Global Information Assurance Certification Paper

STORE COMPUTER

INFORMATION SECURITY MANAGEMENT SYSTEM

Implementing an Effective Security Model for
the Computers in XYZ's 5,000 Stores

By

Adrian Jones

Practical Assignment (Version 1.1) for

GIAC Certified ISO-17799 Specialist Certification

Submission Date: August 25, 2004

TABLE OF CONTENTS

ABSTRACT

XYZ is deploying a computing device to each of its 5,000 retail stores. This is being done in an attempt to improve communication with the stores and offer the store employees Computer-Based Training. Network connectivity to the stores currently exists via satellite (VSAT) technology. The devices to be placed in the stores will communicate with the systems at corporate using this VSAT network.

An Information Security Management System (ISMS) needs to be developed and implemented for this new infrastructure. Due to its complex nature, this new infrastructure will need to follow strict security standards. The ISO 17799 standard has been selected as a guideline for implementing effective security controls. The Plan, Do, Check, Act (PDCA) model has been selected as the appropriate method for implementing the ISMS.

New security policies, procedures, and standards will need to be developed specifically for this infrastructure. Project and security teams will be created to address the implementation issues. The teams will perform risk assessments to determine vulnerabilities, apply the appropriate ISO controls, and determine whether the risk has been effectively mitigated (to an acceptable level).

In the Planning stage of PDCA, the problems and applicable controls will be selected. In the Do stage of PDCA, the steps for improving (or implementing, in this case) the ISMS are will be described. In keeping with the PDCA model, audits will be performed (Check) to ensure that the controls are effective. The final step of the PDCA, Act, will be used to remedy or improve controls that are found to be insufficient.

THE SYSTEM

Background

XYZ has over 5,000 retail stores. Executive Management has determined that the lack of communication between the store employees and the teams that support store operations is a causal factor for several problems: high shrink numbers; high store employee turnover; customer dissatisfaction due to poorly trained employees; excessive shipments of goods, due to poor communication; and an inability to efficiently schedule late shipments, due to the lack of real-time communication.

To address this problem, the decision was made to introduce a computing device to each store. The expectation is that this computing device can be used to increase communication with the employees at each store. The device will also be used to provide computer-based training to store employees- a method of training which would be more standardized and formal than the ad-hoc training historically provided. Finally, the computing devices can also be used to administer tests to help confirm the effectiveness of the training.

Existing IT Infrastructure

The existing IT infrastructure of the company consists of the following. A single corporate office hosts the majority of computing systems. A heterogeneous mixture of technologies is used to support the company's operations.

Each of the company's stores hosts at least one cash register. Sales and payroll information are gathered and compiled at the stores on cash registers. This information is transferred to the computing systems at corporate where it is processed. Currently, a private VSAT network is used as the communications medium for moving data to and from the stores.

Since important information traverses the private VSAT network, the integrity of this network is of the utmost importance. Due to the nature of VSAT networks, bandwidth is limited, which makes it vulnerable to many threats (e.g. Denial Of Service attacks, viruses, etc.). Special care will be taken to protect this network. The systems utilizing the VSAT network must also be protected from harm since downtime for these systems significantly impacts the business (I.E. sales and payroll data cannot be sent).

Each of the company's ten nationwide distribution centers has a data center that hosts a diverse set of computing platforms. Dedicated IT personnel work in each of these locations. One overseas location also hosts several computing systems. This location also has dedicated IT personnel.

All of the IT personnel in remote (non-corporate) locations have limited administrative permissions. Only corporate IT personnel possess full administrative authority. None of the systems in the distribution centers or in the overseas location can communicate with the VSAT network directly.

The Information Security Management System

Computing devices will be placed at each of the company's stores. Security is XYZ's primary concern for this new infrastructure. As a standard practice, all systems at XYZ must pass a rigorous security assessment before they are approved for implementation.

For this implementation, however, the company has decided that the systems, polices, and procedures related to this new infrastructure will need to meet ISO 17799 standards for security. Installing computing devices in each of the company's 5,000 stores will make these systems targets for misuse (e.g. disgruntled personnel) and accidents.

