

**Deloitte.**

Electoral Cyber Security Maturity Review  
Whole of Nation Report

October 2018

## Table of Contents

Executive Summary .....	4
Overall Assessment .....	4
Recommendations.....	5
1. Introduction .....	7
Electoral Cyber Maturity Review.....	8
<i>Assessment Framework</i> .....	8
<i>Conduct of Jurisdictional Reviews</i> .....	9
2. Whole of Nation Assessment and Recommendations .....	11
Key findings.....	11
Recommendations.....	12
Monitoring, Detection and Response Capability.....	13
Threat Intelligence Sharing .....	13
Assurance Mechanisms .....	14
Share Resources and Better Practices .....	14
Electoral Systems deemed as 'Critical Infrastructure' .....	15
3. Glossary.....	17
4. Appendices .....	19
Appendix A - Summary of Jurisdictional Reviews against Assessment Framework.....	19
Foundational Elements.....	19
Strategy and Governance .....	20
Protect/Secure.....	21
Monitor/Detect.....	22
Respond/Recover .....	23
Future State Processes .....	24
Essential Eight .....	25
Appendix B – The Future State of Australia's Electoral Systems .....	31
Key Considerations .....	31
Appendix C – Three Lines of Defence Model .....	34

#### Inherent Limitations

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

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

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

Recommendations and suggestions for improvement should be assessed by management for their full commercial impact before they are implemented. We believe that the statements made in this report are accurate, but no warranty of completeness, accuracy, or reliability is given about the comments and representations made by and the information and documentation provided by the Electoral Commission personnel. We have not attempted to verify these sources independently unless otherwise noted within the report.

#### Limitations of use

This report is intended solely for the information and internal use of Home Affairs and the Australian Cyber Security Centre (ACSC), in accordance with our Work Order of 13 June 2018, and is not intended to be and should not be used by any other person or entity. No other person or entity is entitled to rely on, in any manner, or for any purpose, this report. We do not accept or assume responsibility to anyone other than Home Affairs for our work, for this report, or for any reliance which may be placed on this report by any party other than Home Affairs.

## Executive Summary

Many aspects of Australian Federal, state and territory electoral processes are now heavily reliant on the use of Information and Communication Technology (ICT). Increased usage of ICT in the Australian electoral system is making delivery of electoral functions more efficient but also presents a significant cyber security risk. The targeting of ICT systems used in electoral systems by various state and non-state actors is increasing. These attacks are not necessarily aimed at stealing data or causing any tangible damage to electoral systems, but rather appear to be aimed at undermining public confidence in the validity of the democratic process.

Electoral systems security should be seen as integral to Australians' trust and confidence in our democracy. Reports of attempted or successful cyber security breaches can spread quickly given the prolific use of social media as a communication platform. This increases the ease with which adversaries can sow doubt in the security and integrity of electoral processes. This risk further increases in highly partisan and closely contested elections, and can undermine public confidence in the integrity of Australian democracy.

Deloitte was appointed by the Department of Home Affairs (Home Affairs) to undertake a review to determine the cyber security maturity of Federal, state, and territory electoral commissions. Deloitte has now completed its review and individual, confidential outcome reports have been delivered to the nine commissions, Home Affairs, and the Australian Cyber Security Centre (ACSC). This Whole of Nation report draws from work undertaken during the jurisdictional reviews, to present an overall picture of Australia's electoral cyber security and identifies ways to strengthen the cyber security of the overall electoral landscape.

## Overall Assessment

s33(a)(i)



Despite the federated nature of the Australian electoral landscape, any perceived lack of trust in the integrity of an individual electoral commission's systems security can be extended to all electoral commissions. Therefore, in the context

**PROTECTED**

of cyber security, all federated elements must be treated as part of one interconnected electoral landscape, and thus subject to the similar level of protection. Electoral commissions must therefore collaborate and take a proactive approach to reducing the likelihood and/or impact of any future cyber incidents and to strengthen the resilience of the overall electoral system.

s33(a)(i)



Released by Department of Home Affairs  
under the *Freedom of Information Act 1982*

**PROTECTED**

~~PROTECTED~~

s33(a)(i)



~~PROTECTED~~

## 1. Introduction

Free and fair elections at all levels of government are a fundamental tenet of Australian democracy. Australian citizens vote for people to represent them through regular elections.

The Australian Electoral Commission (AEC) administers federal elections. State and territory electoral commissions administer relevant state, territory, and local council elections. All states and territories have their own legislative provisions governing the electoral process, such as election timings and how the results are determined. Notwithstanding the differences in the detail of processes followed between federal, state, territory and local elections, broadly, the electoral process consists of the following three sets of activities:

1. Pre-election;
2. Election day; and
3. Post-election.

With rapid advancements in ICT solutions as a driver of efficiency, integration of ICT throughout electoral functions and processes is also increasing. Hence, consideration and action must be taken to develop and implement robust cyber security measures across jurisdictions.

