NSW Electoral Commission

Post-Election Report – Specified Procedures in relation to the online and telephone voting system ("iVote") for 2019 NSW State Election

June 2019

NSW
Electoral
Commission

Disclaimer

This Post-Election Report ("deliverable") has been prepared by PricewaterhouseCoopers ABN 52 780 433 757 ("PwC") pursuant to an agreement for the procurement of specified procedures in relation to iVote for the 2019 NSW State general election between PwC and the NSWEC dated 1 February 2019.

This deliverable is based on information made available to PwC up to the date of this deliverable and PwC reserves the right to amend its opinions, if necessary, based on factual information that comes to PwC's attention after that date. For the purposes of preparing this deliverable, reliance has been placed on information and instructions provided to PwC. PwC has not sought to verify the accuracy or completeness of the information made available.

This deliverable has been prepared for the sole use of NSWEC, and is subject to the limitations, exclusions and qualifications described in it and in PwC's agreement with NSWEC. PwC, its partners, its agents and servants specifically deny any liability whatsoever to any other party who may use or rely on the whole, or any part, of this deliverable or to the parties to whom it is addressed for the use, whether in whole or in part, for any purpose other than those agreed with PwC. This deliverable should not be used for any other purpose without PwC's prior written consent.

PwC does not accept any duty of care (whether in contract, tort (including negligence) or otherwise) to any person other than NSWEC, and will not be responsible for any loss suffered by a third party who relies upon this deliverable.

It is the responsibility of NSWEC to determine whether PwC's engagement satisfies NSWEC's obligations to appoint an independent auditor to perform certain services under section 156 of the Electoral Act 2017 (NSW) and any other requirements in that Act applicable to the appointment or role of the independent auditor.

Liability limited by a scheme approved under Professional Standards Legislation.

Contents

Section	Page
Introduction	4
Executive Summary	8
Detailed findings	17
Summary of findings from pre-election report	46
Appendix A – Control Assessment Framework	48
Appendix B – iVote process overview	54
Appendix C – Incident Details	57
Appendix D – Incidental Unlock Procedures	61
Appendix E – System Overview	63
Appendix F – Security Systems Overview	65
Appendix G – NSWEC Risk Assessment Matrix	68
Appendix I – Project Timelines	71
Appendix J – Glossary	73

Introduction

1

Introduction (1/3)

Background

The NSW Electoral Commission's online and telephone voting platform, iVote, was first used in the 2011 state general election, and has been subsequently used in the 2015 state general election and a number of by-elections. The iVote platform has three key components - the registration and credential management system, the voting system and the verification system.

Prior to the 2019 NSW State Election, the NSW Electoral Commission ("NSWEC") undertook a significant refresh and uplift of the iVote. A key driver for this was to increase transparency to the voters and the political party scrutineers. Additionally, Section 156 of the Electoral Act 2017 requires the NSWEC to appoint an independent auditor to:

- conduct audits of the information technology used under the procedures approved in accordance with section 155 of the Act; and
- provide the results of those audits to the NSWEC:
  - at least 7 days before voting commences in the Election ("pre-election Report"); and
  - within 60 days after the return of the writs for the Election ("post-election Report").

In order to drive transparency and meet the requirement of the Electoral Act 2017, the NSWEC has developed a control assessment framework which draws guidance from the Electoral Council of Australia and New Zealand ("ECANZ") principles and a number of best practice processes to help protect the security and integrity of the system. The best practice frameworks used to create the controls include:

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

To assist the Electoral Commissioner fulfil their obligation to engage an independent person under section 156 of the Electoral Act 2017, the NSWEC has engaged PwC to perform the procedures specified in the Control Assessment Framework in relation to iVote.

Introduction (2/3)

Objective and scope

The NSWEC, in consultation with PricewaterhouseCoopers (PwC), has specified the procedures to be undertaken by PwC, and these procedures are set out in the Control Assessment Framework ("Framework") in Appendix A. PwC has performed the specified procedures during the fieldwork through a mix of inquiry, document review, system review and observations. The engagement was divided into two phases – pre and post election.

Phase 1

- Performed specified procedures as per agreed test procedures defined in the framework before the Election.
- Documented the results in the "pre-election report" **(submitted on 01 March, 2019).**

Phase 2

- Performed specified procedures as per agreed test procedures defined in the framework both during and after the Election.
- Documented the results in the "post-election report **(this report).**

Deliverable

#	Deliverable	Description
1	Audit Plan (Completed)	The audit plan outlines the activities that PwC will perform along with the timelines. The audit plan is published on the NSWEC website.
2	Pre-Election Report (Submitted – 01 March 2019)	Pre-election report outlines PwC's findings in relation to each procedure, where an exception is noted for the procedures performed prior to the Election. The fieldwork for this report was completed on 21 February 2019.
3	Post-Election Report (Completed – this report)	Post-election report provides PwC's findings in relation to each procedure, where an exception is noted. The fieldwork for this report was completed on 19 April 2019.

Introduction (3/3)

Scope exclusions

PwC's engagement does not constitute an audit in accordance with Australian Auditing Standards or a review in accordance with Australian Auditing Standards applicable to review engagements. Accordingly, no such assurance is provided in this deliverable.

PwC is not required, as part of its engagement, to provide any recommendations on the current control design, nor does the engagement require PwC to design any future controls. All control design decisions are the sole responsibility of the NSWEC management.

In order to conduct the engagement, PwC did not get involved in or had undertaken any of the following activities:

- Determining whether a person is an "eligible elector" within the meaning of section 152 of the Act.
- Approving procedures for technology assisted voting in accordance with section 155 of the Act.
- Providing or sourcing the information technology used under the approved procedures.
- Reviewing the source code underlying such information technology.
- Performing the role of "independent monitor" within the meaning of section 157 of the Act.
- Reviewing the devices used by a voter and the accuracy of the conversion of inputs provided by devices into iVote.

Additionally, while PwC performed the specified procedures set out in the Framework, PwC did not perform those procedures in relation to the following elements of iVote:

- Design and operational effectiveness of the legal, operational and technical Standards for e-Voting.
- Design and operational effectiveness of the cyber security controls in place to protect iVote.
- Design and operational effectiveness of the cyber security monitoring and protection mechanisms in place during live voting.
- Design and operational effectiveness of the controls in place to prevent fraudulent or inaccurate online voting.
- Review of the system architecture and supporting infrastructure.
- Review of NSWEC's alignment to the Australian Privacy Principles or any other privacy laws or policies.

Lastly, PwC did not and will not assess the adequacy of NSWEC's information technology security testing, nor will PwC otherwise manage the risk of critical failure in iVote caused by a Distributed Denial-of-Service attack or other adverse event. It is a matter for the NSWEC, and the third party contractors used in operating iVote, to ensure that iVote operates as intended.

2

Executive Summary

Control Assessment Framework

Procedures performed by PwC

The NSWEC Control Framework consists of 133 controls across 25 control objectives. For pre-election report, PwC initiated fieldwork on 4 February 2019, and performed the specified procedures during the fieldwork through a mix of inquiry, document review, system review and observations. PwC closed the fieldwork for the **pre-election report** on 21 February 2019, and reported the results of specified procedures performed until the closure of fieldwork in the pre-election report.

The results of the lockdown and election and post-election procedures are reported in the **post-election report** (this report).

Following is the status of specified procedures, at the closure of fieldwork for the post-election report (19 April 2019):

A	B	C	D
Total Number of specified procedures in the NSWEC Control Assessment Framework	Number of specified procedures reported in the Pre-election report	Number of specified procedures completed by 10 March 2019 and reported in this report (post-election report)	Number of additional procedures performed
133	45	133	4

Please refer to Appendix A for NSWEC Control Assessment Framework.

Key iVote systems (overview)

iVote is NSW Electoral Commission's online and telephone voting platform, which was first used in the 2011 state general election, and has been subsequently used in the 2015 state general election and a number of by-elections. iVote platform consists of different systems, which enables a voter to perform registration, vote and then verify his vote. For security considerations, all these components are hosted and managed by different entities.

1. iVote - registration and credential management system

Developed by: NSW Electoral Commission

Hosted and Managed by: Secure Logic (Service Provider)

The registration and credential management system is developed by NSWEC to allow the voter to apply to vote using iVote. Once the voter has successfully applied, the credential management system receives the application from the registration system and creates an iVote number for the voter.

2. iVote - voting system (Comprised of networked and air-gapped offline component)

Developed by: Scytl

Hosted and Managed by: Network component - Secure Agility (Service Provider), Air-gapped offline component - managed by NSWEC.

