Deloitte.


**NSW iVote Review**

Testing Timeline and Control Objectives

# Section I: Background and Timing

# Section I: Background and Timing

## Overview

The iVote system is a remote electronic voting system, enabled by NSW State legislation to provide technology-assisted voting to eligible electors.

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

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

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

As at July 2021, the iVote system has been previously used as a remote electronic voting system for the following elections:

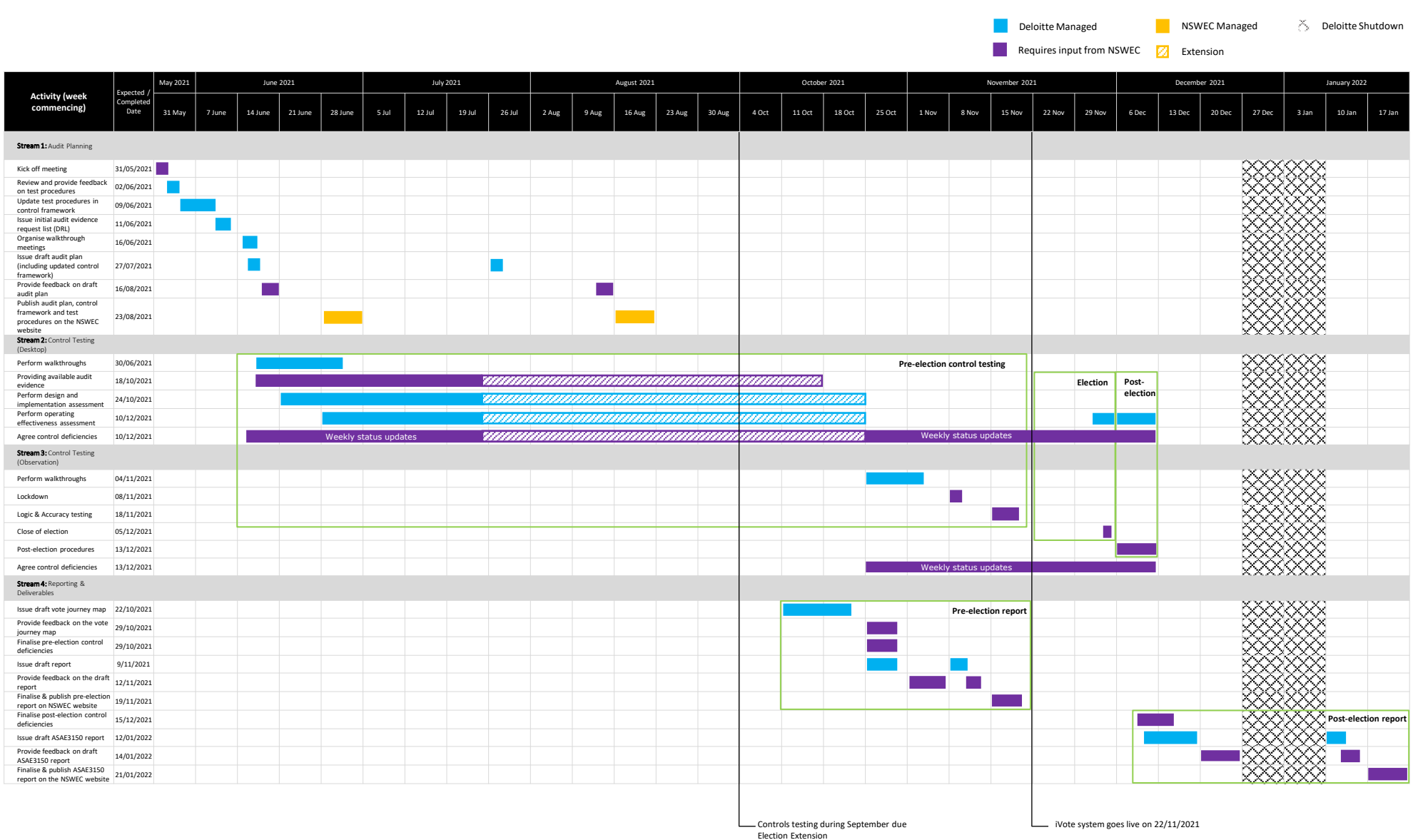
- 2011 NSW State General Election;
- 2015 NSW State General Election;
- 2019 NSW State General Election; and,
- 11 NSW State by-elections from November 2011 to May 2021.

