Elections ACT

Upgrade of eVACS® for the 2020 ACT Legislative Assembly Election

HAZOPS Analysis

Document Status: Final
Version 1.0
January 2020

Copyright Notice

Disclaimer

In compiling this HAZOPS Analysis, Software Improvements Pty Ltd has relied upon the accuracy and completeness of information provided by Elections ACT.

eVACS®

Where used in this HAZOPS Analysis, eVACS has the same meaning as eVACS®.

Document Control Information

The controlled version of this document is in electronic form.

All hardcopy versions are uncontrolled.

Modifications

Date of this Revision	Version	Comment	Author	Reviewer	Release
2019-10-09	0.1	Initial Draft	CJB	CVB	
2019-09-16	0.2	Post review of structure and inclusion of HAZOPS table	CJB	RB, CVB	
2019-10-28	0.3	Revision based on reviewers comments	CJB	CVB	
2019-12-28	0.4	Revision based on comments from EACT Note: file was labelled v0.5	CJB	CVB	2020-01-03
2020-01-14	1.0	Inclusion of EACT edits and revision after meeting with EACT	CJB		2020-01-21

Distribution

Name and Appointment	Document Name	Date of Issue	Version
Jiv Sekon, Project Manager, EACT Rohan Spence, DEC, EACT	HAZOPS Analysis	2019-10-31	0.3
Rohan Spence, DEC, EACT Jiv Sekon, Project Manager, EACT	HAZOPS Analysis	2020-01-03	0.4
Rohan Spence, DEC, EACT Jiv Sekon, Project Manager, EACT	HAZOPS Analysis	2020-01-21	1.0

Contents

1. Introduction

1.1 Document purpose

One of the Contract requirements for the upgrade of eVACS® [2] is to create a HAZOPS document. The rationale behind requiring a Hazard of Operations Study (HAZOPS) is that in order to minimise the potential for fraud and vote manipulation it is important to:

1) identify potential hazards and risk exposure (probability and consequence of occurring),
2) assess the consequences and probability of those identified hazards occurring, and subsequently the risk exposure, and
3) devise means to reduce the consequences or probability of occurrence down to an acceptable level (R4[1] in [1] and [2]).

In this context both real and perceived electoral integrity issues need to be considered in order to identify safe-guards to be put in place so as to minimise the risk exposure[1].

Elections ACT identified the document as being “used when communicating the effective mitigation practices in place when faced with outside queries over the system’s integrity” (R4 in [1]).

1.2 Defining the HAZOPS analysis

HAZOP usually refers to a Hazard and Operability study (initially HazOPS but now generally referred to as HAZOPS), being a structured and systematic technique for system examination and risk management. Initially developed in the 1960s to analyse major chemical process systems, the approach has since been extended to other industrial operations, other types of process systems, and other complex systems such as software development and operation.

A HAZOP study is therefore being used to expose potential hazards/threats in regard to the eVACS® election system, and to identify ways to mitigate the risk of harm when such a system is exposed to such hazards or threats. In the elections context, the system for analysis therefore includes not just the development of the eVACS® software but equally importantly the environments in which eVACS® operates (section 1.3).

A HAZOP study is typically conducted by:

1) systematically progressing through a design (or model) of a system,
2) evaluating each component – corresponding to an *attribute* - of the design, and
3) applying a set of relevant *guidewords* to each *attribute,*

in order to identify a *deviation* from what might be assumed or expected.

Each potential hazard/threat is exemplified in terms of a *deviation* or valid *attribute-guideword* combination.

[1] R4 is a reference to Requirement 4 in the cited documents

The *cause* of each *deviation* is recorded (if known) together with any of one or more *consequences* surrounding the *deviation.*

If a *safeguard* exists to counteract the potential hazard/threat (*deviation*), then that is also recorded.

Recommendations to prevent the *cause* or diminish the *consequence(s)* of a potential hazard typically are to describe new/extra *safeguards* to be installed/implemented.

Finally, the *severity* of the *consequence* is assessed in terms of *Minor*, *Moderate*, *Critical* or *Catastrophic*.

A HAZOPS is presented in tabular form containing six columns defined as follows:

Column	Column Label	Description
1	Item #	A unique identifier assigned to each row in the table representing a *deviation*
2	Deviation (hazard/threat)	Anything credible that might cause unexpected/inappropriate operation of the system
3	Cause	One or more events that might have caused a *deviation*
4	Consequence	Outcome of a *deviation* becoming a harmful incident
5	Safeguards	Any existing equipment or processes that counteract the *consequence* or cancel out the *causes*
6	Recommendations	Identified as having potential to prevent the *cause* or diminish the *consequence*

The detailed HAZOPS for eVACS® is provided at Appendix 3 and builds on an earlier HAZOP study [6] and the description of the security features of eVACS® [5].

In election systems the main hazards/threats surround activities that have the potential to expose how one or more electors have voted, and/or the potential to corrupt votes. These potential hazards/threats are not unique to electronic election system; indeed, Elections ACT has in place various processes/procedures (safeguards) associated with paper-based voting to reduce the risk of such hazards/threats causing ’harm’ to individual electors and the community as a whole.

1.3 Reference documents

References where cited in this document are referenced by number, e.g. a reference to the HAZOP Study from March 2019 is referenced as [6]

1. Business Requirements Specification ICT business System upgrade - eVACS®, version 1.0;

2. Contract – Electronic Voting and Counting System (eVACS®) Enhancements, Services and Support: ACTGS reference 636238 Final Version 23 July 2019, including the Statement of Requirements at Schedule 2 being a modified version of the Business Requirements Specification [1];

3. Software Improvements Pty Ltd, eVACS® Operational Concept Description, 2019

4. Software Improvements Pty Ltd, eVACS® Systems Specification Parts 1 and 2, 2019

5. Software Improvements Pty Ltd, Security and eVACS®, May 2019

6. Software improvements Pty Ltd, HazOP Study for ACT Election System, Final, 15 March 2019

7. Boughton, CJ (2006), Maintaining Democratic Values in e-Voting with eVACS®, Proceedings of the 2nd International Workshop on Electronic Voting, Bregenz, Austria

8. IEC 61508 - Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems.

1.4 Acronyms

ACT	Australian Capital Territory
BVI	Blind or Vision Impaired
CJB	Carol Boughton
CVB	Clive Boughton
EACT	Elections ACT (ACT Electoral Commission)
EMS	Election Management System
eVACS® / eVACS / EVACS	electronic Voting and Counting System
HAZOPS	Hazard and Operability Study
HTTPS	HyperText Transfer Protocol Secure
IEC	International Electrotechnical Commission
IVR	Interactive Voice Response
LAN	Local Area Network
PIN	Personal Identification Number
RB	Russell Baird
UPS	Uninterrupted Power Supply
USB-FD	USB Flash Drive cleaned and secure

1.5 Definitions

e-voting	electronic voting
e-voting card	A card with a QR code used by voters to start and end their electronic voting session
Master Admin barcode	A location specific card with a QR code used by an official to authorise administrative activities
QR code	Two dimensional barcode
Voting Token	A randomly generated 7 digit numeric code issued to registered telephone voters

2. Understanding eVACS®

2.1 Election principles

There are six principles of democratic elections [7]:

1) The **doorkeeper** principle
   Each person desirous of voting must be personally and positively identified as an eligible voter and permitted to complete no more than the correct number of ballot papers.

2) The **secrecy** principle
   Admitted voters must be permitted to vote in secret.

3) The **verification, tally and audit** principle
   There must be some mechanism to ensure that valid votes, and only valid votes, are received and counted. This mechanism must be sufficiently open and transparent to allow scrutiny of the votes.

4) **Equality** (in political participation)
   - Racial equality
   - Multi-lingual access
   - Disability access
   - Inter-jurisdictional access (no differential treatment to voters based on where they reside)

5) Security
   The resistance of votes and vote totals to fraud and other forms of manipulation

6) Transparency
   The capacity to produce auditable results in which both candidates and voters can justifiably have confidence.

These six principles are not only reflected in the design of eVACS®, but they also provide a guide as to how to consider the *deviations* referred to in section 1.2 in the context of elections by asking questions of the form listed in Table 1.

Table 1 – Linking election principles and HAZOP *deviations*

Principle	Question
Doorkeeper	How could a person impersonate someone else on the electoral roll? How could a person receive, or access, more ballot papers than they are entitled to?
Secrecy	How could the secrecy arrangements be violated?
Verification, tally & audit	Could the mechanisms in place be modified without detection?
Equality	By introducing special arrangements to ensure equality, can the processes to support other principles be weakened?
Security	How could the security procedures be breached?
Transparency	Are there ways for nefarious activities to be undertaken without an observable impact on the transparency procedures in place?

A high level description of the application within eVACS® of the six election principles is provided at Appendix 1.

2.2 eVACS® operating environments

In the elections context, the system for HAZOP analysis includes not just the development of the eVACS® software but equally importantly the environments in which eVACS® operates (section 1.2).

There are three different physical environments in which different modules of eVACS® operate (Figure 1), and a fourth environment that impacts on the operations of eVACS®:

1. an access controlled location where the election server is located and scanning of ballot papers is undertaken,

2. multiple polling places where electronic voting takes place,

3. a secure location where the telephone voting system is located, and

4. the public environment through which votes are transported from voting servers to the election server location, or the locations where telephone voting takes place.

In this section the hazards of each environment are considered, whereas hazards with the actual operation of eVACS® and how they are being addressed, including security, are presented in sections 2.3 and 2.4.

2.2.1 Election server environment

In order to ensure only authorised access to the Election server, the server is located in an access controlled environment. As well, access to the server is controlled (with two factor authentication, being password and Master Admin barcode) and logged.

Hazards associated with the election server relate primarily to:

- destruction of the server
- introduction of nefarious code
- uploading incorrect election information,
- misspelling and/or mispronouncing party and candidate names,
- entered passwords (e.g. end of day password) not protected appropriately, and
- having the network for creating voting servers installed appropriately to support installation of voting server software.

The setup of voting servers requires a local area network connected to the election server, but only for the time required to complete the installation of a server for each polling place (represented by the Temporary LAN in Figure 1 with up to n servers as part of the temporary network).

Although data entry also requires a network connected to the election server, this is less of an issue as data entry, if used, occurs after polling closes and any problems with the network can be resolved without the same critical time pressures.

2.2.2 Polling place environment

Ensuring that only those enrolled to vote are able to vote, and only in elections to which they are entitled to vote, is the responsibility of polling officials either at a polling place or when a person is seeking to register to vote by telephone (section 2.2.3).

