Global Information Assurance Certification Paper

GIAC Certified ISO-17799 Specialist (G7799) Practical Assignment V 1.1

Implementing an ISO 17799 ISMS (Information Security Management System) for DRE (Direct Recording Electronic) Election Management System

Submitted by Brad P. Towers *CISSP, GCWN*
G7799 Practical Assignment, Version 1.1
SANS Fire Monterey, July 2004
Date Submitted: December , 2004

Executive Summary

The Independence County Auditor's Office requested that the County's Information Services Department develop an ISMS (Information Security Management System) for the electronic voting system utilizing the ISO 17799 standard. This paper provides an analysis of security controls, personnel interviews, as well as a documentation review. The focus of this project was to ensure that the controls in place by the Independence County Auditor's Office sufficiently mitigated the risks that are endemic to the election process using DRE's as well as comply with the ISO 17799 standard. Overall, the goal of this implementation is to measure the level of assurance that the security controls implemented by the Independence County Auditor's Office are fully formed, correctly implemented, and effective.

Part One: Defining the System

In terms of ISO 17799 a System can is defined as: “A collection of processes and procedures designed to accomplish a specific business objective.” In the case of Independence County, the “system” we will be working with and defined in our ISMS Scope is the “Election Management System”. When we speak of the election management system, we will be speaking of:

- The voter registration system.
  - How do County constituents register to vote?
  - How is the voter information maintained?
  - Who has access to it?
  - How is voter registration information introduced into the election management software
- The ballot creation system
  - Creating election and County specific ballots for each voting precinct, and the eligible voters within each precinct.
  - Introducing the ballots into the AVC Edge systems
- The vote casting systems
  - The vote casting system includes the DRE’s, as well as paper based “absentee” ballots.
  - Polling place voter reconciliation
- The vote tabulation system
  - The vote tabulation system includes counting the paper “absentee” ballots with an optical scanning solution.
  - Using an electronic reader to tally the DRE memory cartridges from each polling place.

Organization

Independence County is the second largest County in the state, with a population of over 730,000 citizens. The County maintains that approximately 350,000 of its citizen’s are registered voters. Of that 350,000, roughly 65% typically vote via an “absentee” paper ballot. The remaining voters vote on DRE’s at their designated polling place on the day of election.

Independence County is obligated by law, HAVA, (Help Americans Vote Act) to make sweeping changes in its election processes and procedures. The Help America Vote Act (HAVA) of 2002 was drafted in the aftermath of the controversial 2000 Presidential election. HAVA was signed into law on October 29, 2002. HAVA requires all states to implement major changes over the next two years.

The most significant and challenging of the new mandates include:

- replacing punch card voting systems currently used by a majority of voters;
- ensuring disabled voters have both secret ballots and access to the polls;
- implementation of a provisional balloting system;
- notifying provisional voters whether their ballot was counted;
- improving training of poll workers;

- educating voters about the process, their election choices, and their rights; including the right to a provisional ballot, the right to ask questions, and the right to get a new ballot to correct a mistake; as well as;
- ensuring that voters can review their ballots and correct any errors before actually casting their votes;
- creating a complaint procedure for voter grievances about the voting process.

Each of these new mandates could and in fact will be considered "business objectives" in our ISMS implementation. The Auditor of Independence County is an elected official. Within Independence County it is the office of the Auditor that is responsible for providing election related services such as voting, voter registration and general electoral services to County citizens.

Occasionally on Election Day, citizens will either arrive at the wrong polling location or not be listed as a registered voter in the poll workers books. In such cases as these, rather than turn away the citizens, the poll workers are instructed to allow the citizens to vote using a "provisional ballot". A "provisional ballot" is a paper-based ballot that is not actually counted until the County Auditors office has determined that the citizen is actually eligible to vote. Upon verification that the voter is eligible to vote in the election, the paper "provisional ballot" is counted via an optical scanning solution.

Current Information Security Posture

Currently, Independence County utilizes a decentralized approach to information assurance/security. Independence County's three branches (Executive, Legislative, and Judicial) comprise twenty-two departments providing various public services to citizens of the County. Of these twenty two departments, eight of them are led by elected officials. The Auditor department is one of the eight departments led by an elected official (The Independence County Auditor). There is no over-arching information security policy within the County. Traditionally, information security has been handled by each department independently. Within the last year however, Independence County has hired an information security manager reporting to the Director of the Department of Information Services (DIS). The information security manager has been tasked with, among other things, creating an over-arching information security program within the County. In addition to the creation of an information security policy, the information security engineer has identified the need for an information classification policy.

Much of the data within the County is considered public and therefore the negative impact to the organization would be minimal should the information be inadvertently or maliciously released. However, there are many departments and instances where the data is in fact not public. It is just this type of situation that creates additional challenges from an information security perspective. Additionally, while the information may technically be "public information", it is not considered public unless there is a formal public disclosure request. Until that time, the County must act with all due care to protect the Confidentiality, Integrity, and Availability of its informational assets. Also, while voter registration information is by law, public, the actual vote cast and recorded by an individual is not public record. The general culture and mindset of long-time County

employees is that “all of the information we deal with is public, therefore we don’t have a need to protect it”. This is a fallacy that needs to be changed.

As mentioned earlier, the Independence County Auditor’s Office requested that the County’s Department of Information Services review the security controls surrounding the election management system, as implemented by County elections officials. DIS was asked to develop possible recommendations to improve the security and sanctity of the elections process. The new information security manager feels the best solution is to develop an ISMS (Information Security Management System) for the election management system utilizing the ISO 17799 standard.

Voting is a fundamental right that we have enjoyed in this Country for hundreds of years. Along with that right, we have long held the expectation that our voting preferences would, or could remain private. However, for many Americans (such as those with visual or auditory impairments) that was not the case. These citizens required assistance in order to cast their vote, thus revealing to someone their voting preference. One component of HAVA was to eliminate the need for this assistance by disabled voters, ensuring they have access to election polls as well as the ability to cast their ballot secretly. DRE’s provide this ability for disabled voters. DRE’s however, are not without their opponents, those who believe that the introduction of electronic voting and recording are a threat to our democratic way of life.

System Details

The DRE’s that Independence County is utilizing is the Sequoia Voting System. The Sequoia voting systems comprises the following components:

- AVC Edge Version 4.1 D
- WinEDS Electronic Management Software Version 2.6
- Card Activator Version 4.2

The AVC Edge is a Touch-Screen Voting System, with a touch-screen monitor, utilizing large typeface. Navigation within the ballot is accomplished with scroll buttons to move forward and backward, and the Contest Box which enables voters to move to any part of the ballot. Voters can review their selections and change their vote at any time before they cast their official ballot. The AVC Edge prevents the voter from overvoting, (that is; casting an official ballot more than once) notifies the voter of undervoting, (When a voter does not cast a vote for all candidates that the voter is eligible to vote for) and allows the voter to review and modify their ballot choices before casting their vote.

In order to ensure HAVA compliance, wheelchair bound voters are accommodated by adjusting the screen's height. The Audio Voting feature allows the AVC Edge to serve blind voters and people who have difficulty reading. Ballots in multiple languages are available on the AVC Edge, allowing a voter to simply choose the preferred language on the first screen. The ballot is then presented in that language until the voting process is complete.

The AVC Edge is supported by the BPS (ballot processing software/system) and the WinEDS election management software, which provides ballot creation, vote tabulation, and reporting.

Both the BPS system and the WinEDS election management software are installed on separate "stand-alone" computers within the confines of the Independence County Auditor's Office. The Independence County Auditor's Office and the election officials use BPS to create the ballot definitions and ballot "styles" that are loaded into the WinEDS and AVC Edge system.

Voter registration data is stored in a separate system known as DIMS (Data Integrity Management System). The voter registration data is manually input into the system by County Auditor's personnel. The WinEDS system is used to create the"election database." This creates the Independence County-specific election type.

Once the ballot definitions are loaded into the AVC Edge, the election officials within Independence County begin the "Logic and Accuracy Testing" (L&A). Upon successful completion of the L&A, each AVC Edge system is secured with seals that are attached to the back of the machine. These seals are used to lock the power controls as well as the compartment housing the PCMCIA cartridge. Each seal is uniquely identified and auditable. The AVC Edge systems are then distributed to the polling locations on the eve of Election Day by Independence County election officials. Upon successful verification of the seals, poll workers and volunteers will open and set up the AVC Edge on Election Day for voting.

No part or component of the Election Management System is connected to any external network. The system acts completely independently within the context of ballot creation, casting, and tallying. No ballots or voter information is transmitted across a network, neither via a modem, nor any form of wireless communications mechanism. Physical access of the entire voting system is under the control and observation of Independence County personnel and their designees (poll workers, poll inspectors, volunteers, etc.) at all times.

