NSW Electoral Commission

X	ECANZ Principles Applicability

Taxonomy

Mapping to COE Standard	The control objectives are mapped to recommendations of Committee of Ministers to member States on standards for e-voting (Adopted by the Committee of Ministers on 14 at the 1289th meeting of the Ministers' Deputies). The CoE provided 49 Recommendations.
Mapping to ISO 27001	ISO 27001 Appendix A has 114 controls in 35 control categories and addresses procedural, technical and operational information security controls.
Mapping to VVSG	Voluntary Voting System Guidelines 2.0 are published by NIST and has 15 key principles for electoral voting system.

						ECANZ Principles										
						Enfranchisement			Integrity						Privacy	
CO#	**Control Objectives**	**Number of Controls**	**Mapping to CoE Standard**	**Mapping to ISO 27001 Appendix A**	**VVSG Mapping**	**Accessibility**	**Usability**	**One person, one vote**	**Security**	**Robustness**	**Transparency**	**Independence**	**Impartiality**	**Accuracy**	**Secrecy of cast vote**	**Privacy of personal Information**
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**	Recommendation # 40	A.5 Security Policies				X	X	X	X	X	X	X	X	X
2	Mechanism should be implemented to make voters effectively and accurately use the internet voting system.	**7**	Recommendation # 4 Recommendation # 14 Recommendation # 16		7.3, 3.3	X	X				X		X			
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**	Recommendation # 5 Recommendation # 10		7.1, 5.1, 5.2, 7.3	X	X				X	X	X	X		
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**	Recommendation # 6 Recommendation # 9 Recommendation # 17 Recommendation # 49		1.2			X			X			X		
5	The voter interface of the internet voting system shall be easy to understand and use.	**5**	Recommendation # 1 Recommendation # 2		8.3, 7.2, 3.3	X	X									
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**	Recommendation # 7 Recommendation # 8 Recommendation # 11 Recommendation # 18 Recommendation # 21	A.9 Access Control	11.3			X	X					X		X
7	Protection of personally identifiable information (PII) and privacy of data collected by the internet voting system shall be ensured.	**8**	Recommendation # 20 Recommendation # 22	A.9 Access Control A.18.2 Compliance with legal and contractual requirements	10.1, 10.2, 6.1										X	X
8	Open standards shall be used to enable various technical components or services, to inter-operate.	**4**	Recommendation # 35		4.1, 4.2, 4.3, 4.4					X	X	X				
9	Detection and monitoring capability shall be developed to detect unauthorized activities.	**6**	Recommendation # 39	A.12.4 Logging and monitoring	9.3,9.4, 15.1, 15.2, 11.1				X	X	X	X	X			
10	Mechanism should be implemented to ensure that only validated personnel are given access to internet voting system.	**5**	Recommendation # 41	A.7 Human Resource Security A.9 Access Control A.15.1 Security in supplier relationships	11.2			X	X					X		
11	Before an election, the electoral management body shall satisfy itself that the internet voting system operates correctly.	**3**	Recommendation # 42	A.14.2 Security in development and support processes	14.3	X	X	X	X	X	X	X	X	X	X	X
12	A procedure shall be established to identify vulnerabilities and regularly installing updated versions and corrections of all relevant software.	**7**	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				X	X						
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**	Recommendation # 18	A.9 Access Control	13.1, 11.2, 11.3, 11.4, 11.5, 15.4				X	X		X			X	X
14	internet voting system's network shall be managed, controlled and segmented to protect information in systems and applications.	**16**		A.13.1 Network security management	15.4				X	X						X
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**		A.14.2 Security in development and support processes	1.3, 9.1, 14.4, 1.1	X	X			X		X		X		

16	Use of secure development practices, testing, and operating environment to ensure integrity of iVote System.	**5**		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				X	X				X	X	X
17	Detection, prevention and recovery controls to protect against malware shall be implemented, and operated.	**3**		A 12.2 Protection from Malware	15.3				X	X						
18	Procedure on encryption shall be developed and implemented for the use of cryptography to protect votes and voter data during election.	**9**	Recommendation # 44, #45	A 10.1 Cryptographic Controls	13.3				X				X	X	X	X
19	Physical protection and guidelines for secure areas (critical office locations, data centre etc.) and equipments shall be designed and applied.	**6**	Recommendation # 32	A 11 Physical and Environmental Security	12.1, 12.2				X	X						
20	Procedures and capabilities related to business continuity and resilience is established to operate effectively during a time of an incident.	**9**	Recommendation # 40	A.17.2 Redundancies	14.1					X						
21	Provisions should be put in place to maintain Confidentiality, Availability and Integrity (CIA) of the voting system.	**2**		A.8.2 Information classification	13.4				X	X				X		X
22	Information security incidents shall be responded and reported to in accordance with the documented procedures.	**5**	Recommendation # 47	A.16 Information security incident management	15.1, 15.2, 15.4				X	X						
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**	Recommendation # 15	A.12.7 Information systems audit considerations	9.2, 6.2			X			X			X		
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**	Recommendation # 26 Recommendation # 19 Recommendation # 25	A 10.1 Cryptographic Controls	10.1, 10.2										X	X
25	Procedures shall be implemented for the management and handling of removable media during the election process.	**3**		A.8.3 Media handling	15.4, 14.3				X							