

# Deloitte.



## **NSW Electoral Commission**

ASAE3150 assurance report over NSW  
Electoral Commission's iVote system

May 2022

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms, and their related entities (collectively, the “Deloitte organisation”). DTTL (also referred to as “Deloitte Global”) and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see [www.deloitte.com/about](http://www.deloitte.com/about) to learn more.

Deloitte is a leading global provider of audit and assurance, consulting, financial advisory, risk advisory, tax and related services. Our global network of member firms and related entities in more than 150 countries and territories (collectively, the “Deloitte organisation”) serves four out of five Fortune Global 500® companies. Learn how Deloitte’s approximately 312,000 people make an impact that matters at [www.deloitte.com](http://www.deloitte.com).

Deloitte Asia Pacific Limited is a company limited by guarantee and a member firm of DTTL. Members of Deloitte Asia Pacific Limited and their related entities, each of which are separate and independent legal entities, provide services from more than 100 cities across the region, including Auckland, Bangkok, Beijing, Hanoi, Hong Kong, Jakarta, Kuala Lumpur, Manila, Melbourne, Osaka, Seoul, Shanghai, Singapore, Sydney, Taipei and Tokyo.

The Australian partnership of Deloitte Touche Tohmatsu is a member of Deloitte Asia Pacific Limited and the Deloitte organisation. As one of Australia’s leading professional services firms, Deloitte Touche Tohmatsu and its affiliates provide audit, tax, consulting, risk advisory, and financial advisory services through approximately 8000 people across the country. Focused on the creation of value and growth, and known as an employer of choice for innovative human resources programs, we are dedicated to helping our clients and our people excel. For more information, please visit our web site at <https://www2.deloitte.com/au/en.html>.

Liability limited by a scheme approved under Professional Standards Legislation.

Member of Deloitte Asia Pacific Limited and the Deloitte organisation.

© 2022 Deloitte Touche Tohmatsu.

# Table of contents

I.	Executive Summary	4
II.	iVote Vote Journey Map	10
III.	Independent Assurance Practitioner's Reasonable Assurance Report	13
IV.	Overview of the Work Performed	18
V.	Control Objectives, Control Activities, Testing of Design and Implementation and Operating Effectiveness	22
VI.	Other Information Provided by NSW Electoral Commission	84

# Section I: Executive Summary

# Section I: Executive Summary

## Overview

The NSW Electoral Commissioner is a statutory appointee responsible for conducting elections for the Parliament of New South Wales, NSW local government and other organisations as required under NSW legislation. The Electoral Commissioner is also a member of the three-member NSW Electoral Commission, which is mainly responsible for enforcing electoral and lobbying laws and may also support, but not direct, the Electoral Commissioner in the conduct of elections. The Electoral Commissioner and the three-member Electoral Commission are both assisted by staff and contractors employed in or engaged by a public sector agency, also referred to as the NSW Electoral Commission (NSWEC). In this report, "NSWEC" is used to describe all three, as may be appropriate in the context.

The 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.

Following the passage of legislation by the NSW Parliament authorising technology-assisted voting in NSW, the NSWEC introduced a remote electronic voting system, named iVote, in March 2011 to provide technology-assisted voting to eligible electors registered to vote in NSW to simplify and increase the participation in the democratic process. As at October 2021, the iVote system had 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.

As a measure to address risks arising from the COVID-19 pandemic, the NSW Government authorised the use of iVote for the first time at local government elections in the *Local Government (General) Amendment Regulation 2021* on 9 July 2021.

With each implementation, iVote has constantly been refined to improve the iVote experience for electors, as well as providing electors with 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. For the 2021 Local Government elections, electors could vote using iVote if they:

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

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

The registration for the iVote voting channel was made available from 9am on Monday, 22 November, until 1pm on Saturday, 4 December. Voting using iVote was made available from 9am on Monday, 22 November, until 6pm on Saturday, 4 December. A pre-election report was completed by Deloitte and published by NSWEC on the NSW Electoral Commission website prior to the iVote voting channel being made available.

## Purpose

At the request of NSWEC, Deloitte Touche Tohmatsu ('Deloitte') undertook an engagement to provide a reasonable assurance report on the design and operating effectiveness of NSWEC's information technology controls within the iVote system during the Local Government 2021 Elections. Over the course of the election, Deloitte has observed key processes throughout the election lifecycle, summarised below:

#	Date of activity	Observation activities
1	08 November 2021 12:15 PM - 10:00 PM	Lockdown of all iVote environments.
2	08 November 2021 8:00 AM - 10:00 PM	Election build
3	09 November 2021 2:30 PM - 10:00 PM	Voting Environment unlock
4	10 November 2021 9:30 AM - 1:00 PM	Ballot Paper Proofing
5	12 November 2021 10:30 AM - 2:15 PM	Registration/Credential Environment unlock
6	15 November 2021 8:30 AM - 3:00 PM	Logic and Accuracy Testing
7	16 November 2021 8:45 AM - 3:45 PM	Logic and Accuracy Testing
8	18 November 2021 9:00 AM - 12:00 PM	Registration/Credential Environment unlock
9	24 November 2021 5:00 PM - 8:00 PM	Registration/Credential Environment unlock
10	25 November 2021 5:20 PM - 9:50 PM	Voting Environment unlock
11	26 November 2021 12:40 PM - 4:40 PM	Assurance Environment unlock
12	27 November 2021 6:00 PM - 10:00 PM	Voting Environment unlock
13	29 November 2021 12:15 PM - 7:20 PM	Voting and Assurance Environment unlock
14	30 November 2021 6:15 PM - 8:45 PM	Registration/Credential Environment unlock
15	01 December 2021 2:45 PM - 4:45 PM	Voting Environment unlock
16	02 December 2021 4:40 PM - 6:35 PM	Registration/Credential Environment unlock
17	04 December 2021 7:20 AM - 2:30 PM	Voting Environment unlock
18	04 December 2021 7:45 AM - 1:20 PM	Registration/Credential Environment unlock
19	04 December 2021 5:30 PM - 6:55 PM	Registration/Credential Environment unlock
20	04 December 2021 6:00 PM - 10:30 PM	Decryption Ceremony activities
21	05 December 2021 8:00 AM - 3:20 PM	Decryption Ceremony activities
22	07 December 2021 10:00 AM - 8:45 PM	Decryption Ceremony activities
23	08 December 2021 9:00 AM - 3:30 PM	Decryption Ceremony activities
24	08 December 2021 10:15 AM - 12:15 PM	Assurance and Registration/Credential Management lockdown removal
25	10 December 2021 11:00 AM - 4:45 PM	Voting Environment lockdown removal
26	13 December 2021 9:00 AM - 8:30 PM	Independent Monitoring
27	16 December 2021 10:30 AM - 12:00 PM	Decryption Ceremony activities

## Scope

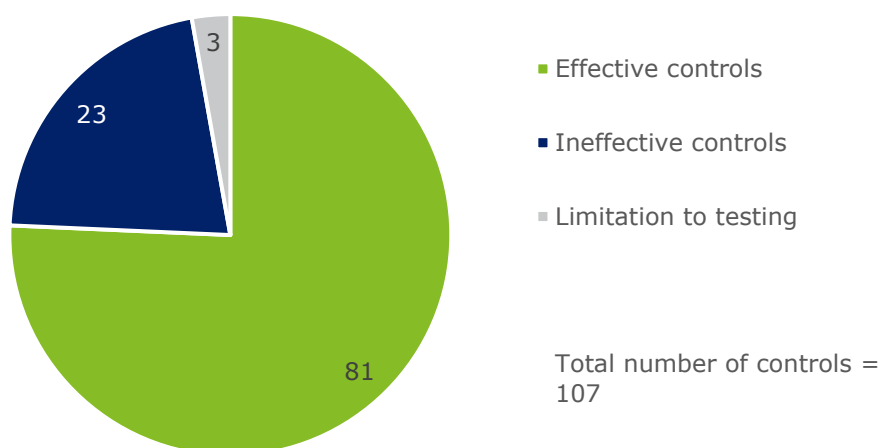
Independent auditing of technology assisted voting is required by Section 156 of the NSW Electoral Act 2017 and by Section 333G of the Local Government (General) Regulation 2021. The NSW Electoral Commissioner has engaged Deloitte as an independent assurance practitioner to assist in independently validating 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). This report summarises the results of the testing of the design and operating effectiveness of the controls within this framework.

## Summary of results

Below is a summary of the report results across the period (8 November 2021 to 23 December 2021). 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 control objectives not met are listed in Section III. The details of the specific controls tested, and the nature, timing and extent of those tests, are listed in Section V.

### iVote Control Framework



Control Objective	# of controls per control objective	# of controls effectively designed and operated	Results	Conclusion (in all material respects)
<b>CO.1</b> - A set of policies for information security shall be defined, reviewed on a periodic basis, published and communicated to all relevant stakeholders operating and managing technology assisted voting.	4	3	Deviation noted, refer to Section V for further detail of deviation and mitigating controls.	Control objective met.
<b>CO.2</b> - A mechanism should be implemented for voters to effectively and accurately use technology assisted voting.	3	3	No deviations noted.	Control objective met.
<b>CO.3</b> - All official voting information shall be presented in an equivalent way, across various voting channels to ensure that voter's intentions are not affected.	4	3	Deviation noted, refer to Section V for further detail of deviation and mitigating controls.	Control objective met.
<b>CO.4</b> - Technology assisted voting shall ensure that only the appropriate number of votes per voter is cast, stored in the electronic ballot box and included in the election result.	5	5	No deviations noted.	Control objective met.

<b>CO.5</b> - The voter interface of technology assisted voting shall be easy to understand and use.	3	3	No deviations noted.	Control objective met.
<b>CO.6</b> - Technology assisted voting shall only grant a user access after authenticating her/him as a person with the right to vote. The voting system shall protect authentication data of the voters, to prevent its misuse, interception, modification, by an unauthorised or malicious user.	3	2	No deviations noted for assessed controls. One control could not be fully tested.	Control objective met.
<b>CO.7</b> - Procedures on encryption shall be developed and implemented for the use of cryptography to protect votes and voter data during election.	9	8	Deviation noted, refer to Section V for further detail of deviation and mitigating controls.	Control objective met.
<b>CO.8</b> - A voter shall be able to verify that their intention is accurately represented in the vote.	2	2	No deviations noted.	Control objective met.
<b>CO.9</b> - The voting system shall ensure votes remain anonymous.	3	3	No deviations noted.	Control objective met.
<b>CO.10</b> - Protection of personally identifiable information (PII) and privacy of data collected by technology assisted voting shall be ensured.	6	4	Deviation noted, refer to Section V for further detail of deviation and mitigating controls. One control could not be fully tested.	Control objective met.
<b>CO.11</b> - Open standards shall be used to enable various technical components or services, to inter-operate.	2	2	No deviations noted.	Control objective met.
<b>CO.12</b> - Procedures are implemented for the management and handling of removable media during the election process.	1	1	No deviations noted.	Control objective met.
<b>CO.13</b> - Controls are implemented to ensure that only validated personnel are given access to technology assisted voting.	5	4	Deviation noted, refer to Section V for further detail of deviation and mitigating controls.	Control objective met.
<b>CO.14</b> - Before an election, the electoral management body will satisfy itself that technology assisted voting operates correctly.	2	2	No deviations noted.	Control objective met.
<b>CO.15</b> - Access control is managed and monitored appropriately based on the principle of need to know and need to use.	6	3	Deviations noted, refer to Section V for further detail of deviations and mitigating controls.	Control objective met.



<b>CO.16</b> - Development, implementation, and changes to new & existing systems, applications and software are documented, authorised, tested and approved.	4	2	Deviations noted, refer to Section V for further detail of deviations and mitigating controls.	Control objective met.
<b>CO.17</b> - Secure development practices, testing, and operating environments are used to ensure the integrity of iVote System.	6	5	Deviation noted, refer to Section V for further detail of deviation and mitigating controls.	Control objective met.
<b>CO.18</b> - A mechanism to protect against malware is implemented and operating.	1	0	Deviation noted, refer to Section V for further detail of deviation and mitigating controls.	Control objective not met.
<b>CO.19</b> - Detection and monitoring capabilities have been implemented to detect unauthorised activities.	6	5	Deviation noted, refer to Section V for further detail of deviation and mitigating controls.	Control objective met.
<b>CO.20</b> - A procedure is established to identify vulnerabilities and regularly install updated versions and corrections of all relevant software.	8	7	No deviations noted for assessed controls. One control could not be fully tested.	Control objective met.
<b>CO.21</b> - Technology assisted voting systems' networks are managed, controlled and segmented to protect information in systems and applications.	10	5	Deviations noted, refer to Section V for further detail of deviations and mitigating controls.	Control objective not met.
<b>CO.22</b> - Physical protection and guidelines for secure areas and equipment are designed and applied.	3	2	Deviation noted, refer to Section V for further detail of deviation and mitigating controls.	Control objective met.
<b>CO.23</b> - Procedures and capabilities related to business continuity and resilience are established to operate effectively during a time of an incident.	6	3	Deviations noted, refer to Section V for further detail of deviations and mitigating controls.	Control objective not met.
<b>CO.24</b> - IT and information security incidents are responded to and reported in accordance with documented procedures.	5	4	Deviation noted, refer to Section V for further detail of deviation and mitigating controls.	Control objective met.