In order for electoral commissions to fulfil their purpose and maintain public trust and confidence in the democratic process, they must be able to safeguard the:

- *Confidentiality* of data, including but not limited to the voters' personally identifiable data and voting preferences in the systems that receive, store, and process a significant amount of Australian citizens' personal data and vote tally data;
- *Integrity* of data and results, to ensure that it is protected from manipulation; and
- *Availability* of systems, such as the systems which automate processes which have strict cut-offs such as voter enrolment and candidates registrations.

Figure 1 below illustrates the key ICT infrastructure supporting the core electoral activities and the potential threats that could affect activities.

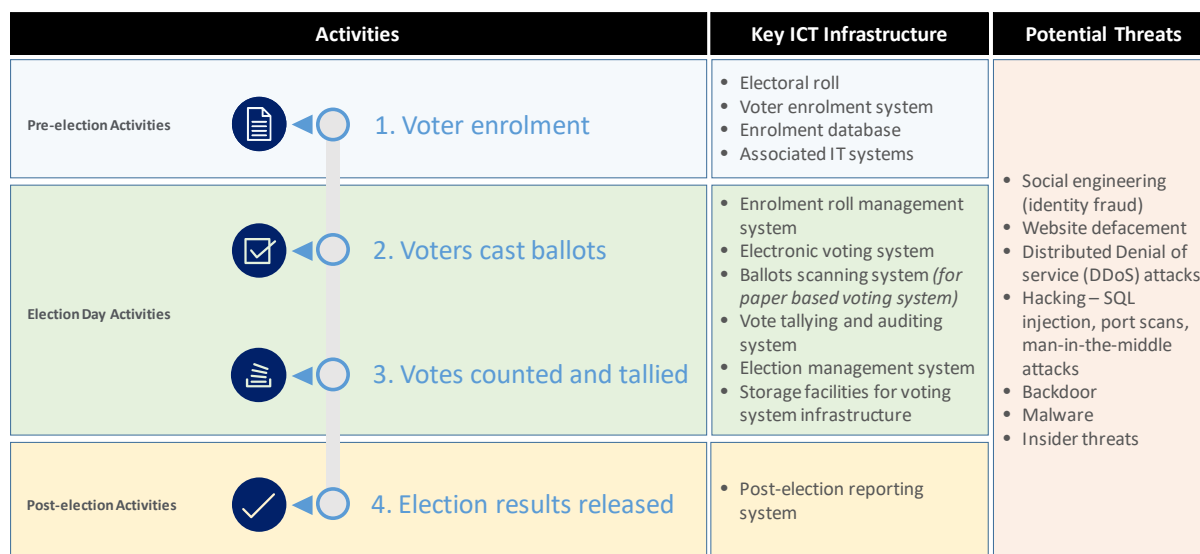


Figure 1: Activities of the Electoral Process

### Electoral Cyber Maturity Review

Deloitte was appointed by the Department of Home Affairs (Home Affairs) to undertake a review and determine the cyber security maturity of federal, state, and territory electoral commissions. The review process was conducted in three phases:

1. Develop and evaluate a common assessment framework for the reviews.
2. Conduct a review of each jurisdiction, which included providing confidential individual outcome reports to each Commission, Home Affairs, and the ACSC.
3. A final, anonymised 'Whole of Nation' report detailing an overall picture of Australia's electoral cyber security, to be provided to the Council of Australian Governments (COAG).

### Assessment Framework

To provide a comprehensive assessment whilst also benchmarking maturity across various jurisdictions, a detailed assessment framework was developed in consultation with Home Affairs, and the Australian Cyber Security Centre (ACSC). The assessment framework incorporated elements of the Australian Government Information Security Manual (ISM), the Australian Signals Directorate (ASD) *Strategies to Mitigate Cyber Security Incidents*, the US National Institute of Standards and Technology (NIST) standards, and Deloitte's internally developed materials.

Deloitte's review of electoral commissions provided an assessment of both governance and technical cyber security maturity against six assessment domains, as outlined in the high-level architecture of the assessment framework in Figure 2 below. It was primarily intended to enable electoral commissions and



its organisational risk holders to better understand the maturity of their cyber security risk management processes.

s47G



#### *Conduct of Jurisdictional Reviews*

The review was undertaken through a series of documentation reviews followed by workshops to discuss and validate information received.

**Document Reviews:** An initial high-level questionnaire and documentation request was distributed to the electoral commissions to gain an understanding of:

- The overall ICT environment (typical to most corporate organisations);
- Relevant policies and procedures; and
- Key electoral business functions and processes.