The networked component of the voting system is supplied by the service provider - Scytl, and hosted by NSWEC's service provider, Secure Agility. It provide voters with a secure platform to cast their vote online or by using the telephone. To enter the voting website, users must enter their iVote number and password created by them while applying for iVote registration. Once they submit their vote, it is securely transferred to the voting system to be included in the electronic ballot box. The user receives a receipt and can lookup on the assurance receipt portal to verify if their vote has been received by the voting system.

The air-gapped offline component of the voting system is hosted by NSWEC and is used for the creation of the encryption keys, voting system configurations, creation of admin and electoral board, and is used for key voting procedures such as cleansing, mixing and decryption.

Key iVote systems (overview) (Cont.)

iVote is NSW Electoral Commission's online and telephone voting platform, which was first used in the 2011 state general election, and has been subsequently used in the 2015 state general election and a number of by-elections. iVote platform consists of different systems, which enables a voter to perform registration, vote and then verify his vote. For security considerations, all these components are hosted and managed by different entities.

3. iVote - assurance system

Developed by: Scytl
Hosted and Managed by: AC3

The assurance system provides the voters with two different methods to verify their vote - the verification mobile application and the telephone verification. In addition, the assurance system maintains copies of the receipts from the voting system. The assurance system is hosted by NSWEC's service provider AC3.

Key iVote processes (Overview)

NSW Electoral Commission established and performed a number of processes and procedures to enhance the confidentiality, integrity and availability of the iVote platform.

1. Lockdown procedures

The purpose of the lockdown procedures, is to disable all users from the servers except for one administrator whose password is split [redacted]. In the lockdown mode, all operating system accounts, except one for each environment, will be locked out. The remaining account password will be re-set and split [redacted]

2. Creation of the administrator board

The creation of the administrator board included appointment of 5 members of ivote administrators. Each of the 5 members are provided with their private keys. A quorum of 2 members is required before any decision is made with regards to any change in the system, or access of the air-gapped offline component of iVote.

3. Creation of the electoral board

The creation of the electoral board included appointment of 6 members of executive management. Each of the 6 members are provided with their private keys. A quorum of 3 members is required before any decision is made with regards to any change in the system, pausing of voting and unlock of any component of iVote..

4. Logic and accuracy testing

The purpose of the logic and accuracy test is to ensure all parts of the iVote platform are functioning correctly prior to the start of voting and the NSWEC is confident in the functioning of the iVote platform.

5. Cleansing process

The cleansing process includes marking the valid votes (removing the votes cast by voters who have voted through another channel), ensuring one vote per voter, validating the integrity of the vote and removing any voter related information from the vote.

6. Mixing and mixing proofs

Mixing is the process of anonymising the voters by ensuring that the votes that have been cast cannot be reconciled with the number of iVote applications. The output of the mixing process is shuffled and re-encrypted votes.

The mixing proof (verifiable mixnet) is the mathematical proof of the error-free completion of the mixing of encrypted votes, and provides confirmation that the mixing process has not corrupted the votes in any way.

Lockdown Procedures observed

Lockdown procedures

The purpose of the lockdown procedure is to disable all users from the servers except for one administrator whose password is split [redacted]. Throughout the period of the review, PwC observed the lockdown procedure for each of the Registration and Credential Management, Voting, and Assurance systems.

1. Lockdown (registration and credential management): 9 February 2019

- Disable the administrator account
- Disable the domain accounts on the domain controller
- Change the password of the lockdown admin account on all three domains
- Disable all local users, except the standard local administrator on the management servers

2. Lockdown (voting system): 7 March 2019

- Disable the administrator account
- Disable the domain accounts on the domain controller
- Configure the lockdown administrator account with a 2FA token
- Change the password of the Lockdown Admin account
- Disable all local users, except the lockdown administrator account.

3. Lockdown (Assurance System) : 7 March 2019

- Configure the lockdown administrator account with 2FA using a Yubikey
- Disable all local users, except the lockdown administrator account.

Summary of findings (post-election report)

Following are the summarised headline findings, based on the specified procedures completed until 19 April 2019. The detailed findings are contained in section 3 of this document. The findings have not been assigned any risk rating as this report is being issued post elections.

Ref	Finding
1	Incorrect name used during the identification of duplicate or invalid votes.
2	Absence of full multi-lingual support in iVote.
3	Unresolved findings from the accessibility testing of iVote platform.
4	Voter information was not deleted from the registration system.
5	A key component of the iVote platform is in-house developed.
6	Lack of adequate coverage of Security Incident and Event Monitoring (SIEM) system.
7	Absence of [redacted] in the security incident and event management (SIEM), until fixed upon highlighting the issue.
8	WAF Logs and [redacted] SIEM are not synced to the same time zone for the registration system logs.
9	Background checks for employees of a critical supplier not performed.
10	Lack of adequate security awareness in the call centre.
11	Inadequate resolution action for the issues identified during the performance testing.
12	Absence of an up-to-date patch management policy.

Summary of findings (post-election report)

Following are the summarised headline findings, based on the specified procedures completed until 19 April 2019. The detailed findings are contained in section 3 of this document. The findings have not been assigned any risk rating as this report is being issued post elections.

Ref	Finding
13	Undocumented configuration changes were made to the Registration and Credential Management System in production.
14	Mechanism to ensure voters use up-to-date mobile app is not implemented.
15	Deficient password practices followed for the iVote platform.
16	User-IDs were not disabled during the lockdown procedures.
17	[redacted] on air-gapped (offline) computers was not disabled.
18	Lack of review of firewall rules to ensure only authorised network traffic is allowed.
19	File Integrity Monitor service was stopped during the lockdown period.
20	Deficiency in the firewall hardening to protect iVote from malicious network traffic.
21	Deficient configuration of anti-virus software and opportunity to improve anti-virus [redacted]
22	Lack of adherence to physical security controls and security monitoring at one of the data centres hosting iVote.
23	Deficient reporting of events and incidents by the service providers.

Summary of findings (post-election report)

Following are the summarised headline findings, based on the specified procedures completed until 19 April 2019. The detailed findings are contained in section 3 of this document. The findings have not been assigned any risk rating as this report is being issued post elections.

Ref	Finding
24	Inadequate time provided to the voters for the verification of votes.
25	Lack of adherence to the removable media procedures at one of the data centres hosting iVote.
26	Deficiency in the monitoring of the system heath and the capacity utilisation of iVote - registration and credential management system.
27	Absence of verification by the service provider before enabling privileged interface of iVote.

Detailed Findings

3

Findings

Finding 1: Incorrect name used during the identification of duplicate or invalid votes.

Control:

4.4 Prior to the final result, the voting system should identify votes which are invalid or duplicate or generated due to error.

Specified Procedure
Review and observe the documented procedure implemented within the iVote platform to help the voting system identify invalid, duplicate, or votes generated due to an error.

Finding / Observation

PwC inspected [redacted] nd noted that procedures were defined for the identification and removal of invalid and duplicate votes.

PwC was informed that the duplicate votes were identified by the comparison of the iVote data with EMA (Election Management Application) which included voting from all sources such as physical, postal, online etc. This comparison was performed during the decryption ceremony held on 24 March 2019.

During the observation of the decryption ceremony, PwC noted that the EMA (Election Management Application) incorrectly identified "Number of iVote Registrations" as "Number of Votes".

On further inquiry and analysis, it was noted that while the naming was incorrect, the count of registrations and votes was accurate.

Findings

Finding 2: Absence of full multi-lingual support in iVote.

Control:

5.1 Internet voting system should enable all voters including people with disabilities and special needs to vote.

Specified Procedure

1. Review if the iVote system is designed to be used with accessibility options (screen readers etc.)
2. Review if the iVote system provides options to the voters to use it in a language best understood by them.

Finding / Observation

During the review of the iVote system it was noted that the voters can cast their vote, verify their vote, and check their receipt in the following languages:

- Arabic;
- English;
- Greek;
- Italian;
- Simplified Chinese;
- Traditional Chinese; and
- Vietnamese.

While it was noted that the language can be changed throughout the phases of casting an online vote, PwC noted that if a user were to incorrectly enter their password or iVote number when attempting to vote they would be required to fill out a Captcha form, however this form remained in English despite the rest of the page being displayed in the language chosen by the voter.

Additionally, PwC noted that Captcha was enforced on all the users registering or voting on the iVote platform, due to the incorrect network configuration. This issue was resolved on 13 March 2019 after performing the required network changes during an incidental unlock.

Findings

Finding 3: Unresolved findings from the accessibility testing of the iVote platform.

Control:

5.1 internet voting system should enable all voters including persons with disabilities and special needs to vote.

