



# Ohio Secretary of State

Office of J. Kenneth Blackwell

---

## Diebold Direct Recording Electronic (DRE) Technical Security Re-Assessment Report

Updated August 18, 2004

**COMPUWARE**



**Compuware Corporation**

1103 Schrock Road, Suite 205

Columbus, Ohio 43229

(614) 847-8212

This page intentionally left blank.

- From Black Box Voting Document Archive -

## Table of Contents

PART ONE: EXECUTIVE SUMMARY .....	1
Introduction.....	1
Work in Scope.....	3
Methodology and Approach.....	5
Platform Review .....	6
Code Review.....	7
DRE System Interfaces and Tasks .....	8
Work Flow/Process Model.....	10
Environment.....	12
Hardware Configuration .....	12
Software Configuration.....	12
Requirements Identified.....	13
Test Scenarios .....	13
Risks Identified .....	14
Potential Vulnerabilities & Recommended Mitigation Strategies .....	14
Conclusion .....	17
PART TWO: DIEBOLD.....	18
Overview.....	18
Step 1: Characterization of the AccuVote-TSX Voting System .....	18
AccuVote-TSX System Interfaces .....	19
Work Flow / Process Model .....	21
Environment.....	24
Hardware Configuration .....	24
Software Configuration.....	24
Network Configuration .....	25
Step 2: Threat Identification .....	26
Step 3: Vulnerability Identification.....	27
Requirements Tested & Test Results .....	27
Test Areas .....	27
Specific Tests and Test Results.....	27
Step 4: Controls Analysis.....	54
Step 5: Threat Likelihood .....	54
Step 6: Impact Analysis .....	56
Step 7: Determine Risks.....	58
Risks Identified.....	58
Risk Levels of Identified Risks.....	82
Step 8: Risk Mitigation Strategies .....	85
Recommended Risk Mitigation Strategies.....	85
Code Review.....	85
Platform Review .....	88
Platform Review (continued).....	89
Physical Testing.....	90

Step 9: Document Results ..... 91  
Conclusion ..... 91  
ATTACHMENT A: Risk Assessment Methodology ..... 1  
ATTACHMENT B: Glossary ..... 1  
ATTACHMENT C: Documents Referenced..... 1

- From Black Box Voting Document Archive -

# PART ONE: EXECUTIVE SUMMARY

## Introduction

The Ohio Secretary of State (SOS) hired Compuware Corporation to conduct an extensive security re-assessment and revalidation of the Direct Recording Electronic (DRE) voting machine from Diebold Election Systems. Diebold is one of four vendors who were qualified by the SOS to help upgrade the state's voting systems as required by the Help America Vote Act of 2002 (HAVA). The four vendors' DREs were assessed by Compuware and documented in a reported titled *Direct Recording Electronic (DRE) Assessment Report*, dated November 21, 2003.

This report covers the re-assessment of Diebold's DRE: the AccuVote-TSX. Compuware will re-assess the Diebold ITA-certified software and hardware. The scope of the re-assessment is to validate that the Diebold risks identified in the original four-vendor assessment have been addressed. Compuware will also run a full set of source code, Platform and Physical regression tests to ensure that new code did not negatively impact existing code.

In order to ensure the integrity of this assessment, the SOS and Compuware set up a secure, real-world testing environment at the State of Ohio Computer Center (SOCC). Compuware obtained the hardware to be tested from Diebold, and set up the equipment in a secure, locked room at the SOCC facility. The assessment team then used this hardware and the ITA certified software to conduct hands-on testing and re-evaluation.

Compuware also requested from Diebold their old source code that was used in the original technical assessment in 2003. We compared the old to the newly certified and concentrate on key areas that are related to security, reliability and code that changed in this new release from the old source code.

*Continued on the next page*

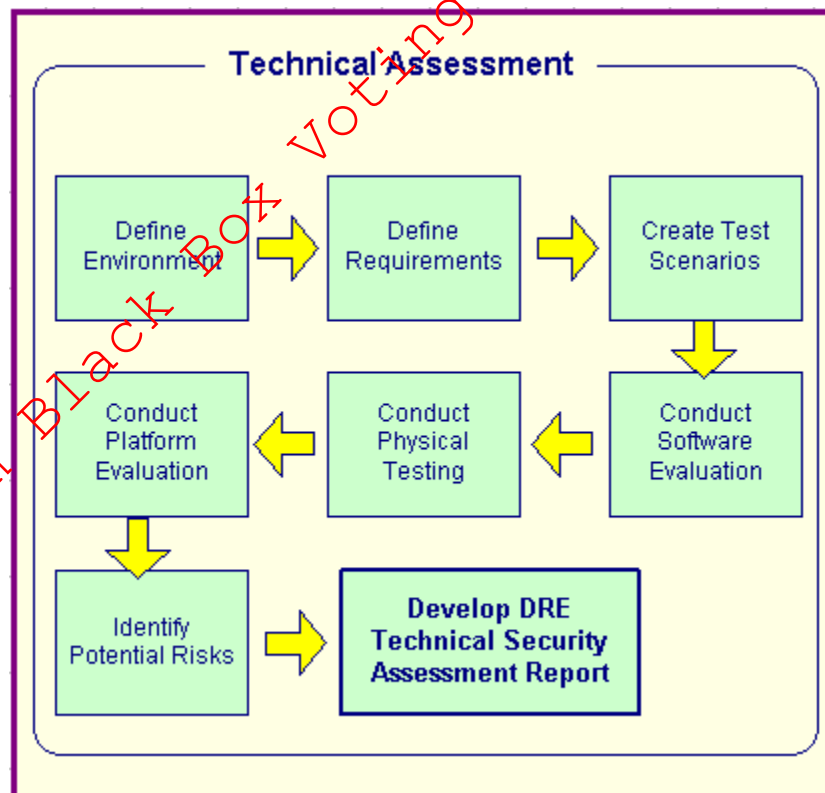
## Introduction (continued)

Compuware conducted a technical review and test of the source code, operating systems, and hardware platforms of the DRE. This report details the steps used to assess the DRE and presents the findings of the technical assessment, including an evaluation of the risks and vulnerabilities that were discovered. The report identifies:

- Requirements tested
- Test scenarios used
- Test results
- Risks identified
- Likelihood and impact of identified risks
- Risk mitigation strategies
- Recommendations

In addition to Compuware's focus on technical assessment, independent consulting firm InfoSENTRY is participating in the security re-assessment. InfoSENTRY is conducting a re-evaluation of the administrative policies and procedures utilized by Diebold to ensure that security is built in and maintained in their voting systems. In addition, InfoSENTRY has delivered election system security policies and procedures to the Secretary of State for implementation.

The following diagram shows the division of responsibilities for the overall security assessment.



**Figure 1 – Security Assessment Overview**

## Work in Scope

The scope of this effort was to provide a Security Assessment for the following DRE voting machine:

- AccuVote-TSX from Diebold Election Systems

The scope is limited to the various hardware and software components of the DRE plus any data input or output streams which service the DRE. For example, we investigated the transfer of the ballot definition data from the respective election management software programs to the DRE, but we did not investigate the election management application itself.

The scope was expanded to also review the source of the Key Card Tool (KCT) and Voter Card Encoder (VCE) components. The KCT is new and was not a part of the original DRE assessment. Diebold added it to fix PIN Card encryption risks.

The assessment was conducted on the hardware and software versions currently approved by the Ohio Board of Voting Machine Examiners for use in Ohio. Although some of the vendors have more recent versions that they have or will be submitting for approval, these more recent products were not evaluated because they are currently not certified for use in the State of Ohio.

Compuware tested the following hardware and software in this technical security re-assessment:

Vendor	Hardware	Software
Diebold Election Systems	<ul style="list-style-type: none"> <li>• AccuVote-TSX, Windows CE 4.1</li> <li>• Boot loader 4-16-2004</li> <li>• Voter Card Encoder from Spyrus</li> </ul>	<ul style="list-style-type: none"> <li>• Global Election Management System (GEMS) version 1.18.22</li> <li>• Ballot Station for AccuVote-TSX 4.5.1</li> <li>• Key Card Tool version 1.0.1</li> <li>• Voter Card Encoder 1.3.2</li> <li>• OpenSSL .97c</li> </ul>

*Continued on the next page*

The following tasks were within the scope of Compuware's assessment.

- Defined environment of DRE – Identified the components of the DRE and all data streams that service the DRE.
- Defined requirements of DRE – Identified and documented the requirements that DREs must meet to operate in a secure environment.
- Run test scenarios – For each specific DRE, implement test scenarios designed to reveal whether the security requirements above were met by the DRE.
- Conducted platform review of DRE – Reviewed the hardware, design documentation, and other vendor information to determine potential security risk areas. Use of removable media, network ports, access controls, and input devices were evaluated.
- Conducted software code review of DRE – Reviewed the software, design documentation, and other vendor information to determine potential security risk areas. Use of encryption, checksums, and passwords were evaluated. Code was also reviewed for existence of software engineering discipline.
- Conducted physical testing of DRE – Test scenarios were executed and results captured.
- Identified and re-evaluated risks identified of DRE – Based on the results of the previous assessment and the current code review, platform review, and physical testing, a list of risks was documented and evaluated for likelihood and severity.
- Identified mitigating strategies – The assessment team recommended solutions that are intended to mitigate or eliminate the risks identified. The goal of the recommended risk mitigation strategies was to reduce the level of risk to the electronic voting system and its data to an acceptable level.

## Methodology and Approach

This assessment was performed based on the methodology documented in National Institute of Standards and Technology (NIST) SP 800-30, *Risk Management Guide for Information Technology Systems*.

The diagram below illustrates the methodology used. (Refer to Attachment A of this document for a detailed explanation of the methodology.)

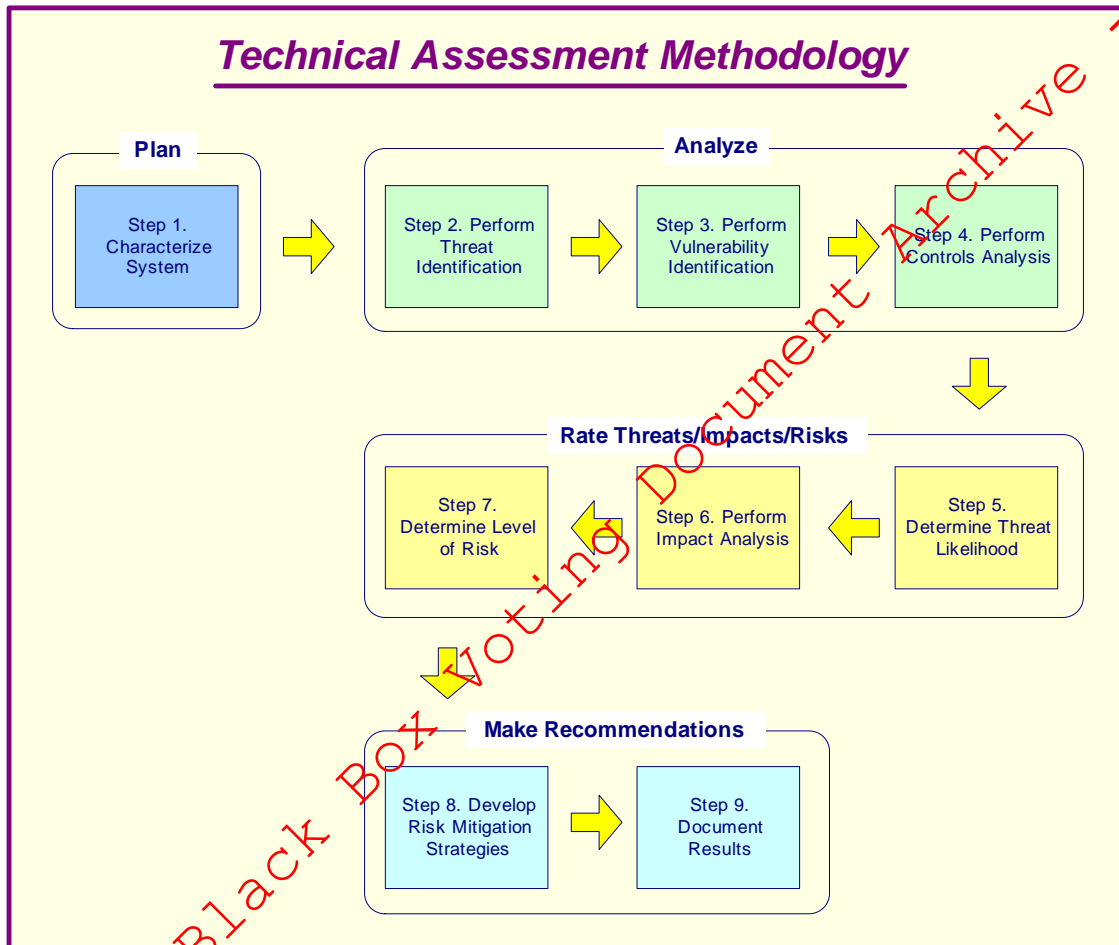


Figure 2 – Technical Assessment Methodology

## Platform Review

This section describes the approach that was followed in the Platform Review portion of the technical security assessment.

### 1. Analyzed and Documented

The security assessment began by making an analysis of the components that comprise the system. Detailed information was collected through study, analysis, product literature, Question and Answer sessions with vendor, and hands-on observations of the product.

- a. Characterized the system through study and analysis of all the physical and logical components of each system.
- b. Performed reviews, demonstrations, and Question and Answer sessions with the vendor.
- c. Documented details and initial findings.

### 2. Identified and Scheduled Tasks

Plans were defined and tasks were scheduled to identify potential risks in the system.

- a. Reviewed details and findings, then mapped out a task trail or procedural methodology based on specification details.
- b. Assigned tasks in a project plan.

### 3. Performed Scans of Hardware and Network Components

Implementing the assigned tasks was specific to the vendor's product / system. Scan implementation proceeded in a logical manner that was defined by the make-up of the system.

- a. Defined a scan policy for each target or system.
- b. Performed or estimated site reconnaissance analysis.
- c. Performed threat identification.
- d. Performed vulnerability scans and identification.
- e. Performed network scans and identification.
- f. Performed exploitation analysis.
- g. Documented findings and impact analysis.
- h. Performed cryptographic analysis.

### 4. Rated Threats/Impacts/Risks

Compiled and assimilated the collected information. Conducted reviews and performed analysis. Documented initial findings and determined threat likelihood, levels of risk, and impact analysis.

- a. Analyzed security loopholes.
- b. Determined the threat likelihood.
- c. Performed impact analysis.
- d. Determined level of risk.

### 5. Made Recommendations and Suggestions

Compiled and documented overall results and findings. Developed risk mitigation strategies. Submitted recommendations and suggestions.

- a. Documented results.
- b. Developed risk mitigation strategies.
- c. Made suggestions and recommendations.
- d. Submitted reports.

## Methodology and Approach (continued)

### Code Review

This section describes the approach that was followed to perform the Code Review portion of the technical security assessment.

1. Reviewed for Standard Programming Practices

The vendor-supplied source code was visually reviewed to make sure it followed industry standard programming practices. The review checked to see if a consistent pattern was followed in having descriptive code comments, and if consistent and self-describing naming conventions were used for variables, modules, and constants. The code should have been broken into separate modules or classes and each module should have had functions that perform specific tasks to make it readable and easy to follow.

2. Reviewed Security Features and Error-Handling Logic

The code should have also implemented security features such as password protection for critical pieces of the vendor software. A review was done to see if industry standard encryption techniques were employed to protect critical data (ballot information, vote record and audit trail) in voting systems and while transferring them across a network to other software systems. The code was also reviewed to see if proper error handling logic had been added consistently throughout the code so that the systems were stable in the event of an error and sufficient information on the state of the system was recorded for future debugging purposes. Code was checked to see if the vote data was stored in multiple locations so that information could be recovered in case of a system disaster. The review also focused on whether industry standard checks had been implemented in the code to make sure the data was not corrupted.

3. Reviewed Database and Third Party Code Security

The data model and any database code supplied were also reviewed to see if referential integrity of the database was maintained, and to assess the security levels implemented for database access at the application level. Attention was paid to any third party components used in the applications, as their use requires strict guidelines, security standards and version control. All third party code supplied by the vendor was reviewed to make sure it did not have code providing additional functionality other than what was needed and that it adhered to the security standard of the application.

4. Reviewed Documentation

The scope of the code review included reviewing the documentation associated with the applications. The requirements documents, system and code design documents, and technical code documents were reviewed to analyze the relationship between code modules and functional requirements of the application. For example, requirements should have been closely tied to modules for easier code management; changes in requirements should have been easily pointed to specific code modules that required modifications.

**Note:** Given the short time frame of the project, it was not possible to review every single line of code in all of the applications. Review of the code was done using a sampling of code files from these applications. Analysis from the sampling of code files was extrapolated to the overall architecture of the applications.

## DRE System Interfaces and Tasks

The following diagram provides a graphical overview of the connections to the DRE. The diagram shows the input/output connections between the DRE and external entities such as the BOEs and voters. The context diagram helps to define the scope of the voting system and the related voting processes and becomes the top level of the analysis hierarchy.

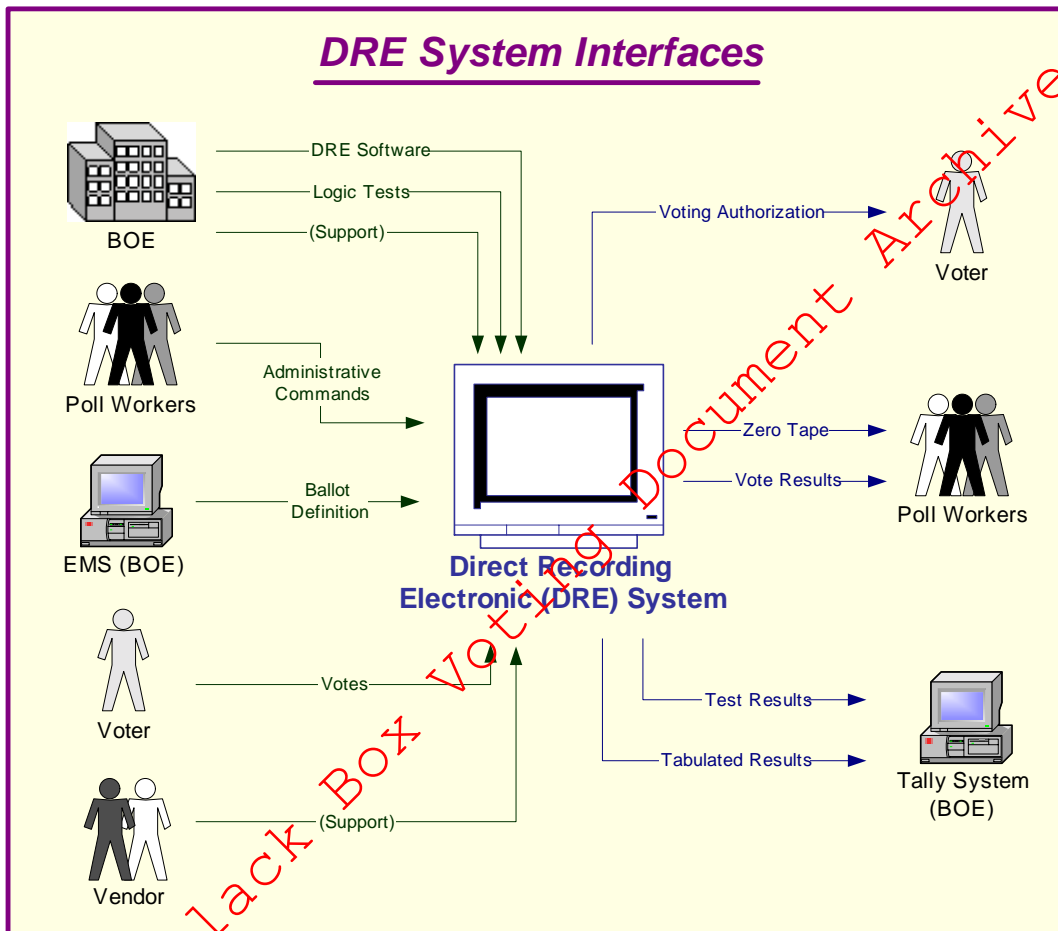


Figure 3 – DRE System Interfaces

Continued on the next page

## DRE System Interfaces and Tasks (continued)

Following is an explanation of the tasks related to the DRE system interfaces.

Inputs	Outputs
<b>Board of Elections</b>	
<ul style="list-style-type: none"> <li>Election Management Software (EMS) is installed on a computer at the Board of Elections (BOE).</li> <li>The BOE uses the EMS to create the ballot definition that is loaded to the DRE.</li> </ul>	
<ul style="list-style-type: none"> <li>Workers at the BOE enter data into the DRE to perform the logic and accuracy testing (LAT).</li> <li>If there is a problem, the BOE troubleshoots the problem and determines if county workers can solve the problem or if the vendor needs to be called.</li> </ul>	Workers at the board verify the results that were entered in the LAT.
<b>Vendor</b>	
If there is a problem with the LAT, the vendor may be called in to repair the unit. If the unit is repaired, it must successfully go through the LAT tests before it may be used in an election.	
<b>Poll Workers</b>	
<ul style="list-style-type: none"> <li>Poll workers set up the booth.</li> <li>Poll workers open the DRE for voting.</li> <li>Poll workers authorize the voter to vote.</li> </ul>	Poll workers print a zero tape from the DRE to ensure there are no pre-existing votes recorded on the unit.
<b>Voter</b>	
Voter takes the authorization to vote to the DRE and votes the ballot. The DRE prevents the voter from over-voting, notifies of under-voting, and presents the ballot choices for review as appropriate.	
<b>Poll Workers</b>	
	<ul style="list-style-type: none"> <li>Poll workers print result tapes from the DRE.</li> <li>Poll workers post one result tape at the precinct.</li> <li>Poll workers remove the media and send the media and a copy of the result tape to the BOE.</li> </ul>
<b>Board of Elections</b>	
	<ul style="list-style-type: none"> <li>The BOE places the media from the DRE into a media reader, and the EMS tally software counts the votes.</li> <li>The BOE prints and releases the results.</li> </ul>

## Work Flow/Process Model

The following diagram provides a graphical overview of the work flow associated with the DRE system interfaces, and represents the next level down from the Context Diagram. This diagram displays the flow of data through the DRE system interfaces in a generic manner.

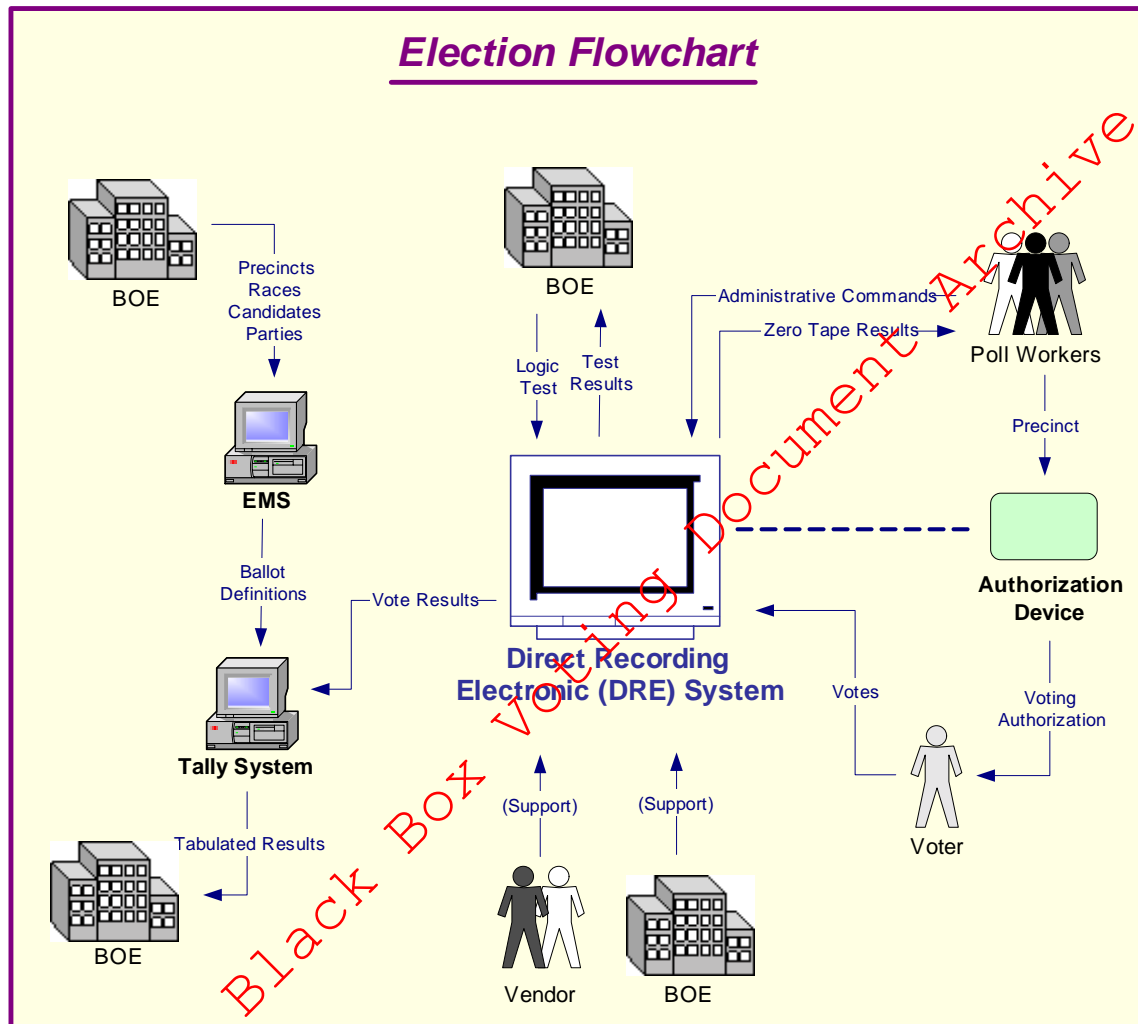


Figure 4 – Election Flowchart

Continued on the next page

## Work Flow/Process Model (continued)

Following is an explanation of the workflow associated with the DRE system interfaces.