# 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 polling place because you have a disability or have difficulties reading
- are a silent elector
- applied for a postal vote but 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 V 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 V 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 processes 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:  
Independent Assurance  
Practitioner's Reasonable  
Assurance Report

## Independent Assurance Practitioner's Reasonable Assurance Report on the Design and Operating Effectiveness of Controls to the NSW Electoral Commission

To the Electoral Commissioner,

### Qualified Opinion

We have undertaken a reasonable assurance engagement on the design and operating effectiveness of controls within the NSW Electoral Commission's (NSWEC) Technology Assisted Voting (iVote) system (the "controls") comprising of the Registration and Credential Management system, the Assurance system and the Voting system, throughout the period from 8 November 2021 to 23 December 2021 relevant to the control objectives included in Section V and specified by NSWEC.

In our opinion, except for the effects of the matters described in the Basis for Qualified Opinion paragraph below, in all material respects:

- a) the controls within NSWEC's Technology Assisted Voting system were suitably designed to achieve objectives outlined in Section V; and
- b) the controls operated effectively as designed, throughout the period from 8 November 2021 to 23 December 2021.

### Basis for Qualified Opinion

Our qualified opinion has been formed on the basis of the matters outlined in this report. Due to deviations identified in the testing of controls in Section V, the following control objectives were not met for the period:

- a) Control objective #18: A mechanism to protect against malware is implemented and operating.
  - a. There were gaps in the operation of the control in place to achieve this objective, as NSWEC could not confirm the operation of this control by two of the three third party vendors throughout the election period.
  - b. In addition, 12 of 33 virtual servers in the Registration / Credential Management environment were not included as part of the daily scan for malware.
- b) Control objective #21: Technology assisted voting systems' networks are managed, controlled and segmented to protect information in systems and applications.
  - a. Documentation to evidence that NSWEC actively monitored perimeter security controls and network-based intrusion detection or prevention systems during the period could not be provided.
  - b. All three iVote environments (Assurance, Registration and Credential Management and Voting) did not have two factor authentication enabled on its firewalls.
  - c. One server was not locked during one of the environment lockdowns. This server's function was to forward iVote system logs to Splunk.
  - d. All voting systems were not protected by host-based security systems.
- c) Control objective #23: Procedures and capabilities related to business continuity and resilience are established to operate effectively during a time of an incident.

Liability limited by a scheme approved under Professional Standards Legislation.

Member of Deloitte Asia Pacific Limited and the Deloitte organisation.

- a. Documentation could not be provided to evidence that NSWEC actively monitored that their third party vendors were backing up data and systems.
- b. Documentation to evidence that NSWEC has successfully restored data from a backup image could not be provided.
- c. Evidence of resolution of failed backups could not be obtained for two servers in the Voting environment that had repeat backup failures during the period.

We conducted our engagement in accordance with Standard on Assurance Engagements ASAE 3150 Assurance Engagements on Controls, issued by the Auditing and Assurance Standards Board. That standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, the controls are suitably designed and implemented to achieve the control objectives and the controls operated effectively throughout the period.

Sliced Tech is a third party who manages the infrastructure hosting for the Voting System. Secure Logic is a third party who manages the infrastructure hosting for the Registration and Credential Management System. AC3 is a third party who manages the infrastructure hosting the Assurance System. The carve-out method has been used in relation to them.

Our assurance engagement excludes the control objectives and related controls at Sliced Tech, Secure Logic and AC3, consequently our procedures did not extend to controls at the third party.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our qualified opinion.

### **Responsibilities of NSW Electoral Commission's Management**

Management are responsible for:

- the functions within the iVote system;
- identifying control objectives in relation to the iVote system;
- identifying the risks that threaten the achievement of the control objectives;
- designing controls to mitigate those risks, so that those risks will not prevent achievement of the identified control objectives;
- operating those controls effectively as designed through the period.

### **Our Independence and Quality Control**

We have complied with the independence and other relevant ethical requirements relating to assurance engagements and apply Auditing Standard ASQC 1 *Quality Control for Firms that Perform Audits and Reviews of Financial Reports and Other Financial Information, Other Assurance Engagements and Related Services Engagements* in undertaking this assurance engagement.

### **Assurance Practitioner's Responsibilities**

Our responsibility is to express an opinion on the suitability of the design to achieve the control objectives and the operating effectiveness of NSWEC's controls within iVote system, based on our procedures included in Section IV. Our procedures included:

- a) obtaining an understanding of the control environment of NSWEC relevant to the iVote system;
- b) examining the reasonable of the control objectives;

Liability limited by a scheme approved under Professional Standards Legislation.

Member of Deloitte Asia Pacific Limited and the Deloitte organisation.

- c) evaluating the design of specific controls by:
  - o assessing the risks that threaten achievement of the control objectives;
  - o evaluating whether the controls as designed are capable of addressing those risks and achieving the related control objectives; and
- d) Performing tests of controls to ascertain whether the degree of compliance with controls is sufficient to provide reasonable assurance that the controls have achieved their objectives throughout the period. This includes making enquiries, inspecting documents, conducting walk throughs and performance of controls to ascertain whether the degree of compliance in controls is sufficient to achieve their control objectives throughout the period.

### **Other Information**

Sections I – V of this report were provided to NSWEC on 21 February 2022. Management responses to the deviations noted in this report were provided as Other Information on 29 April 2022. Management is responsible for the other information. The other information comprises the information included in Section I and Section II for the period 8 November 2021 to 23 December 2021, but does not include the control objectives and controls stated in Section V and our assurance report thereon.

Our opinion in Section III on the design and operation of controls related to the control objectives stated in Section V does not cover the other information and we do not express any form of assurance conclusion thereon.

In connection with our assurance engagement, our responsibility is to read the other information and, in doing so, consider whether the other information is materially inconsistent with our knowledge obtained during the assurance engagement, or otherwise appears to be materially inconsistent or contains a material misstatement of fact. If, based on the work we have performed, we conclude that there is a material inconsistency or a material misstatement of fact of this other information, we are required to report that fact. We have nothing to report in this regard.

### **Inherent Limitations**

Because of the inherent limitations of an assurance engagement, together with the inherent limitations of any system of controls there is an unavoidable risk that some deficiencies in the design or deviations in the operating effectiveness of controls may not be detected, even though the engagement is properly planned and performed in accordance with Standards on Assurance Engagements.

An assurance engagement on the operating effectiveness of controls is not designed to detect all instances of controls operating ineffectively as it is not performed continuously throughout the period and the tests are performed on a sample basis. Any projection of the outcome of the evaluation of the suitability of the design of controls to future periods is subject to the risk that the controls may become inadequate because of changes in conditions, or that the degree of compliance with them may deteriorate.

The system, within which the controls that we will test are designed to operate, will not be examined except to the extent the system is relevant to the achievement of the control objectives. Accordingly, no opinion will be expressed as to the design or effectiveness of the system of controls as a whole.

### **Restricted Use**

This report has been prepared for the NSWEC for the purpose of assisting them in their reporting on the controls over the iVote system. We disclaim any assumption of responsibility for any reliance on this report to any person other than the NSWEC or for any purpose other than that for which it was prepared.

Liability limited by a scheme approved under Professional Standards Legislation.

Member of Deloitte Asia Pacific Limited and the Deloitte organisation.



We understand that the NSW Electoral Commission will publish a copy of this report on their website. We do not accept responsibility for the electronic presentation of this report on the NSW Electoral Commission's website. The security and controls over information on the website is not evaluated or addressed by the independent assurance practitioner. The examination of the controls over the electronic presentation of this report on the NSW Electoral Commission's website was beyond the scope of our engagement.

DELOITTE TOUCHE TOHMATSU



**Duncan Auty**  
Partner  
Sydney, 02 May 2022

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

# Section IV: Overview of the Work Performed

## Section IV: 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 pertaining to the Local Government Elections 2021.

Deloitte Touche Tohmatsu's engagement was conducted in accordance with the Standard on Assurance Engagements 3150, *Assurance Engagements on Controls*, issued by the Auditing and Assurance Standards Board. Testing of controls was restricted to the control objectives and related control activities listed in Section V 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 V.

### 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 samples throughout the period 8 November 2021 – 23 December 2021. In determining the nature, timing and extent of tests we considered the following:

- Nature and frequency of the controls being tested
- Types of available evidential matter
- Nature of the control objectives to be achieved
- Assessed level of control risk
- Expected effectiveness of the test, and
- 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:

- Standard "out of the box" reports as configured within the system
- Parameter-driven reports generated by NSWEC systems
- Custom-developed reports that are not standard to the application such as scripts, report writers, and queries
- Spreadsheets that include relevant information utilised for the performance or testing of a control
- 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 V, 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 V throughout the 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:

<b>Test</b>	<b>Description</b>
<b>Inquiry</b>	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.
<b>Observation</b>	Observed the performance of the control multiple times throughout the report period to evidence application of the specific control activity.
<b>Inspection of documentation</b>	If the performance of the control is documented, inspected documents and reports indicating performance of the control.
<b>Reperformance of monitoring activities or manual controls</b>	Obtained documents used in the monitoring activity or manual control activity and independently reperfomed the procedures. Compared any deviation items identified with those identified by the responsible control owner.
<b>Reperformance of programmed processing</b>	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 considered 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.

## Reporting on 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 used judgement in considering the overall operating effectiveness of the control by considering the number of deviations detected, the potential significance of the deviation, as well as other qualitative aspects of the deviations such as the cause of the deviation.

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

If we found 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 considered whether the deviation is representative of systematic or intentional deviations.

If control deviations were found in tests of controls which operate daily or less frequently, the sample size could not be extended and we assessed such controls as ineffective.

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

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

This Section presents the following information provided by NSW Electoral Commission:

- The control objectives specified by the management of NSW Electoral Commission.
- The controls established and specified by NSW Electoral Commission to achieve the specified control objectives.

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 effectively 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 control has 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.	<ol style="list-style-type: none"> <li>1. Enquire with management to determine whether NSWEC have a defined and documented Information Security Policy in place for the iVote system.</li> <li>2. Obtain and inspect the NSWEC Information Security Policy to determine if it is:               <ul style="list-style-type: none"> <li>- Approved by senior management;</li> <li>- Reviewed on a regular, predefined basis; and,</li> <li>- Covers relevant and key areas of security in line with better practice (i.e. NIST).</li> </ul> </li> <li>3. Obtain and inspect screenshot of the intranet or equivalent to determine if policy is available to all relevant stakeholders including key subcontractors.</li> <li>4. Obtain and inspect evidence of employee acknowledgement of policy/procedures, on starting and periodically during employment.</li> </ol>	<p><b>The following deviation was noted:</b></p> <p>The NSWEC Information Security Policy has not been reviewed according to the defined review frequency.</p>
1.02 	Appropriate standards, guidelines, and procedures are in place to manage information security in accordance with the information security policy.	<ol style="list-style-type: none"> <li>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.</li> <li>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:               <ul style="list-style-type: none"> <li>- Cryptographic Key Management Standard;</li> <li>- Access Control policy/procedure;</li> <li>- Network Security policy/procedure;</li> <li>- Security Monitoring policy/procedure; and,</li> <li>- Documents listing out security controls for iVote.</li> </ul> </li> </ol>	No deviations noted.



Control Reference	Control Activity	2021 Test Procedures	Results of Tests
1.03 	A risk register is maintained and regularly reviewed which captures identified risks to technology assisted voting.	<ol style="list-style-type: none"> <li>1. Enquire with management to determine whether a risk register is maintained which captures identified risk to iVote.</li> <li>2. Obtain and inspect the risk register to determine whether:               <ul style="list-style-type: none"> <li>• A risk register is maintained which captures identified risk to iVote;</li> <li>• A risk owner and treatment plan is identified; and,</li> <li>• A regular review is performed over this risk register.</li> </ul> </li> </ol>	No deviations noted.
1.04 	A risk mitigation program is established to identify and mitigate the risks identified in the risk register.	<ol style="list-style-type: none"> <li>1. Enquire with management to determine whether a risk mitigation program is utilised to identify and mitigate risks identified in the risk register.</li> <li>2. Obtain and inspect the risk register to determine the total number of risks identified as part of the iVote operation.</li> <li>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.</li> </ol>	No deviations noted.