The Information Security group will work with the various members of the project team and Executive Management to build an Information Security Management System (ISMS) for securing and administering this infrastructure in a manner that complies with ISO 17799 standards.

The Information Technology department uses ISO 17799 and other industry standards as guidelines for many of its IT processes, so using the standard for this implementation will dovetail with existing security policies and procedures.

THE PLAN

Project Teams

Key members of the company have been selected to participate in this project. One or more members of the following departments have been chosen: Executive Management, Store Operations, Store Information Systems, Infrastructure Services, Information Security, Internal Audit, Training, and Store Facilities. It was decided that two forums would be initiated for this project.

First, a Project-Guidance Forum was established. Its primary focus is the overall execution of the project**:** forum where acceptance is finalized, timelines are established, progress is monitored, and responsibilities are delegated.

A second forum was established to deal with design (and security) issues. ISO 17799 indicates, in 4.1.1, that a security forum should be established in order to provide direction for the organization. A dedicated security forum already exists

at XYZ; however, its scope was too broad to deal with design issues at a detailed level.

It was decided that it would be appropriate to address design and security issues in the Design Forum. The members of the Design Forum are responsible for deciding which technologies are to be used, defining how technologies should be implemented and administered, creating security policies and procedures, etc.

This Design Forum consists of personnel from the following departments: Store Facilities, Store Information Systems, Infrastructure Services, Information Security, and Internal Audit.

The Design Forum will address many of the key elements defined in ISO 17799, namely:

- 3.1.1 – Information Security policy document
  - The team will determine the content and format of security policies and procedures
- 4.1.1.a – reviewing and approving security policy and overall responsibilities
- 4.1.1.b – monitoring significant changes in the exposure of information assets to major threats
- 4.1.1.c – reviewing and monitoring information security incidents
- 4.1.1.d – approving major initiatives to enhance information security
- 4.1.2.a – agrees specific roles and responsibilities for information security across the organization [as appropriate for this project]
- 4.1.2.b – agrees specific methodologies and processes for information security
- 4.1.2.d – ensures that security is part of the information planning process
- 4.1.2.e – assesses the adequacy and coordinates the implementation of specific information security controls for new systems or services

Furthermore, it was decided that the Design Forum would continue to operate for one year after the implementation of the new infrastructure has been completed, and that security would be its main focus. One year after the implementation phase of the project has been completed, this forum is to be dissolved – if appropriate at that time – and security issues should be handled by the company's primary Information Security Forum.

Per objective 4.1.3 of ISO 17799, the following managerial and security roles were defined.

Position	**Role/Responsibilities**	**Project-Guidance Forum**	**Design Forum**
CIO, Information Systems	Representative for Executive Management; providing top-level of "show of support" for	X	

	initiative; ultimate responsibility for system sign-offs		
Manager, Store Information Systems	Project Manager; keep the appropriate team members involved; define, monitor, and enforce timelines; etc.	X	X
Director, Store Facilities	Lead team member for physical security in each store, in accordance with ISO 17799, 7.x, Physical and Environmental Security	X	X
Senior Facilities Specialist, Store Facilities	Lead technical specialist responsible for physical security in each store, in accordance with ISO 17799, 7.x, Physical and Environmental Security	X	X
Senior Technician, Store Information Systems	Provide in-house Information Security advise for the computing devices to be implemented in the stores and for the cash registers in the stores currently; in accordance with ISO 17799, 4.1.5, Specialist Information Security Advice	X	X
Senior Systems Administrator, Infrastructure Services	Provide in-house Information Security advise for the infrastructure that will support the computing devices in the stores; in accordance with ISO 17799, 4.1.5, Specialist Information Security Advice	X	X
Senior IT Auditor, Internal Audit	This position is not part of the IT department; the Internal Audit team's role is to observe the activities related to the project, but input is restricted; the IA team will ensure that the IT teams – and the Design team, in particular – have followed the ISO guidelines; this position will fulfill the role that ISO 17799, 4.1.7 specifies: independent review of Information Security	X	X
Senior Director, Training	Primary point of contact for all training-related issues for this project; this person's team will provide training related to field and store managers using various mechanisms; ISO 17799, 6.2.1 describes the training and user education requirements	X	
Manager, Information Security	Guides both the Project-Guidance and Design forums in order to align the project and its security aspects with ISO and other industry standards; must provide sign-off for security-related matters	X	X

Members of the Design Forum are granted the authority to make decisions regarding that will influence the direction of the project and technologies related to it. Although all members of the Design Forum will contribute to the design and security of this implementation, the Manager of Information of Security has been granted the authority to veto a proposal if it can be shown that a material weakness exists.