Inputs	Outputs
<b>Board of Elections</b>	
<ul style="list-style-type: none"> <li>Election Management Software (EMS) is installed on a computer or on a closed network at the BOE.</li> <li>Precincts are entered into the EMS either by data entry or by loading from the county voter registration system.</li> <li>Races are defined in the EMS and related to the precincts.</li> <li>Candidates are entered into the EMS and related to the races.</li> <li>The BOE uses the EMS to create the ballot definition that is loaded to the DRE.</li> <li>A copy of the database is transferred to the Tally software.</li> </ul>	
<ul style="list-style-type: none"> <li>Workers at the BOE enter data into the DRE to perform the logic and accuracy testing (LAT).</li> <li>If there is a problem, the BOE troubleshoots the problem and determines if county workers can solve the problem or if the vendor needs to be called.</li> </ul>	Workers at the BOE verify the results that were entered in the LAT.
<b>Vendor</b>	
If there is a problem with the LAT, the vendor may be called in to repair the unit. If the unit is repaired, it must successfully go through the LAT tests before it may be used in an election.	
<b>Poll Workers</b>	
<ul style="list-style-type: none"> <li>Poll workers set up the booth.</li> <li>Poll workers open the DRE for voting.</li> <li>Poll workers authorize the voter to vote.</li> </ul>	Poll workers print a zero tape from the DRE to ensure there are no pre-existing votes recorded on the unit.
<b>Voter</b>	
Voter takes the authorization to vote to the DRE and votes the ballot. The DRE prevents the voter from over-voting, notifies of under-voting, and presents the ballot choices for review as appropriate.	
<b>Poll Workers</b>	
	<ul style="list-style-type: none"> <li>Poll workers print result tapes from the DRE.</li> <li>Poll workers post one result tape at the precinct.</li> <li>Poll workers remove the media and send the media and a copy of the result tape to the BOE.</li> </ul>
<b>Board of Elections</b>	
	<ul style="list-style-type: none"> <li>The BOE places the media from the DRE into a media reader, and the EMS tally software counts the votes.</li> <li>The BOE prints and releases the results.</li> </ul>

## Environment

### Hardware Configuration

Following is a summary of the hardware configuration for the DRE.

Processor Type	Processor Clock Speed	Memory	Operating System	Communications Slots	Interfaces
<b>Diebold AccuVote-TSX</b>					
Hitachi SH3 Family of microprocessors	118 MHz	<ul style="list-style-type: none"> <li>16MB Flash ROM</li> <li>32MB RAM - No hard disk</li> <li>PCMCIA card – 128MB</li> </ul>	Windows CE 4.1	<ul style="list-style-type: none"> <li>2 PCMCIA card slots</li> <li>Smart card reader slot (ISO 7816)</li> <li>Phone Jack: Though attached to the motherboard is an optional modem.</li> </ul>	<ul style="list-style-type: none"> <li>RS-232 for Keypad (output)</li> <li>Audio, mini-8 stereo</li> <li>Touch Screen</li> </ul>

### Software Configuration

Following is a summary of the software configuration for the DRE.

Firmware	User Interface	Internal Storage	Communications Protocols	Security
<b>Diebold AccuVote-TSX</b>				
<ul style="list-style-type: none"> <li>Operating system is Windows CE 4.1.0</li> <li>Boot Loader 4-16-2004</li> <li>Ballot Station 4.5.1</li> </ul>	<ul style="list-style-type: none"> <li>Uses a touch screen with a GUI interface with simple controls.</li> <li>The font is Arial, and there is a minimal amount of graphics.</li> </ul>	<ul style="list-style-type: none"> <li>Data is stored in binary flat files on the PC Card.</li> <li>Additional fonts and audio are also stored on the Flash Memory.</li> </ul>	<ul style="list-style-type: none"> <li>When an optional network card is inserted. Uses TCP/IP over an Ethernet connection.</li> <li>SSL is used to encrypt data over the local network.</li> <li>Uses IDE interface to communicate with removable storage media.</li> <li>PPP/RAS encrypted by SSL over a modem</li> </ul>	<ul style="list-style-type: none"> <li>Access is limited by smart card and PIN.</li> <li>Smart card security keys can be modified for each election.</li> <li>Some Contents of Removable storage media are encrypted DES.</li> </ul>

Continued on the next page

## Requirements Identified

Following is a summary of the number of requirements tested during Compuware's security assessment.

Vendor	Number of Requirements Identified	Number of Requirements Not Applicable
Diebold	96	1

## Test Scenarios

Following is a summary of the number of test scenarios conducted during Compuware's technical security assessment.

Vendor	Number of Test Scenarios			
	Code Review Tests	Platform Review Tests	Physical Tests	Total
Diebold	30	18	47	95

## Risks Identified

The results of each test scenario were evaluated and specific risk statements were identified for each vendor. Each risk was analyzed and assigned a likelihood of LOW, MEDIUM, or HIGH. Similarly each risk was assigned an impact of LOW, MEDIUM, or HIGH. An overall risk level was assigned by combining the likelihood with the impact.

## Potential Vulnerabilities & Recommended Mitigation Strategies

Compuware has recommended a risk mitigation strategy for each of the risks identified above. These vendor specific mitigation strategies can be found in the Recommended Risk Mitigation Strategy sections of this document for the vendor. The goal of each recommended risk mitigation strategy is to reduce the level of risk to the electronic voting system to an acceptable level.

While conducting the discovery for information on this security assessment a number of general vulnerabilities to the election process were noted. The following mitigation strategies address those general risks and we recommend the SOS implement them in a timely manner in addition to the vendor specific mitigation strategies.

### 1. The SOS should implement an Information Technology and Security Policy Standards Document for all related material within any election using a DRE system.

- a. This point is brought to light since Ohio uses the FEC Standards Document, which is very broad in its security concerns.
- b. The SOS needs to develop a document that would be a formal and concise set of standards for all IT and Software Testing. This document would not be as broad as the Federal Standards and would cover new technology and risks.
- c. The creation of a formal Security Plan would fall in line with a new set of IT and Software Testing Standards for the State of Ohio.

*Continued on the next page*

## **Potential Vulnerabilities & Recommended Mitigation Strategies (continued)**

2. **The SOS needs to consider the creation of a Security Director position to oversee Policies, Procedures, Information Technology and Security concerns regarding any election in which a DRE system is used.**
  - a. This position would require a broad security background ranging from Information Technology, Secure VPN's and LAN-WAN Management to policy and standards creation.
  - b. A landline telecommunication background would also be helpful when dealing with remote counties who have limits in their network.
  - c. The position's responsibilities would include, but are not limited to, Independent Verification and Validation that the security policies and procedures are followed.
3. **The SOS should consider the implementation of a statewide set of security policies and standards for all counties to follow when using any DRE system.**
  - a. One set of security standards and policies should be in place for all counties to adhere to during any election using a DRE system, otherwise there would be inconsistencies in all counties.
  - b. If one set of policies is not followed by all BOEs, a county not following policy will risk the potential for an unsecured election.
  - c. Before any election using a DRE system with any electronic transmission of results is conducted, transmission and auditing requirements need to be defined and implemented.
  - d. Security documentation for the entire election process is necessary for election integrity.
4. **After the above three recommendations have been addressed, the SOS will need to consider the creation of a formal Security Training and Awareness Program for all counties.**
  - a. To properly implement the new Security Standards and Policies for electronic voting in Ohio, all counties will need to be properly trained.
  - b. This will insure that all elections using a DRE system can be secure for both the voter and all of the County Boards of Elections.
  - c. If training is not provided to the counties, there is the risk that security controls could be thwarted and the election could be compromised.
  - d. A testing or validation process should be implemented which documents that the training was delivered and that the recipient comprehended the essential points of the training.

*Continued on the next page*

## **Potential Vulnerabilities & Recommended Mitigation Strategies (continued)**

5. **The SOS should require Ohio Voting Machine vendors to demonstrate their software development capabilities by achieving Software Engineering Institute CMM Level 2 certification within one year and achieving CMM Level 3 certification within three years.**
  - a. CMM Level 2 ensures the vendor utilizes policies and procedures for managing a software project and has instituted basic software management controls.
  - b. CMM Level 3 ensures a standard process for developing and maintaining software is documented and used across the organization. The process integrates both software engineering practices and management processes into a coherent process.
  - c. Organizations who have adopted the CMM have reported improvements in productivity and released application quality as a result.
  
6. **As new versions of DRE software and hardware are released for use in Ohio, the SOS should conduct independent testing similar to this assessment to ensure the voting systems continue to meet all necessary security requirements.**
  - a. This process recognizes that each modification to the installed base of voting machines carries the potential to introduce unintended security risks.
  - b. Future versions of vendor DRE hardware and software should become more secure as risks are identified and addressed.

The above recommendations apply for a DRE System that is not connected to a network. If the systems being used were to be connected to a network for possible voter identification, elections results or election setup, the recommendations above would need to be amended. Since there is a possibility for the County Boards of Elections to connect DREs to a network in the future, it is recommended that all possible network security issues be included in any future document.

Currently the SOS and County Boards of Elections have no formal Information Technology, Software or Security Standards and Policies Guidelines with regard to DRE systems. If the County Boards of Elections proceed with an election without using the above recommendations, they have a high risk of vulnerabilities. These vulnerabilities could result in election tampering and fraud when using a DRE System.

## Conclusion

Compuware conducted study of one DRE voting system from a vendor who was qualified by the state of Ohio to help upgrade the state's voting systems as required by HAVA. Our study identified specific security vulnerabilities that might be exploited during an election and recommended actions to mitigate these vulnerabilities. The scope of this study was limited to reviewing the technical implementation of each DRE plus reviewing each data stream into and from the DREs. It did not include a review of the policies, procedures, or work practices of either the vendors or the Ohio Secretary of State.

During the course of our study, Compuware identified several significant security issues, which left unmitigated would provide an opportunity for an attacker to disrupt the election process or throw the election results into question. These are documented throughout this assessment report. Following careful consideration of each of these security issues, we developed mitigation recommendations for the Secretary of State to implement which we believe will limit the likelihood of a successful attack or inadvertent disruption to the election process. Provided that mitigating strategies are executed for each risk identified before the systems are used in an election, Compuware concluded that the Secretary of State can securely deploy these voting machines.

Election policies and procedures have long been used to ensure fair and accurate election results. The deployment of electronic voting technology will not lessen the need for well thought out and consistently enforced policies and procedures.

## PART TWO: DIEBOLD

### Overview

This section details the assessment for the Diebold AccuVote-TSX DRE. The AccuVote-TSX system is a voter-activated interactive touch-screen system. Using a smart card as the voter authorization, the AccuVote-TSX permit voters to view and cast their votes by touching target areas on an electronically generated ballot.

Each unit provides a direct-entry computerized voting application that automatically records and stores appropriate ballot information and results. At the end of the voting period, the system can print precinct totals to be included as part of the permanent record.

The AccuVote-TSX is supported by the Global Election Management System (GEMS) software, which provides ballot creation, vote tabulation, and reporting.

The AccuVote-TSX prevents the voter from overvoting, notifies the voter of undervoting, and allows the voter to review and modify their ballot choices before casting their ballot.

Compuware tested the following hardware and software in this technical security assessment:

Hardware	Software
<ul style="list-style-type: none"> <li>• AccuVote-TSX, Windows CE 4.1</li> <li>• Boot loader 4-16-2004</li> <li>• Voter Card Encoder from Spyrus</li> </ul>	<ul style="list-style-type: none"> <li>• Global Election Management System (GEMS) version 1.18.22</li> <li>• Ballot Station for AccuVote-TSX 4.5.1</li> <li>• Key Card Tool version 1.0.1</li> <li>• Voter Card Encoder 1.3.2</li> <li>• OpenSSL .97c</li> </ul>

### Step 1: Characterization of the AccuVote-TSX Voting System

In Step 1, the AccuVote-TSX was examined for the following:

- AccuVote-TSX system interfaces – input/output connections between the AccuVote-TSX and external entities, and the related voting processes
- Work flow / process model – flow of data through the AccuVote-TSX system interfaces, and the related voting processes
- AccuVote-TSX environment
  - Hardware configuration
  - Software configuration
  - Network configuration

### AccuVote-TSX System Interfaces

The following diagram provides a graphical overview of the connections to the AccuVote-TSX. The diagram shows the input/output connections between the AccuVote-TSX and external entities such as the BOEs and voters.

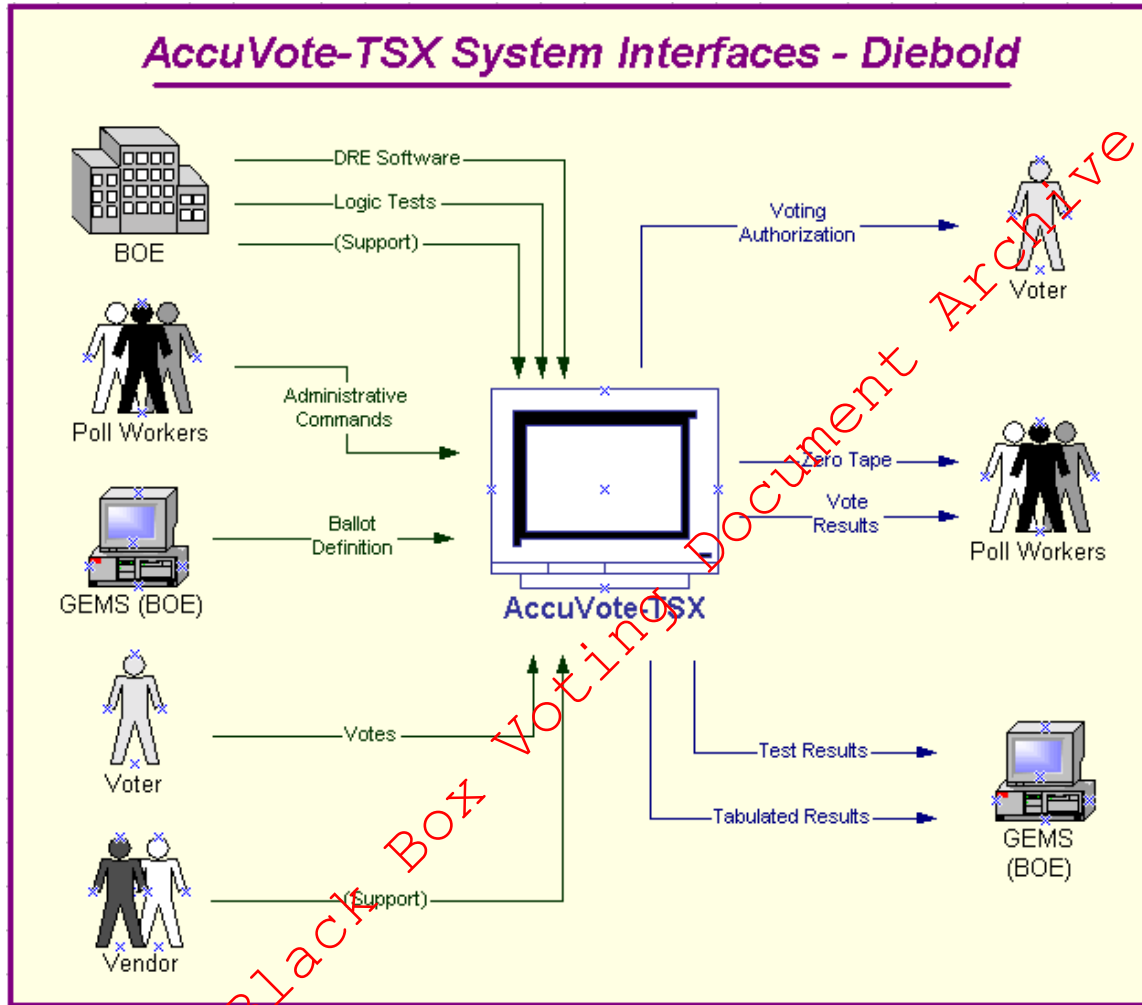


Figure 5 – AccuVote-TSX System Interfaces - Diebold

Continued on the next page

## AccuVote-TSX System Interfaces (continued)

Following is an explanation of the tasks related to the AccuVote-TSX system interfaces.

Inputs	Outputs
<b>Board of Elections</b>	
<ul style="list-style-type: none"> <li>Global Election Management Software (GEMS) is installed on a computer at the Board of Elections (BOE).</li> <li>The BOE uses the GEMS to create the ballot definition that is loaded onto the AccuVote-TSX.</li> </ul>	
<ul style="list-style-type: none"> <li>Workers at the BOE enter data into the AccuVote-TSX to perform the logic and accuracy testing (LAT).</li> <li>If there is a problem, the BOE troubleshoots the problem and determines if county workers can solve the problem or if the vendor needs to be called.</li> </ul>	Workers at the board verify the results that were entered in the LAT.
<b>Vendor</b>	
If there is a problem with the LAT, the vendor may be called in to repair the unit. If the unit is repaired, it must successfully go through the LAT before it may be used in an election.	
<b>Poll Workers</b>	
<ul style="list-style-type: none"> <li>Poll workers set up the booth.</li> <li>Poll workers open the AccuVote-TSX for voting.</li> <li>Poll workers authorize the voter to vote by issuing the voter a smart card.</li> </ul>	Poll workers print a zero tape from the AccuVote-TSX to ensure there are no pre-existing votes recorded on the unit.
<b>Voter</b>	
<ul style="list-style-type: none"> <li>Voter receives the smart card and inserts it into the AccuVote-TSX, which presents the correct ballot for the voter.</li> <li>Voter votes the ballot. The AccuVote-TSX prevents the voter from over-voting, notifies of under-voting, and presents the ballot choices for review as appropriate.</li> </ul>	
<b>Poll Workers</b>	
Poll worker receives the smart card from the voter after the voter casts the ballot.	<ul style="list-style-type: none"> <li>Poll workers print result tapes from the AccuVote-TSX.</li> <li>Poll workers post one result tape at the precinct.</li> <li>Poll workers remove the media and send the media and a copy of the result tape to the BOE.</li> </ul>
<b>Board of Elections</b>	
	<ul style="list-style-type: none"> <li>The BOE places the media from the AccuVote-TSX into a media reader, and the votes are counted by the GEMS tally software.</li> <li>The BOE prints and releases the results.</li> </ul>

### Work Flow / Process Model

The following diagram provides a graphical overview of the workflow associated with the AccuVote-TSX system interfaces, and represents the next level down from the Context Diagram. This diagram displays the flow of data through the AccuVote-TSX system interfaces.

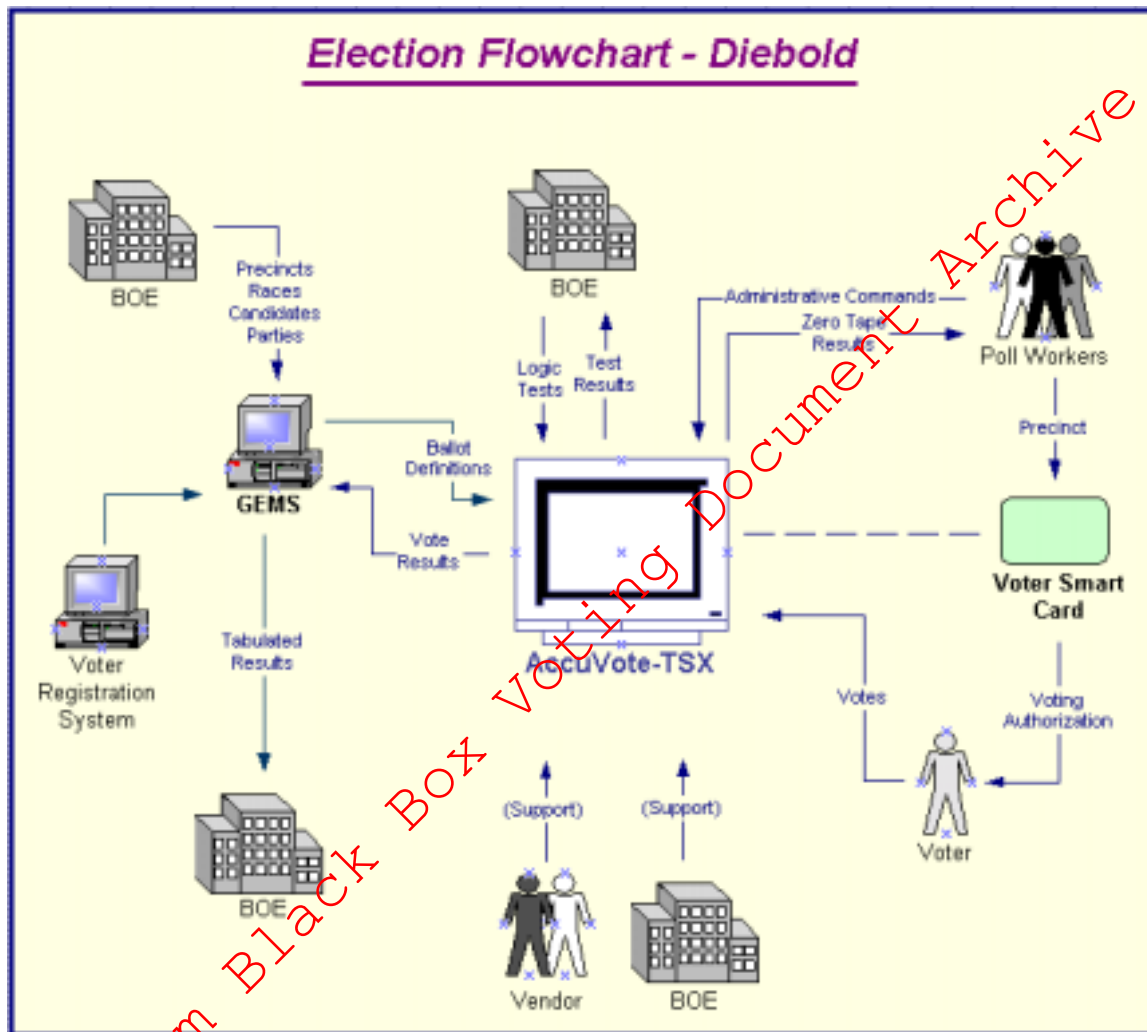


Figure 6 – Election Flowchart - Diebold

Continued on the next page

### Work Flow/Process Model (continued)

Following is an explanation of the workflow associated with the AccuVote-TSX system interfaces.

Inputs	Outputs
<b>Board of Elections</b>	
<ul style="list-style-type: none"> <li>Global Election Management Software (GEMS) is installed on a computer or on a standalone network at the BOE.</li> <li>Precincts are entered into the GEMS either by data entry or by loading from the county voter registration system.</li> <li>Races are defined in the GEMS and related to the precincts</li> <li>Candidates are entered into the GEMS and related to the races.</li> <li>The BOE uses the GEMS to create the ballot definition that is loaded to the AccuVote-TSX.</li> </ul>	
<ul style="list-style-type: none"> <li>The PCMCIA card that contains the ballots is inserted into the AccuVote-TSX.</li> <li>Workers at the BOE enter data into the AccuVote-TSX to perform the logic and accuracy testing (LAT).</li> <li>If there are problems, the BOE troubleshoots the problem and determines if county workers can solve the problem or if the vendor needs to be called.</li> </ul>	Using the GEMS Tally feature, workers at the BOE verify the results that were entered in the LAT.
<b>Vendor</b>	
If there is a problem with the LAT, the vendor may be called in to repair the unit. If the unit is repaired, it must successfully go through the LAT before it may be used in an election.	
<b>Poll Workers</b>	
<ul style="list-style-type: none"> <li>Poll workers set up the AccuVote-TSX voting booth.</li> <li>Poll workers open the AccuVote-TSX for voting.</li> <li>Poll workers authorize the voter to vote by issuing the voter a smart card.</li> </ul>	Poll workers print a zero tape from the AccuVote-TSX to ensure there are no pre-existing votes recorded on the unit.
<b>Voter</b>	
<ul style="list-style-type: none"> <li>Voter receives the smart card and inserts it into the AccuVote-TSX, which presents the correct ballot for the voter.</li> <li>Voter votes the ballot. The AccuVote-TSX prevents the voter from over-voting, notifies of under-voting, and presents the ballot choices for review as appropriate.</li> </ul>	

Continued on the next page

**Work Flow/Process Model (continued)**

Inputs	Outputs
<b>Poll Workers</b>	
Poll worker receives the smart card from the voter after the voter casts the ballot.	<ul style="list-style-type: none"> <li>• Poll workers print result tapes from the AccuVote-TSX.</li> <li>• Poll workers post one result tape at the precinct.</li> <li>• Poll workers remove the PCMCIA card and send the card and a copy of the result tape to the BOE.</li> </ul>
<b>Board of Elections</b>	
	<ul style="list-style-type: none"> <li>• BOE places PCMCIA card from the AccuVote-TSX into an AccuVote-TSX that is serving as a media reader, and the GEMS tally software counts the votes.</li> <li>• The BOE prints and releases the results.</li> </ul>

## Environment

### Hardware Configuration

Following is a summary of the hardware configuration of the Diebold AccuVote-TSX that was tested.