**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.	<ol style="list-style-type: none"> <li>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.</li> <li>2. Obtain and inspect help files (including instructional videos / media) and FAQs to determine whether help files and FAQs:               <ul style="list-style-type: none"> <li>- Are available for voters on the iVote website;</li> <li>- Provide information to voters about the steps for registration in order to use iVote;</li> <li>- Are made available online to help build awareness of the:                   <ul style="list-style-type: none"> <li>o Timelines for using iVote for voting;</li> <li>o Details of the candidates and other available choices; and,</li> <li>o Details on how to register for iVote and use iVote system.</li> </ul> </li> <li>- Provides information to voters about the steps for a voter to cancel their selection and re-submit their vote.</li> </ul> </li> </ol>	No deviations noted.
2.02 	Technology assisted voting provides feedback on the confirmation of valid/invalid options and on successful completion of voting procedure.	<ol style="list-style-type: none"> <li>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.</li> </ol>	No deviations noted.
2.03 	Voters are able to test/perform a demonstration to familiarise themselves with the system.	<ol style="list-style-type: none"> <li>1. Obtain and inspect evidence to determine whether iVote has a test/demonstration version for voting made available to the voters.</li> </ol>	No deviations noted.

**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.	<ol style="list-style-type: none"><li>1. Enquire with management to determine whether candidate information on iVote is equivalent to the physical ballot.</li><li>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.</li><li>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.</li></ol>	<p><b>The following deviations were noted:</b></p> <p>The NSWEC Election Operations team conducted iVote Ballot Proof Checking sessions on 10 November 2021 and 11 November 2021. The following observation(s) were noted:</p> <ul style="list-style-type: none"><li>• Checked ballot papers were to be signed by two proofers before being marked as complete. For one sample, the ballot paper was marked as complete without the proofer signatures.</li><li>• Proofers were to check, on mobile and desktop versions of the iVote page, if:<ol style="list-style-type: none"><li>i. Instructions for iVote landing page were as described on the checklist and there were no typographical errors</li><li>ii. The number of candidates on the respective form was explicitly stated</li><li>iii. The Council and ward name was spelt correctly</li><li>iv. The ballot paper draw order appeared the same as the physical ballot</li><li>v. The spelling of the candidate, party and/or political affiliation was spelt correctly.</li></ol>For one sample, the ballot paper proofing did not check steps i, ii and iii above.</li><li>• Proofers were required to notify supervisor staff of any discrepancies for the supervisor to triage and make a determination on the actions to take. For one sample, the proofers did not engage the supervisor for a discrepancy in the sample.</li></ul> <p><b>Mitigating control:</b> The following requirements were checked as part of system testing which checked that technology assisted voting is equivalent to the physical ballot as a first check prior to iVote Ballot Proof Checking:</p>


Control Reference	Control Activity	2021 Test Procedures	Results of Tests
			i. Instructions for iVote landing page were as described on the checklist and there were no typographical errors ii. The number of candidates on the respective form was explicitly stated iii. The Council and ward name was spelt correctly Refer to control 14.01.
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: <ul style="list-style-type: none"> <li>• Help documents;</li> <li>• Technology Assisted Voting Approved Procedures;</li> <li>• FAQs; and,</li> <li>• Accessibility information - screen readers, AUSLAN document.</li> </ul> 3. Test that language used for ballot paper instructions are replicated in iVote voting instructions unless stated otherwise in the Technology Assisted Voting Procedures.	No deviations noted.
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.	No deviations noted.



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.	<ol style="list-style-type: none"> <li>1. Enquire with management to determine whether iVote allows users to cast their vote without providing a preference.</li> <li>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).</li> </ol>	No deviations 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.	No deviations noted.
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.	No deviations noted.
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.	No deviations noted.




Control Reference	Control Activity	2021 Test Procedures	Results of Tests
4.04	 <p>Prior to the final result, the voting system identifies votes which are invalid, duplicated or generated due to an error.</p>	<ol style="list-style-type: none"> <li>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.</li> <li>2. Obtain and inspect documented procedure implemented and determine whether it is defined to ensure invalid/duplicate votes are removed.</li> <li>3. Obtain and inspect iVote generated reporting to determine total number of votes that are invalid, duplicated or generated due to error.</li> <li>4. Obtain and inspect evidence to indicate these votes are not included in the final vote results.</li> <li>5. Observe during the decryption ceremony to determine whether the iVote system identifies invalid, duplicate, or votes generated due to error. Check whether the following information is captured: <ul style="list-style-type: none"> <li>• Number of voters – registered;</li> <li>• Voters who voted (data from iVote);</li> <li>• Duplicate voters where an additional channel of voting has been used and supports a real time voter roll;</li> <li>• Voters who voted (data from verification system); and,</li> <li>• Votes with errors.</li> </ul> </li> </ol>	No deviations noted.


Control Reference	Control Activity	2021 Test Procedures	Results of Tests
4.05	  <p>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.</p>	<ol style="list-style-type: none"> <li>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.</li> <li>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.</li> <li>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.</li> <li>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.</li> <li>5. Where applicable, obtain and inspect evidence of discarding and/or remediation of votes with errors.</li> </ol>	No deviations noted.



**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.	<ol style="list-style-type: none"> <li>1. Enquire with management to understand whether iVote enables all voters (including persons with disabilities) to vote.</li> <li>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.)</li> <li>3. Obtain and inspect the Web Content Accessibility Guidelines (WCAG) 2.0 to determine the requirements that iVote is required to meet.</li> <li>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.</li> <li>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.</li> </ol>	No deviations 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.	<ol style="list-style-type: none"> <li>1. Enquire with management to understand how iVote operates in a uniformly manner across different types of devices.</li> <li>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.).</li> <li>3. Observe at Ballot Proofing sessions to determine if iVote is checked using various devices.</li> <li>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.).</li> </ol>	No deviations noted.

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.	<ol style="list-style-type: none"> <li>1. Enquire with management to determine whether a mechanism has been established for voters to speak with voting staff about iVote queries.</li> <li>2. Obtain and inspect evidence to determine whether a call centre was operating to help voters with their iVote queries throughout the voting period.</li> </ol>	No deviations noted.





**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
<p>6.01</p> 	<p>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.</p>	<ol style="list-style-type: none"> <li>1. Enquire with management to understand how the registration process authenticates voters prior to voting. Further understand how voters are provisioned unique iVote Numbers.</li> <li>2. Obtain and inspect process documentation to ensure that iVote numbers generated by the Credential Management System are unique in nature.</li> <li>3. Re-perform registration in the production environment of the iVote System to ensure that upon application of an iVote number, users are required to setup their own PIN/Password.</li> </ol>	<p>No deviations noted.</p>
<p>6.02</p> 	<p>In order to reset the PIN/Password and generate new credentials users must re-verify their identity.</p>	<ol style="list-style-type: none"> <li>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.</li> <li>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.</li> <li>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.</li> </ol>	<p>No deviations noted.</p>
<p>6.03</p> 	<p>The authentication data is securely erased from technology assisted voting when it is no longer required.</p>	<ol style="list-style-type: none"> <li>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.</li> <li>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.</li> <li>3. Observe the data removal process for a prior election to determine whether authentication data is securely erased from iVote when it is no longer required.</li> </ol>	<p><b>Limitation to testing:</b></p> <p>Although policies and procedures to securely erase authentication, security and privacy data are defined, we were unable to check the secure erasure of authentication, security and privacy data as the deletion of data for the 2021 Local Government Elections will be conducted approximately six months after election day and therefore is outside the period.</p>


**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
<p>7.01</p> 	<p>An encryption policy is formally documented with approved encryption standards to be used.</p>	<ol style="list-style-type: none"> <li>1. Enquire with management to determine whether NSWEC has a defined and documented Encryption Policy in place for the iVote system.</li> <li>2. Obtain and inspect the NSWEC Encryption Policy to determine whether the policy is: <ul style="list-style-type: none"> <li>• Approved by senior management;</li> <li>• Reviewed on a regular, predefined basis; and,</li> <li>• Defines approved encryption and cryptography standards used on iVote systems.</li> </ul> </li> </ol>	<p><b>The following deviation was noted:</b></p> <p>The Cryptographic Policy has not been reviewed according to the defined review frequency.</p> <p><b>Mitigating control:</b> Although the NSWEC Cryptographic Policy was not reviewed within the defined review frequency, the iVote system has been observed to encrypt Registration applications, voter details logging in using iVote, and votes submitted via iVote. Refer to control 7.07.</p>
<p>7.02</p> 	<p>Cryptographic key management life cycle is documented and includes:</p> <ul style="list-style-type: none"> <li>- Key generation</li> <li>- Storage, distribution and installation</li> <li>- Key usage and rotation</li> <li>- Backup and recovery</li> <li>- Key revocation and suspension</li> <li>- Secure destruction.</li> </ul>	<ol style="list-style-type: none"> <li>1. Enquire with management to determine whether NSWEC has a defined and documented Encryption Policy in place for the iVote system.</li> <li>2. Obtain and inspect the NSWEC Encryption Policy to determine if the procedures are defined for the following areas: <ul style="list-style-type: none"> <li>• Key and certificate generation;</li> <li>• Storage, distribution and installation;</li> <li>• Key usage and rotation;</li> <li>• Backup and recovery;</li> <li>• Key revocation and suspension; and,</li> <li>• Secure destruction.</li> </ul> </li> </ol>	<p>No deviations noted.</p>
<p>7.03</p>  	<p>A quorum of electoral officers is required for the decryption of votes prior to the end of the election.</p> <p>A private key is shared between members to prevent a single electoral officer from decrypting the votes.</p>	<ol style="list-style-type: none"> <li>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.</li> <li>2. Observe the private key splitting process to determine whether: <ul style="list-style-type: none"> <li>• The key is split between multiple, appropriate members of the Electoral Commission; and</li> </ul> </li> </ol>	<p>No deviations noted.</p>



Control Reference	Control Activity	2021 Test Procedures	Results of Tests
		<ul style="list-style-type: none"> <li>• Pins to card are written down and stored in a tamper-proof envelope which is stored within the Commissioner’s safe.</li> </ul> <p>3. During decryption night, observe if a quorum of members are present to input their portion of the split password.</p>	
<p>7.04</p> 	<p>Mechanisms are implemented to ensure integrity of the votes captured from the voter.</p>	<p>1. Enquire with management to understand the encryption mechanism in place to ensure integrity of the votes captured from the voter.</p> <p>2. Obtain and inspect documented procedures to determine whether a voting receipt is captured in a separate system (assurance).</p> <p>3. Observe Logic and Accuracy testing to verify:</p> <ul style="list-style-type: none"> <li>• Receipts are sent to all voters after vote submission; and,</li> <li>• voters can verify their vote with the mobile application.</li> </ul>	<p>No deviations noted.</p>
<p>7.05</p> 	<p>Scrutineers are invited to the decryption process after the end of the elections and votes are only decrypted after the close of voting.</p>	<p>1. Enquire with management to understand the key decryption process.</p> <p>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.</p> <p>3. Obtain and inspect documented procedures to determine whether key stakeholders such as scrutineers are present during the decryption ceremony.</p> <p>4. Observe the decryption process to determine whether scrutineers are present during the decryption ceremony.</p>	<p>No deviations noted.</p>

Control Reference	Control Activity	2021 Test Procedures	Results of Tests
7.06 	iVote numbers and passwords are not stored in the voting or assurance system.	<ol style="list-style-type: none"> <li>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.</li> <li>2. Obtain and inspect evidence that iVote numbers and passwords are not stored in the voting or assurance system.</li> </ol>	No deviations noted.
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.	<ol style="list-style-type: none"> <li>1. Enquire with management to determine whether NSWEC has a defined and documented Encryption Policy in place for the iVote system.</li> <li>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.</li> <li>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.</li> <li>4. Observe onscreen and obtain screenshots to determine that voter information/voter preference is not transmitted in cleartext inside the NSWEC environment after SSL offload.</li> </ol>	No deviations noted.
7.08  	Backups are protected using encryption and are stored in an offsite location.	<ol style="list-style-type: none"> <li>1. Enquire with management to determine whether NSWEC has a defined and documented Encryption Policy in place for the iVote system backups.</li> <li>2. Obtain and inspect the NSWEC Encryption Policy to determine whether the policy defines how backups of relevant iVote systems is encrypted and stored.</li> <li>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: <ul style="list-style-type: none"> <li>• Registration system;</li> <li>• Voting system components;</li> <li>• Assurance system; and,</li> <li>• Offline systems.</li> </ul> </li> </ol>	No deviations noted.

Control Reference	Control Activity	2021 Test Procedures	Results of Tests
7.09 	An encryption mechanism is implemented in the verification system to ensure that voters can decrypt and read only their vote.	<ol style="list-style-type: none"> <li>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.</li> <li>2. Observe 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).</li> </ol>	No deviations noted.

**CONTROL OBJECTIVE 8–**



**Control Objective: A voter is able to verify that their intention is accurately represented in the vote.**




<b>Control Reference</b>	<b>Control Activity</b>	<b>2021 Test Procedures</b>	<b>Results of Tests</b>
8.01 	A voter is able to verify that their vote has been accurately entered into electronic ballot box without any alteration.	<ol style="list-style-type: none"><li>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.</li><li>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.</li><li>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.</li></ol>	No deviations noted.
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.	<ol style="list-style-type: none"><li>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.</li><li>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.</li><li>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.</li></ol>	No deviations noted.