Part Two: Plan

The implementation of an ISO 17799 ISMS involves twelve steps that can be distilled down to four distinct phases. These four phases are: PLAN, DO, CHECK, ACT. Our ISMS of the election management system will follow these four phases as we go through the necessary twelve steps.

ISMS Plan

Identify the Problem

Prior to actually defining the Scope of our ISMS, we need to identify what problem or problems we are trying to solve through the implementation of ISO 17799. In fact, there are several problems that we have to deal with regarding the election management system.

The first problem we will identify is the lack of a comprehensive security program surrounding the system. While there are numerous controls implemented by the Independence County Auditor, there is no all-inclusive security program in place. The focus of this project is to help alleviate that problem. With a comprehensive security program in place, including Security Awareness Training for all County employees, the necessary policies, procedures, and guidelines approved and published, a data classification scheme, we will be able to ensure we have solved this problem.

The second problem we will be working with is the potential alteration of election data as votes are cast on the DRE's. When citizens cast their vote using DRE's, they need to be assured that the vote they cast cannot easily be altered to redirect their vote to an alternate candidate.

The final problem that needs to be identified with regards to electronic voting is the "public perception" surrounding the security of electronic voting and DRE's. While not necessarily a problem that can be solved or quantitatively measured, it is believed that through a thorough ISMS implementation, we will actually be able to help ease the fears many constituents have of DRE's. This problem is one that will be very difficult, if ever possible to solve or measure our progress on. The true believers, those that feel that DRE's and electronic voting are a threat to our Democracy, will never be easily dissuaded.

In our next step *Analyze the Problem;* we will discuss each of these problems in more detail, decomposing the processes surrounding each in our effort to identify the "*root causes*".

Analyze the Problem

Independence County is in the early stages of creating a formalized information security program. For instance, currently the County has few formalized policies and procedures for responding to security issues and/incidents. The information security manager is working on the creation of a Security Awareness Program for all County employees. This will give County employees the ability to identify what is a security incident, as well as how to report when a security incident is occurring. The Security Awareness training will also educate the employees as to the impact that each one has on information assurance within their department, as well as the County at large. Without any form of security awareness training it is difficult to expect County employees to adhere to new security policies and procedures.

The information security manager is also working on a data classification scheme. As was discussed earlier, many County employees are under the mistaken impression that all of the information handled within the County is public information, therefore the need for information security is non-existent. A data classification scheme would identify that information which would require a higher level of care when handling. Information officially classified as Public would require fewer controls when handling. Data that is not quite ready for public consumption; would require more controls, and a higher level of care when handling.

In addition to the data classification scheme, work is in progress on the creation of a "high-level" security policy. This "high-level" policy will require the creation of a security committee comprised of several departmental Directors, members of the County Council, as well as the County Executives office. The main focus of this committee will be to identify the overall business objectives of the various departments and provide the necessary upper management direction and support for adoption of the security policies.

The next problem that needs to be analyzed is the potential alteration of election data. As citizens vote for their candidate of choice, they need to have the assurance that their vote will actually be counted, AND it will be counted for the candidate/party they intended. The perception among DRE opponents is that we don't know, with 100% certainty, that the votes cast are actually being counted as expected. DRE's are considered, by their opponents, to be "black boxes" whose inner workings are hidden from public scrutiny, and consequently cannot be trusted. Therefore we (America collectively) should not be using them.

For hundreds of years our society has relied upon machines and/or computers to perform tasks that were considered boring, or impossible for humans to perform efficiently. Many of these systems have the capacity to seriously alter or take human life. Americans rely on computers to execute complex medical procedures, perform large-scale financial transactions, and guide aircraft safely through the skies of our airspace while transporting hundreds of thousands of people daily.

The argument that, because a machine contains code that is not available to all for public scrutiny it should NOT be used, is an inherently flawed argument. Perfection (100% accuracy) of computer systems is never required or even expected in any system used today. With the appropriate safety procedures and security controls in place, the expectation is that risk will be reduced to an acceptable level. The Federal Election Commission (FEC) standard 3.2.1, allows a maximum error rate of 1 in 500,000 voting positions. Assuming a typical ballot size of 235 positions, this would be an allowed error of almost one in every 2000 ballots, or 0.2% of the vote.
Also, voters have a choice, that is, they are not required to use DRE's. A voter who chooses to avoid voting machines may opt to cast a paper ballot at their polling place, or cast their vote via an absentee ballot.

Now that we have identified and analyzed a few of the problems with the system, we need to identify the scope of the system we will be working with.

ISMS Scope

The *scope* for our ISMS here is the election management system. As was defined earlier in our plan, the election management system is comprised of the following:

- The voter registration system DIMS. (Data Integrity Management System)
- The ballot creation system BPS (Ballot Processing Software/System)
    - The Independence County Auditor's Office and the election officials use BPS to create the ballot definitions and ballot

"styles" that are loaded into the WinEDS and AVC Edge system.
- The vote casting systems
  - The AVC Edge is the defined vote casting system for Independence County.
- The vote tabulation system
  - The WinEDS Election Management software, which provides ballot creation, vote tabulation, and reporting.

Now that we have defined what is included in the scope of our ISO 17799 ISMS, we need to specifically define what is out of scope.

Out of Scope
In this ISMS, there will not be and attempt to justify the existence of the DRE's and the movement toward electronic voting. This is a legal issue that the County is forced to comply with. What we will be doing is ensuring that the election management system as defined earlier applies the necessary controls for ISO 17799 compliance. What is NOT included in the scope of this project is a technical review of any source code of any part of the election management system. Currently, Sequoia, like all of the makers of DRE's, maintains a "closed source" system. That is; the source code is reviewed by an external organization (that is certified by the Federal Elections Commission) and held in escrow. The source code is not "open source", thus not readily available to all.

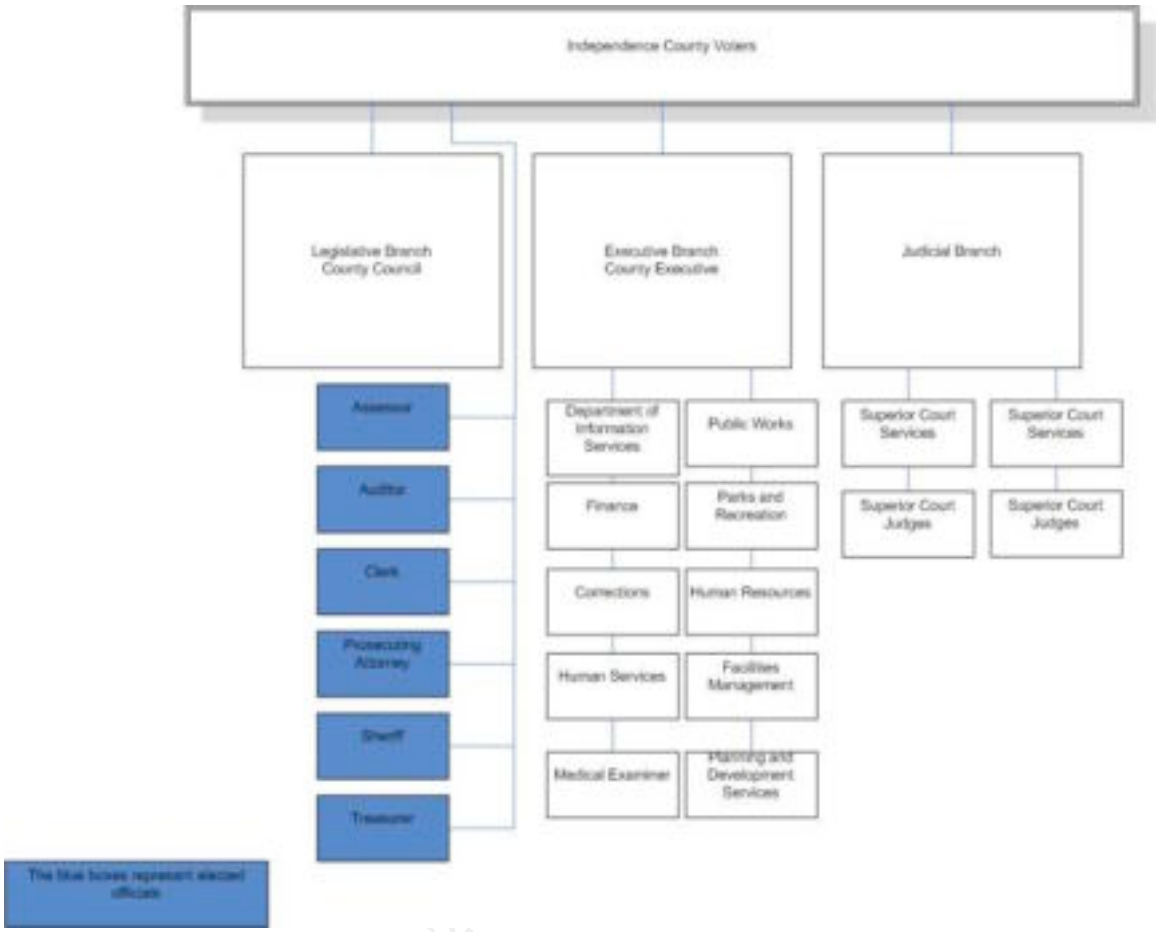
Project Plan
The implementation plan for our ISMS will be utilizing a phased approach. Below is the table that outlines our phases and the steps within each phase.