Processor Type	Processor Clock Speed	Memory	Operating System	Communications Slots	Interfaces
Hitachi SH3 Family of microprocessors	118 MHz	<ul style="list-style-type: none"> <li>• 16MB Flash ROM</li> <li>• 32MB RAM - No hard disk</li> <li>• PCMCIA card – 128MB</li> </ul>	Windows CE 4.1	<ul style="list-style-type: none"> <li>• 2 PCMCIA card slots</li> <li>• Smart card reader slot (ISO 7816)</li> <li>• Phone Jack</li> </ul>	<ul style="list-style-type: none"> <li>• Keypad, 12 key numeric through RS-232</li> <li>• (output) Audio, mini stereo</li> <li>• Touch Screen</li> </ul>

### Software Configuration

Following is a summary of the software configuration of the Diebold AccuVote-TSX that was tested.

Firmware	User Interface	Internal Storage	Communications Protocols	Security
<ul style="list-style-type: none"> <li>• Operating system is Windows CE 4.1.0</li> <li>• Boot Loader 4-16-2004</li> <li>• Ballot Station 4.5.1</li> </ul>	<ul style="list-style-type: none"> <li>• Uses a touch screen with a GUI interface with simple controls.</li> <li>• The font is Arial, and there is a minimal amount of graphics.</li> </ul>	<ul style="list-style-type: none"> <li>• Data is stored in binary flat files on the PCMCIA Card.</li> <li>• Additional fonts and audio are also stored on the Flash Memory.</li> </ul>	<ul style="list-style-type: none"> <li>• When an optional network card is inserted. Uses TCP/IP over an Ethernet connection.</li> <li>• SSL is used to encrypt data over the local network.</li> <li>• Uses IDE interface to communicate with removable storage media.</li> </ul>	<ul style="list-style-type: none"> <li>• Access is limited by smart card and PIN.</li> <li>• Smart card security keys can be modified for each election.</li> <li>• Some Contents of Removable storage media are encrypted DES.</li> </ul>

## ***Environment (continued)***

### **Network Configuration**

There is a network-based LAN/WAN port intended for communication of ballot definitions and voting results between the AccuVote-TSX and the GEMS election management software. The network functionality is provided by a removable PCMCIA network card using standard TCP/IP protocol over an Ethernet connection. Diebold has limited their firmware to only recognize a small number of PCMCIA network cards. This networking capability should be removed from the AccuVote-TSX during balloting. A locking door covers the port where the PCMCIA modem is installed during the election process.

*- From Black Box Voting Document Archive*

## Step 2: Threat Identification

A threat is the potential for a particular threat-source to successfully exercise a particular vulnerability. Vulnerability is a weakness that can be accidentally triggered or intentionally exploited. A threat-source does not present a risk when there is no vulnerability that can be exercised. In determining the likelihood of a threat, one must consider threat-sources, potential vulnerabilities (Step 3), and existing controls (Step 4).

In Step 2, the assessment team determined the potential threats posed to the AccuVote-TSX voting system. Following is a list of potential threats to which the AccuVote-TSX voting system could be exposed.

Threat-Source	Motivation	Threat Actions
Hacker, cracker	Challenge Ego Rebellion	<ul style="list-style-type: none"> <li>Hacking</li> <li>Social engineering</li> <li>System intrusion, break-ins</li> <li>Unauthorized system access</li> </ul>
Computer criminal	Destruction of information Illegal information disclosure Monetary gain Unauthorized data alteration	<ul style="list-style-type: none"> <li>Computer crime (e.g., cyber stalking)</li> <li>Fraudulent act (e.g., replay, impersonation, interception)</li> <li>Information bribery</li> <li>Spoofting</li> <li>System intrusion</li> </ul>
Terrorist	Blackmail Destruction Exploitation Revenge	<ul style="list-style-type: none"> <li>Bomb/Terrorism</li> <li>Information warfare</li> <li>System attack (e.g., distributed denial of service)</li> <li>System penetration</li> <li>System tampering</li> </ul>
Campaign and political entities	Competitive advantage Economic espionage Change outcome of election	<ul style="list-style-type: none"> <li>Economic exploitation</li> <li>Information theft</li> <li>Intrusion on personal privacy</li> <li>Social engineering</li> <li>System penetration</li> <li>Unauthorized system access (access to classified, proprietary, and/or technology-related information)</li> </ul>
Insiders (poorly trained, disgruntled, malicious, negligent, dishonest, or terminated employees)	Curiosity Ego Intelligence Monetary gain Revenge Unintentional errors and omissions (e.g., data entry error, programming error)	<ul style="list-style-type: none"> <li>Assault on an employee</li> <li>Blackmail</li> <li>Browsing of proprietary information</li> <li>Computer abuse</li> <li>Fraud and theft</li> <li>Information bribery</li> <li>Input of falsified, corrupted data</li> <li>Interception</li> <li>Malicious code (e.g., virus, logic bomb, Trojan horse)</li> <li>Sale of personal information</li> <li>System bugs</li> <li>System intrusion</li> <li>System sabotage</li> <li>Unauthorized system access</li> </ul>

## Step 3: Vulnerability Identification

The analysis of the threat to an electronic voting system must include an analysis of the vulnerabilities associated with the system environment. In Step 3, the assessment team identified vulnerabilities (flaws or weaknesses) of the system. Results from audits, tests, inspections, and an examination of the current state of the AccuVote-TSX, Key Card Tool, and Voter Card Encoder components of the Diebold voting system were used to determine existing weaknesses.

The assessment team conducted a comprehensive review of compliance to both technical and non-technical requirements to identify vulnerabilities. In addition to identifying weaknesses in the above, the team also assessed external entities and their connectivity to the AccuVote-TSX voting system.

### Requirements Tested & Test Results

This section documents the requirements that were tested, the tests conducted, and the results of each test.

#### Test Areas

Tests were conducted in the following areas.

1. Code Review Tests
2. Platform Review Tests
3. Physical Tests

#### Specific Tests and Test Results

The assessment team tested the specific scenarios listed below. For each scenario, the table lists:

- Description of the requirement tested
- Test Scenario that covered the requirement
- Test Results

No.	Requirement	Test Scenario	Test Results
<b>Code Review</b>			
<b>Standardization</b> - Naming conventions of variables, constants and modules should be consistent across the application. Construction of modules within an application should also be consistent. This is important for knowledge transfer and code maintenance.			
1.01	There shall be a standard method in the naming of functions and variables.	Perform visual review of source files for AccuVote-TSX, Key Card Tool and Voter Card Encoder. Function names will be checked for proper case formatting of concatenated words. Names of functions should clearly describe its purpose.	The Code for the AccuVote -TSX DRE has been certified as being FEC 2002 Compliant. Some functions and variables could use additional comments to help clarify their purpose.  The function and variable names are intelligible and readable. The naming convention is consistent across modules.

*Continued on the next page*

No.	Requirement	Test Scenario	Test Results
1.02	There shall be a standard method in the construction of modules.	Perform visual review of source files for AccuVote-TSX, Key Card Tool and Voter Card Encoder. Modules should contain a consistent format and location for module component TSX. Modules should begin with comments describing the modules content TSX. Location of methods and variables with associated comments should be consistent throughout.	The Code for the AccuVote-TSX DRE has been certified as being FEC 2002 Compliant. Some modules could use additional comments to help clarify their purpose. Single line descriptions were found not to be sufficient in fully explaining the module's purpose.  Code in the Voter Card Encoder module was found to have sufficient comments explaining the module purpose.
<b>Coding Conventions</b> - The application should be broken down into modules with each module performing a single function. There should be single entry and exit points within a module. There should be consistent error handling throughout the application. Naming of variables, constants and modules should be descriptive and self-explanatory.			
1.03	There shall be a standard methodology used for the construction of modules.	Perform visual review of source code for AccuVote-TSX, Key Card Tool and Voter Card Encoder. Modules should use a clear methodology of construction. Files will be reviewed to see if a coding industry standard is used in the naming of modules, functions, variables and constants.	The Code for the AccuVote-TSX DRE has been certified as being FEC 2002 Compliant. The construction of the modules is consistent across all files. Components of each module are usually easy to identify. Some files contained multiple modules, which were difficult to find, buried in the file. File names should match more closely with the enclosed modules. And multiple modules should be divided into separate files.
1.04	The naming of variables and functions shall be clear and descriptive.	Perform visual review of source code for AccuVote-TSX, Key Card Tool and Voter Card Encoder. Function and variable names should be "self documenting" as well as contain properly typed and sized attributes, and return types.	The Code for the AccuVote-TSX DRE has been certified as being FEC 2002 Compliant. Variables are appropriately named and are used throughout the source code. Some areas could use more descriptive names and comments describing their purpose.

Continued on the next page

**Requirements Tested & Test Results (continued)**

No.	Requirement	Test Scenario	Test Results
1.05	There shall be a consistent way to handle system errors.	Perform visual review of source code for AccuVote-TSX, Key Card Tool and Voter Card Encoder for implementation of error handling code. All methods should contain error-handling logic. Systems should remain stable in the event of an error. When an error occurs, sufficient information regarding the state of the system and system parameters should be recorded for future debugging.	The Code for the AccuVote-TSX DRE has been certified as being FEC 2002 Compliant. The System using C++ uses standard error handling procedures like Try/Catch as is expected. More information should be included when logging errors, Especially errors that might be the result of user errors or apparent tampering during an election. Additional information needs to be added to the audit logs and error messages. The Voter Card Encoder module is written in C and not all methods have implemented the error handling logic.
<b>Code Documentation</b> - All source code should be sufficiently commented, with clear descriptions of what is being accomplished by each module, the names of calling functions, and the inputs and outputs to the modules. Consistency should be maintained in commenting the code for ease of readability.			
1.06	The comments in the code shall be descriptive and present in the code.	Perform visual review of source code for AccuVote-TSX, Key Card Tool and Voter Card Encoder. Comments will be reviewed for simple descriptive content. Comments should appear at the beginning of each module, function. All module level variables, constants, and structures should be commented as well. Function parameters and return values should describe appropriate values. Comments should also appear in methods to help clarify complex code and logic behind expressions.	The Code for the AccuVote-TSX DRE has been certified as being FEC 2002 Compliant. Compuware would prefer that there be lengthier descriptions for classes and modules, beyond what FEC 2002 might require. In many locations the descriptions were found to be inadequate for a clear understanding of the functions purpose. Also, there were no descriptions associated with marked revisions, in the method comments
1.07	The comments shall have a consistent look in their layout.	Perform visual review of source code for AccuVote-TSX, Key Card Tool and Voter Card Encoder. Comments should have a common format with standard fields for information. Some standard fields should be a description, parameters, return types, a change log.	The Code for the AccuVote-TSX DRE has been certified as being FEC 2002 compliant. This was very consistent through out the entire source for AccuVote-TSX, Key Card Tool, and the Voter Card Encoder.

Continued on the next page

**Requirements Tested & Test Results (continued)**

No.	Requirement	Test Scenario	Test Results
1.08	The modules shall be commented describing their contents.	Perform visual review of source code for AccuVote-TSX, Key Card Tool and Voter Card Encoder. Modules should have a standard comment identifier at the beginning of each module. Module comments should contain the name and description of the module, a copyright notice, and a change log.	<p>The Code for the AccuVote-TSX DRE has been certified as being FEC 2002 Compliant. The descriptions of the modules is inadequate at times. Some Modules only have single line descriptions which clearly can not give enough detail describing the functionality of the module.</p> <p>The Voter Card Encoder has standard comments at the beginning of each function and a change log. But the log does not indicate the changes made and the reason for making them. A copyright notice is available at the beginning of modules.</p>
1.09	There shall be a close relationship of the requirements to the code modules that implement the requirements.	Perform visual review of the source code for AccuVote-TSX, Key Card Tool and Voter Card Encoder. Modules will be reviewed for their functional content. The variables and functions should be closely related and work directly to perform a clear task.	<p>The Code for the AccuVote-TSX DRE has been certified as being FEC 2002 compliant. In reviewing the code modules and the provided software requirements, for the smaller modules it was clear in the relationships of module components. For large modules, the descriptions were not sufficient for a clear understanding of the module content's. Additionally, larger modules with multiple classes should be divided further, with their file names being more representative of the class that is enclosed.</p> <p>Requirement documents, system and code design documents and technical documents were not available for Voter Card Encoder.</p>

Continued on the next page

**Requirements Tested & Test Results (continued)**

No.	Requirement	Test Scenario	Test Results
<b>Coding Complexity</b> - Code should be simple in construction. It should be easy to read and follow. Modules should perform single tasks and should have single points of entry and exit.			
1.10	The system shall be divided into modules.	The source code for AccuVote-TSX, Key Card Tool and Voter Card Encoder will be visually reviewed to verify if the code has been properly modularized. Modules should be an appropriate length and encapsulate related functionality.	<p>The Code for the AccuVote-TSX DRE has been certified as being FEC 2002 Compliant. The source code has been broken into functional areas and then further broken down into individual source modules. Some modules are very long, and their descriptions are not sufficiently informative. There are compound modules containing multiple classes, which should be separated into individual files.</p> <p>The Voter Card Encoder code was found to be properly modularized.</p>
1.11	The source code shall use simple logic structures.	The source code for AccuVote-TSX, Key Card Tool and Voter Card Encoder will be visually reviewed for the use of simple and clear logical structures. There should be the use of constants (consts) and data structures (structs) to improve code readability and reliability.	<p>The Code for the AccuVote-TSX DRE has been certified as being FEC 2002 Compliant. The source code does have a lot of use of simple data structure constructs. Some custom defined constructs could use more descriptions as to their purpose and construction. This applies also to "pound defines". Variables are passed around by reference for efficiency in memory usage and system speed. Because of the FEC 2002 compliance the variable names have improved and are clearer in complex sections. There is the appearance of some hard coded default values. It would be helpful for more details on why these defaults are there and when and how they are changed.</p>

Continued on the next page

**Requirements Tested & Test Results (continued)**

No.	Requirement	Test Scenario	Test Results
1.12	The source code shall have an appropriate size of modules and the number of functions performed by them.	The source code for AccuVote-TSX, Key Card Tool and Voter Card Encoder will be visually reviewed to verify if the code has been properly modularized. Modules should encapsulate related functionality into logical groupings with clear interfaces. Interfaces should be well defined as to their use.	<p>The Code for the AccuVote-TSX DRE has been certified as being FEC 2002 Compliant. Some of the modules are quite large and appear to contain critical areas of functionality where considerable processing is required. Single line descriptions should be improved to more clearly describe the functionality of functions and their purpose in the large modules. There are compound modules containing multiple classes, which should be separated into individual files.</p> <p>The modules in Voter Card Encoder were found to be of appropriate size.</p>
<b>Classes / Modules</b> - Use of classes / modules can make the code smaller and reusable.			
1.13	There shall be the existence of classes and modules.	The source code for AccuVote-TSX, Key Card Tool and Voter Card Encoder will be visually reviewed to verify implementation of classes and proper modularization of the source files.	<p>The Code for the AccuVote-TSX DRE has been certified as being FEC 2002 Compliant. It was difficult at times to find the necessary functionality to review and test for security purposes. Longer descriptions would have been more helpful, and having modules clearly marking key components would have been helpful.</p> <p>The Voter Card Encoder is written in C. It has proper modularization and implementation of functions.</p>

*Continued on the next page*

**Requirements Tested & Test Results (continued)**

No.	Requirement	Test Scenario	Test Results
1.14	The functions performed by the classes shall be self-contained where appropriate.	The source code for AccuVote-TSX, Key Card Tool and Voter Card Encoder will be visually reviewed. The name and description of the class should be simple and clear. The task performed by the function should be easy to understand, simple to define, and atomic.	<p>The Code for the AccuVote-TSX DRE has been certified as being FEC 2002 Compliant. The C++ source code has an appropriate use of encapsulation and interfaces. The use of access qualifiers are appropriate and makes interfaces clear, and to understand how to use the modules.</p> <p>Some functions are only called by the Windows CE operating system, or enclosed framework. When these are noted in the comments, it would be helpful for additional explanations on when those functions would be called.</p> <p>The function names are intelligible and readable in the Voter Card Encoder system.</p>
<p><b>Third Party Components</b> - Use of third party components requires strict guidelines, security standards and version control. Attention will be paid to controls around third party components used in the applications.</p>			
1.15	Any use of third party components in the firmware shall be inspected.	The source code for AccuVote-TSX, Key Card Tool and Voter Card Encoder will be visually reviewed to find any use of third party products. The makers and the versions of any found third party applications will be noted.	<p>There is use of several third party components. Audio playback is from an open source library named Fmod. The version used is not known. Access of the external flash memory is from FlashFx from the Datalight Corporation. Both of these are used as packages and the source code was not available. Additional third party packages include OpenSSL functionality and the Windows CE operating system. There are apparent additional references to other packages which we were not able to investigate in our evaluation.</p> <p>The Voter Card Encoder uses the SDK from Spyrus who are the manufacturers of the Voter Card Encoder unit.</p>

Continued on the next page

**Requirements Tested & Test Results (continued)**

No.	Requirement	Test Scenario	Test Results
1.16	Any third party components shall be secure and not create a risk.	If the source is available for any used third party products, the source will be reviewed for client modifications. Third party source code should only contain the necessary functionality with unused areas removed or disabled. If the source is not available then further study will be required.	Diebold receives executable third party packages. Updates come from the owner of the source code. In the case of Fmod and OpenSSL, it is an open source package where the source code is freely available to anyone. Additionally there were references to other files that did not appear to be logical as to the purpose of their inclusion. Third party source code and libraries needed for a given version are placed under Diebold's version control system.
<b>Database Review</b> - Database integrity and data security is vital for correct data reporting. The code review will include the following:			
1.17	The database shall be well designed.	The data model and database source code for AccuVote-TSX, Key Card Tool and Voter Card Encoder will be reviewed for existence of proper keys and normalization.	The internal storage system for the TSX and Voter Card Encoder do not use a relational database, therefore there are no relational keys or normalization. The ballot definitions and the votes themselves are stored into binary flat files.
1.18	The data in the database shall be secure.	The source code for AccuVote-TSX, Key Card Tool and Voter Card Encoder will be visually reviewed for user access levels and roles implemented as part of security.	The files containing the votes and the Audit log is encrypted with DES. The contents of the card including the ballot definitions, sound files, and card labels were not found to be encrypted. There was no additional security found on the removable media to prevent access or to change contents. The Voter Card Encoder does not encrypt the data on the smart cards. One needs a supervisor card to clear the contents of the VCE unit and then load it with information from master voter cards. The Voter Card Encoded does not use a relational database.

Continued on the next page

**Requirements Tested & Test Results (continued)**

No.	Requirement	Test Scenario	Test Results
<b>Data Integrity</b> - Review the internal data storage of the system using the following criteria:			
1.19	There shall be ways to verify the correctness of system data.	Source code for AccuVote-TSX, Key Card Tool and Voter Card Encoder will be reviewed and tested in order to check for CRC techniques in verifying the correctness of data that is stored in memory. Can the software identify data that has been improperly modified?	<p>The ballots and card contents do use a checksum value that is calculated when the data is created. Checksums are verified at loading time of new election storage media. CRC16 is used to checksum voter ballots and the audit log. A larger set of data like the text of a ballot uses CRC32. CRC16 has a data size limitation and should not be used for data over 4KB. It was unclear in our testing if anything over 4KB would be check summed with CRC16 but from a visual inspection into the data types their size appears to be fine.</p> <p>The Voter Card Encoder uses CRC16 algorithm to check the correctness of data while reading, writing and clearing the voter cards.</p>
1.20	There shall not be any means by which a voter can be identified.	The source code for AccuVote-TSX, Key Card Tool and Voter Card Encoder will be reviewed to make sure that an algorithm is implemented to make sure voter records are stored in random order. The Cast Vote Records should not have time stamp associated with it.	<p>The votes are check summed with CRC16, and a random serial number is generated during storage of a completed ballot. The ballot is stored sequentially in memory, and on the removable flash card.</p> <p>When the ballot is written it is also encrypted with DES.</p> <p>The Voter card encoder does not store the cast ballots and it does not have any information by which a voter can be identified.</p>

*Continued on the next page*

**Requirements Tested & Test Results (continued)**

No.	Requirement	Test Scenario	Test Results
1.21	The system shall be secure and prevent any access other than from authorized voters or supervisors.	The source code for AccuVote-TSX, Key Card Tool and Voter Card Encoder will be reviewed to verify the system is secure and allows each voter to only vote once by issuing unique access codes.	A voter card controls voter access. The voter card is a smart card issued only from Diebold. Voter cards are activated by using the Voter Card Encoder, which allows the AccuVote-TSX to display the correct ballot for the voter. Immediately after voting the card is disabled by changing a flag and is ejected from the DRE. The voter is to return the card to the poll workers. Knowing the security key is required to access the voter card. Voter cards are keyed to an election and can not be used for any other elections. Supervisory passwords can be up to 10 digits long, and are only good for the election they are created for.
1.22	There shall be a system to protect and back up data in the event of a disaster.	The source code for AccuVote-TSX, Key Card Tool and Voter Card Encoder will be reviewed to verify there is a means by which votes can be recovered in case of a system disaster.	All results are stored on the removable flash memory. Additionally the results are stored on an internal memory that can be retrieved if needed. There does exist error handling and backup that allows votes to be recovered from a machine if the removable media is lost or damaged.
<b>Encryption Standards</b> - Review of encryption standards used in the DREs and the supporting software will be a point of primary focus while the source code is being reviewed.			
1.23	There shall be a strong method of encryption used.	The strength of encryption will be reviewed. The types of encryption will be reviewed to see if it is sufficient.	Diebold stores ballots, audio, audit logs and Cast Vote Records on the PCMCIA removable media. The Cast Vote Records and the Audit Log is encrypted with a DES encryption package.  The Voter card encoder does not implement any encryption.

*Continued on the next page*

**Requirements Tested & Test Results (continued)**

No.	Requirement	Test Scenario	Test Results
1.24	The data shall be encrypted including "ballot definitions" and other data on the DREs.	Ballot Definitions and Cast Vote Records should be protected and be verifiable they are correct. Encryption should be powerful enough to block access to stored data.	Diebold stores ballots, audio, audit logs and Cast Vote Records on the PCMCIA removable media. The Cast Vote Records and the Audit Logs are encrypted with a DES encryption package. There is no protection that prevents access to the file system of the removable media card.
1.25	There shall be the use of cryptographic operations during voter authorization.	Various means of "voter identification" should be secure. The data on a voter authorization token should not be discernable.	Voter Smart cards are used to allow access to an AccuVote-TSX. Voter cards are keyed to an election and can only be used for the current election. The contents of a voter card are encrypted with DES and could not be retrieved without knowing the proper keys
1.26	There shall be the use of encryption keys protecting types of removable media. Those keys shall be protected during the transportation of Ballot Definitions and Voting Records.	Encryption keys should be randomly generated every time and sufficiently long so that it is not easy to guess. The key its self should be kept private and not easily discovered.	The Key Card Tool, allows an election official to create a 64bit, user definable public key that is loaded onto all of the DRE's. It is up to the election officials to track and change the keys for every election. Though some of the files on the removable media are encrypted, access is still possible to the file system of the media. The data in the Voter Card Encoder is not encrypted. Although provision is available for the keys generated from the KCT software to be stored in the VCE unit.
1.27	Any data transmitted shall be encrypted over communication links.	Transmission protocols will be checked for the use on encryption. Data should never travel over a wire without protection. The contents of the transmission should be verifiable as to their contents and correctness. Any type of tampering should be identifiable if not impossible.	SSL is used to encrypt data transmissions over a network or a modem.  The Key Card Tool, Allows an election official to create a 64bit, user definable public key which is loaded onto all of the DRE's.

Continued on the next page

**Requirements Tested & Test Results (continued)**

No.	Requirement	Test Scenario	Test Results
1.28	The AccuVote-TSX shall not have unencrypted cast ballot records.	Check the vote records on the AccuVote-TSX, GEMS software, and transfer medium to ensure that the records are encrypted.	The Cast Vote Records on the removable flash media are encrypted using DES. SSL is used to encrypt data transmissions, over LAN or modem. The encryption Key can be made election specific via the Key Card Tool.
1.29	The AccuVote-TSX shall not have unencrypted audit logs.	Check the audit logs on the AccuVote-TSX to ensure that they are encrypted.	Contents of the audit logs are encrypted using DES.
1.30	The system shall not store or use passwords without encryption.	Perform code review to ensure that passwords used in all software are encrypted.	Supervisor passwords are stored on the smartcards whose contents are encrypted with DES. Passwords can be modified using the Key Card Tool by creating new supervisor cards. The Voter Card Encoder unit does not store passwords. The smart card is authenticated by verifying the card against the factory key and auth key. The cards fresh from the factory are initially identified against the hard coded factory key and these keys are replaced by the encrypted smart card key.