As shown in the table above, the CIO of Information Systems will provide a show of "top-level support" for the project. The CIO, like Manager of Information

Security, retains the authority to veto any design proposals, as his responsibilities also include signing-off for: risk acceptance, technical designs, etc.

It should also be noted that although the CIO is not part of the Design Forum, security related issues and decisions are presented and addressed in the Project-Guidance Forum- once they are condensed into a format that is appropriately concise and comprehensible; whereas, in the Design Forum many ideas are proposed, considered, and accepted, modified, or rejected. Thus, the decisions that are made by the members of the Design Forum will be discussed in the Project-Guidance Forum meetings, at which time they are subjected to further scrutiny by that committee and the CIO.

Ultimately, the owners of the various technologies will be responsible for implementing and supporting the systems that are implemented. These technology owners hold considerable authority in the decision-making process for design and security issues. The ultimate authority to veto a proposed design due to a security weakness is held only by the CIO and the Manager of Information Security. Non-security related issues are primarily under the control of the technology owners; although, they too are subject to the CIO's approval.

General Policy Information

The company's existing security policies are insufficient to cover the scope of the new infrastructure. For example, use of the computing devices in the stores will be restricted to a defined period of time; whereas, users in the corporate office do not have such restrictions.

ISO 17799, 3.1.1 states, "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." The objective continues on to describe the guidelines that should be considered in creating the document.

A security policy will be created for the stores specifically. The Manager of Information Security will be designated as the owner of the security policy for the stores – per objective 3.1.2 of ISO 17799 – and will be responsible for maintaining and updating it as often as is necessary. When appropriate, the Manager of Information Security will collaborate with the technology owners and the CIO to obtain additional input and consensus for the security policy's content.

The Training department will be involved in the dissemination and communication of the security policy. The users of the computing devices in each store will be required to complete "general usage" and "security policy" training prior to being granted approval to work on the devices.

The security policy will explain the process for reporting and handling security incidents (ISO 17799, 6.3.1). It will also describe the process for reporting weaknesses and malfunctions (ISO 17799, 6.3.2, 6.3.3). Since the most of the new users have not interacted with the company's information systems previously, every user will be required to read, accept, and sign a confidentiality agreement before being granted access (ISO 17799, 6.1.3).

Standards

The members of the Design Forum will produce a standard configuration for each of the computing devices and pieces of the infrastructure. Examples of this are outlined below.

Item	Description	Standard
Computing Device	The physical and logical device to be place at each store. This is the device that the store employees will directly access.	Floppy drives will not be installed on the devices; CDROMs and USB devices will be disabled from the boot sequence in BIOS, which will be locked; the device will run operating system X, with all unnecessary services disabled.
VSAT Router in Store	The satellite and routing interface in the store. This receives and sends data, computes routes, etc.	All VSAT Routers in the stores will run a secure operating system with minimal services loaded; routes will be tightly controlled using Access Control Lists; hardware hosting the operating system will be protected from tampering.
VSAT Firewall	The Firewall that will protect the corporate network and resources from the VSAT network (vice-versa)	The VSAT Firewall will be configured to allow only specified ports to communicate; Access Control Lists will limit communication to specified IP Address or Ranges.

The Project Timeline

Executive Management determined that the need for this technology was very high. For this reason, the timeline for designing and implementing the new infrastructure is very short. Although this will present hurdles, they will be overcome through effective, efficient planning.

The project plan outlined below describes the proposed timelines for meetings, implementation schedules, and so forth. All of these items and dates are subject to change, in accordance with the needs of the project.

