Business Requirements Specification

ICT business system upgrade

– eVACS®

Elections ACT

2018-19

Revision History

Document Amendment Register

Version	Version Date	Author	Amendment Description
v0.1	4 December 2018	Trisha Benson	Initial Draft
	7 February 2019	Ro Spence	Comments
v0.2	8 February 2019	Trisha Benson	Draft 2
	14 March 2019	Ro Spence	Comments
	18 March 2019	Dr Carol Boughton	Comments
v0.3	18 March 2019	Trisha Benson	Draft 3
v0.4	9 April 2019	Trish Benson	Draft 4 following mtg with SI
V0.5	30 April 2019	Ro Spence	Final amendments before provision to SI
V0.6	3 May 2019	Ro Spence	After comments from SI
V1.0	5 June 2019	Ro Spence	Final for contract

1. Introduction

1.1. Definitions

Current system:	The June 2014 version of eVACS®, the Electronic Voting and Counting System originally built by Software Improvements for use by Elections ACT at the 2001 ACT Legislative Assembly Election. Following upgrades for all subsequent elections, the current system was used by Elections ACT at the 2016 ACT Legislative Assembly election
Elections ACT:	The ACT Electoral Commission
IRAP:	Information Security Registered Assessors Program. An Australian Signals Directorate initiative to assess the implementation, appropriateness and effectiveness of a system's security controls.
The system:	eVACS®
Vendor:	Software Improvements Pty Ltd

1.2. Purpose

The purpose of this document is to outline to the vendor of eVACS®, Software Improvements Pty Ltd, the requirements for upgrade of eVACS® from the current system, deployed for the 2016 ACT election, to a system with improved security and functionality, ready for deployment at the 2020 ACT election. This document follows the successful business case to ACT Treasury for funding announced in the 2018-19 budget.

See: G:\EC\3.2FinancialManagement\3.2.1BudgetAndEstimates\2018-19\2018-19 Budget\Budget bids\EVACS upgrade - Capital budget bid\Business case\ACT Electoral Commission ICT Business Case 2018-19 - FINAL.pdf

1.3. Business problem

Following recommendations made by the ACT Auditor-General in relation to the 2016 ACT election, RSM Australia was commissioned to review electronic voting in the ACT. Their report advised that eVACS® requires major modernisation of the underlying technologies and hardware to address risks identified by the review. These include: a vulnerable operating system, together with the absence of modern data management and security protocols, such as database level encryption, which improve robustness and security within any ICT business system; a 2001 originating system which cannot meet the compatibility requirements of modern hardware, especially by 2020; and a shortage of software developers and support personnel skilled in maintaining a system developed in outdated and vulnerable technologies.

The risks identified are critical when considered in reference to an ICT business system fundamental to the integrity of an election process and crucial to the successful delivery of an ACT Legislative Assembly election.

Addressing concerns raised by MLAs, centred around the perceived antiquity of the system, emanating from the use of keypads for navigation, this project includes the introduction of touchscreen functionality to the eVACS® system.

Telephone voting functionality is also being introduced to address submissions to the *Select Committee Inquiry into 2016 ACT Election and the Electoral Act* by representatives from the blind and vision-impaired community.

This project is intended to fully upgrade the ACT Electoral Commission's ageing, mission-critical ICT business system – the Electronic Voting and Counting System (eVACS®), to ensure its reliability, security and supportability at the 2020 ACT Legislative Assembly election.

1.4. Key stakeholders

Name	Position	Project position	Contact Details
Damian Cantwell AM	ACT Electoral Commissioner	Project Sponsor and Financial Delegate	[redacted]
Ro Spence	ACT Deputy Electoral Commissioner	Program Manager	[redacted]
TBA	Elections Operations Manager	Project Manager	[redacted]
Carol Boughton Clive Boughton	Software Improvements – Managing Directors	Vendor	[redacted]

1.5. Project scope – inclusions

- [redacted]

1.6. Project scope – exclusions

- [redacted]

2. Overview

2.1. Perspective

eVACS® has been used at the 2001, 2004, 2008, 2012 and 2016 ACT elections and has gone through upgrades between each election. The system comprises five modules – setup; voting; data entry; counting and reporting.