Continued on the next page

**Requirements Tested & Test Results (continued)**

No.	Requirement	Test Scenario	Test Results
1.31	The system shall not use hard-coded passwords.	Perform code review to ensure that the system does not use hard coded passwords.	<p>With the addition of the Key Card Tool, important keys and passwords can be set before each election. These include the Smart Card Key, The Data Key, and the Supervisor's password. The Supervisor's password can be a maximum of 10 digits. The password is stored in an encrypted form on the supervisor card. Using the Key Card Tool it is possible to create different supervisor passwords for an election. Despite the possibility of having multiple passwords there does not appear the ability to identify individual supervisor cards for security purposes.</p> <p>The Key Card Tool is capable of identifying unauthorized cards when inserted into the reader.</p> <p>The Voter card encoder unit does not store passwords. The smart card is authenticated by verifying the card against the factory key and smart card key. The value of the factory key is hard coded in the source code. The cards fresh from the factory are initially identified against the hard coded factory key and these keys are replaced by the encrypted smart card key.</p>

*Continued on the next page*

No.	Requirement	Test Scenario	Test Results
<b>Platform Review</b>			
2.01	The AccuVote-TSX shall not allow supervisor privileges to unauthorized individuals.	Utilizing the EMVCo ACS ACR80 Smart Card Terminal. 1. Attempted simple reads with generic ACR80 software. 2. Attempted to use generic ACS cards with the Diebold KCT software and hardware to generate a counterfeit election . 3. Attempted to use ACR80 hardware with KCT software to read and/or generate counterfeit election smart. 4. Attempt to convert a valid Voter smart card into a Supervisor smart card that is recognized by the AccuVote-TSX.	Recreating this test, tester was unable to upgrade a Key Card to a Supervisor card. The KCT software would not allow the operation. At present we have been unable to read or write to the Key Cards supplied by Diebold with the ACR80 Card Tool. We were unable to manufacture a counterfeit Voter smart card or to convert a Voter smart card into a Supervisor Card.
2.02	The system shall not allow unauthorized modification of the Ballot Definition file.	Try to modify the Ballot Definition file on the PCMCIA card before loading it on the AccuVote-TSX. Try to modify the card using a simple laptop and then insert it in the AccuVote-TSX.	File would not load from the PCMCIA card. The system warned of a bad file and would not load the files from the card. The AccuVote-TSX recognized that the files were changed on something other than the AccuVote-TSX or voting software.
2.03	The AccuVote-TSX shall not allow the installation and/or execution of an unauthorized program.	Install a program on a PCMCIA card, insert it in the AccuVote-TSX, and install and/or execute the unauthorized program.	The system would not load an executable file by itself, and attempts to use the Win CE to find the file on the PCMCIA card were unsuccessful.
2.04	The system shall not allow for security breaches via the internet.	Inspect the AccuVote-TSX for network accessible ports.	The AccuVote-TSX connects to the network through a PCMCIA network card with Windows CE TCP/IP protocols. This is the normal port for loading ballot definitions and uploading cast ballot records.
2.05	The system shall not allow for security breaches via the internet.	Try to access, modify, or disrupt the functioning of the AccuVote-TSX software while connected to a network.	Attempts were made to connect to the AccuVote-TSX from the GEMS server. FTP Connections were refused by the AccuVote-TSX. This was also attempted from a laptop computer attached to the network with similar results.

Continued on the next page

**Requirements Tested & Test Results (continued)**

No.	Requirement	Test Scenario	Test Results
2.06	The AccuVote-TSX shall be resistant to tampering, lock up, intrusion or vandalism.	Try to bring the system down, lock up the operating system, change or erase log files, or any other form of Denial of Service (DoS), Distributed Denial of Service (DDos), or other result which benefits the attacker.	Keyboard port has been removed. At present time there is no way to accomplish this test.
2.07	The AccuVote-TSX shall not allow supervisor privileges to unauthorized individuals	<p>Utilizing the EMVCo ACS ACR80 Smart Card Terminal. Tests were performed to change a voter smart card to supervisor card.</p> <ol style="list-style-type: none"> <li>1. Attempted simple reads with generic ACR80 software.</li> <li>2. Attempted to use generic ACS cards with the Diebold KCT software and hardware to generate a counterfeit election .</li> <li>3. Attempted to use ACR80 hardware with KCT software to read and/or generate counterfeit election smart.</li> <li>4. Attempt to convert a valid Voter smart card into a Supervisor smart card that is recognized by the AccuVote-TSX.</li> </ol>	<p>Recreating this test, we were unable to upgrade a Key Card to a Supervisor card with the equipment we had available. The KCT software would not allow the operation. At present we have been unable to read or write to the Key Cards supplied by Diebold with the ACR80 Card Tool. This does not prove a working smart card cannot be counterfeited but does indicate it is not an easy task to accomplish</p> <p>There is a risk that an unauthorized person might be able to create and use a counterfeit smart card to access supervisory functions or cast extra ballots.</p>
2.08	The operating system on the AccuVote-TSX shall be hardened against unintended intrusion, operations, or forced errors.	Try to cause a kernel panic, system failure, or indefinite wait state, or other operating system lock-up within the operating system or sub-system. With the access panel open and a keyboard or keypad plugged in, multiple or simultaneous keystrokes hit or key combinations pressed simultaneously was the main method of attack.	<p>No attempts could be made while the cover was locked.</p> <p>When the cover was open, ports were available but we were unable to produce any kernel panics, wait states, or other operating system lock-ups, freezes, or general protection faults or invalid page faults in the AccuVote-TSX.</p>
2.09	The system shall password protect supervisor functions.	Observe that functions are password protected, the minimum length of passwords, and that they can be changed.	The supervisor functions are password protected. Diebold has corrected the issue of a hard-coded four digit PIN. The PIN is assignable at Ballot creation and can be any length between 0 and 10 digits.

Continued on the next page

**Requirements Tested & Test Results (continued)**

No.	Requirement	Test Scenario	Test Results
2.10	The system shall not allow corruption of the O/S, application program, ballot definition, or voter data.	Try to create an attack on flash memory using files loaded on the PCMCIA card.	File would not load from the PCMCIA card. The system warned of a bad file and would not load the files from the card. The AccuVote-TSX recognized that the files were changed on something other than the AccuVote-TSX or voting software.
2.11	The system shall not allow undetected tampering with or modification to the contents of removable media.	Change the contents on a removable media card and use the card. Determine if the system reports the card has been modified.	When the clear text parts of a binary file were changed, the system recognized it as a bad file and would not load it onto the AccuVote-TSX.
2.12	The AccuVote-TSX shall maintain a protective counter of the total number of votes cast in all elections.	Try to modify protective counter.	There was no way to access the protective counter through ports, PCMCIA card or Supervisor smart card via telnet, FTP, voter card changes, or additions to the PCMCIA card to change the protective counter.
2.13	The AccuVote-TSX shall not allow "Man-in-the-middle" attacks when communicating between the Election Management Software and the AccuVote-TSX.	Examine the hardware and communication architecture to determine if TCP hijacking attacks are possible.	The AccuVote-TSX is not on a network and uses a direct connection to the management software within a few feet.
2.14	The AccuVote-TSX shall protect all COM ports from intrusions or vulnerabilities.	Try to gain access via an open TCP/UDP or serial or USB or other port.	An Nmap scan revealed the following ports/services were filtered: 21/tcp-ftp, 389/tcp-ldap, 1720/tcp-H.323/Q.931 (where H.323 is the teleconferencing protocol for voice/data/video IP telephony). Filtered ports are usually covered by a firewall, filter or other device. The following ports are also open (where an open port is defined as "will accept connections on that port"): 21/tcp-ftp, 25/tcp-smtp, 110/tcp-pop3, 389/tcp-ldap, 1002/tcp-unknown, 1720/tcp-H.323/Q.931 (Q.931 is an ISDN connection control protocol). AccuVote-TSX refused an FTP connection on port 21.
2.15	The AccuVote-TSX shall be resistant to introduction of Trojans, viruses, or any other form of malware.	Try to introduce any type of malicious software (malware) into the system.	Putting a program on a PCMCIA card did not work since the system would not load it. Attempts to load a program through an open port were unsuccessful.

Continued on the next page

**Requirements Tested & Test Results (continued)**

No.	Requirement	Test Scenario	Test Results
2.16	The system shall have a programmable memory device that is sealed in the unit with means of tamper detection.	Inspect the hardware design documents and physical hardware.	The system was sealed shut with no access to the flash memory. When the PCMCIA card slot is locked, there is no way to access it without the key. Same findings as initial assessment. Other than the physical damage caused by attempting to circumvent the lock, there is no passive tamper detection system.
2.17	The system shall provide for safeguards against and evidence of tampering, theft or damage of the system and units.	Inspect the physical hardware for location of seals and locks and for safeguards against and evidence of tampering.	The inspection of the AccuVote-TSX concurs with the findings of the initial assessment. The only difference would be that the Case Assembly screws and the PCMCIA card port access slots need a passive tamper-evident seals. The AccuVote-TSX is a man-portable unit (it will fit in a large briefcase) and theft control would have to be procedural and an access.
2.18	In the event of the failure of a unit, the system shall retain a record of all votes cast prior to the failure	Voted on unit, then removed power. The unit was left on overnight to drain the battery. The unit was started back up and checked for correct data.	Test vote was conducted and all power was removed including the battery. After power was restored all ballot information was accessible including the vote tallies and counts.
<b>Physical Testing</b>			
3.01	There shall be a programmable memory device sealed in unit with means of tamper detection.	Check PCMCIA card to determine whether it can be removed easily and can be locked.	This is still the same setup. The power switch is in the same compartment as the PCMCIA Flash memory card with the ballot information. The PCMCIA card is housed in a lockable compartment and it cannot be removed when locked.
3.02	Poll opening reports should have all system audit information required	Conduct logic and accuracy tests and verify system audit information is present.	Accuracy and logic tests were conducted before the election. System audit information is displayed on the resulting print out.
3.03	The system shall store logic and accuracy test results in memory of the main unit processor and Election Day device	Conduct logic and accuracy test and verify results are recorded in the on-board memory by printing the audit log.	Accuracy and logic tests were conducted before the election to verify system information was correct. Logic and accuracy test result were printed in the audit log.

Continued on the next page

**Requirements Tested & Test Results (continued)**

No.	Requirement	Test Scenario	Test Results
3.04	The system shall provide logic and accuracy tests in the memory of the main processor and the programmable memory device used on Election Day, including zero printouts before each election and a precinct tally printout at the close of each election	Conduct logic and accuracy testing before election is started. Print a zero tape before an election and a result tape after an election.	Accuracy and logic tests were conducted before the election to verify counters are working properly and the programming for each voting device is correct. A zero tape printout was created and verified that no votes were cast before the start of the election. After voting was closed, a result tape was printed.
3.05	The system shall control logic and data processing methods to detect errors and provide correction method.	Create an instance where a known error will occur on the AccuVote-TSX. For instance, enter a voter card after it has been de-activated.	AccuVote-TSX displays a concise error message. This is standard throughout all error handling functions on the AccuVote-TSX.
3.06	The AccuVote-TSX shall provide a mechanism for executing test procedures which validate the correctness of election programming for each voting device and polling place and insure that the ballot display corresponds with the installed election program.	Conduct a logic and accuracy test.	The AccuVote-TSX contains a Test Mode separate from the Election Mode to verify function and Ballot accuracy.  Accuracy and logic tests were conducted before the election to verify counters are working properly and the programming for each voting device is correct.
3.07	The EMS software shall not allow unauthorized modification of the Ballot Definition data.	Try to modify the Ballot Definition in the GEMS software using a database viewer/program.	<b>This is still an issue.</b>  We were capable of viewing the ballot definition file through Microsoft Access. Changes could be made to the database and all records can be viewed. The audit log is also stored in the database and could be viewed and edited.
3.08	The system shall present the ballot to the voter in a clear and unambiguous manner.	Create an election ballot definition file and transfer the file to the AccuVote-TSX. Open election and look at ballot.	The ballot is presented in a clear and unambiguous manner.

Continued on the next page

**Requirements Tested & Test Results (continued)**

No.	Requirement	Test Scenario	Test Results
3.09	The AccuVote-TSX shall not allow voters to vote multiple times.	<p>Utilizing the EMVCo ACS ACR80 Smart Card Terminal Tester insert a counterfeit smart card into the AccuVote-TSX and try to use it to vote.</p> <ol style="list-style-type: none"> <li>1. Attempted simple reads with generic ACR80 software.</li> <li>2. Attempted to use generic ACS cards with the Diebold KCT software and hardware to generate a counterfeit election .</li> <li>3. Attempted to use ACR80 hardware with KCT software to read and/or generate counterfeit election smart.</li> <li>4. Attempt to convert a valid Voter smart card into a Supervisor smart card that is recognized by the AccuVote-TSX.</li> </ol>	Unable to produce a working counterfeit smart card.
3.10	The AccuVote-TSX shall not allow voters to vote multiple times.	<p>Utilizing the EMVCo ACS ACR80 Smart Card Terminal Tester inserted an authorized smart card into the AccuVote-TSX and try to use it to vote multiple times.</p> <ol style="list-style-type: none"> <li>1. Attempted simple reads with generic ACR80 software.</li> <li>2. Attempted to use generic ACS cards with the Diebold KCT software and hardware to generate a counterfeit election .</li> <li>3. Attempted to use ACR80 hardware with KCT software to read and/or generate counterfeit election smart.</li> <li>4. Attempt to convert a valid Voter smart card into a Supervisor smart card that is recognized by the AccuVote-TSX.</li> </ol>	Once a vote has been cast, the smart card used is deactivated. When trying to insert the deactivated smart card to vote again, the card is ejected from the reader.

Continued on the next page

**Requirements Tested & Test Results (continued)**

No.	Requirement	Test Scenario	Test Results
3.11	The system shall not allow voting access to unauthorized persons.	<p>Create a counterfeit Voter Access smart card then attempt to use it so it is recognized and authenticated by the AccuVote-TSX.</p> <ol style="list-style-type: none"> <li>1..Attempted simple reads with generic ACR80 software.</li> <li>2. Attempted to use generic ACS cards with the Diebold KCT software and hardware to generate a counterfeit election .</li> <li>3. Attempted to use ACR80 hardware with KCT software to read and/or generate counterfeit election smart.</li> <li>4. Attempt to convert a valid Voter smart card into a Supervisor smart card that is recognized by the AccuVote-TSX.</li> </ol>	<p>In recreating this test, we were unable to upgrade a Key Card to a Supervisor card. The KCT software would not allow the operation. At present we have been unable to read or write to the Key Cards supplied by Diebold with the ACR80 Card Tool.</p>
3.12	The AccuVote-TSX shall not allow viewing or changing vote results during the election process.	Insert a supervisor card in the AccuVote-TSX and try to view or change vote results.	The supervisor menu does not allow a user to change or view vote results. Results can only be viewed and/or printed after election has been closed.
3.13	The AccuVote-TSX shall not allow the accidental or unauthorized closing of the election.	Insert a Supervisor Card in the AccuVote-TSX and try to terminate the election early.	<p>With the use of a supervisor card and the correct PIN number, we were able to close the election early.</p> <p>Inserted the supervisor card, entered the four-digit pin, and the AccuVote-TSX prompted, "Do you want to close the polls? Yes/No".</p> <p>This is a function of the supervisor and a conscious decision must be made to do this. The AccuVote-TSX also warns that no further voting is allowed for this election</p>

Continued on the next page

**Requirements Tested & Test Results (continued)**

No.	Requirement	Test Scenario	Test Results
3.14	The AccuVote-TSX shall not allow the accidental or unauthorized reset of the AccuVote-TSX.	Insert a Supervisor card in the AccuVote-TSX and try to reset the AccuVote-TSX.	The AccuVote-TSX cannot be reset during voting. Once voting is closed, the AccuVote-TSX can be reset with a supervisor card and the correct PIN number. Resetting clears the memory on the AccuVote-TSX and can clear the PCMCIA card as well. This is a function of the supervisor and a conscious decision must be made to reset the machine.
3.15	The AccuVote-TSX shall not allow the use of an unauthorized PIN to access supervisor functions.	Insert an authorized supervisor card in the AccuVote-TSX and try to access supervisor functions using an incorrect PIN.	The error functionality is the same as the first assessment. The AccuVote-TSX will display an error message and prompt the user to reenter a valid PIN code. The single default PIN code has been changed to accept a user defined PIN code that is established on the GEMS Server and will accept PIN codes from 0 to 10 digits long. User is denied access when using an incorrect PIN. An error message is clearly displayed to the user.
3.16	The AccuVote-TSX shall not lose voter information, vote count, Ballot Definition information, etc. due to a power outage during the election.	Start voting on the AccuVote-TSX, and then disconnect batteries/power for 30 minutes to simulate a power outage, Resume power and start up the AccuVote-TSX, and check the voter information.	Removed the AccuVote-TSX from the voting stand, which removed AC Power from the unit. The battery was then removed from the AccuVote-TSX without powering down. Battery was replaced in the unit and power restored. After the AccuVote-TSX was rebooted, it was verified that no ballot information or vote tallies were lost.
3.17	The AccuVote-TSX shall not lose voter information, vote count, Ballot Definition information, etc. due to a power outage during the election.	Start voting on the AccuVote-TSX, and then disconnect power for thirty minutes to simulate a power outage, and then resume power. Cast votes before, during, and after the disruption.	17a) Removed power cord and AccuVote-TSX voting machine has a battery backup that powered the machine. The battery is sealed within the machine and could not be removed. 17b) Removed the AccuVote-TSX from the voting stand, which removed AC Power from the unit. The battery was then removed from the AccuVote-TSX and without powering down. Battery was replaced in unit and power restored. After the AccuVote-TSX was rebooted, it was verified that no ballot information or vote tallies were lost.

Continued on the next page

**Requirements Tested & Test Results (continued)**

No.	Requirement	Test Scenario	Test Results
3.18	The AccuVote-TSX shall not allow for modification of the “protective counter” which tracks the total number of votes cast on the machine.	Try to modify the protective counter on the AccuVote-TSX.	The Counter was not able to be accessed or changed. Supervisor functions will not allow the altering of counts on the AccuVote-TSX voting machine. Counter is stored within the CPU on the AccuVote-TSX. The number on the counter is printed out before the election and after the election as well.
3.19	The AccuVote-TSX shall not allow modification that forces it to use the same storage device for all of the data.	Modify the AccuVote-TSX so that only core flash memory is available and see if the system will allow voting.	The AccuVote-TSX will not boot into Election Mode without the PCMCIA Flash Memory card being installed. User is prompted to turn off machine or insert memory card. The system will not allow only one memory source.
3.20	The system shall not allow supervisor access to unauthorized persons.	Try to convert a Voter Access card to a Supervisor card then access and perform supervisor functions in the AccuVote-TSX.  1. Attempted simple reads with generic ACR80 software.  2. Attempted to use generic ACS cards with the Diebold KCT software and hardware to generate a counterfeit election .  3. Attempted to use ACR80 hardware with KCT software to read and/or generate counterfeit election smart.  4. Attempt to convert a valid Voter smart card into a Supervisor smart card that is recognized by the AccuVote-TSX.	Unable to convert a Voter Access card to a Supervisor card.
3.21	The audit logs shall record all instances of supervisor access to the AccuVote-TSX.	Review audit log after completing successful vote test and ensure each step that used supervisor access is correctly logged.	Each time a supervisor card is used, the action is logged within the audit logs specific to the AccuVote-TSX.

Continued on the next page

**Requirements Tested & Test Results (continued)**

No.	Requirement	Test Scenario	Test Results
3.22	<p>The system audit log shall contain sufficient information to allow the auditing of all operations related to central site ballot tabulation, results consolidation, and report generation. It shall include a/an</p> <ul style="list-style-type: none"> <li>• Identification of the program and version being run</li> <li>• Identification of the election file being used</li> <li>• Record of all options entered by the operator</li> <li>• Record of all actions performed by the subsystem</li> <li>• Record of all tabulation and consolidation input</li> </ul>	Print a copy of the audit log and verify all items are recorded.	Audit logs printed and all information listed in requirement was printed and verified.
3.23	The system audit log must be created and maintained by the system in the sequence in which operations were performed.	Review audit log after completing successful vote test and ensure each step that used supervisor access is correctly sequenced.	The audit log is generated in sequential order and each transaction within the audit log is time stamped.
3.24	The system audit log must be created and maintained by the system in the sequence in which operations were performed.	Print a copy of the audit log and verify all steps are recorded sequentially.	All steps in the audit log are recorded sequentially.
3.25	The system shall provide for safeguards against and evidence of tampering, theft or damage of the system and units.	Review audit logs to verify any act will be recorded and logged with a timestamp.	All actions to the AccuVote-TSX are recorded in the audit log with a time stamp. This includes opening and closing the polls, voting, inserting invalid voting cards, loss of power, and supervisor access.
3.26	The media/medium in which vote counts are transferred to the Tally software shall not allow modification of the vote count.	Try to access and modify the vote count on the PCMCIA media or medium (telephone line, etc.) before the vote count is loaded into the GEMS software.	We were unable to alter vote counts on the PCMCIA card, which stores the data. The data is stored in a binary format and it was difficult to read vote records and counts. It was possible to change the data on the PCMCIA card but the AccuVote-TSX would not recognize the modified card as valid for the election.

Continued on the next page

**Requirements Tested & Test Results (continued)**

No.	Requirement	Test Scenario	Test Results
3.27	The system shall ensure that a voter's exact voting record cannot be traced back to the voter.	Try to access the information needed to reconstruct a voter's exact voting record.	Individual vote records are not reported from the AccuVote-TSX or tally software. The voting records are not kept in any specific order and the voter is kept anonymous. The system will provide for provisional voting by creating a sequence to list provisional voter records.
3.28	The system shall prevent modification of the voter's vote after the ballot is cast.	Verify vote cannot be altered once the ballot has been cast by using available supervisor functions on the AccuVote-TSX.	User cannot alter vote ballots cast. There is no supervisor function to allow for the votes cast to be altered.
3.29	The system shall protect the secrecy of the vote such that the vote may not be observed during the voter's selection of preferences, during the casting of the ballot, and as the voted ballot is transmitted for recording on a storage device.	When the vote is being cast, others should not be allowed to view the voter's selection of preferences.	The DRE test unit supplied for evaluation has limited external privacy provisions installed. The voting stand has a plastic clam shell screen that shelters the DRE. The Touch screen provides some additional privacy while voting because the LCD Screen characteristics degrade the video when viewed from an angle. Current software functionality concurs with the first assessment report.
3.30	The system shall prohibit voted ballots from being accessed by anyone until after the close of polls.	Verify reports can only be executed after the polls have been closed.	Supervisor functions to print reports are not available until the polls are closed. Reports can only be created after polls have closed.
3.31	The system shall provide that each voter's ballot is secret and the voter cannot be identified by image, code or other methods.	Conduct a mock election and cast votes. Close the election and print out a record of each individual vote cast.	Individual vote records are not reports created from the AccuVote-TSX. The voting records are listed in no specific order and the voter is kept anonymous. Provisional voting is handled differently. Voter records can be re-constructed to verify if the vote cast is allowed or not allowed. This function is performed on GEMS.

Continued on the next page

**Requirements Tested & Test Results (continued)**

No.	Requirement	Test Scenario	Test Results
3.32	The system shall provide a summary screen at the end of the ballot showing what the voter has chosen prior to the final vote being cast.	Vote for all issues and/or candidates and before casting the ballot, verify a summary of all votes is presented.	A summary of all votes for each race for the particular user is displayed before we can cast the ballot. Corrections to any race can be made at this point.
3.33	The AccuVote-TSX shall not allow unauthorized modification to its operating system.	Try to modify the operating system on the AccuVote-TSX by loading a new operating system off the PCMCIA card.	Attempted to load a counterfeit program using the PCMCIA card. Error message was clearly presented to user stating the program cannot be loaded. Error message was generated based on a CRC check of files on the PCMCIA card.
3.34	The DRE shall not allow printing of summary reports before the sequence of events required for closing of the polls are completed.	As a Supervisor, print reports before closing the election.	The DRE will not allow any reports to be created or printed until the election has been closed using a supervisor card.
3.35	There shall be no loss of data during generation of reports including results, images and inaccurate vote counts.	Print out reports after election has been closed and verify no inaccuracies exist.	Printed election reports after the close of the election and verified no results were lost during this function.
3.36	<p>The system shall provide printed records regarding the opening and closing of the polls and include the following:</p> <ul style="list-style-type: none"> <li>• Identification of election, including opening and closing date and times</li> <li>• Identification of each unit</li> <li>• Identification of ballot format</li> <li>• Identification of candidate and/or issue, verifying zero start</li> <li>• Identification of all ballot fields and all special voting options</li> <li>• Summary report of votes cast for each device, or ability to extract same</li> </ul>	Close the election and print out a copy of the audit log and review all transactions.	All transactions are captured on the audit logs including specific information about the AccuVote-TSX, definition of the election, and all actions occurring on the AccuVote-TSX during the election. All items identified in this requirement are present.

Continued on the next page

**Requirements Tested & Test Results (continued)**

No.	Requirement	Test Scenario	Test Results
3.37	The system shall produce a paper audit trail. To guard against fraud, systems shall not produce individual paper records that voters could remove from the polling place.	Complete and close an election and print out a copy of the audit log from a specific AccuVote-TSX.	An audit log is printed out using a specific supervisor function. The audit log produces a report that is a paper trail to guard against fraud.
3.38	The system shall provide printout results containing candidates and/or issues in an alphanumeric format next to the vote totals.	Conduct a mock election and cast multiple votes. Once the voting is closed, print out results of the election using the supervisor functions.	Supervisor must close election and select the option to print votes cast. The printout presents the votes cast in a summary format.
3.39	The system shall allow for extraction of data from memory devices to a central host.	Close the election and transfer results to tally software (GEMS). This is done by connecting the AccuVote-TSX to the Tally software through a network connection using a PCMCIA PC adapter card.	Results of ballots cast transferred to GEMS (tally software) with no problems.
3.40	The Tally software shall not allow the double counting of votes from a precinct or AccuVote-TSX.	Upload election results from an AccuVote-TSX to the tally software. Upload them a second time.	We tried to upload the same results twice to GEMS software. An error message is presented stating the results have already been uploaded.
3.41	The Tally software shall not allow modification of the vote count.	Try to modify the vote tally in the GEMS software using a tool such as MS Excel or MS Access.	Tester was able to modify vote counts and ballot information using MS Access on a separate machine. Databases are not password protected or encrypted and thus are accessible to unauthorized change.
3.42	The system shall provide for summary reports of votes cast on each voting device by extracting information from a memory device or a removable data storage device.	Conduct a mock election for two different AccuVote-TSX units (or memory devices) and verify a report can be created that list counts for each device.	Supervisor must close election and select the option to print votes cast. This can only be done when election has been closed. Once all AccuVote-TSX voting machines have closed all results are uploaded to GEMS where reports are created. Reports can be created to show results for each AccuVote-TSX.