1		**Store Computing Device Timeline**	**358 days?**	**Mon 7/19/04**	**Wed 11/30/05**
2		**Project-Guidance Forum**	**1 day?**	**Mon 7/19/04**	**Mon 7/19/04**
3		Project Kick-off	1 day?	Mon 7/19/04	Mon 7/19/04
4		**Design Forum (Plan)**	**19 days?**	**Mon 7/26/04**	**Thu 8/19/04**
5		**Analysis**	**19 days?**	**Mon 7/26/04**	**Thu 8/19/04**
6		**VSAT Design**	**10 days?**	**Mon 7/26/04**	**Fri 8/6/04**
7		Develop requirements for device communication	1 day?	Mon 7/26/04	Mon 7/26/04
8		Evaluate design possibilities	3 days?	Mon 8/2/04	Wed 8/4/04
9		Create proposed design	2 days?	Thu 8/5/04	Fri 8/6/04
10		**Computing Device Design**	**13 days?**	**Mon 8/2/04**	**Wed 8/18/04**
11		Determine operating system	1 day?	Mon 8/9/04	Mon 8/9/04
12		Identify necessary software	1 day?	Tue 8/10/04	Tue 8/10/04
13		Configure operating system security	1 day?	Mon 8/2/04	Mon 8/2/04
14		Evaluate manageability requirements	3 days?	Wed 8/11/04	Fri 8/13/04
15		Design device management structure	3 days?	Mon 8/16/04	Wed 8/18/04
16		**Security Assessment Session 1**	**1 day?**	**Thu 8/19/04**	**Thu 8/19/04**
17		Identify the major risks	1 day?	Thu 8/19/04	Thu 8/19/04
18		**Project-Guidance Forum**	**15 days?**	**Mon 8/2/04**	**Fri 8/20/04**
19		Project Status Meeting	1 day?	Mon 8/2/04	Mon 8/2/04
20		Evaluate options for training	1 day?	Mon 8/9/04	Mon 8/9/04
21		Evaluate VSAT and Computing Device/Management designs	1 day?	Fri 8/20/04	Fri 8/20/04
22		**Design Forum**	**2 days?**	**Mon 8/23/04**	**Tue 8/24/04**
23		Review new information and ideas	1 day?	Mon 8/23/04	Mon 8/23/04
24		Create formal proposal for VSAT and Device/Management desigr	1 day?	Tue 8/24/04	Tue 8/24/04
25		**Project-Guidance Forum**	**1 day?**	**Wed 8/25/04**	**Wed 8/25/04**
26		Review and accept or modify proposal for VSAT/Device design	1 day?	Wed 8/25/04	Wed 8/25/04
27		**Design Forum**	**2 days?**	**Fri 8/27/04**	**Mon 8/30/04**
28		Evaluate physical security of store environment	1 day?	Fri 8/27/04	Fri 8/27/04
29		Discuss security policy elements	1 day?	Mon 8/30/04	Mon 8/30/04
30		**Project-Guidance Forum**	**1 day?**	**Tue 8/31/04**	**Tue 8/31/04**
31		Project Status	1 day?	Tue 8/31/04	Tue 8/31/04
32		Discuss physical security and security policy proposals	1 day?	Tue 8/31/04	Tue 8/31/04
33		**Design Forum**	**24 days?**	**Mon 8/2/04**	**Thu 9/2/04**
34		Create final proposal for physical security and security policies	1 day?	Mon 8/2/04	Mon 8/2/04
35		**Security Assessment Session 2**	**2 days?**	**Wed 9/1/04**	**Thu 9/2/04**