Specified Procedure

1. Review if the iVote system is designed to be used with accessibility options (screen readers etc.)
2. Review if the iVote system can be designed by the voter to use in a language best understood by them.

Finding / Observation

PwC was informed that Accessibility testing for iVote was conducted by Vision Australia against Web Content Accessibility Guidelines (WCAG 2.1). PwC reviewed the post-rectification reports and noted that there were unresolved issues present in all the following components of iVote:

1. iVote voting website (1 unresolved issue)
2. iVote landing page (1 partially unresolved issue)
3. iVote registration page (1 unresolved issue, 2 partially unresolved issues)
4. iVote voting mobile website (2 unresolved issue, 1 partially unresolved issue)
5. iVote receipt (1 unresolved issue, 1 partially unresolved issue)
6. iVote verification app (1 unresolved issue)

In addition, it was noted that NSW Electoral Commission did not receive a Vision Australia certificate to say that their website was in alignment to the Web Content Accessibility Guidelines.

Findings

Finding 4: Voter information was not deleted from the registration system.

Control:

6.4 The authentication data should be securely erased from the internet voting system when it's no longer required.

Specified Procedure

Review if the procedure is defined to securely erase authentication data when it was no longer required.

Finding / Observation

PwC was informed that the voter credential (encrypted pin hash) is created by the voter during the registration process [redacted] After [redacted], encrypted pin hash is deleted from the [redacted].

During the incidental unlock to analyse an issue related to the encrypted pin hashes, it was noted that the encrypted pin hash for three users was not deleted from the Registration system.

On inquiry with the NSWEC team, PwC was informed that this issue was due to a defect in the iVote - registration system interface.

Findings

Finding 5: A key component of the iVote platform is in-house developed.

Control:

8.4 COTS products should be used in the election process wherever possible.

Specified Procedure
Review the various products used in the election management processes to identify whether any in-house developed tool was used.

Finding / Observation

During the review of the COTS products used by the NSW Electoral Commission, PwC noted that while NSW Electoral Commission uses multiple COTS products to conduct the election process, an inventory of such software was not maintained.

PwC noted that the registration and credential management system were developed in-house because of a lack of COTS options.

The usage of in-house developed registration and credential management systems was documented and informed to the various stakeholders through the NSWEC iVote Strategy Document.

Findings

Finding 6: Lack of adequate coverage of Security Incident and Event Monitoring (SIEM) system.

Control:

9.3 A Security incident and event management (SIEM) should be implemented for real time monitoring of events and management of security incidents.

Specified Procedure

1. Review documentation to confirm that a Security Incident and Event Management (SIEM) system was implemented at NSWEC.
2. Review if the SIEM covered all components of the iVote platform - (i) registration, (ii) voting, and (iii) assurance.
3. Review if parsers and correlation rules are created for identification of events and incidents.

Finding / Observation

PwC was informed that NSWEC had implemented three levels of security monitoring using the following mechanisms:

[redacted]

PwC reviewed the security monitoring capability implemented at all 3 levels and noted the following deficiencies:

- [redacted]
- [redacted]
- [redacted]

Findings

Finding 7: Absence of [redacted] in the security incident and event management (SIEM), until fixed upon highlighting the issue.

Control:

9.4 Security events logged into log management and security incident management system must capture the key events and detailed description in the logs.

Specified Procedure

1. Review the sample log information from the iVote platform and validate if key events [redacted] were captured.

2. Review the log information to validate whether the logs included information such as [redacted] of the event.

Finding / Observation

PwC reviewed the information captured in security events and noted that the [redacted] Upon highlighting the issue, NSWEC implemented a fix [redacted]

[redacted]

While [redacted] information was not available in [redacted] this information was getting captured in the firewall logs.

Findings

Finding 8: WAF Logs and [redacted] SIEM are not synced to the same time zone for the registration system logs.

Control:

9.6 All internet voting components should be synced with a network time protocol to ensure integrity of logs.

Specified Procedure
For all components of iVote, confirm that they are synchronised with the NTP to ensure the integrity of the system logs.

Finding / Observation

During the review of the WAF and DDoS service [redacted], it was observed that while NTP is in place, Web Application Firewall (WAF) logs were stored locally in Australian Eastern Daylight Savings Time (AEDT), whereas when transferred to [redacted] SIEM, WAF logs were recorded under Greenwich Mean Time (GMT).

Findings

Finding 9: Background checks for employees of a critical supplier not performed.

Control:

10.3 Requirement for background verification and contractual obligation shall be communicated to all third parties working on the internet voting system for implementation.

Specified Procedure

1. For critical IT suppliers, review the supplier contracts and confirm if there is a requirement for performing background checks.
2. Confirm that the third party suppliers share the background check information with NSWEC.

Finding / Observation

During the review of background checks for suppliers, PwC noted that while background checks are performed for NSW Electoral Commission full time and contracted employees, the background checks for the employees from Scytl were not provided due to the Employment and Labour Law in Spain restricting the ability for companies to perform background checks on Spanish company employees.

Findings

Finding 10: Lack of adequate security awareness in the call centre.

Control:

10.4 All employees of the organization shall receive an appropriate awareness programme and education and training that is relevant for their job function.

Specified Procedure

1.Review the internal records to validate whether the users have undergone regular awareness programs.
2.Review the internal communication email circulated to the employees regarding the security policies.
3. Perform the physical review to assess whether the users have adhered to the policy of clear desk and clear screen.

Finding / Observation

[redacted]

Findings

Finding 11: Inadequate resolution action for the issues identified during the performance testing.

Control:

11.1 Detailed testing including user acceptance testing (UAT) should be performed before the deployment of the internet voting system.

Specified Procedure

1. Inspect and review the testing performed prior to the deployment of iVote in production.
2. Inspect and review if the test cases and results were approved.

Finding / Observation

PwC determined through inquiry that NSWEC performed testing on the pre-production environment to ensure that all elements of the iVote platform operated as per requirements.

Upon review of the test plan and the performance test summary report, it was noted that the load testing was conducted for all the components of the iVote platform including the IVR. However, it was noted that there was one potentially significant performance issue identified during testing, which could not be adequately resolved due to the time constraints and the amount of rework required.

Findings

Finding 12: Absence of an up-to-date patch management policy.

Control:

12.3 Patch management policy should be documented and operationalised.

Specified Procedure

1. Review and confirm whether a patch management policy is documented and operationalised.

Finding / Observation

Through inspection of the [redacted] document on 8 February 2019, it was noted that NSWEC has a defined patch management policy to apply critical security patches to all of its operating systems on servers, applications and databases.

PwC noted that the patching policy has not been updated since 2012, and it does not currently include the procedures to apply critical patches during the lockdown period.

While the patching policy was not up-to-date, we noted that all components of the iVote platform were updated with the latest patches prior to the lockdown.

Findings

Finding 13: Configuration changes made to the iVote - registration system in the production environment were not documented.

Control:

12.5 All updates and patches should be reviewed and tested before deployment.

Specified Procedure

Inquire whether the relevant patches are tested in the lower environment before deployment.

Finding / Observation

On 22 March 2019 the performance of the registration system was severely degraded. As a result, the system was unlocked to troubleshoot and fix the root cause of the issue.

While the system was in an unlocked state for 11 hours, several configuration related changes were made to the registration system. [redacted]

While these changes were made in the presence of the electoral board members and were documented retrospectively, these were not documented at the time the changes were being made and were not tested in the lower environment.

Findings

Finding 14: Mechanism to ensure voters use up-to-date mobile app is not implemented.

Control:

12.7 Mechanism should be implemented to ensure that latest mobile app/application is used by the voters.

Specified Procedure

1. Confirm whether a forced update is implemented for Mobile App.

Finding / Observation

PwC noted through inquiry that there was no mechanism implemented to ensure that voters always used the most up-to-date version of the verification mobile app. However, PwC was informed that there were no security updates to the verification mobile app throughout the election period.

Findings

Finding 15: Deficient password practices followed for the iVote platform.

Control:

13.2 A strong password policy should be implemented for all components of internet voting system which includes using a split password shared between two senior executives (members of the Electoral Board) during the lockdown period.

Specified Procedure

1. Review the access management policy and evaluate if two factor authentication was mandated for privileged access to key iVote components.

2. Review the password policy for all components of iVote system and evaluate if it meets the required guidelines.
   a. A minimum length of 8 characters.
   b. A minimum complexity of at least 3 of the following character types (numbers, lower case letters, non-alphanumeric characters, & upper case letters).
   c. Passwords must be changed at least every 90 days.
   d. Restrict password history to 5.
   e. 5 unsuccessful password attempts within a 24-hour period must disable/lock the account.
   f. Password are protected in storage using one-way hash and are encrypted in transmission.