Continued on the next page

**Requirements Tested & Test Results (continued)**

No.	Requirement	Test Scenario	Test Results
3.43	The system shall provide for easily downloading results from balloting into the final tally of votes.	Conduct a mock election and have multiple voters cast ballots. Once the election is closed, the supervisor card must be used to selection the option of transferring votes to GEMS software for tallying and reporting.	Accessed these functions using a supervisor card. The supervisor then uploaded all results of the vote from each AccuVote-TSX voting machine.
3.44	The system shall accurately report all votes cast.	Set up a mock election and cast multiple votes. Verify all votes have been included in reports created by GEMS.	All votes cast were included in counts recorded by GEMS software. All reports in GEMS accurately reflect number of votes cast on AccuVote-TSX.
3.45	The system shall provide a cumulative, canvass and precinct report of absentee voting, provisional ballot voting and Election Day voting as one total.	Verify election management software has the ability to handle provisional and absentee ballot voting.	Verified that functionality for recording absentee and provisional voting exists in the GEMS software.
3.46	The system shall provide a cumulative, canvass and precinct report of Election Day Voting as one total.	Complete an election. Print the reports from the Host computer.	Printed the reports from the GEMS software. Verified that provisional voting and absentee ballots were included.
3.47	The system shall not lose votes, corrupt media or have performance issues due to the presence of a magnetic field.	A magnet is placed on the LCD unit on the AccuVote-TSX smart card reader when voting and PCMCIA slot when recording the votes.	There was no visible degradation on the display. During voting, the magnet did not have any effect on the smart card reader. The PCMCIA card did not get corrupted because of the magnetic field and no votes were lost.

## Step 4: Controls Analysis

The Secretary of State has not been required to have a security plan in place for electronic voting systems in the past. As a result of HAVA, the requirement now exists.

Based on the findings of the initial security assessment and this re-assessment, the Secretary of State will develop a new security plan or modify the existing security plan to include risk mitigation strategies to minimize or eliminate the likelihood of threat.

## Step 5: Threat Likelihood

In Step 5, the assessment team examined the threats identified in Step 2 against each potential vulnerability, and assigned a likelihood rating. The likelihood rating indicates the probability that a potential vulnerability may be exercised, taking into account the nature of the threat, motivation and capability of the threat-source (if human), and existence and effectiveness of current controls.

Each potential vulnerability was assigned a threat likelihood rating of High, Medium, or Low. The following table lists the potential vulnerabilities identified and their likelihood rating.

Potential Vulnerability Identified	Threat Likelihood Rating
Hacking	Medium
System intrusion, break-ins -Physical	Medium
Unauthorized system access- Physical	Medium
Fraudulent act	Low
Information bribery	Low
Spoofing	Low
System intrusion	Medium
Bomb/Terrorism	Low
Information warfare	Low
System attack	Medium
System penetration	Medium
System tampering	Medium
Economic exploitation	Low
Information theft	Medium
Intrusion on personal privacy	Low
Unauthorized system access (access to classified, proprietary, and/or technology-related information)	Medium

Unauthorized system access	Medium
System sabotage	Medium
System bugs	Medium
Malicious code	Medium
Fraud and theft	Low
Input of falsified, corrupted data	Low
Interception	Low

- From Black Box Voting Document Archive -

## Step 6: Impact Analysis

In Step 6, the assessment team determined the adverse impact(s) that would likely occur if a threat-source were able to successfully exploit a vulnerability or weakness. The team followed the process below to determine the adverse impact resulting from a successful exploitation of a vulnerability:

- Determined the criticality of the electronic voting system and data to accomplishing the SOS' mission.
- Determined the probable adverse impact of a successful exploitation of a vulnerability.
- Determined the adverse impact of a security event in regard to loss or degradation of the system's integrity, availability, and confidentiality.
- Assigned a rating of High, Medium, or Low to each vulnerability to indicate the magnitude of impact resulting from a successful exploitation of the vulnerability.

The following table shows the magnitude of impact rating that was assigned to each potential vulnerability.

Potential Vulnerability Identified	Magnitude of Impact Rating
<b>Code Review</b>	
<b>Third Party Software:</b> The Diebold AccuVote-TSX is written with additional third party components. Although the third party software is included in the DRE, Diebold does not maintain the system. There is a potential risk that a security flaw in these third party products could be inadvertently introduced and exploited. In order to exploit a vulnerability it would require the attacker to be able to create, compile and include malicious files on the AccuVote-TSX when the firmware is upgraded.	Low
<b>Platform Review</b>	
Smart Card - with access to a smart card (voter-supervisor) with the proper training and understanding of the smart card, a counterfeit card can be made.	Medium
Smart Card Writer - with access to the small handheld writer, someone could use a voting card more than once while at the voting booth.	High
PCMCIA Card - the cards are not secured in any way with DES or PGP Keys to prevent attacks.	Medium
PCMCIA Card - with access to the card and proper training any unencrypted binary files on the card can be broken and changed.	Medium
<b>Physical Testing</b>	
Diebold's voting system uses the Jet database engine to run the database to store the Ballot definition, Audit logs and Tally results.	High

Potential Vulnerability Identified	Magnitude of Impact Rating
The Database has no password protection. The audit logs and the tally results can be changed utilizing MS Access or other database reader software.	
Using a supervisor smart card, one can end the elections early, reset the AccuVote-TSX, or clear the PCMCIA card.	High
PCMCIA card (which stores the ballot definition and results) could be corrupted.	Low

— From Black Box Voting Document Archive —

## Step 7: Determine Risks

The purpose of Step 7 is to assess the level of risk to the electronic voting system. In this step, the assessment team identified the risk(s), if any, arising out of each test scenario. After identifying the risks, the team assigned a risk rating for each vulnerability by combining the results of the Impact Analysis established in Step 6 with the Likelihood of Threat established in Step 5. The combination of the impact analysis and the threat likelihood versus the security controls in place were applied to a risk-level matrix to determine the resultant risk-level.

### Risks Identified

The assessment team identified the following vulnerabilities of the AccuVote-TSX voting system. For each vulnerability identified, the table lists the relevant requirement tested, test scenario, and test results which identified the vulnerability.

No.	Test Scenario	Test Result	Risk Identified
<b>Code Review</b>			
1.01	Perform visual review of source files. Function names will be checked for proper case formatting of concatenated words. Names of functions should clearly describe its purpose.	The Code for the AccuVote-TSX DRE has been certified as being FEC 2002 Compliant. Some functions and variables could use additional comments to help clarify their purpose.  The function and variable names are intelligible and readable. The naming convention is consistent across modules.	None.
1.02	Perform visual review of source files. Modules should contain a consistent format and location for module components. Modules should begin with comments describing the modules contents. Location of methods and variables with associated comments should be consistent throughout.	The Code for the AccuVote-TSX DRE has been certified as being FEC 2002 Compliant. Some modules could use additional comments to help clarify their purpose. Single line descriptions were found not to be sufficient in fully explaining the module's purpose.  Code in the Voter Card Encoder module was found to have sufficient comments explaining the module purpose.	None.

Continued on the next page

**Risks Identified (continued)**

No.	Test Scenario	Test Result	Risk Identified
1.03	Perform visual review of source code. Modules should use a clear methodology of construction. Files will be reviewed to see if a coding industry standard is used in the naming of modules, functions, variables and constants.	The Code for the AccuVote-TSX DRE has been certified as being FEC 2002 Compliant. The construction of the modules is consistent across all files. Components of each module are usually easy to identify. Some files contained multiple modules, which were difficult to find, buried in the file. File names should match more closely with the enclosed modules. And multiple modules should be divided into separate files.	None.
1.04	Perform visual review of source code. Function and variable names should be "self documenting" as well as contain properly typed and sized attributes, and return types.	The Code for the AccuVote-TSX DRE has been certified as being FEC 2002 Compliant. Variables are appropriately named and are used throughout the source code. Some areas could use more descriptive names and comments describing their purpose.	None.
1.05	Perform visual review of source code for implementation of error handling code. All methods should contain error-handling logic. Systems should remain stable in the event of an error. When an error occurs, sufficient information regarding the state of the system and system parameters should be recorded for future debugging.	The Code for the AccuVote-TSX DRE has been certified as being FEC 2002 Compliant. The System, written in C++, uses standard error handling procedures like Try/Catch as is expected. More information should be included when logging errors, Especially errors that might be the result of user errors or apparent tampering during an election. Additional information needs to be added to the audit logs and error messages.  The Voter Card Encoder module is written in C and not all methods have implemented the error handling logic.	None.

Continued on the next page

**Risks Identified (continued)**

No.	Test Scenario	Test Result	Risk Identified
1.06	Perform visual review of source code. Comments will be reviewed for simple descriptive content. Comments should appear at the beginning of each module, function. All module level variables, constants, and structures should be commented as well. Function parameters and return values should describe appropriate values. Comments should also appear in methods to help clarify complex code and logic behind expressions.	The Code for the AccuVote-TSX DRE has been certified as being FEC 2002 compliant. It would be preferable that there be lengthier descriptions for classes and modules, beyond what FEC 2002 might require. In many locations the descriptions were found to be inadequate for a clear understanding of the functions purpose. Also, there were no descriptions associated with marked revisions, in the method comments	None.
1.07	Perform visual review of source code. Comments should have a common format with standard fields for information. Some standard fields should be a description, parameters, return types, a change log.	The Code for the AccuVote-TSX DRE has been certified as being FEC 2002 Compliant. The comments are very consistent through out the entire source for AccuVote-TSX, Key Card Tool, and the Voter Card Encoder.	None.
1.08	Perform visual review of source code. Modules should have a standard comment identifier at the beginning of each module. Module comments should contain the name and description of the module, a copyright notice, and a change log.	The Code for the AccuVote-TSX DRE has been certified as being FEC 2002 Compliant The descriptions of the modules is inadequate at times. Some Modules only have single line descriptions, which clearly can not give enough detail describing the functionality of the module.  The Voter Card Encoder has standard comments at the beginning of each function and a change log. But the log does not indicate the changes made and the reason for making them. A copyright notice is available at the beginning of modules.	None.

Continued on the next page

**Risks Identified (continued)**

No.	Test Scenario	Test Result	Risk Identified
1.09	Perform visual review of the source code. Modules will be reviewed for their functional content. The variables and functions should be closely related and work directly to perform a clear task.	The Code for the AccuVote-TSX DRE has been certified as being FEC 2002 Compliant. In reviewing the code modules and the provided software requirements, for the smaller modules it was clear in the relationships of module components. For large modules, the descriptions were not sufficient for a clear understanding of the module contents. Additionally, larger modules with multiple classes should be divided further, with their file names being more representative of the class that is enclosed.  Requirement documents, system and code design documents and technical documents were not available for Voter Card Encoder.	None.
1.10	The source code will be visually reviewed to verify if the code has been properly modularized. Modules should be an appropriate length and encapsulate related functionality.	The Code for the AccuVote-TSX DRE has been certified as being FEC 2002 Compliant. The source code has been broken into functional areas and then further broken down into individual source modules. Some modules are very long, and their descriptions are not sufficiently informative. There are compound modules containing multiple classes, which should be separated into individual files.  The Voter Card Encoder code was found to be properly modularized.	None.

Continued on the next page

**Risks Identified (continued)**

No.	Test Scenario	Test Result	Risk Identified
1.11	The source code will be visually reviewed for the use of simple and clear logical structures. There should be the use of constants (consts) and data structures (structs) to improve code readability and reliability.	The Code for the AccuVote-TSX DRE has been certified as being FEC 2002 Compliant. The source code does have a lot of use of simple data structure constructs. Some custom defined constructs could use more descriptions as to their purpose and construction. This applies also to "pound defines". Variables are passed around by reference for efficiency in memory usage and system speed. Because of the FEC 2002 compliance the variable names have improved and are clearer in complex sections. There is the appearance of some hard coded default values. It would be helpful for more details on why these defaults are there and when and how they are changed.	None.
1.12	The source code will be visually reviewed to verify if the code has been properly modularized. Modules should encapsulate related functionality into logical groupings with clear interfaces. Interfaces should be well defined as to their use.	The Code for the AccuVote-TSX DRE has been certified as being FEC 2002 Compliant. Some of the modules are quite large and appear to contain critical areas of functionality where considerable processing is required. Single line descriptions should be improved to more clearly describe the functionality of functions and their purpose in the large modules. There are compound modules containing multiple classes, which should be separated into individual files.  The modules in Voter Card Encoder were found to be of appropriate size.	None.
1.13	The source code will be visually reviewed to verify implementation of classes and proper modularization of the source files.	The Code for the AccuVote-TSX DRE has been certified as being FEC 2002 Compliant. It was difficult at times to find the necessary functionality to review and test for security purposes. Longer descriptions would have been more helpful, and having modules clearly marking key components would have been helpful.  The Voter Card Encoder is written in C. It has proper modularization and implementation of functions.	None.

Continued on the next page

1.14	The source code will be visually reviewed. The name and description of the class should be simple and clear. The task performed by the function should be easy to understand, simple to define, and atomic.	<p>The Code for the AccuVote-TSX DRE has been certified as being FEC 2002 Compliant. The C++ source code has an appropriate use of encapsulation and interfaces. The use of access qualifiers are appropriate and makes interfaces clear, and to understand how to use the modules.</p> <p>Some functions are only called by the Windows CE operating system, or enclosed framework. When these are noted in the comments, it would be helpful for additional explanations on when those functions would be called. The function names are intelligible and readable in the Voter Card Encoder system.</p>	None.
1.15	The source code will be visually reviewed to find any use of third party products. The makers and the versions of any found third party applications will be noted.	<p>There is use of several third party components. Audio playback is from an open source library named Dmod. The version used is not known. Access of the external flash memory is from FlashFx from the Datalight Corporation. Both of these are used as packages and the source code was not available. Additional third party packages include an OpenSSL functionality and the Windows CE operating system. There are apparent additional references to other packages which we were not able to investigate in our evaluation.</p> <p>The Voter Card Encoder uses the SDK from Spyrus who are the manufacturers of the Voter Card Encoder unit.</p>	None.

Continued on the next page

**Risks Identified (continued)**

No.	Test Scenario	Test Result	Risk Identified
1.16	If the source is available for any used third party products, the source will be reviewed for client modifications. Third party source code should only contain the necessary functionality with unused areas removed or disabled. If the source is not available then further study will be required.	Diebold receives executable third party packages. Updates come from the owner of the source code. In the case of Fmod and OpenSSL, it is an open source package where the source code is freely available to anyone. Additionally there were references to other files that did not appear to be logical as to the purpose of their inclusion.  Third party source code and libraries needed for a given version are placed under Diebold's version control system.	The Diebold AccuVote-TSX and GEMS contain additional third party components. Although the software is included in the AccuVote-TSX, Diebold does not maintain these third party components. There is a risk that a security flaw in these third party products could be inadvertently introduced and cause disruption of the election process.  Note: In order to exploit a vulnerability it would require the attacker to be able to create, compile and include malicious files on the AccuVote-TSX when the firmware is upgraded.
1.17	The data model and database source code will be reviewed for existence of proper keys and normalization.	The internal storage system for the TSX and Voter Card Encoder do not use a relational database, therefore there are no relational keys or normalization. The ballot definitions and the votes themselves are stored into binary flat files.	None.

Continued on the next page

**Risks Identified (continued)**

No.	Test Scenario	Test Result	Risk Identified
1.18	The source code will be visually reviewed for user access levels and roles implemented as part of security.	<p>The files containing the votes and the Audit log is encrypted with DES. The Contents of the card including the ballot definitions, sound files, and card labels were not found to be encrypted. There was no additional security found on the removable media to prevent access or to change contents.</p> <p>The Voter Card Encoder does not encrypt the data on the smart cards. One needs a supervisor card to clear the contents of the VCE unit and then load it with information from master voter cards. The Voter Card Encoded does not use a relational database.</p>	None.
1.19	Source code will be reviewed and tested in order to check for CRC techniques in verifying the correctness of data that is stored in memory. Can the software identify data that has been improperly modified?	<p>The ballots and card contents do use a checksum value that is calculated when the data is created. Checksums are verified at loading time of new election storage media. CRC16 is used to checksum voter ballots and the audit log. Larger sets of data like the text of a ballot use CRC32. CRC16 has a data size limitation and should not be used for data over 4KB. It was unclear in our testing if anything over 4KB would be check summed with CRC16 but from a visual inspection of the data types their size appears to be fine.</p> <p>The Voter Card Encoder uses CRC16 algorithm to check the correctness of data while reading, writing and clearing the voter cards.</p>	None.

Continued on the next page

**Risks Identified (continued)**

No.	Test Scenario	Test Result	Risk Identified
1.20	The source code will be reviewed to make sure that an algorithm is implemented to make sure voter records are stored in random order. The Cast Vote Records should not have time stamp associated with it.	<p>The votes are check summed with CRC16, and a random serial number is generated during storage of a completed ballot. The ballot is stored sequentially in memory, and on the removable flash card.</p> <p>When the ballot is written it is also encrypted with DES.</p> <p>The Voter card encoder does not store the cast ballots and it does not have any information by which a voter can be identified.</p>	None.
1.21	The source code will be reviewed to verify the system is secure and allows each voter to only vote once by issuing unique access codes.	<p>A voter card controls voter access. The voter card is a smart card issued only from Diebold. Voter cards are activated by using the Voter Card Encoder, which allows the AccuVote-TSX to display the correct ballot for the voter. Immediately after voting the card is disabled by changing flag and is ejected from the DRE. The voter is to return the card to the poll workers. Knowing the security key is required to access the voter card. Voter cards are keyed to an election and can not be used for any other elections. Supervisory passwords can be up to 10 digits long, and are only good for the election they are created for.</p>	<p>Even though the keys and passwords can be changed, due to their long nature there is a risk that the keys could be lost or discovered if not stored in a secure place.</p> <p>The risk is now someone has to write down and securely store the codes.</p>
1.22	The source code will be reviewed to verify there is a means by which votes can be recovered in case of a system disaster.	All results are stored on the removable flash memory. Additionally the results are stored on an internal memory that can be retrieved if needed. There does exist error handling and backup that allows votes to be recovered from a machine if the removable media is lost or damaged.	None.
1.23	The strength of encryption will be reviewed. The types of encryption will be reviewed to see if it is sufficient.	<p>Diebold stores ballots, audio, audit logs and Cast Vote Records on the PCMCIA removable media. The Cast Vote Records and the Audit Log is encrypted with a DES encryption package.</p> <p>The Voter card encoder does not implement any encryption.</p>	None.

Continued on the next page

**Risks Identified (continued)**

No.	Test Scenario	Test Result	Risk Identified
1.24	Ballot Definitions and Cast Vote Records should be protected and be verifiable they are correct. Encryption should be powerful enough to block access to stored data.	Diebold stores ballots, audio, audit logs and Cast Vote Records on the PCMCIA removable media. The Cast Vote Records and the Audit Logs are encrypted with a DES encryption package. There is no protection that prevents access to the file system of the removable media card.	In this release Diebold implemented digital signature. DES encryption is used when Cast Vote Records and the audit log are stored. In our opinion there is a risk that security policy and procedures need to be implemented to protect any and all data files or audio files. There is also a security risk that access to the removable media's file system will not be protected unless policy and procedures are implemented to protect it at election time.
1.25	Various means of "voter identification" should be secure. The data on a voter authorization token should not be discernable.	Voter Smart cards are used to allow access to an AccuVote-TSX. Voter cards are keyed to an election and can only be used for the current election. The contents of a voter card are encrypted with DES and could not be retrieved without knowing the proper keys.	With the addition of the Key Card Tool, the encryption keys could be discovered. The codes can be changed, but now must be recorded and may not be stored in a secure place. The risk is now someone has to write down and securely store the codes.
1.26	Encryption keys should be randomly generated every time and sufficiently long so that it is not easy to guess. The key its self should be kept private and not easily discovered.	The Key Card Tool allows an election official to create a 64bit, user definable public key that is loaded onto all of the DRE's. It is up to the election officials to track and change the keys for every election. In this release Diebold implemented digital signature. Though some of the files on the removable media are encrypted, access is still possible to the file system of the media. The data in the Voter Card Encoder is not encrypted. Although provision is available for the keys generated from the KCT software to be stored in the VCE unit.	a) The Diebold AccuVote-TSX does use DES encryption. The DES key could be discovered. The codes can be changed, but now must be recorded and may not be stored in a secure place. The risk is now someone has to write down and securely store the codes. b) There is a risk that an unauthorized person could decrypt the contents of the removable PCMCIA card using the key if it is discovered. c) There is a risk that file-level access to the removable media is not secured.

Continued on the next page

**Risks Identified (continued)**

No.	Test Scenario	Test Result	Risk Identified
1.27	Transmission protocols will be checked for the use on encryption. Data should never travel over a wire without protection. The contents of the transmission should be verifiable as to their contents and correctness. Any type of tampering should be identifiable if not impossible.	In this release Diebold implemented digital signature. SSL is used to encrypt data transmissions over a network or a modem. The Key Card Tool allows an election official to create a 64-bit, user definable public key which is loaded onto all of the DRE's.	The Diebold AccuVote-TSX does use SSL encryption. The SSL key could be discovered. The codes can be changed, but now must be recorded and may not be stored in a secure place. The risk is now someone has to write down and securely store the codes.
1.28	Check the vote records on the AccuVote-TSX, GEMS software, and transfer medium to ensure that the records are encrypted.	The Cast Vote Records on the removable flash media are encrypted using DES. SSL is used to encrypt data transmissions, over LAN or modem. The encryption Key can be made election specific via the Key Card Tool.	Same as 1.26(a) and 1.27
1.29	Check the audit logs on the AccuVote-TSX to ensure that they are encrypted.	Contents of the audit logs are encrypted using DES.	Same as 1.26(a)
1.30	Perform code review to ensure that passwords used in all software are encrypted.	Supervisor passwords are stored on the smartcards whose contents are encrypted with DES. Passwords can be modified using the Key Card Tool by creating new supervisor cards. The Voter Card Encoder unit does not store passwords. The smart card is authenticated by verifying the card against the factory key and auth key. The cards fresh from the factory are initially identified against the hard coded factory key and these keys are replaced by the encrypted smart card key.	None.

Continued on the next page

**Risks Identified (continued)**

No.	Test Scenario	Test Result	Risk Identified
1.31	Perform code review to ensure that the system does not use hard-coded passwords.	<p>With the addition of the Key Card Tool, important keys and passwords can be set before each election. These include the Smart Card Key, The Data Key, and the Supervisor's password. The Supervisor's password can be a maximum of 10 digits. The password is stored in an encrypted form on the supervisor card. Using the Key Card Tool it is possible to create different supervisor passwords for an election. Despite the possibility of having multiple passwords there does not appear the ability to identify individual supervisor cards for security purposes.</p> <p>The Key Card Tool is capable of identifying unauthorized cards when inserted into the reader.</p> <p>The Voter card encoder unit does not store passwords. The smart card is authenticated by verifying the card against the factory key and smart card key. The value of the factory key is hard coded in the source code. The cards fresh from the factory are initially identified against the hard coded factory key and these keys are replaced by the encrypted smart card key.</p>	None
No.	Test Scenario	Test Result	Risk Identified
<b>Platform Review</b>			
2.01	Attempt to convert a valid Voter smart card into a Supervisor smart card that is recognized by the AccuVote-TSX.	<p>Recreating this test, tester was unable to upgrade a Key Card to a Supervisor card. The KCT software would not allow the operation. At present we have been unable to read or write to the Key Cards supplied by Diebold with the ACR80 Card Tool.</p> <p>We were unable to manufacture a counterfeit Voter smart card or to convert a Voter smart card into a Supervisor Card.</p>	<p>This does not prove a working smart card cannot be counterfeited but does indicate it is not an easy task to accomplish.</p> <p>There is a risk that an unauthorized person might be able to create and use a counterfeit smart card to access supervisory functions or cast extra ballots.</p>

Continued on the next page

**Risks Identified (continued)**

No.	Test Scenario	Test Result	Risk Identified
2.02	Try to modify the Ballot Definition file on the PCMCIA card before loading it on the AccuVote-TSX. Try to modify the card using a simple laptop and then insert it in the AccuVote-TSX.	File would not load from the PCMCIA card. The system warned of a bad file and would not load the files from the card. The AccuVote-TSX recognized that the files were changed on something other than the AccuVote-TSX or voting software.	There is a risk while it will not use these altered files it will also lose the ability to count any votes that are recorded prior to the files being altered by invalidating the media - Thus leading to the disruption of the election. The system actually performed in the manner it was programmed but the code should be reviewed and improved. Another risk is that an election-ready PCMCIA card might be corrupted using a laptop PC resulting in disruption of the voting process.
2.03	Install a program on a PCMCIA card, insert it in the AccuVote-TSX, and install and/or execute the unauthorized program.	The system would not load an executable file by itself, and attempts to use the Win CE to find the file on the PCMCIA card were unsuccessful.	None.
2.04	Inspect the AccuVote-TSX for network accessible ports.	The AccuVote-TSX connects to the network through a PCMCIA network card with Windows CE TCP/IP protocols. This is the normal port for loading ballot definitions and uploading cast ballot records.	None.
2.05	Try to access, modify, or disrupt the functioning of the AccuVote-TSX software while connected to a network.	Attempts were made to connect to the AccuVote-TSX from the GEMS server. FTP Connections were refused by the AccuVote-TSX. This was also attempted from a laptop computer attached to the network with similar results.	None.
2.06	Try to bring the system down, lock up the operating system, change or erase log files, or any other form of Denial of Service (DoS), Distributed Denial of Service (DDoS), or other result which benefits the attacker.	Keyboard port has been removed. At present time there is no way to accomplish this test.	None

Continued on the next page

**Risks Identified (continued)**

No.	Test Scenario	Test Result	Risk Identified
2.07	Try to gain supervisor rights or system rights by any means necessary.	Recreating this test, we were unable to upgrade a Key Card to a Supervisor card with the equipment we had available. The KCT software would not allow the operation. At present we have been unable to read or write to the Key Cards supplied by Diebold with the ACR80 Card Tool. This does not prove a working smart card cannot be counterfeited but does indicate it is not an easy task to accomplish.	There is a risk that an unauthorized person might be able to create and use a counterfeit smart card to access supervisory functions or cast extra ballots.
2.08	Try to cause a kernel panic, system failure, or indefinite wait state, or other operating system lock-up within the operating system or sub-system. With the access panel open and a keyboard or keypad plugged in, multiple or simultaneous keystrokes hit or key combinations pressed simultaneously was the main method of attack.	No attempts could be made while the cover was locked.  When the cover was open, ports were available but we were unable to produce any kernel panics, wait states, or other operating system lock-ups, freezes, or general protection faults or invalid page faults in the AccuVote-TSX.	None.
2.09	Observe that functions are password protected, the minimum length of passwords, and that they can be changed.	The supervisor functions are password protected. Diebold has corrected the issue of a hard-coded four digit PIN. The PIN is assignable by using the Key Card Tool and can be any length between 0 and 10 digits.	None.
2.10	Try to create an attack on flash memory using files loaded on the PCMCIA card.	File would not load from the PCMCIA card. The system warned of a bad file and would not load the files from the card. The AccuVote-TSX recognized that the files were changed on something other than the AccuVote-TSX or voting software.	None.