Following the 2016 ACT election, Elections ACT commissioned an independent external review of electronic voting in the ACT to be conducted by RSM Australia.

The review ultimately found that the current eVACS® solution provides an effective electronic voting solution for ACT pre-polling voting activities. However, for the solution to be effectively delivered for future elections, a number of activities must be undertaken with regards to the design, security and frameworks surrounding the solution.

By accepting and implementing many of the recommendations from this review, the aim of this upgrade project is to ensure that:

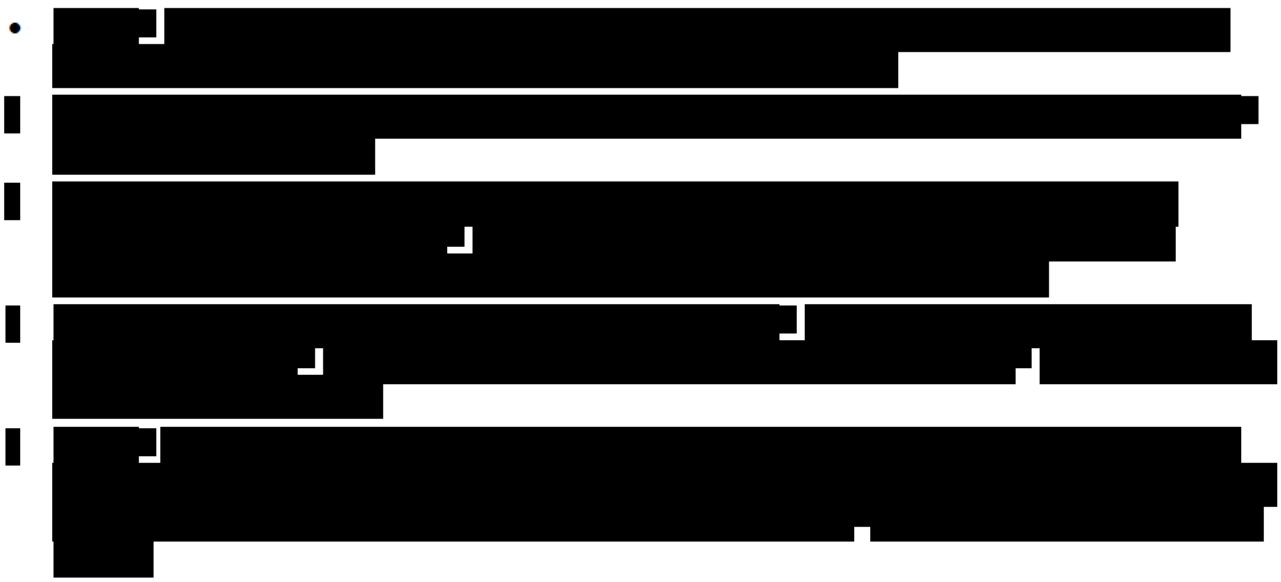
(a) election data security throughout the system continues to be maintained effectually; through improvements in design, security and functionality;
(b) eVACS® continues to be an effective, usable, reliable and trustworthy voting medium for use by ACT electors; and
(c) the Commission can continue to source ongoing avenues of support prior to, during and following the 2020 ACT Legislative Assembly election.

The Commission has a licence to use eVACS® in perpetuity granted by the owners of the system, Software Improvements Pty Ltd.

The counting module of eVACS® is reliant upon an output from the ACT Electoral Commission's ballot paper scanning system.

Currently, the setup module is reliant on files from the Commission's election management system (TIGER) while files from the reporting module are uploaded to TIGER following the counting process.

2.2. Types of users



- [redacted]

2.3. Operating environment

The hardware configuration and specifications to be purchased for the 2020 election are yet to be determined and will be dependent on the modernisation of the underlying technologies. The RSM Australia Review (2017) also identified that contemporary hardware would proactively improve data protection and permit the ability to leverage off advancements in hardware specifications (G:\EC\3.4InformationTechnology\ICT Projects\Project - EVACS\2017 – Review\Report - FINAL - ACT eVACS review report - 14 Feb 2018 – pg. 42).