**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.	<ol style="list-style-type: none"> <li>1. Enquire with management to understand how personal identifying information (PII) is stored within the iVote system.</li> <li>2. Obtain and inspect NSWEC documentation to determine whether procedures exist to separate a voter's PII from the vote.</li> <li>3. Obtain and inspect system configuration documentation to determine whether systems are designed to keep PII separate from the vote.</li> <li>4. Observe onscreen and obtain a screenshot of the database for a sample of one vote across iVote systems to determine whether PII is stored separately from the vote.</li> </ol>	No deviations noted.
9.02 	Procedures are defined to prevent the link between the voter and the voter's preference to be established.	<ol style="list-style-type: none"> <li>1. Enquire with management to understand the procedures defined to prevent the establishment of a voter and their preference.</li> <li>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.</li> <li>3. Obtain and inspect evidence of daily cleansing during voting period to determine whether prior votes are discarded when a voter re-votes.</li> </ol>	No deviations noted.



Control Reference	Control Activity	2021 Test Procedures	Results of Tests
9.03	   <p>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.</p>	<ol style="list-style-type: none"> <li>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.</li> <li>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.</li> <li>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.</li> </ol>	No deviations noted.

**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
<p>10.01</p> 	<p>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.</p>	<p>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.</p> <p>2. Obtain and inspect the PIA to determine that the following has been captured:</p> <ul style="list-style-type: none"> <li>• Information required during registration;</li> <li>• Information implicitly and explicitly captured from voters during voting process;</li> <li>• Information implicitly and explicitly captured from voters during verification process;</li> <li>• Purpose of collection and processing each data attribute; and,</li> <li>• Retention period.</li> </ul>	<p>No deviations noted.</p>
<p>10.02</p> 	<p>The voter must be made aware of the information collected from them during all phases of election (registration to results).</p>	<p>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).</p> <p>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.</p> <p>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.</p>	<p><b>The following deviation was noted:</b></p> <p>Notice of Personally Identifiable Information (PII) retention was not explicitly highlighted for the registration stage. It is noted that the privacy policy was included as a link in the website footer; however, notice of the specific private information collected was not explicitly referenced during the registration process.</p> <p><b>Mitigating control:</b> The iVote system only captures the information described in the Privacy Impact Assessment which is the minimum data required for voting. Refer to control 10.03.</p>

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.	<ol style="list-style-type: none"> <li>1. Enquire with management to determine whether iVote only captures only the information described in the Privacy Impact Assessment.</li> <li>2. Obtain and inspect system documentation to determine whether only the following is captured by the iVote system, in line with the PIA: <ul style="list-style-type: none"> <li>• Information required during registration;</li> <li>• Information captured from voters during voting process; and,</li> <li>• Information captured from voters during verification process.</li> </ul> </li> <li>3. Observe voting stages (registration, voting and verification) onscreen to check that only the following information is captured in line with PIA: <ul style="list-style-type: none"> <li>• Information required during registration;</li> <li>• Information captured from voters during voting process; and,</li> <li>• Information captured from voters during verification process.</li> </ul> </li> </ol>	No deviations 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.	<ol style="list-style-type: none"> <li>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.</li> <li>2. Obtain and inspect NSWEC documentation and observe in-person for a prior election to determine whether procedures are defined and implemented to: <ul style="list-style-type: none"> <li>• Ensure that the voter information from all the system components of iVote (including storage systems and backup systems) is securely deleted after the elections;</li> <li>• Ensure that voter information from backup tapes is securely deleted after the elections.</li> </ul> </li> </ol>	<p><b>Limitation to testing:</b></p> <p>Although procedures are in place requiring deletion of data, we were unable to check the deletion of voter information from all the system components of iVote (including storage systems and backup systems) as the deletion of data for the 2021 Local Government Elections is conducted approximately six months after election day. This is outside of the period.</p>


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.	<ol style="list-style-type: none"> <li>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.</li> <li>2. Obtain and inspect NSWEC documentation to determine whether: <ul style="list-style-type: none"> <li>• Voter information on production instances of iVote was not used in development and test environment; and,</li> <li>• Only information required to conduct the election was collected by the iVote system.</li> </ul> </li> </ol>	No deviations 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)	<ol style="list-style-type: none"> <li>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.</li> <li>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.</li> <li>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.</li> </ol>	No deviations noted.

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

<b>Control Reference</b>	<b>Control Activity</b>	<b>2021 Test Procedures</b>	<b>Results of Tests</b>
11.01 	Standard data exchange and data formats are used in the voting and assurance system and avoid the use of proprietary frameworks.	<ol style="list-style-type: none"><li>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.</li><li>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.</li></ol>	No deviations noted.
11.02 	Standard publicly available encryption algorithms are used and use of proprietary algorithms are avoided.	<ol style="list-style-type: none"><li>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.</li><li>2. Obtain and inspect NSWEC documentation to determine whether iVote uses publicly available encryption algorithms.</li></ol>	No deviations noted.



**CONTROL OBJECTIVE 12–**

**Control Objective: Procedures are implemented for the management and handling of removable media during the election process.**



<b>Control Reference</b>	<b>Control Activity</b>	<b>2021 Test Procedures</b>	<b>Results of Tests</b>
12.01 	The usage of removable media for elections during the lockdown is documented and restricted.	<ol style="list-style-type: none"><li>1. Enquire with management to understand how usage of removable media for elections during the lockdown is documented and restricted.</li><li>2. During the election, observe whether the following information was documented and followed:<ul style="list-style-type: none"><li>• Type of removable media;</li><li>• Step in the election process and task for which the removable media was used;</li><li>• System which were used to transfer information using the device;</li><li>• Controls implemented to protect sensitive information on removable media;</li><li>• Name/type of the systems between which information was to be shared using USB/removable media;</li><li>• Impact on the voting process if the removable media was to be lost/misplaced/stolen; and,</li><li>• That appropriate removable device has been whitelisted.</li></ul></li><li>3. Obtain and inspect evidence of an Impact Assessment on an election scenario whereby removable media is lost, misplaced and/or stolen.</li></ol>	No deviations noted.


**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.	<ol style="list-style-type: none"> <li>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.</li> <li>2. Obtain and inspect a list of to determine the total number of users that have worked on the iVote system.</li> <li>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: <ul style="list-style-type: none"> <li>• Design and architecture;</li> <li>• Execution/Code;</li> <li>• Testing;</li> <li>• Deployment and maintenance; and,</li> <li>• Security.</li> </ul> </li> </ol>	No deviations noted.
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.	<ol style="list-style-type: none"> <li>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.</li> <li>2. Obtain and inspect evidence of NSWEC requirements for third party vendors of the requirements for background checks.</li> <li>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.</li> </ol>	No deviations noted.



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.	<ol style="list-style-type: none"> <li>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.</li> <li>2. Obtain and inspect a list of employees and external party users that are involved in iVote processes.</li> <li>3. For the sample selected, obtain and inspect evidence of completion of Cyber Security Awareness training to determine if the users have completed awareness program and training in a timely manner.</li> <li>4. Obtain and inspect evidence of email requests/reminders automatically sent via the Learning Management System to employees to notify them that outstanding training is to be completed.</li> <li>5. Obtain and inspect evidence to ensure where major policy changes are made, employees are notified of revisions via email or other communication channels.</li> </ol>	No deviations noted.
13.04 	Roles and responsibilities are documented and communicated to members of the election and admin boards.	<ol style="list-style-type: none"> <li>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.</li> <li>2. Observe the initiation ceremony to determine: <ul style="list-style-type: none"> <li>• Processes of creation of election and admin board; and,</li> <li>• Delegation of roles and responsibilities to election and admin board members.</li> </ul> </li> </ol>	<p><b>The following deviation was noted:</b></p> <p>Election operators did not confirm with two of five administrator board members that they had read the iVote Electoral &amp; Admin Board Member briefing document and were aware of their role, obligations, and responsibilities before they were provisioned a smart card.</p> <p><b>Mitigating control:</b> Although roles and responsibilities were not formally communicated, the two staff were observed to be following the agreed process during the initiation ceremony. Refer to control 14.02.</p>


Control Reference	Control Activity	2021 Test Procedures	Results of Tests
13.05 	<p>NSWEC has formal agreements with all third parties including statements of responsibilities such as;</p> <ul style="list-style-type: none"> <li>- compliance to all applicable regulatory requirements;</li> <li>- adherence to NSWEC's policies and procedures, including the protection of voter's information.</li> </ul>	<ol style="list-style-type: none"> <li>1. Enquire with management to determine whether NSWEC has formal agreements with all third parties including statements of responsibilities.</li> <li>2. Obtain and inspect a list of third parties to determine the total number of vendors involved in the operation of the iVote System.</li> <li>3. Where applicable, obtain security certifications for all vendors (including IS27001 and IRAP reporting).</li> <li>4. For all vendors, obtain and inspect contracts to determine if the following is monitored: <ul style="list-style-type: none"> <li>• Compliance to all applicable regulatory requirements; and,</li> <li>• Adherence to NSWEC's policies and procedures, including the protection of voter's information (via Non-Disclosure Agreement clauses or other).</li> </ul> </li> </ol>	No deviations noted.



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



<b>Control Reference</b>	<b>Control Activity</b>	<b>2021 Test Procedures</b>	<b>Results of Tests</b>
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. Obtain and inspect evidence of UAT and PRT reporting across all iVote platforms (registration, voting and assurance) and determine if test cases and results were reviewed and approved by appropriate management before deployment.	No deviations noted.
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: <ul style="list-style-type: none"> <li>• Test votes cast in accordance with the approved procedures were accurately reflected in the corresponding test ballot papers produced; and,</li> <li>• All voting devices are included in L&amp;A testing.</li> </ul>	No deviations noted.


**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.	<ol style="list-style-type: none"><li>1. Enquire with management to determine whether NSWEC has a defined and documented Access Control Policy in place for the iVote system.</li><li>2. Obtain and inspect NSWEC Access Control Policy to determine whether the policy is:<ul style="list-style-type: none"><li>• Approved by senior management;</li><li>• Reviewed on a regular, predefined basis;</li><li>• Covers access management requirements for user (regular users and privileged users) of iVote systems (including offline systems) and networking/security devices;</li><li>• Covers access management requirements for suppliers/contractors; and,</li><li>• Defines the requirement for two factor authentication for privileged access to key iVote components.</li></ul></li><li>3. Obtain and inspect screenshot of intranet or equivalent to determine if policy is available to all relevant stakeholders including key subcontractors.</li><li>4. Obtain and inspect evidence of policy/procedure acknowledgment, on starting and periodically during employment.</li></ol>	<p><b>The following deviation was noted:</b></p> <p>The NSWEC Access Control Policy had not been reviewed according to the defined review frequency.</p>


Control Reference	Control Activity	2021 Test Procedures	Results of Tests
15.02	 <p>A password policy aligned to the criticality of technology assisted voting is defined and implemented.</p>	<ol style="list-style-type: none"> <li>1. Enquire with management to determine whether NSWEC has a defined and documented Password Policy in place for the iVote system.</li> <li>2. Obtain and inspect NSWEC Password Policy to determine if the Password Policy is: <ul style="list-style-type: none"> <li>• Approved by senior management;</li> <li>• Reviewed on a regular, predefined basis; and,</li> <li>• Mandates the password requirements for all iVote systems.</li> </ul> </li> <li>3. Obtain and inspect screenshot of intranet or equivalent to determine if policy is available to all relevant stakeholders including key subcontractors.</li> <li>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.</li> </ol>	<p><b>The following deviations were noted:</b></p> <ul style="list-style-type: none"> <li>• Password age was not configured to meet NSWEC Access Control Policy for Registration and Credential management servers of 72 days maximum (set to 999 days).</li> <li>• Password age was not configured to meet NSWEC Access Control Policy for Voting system servers (configured to 90 days).</li> <li>• Configuration of Assurance environments: <ul style="list-style-type: none"> <li>– Password lockout threshold and duration was not configured to meet NSWEC Access Control Policy.</li> <li>– Password history was not configured to meet NSWEC Access Control Policy.</li> </ul> </li> </ul> <p><b>Mitigating controls:</b> Although password age was not configured to meet the NSWEC Password Policy, access to all individual user accounts were disabled as part of the iVote system lockdown. Additionally, three senior NSWEC staff were required to unlock the system.</p> <p>Refer to control 15.03 for testing details.</p> <p>NSWEC management reviewed all source code changes prior to go-live to mitigate the risk of unauthorised changes prior to lockdown.</p> <p>Refer to control 16.04 and 17.04 for testing details.</p>
15.03	 <p>During lockdown, a list of approved users to be enabled is documented, to ensure that only approved system accounts remain enabled.</p>	<ol style="list-style-type: none"> <li>1. Enquire with management to understand what user accounts are to be kept enabled during lockdown.</li> <li>2. Obtain and inspect a list of enabled users during lockdown to determine whether only approved system accounts remain enabled.</li> </ol>	<p>No deviations noted.</p>

Control Reference	Control Activity	2021 Test Procedures	Results of Tests
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.	<ol style="list-style-type: none"> <li>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.</li> <li>2. Obtain and inspect a list of user-IDs in the iVote system prior to the lockdown period (registration, voting and assurance).</li> <li>3. For a sample of users created in the period, inspect evidence of approvals to determine whether approval was granted by authorised NSWEC staff and that the access provisioned matches the access approved.</li> </ol>	No deviations noted.
15.05 	Users that no longer require physical and/or logical access are removed from systems in a timely manner.	<ol style="list-style-type: none"> <li>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.</li> <li>2. Obtain and inspect a HR list of employees offboarded from NSWEC.</li> <li>3. For a sample of offboarded users, obtain and inspect evidence to determine whether:               <ul style="list-style-type: none"> <li>• Physical access components (keys, swipe passes, hard-tokens, etc) were returned to NSWEC where applicable; and,</li> <li>• Logical access to all iVote systems was removed in a timely manner by performing comparing between active iVote staff user listing and HR leaver listing to determine if former iVote staff maintained access post-termination.</li> </ul> </li> <li>4. Obtain and inspect evidence of monitoring of third party terminations to ensure access to key iVote services are restricted to current staff only.</li> </ol>	No deviations noted.