Phase	Actions	Deliverables
1	Identify ISMS need	The first task we need to do is; identify the need and establish the importance of an ISMS implementation.
2	Define the Scope	We must identify all systems and business processes that will be covered with our ISMS implementation.
3	Identify and define "business objectives"	While it is understood that Independence County is not a private "for profit" business, the objectives of each department need to be clearly defined. In our case, we need to identify and document the business objectives of the Auditors office, and the elections division in particular.
4	Policy Creation	The Security Committee will have a High Level Security Policy to create. From this policy, management's intent and

		expectations with regards to Information Security will be defined.
5	Asset Identification	Independence County must identify and classify all assets that included in the ISMS. All assets must also have the sensitivity defined. We will not be looking necessarily at how secret the information is, but how important is it to the business processes defined in our scope.
6	Risk Identification	Perform a risk analysis on all assets identified in the previous step.
7	Risk Management Plan	Creation of a "treatment plan" for all risks documented during the risk analysis.
8	Implementation Plan	Creation of plan for implementing the necessary controls to mitigate risks identified during phase 6.
9	Statement of "Exclusion"	Create documentation outlining specifically what was excluded from our Election Management System ISMS and WHY certain systems/processes/procedures were excluded.
10	Monitor, Maintain, & Improve	Create the necessary processes to monitor, maintain and possibly improve the ISMS as changes are made, or new risks identified.

Management Structure, Support, and Approval

Independence County is comprised of the three branches of government (Judicial, Legislative, and Executive) with the Department of Information Services (DIS) residing under the Executive branch. The Director of DIS is appointed by and directly reports to the County Executive. DIS however, provides information services and resources to all three branches of government. Below is a County wide organization chart, below that is an organizational chart for DIS, showing more detailed infosec responsibilities. At this time, there is only one person the, Information Security Manager (ISM), who is responsible for Infosec in the County. The expectation is that as the ISM creates the formal security program across the County, and as more departments are aware of the role, the work will become more than a single person is able to handle. At that time, DIS will begin to create a new Information Security division, bringing on the appropriate personnel to manage Infosec.

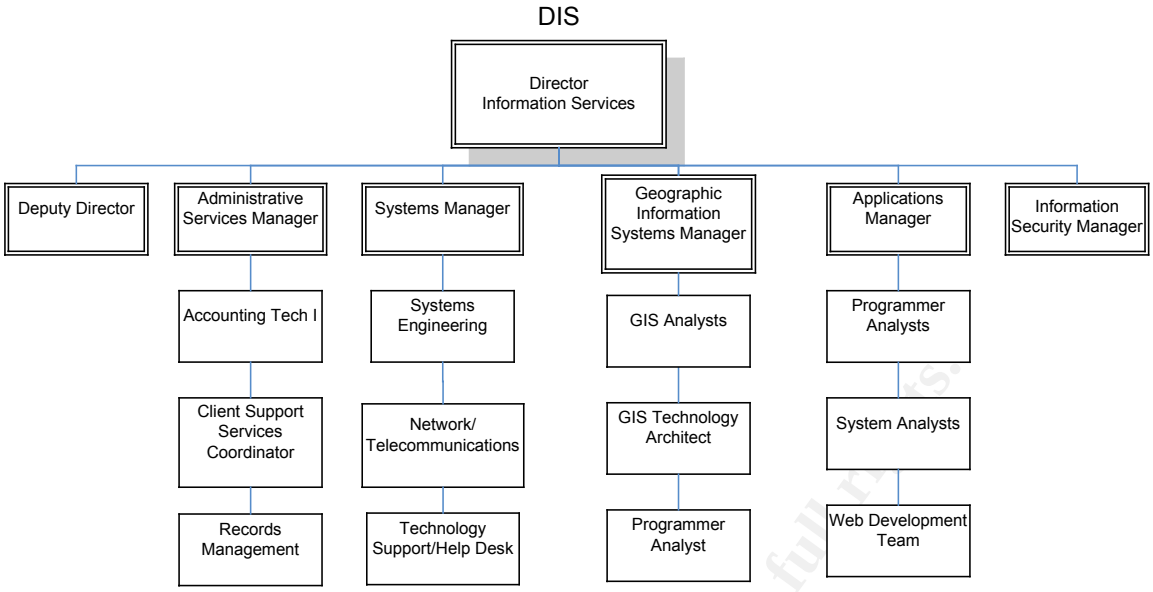


Within the Department of Information Services (DIS) there are three divisions reporting up to the Director of DIS. Information Security is represented by the new Information Security Manager (ISM). Prior to the hiring of the Information Security manager, there were no full time employees whose sole focus was Information Security. The information security manager reports directly the Director of DIS. The information security manager was aligned directly under the DIS director due to the nature of Infosec.

Information security not only extends across each of the three divisions identified below, it stretches across the entire County, reaching all departments in some way or another.

Below is the organizational chart for the Department of Information Services.

Independence County



Security Committee

To best ensure that the policies written would be adopted and implemented, the Information Security Manager worked directly with members from the Executives office, as well as members of the County councils office. The DIS director proposed the creation of an "Information Services Board" made up of the County Executive, the Deputy Executive, the eight members of the County council and several County departmental Directors. The "Information Services Board" will be responsible for the oversight of all IS projects that encompassed more than two County departments. The board will meet once a quarter to discuss the status of the projects.

Because Information Security is one issue that reaches across boundaries and departments, the general consensus is that a "security committee" should be created. The security committee will be made up of Directors and Managers from the various departments across the County.

The first task given to the security committee was the creation of several information security policies. Given that committees tend to oftentimes work in perpetuity unless there is an external motivator of some sorts, a deadline was created for the first policy. The security committee was told that within eight weeks of their first meeting, they must have a "High Level Security Policy" (HLSP) statement created. Below we will see the framework and a few of the guiding principles used by the security committee during this process.

Security Policies

As mentioned earlier in this document Independence County has no overarching information security policy. In undertaking the creation of an Information Security framework, including the necessary policies and procedures, the Security Committee will be utilizing the following framework.

Security Policy Framework

Policy Recommendations

County upper-level management must take a proactive role in supporting and providing enforcement for security policies. Without sufficient management level support, security will not be seen as important and critical to the continued success of Independence County. The management level must set the value of information to the organization and commit to its protection.

The following should be considered when developing security policies:

- The policies should not put excessive restrictions on operations and employees;
- The organization must be serious about security and provide enforcement mechanisms;
- The organization must be quick to develop and implement security policy without excessive delay of new program or service delivery.

Phase 1

Two critical aspects of Independence County's security policies will be to clearly define the County assets and appropriate uses of Independence County's information systems to the entire organization. The County assets must include tangible and intangible assets. In order to hold employees accountable for their actions and to have effective enforcement mechanisms, employees must clearly understand what behaviors and use are acceptable or unacceptable. Without a clear definition of what inappropriate behavior is, employees cannot realistically be held accountable. Base security architecture policies should be written and published for the following:

- County Assets, Resources and Expected Level of Privacy;
- County Authority and Responsibility Policy;
- Acceptable Use of County Assets and Resources;

These three policies are the base architecture for the remaining policies, because they will provide a definition of all assets and resources belonging to Independence County, who is responsible for what actions, and what the appropriate uses are of those assets.

Phase 2

From the three base policies, the following can be added on for a complete set of Independence County security architecture policies:

- Record Retention and Information Management Policy;
- System Surveillance Policy;
- Disaster Recovery and Business Resumption Policy;
- Public Information and Media Policy;
- Third Party/Partner Access Policy.