2016	2020
eVACS® is currently a Linux-based operating system on standalone LANs.	• eVACS® will continue to function as an isolated LAN within each voting centre however, based on RSM comments and security recommendations from various stakeholders, thought should be given to improving the security provisions of eVACS® through the inclusion of an embedded operating system.
• At the 2012 and 2016 elections, WYSE terminals were imaged to function as the voting client terminals.	• In an effort to reduce the number of peripherals and cable connections required (in response to RSM comments and recommendations) Elections ACT expects to engage voting machines that comprise an 'all-in-one' (CPU and monitor) unit. This is also likely to streamline deployment of the hardware within a pre-poll centre.
• eVACS® polling place servers are ordinary PC boxes. Server boxes require two IDE hard drives and a CD burner.	• The current servers owned by Elections ACT and used at the 2012 and 2016 election are aging and Elections ACT anticipates purchasing new units to serve as polling place and election HQ servers. • While the exact specification and determinations are yet to be made, it is likely, based on currently available common contemporary hardware, and purported greater reliability over Hard Disk Drives, that each server will incorporate a Solid State Drive (SSD) configured to provide RAID at an appropriate level. • Servers are increasingly being built without optical drives such as CD/DVD drives. Accordingly, it is likely that an appropriate

	solution will need to be found to replace the processes currently performed via the CD-ROM drive. The redeveloped software will need to support, in a secure way, an appropriate means to install/create/upload setup files as well as producing the cumulative vote records at the end of each voting day.
• Normal desktop monitors (23″) are used as the screen for the voting terminals and servers.	• In an effort to reduce the number of peripherals and cable connections required (in response to RSM comments and recommendations) Elections ACT expects to engage voting machines that comprise an 'all-in-one' (CPU and monitor) unit. • As touch-screen functionality is being introduced, these all-in-one units will be required to support touch as a navigation mechanism.
• eVACS® is currently written in 'C'.	• eVACS® is to be converted largely on a like-for-like basis in the Ada programming language. With the exception of the data entry module that will remain in 'C' code.
• Barcode scanners are used to read barcodes which initiate and end the casting of a vote by an elector.	• QR code readers and codes will replace the current barcode scanners, to enable multi-directional scanning.
• Blind and vision impaired electors are able to cast a vote using a specially provisioned voting terminal that connects to a telephone style keypad and headphones allowing the elector to navigate through the system via audible instructions and confirmations.	• Blind and vision impaired electors will continue to be able to cast a vote as has been previously provisioned, but will also be able to cast a vote without having to attend a polling place by casting their vote over an eVACS® provisioned telephone system.

2.4. Constraints

[redacted]

2.5. Assumptions

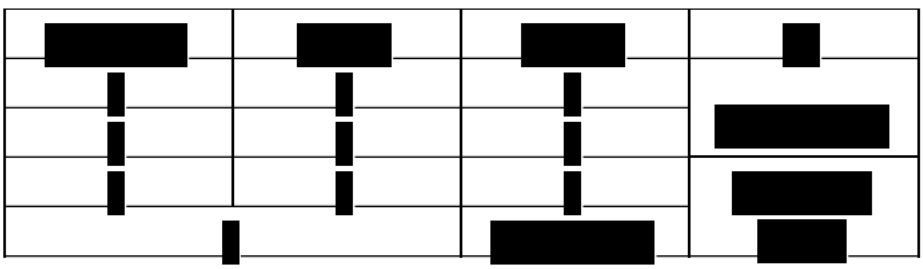
- [redacted]