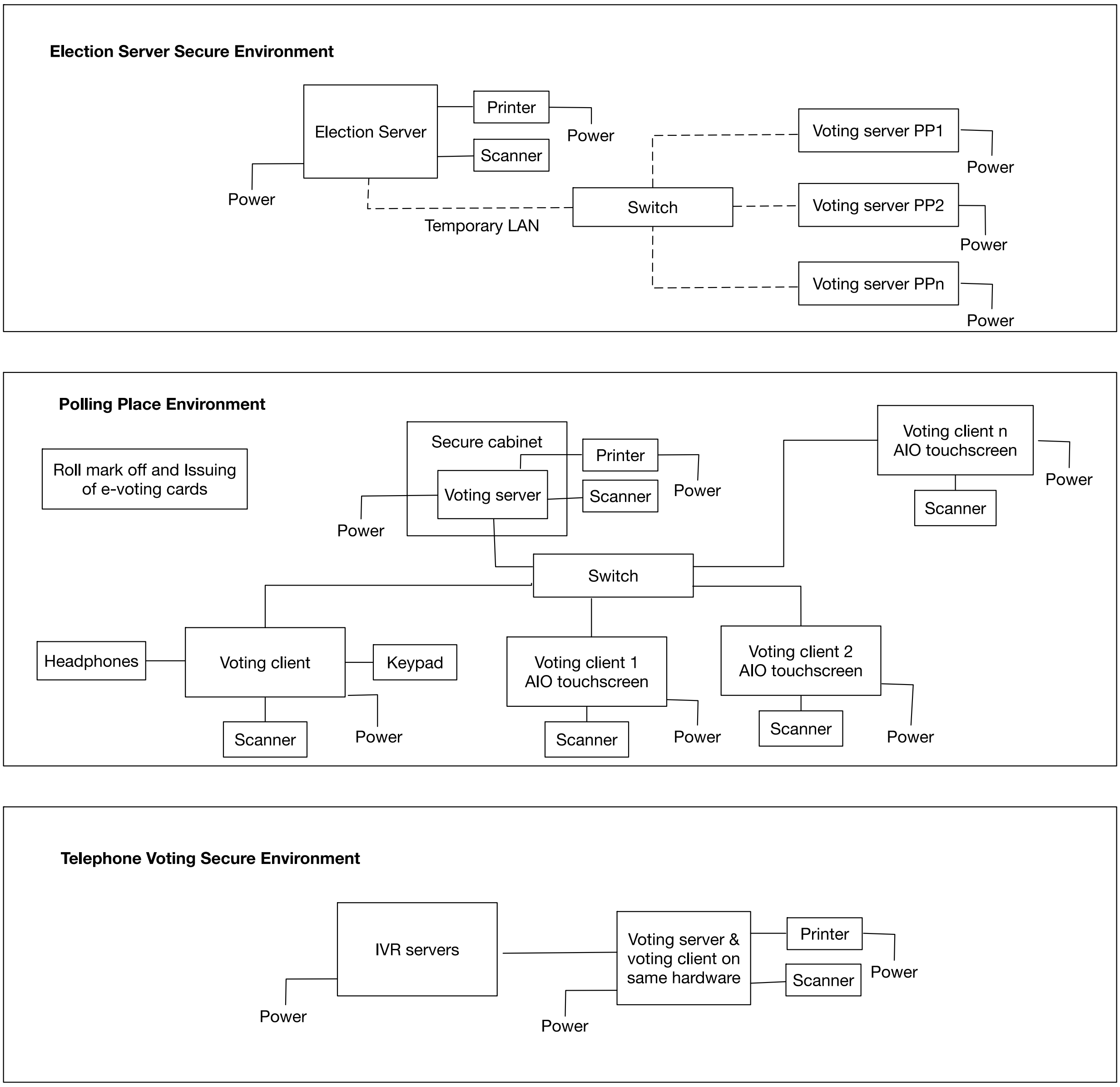

Figure 1 – eVACS physical operating environments

When voting at polling places a polling official issues the elector with an e-voting card that contains a barcode identifying the electorate in which the person is enrolled to vote and the specific polling place for which the barcode can be used. The e-voting card when scanned determines the electorate and hence the correct ballot to be displayed, and associated audio to be played if the elector is using headphones.

At each polling place supporting electronic voting, multiple voting clients are connected via a LAN to the polling place server, with the latter located in a secure cabinet. Voting clients have minimal software installed from the voting server, basically supporting the reading of e-voting cards, use of keypad where provided, and communication with the voting server. All actions on the voting client and voting server are logged.

Risks associated with the setup for voting at polling places are addressed in section 2.4.4.

All of the polling place servers (referred to in section 2.1.2) are identical when setup and can be delivered to any electronic polling places. Therefore, before voting can commence at a polling place, the polling place at which the server is located must become known to the server in order for the issued e-voting cards to be accepted by the server.. This requires an official to select from a list of names initially displayed on the server and then to scan the Master Admin barcode for the polling place. There must be a match between the name selected and that of the Master Admin barcode identified polling place name.

There is the potential for an incorrect selection from the list of polling place names and/or for the wrong Master Admin barcode to be delivered to a particular polling place. Although this has no impact on vote data, the outcome is a potential delay in the commencement of electronic voting at the polling place.

2.2.3 Telephone voting system environment

The telephone voting system (IVR servers and telephone voting server) location is within a Security Operations Centre of a Government Community Infrastructure providing secure cloud services. Access to the Centre is controlled and logged. Access to the telephone voting server is also logged and, for anything other than starting and stopping voting services, requires use of a Master Admin barcode or password.

When registering to vote by telephone, the elector once established as enrolled in the ACT provides a Personal Identification Number (PIN) and subsequently receives a Voting Token linked to their PIN and based on the electorate in which they are enrolled to vote. When voting by telephone, the elector first enters their PIN and then their Voting Token, if the pair match with a pair in the database the electorate information in the Voting Token is used to ensure the audio for the ballot for that electorate is transferred to the IVR servers in response to key presses on the voter's telephone.

In the case of the telephone voting system, functions equivalent to those of the voting clients at polling places, are performed as part of the IVR functionality within the telephone voting system.

In order for the telephone voting system to operate, the PIN/Voting Token pairs must be available in the Telephone Voting Server database. As proposed by Elections ACT, registering for telephone voting can only occur during hours when normal voting is available, and uploading of PIN/Voting Token pairs is expected to occur on multiple occasions during each day in which registration is to be made available. Delays in uploading PIN/Voting Token pairs beyond voter expectations could impact negatively on the outcomes of the initial trial of telephone voting.

2.2.4 Public environment

At the close of polling on each pre-polling day and election day, cumulative votes are downloaded from each voting server (at each polling place and for telephone voting) and physically transported to the location of the election server.

There are two obvious concerns associated with such transportation:

1) safety of individuals involved in such transportation, and
2) security of vote data.

Specific hazards derived from the first concern relate to the means of transport utilised, currently motor vehicles for travelling from polling places and most likely on foot from the telephone voting location and electronic voting centres close to Elections HQ. In the ACT the risk of involvement in a traffic accident or the possibility of being harmed whilst a pedestrian are both very low.

Security of the vote data is addressed in section 2.4.2 but from a 'harm' perspective having the data stolen is not really of consequence as the vote data can easily be downloaded again and importantly the data cannot be read from the transportation media (as data is encrypted), nor modified without detection should an attempt be made to upload the votes to the election server.

The second type of public environment covers those locations where telephone voting takes place.

2.3 A model/design of the eVACS® software system

As mentioned in section 1.2, in order to undertake a HAZOPS effectively it is necessary to have a model or design of the system under study. It is not necessary that the model/design be detailed, but it does need to at least represent essential characteristics of the system. eVACS® is a critical information system for Elections ACT, and from a software perspective an entity-relationship model is appropriate.

Figure 2 depicts the major data entities (*Vote_Entity, Barcode_Entity*[2]*, and Elector_Entity*) and the relationships that pertain to electors and their votes within eVACS®. In this case there is only one relationship: **R1** - showing that one *Barcode_Entity* is not related to a vote, or just one *Vote_Entity* expressed as 0..1 in Figure 2. Initially barcodes are listed in the database without any relationships to anything else, albeit that the barcode contains an electorate and polling place identifier. The relationship **R1** is formed when a barcode is scanned and a ballot for the particular electorate is identified/displayed. Once the vote is committed (with or without any preferences) the relationship **R1** is severed and the barcode is marked as used and thus cannot be used again to form another **R1** relationship, hence the description 0..1.

As per Figure 1, each polling place at which electronic voting is available, contains a polling place server to which many voting clients are connected. Each polling official at each polling place has access to an electronic copy of the complete electoral roll for the ACT (completely separate from eVACS®). As an elector enters a polling place, she/he is guided to an official who obtains the elector's name and address details and then marks them on the roll as ‘voted’ before issuing the elector with a barcode, now e-voting card, (containing a QR barcode to vote electronically) or a paper ballot (to fill out with a pencil). Barcodes are issued in random order and are not related to the elector, except that the barcode is selected to enable electronic voting in the electorate in which the voter is enrolled.

Apart from the voter, the only person who potentially knows the details of the barcode issued to them is the polling official who has just marked off their name on the electoral roll. Hence, the polling official has access to two pieces of the information necessary to link a vote to a voter. In order to actually link the barcode with a vote, the official has to gain access to the votes database on the voting server while a vote is in progress. The following security features of eVACS® exclude the possibility of such access ever being attained: limited menu functions available during voting, unused ports are inoperative both via programming and physically, and the server is located in a secure box.

The important thing to note in Figure 2 is that there is no intended relationship between the *Elector_Entity* and the *Vote_Entity*, which is as it should be. Essentially this means that elector privacy should not be at risk.

[2] The relationship **R1** also applies for telephone voting in which Voting_*Token_Entity* can be substituted for *Barcode_Entity* . Relationships **R2** to **R4** do not apply to telephone voting

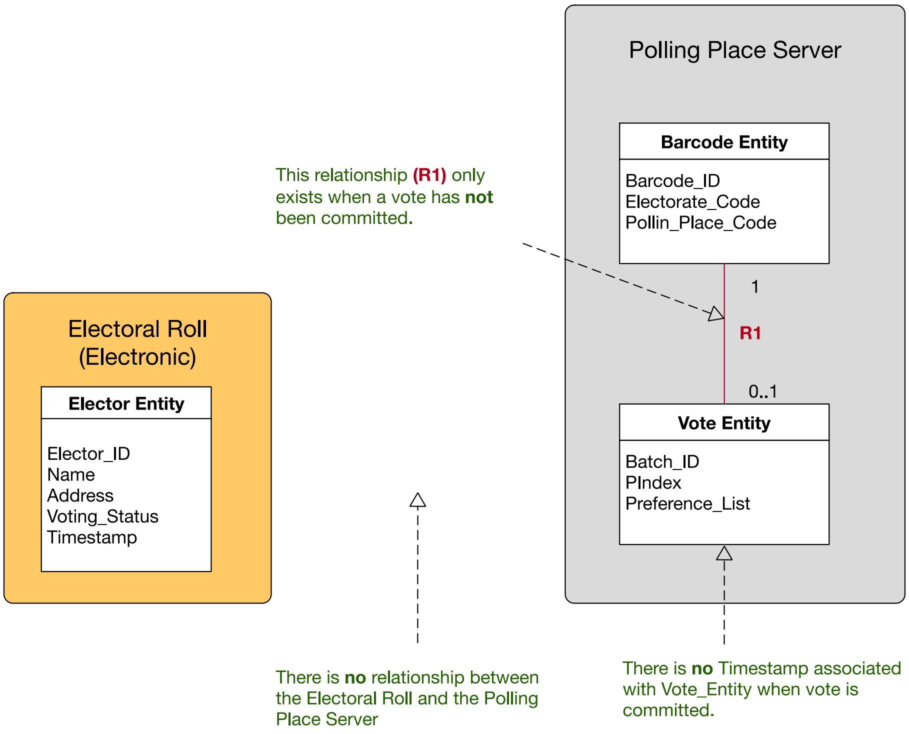
Polling Place Server
Barcode Entity
Barcode_ID
Electorate_Code
Pollin_Place_Code
This relationship (R1) only exists when a vote has not been committed.
1
R1
0..1
Vote Entity
Batch_ID
PIndex
Preference_List
Electoral Roll (Electronic)
Elector Entity
Elector_ID
Name
Address
Voting_Status
Timestamp
There is no relationship between the Electoral Roll and the Polling Place Server
There is no Timestamp associated with Vote_Entity when vote is committed.