Continued on the next page

**Risks Identified (continued)**

No.	Test Scenario	Test Result	Risk Identified
2.11	Change the contents on a removable media card and use the card. Determine if the system reports the card has been modified.	When the clear text parts of a binary file were changed, the system recognized it as a bad file and would not load it onto the AccuVote-TSX.	None.
2.12	Try to modify protective counter.	. There was no way to access the protective counter through ports, PCMCIA card or Supervisor smart card via telnet, FTP, voter card changes, or additions to the PCMCIA card to change the protective counter.	None.
2.13	Examine the hardware and communication architecture to determine if TCP hijacking attacks are possible.	The AccuVote-TSX is not on a network and uses a direct connection to the management software within a few feet.	This risk should be mitigated through proper policies and procedures and only permitting the use of the networking component of the DRE in a secured isolated network. The DRE machines at voting locations will not have an Ethernet card as part of their configuration.
2.14	Try to gain access via an open TCP/UDP port.	An Nmap scan revealed the following ports/services were filtered: 21/tcp-ftp, 389/tcp-ldap, 1720/tcp-H.323/Q.931 (where H.323 is the teleconferencing protocol for voice/data/video IP telephony). Filtered ports are usually covered by a firewall, filter or other device. The following ports are also open (where an open port is defined as "will accept connections on that port"): 21/tcp-ftp, 25/tcp-smtp, 110/tcp-pop3, 389/tcp-ldap, 1002/tcp-unknown, 1720/tcp-H.323/Q.931 (Q.931 is a ISDN connection control protocol). AccuVote-TSX refused an FTP connection on port 21.	Same as 2.06 - Ports on the AccuVote-TSX are covered by a locking panel. There is a risk that if the cover is unlocked during an election, the exposed ports could be used to disrupt the AccuVote-TSX.
2.15	Try to introduce any type of malicious software (malware) into the system.	This result did not differ from the first assessment. Putting a program on a PCMCIA card did not work since the system would not load it. Attempts to load a program through an open port were unsuccessful.	None.

Continued on the next page

**Risks Identified (continued)**

No.	Test Scenario	Test Result	Risk Identified
2.16	Inspect the hardware design documents and physical hardware.	The system was sealed shut with no access to the flash memory. When the PCMCIA card slot is locked, there is no way to access it without the key. Same findings as initial assessment. Other than the physical damage caused by attempting to circumvent the lock, there is no passive tamper detection system.	None.
2.17	Inspect the physical hardware for location of seals and locks and for safeguards against and evidence of tampering.	The inspection of the AccuVote-TSX concurs with the findings of the initial assessment. The only difference would be that the Case Assembly screws and the PCMCIA card port access slots need a passive tamper-evident seals. The AccuVote-TSX is a man-portable unit (it will fit in a large briefcase) and theft control would have to be procedural and an access.	None.
2.18	Voted on unit, then removed power. The unit was left on overnight to drain the battery. The unit was started back up and checked for correct data.	Test vote was conducted and all power was removed including the battery. After power was restored all ballot information was accessible including the vote tallies and counts.	None.
<b>Physical Testing</b>			
3.01	Check PCMCIA card to determine whether it can be removed easily and can be locked.	This is still the same setup. The power switch is in the same compartment as the PCMCIA Flash memory card with the ballot information. The PCMCIA card is housed in a lockable compartment and it cannot be removed when locked.	There is a risk that the PCMCIA card can be removed if the compartment is not locked. This is still the same setup. The power switch is in the same compartment as the PCMCIA Flash memory card with the ballot information.
3.02	Conduct logic and accuracy tests and verify system audit information is present.	Accuracy and logic tests were conducted before the election. System audit information is displayed on the resulting printout.	None.

Continued on the next page

**Risks Identified (continued)**

No.	Test Scenario	Test Result	Risk Identified
3.03	Conduct logic and accuracy test and verify results are recorded in the on-board memory by printing the audit log.	Accuracy and logic tests were conducted before the election to verify system information was correct. Logic and accuracy test result were printed in the audit log.	None
3.04	Conduct logic and accuracy testing before election is started. Print a zero tape before an election and a result tape after an election.	Accuracy and logic tests were conducted before the election to verify counters are working properly and the programming for each voting device is correct. A zero tape printout was created and verified that no votes were cast before the start of the election. After voting was closed, a result tape was printed.	None.
3.05	Create an instance where a known error will occur on the AccuVote-TSX. For instance, enter a voter card after it has been de-activated.	AccuVote-TSX displays a concise error message. This is standard throughout all error handling functions on the AccuVote-TSX.	None.
3.06	Conduct a logic and accuracy test.	The AccuVote-TSX contains a Test Mode separate from the Election Mode to verify function and Ballot accuracy. Accuracy and logic tests were conducted before the election to verify counters are working properly and the programming for each voting device is correct.	None.
3.07	Try to modify the Ballot Definition in the GEMS software using a database viewer/program.	We were capable of viewing the ballot definition file through Microsoft Access. Changes could be made to the database and all records can be viewed. The audit log is also stored in the database and could be viewed and edited.	GEMS uses the MS database Jet engine to store ballot definition data and election results. Any ODBC compliant tool could view the data in the database. There is a risk that an unauthorized person with access to the GEMS server can access the database and change ballot definition files and election results.

Continued on the next page

**Risks Identified (continued)**

No.	Test Scenario	Test Result	Risk Identified
3.08	Create an election ballot definition file and transfer the file to the AccuVote-TSX. Open election and look at ballot.	The ballot is presented in a clear and unambiguous manner.	None.
3.09	Insert a counterfeit smart card into the AccuVote-TSX and try to use it to vote.	Unable to produce a working counterfeit smart card.	None.
3.10	Insert an authorized smart card into the AccuVote-TSX and try to use it to vote multiple times.	Once a vote has been cast, the smart card used is deactivated. When trying to insert the deactivated smart card to vote again, the card is ejected from the reader.	None.
3.11	Create a counterfeit Voter Access smart card then attempt to use it so it is recognized and authenticated by the AccuVote-TSX.	In recreating this test, we were unable to upgrade a Key Card to a Supervisor card. The KCT software would not allow the operation. At present we have been unable to read or write to the Key Cards supplied by Diebold with the ACR80 Card Tool.	None.
3.12	Insert a supervisor card in the AccuVote-TSX and try to view or change vote results.	The supervisor menu does not allow a user to change or view vote results. Results can only be viewed and/or printed after election has been closed.	None.
3.13	Insert a Supervisor Card in the AccuVote-TSX and try to terminate the election early.	With the use of a supervisor card and the correct PIN number, we were able to close the election early. Inserted the supervisor card, entered the PIN, and the AccuVote-TSX prompted, "Do you want to close the polls? Yes/No". This is a function of the supervisor and a conscious decision must be made to do this. The AccuVote-TSX also warns that no further voting is allowed for this election.	None.
3.14	Insert a Supervisor card in the AccuVote-TSX and try to reset the AccuVote-TSX.	The AccuVote-TSX cannot be reset during voting. Once voting is closed, the AccuVote-TSX can be reset with a supervisor card and the correct PIN number. Resetting clears the memory on the AccuVote-TSX and can clear the PCMCIA card as well. This is a function of the supervisor and a conscious decision must be made to reset the machine.	None.

Continued on the next page

**Risks Identified (continued)**

No.	Test Scenario	Test Result	Risk Identified
3.15	Insert an authorized supervisor card in the AccuVote-TSX and try to access supervisor functions using an incorrect PIN.	The error functionality is the same as the first assessment. The AccuVote-TSX will display an error message and prompt the user to reenter a valid PIN code. The single default PIN code has been changed to accept a user defined PIN code that is established on the GEMS Server and will accept PIN codes from 0 to 10 digits long. User is denied access when using an incorrect PIN. An error message is clearly displayed to the user.	None.
3.16	Start voting on the AccuVote-TSX, and then disconnect batteries/power for 30 minutes to simulate a power outage, Resume power and start up the AccuVote-TSX, and check the voter information.	Removed the AccuVote-TSX from the voting stand, which removed AC Power from the unit. The battery was then removed from the AccuVote-TSX without powering down. Battery was replaced in the unit and power restored. After the AccuVote-TSX was rebooted, it was verified that no ballot information or vote tallies were lost.	None.
3.17	Start voting on the AccuVote-TSX, and then disconnect power for thirty minutes to simulate a power outage, and then resume power. Cast votes before, during, and after the disruption.	17a) Removed power cord and AccuVote-TSX voting machine has a battery backup that powered the machine. The battery is sealed within the machine and could not be removed. 17b) Removed the AccuVote-TSX from the voting stand, which removed AC Power from the unit. The battery was then removed from the AccuVote-TSX and without powering down. Battery was replaced in unit and power restored. After the AccuVote-TSX was rebooted, it was verified that no ballot information or vote tallies were lost.	None.

Continued on the next page

**Risks Identified (continued)**

No.	Test Scenario	Test Result	Risk Identified
3.18	Try to modify the protective counter on the AccuVote-TSX.	The Counter was not able to be accessed or changed.  Supervisor functions will not allow the altering of counts on the AccuVote-TSX voting machine. Counter is stored within the CPU on the AccuVote-TSX. The number on the counter is printed out before the election and after the election as well.	None.
3.19	Modify the AccuVote-TSX so that only core flash memory is available and see if the system will allow voting.	The AccuVote-TSX will not boot into Election Mode without the PCMCIA Flash Memory card being installed.  User is prompted to turn off machine or insert memory card. The system will not allow only one memory source.	None.
3.20	Try to convert a Voter Access card to a Supervisor card then access and perform supervisor functions in the AccuVote-TSX.	Unable to convert a Voter Access card to a Supervisor card.	None.
3.21	Review audit log after completing successful vote test and ensure each step that used supervisor access is correctly logged.	Each time a supervisor card is used, the action is logged within the audit logs specific to the AccuVote-TSX.	None.
3.22	Print a copy of the audit log and verify all items are recorded.	Audit logs printed and all information listed in requirement was printed and verified.	None.
3.23	Review audit log after completing successful vote test and ensure each step that used supervisor access is correctly sequenced.	The audit log is generated in sequential order and each transaction within the audit log is time stamped.	None.
3.24	Print a copy of the audit log and verify all steps are recorded sequentially.	All steps in the audit log are recorded sequentially.	None.
3.25	Review audit logs to verify any act will be recorded and logged with a timestamp.	All actions to the AccuVote-TSX are recorded in the audit log with a time stamp. This includes opening and closing the polls, voting, inserting invalid voting cards, loss of power, and supervisor access.	None.

Continued on the next page

**Risks Identified (continued)**

No.	Test Scenario	Test Result	Risk Identified
3.26	Try to access and modify the vote count on the PCMCIA media or medium (telephone line, etc.) before the vote count is loaded into the GEMS software.	We were unable to alter vote counts on the PCMCIA card, which stores the data. The data is stored in a binary format and it was difficult to read vote records and counts. It was possible to change the data on the PCMCIA card but the AccuVote-TSX would not recognize the modified card as valid for the election.	<p>The AccuVote-TSX uses a standard PCMCIA card which can be inserted in a Windows PC. When files were modified, the files would not load from the PCMCIA card. The system warned of a bad file and would not load the files from the card.</p> <p>There is a risk while it will not use these altered files it will also lose the ability to count any votes that are recorded prior to the files being altered by invalidating the media - Thus leading to the disruption of the election. The system actually performed in the manner it was programmed but the code should be reviewed and improved.</p> <p>Another risk is that an election-ready PCMCIA card might be corrupted using a laptop PC resulting in disruption of the voting process.</p>
3.27	Try to access the information needed to reconstruct a voter's exact voting record.	Individual vote records are not reported from the AccuVote-TSX or tally software. The voting records are displayed in a random order and the voter is kept anonymous. The system will provide for provisional voting by creating a sequence to list provisional voter records.	None.
3.28	Verify vote cannot be altered once the ballot has been cast by using available supervisor functions on the AccuVote-TSX.	User cannot alter vote ballots cast. There is no supervisor function to allow for the votes cast to be altered.	None.

Continued on the next page

**Risks Identified (continued)**

No.	Test Scenario	Test Result	Risk Identified
3.29	When the vote is being cast, others should not be allowed to view the voter's selection of preferences.	The DRE test unit supplied for evaluation has limited external privacy provisions installed. The voting stand has a plastic clam shell screen that shelters the DRE. The Touch screen provides some additional privacy while voting because the LCD Screen characteristics degrade the video when viewed from an angle. Current software functionality concurs with the first assessment report.	None.
3.30	Verify reports can only be executed after the polls have been closed.	Supervisor functions to print reports are not available until the polls are closed. Reports can only be created after polls have closed.	None.
3.31	Conduct a mock election and cast votes. Close the election and print out a record of each individual vote cast.	Individual vote records are not reports created from the AccuVote-TSX. The voting records are listed in a random order and the voter is kept anonymous. Provisional voting is handled differently. Voter records can be re-constructed to verify if the vote cast is allowed or not allowed. This function is performed on GEMS.	None.
3.32	Vote for all issues and/or candidates and before casting the ballot, verify a summary of all votes is presented.	A summary of all votes for each race for the particular user is displayed before we can cast the ballot. Corrections to any race can be made at this point.	None.
3.33	Try to modify the operating system on the AccuVote-TSX by loading a new operating system off the PCMCIA card.	Attempted to load a counterfeit program using the PCMCIA card. Error message was clearly presented to user stating the program cannot be loaded. Error message was generated based on a CRC check of files on the PCMCIA card.	None.
3.34	As a Supervisor, print reports before closing the election.	The DRE will not allow any reports to be created or printed until the election has been closed using a supervisor card.	None.
3.35	Print out reports after election has been closed and verify no inaccuracies exist.	Printed election reports after the close of the election and verified no results were lost during this function.	None.

Continued on the next page

**Risks Identified (continued)**

No.	Test Scenario	Test Result	Risk Identified
3.36	Close the election and print out a copy of the audit log and review all transactions.	All transactions are captured on the audit logs including specific information about the AccuVote-TSX, definition of the election, and all actions occurring on the AccuVote-TSX during the election. All items identified in this requirement are present.	None.
3.37	Complete and close an election and print out a copy of the audit log from a specific AccuVote-TSX.	An audit log is printed out using a specific supervisor function. The audit log produces a report that is a paper trail to guard against fraud.	None.
3.38	Conduct a mock election and cast multiple votes. Once the voting is closed, print out results of the election using the supervisor functions.	Supervisor must close election and select the option to print votes cast. The printout presents the votes cast in a summary format.	None.
3.39	Close the election and transfer results to tally software (GEMS). This is done by connecting the DRE to the Tally software through a network connection using a PCMCIA PC adapter card.	Results of ballots cast transferred to GEMS (tally software) with no problems.	None.
3.40	Upload election results from a DRE to the tally software. Upload them a second time.	We tried to upload the same results twice to GEMS software. An error message is presented stating the results have already been uploaded.	None.
3.41	Try to modify the vote tally in the GEMS software using a tool such as MS Excel or MS Access.	Tester was able to modify vote counts and ballot information using MS Access on a separate machine. Databases are not password protected or encrypted and thus are accessible to unauthorized change.	Same as 3.07 - GEMS uses the MS Access database to store ballot definition data and election results. There is a risk that an unauthorized person with access to the GEMS server can access the database and change ballot definition files and election results.

Continued on the next page

**Risks Identified (continued)**

No.	Test Scenario	Test Result	Risk Identified
3.42	Conduct a mock election for two different AccuVote-TSXs (or memory devices) and verify a report can be created that list counts for each device.	Supervisor must close election and select the option to print votes cast. This can only be done when election has been closed. Once all AccuVote-TSX voting machines have closed all results are uploaded to GEMS where reports are created. Reports can be created to show results for each AccuVote-TSX.	None.
3.43	Conduct a mock election and have multiple voters cast ballots. Once the election is closed, the supervisor card must be used to selection the option of transferring votes to GEMS software for tallying and reporting.	Accessed these functions using a supervisor card. The supervisor then uploaded all results of the vote from each AccuVote-TSX voting machine.	None.
3.44	Set up a mock election and cast multiple votes. Verify all votes have been included in reports created by GEMS.	All votes cast were included in counts recorded by GEMS software. All reports in GEMS accurately reflect number of votes cast on AccuVote-TSX.	None.
3.45	Verify election management software has the ability to handle provisional and absentee ballot voting.	Verified that functionality for recording absentee and provisional voting exists in the GEMS software.	None.
3.46	Complete an election. Print the reports from the Host computer.	Printed the reports from the GEMS software. Verified that provisional voting and absentee ballots were included.	None.
3.47	A magnet is placed on the LCD unit on the AccuVote-TSX smart card reader when voting and PCMCIA slot when recording the votes.	There was no visible degradation on the display. During voting, the magnet did not have any effect on the smart card reader. The PCMCIA card did not get corrupted because of the magnetic field and no votes were lost.	None.

## Risk Levels of Identified Risks

Each Threat-Source/Vulnerability was assigned a rating of High, Medium, or Low to represent the degree or level of risk to which the electronic voting system might be exposed if a given vulnerability were exercised. Following is a description of the High, Medium, and Low ratings.

Risk Level	Risk Description and Necessary Actions
High	If an observation or finding is evaluated as a high risk, there is a strong need for corrective measures. An existing system may continue to operate, but a corrective action plan must be put in place as soon as possible.
Medium	If an observation is rated as medium risk, corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time.
Low	If an observation is described as low risk, it must determine whether corrective actions are still required or whether the risk can be accepted.

The following table shows the rating assigned to each identified risk.

No.	Risk Identified	Risk Likelihood	Impact Rating	Risk Level
<b>Code Review</b>				
1.16	The Diebold AccuVote-TSX and GEMS contain additional third party components. Although the software is included in the AccuVote-TSX, Diebold only receives the executable third party components. There is a risk that a security flaw in these third party products could be inadvertently introduced and cause disruption of the election process.  Note: In order to exploit a vulnerability it would require the attacker to be able to create, compile and include malicious files on the AccuVote-TSX when the firmware is upgraded.	Low	High	Low
1.21	Even though the keys and passwords can be changed, due to their long nature there is a risk that the keys could be lost or discovered if not stored in a secure place.	Medium	High	Medium
1.24	In this release Diebold implemented digital signature. DES encryption is used when Cast Vote Records and the audit log are stored. In our opinion there is a risk that security policy and procedures need to be implemented to protect any and all data files or audio files. There is also a security risk that access to the removable media's file system will not be protected unless policy and procedures are implemented to protect it at election time.	Low	Low	Low

Continued on the next page

**Risk Levels of Identified Risks (continued)**

1.25	With the addition of the Key Card Tool, the encryption keys could be discovered. The codes can be changed, but now must be recorded and may not be stored in a secure place. The risk is now someone has to write down and securely store the codes.	Low	Medium	Low
1.26(a) 1.28 1.29	The Diebold AccuVote-TSX does use DES encryption. The DES key could be discovered. The codes can be changed, but now must be recorded and may not be stored in a secure place.	Low	Medium	Low
1.26(b)	There is a risk that an unauthorized person could decrypt the contents of the removable PCMCIA card using the key if it is discovered.	Low	Medium	Low
1.26(c)	There is a risk that file-level access to the removable media is not secured.	Low	Low	Low
1.27 1.28	The Diebold AccuVote-TSX does use SSL encryption. The SSL key could be discovered. The codes can be changed, but now must be recorded and may not be stored in a secure place. The risk is now someone has to write down and securely store the codes.	Low	Medium	Low
<b>Platform Review</b>				
2.01	There is a risk that an unauthorized person might be able to create and use a counterfeit smart card to access supervisory functions or cast extra ballots.	Low	Medium	Low
2.02	The AccuVote-TSX uses a standard PCMCIA card which can be inserted in a Windows PC. When files were modified, the files would not load from the PCMCIA card. The system warned of a bad file and would not load the files from the card.  There is a risk while it will not use these altered files it will also lose the ability to count any votes that are recorded prior to the files being altered by invalidating the media - Thus leading to the disruption of the election. The system actually performed in the manner it was programmed but the code should be reviewed and improved.  Another risk is that an election-ready PCMCIA card might be corrupted using a laptop PC resulting in disruption of the voting process.	Low	Low	Low
2.07	There is a risk that an unauthorized person might be able to create and use a counterfeit smart card to access supervisory functions or cast extra ballots.	Low	Medium	Low

Continued on the next page

**Risk Levels of Identified Risks (continued)**

2.13	A network port is provided for loading the ballot definitions and downloading cast vote records. This should be done on a point-to-point network. There is a risk of a TCP hijacking attack if the AccuVote-TSX is connected to an intranet or internet. The DRE machines at voting locations will not have an Ethernet card as part of their configuration.	Low	High	Low
2.14	Ports on the AccuVote-TSX are covered by a locking panel. There is a risk that if the cover is unlocked during an election, the exposed ports could be used to disrupt the AccuVote-TSX.	Low	Low	Low
<b>Physical Testing</b>				
3.01	There is a risk that the PCMCIA card can be removed if the compartment is not locked. This is still the same setup. The power switch is in the same compartment as the PCMCIA Flash memory card with the ballot information.	Low	Medium	Low
3.07 3.41	GEMS uses the MS database Jet engine to store ballot definition data and election results. Any ODBC compliant tool could view the data in the database. There is a risk that an unauthorized person with access to the GEMS server can access the database and change ballot definition files and election results.	High	High	High
3.26	The AccuVote-TSX uses a standard PCMCIA card which can be inserted in a Windows PC. When files were modified, the files would not load from the PCMCIA card. The system warned of a bad file and would not load the files from the card. There is a risk while it will not use these altered files it will also loose the ability to count any votes that are recorded prior to the files being altered by invalidating the media - Thus leading to the disruption of the election. The system actually performed in the manner it was programmed but the code should be reviewed and improved. Another risk is that an election-ready PCMCIA card might be corrupted using a laptop PC resulting in disruption of the voting process.	Low	Medium	Low

## Step 8: Risk Mitigation Strategies

In Step 8, the assessment team recommended solutions that are intended to mitigate or eliminate the risks identified in Step 7. The goal of the recommended risk mitigation strategies is to reduce the level of risk to the electronic voting system and its data to an acceptable level.

### Recommended Risk Mitigation Strategies

The assessment team recommends the following mitigation strategies for the risks identified during this assessment.

#### Code Review

No.	Risk Identified	Recommended Mitigation Strategy
<b>High Risk</b>		
N/A		
<b>Medium Risk</b>		
1.21	Even though the keys and passwords can be changed, due to their long nature there is a risk that the keys could be lost or discovered if not stored in a secure place.	We recommend the Secretary of State require that administrative policies and procedures be put into place to mitigate this risk. The policies should cover the secure storage of the keys, and should require that keys be changed for every election.
<b>Low Risk</b>		
1.16	The Diebold AccuVote-TSX and GEMS contain additional third party components. Although the software is included in the AccuVote-TSX, Diebold only receives the executable third party components. There is a risk that a security flaw in these third party products could be inadvertently introduced and cause disruption of the election process.  Note: In order to exploit a vulnerability it would require the attacker to be able to create, compile and include malicious files on the AccuVote-TSX when the firmware is upgraded.	We recommend the Secretary of State should require all Ohio Voting Machine vendors to demonstrate their software development capabilities by achieving Software Engineering Institutes CMM Level2 assessment by end of 2005.  We recommend the Secretary of State require that an independent security assessment be conducted on each release of the AccuVote-TSX.