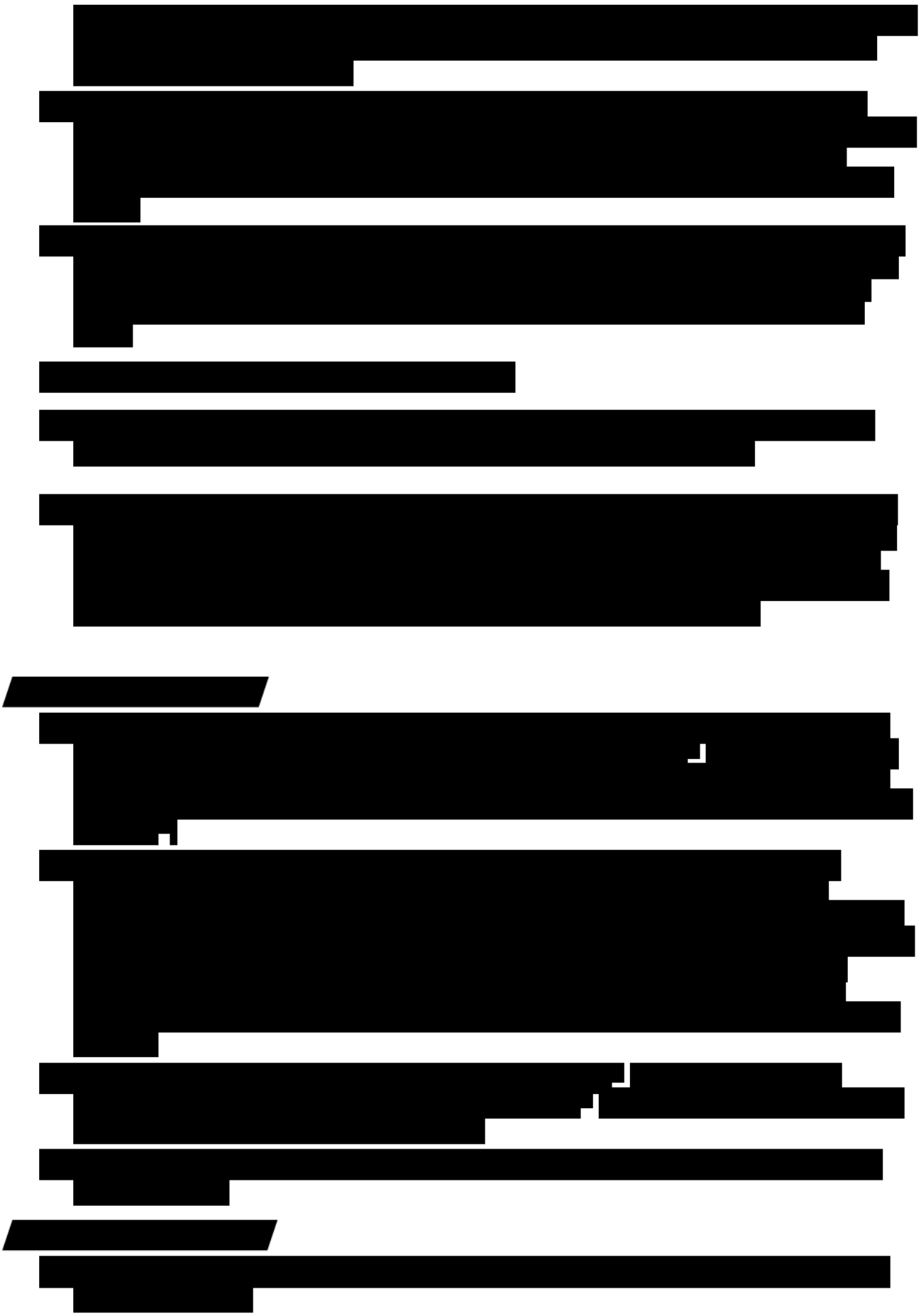
- [redacted]

3. Requirements

[redacted]

(c) [redacted]