3. Inspect and confirm if the password was split and shared between two senior executives, and is either a long, randomly generated string or key based.

Finding / Observation

During the review of [redacted], PwC noted that the password for the following components of iVote platform were [redacted]

- [redacted]
- [redacted]
- [redacted]

[redacted]

Findings

Finding 15: Deficient password practices followed for the iVote platform. (Cont.)

Finding / Observation

PwC observed that [redacted]. While [redacted] the password used to [redacted] as easily predictable and the default admin account had not been modified after the creation of the designated NSW Electoral Commission admin account to perform critical iVote activities.

Findings

Finding 16: User-IDs were not disabled during the lockdown procedures.

Control:

13.3 During lockdown all system accounts except one should be disabled.

Specified Procedure

During lockdown observation, validate that all system accounts except one are disabled and account's password is shared [redacted].

Finding / Observation

At the start of the elections, NSWEC performed the lockdown procedures for each of the systems of iVote, which included disabling all users from the servers except for one administrator whose password is split [redacted]

PwC observed:

- For the lockdown procedure performed for the voting system on the 7 March 2019, all of user accounts were not disabled. These accounts remained enabled until 9 March 2019.
- For the incidental unlock procedure performed for registration and credential management system on the 16 March 2019, one of the user accounts was not disabled. This account remained enabled until the 18 March 2019 when the next incidental unlock was performed.
- PwC noted that [redacted] were kept enabled throughout the election period, which could be used to login and access the registration system during the lockdown period.

Findings

Finding 17: [redacted] *on air-gapped (offline) computers was not disabled.*

Control:

14.01 The network hosting the internet voting system should be segregated based on the defined security model to achieve defence in depth.

Specified Procedure

1. Verify if the network hosting the voting system are logically segregated(using VLANs etc.) in order to align with the NSWEC's security model.
2. Verify if voting system and assurance system is segregated.

Finding / Observation

During the review, PwC observed that NSW Electoral Commission used 2 computers for critical tasks such as encryption key generation, mixing of votes, cleansing process and decryption were air-gapped (not connected to any network).

[redacted]

[redacted]

Findings

Finding 18: Lack of review of firewall rules to ensure only authorised network traffic is allowed.

Control:

14.13 Firewall rules should be reviewed on a regular basis [redacted] should be allowed basis an explicit approval from NSWEC.

Specified Procedure

1.Inspect the documentation maintained for the regular review of the firewall rules and check the frequency of review.

2.For a sample of rules check whether [redacted] are allowed or not if allowed check if they have approval from NSWEC.

Finding / Observation

PwC noted firewall rules of all the three iVote system components – registration system, voting system and assurance system were not reviewed by NSWEC due to a significant delay by the service providers in providing the firewall configuration to NSWEC. The tickets raised by NSWEC to the service providers were not actioned upon till the close of elections.

PwC reviewed the firewall rules and noted that some of the rules allowed wider access than required.

Findings

Finding 19: File Integrity Monitor service was stopped during the lockdown period.

Control:

14.14 The hosts (servers) should be protected using host based intrusion prevention system and file integrity monitor. All logs must be integrated with SIEM.

Specified Procedure

1. Check whether all logs are fed into the SIEM .
2. Review documented procedures to confirm if Host based intrusion prevention system has been deployed to protect the host servers.
3. Review the network diagram of the system

Finding / Observation

PwC was informed that [redacted] ile integrity monitoring was deployed on all instances of iVote platform. During the incidental unlock observation on 22 March 2019, PwC noted that [redacted] without any authorised approval during the troubleshooting.

Findings

Finding 20: Deficiency in the firewall hardening to protect iVote from malicious network traffic.

Control:

14.8 Firewall rules must be define to restrict network communication based on 'need to know' principle.

Specified Procedure

1. Inspect and review firewall configuration and evaluate if base rule of "Deny All" was implemented.
2. Evaluate and inspect the firewall rules to evaluate if command and control ports were restricted to management zone.

Finding / Observation

PwC was informed that the firewall for each iVote component is managed by the respective service provider and firewall rule was created or modified only after an explicit approval from NSWEC. PwC was informed that firewalls of various components of iVote was not hardened by NSWEC prior to the lockdown of iVote platform.

PwC reviewed the firewall rules and noted that some firewall rules allowed wider access than required.

[redacted]

PwC was informed that [redacted] was used to monitor [redacted] and an incidental unlock was performed to identify the problem. Based on th [redacted] NSWEC informed PwC that there was no realised incident [redacted].

Findings

Finding 21: Deficient configuration of anti-virus software and opportunity to improve anti-virus [redacted] solution.

Control:

17.1 Antivirus/anti-malware scanning agents should be installed on all components of internet voting system, both servers and workstation. The signatures are updated on regular basis and anti-malware is configured to perform regular scans and quarantine upon detection.

Specified Procedure

1. Compare with the systems inventory/CMDB, and review if the anti-malware scanning agents are installed on all components of iVote platform (registration, voting, assurance and desktops/laptops).
2. Inspect and review anti-malware agents on the Windows and Linux systems.
3. Signatures are updated on all iVote servers and end-points.

Inspect and review if the anti-virus/anti-malware scanning tools are configured for all components of iVote platform in such a way so as to ensure:

- Regular scans full system (server and endpoints) scans are enabled.
- Appropriate quarantine measures are configured.
- Auto update of signature and engine should be enabled.

Finding / Observation

PwC noted that [redacted] did not have an [redacted]
Although [redacted] was enabled for protection from the malware [redacted]

Findings

Finding 22: Lack of adherence to physical security controls and security monitoring at one of the data centres hosting iVote.

Control:

19.2 Resources are in place to monitor alert and respond in case of an physical intrusion.

Specified Procedure

[redacted]

Finding / Observation

During the data center visit and the review of the the physical and environmental security controls, [redacted]

[redacted]

Findings

Finding 23: Deficient reporting of events and incidents by the service providers.

Control:

22.3 Daily Incident report is prepared based on the activity monitoring during the system lockdown period.

Specified Procedure

Review and confirm whether procedures existed to monitor all security incidents, and the reports are created and shared internally on a daily basis for the events generated during the lockdown period.

Finding / Observation

PwC reviewed the security monitoring and reporting for all the components of iVote platform and noted that NSWEC service providers [redacted] provided daily incidents reports [redacted].

[redacted]

Findings

Finding 24: Inadequate time provided to the voters for the verification of votes.

Control:

23.1 A voter should be able to verify through phone, mobile app or web application platform that his/her vote has been accurately entered into electronic ballot box without any alteration.

Specified Procedure

1. Review iVote related documents to confirm if the mechanism exists for the voter to verify if his vote has been captured as he intended.

Finding / Observation

PwC was informed that iVote is configured to allow the voter to perform verification of their vote within 1 hour of the casting the vote. We reviewed the verification procedure and noted that all the voters who voted till 22 March 2019, had an option to perform verification within 1 hour of casting their vote.

However, during the observation on the last day of election - 23 March 2019, PwC noted that voters who had cast their vote between 5:00 pm to 6:00 pm did not get requisite 1 hour to perform verification of their vote due to the closure of the voting and verification system.

We were informed that the closure of verification at 6:00 pm was by design, since the elections are marked as closed at 6:00 pm.

Finding 25: Lack of adherence to the removable media procedures at one of the data centres hosting iVote.

Control:

25.2 Critical voting related information stored on the removable media must be securely erased after the completion of the relevant task or activity successfully.

Specified Procedure

During the election observation, observe and confirm whether the voting related information has been securely erased in the USB Media after completion of the respective steps.

Finding / Observation

[redacted]

[redacted]

[redacted] performed an incident review and informed PwC that it had identified and implemented a number of measures including awareness refresher for its engineering and support staff.

Findings

Finding 26: Deficiency in the monitoring of the system heath and the capacity utilisation of iVote - registration and credential management system.

Additional Control:

AP 1: Performance of iVote system components shall be monitored to determine the degree of capacity utilisation and to identify operational warning and exceptions.

Additional Procedure

1. Review the operational dashboards and reports to verify whether the performance of the iVote platform was consistently reviewed during the election period.

Finding / Observation

PwC was informed that performance of all the components of iVote system is monitored by the respective service providers and their health report was shared with NSWEC on a exception basis.

On 5 March 2019, it was noted that [redacted] which led to an unplanned downtime of the system. On inquiry, it was noted that there was no communication from the service provider, [redacted].

On 18 March 2019 and 22 March 2019, it was noted that [redacted]. However, there was no communication from the service provider [redacted].