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.	<ol style="list-style-type: none"> <li>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.</li> <li>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.</li> <li>3. Obtain and inspect evidence to show that third party access is reviewed and any inappropriate access corrected.</li> </ol>	<p><b>The following deviation was noted:</b></p> <p>A formal periodic user access review was not completed prior to the lead up of the 2021 Local Government Elections per requirements stipulated in the NSWEC Access Control Policy.</p> <p><b>Mitigating controls:</b> Prior to the onboarding of new users to the NSWEC environment, management approval is required before the provisioning of new user access.</p> <p>Refer to control 15.04 for testing details.</p>


**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.	<ol style="list-style-type: none"> <li>1. Enquire with management to understand the change management process.</li> <li>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.</li> <li>3. For a sample of changes, inspect evidence to determine whether:                             <ul style="list-style-type: none"> <li>• Changes follow the change management process;</li> <li>• Changes are initially approved by management to be developed;</li> <li>• Changes were tested; and,</li> <li>• Changes are approved by management before deployment to production environments.</li> </ul> </li> </ol>	<p><b>The following deviation was noted:</b></p> <p>The ICT Technical Change Management Policy had not been reviewed according to the defined review frequency.</p> <p>Although the development and production environments were logically separated for Registration and Credential Management systems, two developers were identified to have access to both environments. It is noted that testing of the change management samples (general and emergency changes) did not identify any unapproved changes being deployed.</p> <p><b>Mitigating controls:</b> NSWEC management reviewed all source code changes prior to go-live to confirm they were appropriate.</p> <p>Refer to control 16.04 and 17.04 for testing details.</p>








Control Reference	Control Activity	2021 Test Procedures	Results of Tests
16.02 	A formal process to conduct emergency changes in production is implemented and approved.	<ol style="list-style-type: none"> <li>1. Enquire with management to determine whether NSWEC has a defined and documented process around emergency changes to the production environment.</li> <li>2. Obtain and inspect the policy/process to determine whether it:               <ul style="list-style-type: none"> <li>• Is approved by senior management;</li> <li>• Is reviewed on a regular, predefined basis;</li> <li>• Defines emergency change procedures; and,</li> <li>• Defines roles and responsibilities of NSWEC staff able to approve of emergency changes.</li> </ul> </li> <li>3. Obtain and inspect screenshot of intranet or equivalent to determine if policy is available to all relevant stakeholders including key subcontractors.</li> <li>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.</li> <li>5. For a sample of emergency changes, inspect evidence to determine whether:               <ul style="list-style-type: none"> <li>• Details of the emergency change;</li> <li>• The change followed the documented process;</li> <li>• Emergency change was approved.</li> </ul> </li> </ol>	<p><b>The following deviations were noted:</b></p> <p>The unlock event on 12 November 2021 could not be linked to a change ticket.</p> <p>No documented evidence of approval could be provided for one of five sampled emergency changes as it was verbally approved.</p> <p>However, Deloitte were present at all emergency changes to observe that for all unlock events management followed a run sheet in line with the documented process and this included details of the emergency change.</p>
16.03 	Development, testing and production environment are logically separated.	<ol style="list-style-type: none"> <li>1. Obtain and inspect evidence of whether the development, testing and production environments are logically segregated.</li> </ol>	No deviations noted.


Control Reference	Control Activity	2021 Test Procedures	Results of Tests
16.04 	Formal software development life cycle management includes maintenance of source code repositories per production environment.	<ol style="list-style-type: none"> <li>1. Enquire with management to determine whether formal software development life cycle management includes maintenance of source code repositories per production environment.</li> <li>2. Obtain and inspect the source repositories for production environments (through separation of source code or any other mechanism). Check access to source code repositories is appropriately restricted and source code maintenance is controlled.</li> </ol>	No deviations noted.

**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
<p>17.01</p> 	<p>Developers are trained on secure development practices.</p>	<ol style="list-style-type: none"> <li>1. Enquire with management to determine whether developers are trained on secure development practices.</li> <li>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.</li> <li>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.</li> <li>4. For a sample of developers, obtain and inspect evidence to determine developer has conducted training and awareness programs on secure development practices.</li> </ol>	<p><b>The following deviation was noted:</b></p> <p>Official training for secure development practices had not been established and completed for NSWEC Registration &amp; Credential Management system developers.</p> <p><b>Mitigating controls:</b> Developed code was reviewed and tested for security flaws prior to go-live.</p> <p>Refer to control 17.02 and 17.05 for testing results.</p>
<p>17.02</p> 	<p>Security testing and mitigation is performed for all components of technology assisted voting in production environments prior to go-live.</p>	<ol style="list-style-type: none"> <li>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.</li> <li>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).</li> <li>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.</li> <li>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.</li> </ol>	<p>No deviations noted.</p>

Control Reference	Control Activity	2021 Test Procedures	Results of Tests
17.03 	Security testing and mitigation is performed for all infrastructure components of the technology assisted voting platform prior to go-live.	<ol style="list-style-type: none"> <li>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.</li> <li>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.</li> <li>3. Where applicable, obtain and inspect evidence of remediation for security deficiencies to determine whether remediation was performed through configuration changes/patch management procedures.</li> </ol>	No deviations noted.
17.04 	The build/deploy of the system in production is validated.	<ol style="list-style-type: none"> <li>1. Enquire with management to determine whether build/deployment of the system in production is validated prior to deployment.</li> <li>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 before release into production.</li> </ol>	No deviations noted.
17.05 	NSWEC provide mechanisms for review and evaluation of the source code for sensitive parts of the technology assisted voting system.	<ol style="list-style-type: none"> <li>1. Enquire with management to determine the mechanisms for review and evaluation of source code for sensitive parts of the iVote systems.</li> <li>2. Obtain and inspect evidence of mechanisms for review and evaluation of source code for sensitive parts of the iVote systems to determine whether: <ul style="list-style-type: none"> <li>• Specified staff are able to review source code; and,</li> <li>• The public are able to review source code.</li> </ul> </li> </ol>	No deviations noted.

Control Reference	Control Activity	2021 Test Procedures	Results of Tests
17.06 	Scrutineers are invited to review and observe select iVote processes in accordance with Section 158 of the Electoral Act 2017.	<ol style="list-style-type: none"> <li>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.</li> <li>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.</li> </ol>	No deviations noted.



**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.	<ol style="list-style-type: none"> <li>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.</li> <li>2. Vendor Reporting is provided to summarise the scans that have occurred during the election period. Where applicable, NSWEC follow-up is conducted for instances of notification.</li> </ol>	<p><b>The following deviations were noted:</b></p> <p>Evidence of Sliced Tech anti-malware reporting could not be sighted for 2 of 6 sampled dates (23 November 2021 and 27 November 2021).</p> <p>AC3 anti-malware reporting was not provided to NSWEC between the period of 22 November 2021 – 24 November 2021 inclusive. As a result, evidence of AC3 anti-malware reporting could not be sighted for 1 of 6 sampled dates (23 November 2021).</p> <p>Upon inspection of the Secure Logic antivirus coverage, it was noted that 12 of 33 production virtual machines in the Registration / Credential Management environment were not included as part of the daily scan.</p>




**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.	<ol style="list-style-type: none"><li>1. Enquire with management to determine whether a log management system (LMS) is implemented for logging of security events.</li><li>2. Obtain and inspect evidence of the LMS to determine whether LMS has been implemented for logging of security events.</li><li>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.</li></ol>	No deviations noted.
19.02 	Log files are immutable for vote casting and cannot be overwritten.	<ol style="list-style-type: none"><li>1. Enquire with management to determine how log files are immutable and cannot be overwritten.</li><li>2. Obtain and inspect NSWEC documentation to determine whether log files that are required to be immutable are defined.</li><li>3. Obtain and inspect LMS configuration to determine whether logs are stored outside the system which generated them.</li><li>4. During the final unlock of the voting system, observe the execution of the Scytl iVote Logs and Proof Validator Tool to determine the immutability of logs exported from the Splunk application server.</li><li>5. Where applicable, observe the investigation and assessment of differences to determine if discrepancies are investigated and remediated in a timely manner.</li></ol>	No deviations noted.



Control Reference	Control Activity	2021 Test Procedures	Results of Tests
19.03	 <p>A Security incident and event management (SIEM) is implemented for real time monitoring of events and management of security incidents.</p>	<ol style="list-style-type: none"> <li>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.</li> <li>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.</li> <li>3. Obtain and inspect the configuration of the SIEM tool to determine whether: <ul style="list-style-type: none"> <li>• SIEM covers all components of iVote system (registration, voting, and assurance systems);</li> <li>• Log sources are integrated with SIEM (e.g. Firewall logs, WAF, access control logs, IDS/IPS, FIM, application level authentication logs, Bridge laptop etc);</li> <li>• Rules are created for identification of events and incidents; and,</li> <li>• All events identified on the web application firewall during lockdown period is logged on SIEM.</li> </ul> </li> <li>4. Obtain and inspect Security Operations Centre reporting to test whether the SOC has access to the anti-malware dashboard and are actively monitoring the anti-malware status of the system.</li> <li>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.</li> <li>6. For a sample of log files, obtain and inspect logs to test: <ul style="list-style-type: none"> <li>• Detection and monitoring capability is implemented on offline systems as these are not integrated with the SIEM; and,</li> <li>• Logs for offline systems are approved by management to confirm no inappropriate access has been made.</li> </ul> </li> </ol>	No deviations noted.







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.	<ol style="list-style-type: none"> <li>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.</li> <li>2. Obtain and inspect a list of security events logged and integrated with the SIEM to determine total number of security incidents.</li> <li>3. For a sample of logs, obtain and inspect a sample log information from iVote (registration, voting and assurance system) and validate if: <ul style="list-style-type: none"> <li>• 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,</li> <li>• 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.</li> </ul> </li> </ol>	<p><b>The following deviation was noted:</b></p> <p>Although Splunk has been implemented to monitor security events such as administrative functions and escalated privileges, evidence could not be provided to determine if Splunk logs contained key event information such as:</p> <ul style="list-style-type: none"> <li>- Timestamp</li> <li>- Host details</li> <li>- Identity of process initiating the event</li> <li>- Detailed description of the event.</li> </ul> <p><b>Mitigating control:</b> A daily Cyber Security stand-up meeting was held to review iVote related cyber security incidents identified through the SIEM.</p> <p>Refer to control 19.03.</p>
19.05 	Sensitive information related to voter and votes is not captured in the logs.	<ol style="list-style-type: none"> <li>1. Enquire with management whether sensitive information related to voter and votes are not captured in logs.</li> <li>2. Obtain and inspect a sample registration log that is ingested into Splunk and determine if voter data is included within the log.</li> <li>3. Obtain and inspect a sample vote log that is ingested into Splunk and determine that voting preference data is not included within the log.</li> </ol>	No deviations noted.
19.06 	All technology assisted voting components is synced with a network time protocol to ensure integrity of logs.	<ol style="list-style-type: none"> <li>1. Enquire with management if all technology assisted voting components are synced with a network time protocol to ensure integrity of logs.</li> <li>2. Observe via Environment Lockdown to determine if all technology assisted voting components are synced with a network time protocol.</li> </ol>	No deviations noted.



**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	 <p>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.</p>	<ol style="list-style-type: none"> <li>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.</li> <li>2. Obtain and inspect the asset listing to determine if assets are:                             <ul style="list-style-type: none"> <li>• 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,</li> <li>• All accounted for and no assets are missing.</li> </ul> </li> <li>3. For a sample of assets, obtain and inspect evidence of review to determine whether assets are reviewed periodically.</li> </ol>	No deviations noted.
20.02	 <p>Vulnerability security assessments are performed to identify vulnerabilities in software and hardware.</p>	<ol style="list-style-type: none"> <li>1. Enquire with management to determine whether security assessments are performed to identify vulnerabilities in both software and hardware assets on a periodic basis.</li> <li>2. Obtain and inspect the asset listing to determine all physical and virtual assets used in the iVote system are subject to vulnerability assessments.</li> <li>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.</li> <li>4. Where applicable, inspect evidence to determine whether remediation was performed to resolve vulnerabilities.</li> </ol>	No deviations noted.