Phase 3

Once the County level security policies are in place, then Information Technology and Communications & Network Services can take over to create a more detailed set of security architecture policies. These policies have to be supported by management and highly visible, but are the responsibility of DIS. Some of the following policies have been started, but are not formally published:

- Account and Password Policies;
- Access Control and Authorization Policy;
- Remote Access Policy;
- Anti-Virus Policy;
- Change Management;
- Media and Material Disposal Policy;
- Incident Handling Guideline;
- TCP/IP and Other Protocols Policy.

Phase 4

Once the base set of security policies are in place, then the security procedures supporting these policies can be written, published, and implemented. The procedures should be owned by individual departments responsible for the various activities. These documents will expand as new technologies and software are implemented within the Independence County environment. This phase will take the longest to develop and implement, due to the individual department responsibilities. The following is an example list of security procedures and best and standard practices:

- Password management, protection, reset, and change on all devices;
- Account Addition, Change, Deletion, and Reset Procedures;
- Group Addition, Change, and Delete Procedures;
- Administrative Account Security and Access Control Procedures for all devices;
- Windows 2000/2003 Server Installation, Administration, and Security;
- HP-UX Server Installation, Administration, and Security;
- Business Continuity;
- Incident Handling;
- Information and Media Disposal;
- Desktop/Laptop Installation, Administration, and Security;
- Remote Access Installation, Administration, and Security;
- Gateway Installation, Administration, and Security for each of supported installations, for example:

  - Cisco Pix;

- Checkpoint Firewall-1;
- NetScreen
  - Individual Application Installation, Administration, and Security, for example:
- Anti-Virus;
- SecuRemote;
- SecureCRT;
  - System and Audit Log Procedures;
  - System Monitoring Procedures;
  - Access Control Procedures;
  - NSOC Operational Procedures.

Definitions

Best Practice	A combination of high level statements and operational steps that are recommended for proficiency.
Guideline	An outline of a policy, conduct, or procedure.
Policies	High level statements intended to provide guidance to those who must make present and future decisions. Policies can be thought of as generalized requirements on which management should focus attention. Policies typically include general statements of goals, objectives, beliefs, ethics, and responsibilities. Policies are often implemented or enforced by the general means for obtaining these things, such as procedures. (Reference 1)
Procedures	Specific operational steps that employees must take to achieve a certain goal. A policy describes only the general means for addressing a specific problem. A procedure provides the solution. For example, a policy may state that all router access must be authenticated. This states what should occur. A procedure will provide the solution for authentication. This states how it occurs. (Reference 2) Standard or Best Practices can be part of procedures.
Standard Practice	A combination of high level statements and operational steps required for proficiency.

High-Level Security Policy Statement

Currently, the security committee is on the “phase 1” policies.
The following policy is the “high-level security policy” that the security committee created, and will be working from as they create the issue and department specific security policies.

Information Security Policy

1.0 Overview
Independence County's intentions for publishing an Information Security Policy are not to impose restrictions that are contrary to Independence County's established culture of openness, trust and integrity. Management is committed to protecting Independence County's employees, partners and the County from illegal or damaging actions by individuals, either knowingly or unknowingly. Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of Independence County. These systems are to be used for business purposes in serving the interests of the County, of our citizens and customers in the course of normal operations. Please review Human Resources policies for further details. Effective security is a team effort involving the participation and support of every Independence County employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2.0 Purpose
The purpose of this policy is to outline Executive Managements commitment to Information Security. These rules are in place to protect the employee and Independence County.

3.0 Scope
This policy applies to employees, contractors, consultants, temporaries, and other workers at Independence County, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Independence County.

4.0 Policy
"Information and information systems are critical and vitally important Independence County assets. Accordingly, Independence County management has a fiduciary duty to preserve, improve, and account for Independence County information and information systems. This means that Independence County management must take appropriate steps to ensure that information and information systems are properly protected from a variety of threats such as error, fraud, embezzlement, sabotage, terrorism, extortion, industrial espionage, privacy violation, service interruption, and natural disaster.

Independence County information must be protected in a manner commensurate with its sensitivity, value, and criticality. Security measures must be employed regardless of the media on which information is stored (paper, overhead transparency, computer bits, etc.), the systems which process it (microcomputers, firewalls, voice mail systems, etc.), or the methods by which it is moved (electronic mail, face-to-face conversation, etc.). Such protection includes restricting access to information based on the need-to-know. Management must devote sufficient time and resources to ensure that information is properly protected."
5.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6.0 Definitions
Term Definition

7.0 Revision History

Area to be addressed:
ISO 17799 3.1.1 Information security policy document
"A policy document should be approved by management, published and communicated, as appropriate, to all employees. It should state management commitment and set out the organization's approach to managing information security."

County Asset Policy

Purpose

All Independence County tangible and intangible assets and resources are the property of Independence County and are subject to auditing, monitoring, and logging.

Scope

This corporate assets policy governs the responsibility and expected level of privacy of company assets and resources on Independence County property and connected to the Independence County network.

This policy applies to all employees, contractors, consultants, temporaries, and other workers at Independence County, including those workers affiliated with third parties who access Independence County computer networks. Throughout this policy, the word "user" will be used to collectively refer to all such individuals. The policy also applies to all computer and data communication systems owned by and/or administered by Independence County.

The following is a basic, but not inclusive, list of Independence County assets: hardware, software, data, people, documentation, supplies, intellectual property, client and community information. Assets are owned by Independence County. Personnel do not have privacy in the use of the assets.

Items brought onto Independence County property will be considered an extension of an Independence County asset, unless specifically identified as the property of other parties, and subject to auditing, monitoring, and logging by Independence County.

Electronic and non-electronic data and information range from voice-mail, email, faxes, telephone, computer data and transmissions to documents, drawings, and notes. When this data or information is stored on, maintained by, or transmitted on Independence County assets, it becomes an Independence County asset and is subject to auditing, monitoring, and logging by Independence County;

Connections to Independence County assets are subject to auditing, monitoring, and logging by Independence County.

Responsibility

All assets, data, and information should have a defined owner.

Asset Owner Security Responsibilities. The asset owner is the individual responsible for asset protection. The following is the list of security responsibilities that are required of each asset owner:

- The asset owner is responsible for defining the criticality of the asset and the level of security required to protect it. This is determined by performing a business impact analysis of the critical functions as determined within the Asset Criticality Guidelines;
- The asset owner works with other personnel to ensure the correct security options are developed and properly implemented;
- Each asset owner is an access authorizer, an approver, for approving asset access;
- Each asset owner is responsible for ensuring the development and on-going support of an asset Disaster Recovery Plan;
- Each asset owner is responsible to see that losses and other security incidents are reported to the accountable manager and take appropriate action to ensure that such incidents are properly resolved.

Data Owner Security Responsibilities. All data should have a defined owner to ensure accountability for its accuracy, integrity, and appropriate use of data contained on the server. Sensitive data must be protected against accidental or unauthorized disclosure, modification or destruction. The following is the list of security responsibilities that are required for each data owner:

- The data owner determines the sensitivity and criticality of the server data. Sensitivity is the degree of confidentiality. Criticality is the impact on the organization, should the data be unavailable.
- The data owner determines the security controls that are to be placed on the data, and communicate those controls to the administrator. Security measures must meet the minimum security requirements outlined in the Asset Criticality Guidelines;
- Each data owner is an access authorizer and approver, for approving resource access to the data;
- The data owner is responsible for maintaining and reporting data access authorization documentation. This document should be reviewed with the server owner and administrator. The data owner is responsible for ensuring that the authorization access is current;
- The data owner determines the data retention requirements of the data. The file and data backup requirements need to be aligned with the data retention requirements and policy.

Support Personnel Security Responsibilities: The following is the list of security related support personnel responsibilities that each person performs:

- Works with customer (asset owner and data owner) to understand security requirements;

- Works with customer (asset owner and data owner) to develop and maintain a server Security Plan that defines all processes needed to ensure adequate security is established and maintained and identifies appropriate user accesses to the asset and data as determined with the customer;
- Establishes security for the administration of the asset prior to implementation and use, including appropriate account access, technical support access capability, as well as backup/emergency support;
- Sets up security on the asset or data prior to implementation to ensure that access is controlled and backup is kept in locked areas or offsite storage, if appropriate;
- Regularly monitors asset and data access activity to identify any unauthorized access as well as maintain a history file for auditing purposes and reports any suspicious activity;
- Works with the asset and data owner in preparing the Disaster Recovery Plan.

User Security Responsibilities: Users do not own accounts or space on the Independence County assets, but are granted the privilege of use. Users should take appropriate measures in protecting sensitive information and applications. The following is the list of security related data personnel responsibilities that should be conveyed to each data users performs for the environment:

- Responsible for ensuring that adequate precautions are able to protect assets;
- Responsible for their own actions within the environment;
- Responsible for reporting inappropriate activity to management that they may become aware of in the course of executing their duties.