Figure 2 – The main data entities and relationships and their respective locations within eVACS®

However, undertaking a HAZOPS on the model/design in Figure 2 suggests that there could be unintended relationships between the *Elector_Entity* and *Vote_Entity* as in Figure 3.

If a *Timestamp* were attached to a committed vote as well as when changing an elector's *Voting_Status* from 'Not voted' to 'Voted' on the electoral roll, an unintentional relationship between an elector and their vote, could be potentially possible. However, eVACS® does not store a *Timestamp* with a vote, in addition when a vote is committed to store it is encrypted and assigned a random number, and votes are then stored in order of the random numbers, ensuring there can be no relationship between time of voting and sequential order of votes in the votes database.

As part of automatic logging of events, a *Timestamped* entry is still made to the audit log when a vote is committed, but there is no mechanism by which an entry in the audit log can be linked with a particular entry in the list of randomly ordered votes.

A relationship (**R2**) between an elector and their vote may exist more deliberately, if an elector attempts to form a unique *Preference_List* that is able to be identified in the published data. This circumstance is addressed in Appendix 3 at ITEM# 1.

Additionally, an unintentional relationship (**R3**) between an elector and their vote may be identified when an elector is alone in a polling place and voting electronically at the very beginning or end of an election. However, the random ordering of votes within eVACS® ensures this relationship cannot be established and the elector's vote cannot be identified in the published data. This circumstance is the topic of ITEM# 2 in Appendix 3.

Finally, an accidental relationship (**R4**) may exist when very few electors (in total) vote at a polling place. This could occur when voters go to a polling place with electronic voting, but the polling place is remote from the voters' electorates. This circumstance is described at ITEM# 3 in Appendix 3.

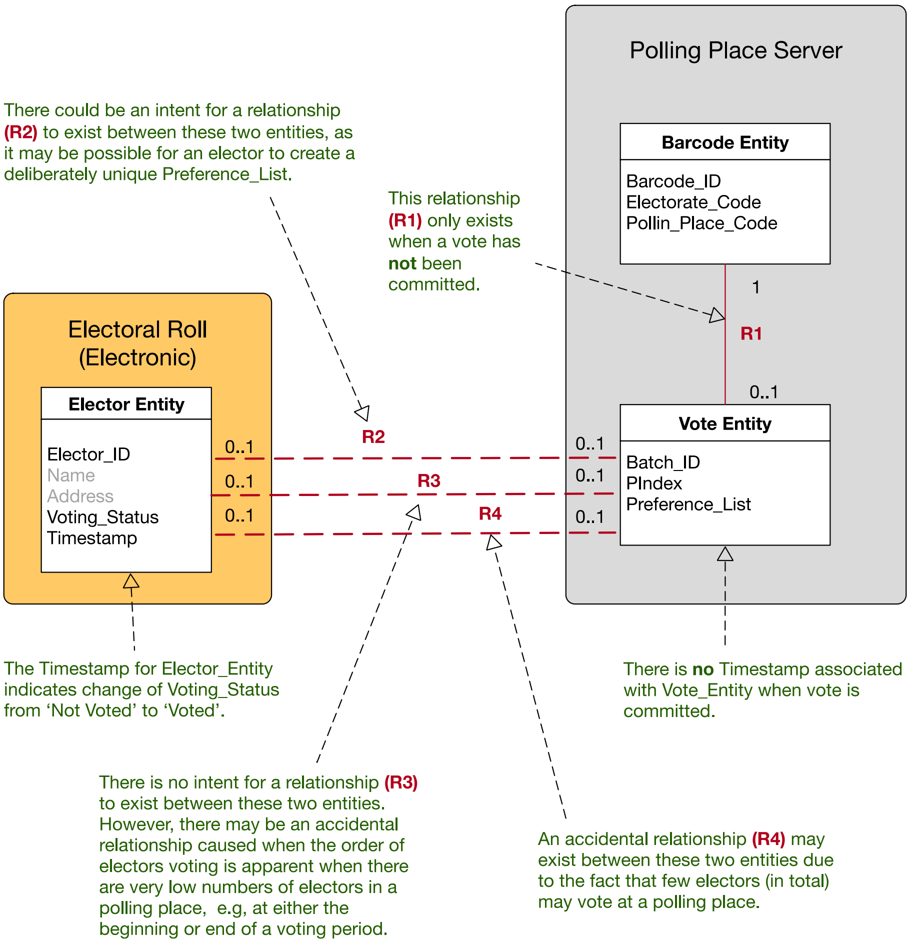
Polling Place Server
Barcode Entity
Barcode_ID
Electorate_Code
Pollin_Place_Code
1
R1
0..1
Vote Entity
Batch_ID
PIndex
Preference_List
Electoral Roll (Electronic)
Elector Entity
Elector_ID
Name
Address
Voting_Status
Timestamp
0..1
0..1
0..1
R2
R3
R4
0..1
0..1
0..1
There could be an intent for a relationship (R2) to exist between these two entities, as it may be possible for an elector to create a deliberately unique Preference_List.
This relationship (R1) only exists when a vote has not been committed.
The Timestamp for Elector_Entity indicates change of Voting_Status from 'Not Voted' to 'Voted'.
There is no Timestamp associated with Vote_Entity when vote is committed.
There is no intent for a relationship (R3) to exist between these two entities. However, there may be an accidental relationship caused when the order of electors voting is apparent when there are very low numbers of electors in a polling place, e.g, at either the beginning or end of a voting period.
An accidental relationship (R4) may exist between these two entities due to the fact that few electors (in total) may vote at a polling place.

Figure 3 – Some possible relationships that may be formed between an elector and their vote

2.4 eVACS® and security

The electronic voting system implemented by Elections ACT comprises more than eVACS® software. The software operates on hardware, in various environments (section 2.2) and involves different authorised users. As a consequence, there are multiple avenues that could be potential threats to maintaining security of the end-to-end electronic voting process.

Looking at security issues is another way of examining threats in the context of a HAZOPS since:

- 'security' is the state of being free from danger or threat, and
- 'security risk' is a person or situation which poses a possible threat to security

where:

- 'hazard' or 'threat' is something that could cause harm, and
- 'risk' is the potential impact (probability and consequence) of such harm

In the elections context the unacceptable outcome of a breach in security is a failure to meet one or more of the election principles identified in section 2.1.

Security threats can be grouped as follows:

- Software related
- Vote protection
- Protection of hardware
- Environment controls
- Access controls

Mitigation strategies are addressed in the following sections describing different aspects of the eVACS® electronic voting system.

2.4.1 Software related security

2.4.1.1 Software development

Implementing sound software engineering practices is critical to ensuring delivered software is fit for purpose. Practices adopted for eVACS® include:

- Accurate documentation with traceable requirements, which have been elicited and agreed with Elections ACT
- Repository with version control (GIT)
- A comprehensive (executable) model of the system to capture and verify that requirements are dealt with appropriately
- Well-documented code (ideally code is auto-generated from the models, but in any case is closely associated with model elements)
- Reviews and extensive testing of model and code
- Repository of code issues identified and how addressed (Bugzilla), together with change control management

Threats centre on failure with these practices, either intentionally or unintentionally, such that poor or malicious code is included in the system.

Mitigation is dependent on:

- each member of the eVACS® team abiding by the practices
- reuse of code that has been shown to do what it is intended to do
- regular review of the model/code, and
- the final audit (see section 2.4.1.2).

In addition, team members have extensive experience either with electronic voting systems or new elements (e.g. IVR server development and deployment) over many years and are long-time employees of their respective company. Given the quality of the individual team members and the engineering practices in place, it is difficult to see any intentional or unintentional injurious code making it into the final delivered code.

2.4.1.2 Software in operation

A key security feature is that the eVACS® software (with supporting documentation and model) is independently audited and locked down prior to use in an election, to ensure that the software only does what it is intended to do, and votes cannot be added, deleted or amended, and no changes can be made to the system when in operation.

The eVACS® system is a closed system in which the software to set up an election first creates an Election server which is then used to install software to create voting servers (connected by a LAN to the Election server) which then have the functionality to install software to create voting clients (connected via a LAN to the voting server at a polling place). Before use in an election, the eVACS®

setup election software is independently audited, along with the Data Entry Client software which is the only other component of eVACS® not contained within the setup election software.

Setting up for an election is two-factor authentication access controlled and is undertaken by the Electoral Commissioner or Deputy Electoral Commissioner who hold security clearances.

When any of the eVACS® software is loaded onto hardware, any software of any nature existing on that hardware is removed before the relevant eVACS® software is loaded. After loading, the BIOS is used to set the Boot sequence to 'Boot from Hardware' so that any attempt to load other/nefarious software via USB ports is thwarted. Access to the BIOS is password controlled.

The operating system used is a cut down version of Linux, only containing the functionality necessary to support eVACS® operations. Providing limited functionality mitigates against attempts to modify the software whilst in operation.

Decommissioning unused ports via the operating system further mitigates attempts to interfere with the operation of the system. .Also, all hardware has their boot sequence set to boot only from hard disk so that an external source will be ignored even if access via a port were achieved.

The voting client and data entry client are both basically dumb terminals, only requiring sufficient software to enable communication with the relevant server, and do not contain any specific election information, and importantly no vote data.

Once the election information for a particular election is available and input to the Election Server, the Voting Server application together with its operating system can be installed on hardware connected via an isolated LAN to the Election Server.

Similarly, once the Voting Server is located at a polling place, the Voting Server is able to install the voting client application and operating system on hardware connected to the Voting Server via an isolated LAN

This closed-system approach addresses potential risks of incorrect, interfered with or substituted software being loaded onto voting server and voting client hardware, by personnel other than the approved Elections ACT officers (EC or DEC) that are provided with access for the purpose of establishing the election event via the Election Server set-up procedures.

2.4.2 Vote protection

Electronic votes have similar safeguards to those in place for paper ballots as well as additional safeguards as follows:

i) votes are encrypted and stored in a physically secure ballot box (a database on the polling place server on two separate disks)

ii) votes cannot be counted until after polling closes (system is configured to prohibit access to election results until the 'polls close' date and time have passed, the option is not made available as a menu item beforehand and access once available is password controlled)

iii) the results of a first preference count, for each electorate, are printed at the polling place, minimising the potential for transposition of results.

iv) the number of e-voting cards (see section 2.4.5 on authorisation) issued are compared with the number of votes in the first preference count and a printed report is available to identify the number of times an e-voting card was scanned to commence a voting session but was not scanned a second time to conclude the voting session

v) at the end of each polling day (pre-poll and election day) votes are exported to media (clean USB-FD). To ensure data is not tampered with during transfer a SHA2 hash code is generated, printed as a QR code and transported, with appropriate security measures, to the security controlled central scrutiny location, with the two copies of vote data.

vi) the hash codes provided at v) are scanned at the Election Server and compared with a hash code calculated by the server for the data received before votes are able to be uploaded.

Information transmitted between the voting server and voting clients uses HTTPS (TLS1.2). Further, the vote preferences held on the server are compared with the touchscreen presses or key strokes that generated those preferences to ensure the voter's actual preferences are what are stored in the database as the elector's vote.

2.4.3 Hardware protection

The following hardware is expected to be used with eVACS® in 2020:

Election Server - is located in multiaccess-controlled premises, and has two-factor access available only to the Electoral Commissioner or Deputy Electoral Commissioner.

Polling Place Server – one at each polling place where electronic voting is available. The Polling Place Server is located out of sight of electors, placed within a locked server cabinet, in locations with limited access after-hours. Access to vote data is date/time and password-controlled. Unused ports are decommissioned both through software and physically. The server is also connected to a UPS.