## Scope

Independent auditing of technology assisted voting is required by Section 156 of the NSW Electoral Act 2017 and by Section 333G of the Local Government (General) Amendment Regulation 2021.
The NSW Electoral Commissioner has engaged Deloitte as an independent auditor to assist in independently validating the iVote control environment prior to and during the NSW Local Government Elections in 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 II of this document, as well as the Electoral Council of Australia and New Zealand (ECANZ). Testing against this control framework will provide the basis of Deloitte's opinion on the design and operating effectiveness of controls in accordance with the defined test procedures. Refer to Section II for further information.

Please refer to the below plan for indicative timings of the independent validation of the iVote control environment for the 2021 Local Government Elections and Appendix A for an accessible version of this timeline.


Deloitte Managed
NSWEC Managed
Deloitte Shutdown
Requires input from NSWEC
Extension
Activity (week commencing)
Expected / Completed Date
May 2021
June 2021
July 2021
August 2021
October 2021
November 2021
December 2021
January 2022
31 May
7 June
14 June
21 June
28 June
5 Jul
12 Jul
19 Jul
26 Jul
2 Aug
9 Aug
16 Aug
23 Aug
30 Aug
4 Oct
11 Oct
18 Oct
25 Oct
1 Nov
8 Nov
15 Nov
22 Nov
29 Nov
6 Dec
13 Dec
20 Dec
27 Dec
3 Jan
10 Jan
17 Jan
Stream 1: Audit Planning
Kick off meeting 31/05/2021
Review and provide feedback on test procedures 02/06/2021
Update test procedures in control framework 09/06/2021
Issue initial audit evidence request list (DRL) 11/06/2021
Organise walkthrough meetings 16/06/2021
Issue draft audit plan (including updated control framework) 27/07/2021
Provide feedback on draft audit plan 16/08/2021
Publish audit plan, control framework and test procedures on the NSWEC website 23/08/2021
Stream 2: Control Testing (Desktop)
Perform walkthroughs 30/06/2021
Providing available audit evidence 18/10/2021
Perform design and implementation assessment 24/10/2021
Perform operating effectiveness assessment 10/12/2021
Agree control deficiencies 10/12/2021
Pre-election control testing
Election
Post-election
Weekly status updates
Weekly status updates
Stream 3: Control Testing (Observation)
Perform walkthroughs 04/11/2021
Lockdown 08/11/2021
Logic & Accuracy testing 18/11/2021
Close of election 05/12/2021
Post-election procedures 13/12/2021
Agree control deficiencies 13/12/2021
Weekly status updates
Stream 4: Reporting & Deliverables
Issue draft vote journey map 22/10/2021
Provide feedback on the vote journey map 29/10/2021
Finalise pre-election control deficiencies 29/10/2021
Issue draft report 9/11/2021
Provide feedback on the draft report 12/11/2021
Finalise & publish pre-election report on NSWEC website 19/11/2021
Finalise post-election control deficiencies 15/12/2021
Issue draft ASAE3150 report 12/01/2022
Provide feedback on draft ASAE3150 report 14/01/2022
Finalise & publish ASAE3150 report on the NSWEC website 21/01/2022
Pre-election report
Post-election report
Controls testing during September due Election Extension
iVote system goes live on 22/11/2021

# Section II:
# NSWEC's iVote Control Objectives

# Section II: NSWEC's iVote Control Objectives

### 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 detailed Control Assessment Framework published on the NSWEC Website (the 'Framework').

The below control objectives will be assessed in relation to the 2021 NSW Local Government Election as part of Deloitte's Independent Audit.