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.	<ol style="list-style-type: none"> <li>1. Enquire with management to determine whether NSWEC has a defined and documented Patch Management Policy in place for the iVote system.</li> <li>2. Obtain and inspect NSWEC Patch Management policy to determine whether the policy is:               <ul style="list-style-type: none"> <li>• Approved by senior management;</li> <li>• Reviewed on a regular, predefined basis; and,</li> <li>• A requirement for known vulnerabilities to be patched is defined and documented.</li> </ul> </li> <li>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.</li> </ol>	No deviations noted.
20.04 	A mechanism is implemented to ensure only required software is installed on technology assisted voting components.	<ol style="list-style-type: none"> <li>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).</li> <li>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.</li> </ol>	<p><b>Limitation to testing:</b></p> <p>As the virtual machines used for iVote in the 2021 Local Government Elections were deployed in April 2021, prior to Deloitte's engagement with NSWEC in May 2021, we were unable to observe the implementation of a golden source image.</p>



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.	<ol style="list-style-type: none"> <li>1. Enquire with management to determine how patches are released to the production environment. Further understand: <ul style="list-style-type: none"> <li>• Where emergency patching is required, the process for approving and deploying changes to the production environment of the iVote system; and,</li> <li>• If a patch release process is documented.</li> </ul> </li> <li>2. Obtain and inspect NSWEC Patch Management policy to determine whether the policy provides governance around patch management processes.</li> <li>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.</li> </ol>	No deviations noted.
20.06 	A mechanism is in place to securely deploy updates/patches/config changes during a locked down state.	<ol style="list-style-type: none"> <li>1. Enquire with management to understand mechanisms in place to securely deploy updates/patches/config changes during a locked down state.</li> <li>2. Obtain and inspect the iVote Patch Management policy to determine whether the policy defines the process for deploying updates/patches/config changes during a locked down state.</li> <li>3. Obtain and inspect a list of changes made during lock down to determine total number of changes during locked state.</li> <li>4. For a sample of changes, test that: <ul style="list-style-type: none"> <li>• Changes were conducted in accordance with the Patch Management Policy; and,</li> <li>• Change has been tested and approved for release by appropriate management.</li> </ul> </li> </ol>	No deviations noted.




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.	<ol style="list-style-type: none"> <li>1. Enquire with management to determine which patch update/config correction mechanisms are disabled where required during lockdown of the system.</li> <li>2. Obtain and inspect the iVote Patch Management policy to determine whether the policy ensures that mechanisms to disable patch update / config correction mechanisms during lockdown of system are documented.</li> <li>3. Where applicable, 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.</li> <li>4. Where applicable, obtain evidence for a sample of services requiring to be patched during lockdown to determine whether:               <ul style="list-style-type: none"> <li>• Service has been approved to continue receiving patching during lockdown; and,</li> <li>• Service continues to receive updates during lockdown.</li> </ul> </li> <li>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 iVote Patch Management policy.</li> </ol>	No deviations noted.
20.08 	A mechanism is implemented to ensure that latest mobile app/application is used by the voters.	<ol style="list-style-type: none"> <li>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.</li> <li>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.</li> </ol>	No deviations noted.

**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.	<ol style="list-style-type: none"><li>1. Enquire with management to determine whether NSWEC has a defined and documented Network Security Policy in place for the iVote system.</li><li>2. Obtain and inspect NSWEC Network Security policy to determine whether the policy:<ul style="list-style-type: none"><li>• Is approved by senior management;</li><li>• Is reviewed on a regular, predefined basis; and,</li><li>• 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.</li></ul></li><li>3. Obtain and inspect screenshot of intranet or equivalent to determine if policy is available to all relevant stakeholders including key subcontractors.</li></ol>	No deviations noted.
21.02 	The network hosting technology assisted voting is segregated based on the defined security model to achieve defence in depth.	<ol style="list-style-type: none"><li>1. Enquire with management to determine whether the network hosting iVote is segregated based on the defined security model to achieve defence in depth.</li><li>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.</li><li>3. Obtain and inspect evidence to determine whether databases are hosted in a secure network zone which is not accessible from untrusted environments.</li></ol>	No deviations 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.	<ol style="list-style-type: none"> <li>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.</li> <li>2. Obtain and inspect NSWEC documentation to determine whether an application layer security system such as web application firewall is implemented.</li> <li>3. Obtain and inspect NSWEC documentation to determine whether a web application firewall is configured to detect and respond.</li> <li>4. Obtain and inspect vendor reports for Secure Logic, Secure Agility and AC3 to determine if NSWEC actively monitors the implementation of perimeter security controls.</li> </ol>	<p><b>The following deviation was noted:</b></p> <p>NSWEC did not receive daily security summaries on the operation of perimeter security controls by AC3 and Sliced Tech during the election period.</p>
21.04 	Network based Intrusion detection or prevention system are implemented for technology assisted voting.	<ol style="list-style-type: none"> <li>1. Enquire with management to determine whether intrusion detection and prevention systems are implemented for iVote components.</li> <li>2. Obtain and inspect the network architecture (or other) to determine whether IDS/IPS is implemented.</li> <li>3. Where applicable, obtain and inspect evidence to determine if IDS/IPS alerts were integrated with the SIEM Platform.</li> <li>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.</li> <li>5. Where applicable, obtain and inspect a sample of resolutions where automatic alerts have been raised within the SIEM.</li> </ol>	<p><b>The following deviation was noted:</b></p> <p>Vendors are responsible for the management and implementation and monitoring of network IDS/IPS. In the event of an incident, vendors are required to notify NSWEC in a timely manner.</p> <p>Although no network IDS/IPS events have been identified by the vendor, daily security summaries on the operation of perimeter security controls by AC3 and Sliced Tech were not provided to NSWEC during the election period.</p>


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.	<ol style="list-style-type: none"> <li>1. Enquire with management to understand how testing of security controls is conducted, as well as frequency and scope of testing.</li> <li>2. Obtain and inspect evidence of latest security incident response testing to determine: <ul style="list-style-type: none"> <li>• If security incident response testing produces reports/performance of red team exercises prior to go-live; and,</li> <li>• Security incident response testing covers all the key components of the iVote platform (registration, voting and assurance systems).</li> </ul> </li> <li>3. Where applicable, obtain and inspect documentation to determine security issues identified in the system reviews / exercises are tracked to resolution.</li> </ol>	No deviations noted.
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.	<ol style="list-style-type: none"> <li>1. Enquire with management to determine whether all network security applications and tools have the administrator console restricted to appropriate staff.</li> <li>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.</li> </ol>	<p><b>The following deviation was noted:</b></p> <p>All three environments (Assurance, Registration and Credential Management and Voting) do not have two factor authentication enabled on the firewalls.</p>
21.07 	Procedures must define the required network controls and configuration changes for system lockdown.	<ol style="list-style-type: none"> <li>1. Enquire with management to determine whether procedures define the required network controls and configuration changes for system lockdown.</li> <li>2. Obtain and inspect NSWEC documentation to ensure that a procedure defines the required network controls and configuration changes for system lockdown.</li> </ol>	<p><b>The following deviation was noted:</b></p> <p>NSWEC locked down all iVote environments on 8 November 2021 across the three vendors. Upon unlock on 26 November 2021 of the Assurance environment, it was noted that access to the Splunk Heavy Forwarder server 'SVRASPSPL2' had not been locked down. This server's function is to forward iVote system logs to Splunk.</p>





Control Reference	Control Activity	2021 Test Procedures	Results of Tests
21.08 	All voting systems are protected during the lockdown using host security system.	<ol style="list-style-type: none"> <li>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.</li> <li>2. Obtain and inspect NSWEC documentation to test if key systems of iVote are protected by Host Security Systems.</li> <li>3. Obtain and inspect evidence to show that an Intrusion Prevention System and/or an Intrusion Detection System is implemented.</li> </ol>	<p><b>The following deviation was noted:</b></p> <p>All voting system were not protected by host-based security systems.</p> <p><b>Mitigating control:</b> Voting systems are monitored for security events and incidents using Splunk.</p> <p>Refer to control 19.03.</p>
21.09 	Procedures and controls are implemented to ensure network performance and availability.	<ol style="list-style-type: none"> <li>1. Enquire with management to determine what procedures and controls are implemented to ensure network performance and availability.</li> <li>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.</li> </ol>	<p>No deviations noted.</p>
21.10 	The network components and traffic of the technology assisted voting systems are segregated.	<ol style="list-style-type: none"> <li>1. Enquire with management to understand the ownership of network components and traffic of the iVote system.</li> <li>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.</li> </ol>	<p>No deviations noted.</p>

**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.	No deviations noted.


Control Reference	Control Activity	2021 Test Procedures	Results of Tests
22.02 	Access to facilities is aligned with Protective Security Policy Framework (PSPF) zones requirements and restricted to approved NSWEC staff.	<p>1. Enquire with management to determine whether access to facilities is aligned with the Protective Security Policy Framework (PSPF) zones or other security requirements.</p> <p>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.</p> <p>3. For NSWEC sites holding critical technology assisted voting assets, obtain and inspect evidence to determine whether the following are implemented:</p> <ul style="list-style-type: none"> <li>• Access control measures at entrances to restrict and record access of employees;</li> <li>• 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,</li> </ul> <p>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 that CCTV logs are maintained for 90 days.</p>	<p><b>The following deviation was noted:</b></p> <p>NSWEC has not defined zone requirements in accordance with Protective Security Policy Framework (PSPF) for premises storing critical technology assisted voting assets (data centres and NSWEC offices). As a result, NSWEC did not actively monitor compliance to PSPF requirements.</p> <p><b>Mitigating controls:</b> All vendors hosting technology assisted voting environments are certified against IEC/ISO 27001:13 which includes physical security controls.</p> <p>Refer to control 22.01 for testing details.</p>



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.	<ol style="list-style-type: none"> <li>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.</li> <li>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.</li> <li>3. Obtain and inspect evidence to determine whether the offline system is stored in a Class B safe with multiple access restrictions.</li> <li>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).</li> </ol>	No deviations noted.


**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.	<ol style="list-style-type: none"> <li>1. Enquire with management to determine whether a Business Impact Analysis has been conducted for all critical iVote services.</li> <li>2. Obtain and inspect evidence of Business Impact Analysis for all key iVote systems and services to determine whether it includes: <ul style="list-style-type: none"> <li>• Business processes/activities/applications/ key staff;</li> <li>• The period of time operations can continue without each of its critical activities (MAO, RTO, RPOs for at least high risk processes); and,</li> <li>• The impact of a disruption over varying periods of time (e.g. legal, reputational, financial, environmental and regulatory) <ul style="list-style-type: none"> <li>○ Recovery requirements; and,</li> <li>○ Internal and external dependencies.</li> </ul> </li> </ul> </li> </ol>	No deviations noted.
23.02 	Business continuity procedures and recovery plans are documented, approved and tested.	<ol style="list-style-type: none"> <li>1. Enquire with management to determine whether business continuity procedures and recovery plans have been developed, reviewed and approved by appropriate management.</li> <li>2. Obtain and inspect the Disaster Recovery Plan (DRP) to determine whether: <ul style="list-style-type: none"> <li>• DRP exists;</li> <li>• DRP is reviewed on a periodic basis;</li> <li>• DRP is signed off by Board/Senior Management;</li> <li>• Version Control is established;</li> <li>• Roles and responsibilities of key stakeholders (including the users who are able to invoke/act the DRP) are defined;</li> <li>• DRP has been aligned to the BIA; and,</li> <li>• DRP establishes scope of coverage (applications, software and hardware).</li> <li>• DR testing is performed.</li> </ul> </li> </ol>	<p><b>The following deviation was noted:</b></p> <p>Review frequencies for both BCP and DR procedures and plans had not been formally established and as a result, the DR Plan tested for the 2021 Local Government Elections was last approved in 2019.</p>

Control Reference	Control Activity	2021 Test Procedures	Results of Tests
		<p>3. Obtain and inspect Business Continuity Plan (BCP) to determine whether:</p> <ul style="list-style-type: none"> <li>• BCP exists;</li> <li>• BCP is reviewed on a periodic basis;</li> <li>• BCP is signed off by Board/Senior Management;</li> <li>• Version Control is established;</li> <li>• Roles and responsibilities of key stakeholders (including the users who are able to invoke/act the BCP) are defined; and,</li> <li>• BCP establishes scope of coverage (applications, software and hardware).</li> </ul> <p>4. Obtain and inspect Business Continuity Plan (BCP) testing results to determine whether:</p> <ul style="list-style-type: none"> <li>• BCP has been tested periodically;</li> <li>• BCP is fit for purpose and provides guidance on how to resume operations in the event of disruption;</li> <li>• Staff are adequately aware of responsibilities when enacting the BCP; and,</li> <li>• NSWEC is able to successfully resume operations in the event of a disruption to all key services and systems.</li> </ul>	
<p>23.03</p> 	<p>Single point of failure of all components of technology assisted voting has been identified and disaster recovery capabilities established.</p>	<p>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.</p> <p>2. Obtain and inspect Single point of failures listing to determine whether:</p> <ul style="list-style-type: none"> <li>• Single point of failures have been identified; and,</li> <li>• Disaster recovery capabilities for these failures have been established.</li> </ul>	<p>No deviations noted.</p>



Control Reference	Control Activity	2021 Test Procedures	Results of Tests
23.04 	Backup of data and systems is performed during system lockdown in accordance with a formalised backup schedule aligned with defined RPO.	<ol style="list-style-type: none"> <li>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.</li> <li>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.</li> </ol>	<p><b>The following deviations were noted:</b></p> <p>One of six sampled backup summaries for Secure Logic was noted to include outdated backup information.</p> <p>Sliced Tech backup summaries were provided to NSWEC on 3 December 2021 and 7 December 2021. These two backup reports provided NSWEC a summary of all successful and unsuccessful backup jobs. Although these backup summaries were provided to NSWEC by Sliced Tech, consistent reporting of failed backups did not occur throughout the election period. As a result, during the lockdown period NSWEC were not aware of two recurring server backup failures in the Voting environment, the first instance of which was before election go-live.</p>
23.05 	Disaster Recovery for technology assisted voting is setup and implemented in a separate geo-redundant data centre.	<ol style="list-style-type: none"> <li>1. Enquire with management to determine whether DR Setup of iVote is implemented in a separate geo-redundant data centre.</li> <li>2. Obtain and inspect evidence to ensure that Production and DR data centres are geo-redundant.</li> </ol>	No deviations noted.