Voting Clients – are connected via a LAN to the Polling Place server and are placed in separate voting booths. Ethernet and power supply cables are located behind the voting booths out of sight of the public. The use of All-In-One touch screen computers in eVACS® allows for the computer back to be hidden with the screen placed face-up on the voting booth shelf. A fixed barcode scanner is provided for the voter to scan their e-voting card. No vote information is stored on the voting client so that no additional physical protection is provided; however, unused ports are decommissioned both via the operating system and physically.

A separate voting client to support B&VI voters is available, with the addition of a keypad for voting.

Telephone voting server and IVR server – are located in a Security Operations Centre of a Government Community Infrastructure providing secure cloud services. Access to the Centre is controlled and logged. Telephone voting server is also password and Master Admin QR code controlled.

Data Entry Clients – are connected via a LAN to the Election Server and are therefore located in secure Elections ACT controlled premises. Access is password-controlled.

Data Entry Server – is an application on the Election Server and does not have separate hardware. Activation is password-controlled via a Data Entry Client.

Threats to eVACS® operations via the hardware arise from:

- Hardware failure, such as failure of scanner, keyboard/keypad, hard disk and touch screen.
- Power supply interrupted, either because power cable is disconnected or from electricity supply interruption from an external cause.

Apart from a disk failure, none of these hardware related threats impact on the election's integrity and will therefore not be considered further, noting that Elections ACT already has in place processes to deal with such threats e.g. polling place servers are maintained on a UPS.

Disk failure has the potential to lose votes but this threat is mitigated by the inclusion of two hard disks in the voting servers. However, replacement of a failed disk and/or attempting to read votes off a failed hard disk may be perceived as an opportunity to tamper with votes unless handled transparently.

2.4.4 Environment controls

As indicated in section 2.2 the Election Server and Telephone Voting Server are setup in access-controlled environments and are thereby physically protected.

At polling places, there are legislative controls that govern what can and cannot happen at the polling place when voting is occurring. However, there is still the potential for an individual to be unreasonable in their behaviour either during voting or when the polling centre is closed. Mitigation measures implemented include:

- having the polling place server hidden from public view and physically secure.
- having the voting clients positioned in the voting booths so that only the screen and scanner, and keypad if connected, are visible to the public
- not having any important information on the voting clients, so that if one is damaged in any way no information can be lost
- securing unused barcodes in a similar manner to unused ballot papers
- restrictions on what electors and others can do in a polling place, e.g. photography is not permitted without authorisation
- polling place out-of-hours protections

To mitigate against a natural disaster or failed out-of-hours protection, on a daily basis after polling closes cumulative votes are exported at each electronic polling place and transported to central scrutiny, as per 2.4.2 (v).

2.4.5 Access controls

Access controls are not the same across all eVACS® modules:

- For the Election server two factor access authentication is provided, where both a password and scanning of a Master Admin QR code are required.
- The Polling Place server menu is very limited and hence not password controlled, except for accessing first preference counts which are password accessible and only after polling closes on election day. Voting operations are barcode controlled.
- Voting clients are only accessible with an authorised barcode.
- Telephone voting is only accessible via a PIN and Voting Token. The Telephone Voting server menu is very limited and requires authorised barcode and/or password to upload PIN/Voting Token pairs and access first preference counts.
- Data Entry is only accessible via individual-assigned passwords

Where access is provided, the only possible actions are those available from the menu displayed. In addition, certain menu items are not available until after polling closes. Further, all passwords must meet ACT Government and ASD password security requirements, meaning that no password will be accepted by eVACS® unless it complies with these standards.

After selecting a preferred language, for an elector using a barcode to access the voting client, the only actions possible are to select candidates in order of preference, modify selections, and confirm preferences.

In the case of telephone voting, access to voting is dependent on a voter registering to vote by telephone, providing a PIN of their choosing, receiving a Voting Token for the electorate in which they are enrolled to vote, and then entering their PIN and Voting Token. Following access, the voter can only select candidates in order of preference, modify selections, choose to listen to what each key does and confirm preferences, as is the case with voting electronically at a polling place.

3. Acceptability and Tolerability of Hazards

How well the ACT public is likely to accept or tolerate risks associated with electronic voting as offered via eVACS® is difficult to estimate, as there have been few instances of reported concerns from ACT electors. Those concerns that have been raised have, in the main, arisen from researchers and the issues raised have had no real impact on the outcome of elections.

At one extreme, an Australian electoral population would almost certainly not tolerate a gross election failure where it is known that votes have been corrupted in some way.

At the other extreme, in the ACT there has been no public protestation against the use of electronic voting, suggesting that the ACT community assumes a low probability of their vote being exposed or corrupted, especially as eVACS® has removed the human element in handling and counting votes via the Hare Clark system, and consequently improved the accuracy of the count. Incidents have occurred surrounding polling place server disk failures, but the RAID configuration (with dual disks) has enabled complete recovery of votes stored on those servers.

In other arenas risks to hazards are measured in terms of the probability of death, but this doesn't apply within the elections context. Nevertheless, the community is not likely to tolerate their votes being exposed/corrupted to any less degree than (say) losing their lives on the road or perhaps in an aircraft accident. Studies in other domains (such as medicine) have revealed similar levels of tolerance to death in regard to surviving surgery or taking prescribed medicinal drugs.

Frequency is only one element of acceptance/tolerance. Any one incident where there are multiple deaths leads to significantly greater community concern than several independent incidents where one person dies.

Relating acceptability/tolerance in terms of frequency and/or multiplicity of some drastic outcome enables the establishment of protective barriers in order to ensure that otherwise hazardous/dangerous systems are adequately safe. The same mentality, of reducing (at least) known hazards to acceptable levels, applies to election systems as it does to transport and medical systems. Identifying and reducing known hazards to acceptable levels, that would otherwise lead to easily corruptible and untrusted electoral systems, is an essential starting point to obtaining elector confidence and trust in the system.

It is very important to Elections ACT that the community be able to trust the election system that is used to help determine who governs. Nonetheless, Elections ACT officials know only too well that any election system has its hazards, and ensuring those hazards are reduced to acceptable levels of occurrence is important - especially when they also know that no system is going to be absolutely risk free.

Based on the quoted levels of tolerance (in terms of fatalities) within different transport and medical arenas, it is possible that the ACT community would tolerate, for example, 1 elector in 100,000 having their vote made public - but only if the cause for the exposure is adequately explained and not likely to have applied to electors more generally. However, it is doubtful that the community would tolerate, for example,10 such incidents in the same election. Obviously, Elections ACT and the vendors of its election system aim for zero incidents of exposure, as well as zero incidents of vote corruption and counting errors.

IEC 61508 - Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems provides a generic description of hazards and risks in the electronic safety domain [8]. These descriptions (Appendix 2) have been modified for the elections domain (Table 2 and section A.2.2) and are referred to in the HAZOPS descriptions in Appendix 3.

The category definitions developed for the elections domain (Table 2 and section A.2.2) are based on 'Votes corrupted, lost or publicly identified' (as opposed to deaths and injuries). Reputational damage in the category definitions refers to Elections ACT experiencing any of negative publicity, public perception or uncontrollable events that affects the ability of the Commission to fulfil its charter.

Table 2 – Consequence categories for the Elections Domain

Elections Domain	
Category	**Definition**
Catastrophic	Election results so impacted that the Court of Disputed Elections requires the election to be re-held and/or irreparable reputational damage.
Critical	Significant election concerns however the Court of Disputed Elections does not rule for an election re-run and/or major reputational damage.
Moderate	Vote preferences of a small number of people are impacted. Moderate reputational damage. Election result not contested in the courts.
Minor	Issues with votes of one or a few people are raised but they have no possible impact on election results. Minor to no reputational damage.

4. eVACS® – possible deviations

As identified in section1.2 the purpose of the HAZOP study is to identify a *deviation* from what might be assumed or expected, and/or design intent.

Based on the descriptions in sections 2 and 3, *deviations* expressed in terms of *guidewords* and *attributes* have been identified and are listed in Table 3. These *deviations* are the numbered items that form the basis of the HAZOPS report provided as Appendix 3.

Table 3 – Guidelines and their application to eVACS® attributes

Guideword	Attribute	Item # in Appendix 3
Accessible	Password	30
Extra/unintentional	Relationship	1, 2 and 3
Inaccessible	Password	14
Inaccurate	Counting	4
Incorrect	Electorate - e-voting card	5
	Electorate - Voting Token	7
	Password	13
	Information	15
	Location – Master Admin QR code	16
	PIN/Voting Token link	8
Insecure	Hardware	17
	Network communication	19
	Vote transportation	27
Invalid	e-voting card	6
	Voting Token/Pair	9
	PIN	12
Less	Votes – electronic at polling place	20

	Votes - telephone	23
Modified	Votes – electronic at polling place	22
	Votes - telephone	25
More	Votes – electronic at polling place	21
	Votes - telephone	24
Nonanonymous	Vote	26
Untimely	Upload - PIN/Voting Token pairs	10
	Recovery - after failed hardware	18
Substitution	Software	29
Unsafe	Transportation	28
Unsuccessful	Upload - PIN/Voting Token pairs	11

5. Summary and Conclusions

The 30 hazard items identified are categorised in terms of consequences (defined in Table 2), and listed in Appendix 3. For 18 of the 30 hazards multiple consequence categories are assigned, reflecting the variability in the extent of the incident that could occur. To ensure consideration of worst case safeguards, each of these hazards has been assigned to the severest consequence category identified for the hazard, as follows:

Category	Number of Items
Catastrophic	12
Critical	1
Moderate	6
Minor	11

The twelve items that could result in catastrophic outcomes if they occurred reflect the importance of:

- the appropriateness and security of passwords (Items 13 and 30),
- ensuring votes and their preferences are always secure (Items 21 to 25),
- ensuring the accuracy of the election information input to eVACS® (Item 15)
- demonstrating and ensuring the reliability and accuracy of the new counting program (Item 4)
- the security of the voting system (hardware and network) at polling places (Items 17 and 19), and
- the security of the eVACS® audited software, to ensure substitution is not possible (Item 29).

Item 15, is the *deviation* described by the guideword 'incorrect' and the attribute 'information', where information refers to all the data uploaded to eVACS® in either Phase 1 or Phase 2. In this case the consequences have been categorised across the full range from Minor to Catastrophic, where Minor applies to the situation where an error in the information is detected before voting commences and can be corrected, although there could be a delay to the start of electronic voting depending on the extent of the error(s). If the error is in ballot information used by electronic voting and paper ballots, recovery is more complicated, but if none or only a few votes are impacted the categorisation could still be Minor or more likely Moderate. However, depending on the extent of the error(s),and when they are discovered, the election results could be brought into question and a re-run of the election ordered (Catastrophic).

Items 17 and 19 are *deviations* described by the guideword 'insecure' and the attributes 'hardware' (Item 17) and 'network communication' (Item 19). Security of the voting server and the network at polling places is critical to ensuring that electronic voting at polling places can be relied upon to record accurately all, and only all, the votes of voters who are issued with and use an e-voting card to vote.

Apart from Item 15 (information accuracy) and Item 4 (reliable counting program) the catastrophic items all depend on security-related safeguards failing to prevent the hazard from becoming an incident.

The one deviation assigned to Critical refers to voting with an invalid PIN/Voting Token pair (Item 9). To avoid such an outcome, the processes for uploading PIN/Voting Token pairs to the telephone voting server must be secure at all times, and the management of Voting Tokens within the EMS must also be secure at all times.

The 17 Items given as Minor or Moderate are categorised Minor (11 of the 17) if only one or very few votes are impacted.