**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 |
|---|---|
| 1.01 | NSWEC have a defined, documented, periodically reviewed and approved information security policy for managing security. The policy is communicated to all relevant stakeholders including key suppliers. |
| 1.02 | Appropriate standards, guidelines, and procedures are in place to manage information security in accordance with the information security policy. |
| 1.03 | A risk register is maintained and regularly reviewed which captures identified risks to technology assisted voting. |
| 1.04 | A risk mitigation program is established to identify and mitigate the risks identified in the risk register. |

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

| Control Reference | Control Activity |
|---|---|
| 2.01 | The voter is informed about how to accurately use technology assisted voting. |
| 2.02 | Technology assisted voting provides feedback on the confirmation of valid/invalid options and on successful completion of voting procedure. |
| 2.03 | Voters are able to test/perform a demonstration to familiarise themselves with the system. |

**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 |
|---|---|
| 3.01 | The candidate information on technology assisted voting is equivalent to the physical ballot. |
| 3.02 | No influential language is used which may influence voters towards/against a particular candidate. |
| 3.03 | The technology assisted voting platform is designed to prevent influencing voters into making a specific choice when casting a vote. |
| 3.04 | Technology assisted voting allows users to cast their vote without providing a preference. |

**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 |
|---|---|
| 4.01 | Identity of the voter must be authenticated during the registration process. |
| 4.02 | Technology assisted voting allows only voters who have successfully completed the registration process for voting to log in and cast a vote. |
| 4.03 | Voters who have changed their vote/re-voted have their previous vote discarded. |
| 4.04 | Prior to the final result, the voting system identifies votes which are invalid, duplicated or generated due to an error. |
| 4.05 | Prior to the final results, the number of votes from the voting system and the assurance system are compared and validated. The final result of technology assisted voting must be clearly established. |

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

| Control Reference | Control Activity |
|---|---|
| 5.01 | Technology assisted voting will enable all voters including persons with disabilities to vote. |
| 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. |
| 5.03 | A mechanism is established for voters to speak to person(s) about using technology assisted voting and ask their queries. |

**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 |
|---|---|
| 6.01 | Each registered voter is provided with unique credentials to access all components of technology assisted voting and voters are allowed to setup their own PIN/Passwords to access the voting system after successful registration |
| 6.02 | In order to reset the PIN/Password and generate new credentials users must re-verify their identity. |
| 6.03 | The authentication data is securely erased from technology assisted voting when it is no longer required. |

**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 |
|---|---|
| 7.01 | An encryption policy is formally documented with approved encryption standards to be used. |
| 7.02 | Cryptographic key management life cycle is documented and includes:<br>- Key generation<br>- Storage, distribution and installation<br>- Key usage and rotation<br>- Backup and recovery<br>- Key revocation and suspension<br>- Secure destruction. |
| 7.03 | A quorum of electoral officers is required for the decryption of votes prior to the end of the election.<br><br>A private key is shared between members to prevent a single electoral officer from decrypting the votes. |
| 7.04 | Mechanisms are implemented to ensure integrity of the votes captured from the voter. |
| 7.05 | Scrutineers are invited to the decryption process after the end of the elections and votes are only decrypted after the close of voting. |
| 7.06 | iVote numbers and passwords are not stored in the voting or assurance system. |
| 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. |
| 7.08 | Backups are protected using encryption and are stored in an offsite location. |
| 7.09 | Encryption mechanism are implemented for the verification system to ensure that voter can decrypt and read only their vote. |

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

| Control Reference | Control Activity |
|---|---|
| 8.01 | A voter is able to verify that their vote has been accurately entered into electronic ballot box without any alteration. |
| 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. |

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

| Control Reference | Control Activity |
|---|---|
| 9.01 | Voter's personal identifiable information (PII) is kept separate from the vote. |
| 9.02 | Procedures are defined to prevent the link between the voter and the voter's preference to be established. |
| 9.03 | A procedure is defined and executed for a technically competent and independent individual to check proofs of the integrity of the mixing and shuffling of votes and decryption of the votes after the election. |

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

| Control Reference | Control Activity |
|---|---|
| 10.01 | A Privacy Impact Assessment (PIA) is conducted, capturing a data inventory of all PI data elements (in any form, whether electronic or paper) and their locations across applications, systems, processes, media and data repositories. The PIA also captures the purpose of the data collected and retention period. |
| 10.02 | The voter must be made aware of the information collected from them during all phases of election (registration to results). |
| 10.03 | Technology assisted voting captures only the information described in the Privacy Impact Assessment. |
| 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. |
| 10.05 | Limit the usage of voter identifiable information data collected by technology assisted voting during and after elections to only information required to conduct the election. |
| 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) |