Continued on the next page

## Recommended Risk Mitigation Strategies (continued)

### Code Review (continued)

No.	Risk Identified	Recommended Mitigation Strategy
<b>Low Risk (continued)</b>		
1.24	In this release Diebold implemented digital signature. DES encryption is used when Cast Vote Records and the audit log are stored. There is a risk that the ballot definitions or audio files can be changed. There is a risk that access to the removable media's file system is not secured.	We recommend the Secretary of State require that administrative policies and procedures be put into place to ensure secure protection for all data files and removable media's file system.
1.25	With the addition of the Key Card Tool, the encryption keys could be discovered. The codes can be changed, but now must be recorded and may not be stored in a secure place.	We recommend the Secretary of State require that administrative policies and procedures be put into place to mitigate this risk. The policies should cover the secure storage of the keys, and should require that keys be changed for every election.
1.26(a) 1.28 1.29	The Diebold AccuVote-TSX does use DES encryption. The DES key could be discovered. The codes can be changed, but now must be recorded and may not be stored in a secure place.	We recommend the Secretary of State require that administrative policies and procedures be put into place to mitigate this risk. The policies should cover the secure storage of the keys, and should require that keys be changed for every election.
1.26(b)	There is a risk that an unauthorized person could decrypt the contents of the removable PCMCIA card using the key if it is discovered.	We recommend the Secretary of State require that administrative policies and procedures be put into place to mitigate this risk. The policies should cover the secure storage of the keys, and should require that keys be changed for every election.  We recommend the Secretary of State require that Diebold encrypt all data files included on the removable media and also use security to prevent unauthorized access to the removable media.
1.26(c)	There is a risk that file-level access to the removable media is not secured.	We recommend the Secretary of State require that Diebold encrypt all data files included on the removable media and also use security to prevent unauthorized access to the removable media.

*Continued on the next page*

No.	Risk Identified	Recommended Mitigation Strategy
<b>Low Risk (continued)</b>		
1.27	The Diebold AccuVote-TSX does use SSL encryption. The SSL key could be discovered. The codes can be changed, but now must be recorded and may not be stored in a secure place. The risk is now someone has to write down and securely store the codes.	We recommend the Secretary of State require that administrative policies and procedures be put into place to mitigate this risk. The policies should cover the secure storage of the keys, and should require that keys be changed for every election.

*Continued on the next page*

## Recommended Risk Mitigation Strategies (continued)

### Platform Review

No.	Risk Identified	Recommended Mitigation Strategy
<b>High Risk</b>		
N/A		
<b>Medium Risk</b>		
N/A		
<b>Low Risk</b>		
2.01 2.07	There is a risk that an unauthorized person might be able to create and use a counterfeit smart card to access supervisory functions or cast extra ballots.	We recommend the Secretary of State require that administrative policies and procedures be put into place to mitigate this risk. The policies should cover the secure storage of the supervisor key(s), and should require that supervisor key(s) be changed for every election. It is highly recommended that the BOE change all of their security codes away from the manufacturer's default.
2.02	<p>The AccuVote-TSX uses a standard PCMCIA card which can be inserted in a Windows PC. When files were modified, the files would not load from the PCMCIA card. The system warned of a bad file and would not load the files from the card.</p> <p>There is a risk while it will not use these altered files it will also lose the ability to count any votes that are recorded prior to the files being altered by invalidating the media - Thus leading to the disruption of the election. The system actually performed in the manner it was programmed but the code should be reviewed and improved.</p> <p>Another risk is that an election-ready PCMCIA card might be corrupted using a laptop PC resulting in disruption of the voting process.</p>	<p>We recommend Diebold perform a technical review of the code and make the necessary improvements to ensure the code will not lose the ability to count any votes that are recorded prior to the files being altered</p> <p>We recommend the Secretary of State require that administrative policies and procedures be put into place to mitigate this risk.</p> <p>We recommend the Secretary of State require that Diebold encrypt all data files included on the removable media and also use security to prevent unauthorized access to the removable media.</p> <p>We recommend that the Secretary of State implements policy and procedures that would handle PCMCIA card's similar as Ohio currently handles ballots.</p>

Continued on the next page

## Recommended Risk Mitigation Strategies (continued)

### Platform Review (continued)

2.13	A network port is provided for loading the ballot definitions and downloading cast vote records. This should be done on a point-to-point network. There is a risk of a TCP hijacking attack if the AccuVote-TSX is connected to an intranet or internet. The DRE machines at voting locations will not have an Ethernet card as part of their configuration.	We recommend the Secretary of State require that administrative policies and procedures be put in place to ensure the AccuVote-TSX is not connected to the internet or to an intranet.  The policies should cover the secure storage of the encryption key, and should require that the encryption key be changed for every election.
2.14	Ports on the AccuVote-TSX are covered by a locking panel.  There is a risk that if the cover is unlocked during an election, the exposed ports could be used to disrupt the AccuVote-TSX.	We recommend the Secretary of State require that administrative policies and procedures be put into place to mitigate this risk.  We recommend the Secretary of State require that when the AccuVote-TSX is in the voting enclosure, all ports, and panels are inaccessible. Additionally, the AccuVote-TSX should be protected from unauthorized removal from the voting enclosure.

*Continued on the next page*

## Recommended Risk Mitigation Strategies (continued)

### Physical Testing

No.	Risk Identified	Recommended Mitigation Strategy
<b>High Risk</b>		
3.07 3.41	<p>GEMS uses the MS database Jet engine to store ballot definition data and election results. Any ODBC compliant tool could view the data in the database.</p> <p>There is a risk that an unauthorized person with access to the GEMS server can access the database and change ballot definition files and election results.</p>	<p>We recommend the Secretary of State require administrative policies and procedures that limit log-on access to the GEMS server.</p> <p>We also recommend the Secretary of State require administrative policies and procedures be put in place which limit the computer programs and tools available on the GEMS server. These policies should limit use of the GEMS server to executing GEMS.</p> <p>We also recommend that the Secretary of State require Diebold to use a database that provides strong password and encryption protection.</p>
<b>Medium Risk</b>		
N/A		
<b>Low Risk</b>		
3.01	<p>There is a risk that the PCMCIA card can be removed if the compartment is not locked.</p> <p>The power switch is in the same compartment as the PCMCIA Flash memory card with the ballot information.</p>	<p>We recommend the Secretary of State require that administrative policies and procedures be put into place to mitigate this risk.</p> <p>We recommend the Secretary of State require that when the AccuVote-TSX is in the voting enclosure, all ports, and panels are inaccessible. Additionally, the AccuVote-TSX should be protected from unauthorized removal from the voting enclosure.</p>
3.26	<p>The AccuVote-TSX uses a standard PCMCIA card which can be inserted in a Windows PC. When files were modified, the files would not load from the PCMCIA card. The system warned of a bad file and would not load the files from the card.</p> <p>There is a risk while it will not use these altered files it will also lose the ability to count any votes that are recorded prior to the files being altered by invalidating the media - thus leading to the disruption of the election.</p> <p>The system actually performed in the manner it was programmed but the code should be reviewed and improved.</p> <p>Another risk is that an election-ready PCMCIA card might be corrupted using a laptop PC resulting in disruption of the voting process.</p>	<p>Same as 2.02 under the Platform Review section above.</p>

## Step 9: Document Results

In Step 9, the assessment team combined the results of Steps 1 through 8 to develop this report detailing the technical security assessment and its findings.

## Conclusion

Compuware has conducted a study of the Diebold AccuVote-TSX voting system to identify specific security vulnerabilities that might be exploited during an election and to recommend actions to mitigate these vulnerabilities. The scope of this study has been limited to reviewing the technical implementation of the AccuVote-TSX and reviewing each data stream into and from the AccuVote-TSX. It has not included a review of the policies, procedures, or work practices of either Diebold or the Ohio Secretary of State.

During the course of our study, Compuware has identified a multiple significant security issue, which left unmitigated would provide an opportunity for an attacker to disrupt the election process or throw the election results into question. It is documented above. Following careful consideration for the security issue, we have developed mitigation recommendations for the Secretary of State to implement which we believe will limit the likelihood of a successful attack on the election process. Provided each of these mitigation recommendations can be enacted, Compuware has concluded the Diebold AccuVote-TSX can be securely deployed by the Secretary of State.

Although all risks documented above must be dealt with appropriately, the most significant risk areas, which will require the most effort to mitigate, include:

Risk Identified	Recommended Mitigation Strategy
<p>GEMS uses the MS database Jet engine to store ballot definition data and election results. Any ODBC compliant tool could view the data in the database.</p> <p>There is a risk that an unauthorized person with access to the GEMS server can access the database and change ballot definition files and election results.</p>	<p>We recommend the Secretary of State require administrative policies and procedures that limit log-on access to the GEMS server.</p> <p>We also recommend the Secretary of State require administrative policies and procedures be put in place which limit the computer programs and tools available on the GEMS server. These policies should limit use of the GEMS server to executing GEMS.</p> <p>We also recommend that the Secretary of State require Diebold to use a database that provides strong password and encryption protection.</p>
<p>Even though the keys and passwords can be changed, due to their long nature there is a risk that the keys could be lost or discovered if not stored in a secure place.</p>	<p>We recommend the Secretary of State require that administrative policies and procedures be put into place to mitigate this risk. The policies should cover the secure storage of the keys, and should require that keys be changed for every election.</p>

*Continued on the next page*

## Conclusion (continued)

Risk Identified	Recommended Mitigation Strategy
<p>Ports on the AccuVote-TSX are covered by a locking panel.</p> <p>There is a risk that if the cover is unlocked during an election, the exposed ports could be used to disrupt the AccuVote-TSX.</p>	<p>We recommend the Secretary of State require that administrative policies and procedures be put into place to mitigate this risk.</p> <p>We recommend the Secretary of State require that when the AccuVote-TSX is in the voting enclosure, all ports and panels are inaccessible. Additionally, the AccuVote-TSX should be protected from unauthorized removal from the voting enclosure.</p>
<p>The Diebold AccuVote-TSX and GEMS contain additional third party components. Although the software is included in the AccuVote-TSX, Diebold does not maintain these third party components. There is a risk that a security flaw in these third party products could be inadvertently introduced and cause disruption of the election process.</p> <p>We also observed that it took up to 3 days to receive additionally requested source code. Based on this observation we viewed it as not having a seamless source control system that manages all parts of the code.</p> <p>Note: In order to exploit a vulnerability it would require the attacker to be able to create, compile and include malicious files on the AccuVote-TSX when the firmware is upgraded.</p>	<p>We recommend the Secretary of State should require all Ohio Voting Machine vendors to demonstrate their software development capabilities by achieving Software Engineering Institutes CMM Level 2 assessment by end of 2005.</p> <p>Following the CMM methodology has many benefits for any software development organization here are 2 key areas.</p> <ul style="list-style-type: none"> <li>• Configuration Management is one of the key areas in Level 2 that would ensure an improved management of DRE solution software and versions for each certification in the vendors development environment.</li> <li>• Software Quality Assurance (SQA) is another key area of CMM Level 2. SQA audits should be scheduled and completed on each updated version of the software before it goes to ITA certification and the SQA Audit report should be sent to the Secretary Of State.</li> </ul> <p>We recommend the Secretary of State require that an independent security assessment be conducted on each release of the AccuVote-TSX.</p>

Election policies and procedures have long been used to ensure fair and accurate election results. The deployment of DRE technology will not lessen the need for well thought out and consistently enforced policies and procedures.

This page intentionally left blank.

- From Black Box Voting Document Archive -

- From Black Box Voting Document Archive -

## ATTACHMENT A: Risk Assessment Methodology

Following is an explanation of the Risk Assessment methodology used by Compuware for this security assessment. The methodology used is in accordance with the National Institute of Standards and Technology (NIST) Nine Steps and is based upon the methodology documented in NIST SP 800-30, *Risk Management Guide for Information Technology Systems*.

The following information is based on NIST SP 800-30, which has been modified for use in this security assessment.

### Overview

Risk assessment is the first process in the risk management methodology. Organizations use risk assessment to determine the extent of the potential threat and the risk associated with an electronic voting system throughout its SDLC. The output of this process helps to identify appropriate controls for reducing or eliminating risk during the risk mitigation process.

Risk is a function of the *likelihood* of a given *threat-source's* exercising a particular potential *vulnerability*, and the resulting *impact* of that adverse event on the organization.

To determine the likelihood of a future adverse event, threats to an electronic voting system must be analyzed in conjunction with the potential vulnerabilities and the controls in place for the IT System in place. Impact refers to the magnitude of harm that could be caused by a threat's exercise of vulnerability. The level of impact is governed by the potential mission impacts and in turn produces a relative value for the IT assets and resources affected (e.g., the criticality and sensitivity of the electronic voting system components and data). The risk assessment methodology encompasses nine primary steps, which are described below.

- Step 1. System Characterization (Section A.1)
- Step 2. Threat Identification (Section A.2)
- Step 3. Vulnerability Identification (Section A.3)
- Step 4. Control Analysis (Section A.4)
- Step 5. Likelihood Determination (Section A.5)
- Step 6. Impact Analysis (Section A.6)
- Step 7. Risk Determination (Section A.7)
- Step 8. Control Recommendations (Section A.8)
- Step 9. Results Documentation (Section A.9).

Steps 2, 3, 4, and 6 can be conducted in parallel after Step 1 has been completed.

### Overview (continued)

Figure A-1 below depicts these steps.

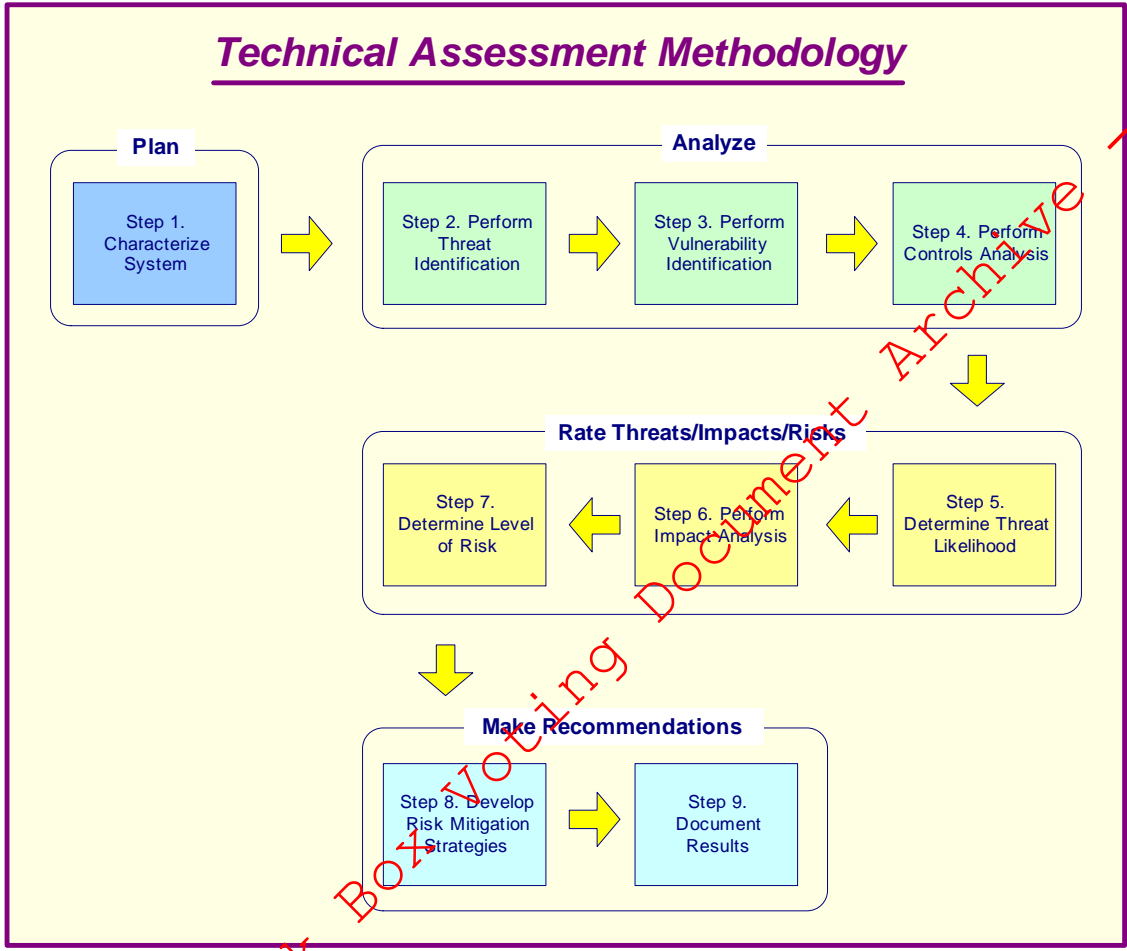


Figure A-1 – Technical Assessment Methodology

## A.1 Step 1: System Characterization

In assessing risks for an electronic voting system, the first step is to define the scope of the effort. In this step, the boundaries of the electronic voting system are identified, along with the resources and the information that constitute the system. Characterizing an electronic voting system establishes the scope of the risk assessment effort, delineates the operational authorization (or accreditation) boundaries, and provides information (e.g., hardware, software, system connectivity, and responsible division or support personnel) essential to defining the risk.

Section A.1.1 describes the system-related information used to characterize an electronic voting system and its operational environment. Section A.1.2 suggests the information-gathering techniques that can be used to solicit information relevant to the electronic voting system processing environment.

The methodology described in this document can be applied to assessments of single or multiple, interrelated systems. In the latter case, it is important that the domain of interest and all interfaces and dependencies be well defined prior to applying the methodology.

### A.1.1 System-Related Information

Identifying risk for an electronic voting system requires a keen understanding of the system's processing environment. The person or persons who conduct the risk assessment must therefore first collect system-related information, which is usually classified as follows:

- Hardware / Software / System interfaces (e.g., internal and external connectivity)
- Data and information
- Persons who support and use the electronic voting system
- System mission (e.g., the processes performed by the electronic voting system)
- System and data criticality (e.g., the system's value or importance to an organization)
- System and data sensitivity

Additional information related to the operational environmental of the electronic voting system and its data includes, but is not limited to, the following:

- The functional requirements of the electronic voting system
- Users of the system (e.g., system users who provide technical support to the electronic voting system; application users who use the electronic voting system to perform business functions)
- System security policies governing the electronic voting system (organizational policies, federal requirements, laws, industry practices)
- System security architecture
- Current network topology (e.g., network diagram)
- Information storage protection that safeguards system and data availability, integrity, and confidentiality
- Flow of information pertaining to the electronic voting system (e.g., system interfaces, system input and output flowchart)
- Technical controls used for the electronic voting system (e.g., built-in or add-on security product that supports identification and authentication, discretionary or mandatory access control, audit, residual information protection, encryption methods)

### A.1.1 System-Related Information (continued)

Operational environment information (continued):

- Management controls used for the electronic voting system (e.g., rules of behavior, security planning)
- Operational controls used for the electronic voting system (e.g., personnel security, backup, contingency, and resumption and recovery operations; system maintenance; off-site storage; user account establishment and deletion procedures; controls for segregation of user functions, such as privileged user access versus standard user access)
- Physical security environment of the electronic voting system (e.g., facility security, data center policies)
- Environmental security implemented for the electronic voting system processing environment (e.g., controls for humidity, water, power, pollution, temperature, and chemicals).

For a system that is in the initiation or design phase, system information can be derived from the design or requirements document. For an electronic voting system under development, it is necessary to define key security rules and attributes planned for the future electronic voting system. System design documents and the system security plan can provide useful information about the security of an electronic voting system that is in development.

For an operational electronic voting system, data is collected about the electronic voting system in its production environment, including data on system configuration, connectivity, and documented and undocumented procedures and practices. Therefore, the system description can be based on the security provided by the underlying infrastructure or on future security plans for the electronic voting system.

### A.1.2 Information-Gathering Techniques

Any, or a combination, of the following techniques can be used in gathering information relevant to the electronic voting system within its operational boundary:

#### Questionnaire

To collect relevant information, risk assessment personnel can develop a questionnaire concerning the management and operational controls planned or used for the electronic voting system. This questionnaire should be distributed to the applicable technical and non-technical management personnel who are designing or supporting the electronic voting system. The questionnaire could also be used during on-site visits and interviews.

#### On-site Interviews

Interviews with electronic voting system support and management personnel can enable risk assessment personnel to collect useful information about the electronic voting system (e.g., how the system is operated and managed). On-site visits also allow risk

assessment personnel to observe and gather information about the physical, environmental, and operational security of the electronic voting system. Appendix A contains sample interview questions asked during interviews with site personnel to achieve a better understanding of the operational characteristics of an organization. For systems still in the design phase, on-site visit would be face-to-face data gathering exercises and could provide the opportunity to evaluate the physical environment in which the electronic voting system will operate.

## Document Review

Policy documents (e.g., legislative documentation, directives), system documentation (e.g., system user guide, system administrative manual, system design and requirement document, acquisition document), and security-related documentation (e.g., previous audit report, risk assessment report, system test results, system security plan, security policies) can provide good information about the security controls used by and planned for the electronic voting system. An organization's mission impact analysis or asset criticality assessment provides information regarding system and data criticality and sensitivity.

## Use of Automated Scanning Tool

Proactive technical methods can be used to collect system information efficiently. For example, a network mapping tool can identify the services that run on a large group of hosts and provide a quick way of building individual profiles of the target electronic voting system(s).

Information gathering can be conducted throughout the risk assessment process, from Step 1 (System Characterization) through Step 9 (Results Documentation).

## Output from Step 1

The outputs from Step 1 are: Characterization of the electronic voting system assessed, a good picture of the electronic voting system environment, and delineation of the system boundary.

## A.2 Step 2: Threat Identification

A threat is the potential for a particular threat-source to successfully exercise a particular vulnerability. Vulnerability is a weakness that can be accidentally triggered or intentionally exploited. A threat-source does not present a risk when there is no vulnerability that can be exercised. In determining the likelihood of a threat (Section A.5), one must consider threat-sources, potential vulnerabilities (Section A.3), and existing controls (Section A.4).

### A.2.1 Threat-Source Identification

The goal of this step is to identify the potential threat-sources and compile a threat statement listing potential threat-sources that are applicable to the electronic voting system being evaluated.

- **Threat:** The potential for a threat-source to exercise (accidentally trigger or intentionally exploit) a specific vulnerability.
- **Threat-Source:** Either (1) intent and method targeted at the intentional exploitation of a vulnerability or (2) a situation and method that may accidentally trigger a vulnerability.

A threat-source is defined as any circumstance or event with the potential to cause harm to an electronic voting system. The common threat-sources can be natural, human, or environmental.

### A.2.1 Threat-Source Identification (continued)

In assessing threat-sources, it is important to consider all potential threat-sources that could cause harm to an electronic voting system and its processing environment. For example, although the threat statement for an electronic voting system located in a desert may not include natural flood because of the low likelihood of such an event's occurring, environmental threats such as a bursting pipe can quickly flood a computer room and cause damage to an organization's IT assets and resources. Humans can be threat-sources through intentional acts, such as deliberate attacks by malicious persons or disgruntled employees, or unintentional acts, such as negligence and errors. A deliberate attack can be either (1) a malicious attempt to gain unauthorized access to an electronic voting system (e.g., via password guessing) in order to compromise system and data integrity, availability, or confidentiality or (2) a benign, but nonetheless purposeful, attempt to circumvent system security. One example of the latter type of deliberate attack is a programmer's writing a Trojan horse program to bypass system security in order to get the job done.

### A.2.2 Motivation and Threat Actions

Motivation and the resources for carrying out an attack make humans potentially dangerous threat-sources. The table below presents an overview of many of today's common human threats, their possible motivations, and the methods or threat actions by which they might carry out an attack. This information will be useful to organizations studying their human threat environments and customizing their human threat statements. In addition, reviews of the history of system break-ins; security violation reports; incident reports; and interviews with the system administrators, help desk personnel, and user community during information gathering will help identify human threat-sources that have the potential to harm an electronic voting system and its data and that may be a concern where vulnerability exists.

#### **Common Threat-Sources**

Natural Threats: Floods, earthquakes, tornadoes, landslides, avalanches, electrical storms, and other such events.

Human Threats: Events that are either enabled by or caused by human beings, such as unintentional acts (inadvertent data entry) or deliberate actions (network based attacks, malicious software upload, unauthorized access to confidential information).

Environmental Threats: Long-term power failure, pollution, chemicals, liquid leakage.

*Continued on the next page*

## A.2.2 Motivation and Threat Actions (continued)

The following table describes the various human threats.

Threat-Source	Motivation	Threat Actions
Hacker, cracker	Challenge Ego Rebellion	<ul style="list-style-type: none"> <li>• Hacking</li> <li>• Social engineering</li> <li>• System intrusion, break-ins</li> <li>• Unauthorized system access</li> </ul>
Computer criminal	Destruction of information Illegal information disclosure Monetary gain Unauthorized data alteration	<ul style="list-style-type: none"> <li>• Computer crime (e.g., cyber stalking)</li> <li>• Fraudulent act (e.g., replay, impersonation, interception)</li> <li>• Information bribery</li> <li>• Spoofing</li> <li>• System intrusion</li> </ul>
Terrorist	Blackmail Destruction Exploitation Revenge	<ul style="list-style-type: none"> <li>• Bomb/Terrorism</li> <li>• Information warfare</li> <li>• System attack (e.g., distributed denial of service)</li> <li>• System penetration</li> <li>• System tampering</li> </ul>
Campaign and political entities	Competitive advantage Economic espionage Change outcome of election	<ul style="list-style-type: none"> <li>• Economic exploitation</li> <li>• Information theft</li> <li>• Intrusion on personal privacy</li> <li>• Social engineering</li> <li>• System penetration</li> <li>• Unauthorized system access (access to classified, proprietary, and/or technology-related information)</li> </ul>
Insiders (poorly trained, disgruntled, malicious, negligent, dishonest, or terminated employees)	Curiosity Ego Intelligence Monetary gain Revenge Unintentional errors and omissions (e.g., data entry error, programming error)	<ul style="list-style-type: none"> <li>• Assault on an employee</li> <li>• Blackmail</li> <li>• Browsing of proprietary information</li> <li>• Computer abuse</li> <li>• Fraud and theft</li> <li>• Information bribery</li> <li>• Input of falsified, corrupted data</li> <li>• Interception</li> <li>• Malicious code (e.g., virus, logic bomb, Trojan horse)</li> <li>• Sale of personal information</li> <li>• System bugs</li> <li>• System intrusion</li> <li>• System sabotage</li> <li>• Unauthorized system access</li> </ul>

*Continued on the next page*

## A.2.2 Motivation and Threat Actions (continued)

An estimate of the motivation, resources, and capabilities that may be required to carry out a successful attack should be developed after the potential threat-sources have been identified, in order to determine the likelihood of a threat's exercising system vulnerability, as described in Section 3.5.