Control Reference	Control Activity	2021 Test Procedures	Results of Tests
23.06	 <p>DR testing and backup recovery is performed prior to go-live to ensure that controls implemented are operating effectively.</p>	<ol style="list-style-type: none"> <li>1. Enquire with management to obtain the frequency of testing, exercising and validation of the Disaster Recovery Plan (DRP).</li> <li>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.</li> <li>3. Obtain evidence of the testing performed on the DRP (including related artefacts) to determine whether: <ul style="list-style-type: none"> <li>• A consistent notification and escalation process is in place across the organisation (and plans), and this process is widely understood and followed;</li> <li>• A process to communicate Disaster Recovery testing to relevant sites is in place; and,</li> <li>• Disaster recovery processes are documented to provide guidance around procedures required to successfully restore key services and systems in the event of a disaster.</li> <li>• 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.</li> </ul> </li> <li>4. Enquire with management to determine: <ul style="list-style-type: none"> <li>• How often backups are scheduled;</li> <li>• How failed backups are rerun; and,</li> <li>• How often backup restorations are tested.</li> </ul> </li> <li>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.</li> <li>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.</li> </ol>	<p><b>The following deviation was noted:</b></p> <p>Although disaster recovery testing had been performed prior to the lead up of the 2021 Local Government Elections, backup recovery capabilities had not been assessed before go-live.</p>




**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
<p>24.01</p> 	<p>A documented incident management procedure or plan is maintained to identify and manage the following incidents during the election process:</p> <ol style="list-style-type: none"> <li>1. Security Incidents.</li> <li>2. IT Incidents.</li> </ol>	<ol style="list-style-type: none"> <li>1. Enquire with management to determine whether NSWEC has a defined and documented Incident Management Policy in place for the iVote system.</li> <li>2. Obtain and inspect the NSWEC Incident Management Policy to determine whether it is: <ul style="list-style-type: none"> <li>• Approved by senior management;</li> <li>• Is communicated to all relevant stakeholders including key subcontractors;</li> <li>• Reviewed on a regular, predefined basis; and,</li> <li>• Defines policies and processes for IT incidents and Security incidents: <ul style="list-style-type: none"> <li>○ Identification and classification as per defined criticality;</li> <li>○ Proper escalation procedure is in place to report the incident;</li> <li>○ Documented recovery procedure for commonly occurring incidents; and,</li> <li>○ Classification criteria for Root Cause Analysis/Problem management process.</li> </ul> </li> </ul> </li> </ol>	<p><b>The following deviation was noted:</b></p> <p>Although incident management documentation had been defined on the iVote confluence page, the incident management process used had not been formally reviewed and approved by Senior Management.</p> <p><b>Mitigating control:</b> All IT incidents are raised and resolved in a timely manner in line with defined procedures.</p> <p>Refer to control 24.02.</p>
<p>24.02</p> 	<p>Daily Incident record is prepared and reviewed based on the security activity monitoring during the system lockdown period.</p> <p>Additionally IT incidents are raised and resolved in a timely manner in accordance to defined procedures.</p>	<ol style="list-style-type: none"> <li>1. Enquire with management to determine whether a Daily Incident record is prepared based on the activity monitoring during the system lockdown period.</li> <li>2. For a sample of daily incident records during system lockdown, perform inspection to determine, in the event of an identified issue, if: <ul style="list-style-type: none"> <li>• A ticket was raised for Security incidents;</li> <li>• A ticket / report was shared internally for triaging and resolution; and,</li> <li>• The incidents were tracked through to resolution.</li> </ul> </li> </ol>	<p>No deviations noted.</p>

Control Reference	Control Activity	2021 Test Procedures	Results of Tests
24.03	 <p>Simulations are conducted prior to the elections to ensure that all involved stakeholders/parties understand their roles and responsibilities.</p>	<p>3. For a sample of IT incident records obtain during system lockdown, obtain and inspect evidence to determine if:</p> <ul style="list-style-type: none"> <li>• A ticket was raised for IT incidents;</li> <li>• A ticket / report was shared internally for triaging and resolution; and,</li> <li>• The incidents were tracked through to resolution.</li> </ul> <p>1. Enquire with management to determine if simulations are conducted prior to the Local Government Elections 2021. Furthermore, determine if simulations allow iVote staff to understand their roles and responsibilities in the management of security incidents.</p> <p>2. Obtain and inspect evidence of security incident response simulations to determine if security exercises have been conducted prior to the election.</p>	No deviations noted.
24.04	 <p>Post incident analysis for a security or IT incident are conducted and learnings identified and addressed.</p>	<p>1. Enquire with management and determine the requirements for Post Incident Reviews (PIR's) for closed security or incident tickets.</p> <p>2. Obtain and inspect the NSWEC Incident Management Procedure and determine if the requirement for PIRs for closed incidents is formally defined.</p> <p>3. Obtain and inspect the listing of all incident tickets within the period to determine the total number of incidents.</p> <p>4. For a sample of relevant incident tickets, perform inspection to determine whether:</p> <ul style="list-style-type: none"> <li>• A PIR review was conducted;</li> <li>• The PIR is attached the incident ticket; and,</li> <li>• PIR contains lessons identified and root cause analysis where applicable.</li> </ul>	No deviations noted.

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.	<ol style="list-style-type: none"> <li>1. Enquire with management and document if procedures and controls are implemented to ensure application and system performance and availability.</li> <li>2. Obtain and inspect evidence of availability monitoring to determine whether monitoring of system availability and performance is in place.</li> <li>3. Where applicable, obtain and inspect evidence of:               <ul style="list-style-type: none"> <li>• Alert / monitoring to notify NSWEC of degrading system performance and availability; and,</li> <li>• Tracking and remediation of issues causing degrading system performance and availability.</li> </ul> </li> </ol>	No deviations noted.

Section VI:  
Other Information Provided by  
NSW Electoral Commission



## Section VI: 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 V.

**Management’s response to deviations noted:**




The NSW Electoral Commissioner has made a determination that the iVote system will not be used for the State General Election scheduled for March 2023 or at any by-elections that may occur prior to this election. Remedies proposed for any deviations noted in this report will be applied as part of the preparation for any future use of the system.




Control Reference	Control Activity	Deviation Noted	Management Response
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.	<p><b>The following deviation was noted:</b></p> <p>The NSWEC Information Security Policy has not been reviewed according to the defined review frequency.</p>	<ul style="list-style-type: none"> <li>The finding is noted. A full review of the NSWEC Information Security Management System (ISMS) framework is currently underway. This review has delayed the review of individual policies within the ISMS. The revised ISMS will include an update to the Information Security Policy.</li> </ul>
3.01 	The candidate information on technology assisted voting is equivalent to the physical ballot.	<p><b>The following deviations were noted:</b></p> <p>The NSWEC Election Operations team conducted iVote Ballot Proof Checking sessions on 10 November 2021 and 11 November 2021. The following observation(s) were noted:</p> <ul style="list-style-type: none"> <li>Checked ballot papers were to be signed by two proofers before being marked as complete. For one sample, the ballot paper was marked as complete without the proofer signatures.</li> <li>Proofers were to check, on mobile and desktop versions of the iVote page, if:               <ol style="list-style-type: none"> <li>Instructions for iVote landing page were as described on the checklist and there were no typographical errors</li> <li>The number of candidates on the respective form was explicitly stated</li> </ol> </li> </ul>	<ul style="list-style-type: none"> <li>The finding is noted. In addition to the mitigating control noted in Section V, ballot proof checking is performed twice on each device. The omitted steps noted by Deloitte during the sampled ballot proof checking session were completed during the second checking ballot proof checking session.</li> </ul>



Control Reference	Control Activity	Deviation Noted	Management Response
		<ul style="list-style-type: none"> <li>iii. The Council and ward name was spelt correctly</li> <li>iv. The ballot paper draw order appeared the same as the physical ballot</li> <li>v. The spelling of the candidate, party and/or political affiliation was spelt correctly.</li> </ul> <p>For one sample, the ballot paper proofing did not check steps i, ii and iii above.</p> <ul style="list-style-type: none"> <li>• Proofers were required to notify supervisor staff of any discrepancies for the supervisor to triage and make a determination on the actions to take. For one sample, the proofers did not engage the supervisor for a discrepancy in the sample.</li> </ul>	
6.03	 <p>The authentication data is securely erased from technology assisted voting when it is no longer required.</p>	<p><b>Limitation to testing:</b></p> <p>Although policies and procedures to securely erase authentication, security and privacy data are defined, we were unable to check the secure erasure of authentication, security and privacy data as the deletion of data for the 2021 Local Government Elections will be conducted approximately 6 months after election day and therefore is outside the audit period.</p>	<ul style="list-style-type: none"> <li>• The finding is noted. A review of the erasure of data will be conducted at the end of the retention period for electoral information.</li> <li>• Management notes that the NSWEC is legislatively required to keep election material for between 6 and 18 months after a local government election event, depending on whether or not a council has resolved to conduct 'countback elections' to fill casual vacancies.</li> </ul>
7.01	 <p>An encryption policy is formally documented with approved encryption standards to be used.</p>	<p><b>The following deviation was noted:</b></p> <p>The Cryptographic Policy has not been reviewed according to the defined review frequency.</p>	<ul style="list-style-type: none"> <li>• The finding is noted. A full review of the NSWEC Information Security Management System (ISMS) framework is currently underway. This has delayed the review of individual policies within the ISMS. The revised ISMS will include an update to the Cryptographic Policy.</li> </ul>




Control Reference	Control Activity	Deviation Noted	Management Response
10.02 	<p>The voter must be made aware of the information collected from them during all phases of election (registration to results).</p>	<p><b>The following deviation was noted:</b></p> <p>Notice of Personally Identifiable Information (PII) retention was not explicitly highlighted for the registration stage. It is noted that the privacy policy was included as a link in the website footer; however, notice of the specific private information collected was not explicitly referenced during the registration process.</p>	<ul style="list-style-type: none"> <li>This issue is noted and will be addressed at future elections.</li> </ul>
10.04 	<p>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.</p>	<p><b>Limitation to testing:</b></p> <p>Although procedures are in place requiring deletion of data, we were unable to check the deletion of voter information from all the system components of iVote (including storage systems and backup systems) as the deletion of data for the 2021 Local Government Elections is conducted approximately 6 months after election day. This is outside of the audit period.</p>	<ul style="list-style-type: none"> <li>The limitation is noted. A review of the erasure of data will be conducted at the end of the retention period for electoral information.</li> <li>Management notes that the NSWEC is legislatively required to keep election material for between 6 and 18 months after a local government election event, depending on whether or not a council has resolved to conduct 'countback elections' to fill casual vacancies.</li> </ul>