Findings

Finding 27: Absence of verification by the service provider before enabling privileged interface of iVote.

Additional Control:

AP 2: Procedures for verification of the user should be established before providing any privileged access to the iVote platform.

Additional Procedure
Verification of the user must be performed before providing privileged access to the iVote platform.

Finding / Observation

As a secure unlock procedure of iVote - voting system, the NSWEC iVote team is required to [redacted] the service provider [redacted] is required to perform verification of the NSWEC iVote team member.

During the observation of incidental unlock [redacted] PwC noted that [redacted] when the NSWEC team member [redacted].

4

Findings from the pre-election report

Summary of findings (pre-election report)

Following are the summarised headline findings and their status after re-testing, based on the procedures performed for pre-election report which was submitted on March 1, 2019.

S.No	Finding	Risk	Re-test Results
1	Application to configure and manage the iVote assurance system, is publicly accessible from the internet.	Extreme	**Closed**
2	Lack of adequate protection and safeguards to protect against [redacted].	High	**Open**
3	Absence of adequate security use-case for security monitoring and intelligence. Refer finding 6 in the post-election report.	High	**Open**
4	Lack of [redacted] to secure the NSWEC iVote Environment.	High	**Open**
5	Lack of [redacted] on devices used to manage NSWEC iVote assurance system.	High	**Open**
6	Lockdown procedures performed without disabling [redacted] ccount.	High	**Open**
7	Non-essential services and accounts are left enabled on registration and credential management system during the lockdown.	High	**Open**
8	Inventory of IT assets, such as applications, and software has not been maintained. Usage of unlicensed software to perform lockdown procedures noted.	Moderate	**Closed**
9	iVote - registration system is [redacted]	Moderate	**Open**
10	Privacy Impact Assessments for iVote systems and processes have not been conducted.	Moderate	**Open**
11	The Information Security Policy has not been updated or reviewed since 2015.	Low	**Closed**
12	IT policies and procedures are not being periodically reviewed and updated.	Low	**Open**

Refer Appendix G for NSWEC Risk Assessment Matrix.

Appendix A – Control Assessment Framework

A

Control Assessment Framework (1/5)

Overview

In the lead up to the 2019 State General Election, the NSWEC undertook a significant refresh and uplift of iVote. A key driver for this refresh was to increase transparency for voters and political party scrutineers.

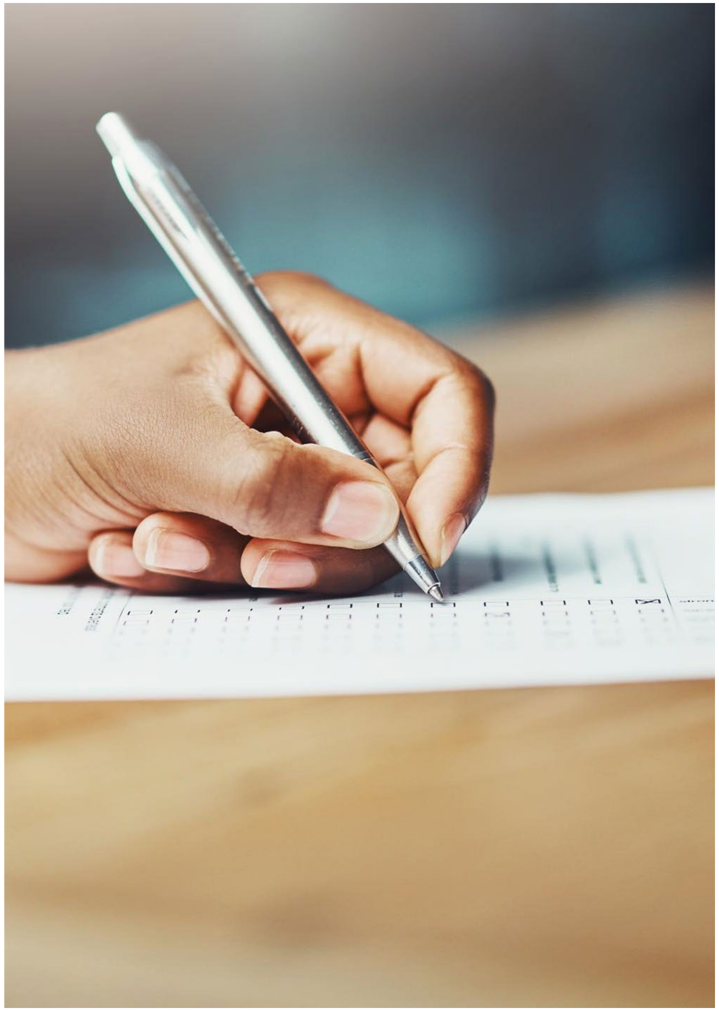
In order to drive transparency and meet the requirement of the Electoral Act 2017, the NSWEC worked to develop a controls framework drawing on guidance from the Electoral Council of Australia and New Zealand (ECANZ) principles and a number of best practice processes to help protect the security and integrity of the system. The best practice frameworks used to create the controls included:

(i) Voluntary Voting Systems Guidelines (VVSG) published by NIST;
(ii) ISO27001:2013 Information Security - Appendix A Clauses; and
(iii) Council of Europe (CoE) recommendations on standards for e-voting.

The Framework has the following components:

1. 25 Control objective covering areas such as accuracy, integrity, usability, cybersecurity, and privacy.
2. 133 Controls and associated test procedures.
3. Each control objective has an associated reference to CoE (Council of Europe recommendations), VVSG and ISO 27001.

This framework was used by PwC to perform the specified procedures and the tests were reported in pre-election report (published on March 1, 2019) and post-election report (this report).



Control Assessment Framework (2/5)

#	Control Objective	No of Controls	Deficient Controls	Mapping to CoE	Mapping to ISO 27001	Mapping to VVSG
1	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 the internet voting system.	**2**	0	Recommendation # 40	A.5 Security Policies	-
2	Mechanism should be implemented to make voters effectively and accurately use the internet voting system.	**7**	0	Recommendation # 4 Recommendation # 14 Recommendation # 16	-	7.3, 3.3
3	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**	0	Recommendation # 5 Recommendation # 10	-	7.1, 5.1, 5.2, 7.3
4	The internet voting system 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.	**4**	1	Recommendation # 6 Recommendation # 9 Recommendation # 17 Recommendation # 49	-	1.2
5	The voter interface of the internet voting system shall be easy to understand and use.	**5**	2	Recommendation # 1 Recommendation # 2	-	8.3, 7.2, 3.3
6	The internet voting system 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.	**5**	1	Recommendation # 7 Recommendation # 8 Recommendation # 11 Recommendation # 18 Recommendation # 21	A.9 Access Control	11.3
7	Protection of personally identifiable information (PII) and privacy of data collected by the internet voting system shall be ensured.	**8**	1	Recommendation # 20 Recommendation # 22	A.9 Access Control A.18.2 Compliance with legal and contractual requirements	10.1, 10.2, 6.1

Control Assessment Framework (3/5)

#	Control Objective	No of Controls	Deficient Controls	Mapping to CoE	Mapping to ISO 27001	Mapping to VVSG
8	Open standards shall be used to enable various technical components or services, to inter-operate.	**4**	1	Recommendation # 35	-	4.1, 4.2, 4.3, 4.4
9	Detection and monitoring capability shall be developed to detect unauthorized activities.	**6**	3	Recommendation # 39	A.12.4 Logging and monitoring	9.3,9.4, 15.1, 15.2, 11.1
10	Mechanism should be implemented to ensure that only validated personnel are given access to internet voting system.	**5**	2	Recommendation # 41	A.7 Human Resource Security A.9 Access Control A.15.1 Security in supplier relationships	11.2
11	Before an election, the electoral management body shall satisfy itself that the internet voting system operates correctly.	**3**	1	Recommendation # 42	A.14.2 Security in development and support processes	14.3
12	A procedure shall be established to identify vulnerabilities and regularly installing updated versions and corrections of all relevant software.	**7**	3	Recommendation # 43	A.8.1 Responsibility for assets A.8.2 Information classification A.12.5 Control of operational software A.12.6 Technical vulnerability management	14.3, 14.4, 15.4
13	An access control policy based on the principle of need to know and need to use, shall be established, documented and periodically reviewed.	**9**	2	Recommendation # 18	A.9 Access Control	13.1, 11.2, 11.3, 11.4, 11.5, 15.4
14	internet voting system's network shall be managed, controlled and segmented to protect information in systems and applications.	**16**	4	-	A.13.1 Network security management	15.4

Control Assessment Framework (4/5)