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

| Control Reference | Control Activity |
|---|---|
| 11.01 | Standard data exchange and data formats are used in the voting and assurance system and avoid the use of proprietary frameworks. |
| 11.02 | Standard publicly available encryption algorithms are used and use of proprietary algorithms is avoided. |

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

| Control Reference | Control Activity |
|---|---|
| 12.01 | The usage of removable media for elections during the lockdown is documented and restricted. |

**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 |
|---|---|
| 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. |
| 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. |
| 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. |
| 13.04 | Roles and responsibilities are documented and communicated to members of the election and admin boards. |
| 13.05 | NSWEC has formal agreements with all third parties including statements of responsibilities such as;<br>- compliance to all applicable regulatory requirements;<br>- adherence to NSWEC's policies and procedures, including the protection of voter's information. |

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

| Control Reference | Control Activity |
|---|---|
| 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. |
| 14.02 | Logic & Accuracy (L&A) testing is conducted to confirm the iVote system functions in line with requirements. |

**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 |
|---|---|
| 15.01 | An access control policy based on the principle of need to know and need to use is documented. |
| 15.02 | A password policy aligned to the criticality of technology assisted voting is defined and implemented. |
| 15.03 | During lockdown, a list of approved users to be enabled is documented, to ensure that only approved system accounts remain enabled. |
| 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. |
| 15.05 | Users that no longer require physical and/or logical access are removed from systems in a timely manner. |
| 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. |

**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 |
|---|---|
| 16.01 | Change control procedures are followed for all changes to the production environment. |
| 16.02 | Ensure that a formal process to conduct emergency changes in production is implemented and approved. |
| 16.03 | Development, testing and production environment are logically separated. |
| 16.04 | Formal software development life cycle management includes maintenance of source code repositories per production environment. |

**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 |
|---|---|
| 17.01 | Developers are trained on secure development practices. |
| 17.02 | Security testing and mitigation is performed for all components of technology assisted voting in production environments prior to go-live. |
| 17.03 | Security testing and mitigation is performed for all infrastructure components of the technology assisted voting platform prior to go-live. |
| 17.04 | The build/deploy of the system in production is validated. |
| 17.05 | NSWEC provide mechanisms for review and evaluation of the source code for sensitive parts of the technology assisted voting system. |
| 17.06 | Scrutineers are invited to review and observe select iVote processes in accordance to Section 158 of the Electoral Act 2017. |

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

| Control Reference | Control Activity |
|---|---|
| 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. |

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

| Control Reference | Control Activity |
|---|---|
| 19.01 | A log management system (LMS) is implemented for logging of security events. |
| 19.02 | Log files are immutable for vote casting and cannot be overwritten. |
| 19.03 | Security incident and event management (SIEM) is implemented for real time monitoring of events and management of security incidents. |
| 19.04 | Security events logged into log management and security incident management system must capture the key events and detailed description in the logs. |
| 19.05 | Sensitive information related to voter and votes is not captured in the logs. |
| 19.06 | All technology assisted voting components is synced with a network time protocol to ensure integrity of logs. |

**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 |
|---|---|
| 20.01 | All the assets utilised in the voting system are identified and an inventory is maintained with relevant details, and is reviewed on a regular basis. |
| 20.02 | Vulnerability security assessments are performed to identify vulnerabilities in software and hardware. |
| 20.03 | The patch management policy is implemented to ensure that all known vulnerabilities are patched. |
| 20.04 | A mechanism is implemented to ensure only required software is installed on technology assisted voting components. |
| 20.05 | All updates and patches are reviewed and tested in non-production environments before deployment into the production. |
| 20.06 | A mechanism is in place to securely deploy updates/patches/config changes during a locked down state. |
| 20.07 | Patch update/config correction mechanisms are disabled where required during lockdown of the system. |
| 20.08 | A mechanism is implemented to ensure that latest mobile app/application is used by the voters. |