**Workshops:** Information gathered, and initial assessment findings were further clarified and maturity ratings validated through interactive workshops. Representatives from each commission included personnel that manage ICT operations, governance, and electoral functions. Key activities conducted in each workshop included:

- A walk-through of the assessment rubric;
- Desktop scenarios;
- In-depth discussions of concerns and risks faced by commissions; and
- A collective agreement on the maturity rating of the Commission for each sub-domain.

As the reviews were 'point-in-time' assessments, the findings and recommendations provided to individual commissions were based on an

assessment of controls implemented at the time of review. As the electoral-specific cyber risk landscape and exposure continues to evolve, electoral commissions were advised to continually review and re-evaluate their cyber security posture and operating environments to ensure that robust mechanisms are in place to manage and mitigate cyber security risks.

The review did not include an in-depth technical assessment, substantive controls testing, or the mitigation of any identified deficiencies.

Deloitte has now completed its review of each jurisdiction and delivered individual, confidential outcome reports to the nine commissions, Home Affairs, and the Australian Cyber Security Centre (ACSC). For a summary of assessment of jurisdictions against the assessment domains of the framework, refer to Appendix A.

Section 2 below provides the overall assessment and recommendations from a Whole of Nation perspective.

2. Whole of Nation Assessment and Recommendations

The cyber security framework, as depicted in Figure 3, provides a view to look at threats and vulnerabilities that present risks to the assets and reputation of electoral commissions and the responses to these risks. Responses can be categorised as one of two types, depending on the vulnerabilities identified:

- Specific recommendations applied at the individual commission level, which have been provided through individual reports; and
- Collaborative responses, which utilise collective knowledge and resourcing across jurisdictions to strengthen cyber security resilience of the overall system.

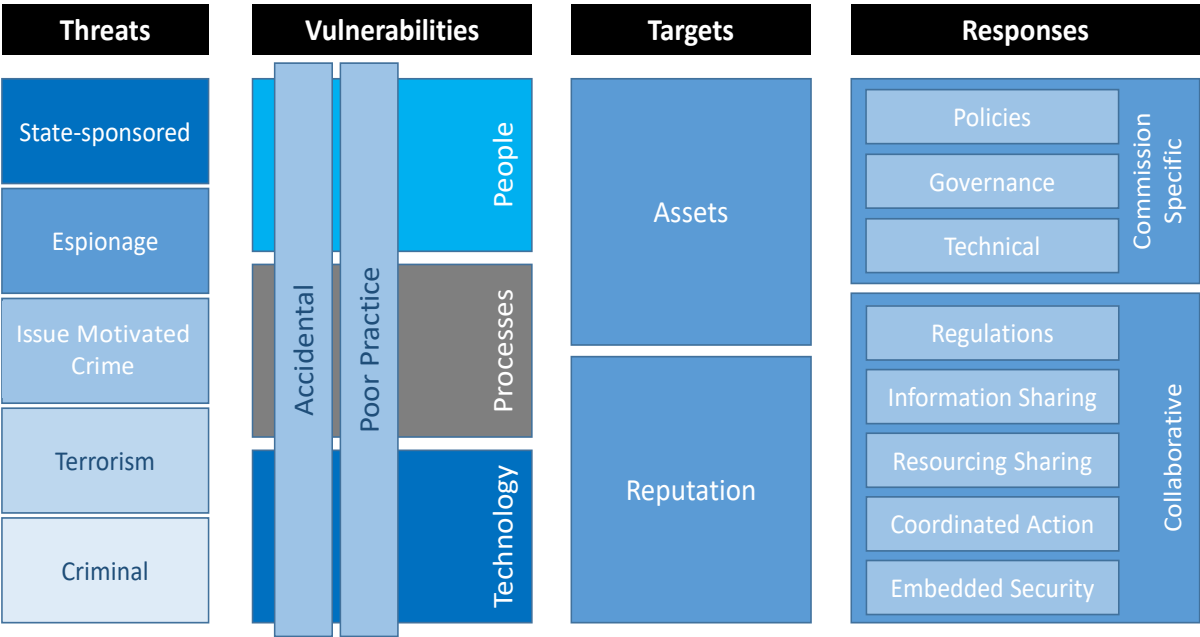


Figure 3: Cyber Security Framework

s33(a)(i)

Released by Department of Home Affairs  
under the Freedom of Information Act 1982

s33(a)(i)



s33(a)(i)



The main concern is not the actual damage that cyber attacks can cause to individual electoral system components, although it exposes the individual jurisdiction to significant reputational damage. The bigger concern is that any reports of attempted or successful breaches gives adversaries the ability to sow doubt in the security and integrity of electoral processes. Therefore, an attack on one part of the system must be seen as an attack on the system as a whole.

s33(a)(i)



To maintain public trust and faith in democratic processes, it is imperative that actions are undertaken to ensure that all elements of electoral processes are provided sufficient protection.