The six *deviations* categorised as Moderate are far less uniform:

- two relate to privacy (1 and 26),
- one relates to software failure (6),
- one could either be software failure or voter intent (20), and
- two relate to security of votes and safety of the carrier when votes are being transported from polling places to central scrutiny (27 and 28).

Of the potential hazards surrounding privacy (Items 1 to 3 previously identified in [6] and Item 26), the hazards identified in Items 2 and 3 are adequately mitigated by ensuring that no timestamp data is related to the vote. Item 1 refers to the casting of a vote with an identifiable set of unique preferences. No safeguards can be put in place to avoid this deviation; however, the difficulty inherent in trying to identify a unique set of preferences is illustrated by the fact that eight per cent of all voters submit a vote with a preference for all candidates on the ballot. Item 26 is dependent on a link being established between a voter and their vote external to eVACS®. For example, the issuing officer at a polling place knows the voter’s name and has the opportunity to learn the ‘details printed on the e-voting card issued to the voter (although accurately noting them would not be a simple task). Only while the voter is voting is the e-voting card linked in any way to the voter’s intentions. The issuing officer, or a colleague working with them, would have to gain access to not just the voting server but to the temporary stores (for key presses/keystrokes and preferences) that are linked to the barcode only while voting is in progress. Should this ever be feasible, the frequency of being able to connect voter name with barcode and then access the server without detection is such that the voters likely to be impacted is at most a few.

With the exception of Item 1, all *deviations* have existing safeguards identified, or in the case of new functionality, such as telephone voting, safeguards are proposed that reflect or extend existing safeguards for similar *deviations*.

The importance of having code reviews, thorough testing and auditing, and having checking processes in place is reinforced by the HAZOPS report.

Appendix 1 – Application within eVACS® of the six election principles

Principle	How principle is met
Doorkeeper Master	Electors are checked against the electoral roll by officials and either: • Issued with an e-voting card for the electorate in which they are enrolled, or • Issued with a voting token for the electorate in which they are enrolled The e-voting card or voting token provided contains the electorate identifier to ensure only the required ballot is issued.
Secrecy	At polling places voting occurs in separate voting booths where the voting screen is placed face-up on the shelf in the voting booth so that only the voter can see the screen. For blind or vision impaired (BVI) voters, where the voting screen is orientated in an upright position, the voting booth is orientated in a manner to ensure that traffic cannot walk directly behind an elector casting their vote. Representatives of the BVI community are invited to review the placement of these booths to ensure continued secrecy. For telephone voting, secrecy is maintained by the voter only using key presses to record their vote details. There is no voice communication required in response to the audio instructions/announcements. E-voting cards and voting tokens are randomly assigned to voters so that there is no link to voter identification.
Verification, tally and audit	For electronic votes (telephone or at polling places) access is controlled via authentication of an e-voting card or voting token (the latter used with a PIN) and once a vote is committed the card or token cannot be authorised for use again. The authentication of scanned paper ballots is managed external to eVACS®. Tallying votes within eVACS® involves no manual intervention and is based on software procedures independently audited to show that the counting process does not add, delete or amend votes. A new report records all vote preferences through the count so that any individual vote can be tracked through the count process.

Equality	i) All electors in a particular electorate receive the same ballot paper contents, albeit the candidates within parties are rotated according to Robson Rotation ii) Multi-lingual access is provided via text for those voting electronically at polling places iii) Disability access to eVACS® is provided by a separate booth suitable for wheelchair access, and voting instructions in English are provided via audio at i) polling places and ii) via telephone voting iv) In the ACT an elector can vote from any polling place
Security	Multi-level security is in place addressing: 1) Software security 2) Vote protection 3) Hardware protection 4) Environment controls, and 5) Access controls
Transparency	Provided via: i) Independent audit of both software and documentation describing the system ii) Publication of source code iii) Scrutiny of scanning of ballot papers (or data entry if used)

Appendix 2 – Extract from IEC 61508[3]

A.2.1 Categories of likelihood of occurrence

Category	Definition	Range (failures per year)
Frequent	Many times in system lifetime	$> 10^{-3}$
Probable	Several times in system lifetime	10^{-3} to 10^{-4}
Occasional	Once in system lifetime	10^{-4} to 10^{-5}
Remote	Unlikely in system lifetime	10^{-5} to 10^{-6}
Improbable	Very unlikely to occur	10^{-6} to 10^{-7}
Incredible	Cannot believe that it could occur	$< 10^{-7}$

A.2.2 Consequence categories

In the Elections Domain, the consequence category definitions are based on 'Votes corrupted, lost or publicly identified'.

Electronic Safety Domain		Elections Domain	
Category	Definition	Category	Definition
Catastrophic	Multiple loss of life	Catastrophic	Election results so impacted that the Court of Disputed Elections requires the election to be re-held and/or irreparable reputational damage.
Critical	Loss of a single life	Critical	Significant election concerns however the Court of Disputed Elections does not rule for an election re-run and/or major reputational damage.
Marginal	Major injuries to one or more persons	Moderate	Vote preferences of a small number of people are impacted. Moderate reputational damage. Election result not contested in the courts.
Negligible	Minor injuries at worst	Minor	Issues with votes of one or a few people are raised but they have no possible impact on election results. Minor to no reputational damage.

[3] Source: https://en.wikipedia.org/wiki/IEC_61508

A.2.3 Risk matrix

The likelihood and consequence categories are typically combined into a risk class matrix

	Consequence			
Likelihood	Catastrophic	Critical	Marginal	Negligible
Frequent	I	I	I	II
Probable	I	I	II	III
Occasional	I	II	III	III
Remote	II	III	III	IV
Improbable	III	III	IV	IV
Incredible	IV	IV	IV	IV

Where:

Class I Unacceptable in any circumstance

Class II Undesirable: tolerable only if risk reduction is impracticable or if the costs are grossly disproportionate to the improvement gained

Class III Tolerable if the cost of risk reduction would exceed the improvement

Class IV Acceptable as it stands, though it may need to be monitored

Appendix 3 – HAZOPS

The following table is the report of HAZOPS into the eVACS® election system. Each of the listed Items reflects a *deviation* identified in terms of a guideword and attribute.

There are two *deviations* which have multiple listings: Less/Votes, More/Votes and Modified/Votes, for each of electronic votes at polling places and telephone votes. The explanation provided under **meaning** for each Item indicates which type of vote is being addressed at the particular Item. Although scanned votes are uploaded to eVACS® for counting, hazards associated with the scanning process are considered to be outside the purview of this report.

Items 1 to 3, identified in the earlier HazOP Study [6], have been reviewed and additional information included. These three items relate to specific ways in which the anonymity of voter's vote could be broken. A more generic view of the possibility of a vote no longer being anonymous is provided at Item 27.

The key people who undertook the HAZOPS are: Dr Clive Boughton, Dr Carol Boughton and Rohan Spence.

ITEM #	HAZARD/THREAT (DEVIATION)		CAUSE OF HAZARD/THREAT	CONSEQUENCE IF HAZARD/THREAT CAUSES HARM	EXISTING SAFEGUARDS AGAINST HAZARD/THREAT CAUSING HARM	RECOMMENDATIONS TO INCREASE SAFEGUARDS
	GUIDE WORD	*ATTRIBUTE*				
1	*Extra/Unnecessary*	*Relationship*	An elector may, of his/her own volition or by coercion, enter a vote that possesses a unique combination of preferences able to be identified when examining the published data.	1. An elector and his/her vote may no longer be secret / private. If done for self-reasons, there is no damaging consequence. 2. An elector may be at risk of coercion. If coerced, then the consequences may be damaging for the individual. 3. The security of the election system may be of concern to some voters if a belief develops that individuals' votes can be identified. [*Such consequences are classified as MINOR or MODERATE because if they were to occur they would likely affect single or a very limited number of electors*]	There are no appropriate means to prevent an elector from entering potentially unique combinations of preferences. Within the Polling Place Server, votes are assigned a random number, and votes are then stored in order of the random numbers. As votes are added to the database the order of storing bears no relationship to the order in which votes were committed. It is therefore not possible for a uniquely preferenced vote to be used to triangulate with another vote in order to find out how a specific elector voted.	COMMENT: To ensure uniqueness the voter must attempt to identify a sequence of preferences that no other voter is likely to use. Identifying candidates who are likely to receive a very small number of preferences will increase the probability of creating a unique preference list. Selecting a candidate for the first preference that is likely to receive hundreds or thousands of first preference votes reduces the probability that the vote will be unique. The question then arises, why would a candidate, a candidate's agent or someone with a vested interest in a candidate who is unlikely to receive a high number of votes, coerce an elector into voting a certain way and require proof through a unique set of preferences. This is unlikely to have an effect on the end result in small numbers, and in large numbers becomes increasingly difficult to ensure a unique set of preferences each time. By producing a unique set of preferences the voter casting that vote is highly likely to be 'burning' their own vote for the sake of attempting to identify someone else's. ADDITIONAL SAFEGUARDS: No additional safeguards required.
	Meaning: Relationship (R2) (see diagram Figure 3) may exist between an elector and a vote when an elector creates a unique Preference_List.					
2	*Extra/Unnecessary*	*Relationship*	When only a small number of electors are in a polling place at the same time (generally this would have to be at the very start or very end of voting in order to provide an accurate Batch_ID + PIndex marker), the order in which those electors vote may (through observation) be able to be aligned with the order in which their votes are saved and published, thereby linking an elector to their vote.	1. An elector and his/her vote may no longer be secret / private. 2. An elector may be at risk of coercion. If coerced, then the consequences may be damaging for the individual. 3. The security of the election system may be of concern to some voters if a belief develops that individuals' votes can be identified. 4. The reputation of the EACT and relevant suppliers of electronic voting solutions will be at stake. [*Such consequences are classified as MINOR because if they were to occur they would likely affect single or a very limited number of electors*]	1. By law, no surveillance equipment is permitted within a polling place during an ACT Legislative Assembly Election. 2. No cameras (of any kind) are allowed to be used within a polling place, unless approved by the Electoral Commissioner, and then with strict requirements not to photograph/film voting screens while voting is in progress. 3. Voters are directed to polling place exits if they are observed to be loitering. 4. No information concerning timing is recorded with a vote and votes are randomly ordered.	COMMENT: This hazard is considered as adequately mitigated, as PIndex numbers are not assigned in sequence order of votes committed. ADDITIONAL SAFEGUARDS: No additional safeguards required.
	Meaning: Relationship (R3) (see diagram Figure 3) should never exist between an elector and a vote - but linking an elector to their vote may be possible.					

ITEM #	HAZARD/THREAT (DEVIATION)		CAUSE OF HAZARD/THREAT	CONSEQUENCE IF HAZARD/THREAT CAUSES HARM	EXISTING SAFEGUARDS AGAINST HAZARD/THREAT CAUSING HARM	RECOMMENDATIONS TO INCREASE SAFEGUARDS
	GUIDE WORD	***ATTRIBUTE***				
3	*Extra/Unnecessary*	*Relationship*	When only a small number of electors (in total) vote at a polling place, The order in which those electors vote may (through observation) be able to be aligned with the order in which their votes are saved and published, thereby linking an elector to their vote.	1. An elector and his/her vote may no longer be secret / private. 2. An elector may be at risk of coercion. If coerced, then the consequences may be damaging for the individual. 3. The security of the election system may be of concern to some voters if a belief develops that individuals' votes can be identified. 4. The reputation of EACT and relevant suppliers of electronic voting solutions will be at stake. [*Such consequences are classified as MINOR because if they were to occur they would likely affect single or a very limited number of electors*]	1. By law, no surveillance equipment is permitted within a polling place during an ACT Legislative Assembly Election. 2. No cameras (of any kind) are allowed to be used within a polling place, unless approved by the Electoral Commissioner, and then with strict requirements not to photograph/film voting screens while voting is in progress. 3. Voters are directed to polling place exits if they are observed to be loitering. 4. No information concerning timing is recorded with a vote and votes are randomly ordered. 5. When there are small numbers of votes (less than 20) collected for a particular electorate and polling place these votes are amalgamated with other votes from similar scenarios and counted and published so as to remove the risk of an elector's vote being revealed. 6. Roll mark-off timestamp data is not made public.	COMMENT: This hazard is considered as adequately mitigated, as PIndex numbers are not assigned in sequence order of votes committed and preference data is published in no logical order ADDITIONAL SAFEGUARDS: No additional safeguards required.
	Meaning: Relationship (R4) (see diagram Figure 3) should never exist between an elector and a vote – but linking an elector to their vote may be possible.					