3.2. Business requirements

Identifier	Requirement for upgrading eVACS®	Rationale and notes
#		This section comprises the justification and explanation of the requirement.
1.	Replicate the functionality and operational procedures of the current eVACS® solution onto a more contemporary technology platform. (all requirements from BR.2 onwards are exceptions to this requirement that are included to improve upon the functionality, security and operational procedures of the system)	eVACS® has successfully functioned as a secure and trusted electronic voting system since the 2001 ACT election. A recent review into electronic voting in the ACT found that while the system has performed well, the technology platform on which it sits is outdated and benefits can be realised if it is migrated to a more modern platform, including the software language. The core of this project is to update eVACS® functionality and process on a like-for-like basis so that the core processes remain. Following this requirement (from #2. onwards) are a suite of further requirements that are designed to upgrade eVACS® so that it can take advantage of modern security protocols and modern hardware, as well as identifying particular areas of eVACS® that can be improved.
	SECURITY AND INTERGRITY	
2.	Physically limiting the availability of ports on the hardware used within the polling place	The RSM review noted a security risk in relation to unused ports on servers and client terminals. To mitigate this risk, Elections ACT seek to ensure the ability to 'decommission' ports that are not necessary for the system to function. In addition to the ability to disable ports Elections ACT is also likely to physically restrict access to the unused ports.
3.	Shall be no less secure in its operations than the 2016 version of eVACS®	It is essential that the upgrade improvements use proven contemporary technologies to ensure the new version of eVACS® maintains a secure voting process throughout the election process. All decisions, whether they be on system architecture, functionality, technology or operational process, should all have security, secrecy and transparency at the forefront of thinking.

		Software Improvements is to deliver an electronic voting solution for electronic votes taken at polling places or via telephone voting (see requirement 41) that completely prohibits the possibility that: • an elector can be matched to their voting preferences; and • an elector's voting preferences can be deleted or altered in any way.
4.	Create a HAZOPS document.	In order to minimise the potential for fraud and vote manipulation it is important to identify potential hazards and risks and then determine the consequences and probability of those identified hazards/risks occurring. It is then important to devise ways and means to reduce the consequences or probability of occurrence down to a level acceptable to the Electoral Commission. Elections ACT would like Software Improvements to work with known experts in this area to create a HAZOPS document, or something similar, as a means to identify potential real and perceived electoral integrity issues and outline the safety-guards in place to minimise the risk of occurrence. This document is likely to be used when communicating the effective mitigation practices in place when faced with outside queries over the system's integrity.
5.	Passwords throughout the system should only be able to be set if they meet ACT Government password security requirements.	It should not be possible to create a password in the system that does not conform to ACT Government and ASD password security standards. Below is the standard taken from the SSICT document: Strong passwords that meet the standard required contain at least three character sets comprising any three of the following: • upper and lower case characters, e.g. a-z, A-Z • have digits and punctuation characters as well as letters, e.g. 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<> ? , . / • are at least ten alphanumeric characters long for standard users, and a minimum of 12 characters for users with privileged access accounts
6.	The entire software code shall be written in a modern language that can provide a safer and more secure environment.	Migrate the current functionality and operating process '*like-for-like'*, from 'C' language to 'Ada'.

7.	Ensure that an elector and their preferences cannot be matched through the use of timestamp data.	The RSM Review identified that there is still potential to link an elector's identity to a vote by using timestamps within eVACS®. As such, the Review recommended updating the underlying algorithm to further minimise this risk of tracing an individual's voting preferences. This could be achieved by shuffling the votes (see requirement 8) to de-link the timestamp from the first scan of the QR Code or removing the capture of timestamp data entirely. The solution should ensure that the elector's identity cannot in any way be linked to their vote.
8.	Shuffle the votes when stored	The current eVACS system stores the votes within the polling place server in consecutive order. In theory this raises the possibility of matching an elector's preferences with the order in which they cast their ballot within the polling place. To eliminate this possibility the vote order should be randomly shuffled within the vote storing module.
9.	Fully encrypt the voting process	RSM review identified that the current solution, which transmits raw voting data between the vote being cast and stored on the polling place server, could be viewed as a risk to vote integrity. eVACS should protect each individual vote throughout the voting process so that it cannot be manipulated at any point and the integrity of the vote cannot be questioned. Some comments from SSICT and ASD in relation to protecting the vote include: ■ Each individual vote, once it has been cast, is encrypted should use *ASD-approved cryptographic algorithms* and transport the encrypted package *using **only** ASD-approved cryptographic protocols.* ■ SSICT asks 'Will the vote be encrypted by the device or will the transmission of data be encrypted?'