## Recommendations

Following are the key recommendations from a 'Whole of Nation' perspective.

## Monitoring, Detection and Response Capability

s33(a)(i)



s33(a)(i)



Well-designed cyber security incident response plans and regular simulation of cyber incidents and testing the effectiveness of current incident response plans is essential to ensure electoral commissions are ready to respond.

At a Whole of Nation level, a multi-stakeholder approach should be applied to ensure consistent procedures are in place for incident detection and response processes. This approach can assist in prioritisation and pooling of resources to better respond to cyber security events if and/or when they do eventuate.

s33(a)(i)




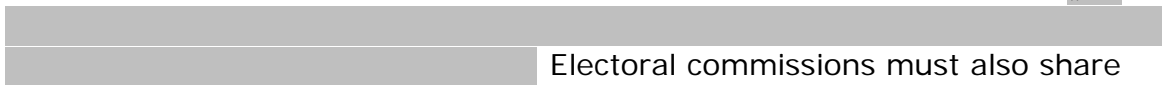
## Threat Intelligence Sharing

s33(a)(i)



Timely threat intelligence is critical to all the commissions to assess whether their systems are vulnerable to specific threats and instigate preventative measures to protect systems and data.

To facilitate a consistent and near real time dissemination of threat intelligence across jurisdictions, a coordinated and consistent approach is required. 

 Electoral commissions must also share threat intelligence through ACSC.

It is recommended that:

s33(a)(i)

### Assurance Mechanisms

Basic cyber capabilities – possessed by even the most amateur malicious actors – prove very effective against targets with poor security practices.<sup>1</sup> Mere drafting of policies and procedures is not sufficient to protect against cyber security adversaries. Periodically reviewing compliance with internal security frameworks and assessing the effectiveness of cyber security controls is also needed.

s33(a)(i)

*Three Lines of Defence Model:* A Three Lines of Defence model is one of the leading risk governance frameworks commonly used across the industry and Commonwealth agencies. The three lines are typically defined as first line being the operational management as owning the risks, second line providing oversight and third line providing independent assurance such as an organisation's internal audit function or an external assurance provider. This model can be considered to review and define risk management roles and responsibilities across the commissions. A suggested Three Lines of Defence Model is provided at Appendix B. It is a generic example only and would require tailoring to meet the needs of commissions.

At a Whole of Nation level, it is worth considering whether resources can be pooled, with leadership from ACSC, to provide the 'third line of defence' through regular independent assurance mechanisms.

It is recommended that:

s33(a)(i)

### Share Resources and Better Practices

s33(a)(i)

s33(a)(i)

s33(a)(i)

There were some examples of well-developed and comprehensive security documentation in some jurisdictions.

s33(a)(i)

As a part of literature scan during the Deloitte review, it was noted that in some of the other comparable international jurisdictions, specific technical guidance has been developed to assist organisations to consider and apply cyber security controls to systems involved in electoral processes. Examples include the European '*Compendium on Cyber Security of Election Technology*' and the US '*The State of Local Election Cybersecurity Playbook*'. There is currently no such guidance for Australian electoral organisations. Such guidance can assist commissions to design their security policies and procedures with targeted security controls to mitigate specific risks.

There is an opportunity for electoral commissions to pool resources to develop generic strategies, policies and procedures and then tailor according to their individual environments. However, care must be taken to ensure that application of these generic resources is fit-for-purpose and specific to the environment and tailored where necessary to address any commission specific threats or vulnerabilities.

It is recommended that:

s33(a)(i)

### **Electoral Systems deemed as 'Critical Infrastructure'**

Over the last few years, there has been a focussed discussion on sectors of Australian economy and government, which require attention due to the criticality of the infrastructure in those sectors to national security. The federal *Security of Critical Infrastructure Act 2018* (the SoCI Act), came into effect in July 2018 to formalise and legislate key processes and structures to manage risks to national security relating to critical infrastructure. Specifically, the SoCI Act provisions are designed to manage the complex and evolving national security risks of sabotage, espionage and coercion posed by foreign involvement in Australia's critical infrastructure. The SoCI Act contains a range of powers, functions and obligations that only apply in relation to specific critical

infrastructure assets in the electricity, gas, water and ports sectors. Critical infrastructure is defined by the SoCI Act as<sup>2</sup>:

physical facilities, supply chains, information technologies and communication networks which, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact the social or economic wellbeing of the nation or affect Australia's ability to conduct national defence and ensure national security.

Based on the above definition, arguably, the Australian electoral infrastructure can be seen as critical to our 'social and economic wellbeing' and therefore consideration should be given to designating Australia's electoral systems as 'critical infrastructure'.

Based on experience in the US, where the Department of Homeland Security designated the US 'elections infrastructure' as critical infrastructure in 2017, this conversation is not going to be easy or uncontroversial. The US experience suggests that there was opposition by the states with allegations of federal overreach, but overall this has formalised ways for various levels of election bodies to work together to enhance the overall security and resilience of the US electoral system.