Violations

Misuse, irresponsibility, unauthorized access, disclosure, duplication, modification, diversion, destruction, loss, or theft of any Independence County asset by users, willingly and deliberately, may result in the loss of computer and/or network resources up to and including termination and legal prosecution.

Area to be addressed:
ISO 17799 5.1 Accountability for assets
All major information assets should be accounted for and have a nominated owner. Accountability for assets helps to ensure that appropriate protection is maintained. Owners should be identified for all major assets and the responsibility for the maintenance of appropriate controls should be assigned. Responsibility for implementing controls may be delegated. Accountability should remain with the nominated owner of the asset.

Acceptable Use Policy

The policy below outlines acceptable use of County resources, specifically the Internet, and e-mail. This policy was taken from SANS Institute "Information Security Policy Project". The format for all department specific policies will be very similar, if not identical to the policy outlined below.

Independence County Acceptable Use Policy

1.0 Overview

The Department of Information Services intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to Independence County established culture of openness, trust and integrity. DIS is committed to protecting Independence County's employees, partners and the County from illegal or damaging actions by individuals, either knowingly or unknowingly. Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of Independence County These systems are to be used for business purposes in serving the interests of the County, and of the citizens of Independence County in the course of normal operations. Please review Human Resources policies for further details.

Effective security is a team effort involving the participation and support of every Independence County employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2.0 Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at Independence County. These rules are in place to protect the employee and Independence County. Inappropriate use exposes Independence County to risks including virus attacks, compromise of network systems and services, and legal issues.

3.0 Scope

This policy applies to employees, contractors, consultants, temporaries, and other workers at Independence County, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Independence County

4.0 Policy

4.1 General Use and Ownership

1. While Independence County's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the County systems remains the property of Independence County. Because of the need to protect Independence County's network, management cannot guarantee the confidentiality of information stored on any network device belonging to Independence County.
2. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible

for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.

3. For security and network maintenance purposes, authorized individuals within Independence County may monitor equipment, systems and network traffic at any time, per DIS's Audit Policy.
4. Independence County reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 Security and Proprietary Information

1. The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or not confidential, as defined by County confidentiality guidelines, details of which can be found in Human Resources policies. Employees should take all necessary steps to prevent unauthorized access to this information.
2. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System level passwords should be changed quarterly. User level passwords should be changed every eighty-nine days. User will NEVER be asked for there passwords by DIS employees or their representatives.
3. All PCs, laptops and workstations must be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off (control-alt-delete for Win2K users) when the host will be unattended.
4. Use encryption of information in compliance with DIS's Acceptable Encryption Use policy.
5. Postings by employees from a Independence County email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Independence County, unless posting is in the course of business duties.
6. All hosts used by the employee that are connected to the Independence County Internet/Intranet/Extranet, whether owned by the employee or Independence County, shall be continually executing approved virus-scanning software with a current virus database.

4.3. Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).
Under no circumstances is an employee of Independence County authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Independence County-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Independence County
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Independence County or the end user does not have an active license is strictly prohibited.
3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
5. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
6. Using an Independence County computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws.
7. Making fraudulent offers of products, items, or services originating from any Independence County account.
8. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
10. Port scanning or security scanning is expressly prohibited unless prior notification to DIS is made.
11. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
12. Circumventing user authentication or security of any host, network or account.
13. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
14. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

15. Providing information about, or lists of, Independence County employees to parties outside Independence County.
16. Using County resources to conduct any form of personal for profit business.

Email and Communications Activities

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within Independence County's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Independence County or connected via Independence County's network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

5.0 Enforcement
Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6.0 Definitions

Term	**Definition**
Spam	Unauthorized and/or unsolicited electronic mass mailings.

7.0 Revision History

Area to be addressed:
ISO 17799 9.4.1 Policy on use of network services
A policy should be formulated concerning the use of networks and network services.
ISO 17799 8.7.5 Policy on acceptable use of electronic office systems

Risk/Threat Identification

There are many approaches to performing a risk analysis. However most can be broken down into one of two types: quantitative and/or qualitative.

A quantitative approach depends on two primary elements;
1. The probability that a specific event will occur
2. The expected recovery cost, should it occur.

Based upon these two events, a single “number” is created. This number is known as the “Annual Loss Expectancy” or ALE. Loss multiplied by Probability equals ALE.

A qualitative risk analysis uses a number of interconnected elements: Threats, Vulnerabilities and Controls. A threat is defined as “the potential for a particular threat source to successfully exercise a particular vulnerability.” A vulnerability is a weakness that can be accidentally triggered or intentionally exploited. A Control is a countermeasure for vulnerability exploitation. It should be noted that 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, and existing or potential controls.

Our next step was to identify possible risks/threats to the election management system. The Threat and Risk Assessment methodology used was based upon the methodology documented and published by the National Institute of Standards and Technology (NIST). Specifically, SP 800-30, *Risk Management Guide for Information Technology Systems.*

During our analysis of the election management system, Independence County Information Services, in conjunction with the Auditor’s Office identified potential threats directed toward the election management system.

The table below outlines our findings:

Threat Source	Motivation	Actions
Hacker	Challenge Ego Notoriety	Hacking the DREs Social Engineering Unauthorized access
Computer Criminal	Illegal disclosure of information Monetary gain Data Alteration/Destruction	Computer Crime (Identity Theft) Information Bribery System Intrusion
Terrorist	Blackmail Destruction Exploitation Revenge Political Motivations	System Attack System Penetration System Tampering
Political Entities	Competitive Advantage Political Espionage Alteration of Election outcome	Information Theft Social Engineering System Penetration Unauthorized system access
Insiders	Curiosity Ego Intelligence Ignorance (unintentional errors) Revenge Political motivations	Browsing of confidential information Computer abuse Fraud Theft System Sabotage Input of false information Information alteration

Vulnerability Identification

In attempting to analyze the threats to the election management system or the voting process in general, one must include an analysis of the potential vulnerabilities associated with the environment. In our analysis, we were looking for potential vulnerabilities associated with the threats identified in the previous section.

Vulnerability	Threat Source	Threat Action
Alteration of the election data	Insiders, Hackers, Political entities, Computer criminals	Unauthorized users connecting to and altering data during election creation process.
Information alteration	Insiders, Hackers, Political entities	Modification/Alteration of the election ballots.
Tampering with the AVC Edge systems	Hackers, Political entities, Computer criminals	Unauthorized users attempting to access the systems and alter the "counting code."
Tampering with the AVC Edge systems after the LAT testing	Hackers, Political entities, Computer criminals	Unauthorized users attempting to access the systems and alter the "counting code."
Attempting to load malicious code into the AVC Edge	Hackers, Computer criminals	Using the "voter activation card" to load a bug, virus, or other malicious code into the system.
Multiple voting for a single user	Political entities, Computer criminals, Hackers	A single user attempting to vote multiple times using a single voter activation card, or introduction of a counterfeit card.
Alteration of the recorded votes on the election cartridges prior to counting	Hackers, Computer criminals, Political entities	Connecting to the AVC Edge systems in an attempt to alter the votes cast, prior to official vote count.
Application Tampering	Hackers	Exploitation of a known vulnerability in a commercial application used in the election process.
System sabotage	Hackers, Computer criminals, Political entities	Accessing supervisory function during an election process, and tampering with the vote process.
Data tampering	Hackers, Computer criminals, Political entities	Modification of the ballot data.
Data theft	Hackers, Computer criminals, Political entities	Downloading of data prior to official count in order to determine election outcome.
System attack	Hackers, Computer criminals, Political entities, Insiders,	Disruption of election process via tampering of AVC Edge systems.
Information Theft	Insiders, Hackers, Computer criminals	Theft of confidential voter information stored in Voter Registration System.

Controls Analysis

Prior to implementation of the Election Management System DREs, Independence County embarked on a coordinated effort to train all election officials and board workers. This training included basic information security awareness and education, operational policies and procedures. **ISO 17799 Sections 6.2.1, 8.1.1** All elections officials, County Auditor personnel, and volunteer poll workers received detailed training on the policies and procedures to follow should an anomaly arise during an election.

The Independence County Auditor's Office, along with the Information Security Manager has designed the system and implemented the following controls in order to safeguard the sanctity of the election process. Many of the controls are in line with and comply with ISO 17799, however, several of the controls have no equal in the 7799 standard, and were implemented as a matter of due care.