#	Control Objective	No of Controls	Deficient Controls	Mapping to CoE	Mapping to ISO 27001	Mapping to VVSG
15	Development and implementation of new systems, applications and software, and changes to existing systems, applications and software, are authorised, tested, approved, implemented and documented.	**3**	0	-	A.14.2 Security in development and support processes	1.3, 9.1, 14.4, 1.1
16	Use of secure development practices, testing, and operating environment to ensure integrity of iVote platform.	**5**	0	-	A.12.1 Operational procedures and responsibilities A.14.2 Security in development and support processes A.9.4 System and application access control	15.4
17	Detection, prevention and recovery controls to protect against malware shall be implemented, and operated.	**3**	1	-	A 12.2 Protection from Malware	15.3
18	Procedure on encryption shall be developed and implemented for the use of cryptography to protect votes and voter data during election.	**9**	0	Recommendation # 44, #45	A 10.1 Cryptographic Controls	13.3
19	Physical protection and guidelines for secure areas (critical office locations, data centre etc.) and equipment shall be designed and applied.	**6**	1	Recommendation # 32	A 11 Physical and Environmental Security	12.1, 12.2
20	Procedures and capabilities related to business continuity and resilience is established to operate effectively during a time of an incident.	**9**	0	Recommendation # 40	A.17.2 Redundancies	14.1
21	Provisions should be put in place to maintain Confidentiality, Availability and Integrity (CIA) of the voting system.	**2**	0	-	A.8.2 Information classification	13.4

Control Assessment Framework (5/5)

#	Control Objective	No of Controls	Deficient Controls	Mapping to CoE	Mapping to ISO 27001	Mappin g to VVSG
22	Information security incidents shall be responded and reported to in accordance with the documented procedures.	**5**	1	Recommendation # 47	A.16 Information security incident management	15.1, 15.2, 15.4
23	A voter shall be able to verify that his or her intention is accurately represented in the vote and that the encrypted vote has entered the electronic ballot box without being altered.	**2**	1	Recommendation # 15	A.12.7 Information systems audit considerations	9.2, 6.2
24	The voting system shall ensure votes remain anonymous and it is not possible to reconstruct a link between the unencrypted vote and the voter.	**2**	0	Recommendation # 26 Recommendation # 19 Recommendation # 25	A 10.1 Cryptographic Controls	10.1, 10.2
25	Procedures shall be implemented for the management and handling of removable media during the election process.	**3**	1	-	A.8.3 Media handling	15.4, 14.3

Appendix B – iVote process overview

B

Key iVote processes (1/2)

Prior to voting

The NSWEC undertook a number of key steps prior to the commencement of voting in order to prepare and secure the system, such as; limiting system access during voting (with their approved third party providers: Secure Logic, AC3 and Secure Agility), creating an electoral board to create and share the private key used to encrypt & decrypt the votes, and undertaking a test vote scenario. These steps were observed by PwC as part of this engagement and have been documented at a high-level below. It should be noted that vendor security due diligence has not been conducted as a part of this review.

iVote system lock down

- Lockdown of the registration and credential management system:
  - The third party hosting provider of the registration and credential management system (Secure Logic) removed all access to servers except sole administration user account. The system was hosted by Secure Logic.
  - The sole administration user password was reset and split for security purposes [redacted].
- Lockdown of the voting system:
  - The third party hosting provider of the voting system (Secure Agility) removed all access to servers except sole administration user account. The voting system was hosted by Secure Agility in their data centres.
  - The sole administration user password was reset and split for security purposes [redacted].
- Lockdown of the assurance system:
  - The third party hosting provider of the assurance system (AC3) removed all access to servers except sole administration user account. The assurance system was hosted by AC3.
  - The sole administration user password was reset and the two factor authentication is applied. [redacted]

Key iVote processes (2/2)

- Creation of the Electoral Board:
  - 6 members of Executive Management were appointed and the private key was shared amongst them on smart cards. A quorum of 3 members was required to construct the private key necessary for decrypting the votes.
- Completion of the election system build on the voting system and assurance system.
- Generation of test vote credentials.
- Printing of the test vote entry sheets.
- Proofing of the iVote ballots sheets (iVote online and Interactive Voice Response (IVR)).
- Test votes cast using iVote voting website and IVR.
- Verification of test votes by phone.
- Verification of votes using the verification app
- Completion of test votes.
- Download of test vote ballot box and transferred to an offline machine for decryption.
- Quorum of Electoral Board (3 members) provided the key for decryption.

Close of voting

- Review of votes cast using iVote vs votes cast at pre-poll locations and accepted postal votes. In the event of duplications, votes cast using iVote were removed.
- Decryption ceremony with quorum of Electoral Board (3 members).
- Decryption of votes.
- The comparison of the receipts in the voting system with the receipts from the assurance system was performed.

Post election

- System cleansing, including removal of votes and test votes and reactivation of system administrators.
- Checking of log integrity and checking logs for evidence of any tampering.

Appendix C – Incident Details

C

Incident Details

Following is the list of incident which occurred during the lockdown period – 11 February 2019 to 24 March 2019.

Incident(s)	Impact
1. **11 February:** iVote applications including the encrypted password/pin not being saved fully.	Planned downtime and iVote registration system unavailability to voters from 11 Feb, 11:30 AM to Feb 12, 3 PM. [redacted]
2. **12 February:** No iVote applications were being sent to credential management from registration system.	Planned downtime and iVote registration system unavailability to voters from 12 Feb, 02:17 PM to 04:32 PM. [redacted]
3. **13 February:** A number of electors who are not registered as Silent electors on the Electoral Roll incorrectly selected as "Silent".	No impact in terms of outage or downtime of iVote platform. [redacted]
4. **21 February:** Multiple incidents including DB replication from prod to DR, logging of [redacted], logging of [redacted] [redacted] [redacted].	Planned downtime and iVote - registration system unavailability to voters from 5:30 PM to 9:00 PM. [redacted]
5. **28 February:** Failure of database replication from primary production to Disaster Recovery (DR) instance.	Planned downtime and iVote - registration system unavailability to voters for 5.5 hours. [redacted]

Incident Details

Following is the list of incident which occurred during the lockdown period – 11 February 2019 to 24 March 2019.

Incident(s)	Impact
6. **05 March:** Credential management system was unresponsive.	Planned downtime and iVote - registration and credential management unavailability to voters during the unlock for 8.5 hours. [redacted]
7. **09 March:** Loss of passwords/PINs due to a defect in the web service call. Recovery of the passwords/PINs [redacted] required.	Planned downtime and iVote - registration and credential management unavailability to voters during the unlock from 10:30 AM to 3:00 PM. Successful recovery of the passwords/ PINs[redacted] [redacted]
8. **09, 10 March:** iVote voting and assurance system logs could not be read [redacted]	No impact in terms of outage or downtime of iVote platform. [redacted]
9. **11 March:** Issue with the voter's session management and update of the voter's activity status.	No impact in terms of outage or downtime of iVote platform. [redacted]
10. **13 March:** Excessive [redacted] consumption in credential manager.	No impact in terms of outage or downtime of iVote platform. [redacted]
11. **13 March:** Significant Degradation in landing page and Registration System.	Unplanned service degradation. [redacted]

Incident Details

Following is the list of incident which occurred during the lockdown period – 11 February 2019 to 24 March 2019.

Incident(s)	Impact
12. **13, 14 March:** Excessive CAPTCHA trigger due to deficient configuration.	Unplanned service degradation and increase in voter calls to reset the passwords. [redacted]
13. **16 March:** Maintenance to address performance and capacity concerns.	No impact in terms of outage or downtime of iVote platform. [redacted]
14. **18 March:** Call centre and online application performance issues.	Unplanned service degradation and unplanned downtime of the call centre service for 1.5 hours. [redacted]
15. **22 March:** Online applications intermittently slow and/or unresponsive.	Unplanned service degradation impacting the voter registration. [redacted]
16. **23 March:** Registration system performance and availability issues.	Unplanned service degradation and impact on the voter registration. [redacted]
17. **23 March:** Voting system performance and availability issues.	Unplanned service degradation and impact on voting. [redacted]
18. **24 March:** Unable to download voter keys extract through user interface.	No impact in terms of outage or downtime of iVote platform. [redacted]

Appendix D – Incidental Unlock Procedures

D

Incidental Unlock Procedures

Incidental Unlock procedures

In addition to lockdown procedures, 19 incidental unlock procedures were also observed by PwC team. These incidental unlocks were performed for implementation of changes, investigation of logs, investigation of incidents and troubleshooting. Each unlock procedure included unlock of the servers by entering the split password by two senior members of NSWEC electoral board, performance of the specified activity and then implementation of the lockdown procedure.