It is recommended that:

s33(a)(i)



---

<sup>2</sup> Critical Infrastructure Centre, *Coverage of the Security of Critical Infrastructure Act 2018*, <https://www.homeaffairs.gov.au/nationalsecurity/Documents/cic-factsheet-coverage-of-security-of-critical-infrastructure-act-2018.pdf>, viewed September 2018.



### 3. Glossary

<u>Term</u>	<u>Definition</u>
<b>Attack surface</b>	Describes all of the different points where an attacker could get into a system, and where they could get data out.
<b>Assurance</b>	The demonstrated ability of an entity to perform its security objectives, determined from evidence produced by the assessment process of an entity.
<b>Cyber attack</b>	A breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant.
<b>Cyber resilience</b>	The ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.
<b>Cyber Security</b>	Measures relating to the confidentiality, availability and integrity of information that is processed, stored and communicated by electronic or similar means.
<b>General users</b>	A user who can, with their normal privileges, make only limited changes to a system and generally cannot bypass system security.
<b>Incident Response Plan (IRP)</b>	The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyber attack against an organisation's information system(s).
<b>Penetration testing</b>	A specialised type of assessment conducted on information systems or individual system components to identify vulnerabilities that could be exploited by adversaries. Such testing can be used to either validate vulnerabilities or determine the degree of resistance organisational information systems have to adversaries within a set of specified constraints (e.g., time, resources, and/or skills).
<b>Privileged users</b>	A user who can alter or circumvent system security protections. This can also apply to users who could have only limited privileges, such as software developers, who can still bypass security precautions. A privileged user can have the capability to modify system configurations, account privileges, audit logs, data files or applications.

<b>Security controls</b>	A safeguard or countermeasure prescribed for an information system or an organisation designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements.
<b>Threat intelligence</b>	Intelligence outlining a circumstance or event with the potential to harm an information system through unauthorised access, destruction, disclosure, modification of data, and/or denial of service. The intelligence may also outline methods to protect an information system or prevent such an event.
<b>Threat scenarios</b>	A set of discrete threat events, associated with a specific threat source or multiple threat sources, partially ordered in time.
<b>Vulnerability assessment</b>	Involves determining possible remediation actions and the level of acceptance for identified weaknesses in system security requirements, design, implementation or operation that could be accidentally triggered or intentionally exploited and result in a violation of the system's security policy.

## 4. Appendices

### Appendix A - Summary of Jurisdictional Reviews against Assessment Framework

#### Foundational Elements

This domain was designed to assess the commission's degree of governance over its data responsibilities, management of its assets, and vendors and third parties. The key questions and criteria for each sub-domain assessed as part of Foundational Elements are outlined below:

- **Know Your Data:** This sub-domain was designed to assess the extent to which electoral commissions were aware of, and could articulate, the value of the data it managed, and whether they understood their data responsibilities.
- **Know Your Assets:** This sub-domain was designed to assess whether electoral commissions identified, prioritised, and managed its assets, based on the criticality of each asset. The review also assessed electoral commissions' asset change management processes.
- **Know Your Vendors and Third Parties:** This sub-domain was designed to assess whether electoral commissions were able to define responsibilities and processes for their vendors and third parties and examined how electoral commissions assessed their vendors and third parties' cyber security posture.

s33(a)(i)



Released by Department of Home Affairs  
under the Freedom of Information Act 1982

## Strategy and Governance

This domain was designed to assess the extent to which the commission implements and manages governance processes, defines and follows risk management strategies, promotes a cyber-aware culture and implements security policies and procedures. The key questions and criteria for each sub-domain assessed as part of Strategy and Governance are outlined below:

- **Overall Governance Processes:** This sub-domain was designed to assess electoral commissions' cyber governance.
- **Risk Management Strategies:** This sub-domain was designed to assess how electoral commissions managed risk, the workflow of risk management, prioritisation of cyber security risks, and the level of staff awareness of cyber security risks and processes.
- **Cyber Security Culture:** This sub-domain was designed to assess the extent to which electoral commissions and their management team promote a "cyber aware" culture. Assessment of this sub-domain also examined personnel's awareness of their responsibilities in maintaining a cyber-secure posture.
- **Security Policies and Procedures:** This sub-domain was designed to assess whether electoral commissions maintained cyber security policies and procedures.

s33(a)(i)



Released by Department of Home Affairs  
under the Freedom of Information Act 1982

## Protect/Secure

This domain was designed to assess the extent to which the commission promotes awareness of cyber threats, provides cyber security training and implements access controls in seeking to protect data held. The key questions and criteria for each sub-domain assessed as part of Protect/Secure are outlined below:

- **Awareness and Training:** This sub-domain was designed to assess whether relevant personnel are aware of their cyber security responsibilities, as well as the frequency of appropriate cyber security training.
- **User and Role-based Access Control:** This sub-domain was designed to assess electoral commissions' processes and controls for checking systems, applications and database access.
- **User Authorisation Process:** This sub-domain was designed to assess the efficiency of electoral commissions' procedures for granting system, application, and database access.
- **Privileged Access Controls:** This sub-domain was designed to assess how electoral commissions implement processes for granting privileged system access, including monitoring and logging access, and associated rules governing the use of privileged accounts.

s33(a)(i)



Released by Department of Home Affairs  
under the *Freedom of Information Act 1982*

### Monitor/Detect

This domain was designed to assess the extent to which the commission applies monitoring and detection policies and procedures, and implements effective strategies. The key questions and criteria for each sub-domain assessed as part of Monitor/Detect are outlined below:

- **Monitoring Processes:** This sub-domain was designed to assess electoral commissions' ability to implement and maintain monitoring processes, as they extend to networks, servers, physical environments, and personnel.
- **Detection Processes:** This sub-domain was designed to assess electoral commissions' ability to define roles and responsibilities for the detection of cyber events to ensure accountability, including how electoral commissions test and improve their detection processes over time.

s33(a)(i)



Released by Department of Home Affairs  
under the *Freedom of Information Act 1982*

## Respond/Recover

This domain was designed to assess the extent to which the commission engages in cyber security incident response and recovery planning, including analysis and mitigation strategies, and communicates to its stakeholders in the event of a cyber-attack. The key questions and criteria for each sub-domain assessed as part of Respond/Recover are outlined below:

- **Response Planning:** This sub-domain was designed to assess electoral commissions' proficiency at planning, implementing, and communicating effective and robust responses to cyber security incidents.
- **Communications:** This sub-domain was designed to assess the preparedness of electoral commissions to handle various internal and external communication requirements in the event of a cyber incident.
- **Analysis:** This sub-domain was designed to assess electoral commissions' capability to undertake effective incident response analyses.
- **Mitigation:** This sub-domain was designed to assess electoral commissions' mitigation capabilities and processes, mitigation activities, controls to prevent expansion of a cyber event, mitigate its impact, and resolve the incident.
- **Recovery Planning:** This sub-domain was designed to assess electoral commissions' understanding of recovery processes and sought to assess the design effectiveness of their recovery policies and procedures.
- **Continuous Improvement:** This sub-domain was designed to assess the ability of electoral commissions to prepare for future incidents and ensure stronger protection for systems and information.

s33(a)(i)

Released by Department of Home Affairs  
under the Freedom of Information Act 1982

### Future State Processes

This domain was designed to assess electoral commissions' incorporation of cyber security, from both a governance and technical point of view, when planning for, designing, testing, and deploying new technologies.

s33(a)(i)





s33(a)(i)

This domain assessed electoral commissions' alignment with the Australian Signals Directorate's (ASD) Essential Eight Strategies to mitigate cyber security incidents. ASD advises that while no single mitigation strategy is guaranteed to prevent cyber security incidents, organisations are recommended to implement eight essential mitigation strategies as a baseline. This baseline, known as the Essential Eight, makes it much harder for adversaries to compromise systems.

1. Application Whitelisting
2. Patch Applications
3. Configure Microsoft Office Macro Settings
4. User Application Hardening
5. Restrict Administrative Privileges
6. Patch Operating Systems
7. Multi-factor Authentication
8. Daily Backups

s33(a)(i)

s33(a)(i)

s33(a)(i)



**Patch Applications** e.g. Flash, web browsers, Microsoft Office, Java and PDF viewers. Patch/mitigate computers with 'extreme risk' vulnerabilities within 48 hours. Use the latest version of applications.

s33(a)(i)



Released by Department of Home Affairs  
under the *Freedom of Information Act 1982*

s33(a)(i)



**Configure Microsoft Office Macro Settings** to block macros from the Internet, and only allow vetted macros either in 'trusted locations' with limited write access or digitally signed with a trusted certificate.

s33(a)(i)



Released by Department of Home Affairs  
under the *Freedom of Information Act 1982*

**User Application Hardening.** Configure web browsers to block Flash (ideally uninstall it), ads and Java on the Internet. Disable unneeded features in Microsoft Office (e.g. OLE), web browsers and PDF viewers.

s33(a)(i)



**Restrict Administrative Users** to operating systems and applications based on user duties. Regularly revalidate the need for privileges. Don't use privileged accounts for reading email and web browsing.

s33(a)(i)



Released by Department of Home Affairs  
under the *Freedom of Information Act 1982*

**Patch Operating Systems.** Patch/mitigate computers (including network devices) with 'extreme risk' vulnerabilities within 48 hours. Use the latest operating system version. Don't use unsupported versions.