ITEM #	HAZARD/THREAT (DEVIATION)		CAUSE OF HAZARD/THREAT	CONSEQUENCE IF HAZARD/THREAT CAUSES HARM	EXISTING SAFEGUARDS AGAINST HAZARD/THREAT CAUSING HARM	RECOMMENDATIONS TO INCREASE SAFEGUARDS
	GUIDE WORD	***ATTRIBUTE***				
4	*Inaccurate*	*Counting*	The Hare-Clark counting algorithm previously used in eVACS® is replaced with a counting method based on stored procedures (held within the votes database) that were developed for use in Hare-Clark elections undertaken via netVote*plus*. The stored procedures are yet to be used on a large-scale election.	1. An incorrect election outcome could result, with the wrong candidates being elected. 2. The ACT Government might be able to be sued. 3. The election result may be disputed in the Court of Disputed Elections. 4. The reputation of EACT and relevant suppliers of electronic voting solutions will be at stake. [*Such consequences are classified as CRITICAL to CATASTROPHOC depending on the outcome of Court deliberations*]	Extensive testing is undertaken of the eVACS system before use in any election comparing the results of known counts with the same data in eVACS. Counting is undertaken independently by both the vendor and EACT using test samples of votes reflecting normal and unusual collections of vote preferences.	COMMENT: Full scale tests using all votes from previous elections should be undertaken. Such testing needs to be undertaken well in advance of when the system is to be audited for use in the 2020 election. Stored procedures are wrapped in SPARK Ada code to maximise integrity. ADDITIONAL SAFEGUARDS: 1. Have existing Hare-Clark algorithm written in C as a backup. 2. Have the Hare-Clark algorithm written in Ada, since it wouldn't suffer from the same memory management issues as 'C' and enables more reliable programming constructs for checking correctness – unlike 'C' or the stored procedures. 3. All teste be run with both versions ('C' and stored procedures) of the counting program
	Meaning: the stored procedures reflecting the Hare-Clark counting requirements as implemented are found to have an error when used in an election					
5	*Incorrect*	*e-voting card*	The e-voting card issued to the voter contains information to determine which ballot is to be displayed to the voter. If an e-voting card is issued for the wrong electorate, and the voter is unaware of their correct electorate and its candidates, then the voter could vote with the wrong ballot.	1. A vote is recorded for a different electorate. 2. The number of people marked as voted will differ from the number of votes recorded for the enrolled electorate as well as the electorate for which the vote is recorded. [*Such consequences are classified as MINOR*]	Electorate based materials have electorate name printed on them and are all colour coded to mitigate the risk of an incorrect ballot paper or barcode being issued to an elector. LAPPERDS screens are also colour coded and LAPPERDS alerts the issuing officer when an elector is voting from outside of their 'home' electorate. Issuing officers are instructed to say "Here is your [electorate name] ballot paper/barcode" when handing it to the elector.	COMMENT: This hazard is considered as adequately mitigated. ADDITIONAL SAFEGUARDS: No additional safeguards are required.
	Meaning: elector votes in an electorate that is not the electorate in which they are enrolled					

ITEM #	HAZARD/THREAT (DEVIATION)		CAUSE OF HAZARD/THREAT	CONSEQUENCE IF HAZARD/THREAT CAUSES HARM	EXISTING SAFEGUARDS AGAINST HAZARD/THREAT CAUSING HARM	RECOMMENDATIONS TO INCREASE SAFEGUARDS
	GUIDE WORD	***ATTRIBUTE***				
6	*Invalid*	*e-voting card*	Unauthorised e-voting card is produced that eVACS cannot detect as invalid.	1. If accepted by the system an extra or fraudulent vote would be recorded. [*Such consequences are classified as MINOR or MODERATE depending on number of additional votes recorded*]	The e-voting card has a barcode with a checksum, which contains information on the date and name of the election for which it is valid, together with the electorate and polling place identifiers. The validity of the checksum is determined first to establish if the e-voting card is from the polling place where being checked and for the current election. The introduction of QR codes reduces the possibility of unauthorised cards being produced.	COMMENT: Whether or not a barcode has been used/not used is separate to valid/invalid. This hazard is considered as adequately mitigated. ADDITIONAL SAFEGUARDS: No additional safeguards are required.
	Meaning: voter is able to vote with an e-voting card that is one of: • not from the polling place where voting • for a different election • not in the appropriate format					
7	*Incorrect*	*Voting token*	The voting token issued to the voter contains information to determine which ballot and audio is to be played to the voter. If a voting token is issued for the wrong electorate, and the voter is unaware of their correct electorate, then the voter could vote in the incorrect electorate.	1. A vote is recorded for a different electorate. 2. The number of people marked as voted will differ from the number of votes recorded for the enrolled electorate as well as the electorate for which the vote is recorded. [*Such consequences are classified as MINOR.*]	The process for issuing voting tokens to registered telephone voters is yet to be detailed but is likely to be automated within the Election Management System (EMS). The voting tokens will be generated by the Election Server and passed electronically to the EMS which will randomly assign a voting token to the PIN for each registered voter based on the electorate in which the voter is enrolled. An email with the voting token is then to be sent to the registered telephone voter.	COMMENT: A manual process for random assignment of a Voting Token to a particular PIN would provide the assignor with access to the PIN/Voting token pair to be used for telephone voting. This would enable the assignor the opportunity to vote in place of the registered voter. ADDITIONAL SAFEGUARDS: Enforce automating the provision of electorate based voting tokens to electors through the EMS.
	Meaning: 'registered telephone voter' is issued with a voting token not for the electorate in which the elector is registered to vote					
8	*Incorrect*	*PIN/voting token pair*	Telephone voter receives a voting token not linked to their registered PIN	1. Voter will be unable to vote by telephone. [*Such consequences are classified as MINOR*]	Checking of the PIN/Voting Token pair is a two stage process. First the PIN is checked against the registered PINs held in the telephone voting server. If after three attempts a matching PIN cannot be found, the caller is advised to go to a polling place. If a PIN match is found, then the Voting Token is entered and checked as having been assigned to that particular PIN. After three failed attempts to match the PIN and Voting Token, the caller is advised to go to a polling place.	COMMENT: This scenario does not directly disenfranchise an elector – other methods of voting are available to the elector. This hazard is considered as adequately mitigated. ADDITIONAL SAFEGUARDS: No additional safeguards are required.
	Meaning: voter is not able to vote with a PIN/Voting Token pair issued by the EACT					

ITEM #	HAZARD/THREAT (DEVIATION)		CAUSE OF HAZARD/THREAT	CONSEQUENCE IF HAZARD/THREAT CAUSES HARM	EXISTING SAFEGUARDS AGAINST HAZARD/THREAT CAUSING HARM	RECOMMENDATIONS TO INCREASE SAFEGUARDS
	GUIDE WORD	***ATTRIBUTE***				
9	*Invalid*	*PIN/voting token pair*	Invalid PIN/Voting Token pair is not detected by eVACS, because 'unauthorised' information has been uploaded to the Telephone Voting server. There are two possibilities: i) an unauthorised USB-FD with additional PIN/Voting Token data was substituted, or ii) the data in the EMS system was tampered with. Note: For a voter to vote by telephone the entered PIN/Voting Token pair must be found to exist in the telephone voting server database.	1.If accepted by the system an unjustifiable vote would be recorded. [*Such consequences are classified as MODERATE or CRITICAL depending on number of additional votes recorded*]	To ensure data cannot be added during transmission of the PIN/Voting Token pairs to the Telephone Voting server, the data is encrypted and then exported to clean, and preferably write once, media. To upload PIN/token data both a password and Master Admin barcode (QR code) are required. To ensure unauthorised data cannot be exported for transfer to the Telephone Voting server the PIN/Voting Token pairs must be stored in the EMS such that any unauthorised additions can be detected. EACT has processes in place to ensure that electors can only vote once (additional votes must be declaration votes which can be rejected before being counted). If a fraudulent PIN/Token arrangement is established against an elector's name and used to vote – additional votes under that elector's name are not possible. En masse activity such as this will likely be detected. To address possibility of PIN/Voting Token pairs not being linked to voters, the number registered for telephone voting be checked against the corresponding number of PIN/Voting Token pairs exported.	COMMENT: PIN and Voting Token to be of different lengths, say 5 and 7 respectively. For each digit there are 10 possibilities (0, 1, 2, 3, 4, 5, 6, 7, 8, 9), so if there were 1000 (10^3) PIN/Voting Token pairs registered, the likelihood of guessing a registered combination is (10^3) / (10^{5+7}) = 10^{-9} It is most unlikely a particular PIN/Voting pair could be guessed. However, the probability of creating a non-EACT issued PIN/Voting Token pair is ($1 - 10^{-9}$) which is almost one. Hence, if non-EACT pairs can be produced there is a large number of invalid pairs that could be uploaded, which equates to a CRITICAL outcome if the hazard eventuates. ADDITIONAL SAFEGUARDS: No additional safeguards are required.
	Meaning: voter is able to vote with a PIN/Voting Token pair not issued by EACT i.e. unauthorised pair					
10	*Untimely*	*PIN/Voting Token*	PIN/Voting Token pairs are not uploaded to the telephone voting server in the time frame advised to those registering.	1. Voters become frustrated and complain to the media. [*Such consequences are classified as MINOR in terms of impact on votes, but could become very disruptive to other EACT election activities*]	Ensure accurate and consistent information regarding when uploads will occur is provided to registered voters: 1) When registering 2) When they receive their voting token in an email 3) Via the EACT website	COMMENT: If unplanned delays occur, a second email should be sent to registered voters advising of the delay. A defined schedule should be set. However, if registrations are few, a decision to immediately transfer the pair could be made. ADDITIONAL SAFEGUARDS: No additional safeguards are required.
	Meaning: voter is unable to vote by telephone in expected timeframe					