Control Reference	Control Activity	Deviation Noted	Management Response
13.04 	Roles and responsibilities are documented and communicated to members of the election and admin boards.	<p><b>The following deviation was noted:</b></p> <p>Election operators did not confirm with two of five administrator board members that they had read the iVote Electoral &amp; Admin Board Member briefing document and were aware of their role, obligations, and responsibilities before they were provisioned a smart card.</p>	<ul style="list-style-type: none"> <li>The finding is noted. Management notes that all iVote Electoral &amp; Admin board members were provided with the briefing document that sets out their role, obligations and responsibilities 4 weeks prior to the iVote election period.</li> </ul>
15.01 	An access control policy based on the principle of need to know and need to use is documented.	<p><b>The following deviation was noted:</b></p> <p>The NSWEC Access Control Policy had not been reviewed according to the defined review frequency.</p>	<ul style="list-style-type: none"> <li>The finding is noted. Management notes that a full review of the NSWEC Information Security Management System (ISMS) framework is currently underway. The revised ISMS will include an update to the Access Control Policy.</li> </ul>
15.02 	A password policy aligned to the criticality of technology assisted voting is defined and implemented.	<p><b>The following deviations were noted:</b></p> <ul style="list-style-type: none"> <li>Password age was not configured to meet NSWEC Access Control Policy for Registration and Credential management servers of 72 days maximum (set to 999 days).</li> <li>Password age was not configured to meet NSWEC Access Control Policy for Voting system servers (configured to 90 days).</li> <li>Configuration of Assurance environments: <ul style="list-style-type: none"> <li>Password lockout threshold and duration was not configured to meet NSWEC Access Control Policy.</li> <li>Password history was not configured to meet NSWEC Access Control Policy.</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>The findings are noted. The password policies have been updated on all servers to ensure they are compliant with the access control policy. Management notes that all system administrator accounts were disabled during the local government elections, except for one account in each system for which a fresh password was set. Registration and Credential Management servers used MFA and do not rely solely on passwords security. This approach complies with the latest advice from the ACSC.</li> </ul>



Control Reference	Control Activity	Deviation Noted	Management Response
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.	<p><b>The following deviation was noted:</b></p> <p>A formal periodic user access review was not completed prior to the lead up of the 2021 Local Government Elections per requirements stipulated in the NSWEC Access Control Policy.</p>	<ul style="list-style-type: none"> <li>The finding is noted. Management acknowledges that a periodic user access review has not been completed per the Access Control Policy. A user access review of the iVote Web Application occurred during Election Build in Nov 21 and Active Directory domain level user access reviews occurred as part of the Upper Hunter final environment unlock in May 21. In response to this finding, a quarterly review schedule has been established in accordance with the Access Control Policy.</li> </ul>
16.01 	Change control procedures are followed for all changes to the production environment.	<p><b>The following deviation was noted:</b></p> <p>The ICT Technical Change Management Policy had not been reviewed according to the defined review frequency.</p> <p>Although the development and production environments were logically separated for Registration and Credential Management systems, two developers were identified to have access to both environments. It is noted that testing of the change management samples (general and emergency changes) did not identify any unapproved changes being deployed.</p>	<ul style="list-style-type: none"> <li>The finding is noted. Management notes that, although the ICT Technical Change Management Policy was reviewed and approved in December 2019, the version published in the Policy Library has not been updated to reflect this review. This gap will be addressed.</li> </ul>
16.02 	A formal process to conduct emergency changes in production is implemented and approved.	<p><b>The following deviations were noted:</b></p> <p>The unlock event on 12 November 2021 could not be linked to a change ticket.</p>	<ul style="list-style-type: none"> <li>The finding is noted. Whilst the unlock on 12 November did not have a change ticket, it was the subject of an extensive risk management process and consultation with Director Cyber Security, system owners and the Election Operations Group. It was a planned event on the election calendar.</li> </ul>



Control Reference	Control Activity	Deviation Noted	Management Response
		No documented evidence of approval could be provided for one of five sampled emergency changes as it was verbally approved.	<ul style="list-style-type: none"> <li>Approval for Emergency Change #1247 was verbally provided but not formally recorded.</li> </ul>
17.01 	Developers are trained on secure development practices.	<p><b>The following deviation was noted:</b></p> <p>Official training for secure development practices had not been established and completed for NSWEC Registration &amp; Credential Management system developers.</p>	<ul style="list-style-type: none"> <li>The finding is noted. While Management notes that formal training is not provided to developers upon engagement, developers are introduced to NSWEC Software Development Standards that include secure development guidelines as part of their induction. The developers engaged to work on iVote systems have prior training and skills in secure development practices and coaching on secure development is included as part of the peer review process included in our software development process.</li> </ul>
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.	<p><b>The following deviations were noted:</b></p> <p>Evidence of Sliced Tech anti-malware reporting could not be sighted for 2 of 6 sampled dates (23 November 2021 and 27 November 2021).</p> <p>AC3 anti-malware reporting was not provided to NSWEC between the period of 22 November 2021 – 24 November 2021 inclusive. As a result, evidence of AC3 anti-malware reporting could not be sighted for 1 of 6 sampled dates (23 November 2021).</p> <p>Upon inspection of the Secure Logic antivirus coverage, it was noted that 12 of 33 production virtual machines in the Registration / Credential Management environment were not included as part of the daily scan.</p>	<ul style="list-style-type: none"> <li>The finding is noted. The relevant systems were being monitored by the provider's respective Cyber teams and if any alerts occurred there would be an immediate direct call to NSWEC.</li> <li>Sliced Tech supplied reports as periodic summaries (including the sampled dates that were not sighted) retrospectively, and no alerts occurred.</li> <li>AC3 missed three reports early in the election period and supplied the missing reports subsequently. No alerts occurred.</li> <li>Secure Logic antivirus coverage is acknowledged as a deviation. These were newly deployed servers that were not externally accessible and initially there was no client available for those machines. The risk was mitigated by access to these servers requiring first to pass through a monitored system. No alerts occurred. This coverage has now been rectified.</li> </ul>

Control Reference	Control Activity	Deviation Noted	Management Response
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.	<p><b>The following deviation was noted:</b></p> <p>Although Splunk has been implemented to monitor security events such as administrative functions and escalated privileges, evidence could not be provided to determine if Splunk logs contained key event information such as:</p> <ul style="list-style-type: none"> <li>- Timestamp</li> <li>- Host details</li> <li>- Identity of process initiating the event</li> <li>- Detailed description of the event.</li> </ul>	<ul style="list-style-type: none"> <li>• The finding is noted. Due to competing election activities, control evidence could not be provided before Deloitte's reporting deadlines. NSWEC confirms that event information (including host details, timestamp and event description) is captured and processed within Splunk.</li> </ul>
20.04 	A mechanism is implemented to ensure only required software is installed on technology assisted voting components.	<p><b>Limitation to testing:</b></p> <p>As the virtual machines used for iVote in the 2021 Local Government Elections were deployed in April 2021, prior to Deloitte's engagement with NSWEC in May 2021, we were unable to observe the implementation of a golden source image.</p>	<ul style="list-style-type: none"> <li>• The limitation is noted. A means of testing this control will be developed.</li> </ul>
21.03 	Perimeter security controls are defined and implemented to protect technology assisted voting.	<p><b>The following deviation was noted:</b></p> <p>NSWEC did not receive daily security summaries on the operation of perimeter security controls by AC3 and Sliced Tech during the election period.</p>	<ul style="list-style-type: none"> <li>• This finding is noted.</li> <li>• Management notes that Sliced Tech summaries were provided as periodic summaries, not daily summaries.</li> <li>• AC3 logs were provided live and not summarised.</li> <li>• Any Cyber incidents detected by all three providers are notified immediately via phone and do not wait for security summary reports.</li> </ul>

Control Reference	Control Activity	Deviation Noted	Management Response
21.04 	Network based Intrusion detection or prevention system are implemented for technology assisted voting.	<p><b>The following deviation was noted:</b></p> <p>Vendors are responsible for the management and implementation and monitoring of network IDS/IPS. In the event of an incident, vendors are required to notify NSWEC in a timely manner.</p> <p>Although no network IDS/IPS events have been identified by the vendor, daily security summaries on the operation of perimeter security controls by AC3 and Sliced Tech were not provided to NSWEC during the election period.</p>	<ul style="list-style-type: none"> <li>• This finding is noted.</li> <li>• Management notes that Sliced Tech summaries were provided as periodic summaries, not daily summaries.</li> <li>• AC3 logs were provided live and not summarised.</li> <li>• Any cyber incidents detected by all three providers are notified immediately via phone and do not wait for a security summary report.</li> </ul>
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.	<p><b>The following deviation was noted:</b></p> <p>All three environments (Assurance, Registration and Credential Management and Voting) do not have two factor authentication enabled on the firewalls.</p>	<ul style="list-style-type: none"> <li>• The finding is noted. Management notes that Two Factor Authentication was available and used on servers, bastion hosts and the voting VPN gateway.</li> <li>• In response to this finding, the firewall multi-factor authentication upgrade has been requested from each vendor.</li> </ul>

Control Reference	Control Activity	Deviation Noted	Management Response
21.07 	Procedures must define the required network controls and configuration changes for system lockdown.	<b>The following deviation was noted:</b>  NSWEC locked down all iVote environments on 8 November 2021 across the three vendors. Upon unlock on 26 November 2021 of the Assurance environment, it was noted that access to the Splunk Heavy Forwarder server 'SVRASPSPL2' had not been locked down. This server's function is to forward iVote system logs to Splunk.	<ul style="list-style-type: none"> <li>The finding is noted. Management notes that when this was discovered the system was checked and it was confirmed that no logins were recorded on the machine in question during the period. The server was immediately locked down correctly.</li> <li>A review and enhancement of the assurance process with a documented checklist that affirms all servers were locked down correctly will be conducted.</li> </ul>
21.08 	All voting systems are protected during the lockdown using host security system.	<b>The following deviation was noted:</b>  All voting system were not protected by host-based security systems.	<ul style="list-style-type: none"> <li>The finding is noted. Management acknowledges that not all voting virtual machines were protected by host-based Intrusion Detection Systems (IDS), although they had host-based anti-malware. It should also be noted that they had Network IDS with SSL interception and that the logs from all those machines were being collected via Splunk.</li> </ul>
22.02 	Access to facilities is aligned with Protective Security Policy Framework (PSPF) zones requirements and restricted to approved NSWEC staff.	<b>The following deviation was noted:</b>  NSWEC has not defined zone requirements in accordance with Protective Security Policy Framework (PSPF) for premises storing critical technology assisted voting assets (data centres and NSWEC offices). As a result, NSWEC did not actively monitor compliance to PSPF requirements.	<ul style="list-style-type: none"> <li>The finding is noted. Management notes that premises used met PSPF entity Zone 2 requirements and containers were SCEC B rated however there is a documentation gap in the zone definitions.</li> </ul>

Control Reference	Control Activity	Deviation Noted	Management Response
23.02 	Business continuity procedures and recovery plans are documented, approved and tested.	<p><b>The following deviation was noted:</b></p> <p>Review frequencies for both BCP and DR procedures and plans had not been formally established and as a result, the DR Plan tested for the 2021 Local Government Elections was last approved in 2019.</p>	<ul style="list-style-type: none"> <li>The finding is noted. Management notes that the BCP procedures and plan was reviewed and signed off by the project owner. The DR plan from 2019 being used for iVote at the 2021 local government elections, was endorsed by the Director, Election Innovation prior to the elections, although the plan review outcome was not formally documented. Management acknowledges there is an opportunity to improve policy revision processes.</li> </ul>
23.04 	Backup of data and systems is performed during system lockdown in accordance with a formalised backup schedule aligned with defined RPO.	<p><b>The following deviations were noted:</b></p> <p>One of six sampled backup summaries for Secure Logic was noted to include outdated backup information.</p> <p>Sliced Tech backup summaries were provided to NSWEC on 3 December 2021 and 7 December 2021. These two backup reports provided NSWEC a summary of all successful and unsuccessful backup jobs. Although these backup summaries were provided to NSWEC by Sliced Tech, consistent reporting of failed backups did not occur throughout the election period. As a result, during the lockdown period NSWEC were not aware of two recurring server backup failures in the Voting environment, the first instance of which was before election go-live.</p>	<ul style="list-style-type: none"> <li>The finding is noted. The Secure Logic daily reports do report on backups, although one report during the reporting period was erroneous and had to be corrected after the period.</li> <li>The Sliced Tech reporting was provided as a periodic summary.</li> <li>The backup failure that occurred was communicated by Sliced Tech immediately via phone and affected only two whole-machine backups not the data backups for those machines. This was unable to be rectified in the election period due to the system being locked down. This was subsequently rectified after the election.</li> <li>Other communication from Sliced Tech such as disk capacity issues were communicated by phone and not via a daily summary. Tracking of daily summaries as a process improvement is acknowledged.</li> </ul>

Control Reference	Control Activity	Deviation Noted	Management Response
23.06 	DR testing and backup recovery is performed prior to go-live to ensure that controls implemented are operating effectively.	<p><b>The following deviation was noted:</b></p> <p>Although disaster recovery testing had been performed prior to the lead up of the 2021 Local Government Elections, backup recovery capabilities had not been assessed before go-live.</p>	<ul style="list-style-type: none"> <li>The finding is noted. Management notes that backup recovery was tested in the lead up to the Upper Hunter by-election for Secure Logic, plus early in 2021 for AC3 and Sliced Tech. Management will revise the election go-live checklists to ensure backup restoration testing is required for go-live.</li> </ul>
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.	<p><b>The following deviation was noted:</b></p> <p>Although incident management documentation had been defined on the iVote confluence page, the incident management process used had not been formally reviewed and approved by Senior Management.</p>	<ul style="list-style-type: none"> <li>The finding is noted. Management notes that the iVote incident management process and documentation had been reviewed and agreed at the operational level, and that all parties followed the process when raising incidents during the elections. Procedures will be updated to ensure formal sign-off occurs and is documented for all future changes to the incident management process.</li> </ul>