		■ ASD suggested that '*transport layer encryption* may be sufficient instead of *message level encryption*, and both transport and message level encryption can work together. If message level encryption is used, consider how encryption keys will be managed.' Based on these comments from each stakeholder, Elections ACT seeks the most appropriate means in which to achieve the improved vote integrity.
10.	Update the methodology used to ensure authenticity of exported data	When daily vote data is copied onto CD-ROMs, a unique code (a hash) is created and recorded. On arrival back at Election HQ the unique code is used to verify that the data on the disk has not been tampered with and is an exact copy of the votes recorded on the polling place server. The mechanism to create this unique code is based on a methodology (MD5) which is obsolete and no longer considered secure. The mechanism to authenticate the data exported from polling place servers for import into the election server should be updated to meet contemporary best practice and the industry standard. ASD recommends that the 'Information Security Manual' on encryption and hashing be consulted in order to update the methodology used to reduce the risk of tampering. https://www.acsc.gov.au/infosec/ism/
11.	Mandate the entry of 'hash code' on the election server	When daily vote data is copied onto CD-ROMs, a unique code (a hash) is created and recorded. On arrival back at Election HQ the unique code is used to verify that the data on the disk has not been tampered with and is an exact copy of the votes recorded on the polling place server. (See requirement 10 for the requirement to change how the code is generated). The Auditor General's performance report found that eVACS could be improved through enforcement of the entering of a unique code before data is transferred from the polling place server to the Election (counting) server.

		Elections ACT acknowledges that by doing so the process of uploading daily votes could become labour intensive. Accordingly, a solution that does not require a long string of alphanumeric characters be typed would be advantageous. See requirement 31 for a potential solution.
	SETUP AND INSTALLATION	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

		[redacted]
15.	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

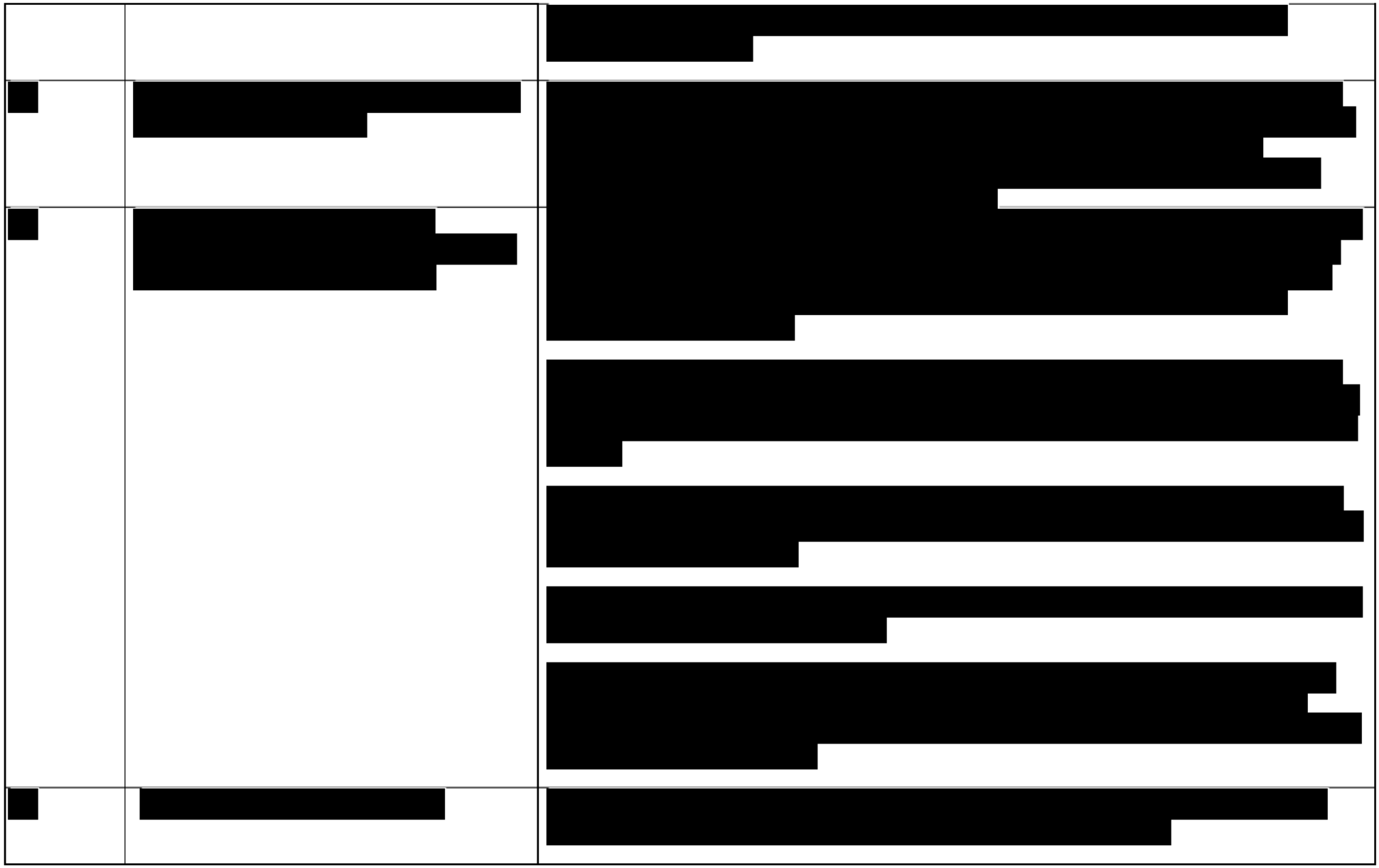
18.	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
	THE VOTING PROCESS	