ITEM #	HAZARD/THREAT (DEVIATION)		CAUSE OF HAZARD/THREAT	CONSEQUENCE IF HAZARD/THREAT CAUSES HARM	EXISTING SAFEGUARDS AGAINST HAZARD/THREAT CAUSING HARM	RECOMMENDATIONS TO INCREASE SAFEGUARDS
	GUIDE WORD	***ATTRIBUTE***				
11	*Unsuccessful*	*PIN/Voting Token*	PIN/Voting Token pair is not uploaded to telephone voting server Email with Voting Token not received	1. Voters become frustrated and complain to the media. [*Such consequences are classified as MINOR in terms of impact on votes, but could become very disruptive to other EACT election activities*]	Information on telephone registration process to have description of what voters should do when the expected process fails e.g. email with Voting Token not received. Extensive testing is undertaken of the eVACS system before use in any election. This scenario does not directly disenfranchise an elector – other methods of voting are available to the elector.	COMMENT: ADDITIONAL SAFEGUARDS: No additional safeguards are required.
	Meaning: registered telephone voter is unsuccessful in voting by telephone					
12	*Invalid*	*PIN*	Voter consistently mis-enters their registered PIN	1. Voter becomes frustrated and complains to the media. [*Such consequences are classified as MINOR since no vote is impacted*]	PIN is checked against the registered PINs held in the telephone voting server, and if after three attempts a matching PIN is not entered, the caller is advised to either hang up and call again once the correct PIN is identified or go to a polling place and vote in person.	COMMENT: Registered telephone voter has the opportunity to further check/find their PIN and ring in again. ADDITIONAL SAFEGUARDS: No additional safeguards are required.
	Meaning: voter is unable to vote by telephone despite entering a PIN					
13	*Incorrect*	*Password*	eVACS has failed to apply the rules governing the use of passwords or has incorrectly matched an entered password with an approved/stored password	1. Enables access to eVACS® features not accessible to an unauthorised person 2. An incorrect election outcome could result. 3. The election result may be disputed in the Court of Disputed Elections. 4. The reputation of EACT and relevant suppliers of electronic voting solutions will be at stake. [*Such consequences are classified as CRITICAL or CATASTROPHIC depending on number of votes impacted*]	Extensive testing is undertaken of the eVACS system before use in any election. Passwords policy complies with ASD requirements Polling place servers are housed in a locked cabinet; Election server and telephone voting server are located in access controlled premises. Access to the election server requires both a password and a Master Admin barcode. (QR code)	COMMENT: ACT Government and ASD requirements for passwords include length and combination of alpha numeric characters and symbols to maximise security of passwords. ADDITIONAL SAFEGUARDS: Where eVACS® passwords are not being used in a secure environment, e.g. at polling places, entering password could also require use of Master Admin barcode. Independent security testing
	Meaning: system accepts an incorrect password					

ITEM #	HAZARD/THREAT (DEVIATION)		CAUSE OF HAZARD/THREAT	CONSEQUENCE IF HAZARD/THREAT CAUSES HARM	EXISTING SAFEGUARDS AGAINST HAZARD/THREAT CAUSING HARM	RECOMMENDATIONS TO INCREASE SAFEGUARDS
	GUIDE WORD	***ATTRIBUTE***				
14	*Inaccessible*	*Passwords*	Poor management of passwords	1. Inability to enter the access password to the election server inhibits undertaking any of the functions on the election server, disrupting the election. The disruption caused is dependent on the status of the election and the frequency that backups of the election server have been made. 2. If polling place password (e.g. end of election password) is not known and voting has not commenced, the password cannot be recovered and the setup process needs to be undertaken again, but any backup containing these passwords cannot be used. 3. If polling place password cannot be entered at close of polling, then the first preference count cannot be undertaken. However, this does not impact on the votes data in the database. [*Such consequences are classified as MINOR since they do not impact on election results*]	Passwords are stored in the EACT safe to protect against being misplaced. Access to the safe is restricted to the Electoral Commissioner and Deputy Electoral Commissioner. Access to the election server requires both a password and a Master Admin barcode. If correct password cannot be entered on election server , the election could be setup again and data restored from the most recent backup. The password for end of election access is not provided to polling place officials until after the close of polling.	COMMENT: The importance of ensuring safe and secure storage of the passwords external to eVACS® is essential to avoid unnecessary stress, risk and time delays. ADDITIONAL SAFEGUARDS: In order to avoid having to setup a completely new election, it would be advisable to leave setting up the passwords associated with voting servers until just before selection of the function to create the voting server installation. Regular backup is recommended in the Election Server User Manual, with particular emphasis on backing up after 'generate barcodes' (now also voting tokens) and loading Phase 2 data.
	Meaning: passwords are inaccessible when required.					
15	*Incorrect*	*Information*	Incorrect information is loaded as part of setup Phase 1 and/or setup Phase 2 Incorrect information could include: a) Ballot data b) name/date of election c) Insufficient barcodes and/or voting tokens generated	1. If insufficient barcodes and/or voting tokens are generated, fewer electronic votes are taken than anticipated. 2. If error in a single electorate ballot is not detected until voting commences, then voters for that electorate would all have to vote with paper ballots 3. If the ballot for more than one electorate has an error, then electronic voting may not be able to proceed 4. Depending on the extent and timing of detection of the error(s) the election result may be disputed in the courts. 5. Voters may not be able to vote in accordance with their preferences until issue was discovered (at which point electronic voting for that electorate would be stopped). [*Such consequences are classified as MINOR if detected before voting commences, CRITICAL if* eVACS® *cannot be used at all or potentially CATASTROPHIC if the Court of Disputed Elections requires the election to be re-run*]	EACT currently maintains strict checks of all information before including as Phase 1 or Phase 2 input. Polling place and ballot information is extracted from another system for which the EACT has processes to check information entered. Ballots for each electorate are previewed on the election server before the voting server installation is created. The same barcodes cannot be regenerated; selecting 'generate barcodes' when barcodes already exist, creates a new set of barcodes that replaces the existing set in the database. Phase 1 and Phase 2 can be rerun; information uploaded previously is automatically deleted.	COMMENT: Election information refers to all information uploaded to eVACS®, including number of barcodes and voting tokens to be generated. ADDITIONAL SAFEGUARDS: No additional safeguards are required.
	Meaning: Election event commenced with inaccurate data installed.					

ITEM #	HAZARD/THREAT (DEVIATION)		CAUSE OF HAZARD/THREAT	CONSEQUENCE IF HAZARD/THREAT CAUSES HARM	EXISTING SAFEGUARDS AGAINST HAZARD/THREAT CAUSING HARM	RECOMMENDATIONS TO INCREASE SAFEGUARDS
	GUIDE WORD	*ATTRIBUTE*				
16	*Incorrect*	*Location*	Master Admin QR code for a particular polling place is delivered to the wrong polling place	1. Barcodes will not be for the polling place of the server and all barcodes will be identified as invalid (assumes barcodes were delivered to correct polling place) 2. At least one other polling place that has the wrong Master Admin barcode. 3. Should be detected no later than the start of pre-polling. Electronic voting will not be available until the correct Master Admin QR code is delivered and the location of the server(s) correctly setup. [*Such consequences are classified as MINOR as no votes will be impacted*]	Ballot papers are always available at all polling locations so that voting is not interrupted.	COMMENT: ADDITIONAL SAFEGUARDS: Master Admin barcodes to have the name of the polling place printed on the card with name and date of election. Official in charge of polling place to have instruction to check paperwork, e-voting cards and Master Admin card are all for the same polling place
	Meaning: Voting server at a polling place is setup for the wrong polling place					
17	*Insecure*	*Hardware*	Inadequate protection of hardware Boot sequence on voting server or voting client is not changed (via BIOS) to Boot from hard drive after software loaded from network	1. Hardware is damaged so that voting is not possible a. If voting client damaged or accessed, will cause disruption while being replaced or taken out of service b. If voting server damaged or accessed, could result in loss or addition of votes recorded since last backup c. If election server damaged or accessed could result in votes database being compromised. 2. Uncertified malicious software is installed, which could impact on integrity of the system and potentially vote preferences [*Such consequences are classified as MINOR if related to voting client or MODERATE if eVACS® unavailable for a period of time or CRITICAL to CATASTROPHIC if impact on Server results in Disputed election to be re-run*]	Voting clients are basically dumb terminals and do not store any vote information. All unused ports are to be disconnected via the operating system and physically The only visible part of the voting client is the screen for voting. Voting server is located in locked cabinet out of sight of people entering polling place. Network connecting client to server is also placed out of sight. Dual storage of votes increases possibility that votes may be recoverable. (Strict processes and procedures in place if corrupted or damaged hard drive needs to be accessed to recover votes) Daily cumulative backup of votes at the close of polling are taken off site. If election server compromised then server can be setup again and all votes, from voting servers and scanning, reloaded. Votes from voting servers are available from existing backups or can be exported again. After hours security processes are employed. Access to BIOS is password controlled	COMMENT: ADDITIONAL SAFEGUARDS: Physical locking of unused ports on voting clients and voting servers
	Meaning: location of system hardware is such that hardware is exposed to interference					

ITEM #	HAZARD/THREAT (DEVIATION)		CAUSE OF HAZARD/THREAT	CONSEQUENCE IF HAZARD/THREAT CAUSES HARM	EXISTING SAFEGUARDS AGAINST HAZARD/THREAT CAUSING HARM	RECOMMENDATIONS TO INCREASE SAFEGUARDS
	GUIDE WORD	***ATTRIBUTE***				
18	*Untimely*	*Recovery*	Inadequate recovery arrangements	1. Reputational damage to EACT if voters complain to media. [*Such consequences are classified as MINOR as no votes will be impacted*]	A replacement voting client can be easily swapped with a failed voting client in a known time frame without disruption to voting. A spare polling place server is always configured. Telephone voting audio to switch to message akin to 'voting is currently unavailable, please try again later' Ballot papers are always available for voting to continue within the polling place. Note: Recovery of a voting server is dependent upon the specific failure.	COMMENT: Need to keep voters advised of circumstances and offer voting with paper ballot. ADDITIONAL SAFEGUARDS: No additional safeguards are required.
	Meaning: electronic voting (at polling places or telephone voting) is stopped for an unacceptable time period after experiencing failure					
19	*Insecure*	*Network communication*	Surreptitious access to network	1. Votes might be added, lost or modified, and/or recorded elsewhere – resulting in a disputed election and possible requirement to re-run election. 2. Order of candidates could be modified 3. Voting client functions could be manipulated 4. Attempt to disrupt election and reputation of EACT and electronic voting vendor[*[Such consequences are classified as MODERATE if affecting only one voting client but could escalate to CRITICAL or CATASTROPHIC depending on the extent of interference and if revealed. Any impact on votes may not be determinable*]	Use of HTTPS for communications across the network ensures such communications cannot be interfered with. Layout of network is located to ensure it is not visible and any access can be observed by officials. Establishment of a LAN, and therefore no connection to the internet, effectively limits opportunity and surface of possible cyber-attack.	COMMENT: ADDITIONAL SAFEGUARDS: No additional safeguards are required.
	Meaning: network connecting voting clients to voting server at a polling place becomes/is insecure					