1. Data from the DIMS (Voter registration database) server is input into the BPS Software via a USB token drive. This USB token drive is physically under the control of elections' personnel at all times. Elections personnel have strict policies that must be followed to maintain the integrity and security of the USB token drive while in transit. **ISO 17799 Section 8.7.2**

2. The WinEDS system is used to create the "Election Database." This creates the Independence County-specific election type. This system is on a stand-alone server with NO network connectivity. The system is in a physically secure area of the Independence County Auditor's Office. Auditor's personnel are the only employees allowed beyond a manned reception desk, once behind the reception area, only elections officials within the Auditors office have access to the locked room where the WinEDS server is located. Access to the room is controlled via a proximity switch lock. **ISO 17799 Section 7.1.1, 7.1.2, 7.2.1**

3. Each touch-screen AVC Edge system is a stand-alone unit and is not networked in any way with any other system. **ISO 17799 Section 8.5.1, 9.6.2**

4. The Logic and Accuracy Testing (L&A), performed by the Independence County Auditor's staff, is done to ensure that each system is accurately recording the votes that are cast on the touch screen.

5. Upon successful completion of the L&A, each AVC Edge system is secured with seals that are attached to the back of the machine. Each seal is uniquely identified and auditable.

6. If a machine is found unlocked or otherwise tampered with, poll workers are instructed to NOT use that particular machine during election set up. The machine is set aside, and examined once the election process is complete.

7. Once the Voter Activation Card has been activated by poll workers, the activation time for that card is set to fifteen minutes before the card is automatically deactivated. Once deactivated, the user will NOT be allowed to vote via the DRE's. When the voter presents a deactivated card to a poll worker, the voter is given a "provisional ballot" to vote with. These "provisional ballots" are not counted until the end of the election, and the polling place voter reconciliation is completed.

8. At the close of election, NO ballot/vote information is transmitted via modem, facsimile, network, or wireless transmission. **ISO 17799 Section 8.5.1, 8.7.7, 9.6.2**

9. The vote tabulation software and hardware at the central counting center is also on a stand-alone network that is not accessible via the County network, or the Internet. **ISO 17799 Section 8.5.1, 9.6.2**

10. None of the systems that together create the electronic voting and tabulation system are accessible via the Internet, or from the Internal Independence County network. **ISO 17799 Section 8.5.1, 9.6.2**

11. All access to the software and systems is password protected. Only authorized poll workers have access to these passwords. Each authorized poll worker has signed a confidentiality agreement, agreeing to keep the passwords confidential at all times. **ISO 17799 Section 9.2.3**

12. After the polls close, at each polling place a reconciliation is made of the number of votes counted, to the number of voters who signed poll books. As part of this reconciliation, the number of registered voters in a particular precinct is compared with the voter numbers voting in the actual election.

13. Physical access to the AVC touch-screen voting devices, as well as the voter activation cards and system, will be strictly controlled and monitored by the board workers at each polling place. Access to the supervisory functions of the AVC Edge is controlled via the back of the machine. ONLY authorized board workers, poll workers will be allowed to access these supervisory screens. **ISO 17799 Sections 7.1.1, 7.1.2**

Platform Analysis

1. The supervisor screen does not have the function to change the vote results, alter the ballot or ballot style during an open election.

2. The supervisor screen does not have the ability to close an election, thus altering the outcome of a particular polling place.

3. Ballot modification is not possible via a rogue PCMCIA card (counterfeit voter activation card) as the system will read the file loaded as bad, and will not load them. Counterfeit or tampered PCMCIA cards cannot be

authenticated and therefore, are not authorized by the AVC Edge system at the polling places. **ISO 17799 Section 10.2.1**

4. The AVC Edge provides no way to access the protected counter through communication ports, the PCMCIA card, touch-screen menus, or any other observable means. **ISO 17799 Section 9.6.2**

5. The AVC Edge is NOT on a LAN/WAN segment, and does NOT dial out over a phone line. **ISO 17799 Section 9.6.2**

6. There are no serial communications ports, TCP (Transmission Control Protocol)/UDP (User Datagram Protocol), Serial, USB, or other ports available. The printer serial port is designed to communicate one way. **ISO 17799 Section 9.6.2**

7. The PCMCIA cards are sealed. Anyone attempting to tamper with the cards would need to break the seal.

8. The AVC Edge uses a PCMCIA card for transporting election results to the counting center. These cards are under the physical control of poll workers, as well as a member of each political party (One Democrat, One Republican) during transportation. **ISO 17799 Section 8.7.2**

9. Upon the AVC Edge system reaching a critical level on battery power, the system discontinues voting and shuts down. Once power is restored, voting can resume and no votes or audit information is lost. This protects against Denial of Service attacks.

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 were 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 Determination
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.

In our next step we examined the risks identified earlier and assigned a **likelihood rating**. The likelihood rating was given based upon the controls in place by the Independence County Auditor's Office, as well as the functionality of the Sequoia Voting System.

Threat Identified	Likelihood Rating
System Sabotage	Medium
System Tampering	Medium
System Penetration	Low
System Attack	Medium
Physical Tampering	Medium
Social Engineering	High
Hacking	Low
Spoofing	Low
Terrorism	Low
Information Theft	Low
Malicious Code	Medium
Interception	Low
Input of Corrupt Data	Medium
Fraud/Theft	Low
Unauthorized System Access	Medium
Political Sabotage	Low
System bug	Medium
Identity Theft	Low
Data Alteration	Low

Impact Analysis

In this step, we determined the adverse impact(s) that would likely occur if a threat source were able to successfully exploit a vulnerability or weakness. In doing so, we were looking at the impact on Independence County and the election process were a vulnerability to be successfully exploited. In order to quantify our analysis, we assigned a rating of High, Medium, or Low to each vulnerability identified 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 each potential vulnerability:

Potential Vulnerability Identified	Impact Rating	Justification
Information Alteration	Medium	None of the electronic voting systems are networked in any way.
Tampering with the AVC Edge systems	High	The systems are under the physical control of Snohomish County personnel at all times.
Attempting to load malicious code into the AVC Edge	High	If a counterfeit card is inserted, the AVC Edge system recognizes the bad file on the card and asks that the card be removed.
Unauthorized Access	High	All systems require a password. Auditor's personnel are the only users that have access to these passwords.
System Sabotage	Medium	The AVC Edge enters supervisor mode without entry of any password. Any voter could place the AVC Edge in supervisor mode in a few seconds.
Data Theft	Low	None of the electronic voting systems are networked in any way. Internet or network-based attacks are not possible.
System Attack	Medium	Physical access to the AVC Edge touch-screen voting devices, as well as the voter activation cards and system is strictly controlled and monitored by the board workers at each polling place.
"Overvoting"	Low	Upon successful voting, the voter activation card is rendered inoperable.

Risk Determination

The purpose of this step is to assess the level of risk to the election process utilizing the Sequoia Voting System. In this step, we identified the risk(s), if any, arising out of our observation of the election process. After identifying the risk(s), the team assigned a risk rating for each vulnerability by combining the results of the Impact Analysis established earlier with the Likelihood of Threat already established. The combination of the impact analysis and the threat likelihood versus the security controls in place were applied to a matrix to determine the resultant risk level.

Risk	Risk Likelihood	Impact Rating	Risk Level

An unauthorized person with access to the administrator account on the WinEDS server might use any ODBC-compliant product to access the election database and modify the database.	Low	High	Low
An unauthorized person with access to the DIMS server could access confidential voter registration information.	Low	Medium	Low
Someone with unauthorized physical access to the AVC Edge machines after the LAT testing, could tamper with the machines.	Low	High	Low
An unauthorized person might access supervisor mode on the AVC Edge and disrupt the polling process by executing supervisor functions	Low	Medium	Low
No password is required to close the polls. Polls are closed on the AVC Edge using a switch on the back of the DRE. The switch is sealed during the election process.	Medium	Medium	Medium
The PCMCIA card used to store and transport vote counts is kept in a compartment on the AVC Edge. An unauthorized user could access the card and disrupt the polls. The compartment is sealed during the election process and the systems are under the physical control of poll workers during the election process.	Medium	High	Low
An unauthorized person might remove the PCMCIA card and attempt to disable the DRE.	Medium	High	Low
The AVC Edge uses a PCMCIA card for transporting election results. An unauthorized person might corrupt the PCMCIA card in transit to the Election Central counting location.	Low	Low	Low

Part Three: Do

Overview

In this phase, we describe in more detail the controls selected, or identified during the Risk Analysis phase. Here we will describe several of the specific problems that were identified prior to defining the Scope of our ISMS, as well as during our Risk Analysis. We start by describing the "problem", moving on to the "actions" taken to solve the problem. Then the steps for implementing the controls are detailed.