Continued on next page

36		Evaluate risks of proposed designs using Risk Models	2 days?	Wed 9/1/04	Thu 9/2/04
37		**Project-Guidance Forum**	**6 days?**	**Mon 9/6/04**	**Mon 9/13/04**
38		**Discuss and approve/modify proposals**	**1 day?**	**Mon 9/6/04**	**Mon 9/6/04**
39		Physical security, security policies, designs	1 day?	Mon 9/6/04	Mon 9/6/04
40		**Security Assessment Session 3**	**1 day?**	**Thu 9/9/04**	**Thu 9/9/04**
41		Discuss and come to consensus on risk mitigation/acceptanc	1 day?	Thu 9/9/04	Thu 9/9/04
42		Discuss and agree upon training methods	2 days?	Thu 9/9/04	Fri 9/10/04
43		**Pre-commencement meetings**	**1 day?**	**Mon 9/13/04**	**Mon 9/13/04**
44		**Security Assessment Session 4**	**1 day?**	**Mon 9/13/04**	**Mon 9/13/04**
45		Formal sign-offs for design and security	1 day?	Mon 9/13/04	Mon 9/13/04
46		**Pilot 250 Stores (Do)**	**9 days?**	**Wed 9/15/04**	**Mon 9/27/04**
47		Hardware Procurement	1 day?	Wed 9/15/04	Wed 9/15/04
48		Have outsourcing partner sign-off confidentiality agreements	1 day?	Thu 9/16/04	Thu 9/16/04
49		Engage in computing device rollout	1 day?	Thu 9/23/04	Thu 9/23/04
50		**User Training**	**3 days?**	**Thu 9/23/04**	**Mon 9/27/04**
51		Store users to be trained by vendor	3 days?	Thu 9/23/04	Mon 9/27/04
52		Security policy to be communicated by vendor	3 days?	Thu 9/23/04	Mon 9/27/04
53		**Perform audit of ISMS for pilot infrastructure (Check)**	**5 days?**	**Mon 11/15/04**	**Fri 11/19/04**
54		Existence, effectiveness, and communication of policies/procedu	5 days?	Mon 11/15/04	Fri 11/19/04
55		Effectiveness and status of physical and logical security controls	5 days?	Mon 11/15/04	Fri 11/19/04
56		**Project-Guidance Forum**	**5 days**	**Mon 11/29/04**	**Fri 12/3/04**
57		**Evaluate rollout success and security**	**5 days**	**Mon 11/29/04**	**Fri 12/3/04**
58		Address security concerns resulting from audit	5 days	Mon 11/29/04	Fri 12/3/04
59		**Implements needed improvements (Act)**	**5 days**	**Mon 12/6/04**	**Fri 12/10/04**
60		Modify policies, procedures, and training as necessary	5 days	Mon 12/6/04	Fri 12/10/04
61		Modify physical and logical controls where necessary	5 days	Mon 12/6/04	Fri 12/10/04
62		**Continue rollout**	**135 days?**	**Mon 12/20/04**	**Fri 6/24/05**
63		Implement remaining stores	117 days?	Mon 12/20/04	Tue 5/31/05
64		Perform Audit (Check) and Improvement (Act) cycle	4 days?	Tue 2/1/05	Fri 2/4/05
65		Perform Audit (Check) and Improvement (Act) cycle	5 days?	Mon 4/4/05	Fri 4/8/05
66		Perform Audit (Check) and Improvement (Act) cycle	5 days?	Mon 6/20/05	Fri 6/24/05
67		Perform first infrastructure-wide Audit of the ISMS	20 days?	Mon 9/5/05	Fri 9/30/05
68		Implement needed improvements	22 days?	Tue 11/1/05	Wed 11/30/05

Risk Assessment

The Project-Guidance and Design forums will address issues surrounding risk as part of this project. It has been determined that four security-centric meetings should be held. In these meetings, topics such as risk identification, mitigation, and acceptance will be covered. The CIO and Manager of Information Security will ultimately sign-off on the risk plan, which will detail: risks, controls applied to said risks, and risks that are deemed acceptable.

Description of Meetings:

- A meeting to go through each model to identify basic risks. This meeting isn't dependent on knowing the final proposed design- it should not delve into the details at this point.
    - Purpose of meeting: to start brainstorming and arm the team information
    - Examples of risks identified:
        - Viruses on the computing devices
        - Risks to VSAT
    - Proposed attendees: Members of Design Forum
- A meeting after a basic design has been agreed upon (e.g. design proposal is accepted). In this meeting, the team should methodically go through risk models, identifying all specific risks and deciding on which controls can be implemented.
    - Purpose of meeting: identify risks and controls, take that information and prepare draft documentation
    - Example of specific risks and controls
        - The PC has a CDROM
        - Preventative Control: The CDROM will only mount when a CD has a security identifier; therefore, the risk is mitigated
    - Proposed attendees: Members of Design Forum
- A meeting to review the draft, discuss new developments, and consider new ideas
    - At this point, the team will probably have a good idea as to which risks have controls and which risks will need to be considered for acceptance
    - Proposed attendees: Members of Project-Guidance Forum
- A meeting to discuss any further findings, if necessary, and sign-off on risk acceptance, if possible
    - Purpose of meeting: potentially sign-off on design and security
    - Barring significant changes, formal, signed documentation should result from this meeting
    - Proposed attendees: Members of Project Guidance Forum