s33(a)(i)



Released by Department of Home Affairs  
under the *Freedom of Information Act 1982*

**Multi-Factor Authentication** including for VPNs, RDP, SSH and other remote access, and for all users when they perform a privileged action or access an important (sensitive/high-availability) data repository.

s33(a)(i)



**Daily Backups** of important new/changed data, software and configuration settings, stored disconnected, retained for at least three months. Test restoration initially, annually and when IT infrastructure changes.

s33(a)(i)



Released by Department of Home Affairs  
under the *Freedom of Information Act 1982*

## Appendix B – The Future State of Australia’s Electoral Systems

When Australia is in a position to implement a large-scale electronic system to support voting processes, a number of considerations must be taken into account. Below is a high-level summary of the key considerations developed by the National Democratic Institute (NDI) and outlined in their publication “Implementing and Overseeing Electronic Voting and Counting Technologies”.<sup>3</sup>

s33(a)(i)

the below considerations need to be addressed during the process of selecting and incorporating future technology solutions into electoral processes.

### Key Considerations

#### Public Confidence

Public confidence relies heavily upon transparency, it is essential voters understand and have confidence in the electronic voting and counting technology in use. Public confidence requires stakeholders are engaged in the process of technology considerations; educated on the technology in use; included in simulation and testing of the systems; able to monitor testing, certification and auditing of the systems and processes; and receive accurate and timely information regarding the introduction, timeline and activities surrounding the technology implementation.

#### Security Measures

The opportunity for systematic manipulation of voting processes means that system security needs to be a priority in the planning process. Security measures need to ensure the ability to authenticate system configuration and generated results; data is not lost in the event of a system interruption; only authorised personnel are able to access the voting, counting and results management functionality; and integrity of functionality is able to be observed and monitored.

#### Auditability and Recount

In order to ensure the accuracy of the generated results, the electronic voting and counting technology must be auditable, and able to conduct a recount. Recounts must include the ability to monitor a manual recount of the casted votes, not simply a repetition of the electronic counting process.

<sup>3</sup> National Democratic Institute, *Implementing and Overseeing Electronic Voting and Counting Technologies*, <https://www.ndi.org/e-voting-guide/how-to-use-this-manual>, viewed September 2018.

### ***Secrecy of the Ballot***

Secrecy of the ballot must be ensured throughout the use of electronic voting and counting technologies. This standard is made more complex by the utilisation of electronic voting and counting systems. For remote voting areas, this can become complex as voters have to first identify themselves and vote electronically using the same interface.

#### **Key Questions**

- Have key stakeholders been consulted openly and widely throughout the decision making process?
- Has the decision making process thoroughly examined the current system, costs versus benefits, technical feasibility, legality and capacity to implement the use of an electronic voting system?

### ***Building the System***

General requirements should provide guidance on the design of the electronic voting and counting systems, and align with any national, international standards and legal frameworks.

#### **Key Questions**

- Has the issue of secrecy, transparency, accountability, usability, security and accessibility been addressed within the general requirements of the electronic voting and counting technologies?
- Does the system allow voters the ability to cast their votes in an accurate, effective and efficient manner?
- Are the processes of defining design requirements open and inclusive to various relevant stakeholders?

### ***Security Requirements***

Security requirements for the electronic voting and counting technologies, as well as any applicable security standards should be detailed.

#### **Key Questions**

- Have the essential levels of testing of the electronic voting and counting systems including, as recommended, stress testing, acceptance testing, performance testing, security testing, usability testing and source code assessment taken place?
- Are external independent actors involved in all review processes?
- Is there a sufficient plan in place to conduct full system testing in advance of the elections?
- Are there mechanisms, such as hashes in place to ensure the software transferred onto the machines can be verified as the EMB-tested and approved version?
- Is the physical security of all technological equipment, protected from attempts to manipulate the systems?



**PROTECTED**

- Has all voting data been encrypted to ensure it can be securely transmitted from individual machines to the tabulation system?
- Are digital signatures in place to ensure data is transmitted from a legitimate source?

**PROTECTED**

## Appendix C – Three Lines of Defence Model

In the Three Lines of Defence model, management control is the first line of defence in risk management, the various risk control and compliance oversight functions established by management are the second line of defence, and independent assurance is the third. Each of these three “lines” plays a distinct role within the organization’s wider governance framework.