Problem: The lack of a formalized written security policy is the first issue we need to address. ISO section 3.1 reads "Management should set a clear policy direction and demonstrate support for, and commitment to, information security through the issue and maintenance of an information security policy across the organization." Section 3.1.1 reads, "A policy document should be approved by management, published and communicated, as appropriate, to all employees. It should state management commitment and set out the organization's approach to managing information security."

Action: The security committee has been tasked with the creation and adoption of both a “high level” security policy statement, as well as several issue and department specific policies.

Steps:

1. Using the direction set forth from the County Executive, the security committee will create a “high level” policy statement, outlining management’s expectations and support regarding information security.

2. Using the policy framework outlined above create the County authority and responsibility policy.

3. Work with representatives from the various departments to create the Information asset policy.

4. Create the acceptable use policy

5. With these policies in completed, approved and communicated to County employees, create the remaining security architecture policies, including:
    - Record Retention and Information Management Policy;
    - System Surveillance Policy;
    - Disaster Recovery and Business Resumption Policy;
    - Public Information and Media Policy;
    - Third Party/Partner Access Policy.
    - Account and Password Policies;
    - Access Control and Authorization Policy;
    - Remote Access Policy;
    - Anti-Virus Policy;
    - Change Management;
    - Media and Material Disposal Policy;
    - Incident Handling Guideline;
    - TCP/IP and Other Protocols Policy.

Problem: ISO Section 6.2.1 specifically relates to “Information security education and training”. “All employees of the organization and, where relevant, third party users, should receive appropriate training and regular updates in organizational policies and procedures. This includes security requirements, legal responsibilities and business controls, as well as training in the correct use of information processing facilities” Without the proper training and education on various information security concepts, election personnel cannot reasonably be expected to enforce the controls necessary to safeguard voter information.

Action: Implementation of a comprehensive information security awareness program.

Steps:

1. Perform an in house assessment in order to determine the current level of security awareness within the County.

2. Identify staff that will be interviewed to gauge the current level of security awareness.

3. Develop questions to ask in interview.

4. Create a matrix to compile the answers in order to identify County strengths and weaknesses with regards to information security awareness.

5. Identify all in-house resources with the information necessary to construct a comprehensive, valuable security awareness program.

6. Identify the format for delivering the awareness training.

7. Develop the material and a method for tracking those who have and have not completed security awareness training.

8. Deliver the training and determine level of understanding.

Problem: The election management system is a complex system comprising several different components. Each of these components introduces a potential risk, and/or entry point for malicious users.

Action: To protect the integrity of the system as well as safeguard the ballots cast, a design determination was made to not connect any of the election management system to any form of network. Each component within the system would act independently with relation to the remaining system components.

Steps:

1. The DIMS (Data Integrity Management System) used for voter registration is a completely stand alone server. The server is NOT a member of the Independence County Domain, nor any other domain. Data (voter registration information) is input into the DIMS server manually. **ISO 17799 Section 8.5.1, Section 9.6.2**
2. The BPS server (Ballot Processing System) is used by Independence County to create the ballot definitions, or "styles" for an election. These ballot styles are then loaded into the WinEDS system manually. **ISO 17799 Section 8.5.1, Section 9.6.2**
3. The WinEDS election management software used is used to compile and tabulate the election results from each polling place. The WinEDS software is installed on a stand alone server. The physical location of the WinEDS server is the Independence County central counting location. The location is physically secure and under control of Independence County personnel at all times. **ISO 17799 Section 8.5.1, Section 9.6.2**

Problem: The components making up the Election Management System (DIMS, BPS, WinEDS, and the AVC Edge machines) would be vulnerable to tampering without the appropriate physical security controls in place.

Action: All components comprising the Election Management System will sited within the confines of the Independence County Auditors office. Physical access to these components will be limited to County personnel only. The operating system of each machine will be "hardened" appropriately.

Steps:

1. Each system will require users to provide a valid username and password in order to successfully access the application.

2. Since these systems are NOT part of a domain, the accounts will reside in the systems Local directory database.

3. Each authorized user will have a local account created for them on the system.

4. All request for changes to account privileges, or new account creation, must be handled by the department's election manager.

5. The systems will be located in a secure, locked area of the Independence County Auditor's office. Access to the area will be restricted, and only County employees are allowed beyond a manned reception desk.
   ISO 17799 Section 7.1.1, 7.1.2

6. Physical access to the AVC touch-screen voting devices, as well as the voter activation cards and system, will be strictly controlled and monitored by the board workers at each polling place. Locks will be placed on the back of each system. Access to the supervisory functions of the AVC Edge is controlled via the back of the machine. ONLY authorized board workers, poll workers will be allowed to access these supervisory screens.
   ISO 17799 Sections 7.1.1, 7.1.2

Statement of Applicability

Throughout the ISMS implementation, all of the 7799 controls were reviewed for applicability. Many of the controls were implemented, and for various reasons, many were not. Below are several statements of applicability for controls that were selected, and one for a control that was not selected.

STATEMENT OF APPLICABILITY For Independence County Election Management System

Implement: Fully
Justification for partial or non-implementation: Not Applicable

3.1 Information Security Policy
3.1.1 *Information Security Policy Document*

Control Reference	Description	Implement	Justify	Method	Comment
3.1.1	Management should set a clear policy direction and demonstrate support for, and commitment to, information security through the issue and maintenance of an information security policy across the organization.	Fully	N/A	Security Committee received clear directive from County management on commitment to information assurance. Policy has been written, approved, and disseminated to all County employees, partners and poll worker volunteers.	The basis of any Information Security Program or ISMS is a formalized Security Policy document.

STATEMENT OF APPLICABILITY For Independence County Election Management System

Implement: Fully
Justification for partial or non-implementation: Not Applicable

7.1 Physical and Environmental Security
7.1.1 & 7.1.2 *Physical Security Perimeter and Physical entry Controls*

Control Reference	Description	Implement	Justify	Method	Comment
7.1.1;7.1.2	Critical or sensitive business information processing facilities should be housed in secure areas, protected by a defined security perimeter, with appropriate security barriers and entry controls.	Fully	N/A	Each component making up the Election Management System is completely separate, and sited in secure location within the Independence County Auditors	To prevent unauthorized access to the various system components

The following statement of applicability defines a 7799 control that was not selected and the justification for not selecting the control.

STATEMENT OF APPLICABILITY For Independence County Election Management System

Implement: No
Justification for partial or non-implementation: Mobile computing not utilized

9.8 Mobile computing and teleworking
9.8.1 & 9.8.2 *Mobile Computing and Teleworking*

Control Reference	Description	Implement	Justify	Method	Comm
9.8.1;9.8.2	To ensure information security when using mobile computing and teleworking facilities. The protection required should be commensurate with the risks mobile working introduces.	N/A	Mobile Computing is not used in any fashion in the Election Management System. There is no network connectivity between components	N/A	N/A

Part Four: Check

Overview

Part three of our four-step PDCA (Plan, Do, Check, & Act) process is "Check". In this phase, a set of processes has been put into place that will ensure compliance with the controls specified in this ISMS. Periodically, the Security Manager will audit compliance to ensure the controls are effective and implemented properly.

Below is the checklist used to verify compliance with the selected controls.

SECTION:	**INFORMATION SECURITY POLICY**
Control:	**3.1.1 – Information Security Policy Document**
Control Objective:	To provide management direction and support for information security.
Control Reasoning:	Management should set a clear policy direction and demonstrate support for, and commitment to, information security through the issue and maintenance of an information security policy across the organization.
Tests Performed:	1. Ensure policies exist 2. Gather and review policies. 3. Determine how policy is disseminated to employees. 4. Gather evidence of management support

	5. Signed documents indicating management approval.

SECTION:	**ASSET CLASSIFICATION AND CONTROL**
Control:	**5.1.1 – Inventory of assets**
Control Objective:	To maintain appropriate protection of organizational assets.
Control Reasoning:	All major information assets should be accounted for and have a nominated owner. Accountability for assets helps to ensure that appropriate protection is maintained. Owners should be identified for all major assets and the responsibility for the maintenance of appropriate controls should be assigned.
Tests Performed:	1. Ensure asset owner (Auditor) has created policies regarding protection of assets under their control. 2. Gather and review policies. 3. Review asset register for appropriate classification scheme. 4. Determine how policy is disseminated to employees.

SECTION:	**PERSONNEL SECURITY**
Control:	**6.2.1 – Information security education and training**
Control Objective:	To ensure that users are aware of information security threats and concerns, and are equipped to support organizational security policy in the course of their normal work.
Control Reasoning:	Users should be trained in security procedures and the correct use of information processing facilities to minimize possible security risks.
Tests Performed:	1. Review training log, class register, to verify all personnel received appropriate training? 2. Interview employees.