Following are the incident unlock and lockdown procedures observed by PwC:

Registration and Credential Management System

1. **12 February 2019**
2. **21 February 2019**
3. **28 February 2019**
4. **5 March, 2019**
5. **8 March, 2019**
6. **13 March, 2019**
7. **16 March, 2019**
8. **18 March, 2019**
9. **18 March, 2019**
10. **22 March 2019**
11. **23 March 2019**
12. **24 March 2019**

Voting System

1. **8 March 2019**
2. **11 March 2019**
3. **13 March 2019**
4. **16 March 2019**

Assurance System

1. **8 March 2019**
2. **9 March 2019**
3. **14 March 2019**

Appendix E – Systems Overview

E

iVote systems overview

iVote - registration and credential management system

The registration and credential management system comprises of two main components and developed by NSWEC to allow the voter to register to vote using iVote, and to manage the voters iVote application. The registration system is an internet facing system that verifies the voters eligibility for iVote against the NSW voting roll. Once the voter has been successfully verified the credential management system receives the application from the registration system and creates an iVote number for the voter.

iVote - voting system

The voting system is supplied by the service provider Scytl and hosted by NSWEC's service provider Secure Agility. The voting system provides voters with a secure platform to cast their vote online or by telephone.

Voting website

To enter the voting website users must enter their iVote number and the password they created when they applied for iVote. The voter can vote on the Legislative Council and Legislative Assembly ballots. Once they submit their vote, it is securely transferred to the voting system to be included in the electronic ballot box. The user receives a receipt and can lookup on the assurance receipt portal to check their vote has been received by the voting system. In addition the assurance system provides the ability for voters to verify that their vote has been stored correctly (see iVote assurance system below).

Telephone voting

Voters have the ability to securely cast their vote via mobile or landline telephone using the Interactive Voice Response (IVR) platform that is part of the Scytl system. An iVote receipt is generated and can be checked in the same way as that of web voting receipt.

iVote - assurance system

The assurance system providers users with two different methods to verify their vote - the verification application and via the telephone verification for those who had voted using IVR. In addition, the assurance system maintain copies of the receipts from the voting system. The assurance system is hosted by NSWEC's service provider AC3.

Appendix F – Security Systems overview

F

Security Systems Overview

Security Information Event Management (SIEM)

The [redacted] monitoring system is used as a logging and intrusion alerting tool for the iVote - registration and credential management, voting and assurance systems. [redacted]

Anti-Virus (AV)

Antivirus/anti-malware scanning agents are installed across all the components of the internet voting system, on both workstations and servers. [redacted] All tools perform scans and update signatures on a regular basis.

Web Application Firewall (WAF)

Firewalls are used to segregate key components within each system to only allow for the required network traffic to flow between components, in accordance to the configured firewall rules. All three components of the iVote platform have appropriate WAFs implemented [redacted].

Two-Factor Authentication (2FA)

Operating system level login to the registration and credential management system, voting system and assurance system is restricted to authorised personnel via 2FA [redacted]

Host based Intrusion Prevention System (OSSEC)

OSSEC is an open-source, host-based intrusion detection system (HIDS) that is used to perform log analysis and monitor file integrity and OS level. It is integrated with the SIEM solution (Splunk) whereupon logs are captured and replicated to the cloud Symantec data system.

Security Systems Overview

File Integrity Monitor [redacted]

[redacted] is implemented on registration and credential management system and acts as a file integrity monitoring tool. The tool monitors the integrity of files by performing comparisons to determine file configurations, additions, deletions and changes. This comprehensive log monitoring supports daily audit of logs and NSWEC's internal reporting.

Access Management

NSWEC performed a lockdown procedure on each of their core systems (registration, voting, and assurance) prior to the election (refer to Appendix B: iVote processes).

DDoS Protection

NSWEC have implemented [redacted] against DDoS attacks. [redacted]

Vulnerability Management

NSWEC performed vulnerability assessment of registration and credential management system [redacted]. The vulnerabilities were then fixed by application of patches. The patch levels of voting and assurance systems were checked by comparing the version of installed packages with CVE scorecards. The vulnerability assessment exercise was performed prior to the lockdown.

Penetration Testing

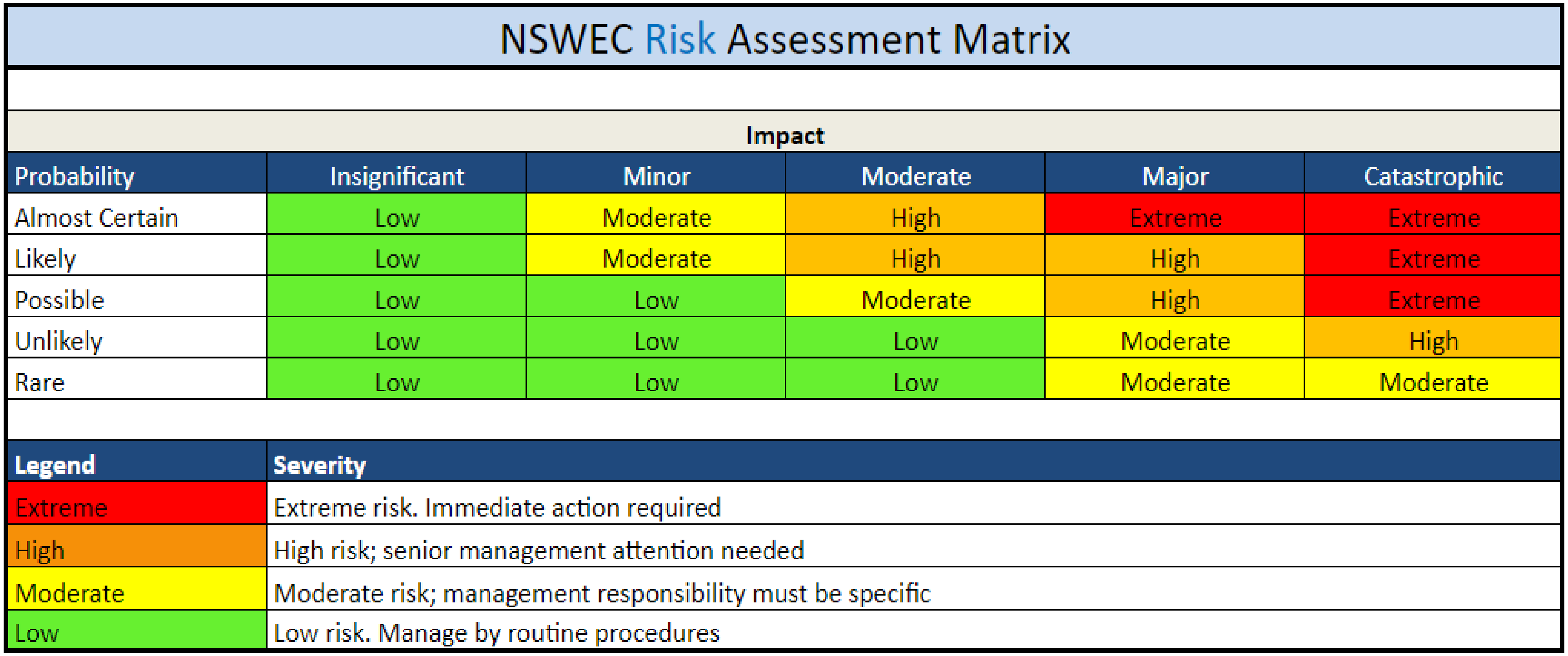
NSWEC perform both internal and external penetration testing on all iVote systems (registration, voting, and assurance). The objective of the exercises was to identify network level and application level vulnerabilities. The penetration testing exercises were performed prior to the lockdown.

Appendix G – NSWEC Risk Assessment Matrix

G

NSWEC Risk Assessment Matrix (1/2)

Following is the NSWEC Risk Assessment Matrix, which was used to quantify the risk of the identified findings.