Understanding each line	1st LOD Commissions’ ‘Front Line’ Staff	2nd LOD Central risk functions	3rd LOD Independent oversight
Overarching Role	<ul style="list-style-type: none"> <li>Own / manage day to day risks</li> </ul>	<ul style="list-style-type: none"> <li>Direct / design risk framework</li> <li>Oversight / support / aggregation / review of reported risks</li> </ul>	<ul style="list-style-type: none"> <li>Independent assurance of risk treatment controls</li> </ul>
Risk Responsibility	<ul style="list-style-type: none"> <li>Manage day to day risks</li> <li>Implement cyber risk management framework</li> <li>Develop treatment plans</li> <li>Manage / monitor risk treatments and escalate issues</li> <li>Risk reporting / profiles</li> </ul>	<ul style="list-style-type: none"> <li>Risk framework / management / risk advice</li> <li>Enforce organisational compliance with risk management frameworks</li> <li>Challenge / oversight of Risk across the commission e.g. reporting, residual risks, control effectiveness</li> <li>Risk Committee reporting</li> </ul>	<ul style="list-style-type: none"> <li>Assess the implementation of the risk management framework</li> </ul>
Appetite	<ul style="list-style-type: none"> <li>Define risk appetite (within governance body approved limits)</li> <li>Operate within tolerances</li> </ul>	<ul style="list-style-type: none"> <li>Facilitate risk appetite development (Commission wide and Divisional Level)</li> <li>Monitor compliance and operationalise</li> </ul>	<ul style="list-style-type: none"> <li>Confirm compliance with defined appetite</li> </ul>
Risk Management Policy	<ul style="list-style-type: none"> <li>Implement / operationalise risk management policies and procedures</li> </ul>	<ul style="list-style-type: none"> <li>Develop and maintain risk management policies and procedures</li> <li>Provide risk management policies</li> <li>Monitor compliance / adherence to approved procedures and standards</li> </ul>	<ul style="list-style-type: none"> <li>Confirm compliance with risk management policies</li> </ul>
Risk Management Framework	<ul style="list-style-type: none"> <li>Implement / operationalise Risk Management Framework</li> <li>Adherence to Risk Management</li> </ul>	<ul style="list-style-type: none"> <li>Develop / validate and maintain risk management methodologies</li> <li>Monitor implementation / on going application and operation of methodologies</li> <li>Manage risk IT systems</li> <li>Validate and test consistency</li> </ul>	<ul style="list-style-type: none"> <li>Test effectiveness and efficiency of treatment plan controls</li> </ul>
Monitoring	<ul style="list-style-type: none"> <li>Monitor risk profile (risk register)</li> <li>Confirm effectiveness of treatment plans (controls)</li> <li>BU key risk and performance Indicators</li> </ul>	<ul style="list-style-type: none"> <li>Monitor key risk and performance indicators</li> <li>Enterprise risk profile / risk categories</li> </ul>	<ul style="list-style-type: none"> <li>Test effectiveness and efficiency of treatment plan controls</li> </ul>
Reporting	<ul style="list-style-type: none"> <li>Regular BU risk reporting</li> <li>Quarterly report for management</li> <li>Committee reporting</li> </ul>	<ul style="list-style-type: none"> <li>Aggregate risks for impact on commission as an enterprise</li> <li>Update Enterprise risk Indicators</li> <li>Risk Committee reporting</li> <li>Reporting emerging trends, industry insights, corporate benchmarking</li> </ul>	<ul style="list-style-type: none"> <li>Report on the effectiveness and efficiency of treatment plan controls</li> </ul>
<b>Risk Culture – We all own risk together</b>			
<div> <div>Tone from the top Clear reporting lines</div> <div>Clear roles and responsibilities Open, honest, transparent conversations and communications</div> <div>Training and development Accountability and ownership</div> </div>			

The Three Lines of Defence Model assists organisations by aligning their risk governance strategy with their overall organisational objectives. It promotes a stronger risk management culture and assists in the reduction of inefficiencies in compliance and risk management.



This document and the information contained in it is confidential and should not be used or disclosed in any way without our prior consent.

**About Deloitte**

Deloitte refers to one or more of Deloitte Touché Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see [www.deloitte.com/au/about](http://www.deloitte.com/au/about) for a detailed description of the legal structure of Deloitte Touché Tohmatsu Limited and its member firms.

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

Deloitte provides audit, tax, consulting, and financial advisory services to public and private clients spanning multiple industries. With a globally connected network of member firms in more than 150 countries, Deloitte brings world-class capabilities and high-quality service to clients, delivering the insights they need to address their most complex business challenges. Deloitte has in the region of 225,000 professionals, all committed to becoming the standard of excellence.

**About Deloitte Australia**

In Australia, the member firm is the Australian partnership of Deloitte Touche Tohmatsu. As one of Australia's leading professional services firms, Deloitte Touche Tohmatsu and its affiliates provide audit, tax, consulting, and financial advisory services through approximately 6,000 people across the country. Focused on the creation of value and growth, and known as an employer of choice for innovative human resources programs, we are dedicated to helping our clients and our people excel. For more information, please visit our web site at [www.deloitte.com.au](http://www.deloitte.com.au).

© 2018 Deloitte Risk Advisory Pty Ltd