ITEM #	HAZARD/THREAT (DEVIATION)		CAUSE OF HAZARD/THREAT	CONSEQUENCE IF HAZARD/THREAT CAUSES HARM	EXISTING SAFEGUARDS AGAINST HAZARD/THREAT CAUSING HARM	RECOMMENDATIONS TO INCREASE SAFEGUARDS
	GUIDE WORD	***ATTRIBUTE***				
20	*Less*	*Votes*	Votes have not been recorded by the voting server due to: 1. Voter has deliberately not completed their vote. 2. Voter has unintentionally not scanned their e-voting card a second time to commit their vote. Voting server has failed to record a committed vote	1. Some intended votes will be lost. 2. Inaccuracy in number of recorded votes. [*Such consequences are classified as MINOR if it is user error or MODERATE depending on number of votes not recorded through system error (as it would be picked up at the end of each day)*]	eVACS® includes a final screen that assists in identifying possible unintentional vote completion issues. LAPPERDS automates a daily reconciliation process of barcodes issued against votes in the server – highlighting if the server is not recording votes in large numbers (system error). Code reviews, thorough testing and independent audit are used to ensure the voting software does commit votes and does not add, delete or modify votes.	COMMENT: eVACS provides a report on the number of occasions a voter did not swipe their e-voting card a second time ADDITIONAL SAFEGUARDS: No additional safeguards are required.
	Meaning: the number of **electronic votes** at a polling place is less than the number of e-voting cards issued					
21	*More*	*Votes*	Votes have been recorded by the voting server either through cyber-attack or insider actions	1. Indicates that the voting system has been maliciously compromised. 2. Potential disputed election and a potential re-run. 3. Major reputational damage. [*Such consequences are classified as CRITICAL or CATASTROPHIC depending on number of additional votes recorded*]	EACT processes check total e-voting cards and number issued on a daily basis against number of votes in ballot box, so that any discrepancy can be identified as soon as possible. Physical and software protections to limit opportunity for maliciously altering the voting servers. Establishment of a LAN, and therefore no connection to the internet, effectively limits opportunity and surface of possible cyber-attack. Use of https for communications between voting server and voting client limits ability to interfere with transmissions. Voting terminals monitored at all times during polling by e-voting officers to limit opportunity for an insider to add multiple votes. Polling procedures ensure that either the OIC or 2IC must be present within the polling place at all times (i.e. no official is in the polling place alone at any time).	COMMENT: With the security protections in place, the most likely way in which this could happen is by a polling place official. ADDITIONAL SAFEGUARDS: At the end of the election, compare the number of e-voting cards issued at a polling place with the number of votes taken plus the number of votes initiated but not completed at that polling place. This could be done on an electorate basis as well as all votes.
	Meaning: the number of **electronic votes** at a polling place is more than the number of e-voting cards issued					

ITEM #	HAZARD/THREAT (DEVIATION)		CAUSE OF HAZARD/THREAT	CONSEQUENCE IF HAZARD/THREAT CAUSES HARM	EXISTING SAFEGUARDS AGAINST HAZARD/THREAT CAUSING HARM	RECOMMENDATIONS TO INCREASE SAFEGUARDS
	GUIDE WORD	***ATTRIBUTE***				
22	*Modified*	*Votes*	Preferences potentially modified by unauthorised access to: 1) polling place network, either directly or indirectly 2) voting server database 3) votes while being transported 4) election server database 5) system, enabling modification of the software	1. eVACS has been compromised. 2. Potential disputed election and a potential re-run. 3. If occurs after vote(s) have been stored, then malicious interference is likely the cause. 4. Major reputational damage. [*Such consequences are classified as MODERATE during voting, otherwise CRITICAL or CATASTROPHIC depending on the extent of interference and if revealed. Any impact on votes may not be determinable*]	Checking of vote preferences being recorded against screen presses or key strokes to ensure vote is being recorded according to voter selections. If mismatch, error is raised and voting client has to be restarted. No vote is recorded and e-voting card is not marked as used. Code reviews, thorough testing, independent audit, and open source policy are used to ensure the voting software does commit votes and does not add, delete or modify votes, and accurately decrypts for counting the encrypted votes. Physical and software protections to limit opportunity for maliciously altering the voting servers. Establishment of a LAN, and therefore no connection to the internet, effectively limits opportunity and surface of possible cyber-attack. Use of https for communications between voting server and voting client limits ability to interfere with transmissions. Access controls are in place for servers and when votes are being transported	COMMENT: ADDITIONAL SAFEGUARDS: No additional safeguards are required.
	Meaning: electronic vote preferences at a polling place are not the same as those chosen by the voter.					
23	*Less*	*Votes*	Telephone voting server has been compromised	1. Incorrect or inaccurate recording of votes 2. Potential disputed election and a potential re-run. 3. Major reputational damage. [*Such consequences are classified as MINOR if difference is small, but CRITICAL or CATASTROPHIC depending on number of additional votes not recorded*]	PIN/Voting Token pair is not marked as used until PIN is re-entered at end of voting session. Code reviews, thorough testing, independent audit and open source code policy are used to ensure the voting software does commit votes and does not add, delete or modify votes.	COMMENT: ADDITIONAL SAFEGUARDS: No additional safeguards are required.
	Meaning: the number of **telephone votes** is less than the number of PIN/Voting tokens marked as used					

ITEM #	HAZARD/THREAT (DEVIATION)		CAUSE OF HAZARD/THREAT	CONSEQUENCE IF HAZARD/THREAT CAUSES HARM	EXISTING SAFEGUARDS AGAINST HAZARD/THREAT CAUSING HARM	RECOMMENDATIONS TO INCREASE SAFEGUARDS
	GUIDE WORD	***ATTRIBUTE***				
24	*More*	*Votes*	Telephone voting server has been compromised. Unauthorised PIN/Voting Token pairs have been uploaded to the telephone voting server	1. Potential incorrect or inaccurate recording of votes 2. Potential disputed election and a potential re-run. 3. Major reputational damage. [*Such consequences are classified as MINOR if difference is small, but CRITICAL or CATASTROPHIC depending on number of additional votes recorded*]	Physical and software protections to limit opportunity for maliciously altering the telephone voting server. Software protections to limit opportunity to maliciously alter the functions within EMS generating the emails and PIN/Voting Token files for upload to the telephone voting server. Protection of PIN/Voting Token pairs when being transported to telephone voting server.	COMMENT: ADDITIONAL SAFEGUARDS: To address possibility of PIN/Voting Token pairs not being linked to voters, the number registered for telephone voting be checked against the corresponding number of PIN/Voting Token pairs exported.
	Meaning: the number of **telephone votes** is more than the number of PIN/Voting tokens registered/issued					
25	*Modified*	*Votes*	Telephone voting server has been compromised. The system has code within the software that is not recording votes correctly (maliciously or inadvertently).	1. Potential disputed election and a potential re-run. 2. Major reputational damage. [*Such consequences are classified as CRITICAL or CATASTROPHIC depending on number of votes impacted*]	Checking of vote preferences against run through of key presses to ensure vote is being recorded according to voter selections. Code reviews, thorough testing, independent audit and open source code policy are used to ensure the voting software commits votes as intended. Physical and software protections to limit opportunity for maliciously altering the voting servers.	COMMENT: ADDITIONAL SAFEGUARDS: No additional safeguards are required.
	Meaning: the preferences of **telephone votes** are modified					
26	*Nonanonymous*	*Votes*	A means to link a voter with their vote is put into place, either accidently or intentionally	1. People have been tracked when voting and their vote preferences identified 2. Although this does not directly impact on the election results, such an event would damage the reputation of EACT and the vendor of eVACS®. 3. Individuals might also claim that the published vote information is not how they voted, either because they don't remember accurately, or they simply wish to discredit the use of the system. [*Such consequences are classified as MODERATE*]	For electronic and telephone voting there is no information within eVACS that links a voter to their vote. For electronic voting, the e-voting card required to vote at a polling place and the voting token for telephone voting are issued to an elector on a random basis. See also Items 2 and 3	COMMENT: ADDITIONAL SAFEGUARDS: No additional safeguards are required.
	Meaning: information about voters and their votes becomes publicly available					

ITEM #	HAZARD/THREAT (DEVIATION)		CAUSE OF HAZARD/THREAT	CONSEQUENCE IF HAZARD/THREAT CAUSES HARM	EXISTING SAFEGUARDS AGAINST HAZARD/THREAT CAUSING HARM	RECOMMENDATIONS TO INCREASE SAFEGUARDS
	GUIDE WORD	***ATTRIBUTE***				
27	*Insecure*	*Transportation*	Media used for transportation of votes from polling place servers and the telephone voting server to Election HQ is insecure. Information on media is insecure.	1. If accepted by the system incorrect votes would be recorded. 2. Possible reputational damage if storage medium was lost [*Such consequences are classified as MINOR or MODERATE depending on number of votes impacted*]	Votes being transported are a cumulative backup and can easily be downloaded again from the voting server, with different checksums and their QR codes. The votes on the media can only be decrypted by the election server, therefore the details of the votes cannot be deciphered or published. There is no information on the media to indicate the voters who cast the votes. If media is handed in with the QR codes for the checksums, the election server is able to determine if the files have been modified. If the media is handed in without the QR codes for the checksums, the data could not be uploaded into the election server (the checksum entry is mandated) and a replacement backup would be sought.	COMMENT: ADDITIONAL SAFEGUARDS: No additional safeguards are required.
	Meaning: votes are lost or modified during transportation					
28	*Unsafe*	*Transportation*	People intent on disrupting the election could accost those transporting the votes Driving or walking in the public environment	1. Media with the daily cumulative votes are stolen, misplaced or destroyed leading to possible reputational damage of EACT [*Such consequences are classified as MINOR or MODERATE depending on harm to the individual*]	Votes being transported are a cumulative backup and can easily be downloaded again from the voting server, with different checksums and their QR codes. The votes on the media can only be decrypted by the election server, therefore the details of the votes cannot be deciphered or published. There is no information on the media to indicate the voters who cast the votes. If media is handed in with the QR codes for the checksums, the election server is able to determine if the files have been modified or already uploaded. If the media is handed in without the QR codes for the checksums, the data could not be uploaded into the election server (the checksum entry is mandated) and a replacement backup would be sought.	COMMENT: ADDITIONAL SAFEGUARDS: No additional safeguards are required.
	Meaning: people involved in transporting votes (downloaded from polling place servers and the telephone voting server) to Election HQ are exposed to risks on the road and/or risks as a pedestrian					

ITEM #	HAZARD/THREAT (DEVIATION)		CAUSE OF HAZARD/THREAT	CONSEQUENCE IF HAZARD/THREAT CAUSES HARM	EXISTING SAFEGUARDS AGAINST HAZARD/THREAT CAUSING HARM	RECOMMENDATIONS TO INCREASE SAFEGUARDS
	GUIDE WORD	***ATTRIBUTE***				
29	Substitution	Software	Unauthorised access to eVACS software is attained Unaudited previous version of software is installed intentionally or inadvertently for official election event creation	1. eVACS does not operate as it should 2. Election results may not reflect the voters' preferences 3. Reputational damage to EACT and electronic voting vendors 4. Potential withdrawal of Legislative Assembly support for electronic voting 5. Potential disputed election and a potential re-run. [*Such consequences are classified as CATASTROPHIC*]	Once the eVACS software has been audited the vendor does not have access to the software and therefore cannot change any of the software comprising eVACS. Returned code from independent auditor is physically certified The returned audited software is kept in the EACT safe. Access to the safe is restricted to the Electoral Commissioner and Deputy Electoral Commissioner. The Deputy Electoral commissioner is the officer responsible for creating official election event	COMMENT: ADDITIONAL SAFEGUARDS: No additional safeguards are required
	Meaning: Some or all of the eVACS software used in an election has been replaced with unaudited software					
30	Accessible	Passwords	Passwords are inadequately protected	1. Unauthorised access to eVACS is obtained 2. Could enable election server functions to be accessed and even election setup changed with incorrect information 3. Reputational damage to EACT and electronic voting vendors 4. Potential withdrawal of Legislative Assembly support for electronic voting 5. Potential disputed election and a potential re-run. 6. Access to first preference count results at polling places could be prematurely provided to individuals, parties or the public. [*Such consequences are classified as MINOR for early release of preference count to CATASTROPHIC if all setup election information is modified*]	Election server passwords are stored in the EACT safe. Access to the safe is restricted to the Electoral Commissioner and Deputy Electoral Commissioner. End of election passwords are only provided to polling place OICs after the close of polls and are kept secure prior to this date (as above) Access to polling place server passwords does not provide access that can allow altering or viewing of votes	COMMENT: ADDITIONAL SAFEGUARDS: No additional safeguards are required
	Meaning: unauthorised use of passwords					

– END OF DOCUMENT –