**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 |
|---|---|
| 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. |
| 21.02 | The network hosting technology assisted voting is segregated based on the defined security model to achieve defence in depth. |
| 21.03 | Perimeter security controls are defined and implemented to protect technology assisted voting. |
| 21.04 | Network based Intrusion detection or prevention system are implemented for technology assisted voting. |
| 21.05 | Network security controls are tested through a combination of system reviews and red team exercises. |
| 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. |
| 21.07 | Procedures must define the required network controls and configuration changes for system lockdown. |
| 21.08 | All voting systems are protected during the lockdown using host security system. |
| 21.09 | Procedures and controls are implemented to ensure network performance and availability. |
| 21.10 | The network components and traffic of the technology assisted voting systems are segregated. |

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

| Control Reference | Control Activity |
|---|---|
| 22.01 | Management has developed a process to define, monitor, and evaluate third-party physical production environment protection requirements across all third party providers. |
| 22.02 | Access to facilities is aligned with Protective Security Policy Framework (PSPF) zones requirements and restricted to approved NSWEC staff. |
| 22.03 | Environmental controls are implemented at data centre and office location for protection of technology assisted voting assets. |

**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 |
|---|---|
| 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. |
| 23.02 | Business continuity procedures and recovery plans are documented, approved and tested. |
| 23.03 | Single points of failure of all components of technology assisted voting have been identified and disaster recovery capabilities established. |
| 23.04 | Backup of data and systems is performed during system lockdown in accordance with a formalised backup schedule aligned with defined RPO. |
| 23.05 | Disaster Recovery for technology assisted voting is setup and implemented in a separate geo-redundant data centre. |
| 23.06 | DR testing and backup recovery is performed prior to go-live to ensure that controls implemented are operating effectively. |

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

| Control Reference | Control Activity |
|---|---|
| 24.01 | A documented incident management procedure or plan is maintained to identify and manage the following incidents during the election process:<br>1. Security Incidents.<br>2. IT Incidents. |
| 24.02 | Daily Incident records are prepared and reviewed based on the activity monitoring during the system lockdown period. |
| 24.03 | Simulations and training are conducted prior to the elections to ensure that all involved stakeholders/parties understand their roles and responsibilities. |
| 24.04 | Post incident analysis for a security or IT incident are conducted and learnings identified and addressed. |
| 24.05 | Procedures and controls are implemented to ensure application and system performance and availability. |

# Appendix A: Accessible Timeline

# Appendix A: Accessible Timeline

**Timeline in Text**

| Stage | Stream | Activity | Expected Date |
|---|---|---|---|
| 1 | Audit Planning | Kick off meeting | 31/05/2021 |
| | | Review and provide feedback on test procedures | 02/06/2021 |
| | | Update test procedures in control framework | 09/06/2021 |
| | | Issue initial audit evidence request list (DRL) | 11/06/2021 |
| | | Organise walkthrough meetings | 16/06/2021 |
| | | Issue draft audit plan (including updated control framework) | 27/07/2021 |
| | | Provide feedback on draft audit plan | 16/08/2021 |
| | | Publish audit plan, control framework and test procedures on the NSWEC website | 23/08/2021 |
| 2 | Control Testing (Desktop) | Perform walkthroughs | 30/06/2021 |
| | | Providing available audit evidence | 18/10/2021 |
| | | Perform design and implementation assessment | 24/10/2021 |
| | | Perform operating effectiveness assessment | 10/12/2021 |
| | | Agree control deficiencies | 10/12/2021 |
| 3 | Control Testing (Observation) | Perform walkthroughs | 04/11/2021 |
| | | Lockdown | 08/11/2021 |
| | | Logic & Accuracy testing | 18/11/2021 |
| | | Close of election | 05/12/2021 |
| | | Post-election procedures | 13/12/2021 |
| | | Agree control deficiencies | 13/12/2021 |
| 4 | Reporting and Deliverables | Issue draft vote journey map | 22/10/2021 |
| | | Provide feedback on the vote journey map | 29/10/2021 |
| | | Finalise pre-election control deficiencies | 29/10/2021 |
| | | Issue draft report | 9/11/2021 |
| | | Provide feedback on the draft report | 12/11/2021 |
| | | Finalise & publish pre-election report on NSWEC website | 19/11/2021 |
| | | Finalise post-election control deficiencies | 15/12/2021 |
| | | Issue draft ASAE3150 report | 12/01/2022 |
| | | Provide feedback on draft ASAE3150 report | 14/01/2022 |
| | | Finalise & publish ASAE3150 report on the NSWEC website | 21/01/2022 |