The threat statement, or the list of potential threat-sources, should be tailored to the individual organization and its processing environment (e.g., end-user computing habits). In general, information on natural threats (e.g., floods, earthquakes, storms) should be readily available. Known threats have been identified by many government and private sector organizations. Intrusion detection tools also are becoming more prevalent, and government and industry organizations continually collect data on security events, thereby improving the ability to realistically assess threats. Sources of information include, but are not limited to, the following:

- Intelligence agencies (for example, the Federal Bureau of Investigation's National Infrastructure Protection Center)
- Federal Computer Incident Response Center (FedCIRC)
- Mass media, particularly Web-based resources such as SecurityFocus.com, SecurityWatch.com, SecurityPortal.com, and SANS.org.

### Output from Step 2

The output from Step 2 is: A threat statement containing a list of threat-sources that could exploit electronic voting system vulnerabilities

## A.3 Step 3: Vulnerability Identification

The analysis of the threat to an electronic voting system must include an analysis of the vulnerabilities associated with the system environment. The goal of this step is to develop a list of system vulnerabilities (flaws or weaknesses) that could be exploited by the potential threat-sources.

The following table presents examples of vulnerability/threat pairs.

Vulnerability	Threat-Source	Threat Action
Terminated employees. System identifiers (ID) are not removed from the system	Terminated employees	Dialing into the company's network and accessing company proprietary data
Company firewall allows inbound telnet, and guest ID is enabled on XYZ server	Unauthorized users (e.g., hackers, terminated employees, computer criminals, terrorists)	Using telnet to XYZ server and browsing system files with the guest ID
The vendor has identified flaws in the security design of the system; however, new patches have not been applied to the system	Unauthorized users (e.g., hackers, disgruntled employees, computer criminals, terrorists)	Obtaining unauthorized access to sensitive system files based on known system vulnerabilities

*Continued on the next page*

### A.3 Step 3: Vulnerability Identification (continued)

**Vulnerability:** A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy.

Vulnerability	Threat-Source	Threat Action
Data center uses water sprinklers to suppress fire; tarpaulins to protect hardware and equipment from water damage are not in place	Fire, negligent persons	Water sprinklers being turned on in the data center

Recommended methods for identifying system vulnerabilities are the use of vulnerability sources, the performance of system security testing, and the development of a security requirements checklist.

It should be noted that the types of vulnerabilities that will exist, and the methodology needed to determine whether the vulnerabilities are present, will usually vary depending on the nature of the electronic voting system and the phase it is in, in the SDLC:

- If the electronic voting system has not yet been designed, the search for vulnerabilities should focus on the organization's security policies, planned security procedures, and system requirement definitions, and the vendors or developers security product analyses (e.g., white papers).
- If the electronic voting system is being implemented, the identification of vulnerabilities should be expanded to include more specific information, such as the planned security features described in the security design documentation and the results of system certification test and evaluation.
- If the electronic voting system is operational, the process of identifying vulnerabilities should include an analysis of the electronic voting system security features and the security controls, technical and procedural, used to protect the system.

*Continued on the next page*

## A.3 Step 3: Vulnerability Identification (continued)

### A.3.1 Vulnerability Sources

The technical and no technical vulnerabilities associated with an electronic voting system's processing environment can be identified via the information-gathering techniques described in Section 3.1.2. A review of other industry sources (e.g., vendor Web pages that identify system bugs and flaws) will be useful in preparing for the interviews and in developing effective questionnaires to identify vulnerabilities that may be applicable to specific electronic voting systems (e.g., a specific version of a specific operating system). The Internet is another source of information on known system vulnerabilities posted by vendors, along with hot fixes, service packs, patches, and other remedial measures that may be applied to eliminate or mitigate vulnerabilities. Documented vulnerability sources that should be considered in a thorough vulnerability analysis include, but are not limited to, the following:

- Previous risk assessment documentation of the electronic voting system assessed
- The electronic voting system's audit reports system anomaly reports, security review reports, and system test and evaluation reports
- Vulnerability lists, such as the NIST I-CAT vulnerability database (<http://icat.nist.gov>)
- Security advisories, such as FedCIRC and the Department of Energy's Computer Incident Advisory Capability bulletins
- Vendor advisories
- Commercial computer incident/emergency response teams and post lists (e.g., SecurityFocus.com forum mailings)
- Information Assurance Vulnerability Alerts and bulletins for military systems
- System software security analyses.

### A.3.2 System Security Testing

Proactive methods, employing system testing, can be used to identify system vulnerabilities efficiently, depending on the criticality of the electronic voting system and available resources (e.g., allocated funds, available technology, persons with the expertise to conduct the test). Test methods include.

- Automated vulnerability scanning tool
- Security test and evaluation (ST&E)
- Penetration testing

The automated vulnerability scanning tool is used to scan a group of hosts or a network for known vulnerable services (e.g., system allows anonymous File Transfer Protocol [FTP], send mail relaying). However, it should be noted that some of the potential vulnerabilities identified by the automated scanning tool may not represent real vulnerabilities in the context of the system environment. For example, some of these scanning tools rate potential vulnerabilities without considering the site's environment and requirements. Some of the vulnerabilities flagged by the automated scanning software may actually not be vulnerable for a particular site but may be configured that way because their environment requires it. Thus, this test method may produce false positives.

*Continued on the next page*

### **A.3 Step 3: Vulnerability Identification (continued)**

ST&E is another technique that can be used in identifying electronic voting system vulnerabilities during the risk assessment process. It includes the development and execution of a test plan (e.g., test script, test procedures, and expected test results). The purpose of system security testing is to test the effectiveness of the security controls of an electronic voting system as they have been applied in an operational environment. The objective is to ensure that the applied controls meet the approved security specification for the software and hardware and implement the organization's security policy or meet industry standards.

Penetration testing can be used to complement the review of security controls and ensure that different facets of the electronic voting system are secured. Penetration testing, when employed in the risk assessment process, can be used to assess an electronic voting system's ability to withstand intentional attempts to circumvent system security. Its objective is to test the electronic voting system from the viewpoint of a threat-source and to identify potential failures in the electronic voting system protection schemes.

The results of these types of optional security testing will help identify a system's vulnerabilities.

#### **A.3.3 Development of Security Requirements Checklist**

During this step, the risk assessment personnel determine whether the security requirements stipulated for the electronic voting system and collected during system characterization are being met by existing or planned security controls. Typically, the system security requirements can be presented in table form, with each requirement accompanied by an explanation of how the system's design or implementation does or does not satisfy that security control requirement.

A security requirements checklist contains the basic security standards that can be used to systematically evaluate and identify the vulnerabilities of the assets (personnel, hardware, software, and information), non automated procedures, processes, and information transfers associated with a given electronic voting system in the following security areas:

- Management
- Operational
- Technical

*Continued on the next page*

### A.3 Step 3: Vulnerability Identification (continued)

The following table lists security criteria suggested for use in identifying an electronic voting system's vulnerabilities in each security area.

Security Area	Security Criteria
Management Security	<ul style="list-style-type: none"> <li>• Assignment of responsibilities</li> <li>• Continuity of support</li> <li>• Incident response capability</li> <li>• Periodic review of security controls</li> <li>• Personnel clearance and background investigations</li> <li>• Risk assessment</li> <li>• Security and technical training</li> <li>• Separation of duties</li> <li>• System authorization and reauthorization</li> <li>• System or application security plan</li> </ul>
Operational Security	<ul style="list-style-type: none"> <li>• Control of air-borne contaminants (smoke, dust, chemicals)</li> <li>• Controls to ensure the quality of the electrical power supply</li> <li>• Data media access and disposal</li> <li>• External data distribution and labeling</li> <li>• Facility protection (e.g., computer room, data center, office)</li> <li>• Humidity control</li> <li>• Temperature control</li> <li>• Workstations, laptops, and stand-alone personal computers</li> </ul>
Technical Security	<ul style="list-style-type: none"> <li>• Communications (e.g., dial-in, system interconnection, routers)</li> <li>• Cryptography</li> <li>• Discretionary access control</li> <li>• Identification and authentication</li> <li>• Intrusion detection</li> <li>• Object reuse</li> <li>• System audit</li> </ul>

The outcome of this process is the security requirements checklist. Sources that can be used in compiling such a checklist include, but are not limited to, the following government regulatory and security directives and sources applicable to the electronic voting system processing environment:

- CSA of 1987 Federal Information
- Processing Standards Publications
- OMB November 2000 Circular A-130
- Privacy Act of 1974
- System security plan of the electronic voting system assessed
- The organization's security policies, guidelines, and standards
- Industry practices.

*Continued on the next page*

### **A.3 Step 3: Vulnerability Identification (continued)**

The NIST SP 800-26, Security Self-Assessment Guide for Information Technology Systems, provides an extensive questionnaire containing specific control objectives against which a system or group of interconnected systems can be tested and measured. The control objectives are abstracted directly from long-standing requirements found in statute, policy, and guidance on security and privacy.

The results of the checklist (or questionnaire) can be used as input for an evaluation of compliance and noncompliance. This process identifies system, process, and procedural weaknesses that represent potential vulnerabilities.

### **A.4 Step 4: Control Analysis**

The goal of this step is to analyze the controls that have been implemented, or are planned for implementation, by the organization to minimize or eliminate the likelihood (or probability) of a threat's exercising a system vulnerability.

To derive an overall likelihood rating that indicates the probability that a potential vulnerability may be exercised within the construct of the associated threat environment (Step 5 below), the implementation of current or planned controls must be considered. For example, a vulnerability (e.g., system or procedural weakness) is not likely to be exercised or the likelihood is low if there is a low level of threat-source interest or capability or if there are effective security controls that can eliminate, or reduce the magnitude of, harm.

Sections A.4.1 through A.4.3, respectively, discuss control methods, control categories, and the control analysis technique.

#### **A.4.1 Control Methods**

Security controls encompass the use of technical and non-technical methods. Technical controls are safeguards that are incorporated into computer hardware, software, or firmware (e.g., access control mechanisms, identification and authentication mechanisms, encryption methods, intrusion detection software). Non-technical controls are management and operational controls, such as security policies; operational procedures; and personnel, physical, and environmental security.

#### **A.4.2 Control Categories**

The control categories for both technical and non-technical control methods can be further classified as either preventive or detective. These two subcategories are explained as follows:

Preventive controls inhibit attempts to violate security policy and include such controls as access control enforcement, encryption, and authentication.

Detective controls warn of violations or attempted violations of security policy and include such controls as audit trails, intrusion detection methods, and checksums.

Section 4.4 further explains these controls from the implementation standpoint. The implementation of such controls during the risk mitigation process is the direct result of the identification of deficiencies in current or planned controls during the risk assessment process (e.g., controls are not in place or controls are not properly implemented).

### A.4.3 Control Analysis Technique

As discussed in Section A.3.3, development of a security requirements checklist or use of an available checklist will be helpful in analyzing controls in an efficient and systematic manner. The security requirements checklist can be used to validate security noncompliance as well as compliance. Therefore, it is essential to update such checklists to reflect changes in an organization's control environment (e.g., changes in security policies, methods, and requirements) to ensure the checklist's validity.

#### Output from Step 4

The output from Step 4 is: List of current or planned controls used for the electronic voting system to mitigate the likelihood of vulnerabilities being exercised and reduce the impact of such an adverse event.

### A.5 Step 5: Likelihood Determination

To derive an overall likelihood rating that indicates the probability that a potential vulnerability may be exercised within the construct of the associated threat environment; the following governing factors must be considered:

- Threat-source motivation and capability
- Nature of the vulnerability
- Existence and effectiveness of current controls

The likelihood that a potential vulnerability could be exercised by a given threat-source can be described as high, medium, or low. The table below describes these three likelihood levels.

Likelihood Level	Likelihood Definition
High	The threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective.
Medium	The threat-source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.
Low	The threat-source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.

#### Output from Step 5

The output from Step 5 is: Likelihood rating (High, Medium, Low) for the potential vulnerability.

## A.6 Step 6: Impact Analysis

The next major step in measuring level of risk is to determine the adverse impact resulting from a successful threat exercise of vulnerability. Before beginning the impact analysis, it is necessary to obtain the following necessary information as discussed in Section 3.1.1:

- System mission (e.g., the processes performed by the electronic voting system)
- System and data criticality (e.g., the system's value or importance to an organization)
- System and data sensitivity

This information can be obtained from existing organizational documentation, such as the mission impact analysis report or asset criticality assessment report. A mission impact analysis (also known as business impact analysis [BIA] for some organizations) prioritizes the impact levels associated with the compromise of an organization's information assets based on a qualitative or quantitative assessment of the sensitivity and criticality of those assets. An asset criticality assessment identifies and prioritizes the sensitive and critical organization information assets (e.g., hardware, software, systems, services, and related technology assets) that support the organization's critical missions.

If this documentation does not exist or such assessments for the organization's IT assets have not been performed, the system and data sensitivity can be determined based on the level of protection required to maintain the system and data's availability, integrity, and confidentiality. Regardless of the method used to determine how sensitive an electronic voting system and its data are, the system and information owners are the ones responsible for determining the impact level for their own system and information. Consequently, in analyzing impact, the appropriate approach is to interview the system and information owner(s).

Therefore, the adverse impact of a security event can be described in terms of loss or degradation of any, or a combination of any, of the following three security goals: integrity, availability, and confidentiality. The following list provides a brief description of each security goal and the consequence (or impact) of its not being met:

**Loss of Integrity:** System and data integrity refers to the requirement that information be protected from improper modification. Integrity is lost if unauthorized changes are made to the data or electronic voting system by either intentional or accidental acts. If the loss of system or data integrity is not corrected, continued use of the contaminated system or corrupted data could result in inaccuracy, fraud, or erroneous decisions. Also, violation of integrity may be the first step in a successful attack against system availability or confidentiality. For all these reasons, loss of integrity reduces the assurance of an electronic voting system.

**Loss of Availability:** If a mission-critical electronic voting system is unavailable to its end users, the organization's mission may be affected. Loss of system functionality and operational effectiveness, for example, may result in loss of productive time, thus impeding the end users. Performance of their functions in supporting the organization's mission.

**Loss of Confidentiality:** System and data confidentiality refers to the protection of information from unauthorized disclosure. The impact of unauthorized disclosure of confidential information can range from the jeopardizing of national security to the disclosure of Privacy Act data. Unauthorized, unanticipated, or unintentional disclosure could result in loss of public confidence, embarrassment, or legal action against the organization.

*Continued on the next page*

## A.6 Step 6: Impact Analysis (continued)

Some tangible impacts can be measured quantitatively in lost revenue, the cost of repairing the system, or the level of effort required to correct problems caused by a successful threat action. Other impacts (e.g., loss of public confidence, loss of credibility, damage to an organization's interest) cannot be measured in specific units but can be qualified or described in terms of high, medium, and low impacts. Because of the generic nature of this discussion, this guide designates and describes only the qualitative categories, high, medium, and low impact (see the table below).

Magnitude of Impact	Impact Definition
High	Exercise of the vulnerability (1) may result in the highly costly loss of major tangible assets or resources; (2) may significantly violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human death or serious injury.
Medium	Exercise of the vulnerability (1) may result in the costly loss of tangible assets or resources; (2) may violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human injury.
Low	Exercise of the vulnerability (1) may result in the loss of some tangible assets or resources or (2) may noticeably affect an organization's mission, reputation, or interest.

### Quantitative versus Qualitative Assessment

In conducting the impact analysis, consideration should be given to the advantages and disadvantages of quantitative versus qualitative assessments. The main advantage of the qualitative impact analysis is that it prioritizes the risks and identifies areas for immediate improvement in addressing the vulnerabilities. The disadvantage of the qualitative analysis is that it does not provide specific quantifiable measurements of the magnitude of the impacts, therefore making a cost-benefit analysis of any recommended controls difficult.

The major advantage of a quantitative impact analysis is that it provides a measurement of the impacts. Magnitude, which can be used in the cost-benefit analysis of recommended controls. The disadvantage is that, depending on the numerical ranges used to express the measurement, the meaning of the quantitative impact analysis may be unclear, requiring the result to be interpreted in a qualitative manner. Additional factors often must be considered to determine the magnitude of impact. These may include, but are not limited to:

- An estimation of the frequency of the threat-source's exercise of the vulnerability over a specified time period (e.g., 1 year)
- An approximate cost for each occurrence of the threat-source's exercise of the vulnerability
- A weighted factor based on a subjective analysis of the relative impact of a specific threat's exercising a specific vulnerability.

### Output from Step 6

The output from Step 6 is: Magnitude of impact rating (High, Medium, or Low).

## A.7 Step 7: Risk Determination

The purpose of this step is to assess the level of risk to the electronic voting system. The determination of risk for a particular threat/vulnerability pair can be expressed as a function of:

- The likelihood of a given threat-source's attempting to exercise a given vulnerability
- The magnitude of the impact should a threat-source successfully exercise the vulnerability
- The adequacy of planned or existing security controls for reducing or eliminating risk.

To measure risk, a risk scale and a risk-level matrix must be developed. Section A.7.1 presents a standard risk-level matrix; Section A.7.2 describes the resulting risk levels.

### A.7.1 Risk-Level Matrix

The final determination of mission risk is derived by multiplying the ratings assigned for threat likelihood (e.g., probability) and threat impact. The table below shows how the overall risk ratings might be determined based on inputs from the threat likelihood and threat impact categories. The matrix below is a 3 x 3 matrix of threat likelihood (High, Medium, and Low) and threat impact (High, Medium, and Low). Depending on the site's requirements and the granularity of risk assessment desired, some sites may use a 4 x 4 or a 5 x 5 matrix. The latter can include Very Low /Very High threat likelihood and a Very Low/Very High threat impact to generate a Very Low/Very High risk level. A Very High risk level may require possible system shutdown or stopping of all electronic voting system integration and testing efforts.

The sample matrix in the table below shows how the overall risk levels of High, Medium, and Low are derived. The determination of these risk levels or ratings may be subjective. The rationale for this justification can be explained in terms of the probability assigned for each threat likelihood level and a value assigned for each impact level.

For example:

- The probability assigned for each threat likelihood level is 1.0 for High, 0.5 for Medium, 0.1 for Low
- The value assigned for each impact level is 100 for High, 50 for Medium, and 10 for Low.

Threat Likelihood		Impact	
Low (10)	Medium (50)	High (100)	
High (1.0)	Low $10 \times 1.0 = 10$	Medium $50 \times 1.0 = 50$	High $100 \times 1.0 = 100$
Medium (0.5)	Low $10 \times 0.5 = 5$	Medium $50 \times 0.5 = 25$	High $100 \times 0.5 = 50$
Low (0.1)	Low $10 \times 0.1 = 1$	Medium $50 \times 0.1 = 5$	High $100 \times 0.1 = 10$

*Risk scale: High (>50 to 100); Medium (>10 to 50); Low (1 to 10)*

## A.7.2 Description of Risk Level

The table below describes the risk levels shown in the above matrix. This risk scale, with its ratings of High, Medium, and Low, represents the degree or level of risk to which an electronic voting system, facility, or procedure might be exposed if a given vulnerability were exercised. The risk scale also presents actions that senior management, the mission owners, must take for each risk level.

Risk Level	Risk Description and Necessary Actions
High	If an observation or finding is evaluated as a high risk, there is a strong need for corrective measures. An existing system may continue to operate, but a corrective action plan must be put in place as soon as possible.
Medium	If an observation is rated as medium risk, corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time.
Low	If an observation is described as low risk, it must determine whether corrective actions are still required or whether the risk can be accepted.

### Output from Step 7

The output from Step 7 is: Risk level (High, Medium, Low).

## A.8 Step 8: Control Recommendations

During this step of the process, controls that could mitigate or eliminate the identified risks, as appropriate to the organization's operations, are provided. The goal of the recommended controls is to reduce the level of risk to the electronic voting system and its data to an acceptable level. The following factors should be considered in recommending controls and alternative solutions to minimize or eliminate identified risks:

- Effectiveness of recommended options (e.g., system compatibility)
- Legislation and regulation
- Organizational policy
- Operational impact
- Safety and reliability

The control recommendations are the results of the risk assessment process and provide input to the risk mitigation process, during which the recommended procedural and technical security controls are evaluated, prioritized, and implemented.

It should be noted that not all possible recommended controls can be implemented to reduce loss. To determine which ones are required and appropriate for a specific organization, a cost-benefit analysis, as discussed in Section 4.6, should be conducted for the proposed recommended controls, to demonstrate that the costs of implementing the controls can be justified by the reduction in the level of risk. In addition, the operational impact (e.g., effect on system performance) and feasibility (e.g., technical requirements, user acceptance) of introducing the recommended option should be evaluated carefully during the risk mitigation process.

### Output from Step 8

The output from Step 8 is: Recommendation of control(s) and alternative solutions to mitigate risk.

## **A.9 Step 9: Results Documentation**

Once the risk assessment has been completed (threat-sources and vulnerabilities identified, risks assessed, and recommended controls provided), the results should be documented in an official report or briefing.

A risk assessment report is a management report that helps senior management, the mission owners, make decisions on policy, procedural, budget, and system operational and management changes. Unlike an audit or investigation report, which looks for wrongdoing, a risk assessment report should not be presented in an accusatory manner but as a systematic and analytical approach to assessing risk so that senior management will understand the risks and allocate resources to reduce and correct potential losses. For this reason, some people prefer to address the threat/vulnerability pairs as observations instead of findings in the risk assessment report.

### **Output from Step 9**

The output from Step 9 is: A Risk Assessment report that describes the threats and vulnerabilities, measures the risk, and provides recommendations for control implementation.

- From Black Box Voting Document Archive

- From Black Box Voting Document Archive -

## ATTACHMENT B: Glossary

Term	Meaning
BOE	Board of Elections
Context Diagram	Diagram that provides a graphical overview of the input/output connections between the DRE and external entities such as the BOEs and voters. The context diagram helps to define the scope of the voting system/process and becomes the top level of the analysis hierarchy.
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
Cryptographic Analysis	Analysis of the strength and methods of data protection using encryption and Cyclic Redundancy Checks.
DDoS	Distributed Denial of Service
DES	Data Encryption Standard
DoS	Denial of Service
DRE	Direct Recording Electronic voting machine
EMS	Election Management System
Exploitation Analysis	Analysis of how and by what means an attacker, if able to discover any weak points in the system, can use weak areas to attack the integrity of a DRE.
FEC	Federal Election Commission
GUI	Graphical User Interface
HAVA	Help America Vote Act of 2002
IDE	Integrated Drive Electronics
Impact Analysis	Analysis of the impacts that could occur if an attacker was able to use a DRE's weakness to affect an election.
IrDA	Infrared Data Association. IrDA ports enable the transfer of data from one device to another via infrared light waves instead of cables.
IT	Information Technology
ITA	Independent Testing Authority
LAN	Local Area Network
LAT	Logic and Accuracy Testing
LCD	Liquid Crystal Display
MB	Megabytes
MFC	Microsoft Foundation Classes
MHz	Megahertz
NIST	National Institute of Standards and Technology

OS	Operating System
Term	Meaning
PC	Personal Computer
PCMCIA	Personal Computer Memory Card International Association. PCMCIA cards (or PC cards) are small, credit card-sized devices that were originally designed for adding additional memory to personal computers. There are now several types of these cards for various uses.
PIN	Personal Identification Number
Reconnaissance Analysis	Analysis for the purpose of gaining information on potential ways that an attacker may be able to gain access to a system.
RAM	Random Access Memory
ROM	Read Only Memory
Smart Card	A small electronic device about the size of a credit card that contains electronic memory, and possibly an embedded integrated circuit.
SOCC	State of Ohio Computer Center
SOS	Ohio Secretary of State
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VPN	Virtual Private Network
WAN	Wide Area Network

## ATTACHMENT C: Documents Referenced

During this technical security assessment, Compuware requested technical documentation but received User Documentation. Compuware reviewed all available documentation relating to the system, its setup, storage, operations and maintenance. Compuware also used reference material for standards and smart card encryption. Following is a list of the documents that were reviewed during this technical security assessment.

File Name if Electronic	Document Title or Description
<b>Diebold</b>	
	FEC 2002 - Standard
Codeset files for AccuVote-TSX , Ballot Station Firmware version 4.5.1	
Codeset files for Key Card Tool version 1.0.1 zip.sda.exe	
Codeset files for Global Election Management System (GEMS) version 1.18.18	
	Smart Card Hand Book by Wolfgang Rankl 3 <sup>rd</sup> Edition
GEMS_1.18_Users_Guide_Revision_6.0.pdf	GEMS 1.18 User's Guide, Revision 6.0, Diebold Election Systems
BS GEMS User Guide.zip.sda.exe	GEMS User's Guide
Key Card Tool User Guide	
AccuVote-TSX Hardware Users Guide.pdf	AccuVote-TSX Hardware Users Guide, Revision 8.0
Ballet Station v4.5 User Guide.pdf	Ballet Station v4.5 User Guide Revision 2.0