SECTION:	**PHYSICAL & ENVIRONMENTAL SECURITY**
Control:	**7.1.1 – Physical Security Perimeter**
Control Objective:	To prevent unauthorized access, damage, and/or interference to business premises, information, and information processing systems.
Control Reasoning:	Physical security is the first line of defense within an organization. Unfettered access to the systems would allow a user to alter data, input false data, or potentially load malicious code.

Tests Performed:	1. Ensure signs clearly delineate area behind which only employees are allowed access. 2. Review building schematics for location/perimeter specifications. 3. Physically inspect location for alternate entrances.

SECTION:	**PHYSICAL & ENVIRONMENTAL SECURITY**
Control:	**7.1.2 – Physical Entry Controls**
Control Objective:	Ensure that only authorized personnel are allowed access to facilities where the Election Management Components are sited.
Control Reasoning:	Unfettered access to the systems would allow a user to alter data, input false data, or potentially load malicious code.
Tests Performed:	1. Interview personnel that man reception desk. 2. Review procedures for employees requesting access to secure area. 3. Review access switch logs. 4. Ensure that employees are required to sign a logbook when accessing secure area. 5. Review logbook

SECTION:	**PHYSICAL & ENVIRONMENTAL SECURITY**
Control:	**7.2.1 – Equipment Siting Protection.**
Control Objective:	To prevent loss, damage or compromise of assets and interruption to business activities.
Control Reasoning:	Equipment should be physically protected from security threats and environmental hazards. Protection of equipment is necessary in order to reduce the risk of unauthorized access to data and to protect against loss or damage.
Tests Performed:	1. Ensure that system components are separate from Independence County network. 2. Visually inspect facility to ensure appropriate environmental controls are in place. 3. Obtain and review policy on eating, and drinking in secure location.

SECTION:	**COMMUNICATIONS & OPERATIONS MANAGEMENT**
Control:	**8.1.1 – Documented operating procedures**
Control Objective:	To ensure the correct and secure operation of information processing facilities.

Control Reasoning:	Responsibilities and procedures for the management and operation of all information processing facilities should be established. This includes the development of appropriate operating instructions and incident response procedures.
Tests Performed:	1. Obtain and review operating procedures 2. Interview relevant employees to determine their understanding of procedures. 3. Observe employees to verify procedures are followed properly.

SECTION:	**COMMUNICATIONS & OPERATIONS MANAGEMENT**
Control:	**8.5.1 – Network Controls**
Control Objective:	To ensure the safeguarding of information in networks and the protection of the supporting infrastructure.
Control Reasoning:	A range of controls are required to achieve and maintain security in computer networks. Various controls should be implemented to ensure the security of data in networks, and the protection of connected services from unauthorized access.
Tests Performed:	1. Review policies and procedures to ensure there is a documented separation between Election Management system, and County infrastructure. 2. Interview appropriate personnel to determine how information flows through system. 3. Visually inspect all components of Election Management system, looking for signs of network connectivity.

SECTION:	**COMMUNICATIONS & OPERATIONS MANAGEMENT**
Control:	**8.7.2 – Security of Media in transit**
Control Objective:	To ensure that the information maintains integrity during transit, as it flows through the system.
Control Reasoning:	Information can be vulnerable to unauthorized access, misuse or corruption during physical Transport. Controls should be applied to safeguard computer media being transported between sites, system components.
Tests Performed:	1. Review policies and procedures created by Independence County Auditor pertaining to data transfer in system components 2. Inspect systems to ensure there is no network connectivity between components

	3. Observe elections personnel as they transfer data (USB Token) following documented policies and procedures.

SECTION:	**COMMUNICATIONS & OPERATIONS MANAGEMENT**
Control:	**8.7.5 – Security of Electronic office systems**
Control Objective:	To provide management direction and support for acceptable use of acceptable use of Electronic office systems.
Control Reasoning:	Policies and guidelines should be prepared and implemented to control the business and security risks associated with electronic office systems.
Tests Performed:	1. Obtain acceptable use policy 2. Review acceptable use policy 3. Interview employees to determine how policy has been communicated to employees.

SECTION:	**ACCESS CONTROL**
Control:	**9.2.3 – User password management**
Control Objective:	Control access to information to authorized personnel only.
Control Reasoning:	Passwords are a common means of validating a user's identity to access an information system or service. The allocation of passwords should be controlled through a formal management process.
Tests Performed:	1. Review procedures for password management. 2. Interview employees on password usage. 3. Review system configuration on password policy. Ensure that password complexity, password history as well as minimum and maximum password expirations are set. 4. Observe personnel during password management. 5. Perform password strength testing/auditing through the use of John the Ripper password cracking tool.

SECTION:	**ACCESS CONTROL**
Control:	**9.4.1 – Policy on use of network services**
Control Objective:	Protection of networked services.
Control Reasoning:	Access to both internal and external networked services should be controlled. This is necessary to ensure that users who have access to networks and network services do not compromise the security of these network services.

Tests Performed:	1. Review policy 2. Determine how policy has been communicated to employees.

SECTION:	**ACCESS CONTROL**
Control:	**9.6.2 – Sensitive information isolation**
Control Objective:	To prevent unauthorized access to information held in information systems.
Control Reasoning:	Some application systems are sufficiently sensitive to potential loss, or house sensitive information, that they require special handling.
Tests Performed:	1. Review policy outlining separation of system components. 2. Interview appropriate personnel to determine how information flows through system. 3. Visually inspect all components of Election Management system, looking for signs of network connectivity.

SECTION:	**SYSTEM DEVELOPMENT AND MAINTENANCE**
Control:	**10.2.1 – Input data validation**
Control Objective:	To prevent loss, modification or misuse of user data in application systems.
Control Reasoning:	Appropriate controls and audit trails or activity logs should be designed into application Systems. These should include the validation of input data, internal processing and output data.
Tests Performed:	1. Review documentation from vendor concerning data validation 2. Load a PCMCIA card with false data and attempt to input counterfeit data into Election Management system. 3. Attempt to load a rogue PCMCIA card. 4. Observe and log results

The checklist above will ensure that the controls as implemented are fully formed, correctly implemented, and effective. This will help determine the overall effectiveness of the ISMS. This checklist will be reviewed prior to each election (regional as well as national) by the County elections manager and/or her delegate within the Auditors department. If any of the measures fail, the information security manager will be notified. The information security manager will work with elections personnel to determine the cause and develop a secure alternate solution where possible.

Part Five: Act

Information assurance is an evolution, an ongoing process. Like any ongoing process, the ISMS require constant attention and continual improvement.

The Information Services Board, which oversees the Security Committee, has mandated that the Security Committee will meet at least weekly until the policies are completed, approved and distributed. At that time, the committee will be scaled back to quarterly meetings, or as appropriate.

The Election Management System and the ISMS be reviewed regularly. The information security manager, working with the election manager has determined that, at a minimum, the system be reviewed prior to each election (regional as well as National). Either the election manager, or her delegate, will review the Election Management System using the checklist above. If during the review, any control fails, or is ineffective, the information security manager will be immediately notified. The information security manager will work with elections personnel to determine the cause and develop a secure alternate solution where possible. Any changes to the system or controls will be communicated to the Security Committee immediately.

The Security Committee will review the audit results as well as the recommendations made by the information security manager and determine if the appropriate steps were taken.

The Security Committee will make the results known to the Information Services board.

The information security manager will, on a yearly basis review the high level information security policy, as well as the department and issue specific policies. Any changes made to the policies will be presented back to the Security Committee for approval.

Closing

Elections have long required strong policies and procedures in place to ensure the fair and democratic nature of election results. However the introduction of DRE (Direct Recording Electronic) voting introduces a new set of risks and requires an additional set of security controls. While the implementation of an ISMS cannot guarantee complete information assurance, the controls resultant of the ISMS will go a long way towards maintaining the sanctity of the election process.

References

1. Thiagarajan, Valliappan in conjunction with the SANS Institute. “ISO 17799 Checklist”. August 2003.
http://www.sans.org/score/checklists/ISO_17799_checklist.doc

2. SANS Institute Security Policy Project
http://www.sans.org/resources/policies

3. “Information Security Policies Made Easy” (ISPME) written by Charles Cresson Wood, NetIQ.

4. Federal Election Commission web site
http://www.fec.gov/pages/vssfinal/vss.html

5. Risk Management Guide for Information Technology Systems. Special Publication 800-30.
http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

6. ISO 17799 Practice for Information Security Management
www.iso.org