of the testing performed on the DRP (including related artefacts) to determine whether: - A consistent notification and escalation process is in place across the organisation (and plans), and this process is widely understood and followed; - A process to communicate Disaster Recovery testing to relevant sites is in place; and, - Disaster recovery processes are documented to provide guidance around procedures required to successfully restore key services and systems in the event of a disaster. - A process has been established for failed Disaster Recovery tests to be re-tested/re-run until the issue has been resolved and the disaster recovery is completed correctly. 4. Enquire with management to determine: - How often backups are scheduled; - How failed backups are rerun; and, - How often backup restorations are tested. 5. Obtain and inspect vendor reports for Secure Logic, Secure Agility and AC3 to determine if NSWEC actively monitors the success of system backups prior to voting (prior to systems being locked down). Where applicable, NSWEC follows up on the remediation of backup failures. 6. Obtain and inspect evidence of vendor engagement or other with Secure Logic, Secure Agility and AC3 to determine successful DR testing using a backup recovery.	To be tested during and post-election.

CONTROL OBJECTIVE 24–
Control Objective: IT and information security incidents are responded to and reported in accordance with documented procedures.

Control Reference	Control Activity	2021 Test Procedures	Results of Tests
24.01	A documented incident management procedure or plan is maintained to identify and manage the following incidents during the election process: 1. Security Incidents. 2. IT Incidents.	1. Enquire with management to determine whether NSWEC has a defined and documented Incident Management Policy in place for the iVote system. 2. Obtain and inspect the NSWEC Incident Management Policy to determine whether it is: - Approved by senior management; - Is communicated to all relevant stakeholders including key subcontractors; - Reviewed on a regular, predefined basis; and, - Defines policies and processes for IT incidents and Security incidents: o Identification and classification as per defined criticality; o Proper escalation procedure is in place to report the incident; o Documented recovery procedure for commonly occurring incidents; and, o Classification criteria for Root Cause Analysis/Problem management process.	To be tested during and post-election.
24.02	Daily Incident record is prepared and reviewed based on the activity monitoring during the system lockdown period.	1. Enquire with management to determine whether a Daily Incident record is prepared based on the activity monitoring during the system lockdown period. 2. For a sample of daily incident records during system lockdown, perform inspection to determine that the following took place: - A ticket was raised for IT/Security incident; - A ticket / report was shared internally for triaging and resolution; and, - The incidents were tracked through to resolution.	To be tested during and post-election.

Control Reference	Control Activity	2021 Test Procedures	Results of Tests
24.03	Simulations and training are conducted prior to the elections to ensure that all involved stakeholders/parties understand their roles and responsibilities.	1. Enquire with management and document the external and internal training programs in place to ensure iVote staff are trained in the management of security incidents. Furthermore, understand how management provides training materials for end-users relating to the identification and escalation of security related incidents. 2. Obtain and inspect screenshots of iVote management security incident training modules and document if the security incident training modules provide coverage of roles and responsibilities for various iVote stakeholders. 3. For a sample of staff, obtain and inspect evidence and determine if: - Security Incident Management training of iVote processes was monitored; and, - Where applicable, outstanding training is escalated in a timely manner. - 4. Obtain and inspect evidence of security incident response simulations to determine if security exercises has been conducted prior to the election.	To be tested during and post-election.
24.04	Post incident analysis for a security or IT incident are conducted and learnings identified and addressed.	1. Enquire with management and determine the requirements for Post Incident Reviews (PIR's) for closed security or incident tickets. 2. Obtain and inspect the NSWEC Incident Management Procedure and determine if the requirement for PIRs for closed incidents is formally defined. 3. Obtain and inspect the listing of all incident tickets within the audit period to determine the total number of incidents. 4. For a sample of relevant incident tickets, perform inspection to determine whether: - A PIR review was conducted; - The PIR is attached the incident ticket; and, - PIR contains lessons identified and root cause analysis where applicable.	To be tested during and post-election.

Control Reference	Control Activity	2021 Test Procedures	Results of Tests
24.05 🔍	Procedures and controls are implemented to ensure application and system performance and availability.	1. Enquire with management and document if procedures and controls are implemented to ensure application and system performance and availability. 2. Obtain and inspect evidence of availability monitoring to determine whether monitoring of system availability and performance is in place. 3. Where applicable, obtain and inspect evidence of: - Alert / monitoring to notify NSWEC of degrading system performance and availability; and, - Tracking and remediation of issues causing degrading system performance and availability.	To be tested during and post-election.

Section V:
Other Information Provided by NSW Electoral Commission

Section V: Other Information Provided by NSW Electoral Commission

The information included in this Section of the report is presented by NSW Electoral Commission to provide additional information on the control deviations noted in the report.

The information included in this Section has not been subjected to the test procedures performed by Deloitte as detailed in Section IV.

Management's response to deviations noted:

Control Reference	Control Activity	Deviation Noted	Management Response
10.02	The voter must be made aware of the information collected from them during all phases of election (registration to results).	• Notice of Personally Identifiable Information (PII) retention was not explicitly highlighted for the following iVote stages: - Registration: The privacy policy is included as a link in the website footer; however notice of specific PII retention was not explicitly referenced throughout the registration process. - Voting: The voting process references external webpages, however, notice of specific PII retention was not explicitly referenced throughout the voting process.	• These minor gaps have been noted and will be addressed after this election.

Liability limited by a scheme approved under Professional Standards Legislation.
Member of Deloitte Asia Pacific Limited and the Deloitte organisation.