22.	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

27.	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
30.	Replace CD-ROMs as the medium for upload and download of data	eVACS® currently uses CD-ROMs as a means for setting up the election server and imaging polling place servers and client terminals, as well as for the down load of daily polling data on a 'Master/Slave' arrangement.

		The benefit of CD-ROMs was that they were assured to be clear of malicious data and were write once. The inclusion of CD-ROM drives on PCs is becoming rare and accordingly eVACS must find a suitable replacement for the use of CD-ROMs throughout the system. The replacement must be able to assure that malicious code will not be introduced to the system and should, if possible, assure that data cannot be deleted or altered.
31.	Replace alphanumeric 'hash code' with QR code produced by polling place server	See requirement 10 for the requirement for updating the hash code methodology. As an alternative to a string of alpha numeric characters, it would make the authentication process easier and less error prone if a unique QR code (or barcode) is generated by the polling place server and printed (see requirement 37) to be transported together with the cumulative data to the Election server for upload. A QR code (or barcode) reader attached to the Election server in Elections HQ would be used to read the code to confirm the data's authenticity before the data is transferred to the counting module. Such a process would remove the potentially time consuming and painstaking task of manually entering a string of characters each time a new data disk is required to be imported.
	REPORTING	
32.	[redacted]	[redacted]

33.	[redacted]	[redacted]



		[redacted]
	ADDITIONAL	
40.	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

		[redacted]
42.	[redacted]	[redacted]

3.3. Ongoing Maintenance/Agreement Plan

Identifier	Requirement for eVACS®	Rationale and notes
43.	[redacted]	[redacted]

3.4. Manuals

Identifier	Requirement for eVACS®2	Rationale and notes
44.	[redacted]	[redacted]

3.5. Backup & Recovery Requirements

Identifier	Requirement for eVACS®	Rationale and notes
45.	[redacted]	[redacted]

Requirements Acceptance Certificate

Accepted by Elections ACT:

Damian Cantwell AM	ACT Electoral Commissioner
Signed:	
Date:	

Accepted by Software Improvements:

Dr Carol Boughton	Managing Director
Signed:	
Date:	
Comments:	