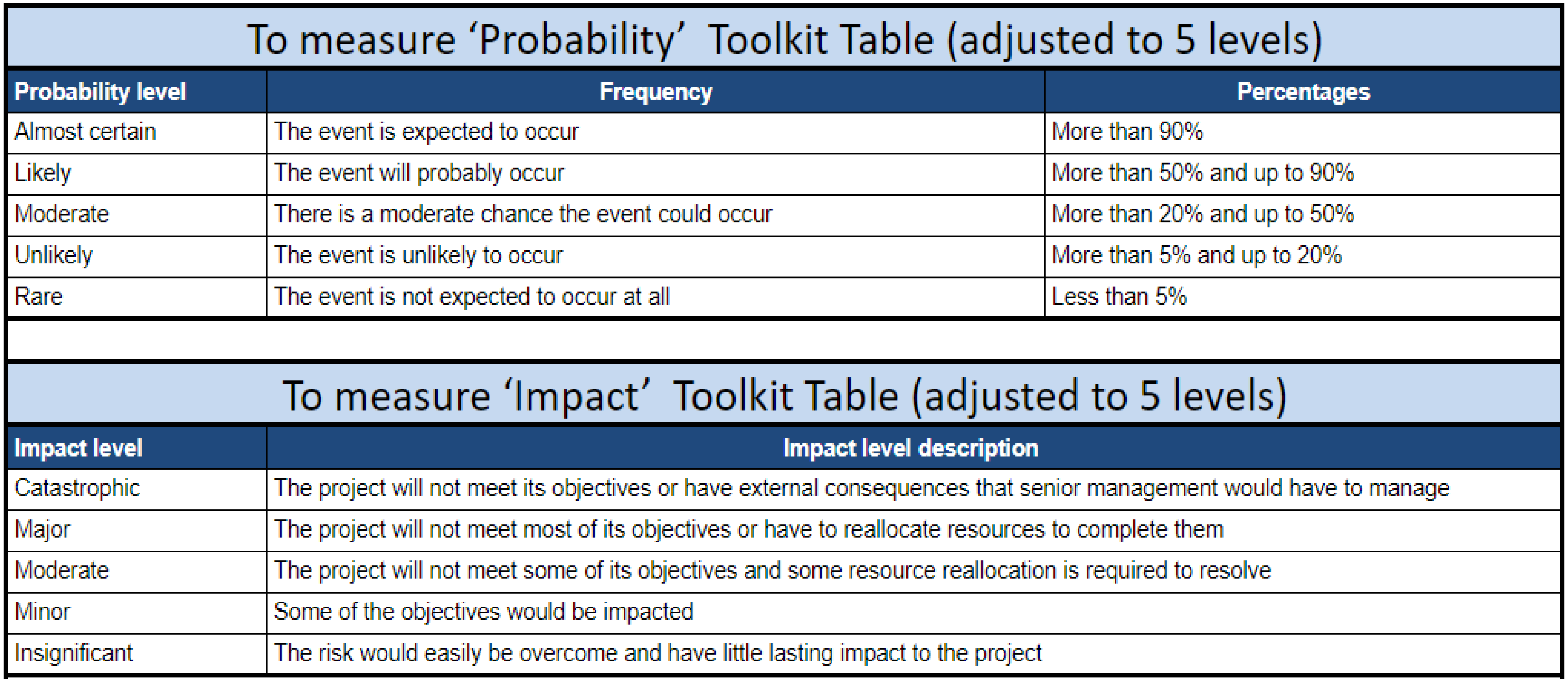


NSWEC Risk Assessment Matrix

	Impact				
Probability	Insignificant	Minor	Moderate	Major	Catastrophic
Almost Certain	Low	Moderate	High	Extreme	Extreme
Likely	Low	Moderate	High	High	Extreme
Possible	Low	Low	Moderate	High	Extreme
Unlikely	Low	Low	Low	Moderate	High
Rare	Low	Low	Low	Moderate	Moderate

Legend	**Severity**
Extreme	Extreme risk. Immediate action required
High	High risk; senior management attention needed
Moderate	Moderate risk; management responsibility must be specific
Low	Low risk. Manage by routine procedures

NSWEC Risk Assessment Matrix (2/2)



To measure 'Probability' Toolkit Table (adjusted to 5 levels)

Probability level	Frequency	Percentages
Almost certain	The event is expected to occur	More than 90%
Likely	The event will probably occur	More than 50% and up to 90%
Moderate	There is a moderate chance the event could occur	More than 20% and up to 50%
Unlikely	The event is unlikely to occur	More than 5% and up to 20%
Rare	The event is not expected to occur at all	Less than 5%

To measure 'Impact' Toolkit Table (adjusted to 5 levels)

Impact level	Impact level description
Catastrophic	The project will not meet its objectives or have external consequences that senior management would have to manage
Major	The project will not meet most of its objectives or have to reallocate resources to complete them
Moderate	The project will not meet some of its objectives and some resource reallocation is required to resolve
Minor	Some of the objectives would be impacted
Insignificant	The risk would easily be overcome and have little lasting impact to the project

Appendix I – Project timelines

I

Timelines - Specified procedures for iVote

Timelines

Stage	Requirement	Activity	Details	Planned Date
1	Performance of specified procedures defined in the Framework	Fieldwork – Performance of specified test procedures as defined in Framework	• Perform walkthrough of security controls through: • Perform enquiry and document reviews. • Perform system reviews and testing.	Feb 4 - Feb 15, 2019
		Preparation of work papers, evidences, and draft report	• Document the results and findings. • Document the recommendations. • Discuss the findings with NSWEC.	Feb 18 - Feb 22, 2019
		Issue of draft Pre-election Report to NSWEC	• Share draft Pre-election Report with NSWEC • Discuss the findings with NSWEC	Feb 23, 2019
Issue of final Pre-election Report			•	March 1, 2019
2	Performance of specified procedures defined in the Framework	Observation and test of controls during the lockdown period	• Observe the lockdown procedures and review the relevant controls implemented.	March 6-8, 2019
		Observation and test of controls during the decryption/end of election	• Observe the decryption procedures and review the relevant controls implemented.	March 23-24, 2019
		Preparation of work papers and evidences	• Document the review results and findings. • Document the recommendations. • Discuss the findings with NSWEC.	March 25 – April 11, 2019
		Issue of draft Post-election Report to NSWEC	• Share draft Post-election Report with NSWEC • Discuss the findings with NSWEC.	April 12, 2019
Issue of final Post-election Report				April 26, 2019

Note: The submission of the final post election report was delayed and report was submitted to the NSWEC on June 18, 2019. The delay was on the account of Preliminary Incident Reports (PIRs) of the incidents occurred during the election period. The PIRs were documented by NSWEC and were later reviewed by PwC.

Appendix J – Glossary

J

Glossary (1/2)

Term	*Explanation*
Elector	A person who is entitled to vote an election.
Electoral Board	The body appointed by the Electoral Commissioner to control the iVote system encryption/decryption process.
Electoral Council of Australia and New Zealand (ECANZ)	A forum where the Australian national, State and territory electoral commissions, and the New Zealand electoral commission, meet to discuss all aspects of electoral administration, encourage mutual cooperation, and consider contemporary electoral challenges aimed at improving access and equality for all eligible electors.
NSWEC	New South Wales Electoral Commission.
iVote	The NSWEC Electronic Commission electronic voting system comprises the software components, hardware, networking, procedures and protocols required to deliver remote electronic voting services for the benefit of eligible NSW electors. The three key components of iVote are: (1) registration and credential management system, (2) voting system, and (3) assurance system.
iVote ecosystem	The systems, infrastructure, process and procedures that together support the three functions of iVote: apply, vote and verify.
iVote number	A unique eight digit number provided to each voter who applies to use the iVote system.
iVote receipt website	Allows voters to verify that their vote is stored in iVote by verifying their receipt number provided to them after submission of the vote.
iVote verification application	A smartphone application that the elector has to install onto their device to verify that iVote has correctly captured and stored their video unaltered.
iVote voting website	The interface the elector uses to cast their vote using iVote. The website is part of the iVote voting system.
Virtual Ballot Box (VBB) or electronic ballot box	A database corresponding to a physical ballot box in which the votes cast using iVote are accumulated

Glossary (2/2)

Term	*Explanation*
iVote IVR Verification	Allows a voter to confirm by phone that their preferences were captured by the system correctly.
Postal voting	A voting channel offered together with the iVote channel for voters unable to attend a voting centre on the day of the election.
Silent elector	An elector who has satisfied the Electoral Commissioner that their residential address should be omitted from any authorised roll or list of electors on the grounds that having that address on a roll or list of electors places or would place the personal safety of the person or of members of the person's family at risk.
Virtual ballot box	A database similar to that of a physical ballot box where the votes cast from iVote are accumulated.
Virtual ballot paper	An electronic ballot paper that is unique to each voter. It is provided online in the iVote voting system for voters to cast their vote.
Voting channel	A method to which voters may choose to cast their vote. NSWEC will provide voters with multiple methods of voting including postal voting, early voting, absent voting and iVote.
Control Assessment Framework	NSWEC has developed a control assessment framework which draws guidance from the Electoral Council of Australia and New Zealand ("ECANZ") principles and a number of global best practices on online voting.