The team's experience and knowledge will be used to identify things like: possible failures, likelihood of failures, and impact of failures. It will then take that information and implement controls (preventative, detective, and reactive) to mitigate the risks. Ultimately, there may be some residual risk, which the team will then have to decide to either deem acceptable or unacceptable.

The FMECA Model

The Design Forum agreed that it would be appropriate to use the FMECA risk model to analyze risks, apply controls to mitigate those risks, and analyze the effectiveness of the controls applied.

FMECA.com (www.fmeca.com) describes the process as follows. "Failure Mode, Effects and Criticality Analysis (FMECA) or simply (FMEA) is a disciplined design review technique that focuses the development of products and processes on prioritized actions to reduce the risk of product field failures, and documents those actions and the review process" (FMECA).

FMECA (Failure Mode, Effects, and Criticality Analysis) (SANS 23-42)

- Steps:
  - 1: "Define the system" (SANS 26)
    - System's mission
    - Interfaces to other systems
    - Expectations for performance and reliability
  - 2: "Create Block Diagrams" (SANS 29)
    - Illustrate system interfaces
    - Illustrate all functional entities and how information flows
  - 3: "Identify all possible individual module or system failures" (SANS 31)
    - Determine the impact of each of these failures
  - 4: "Analyze each possible failure in terms of a worst-case scenario" (SANS 33)
    - Assign a Severity Level to each scenario:
      - Category 1- Catastrophic
        - Business processes would be severely impacted, may prevent point-of-sale processes
      - Category 2- Critical
        - Business processes would be seriously impacted, causing loss of productivity, but impacting sales
      - Category 3- Marginal
        - Business processes may be slowed, but critical processes should not be impacted
      - Category 4- Minor
        - Business processes would not be impacted, but proactive measures may be affected
  - 5: Identify existing mechanisms for "detecting" failures, and all compensating controls to prevent these failures
  - 6: Define additional controls where needed
  - 7: Analyze effects of additional controls
    - Does the control interrupt the system's mission?
    - Does the control interrupt future plans for the system?
    - Does the control create other risks?
  - 8: Document the analysis
    - Describe the problems found and the solutions
    - Document residual risks
      - Risks for which no control could be implemented

        - Describe the potential impact of residual risks
    - At this point, we would:
        - 1: Use other risk models to assess the system, and
        - 2: Determine which risks are acceptable
            - Executive Management should agree that the risks are acceptable and sign-off if in agreement

Policies

This infrastructure will be designed to support the company's stores. Its scope will not extend beyond this point. Furthermore, the existing corporate infrastructure differs greatly in many aspects from the proposed design for the stores. Much of the existing corporate policy, for example, would not be applicable to the stores. For this reason, the Project-Guidance Forum came to a consensus that specific policies should be created for the stores.

Three security-related policies are to be created. They are outlined below.

- Policy Name: Store Information Systems Security Policy
    - Purpose: In accordance with ISO 17799, 3.1.x, the policy will:
        - Demonstrate management's support for security
        - Define management's approach to Information Security management
        - Describe the scope of Information Security as it relates to the stores and the store infrastructure
        - Reference more detailed security policies and procedures
    - Audience:
        - Users of the store information systems
        - Administrators of backend information systems for stores
    - Addressing:
        - Definition of Information Security
        - Management's commitment to Information Security
        - User responsibilities
        - Consequences of policy violations
            - References to HR policies for consequences (ISO 17799, 6.3.5)
        - References to Acceptable Usage policy
        - References to Administrative Responsibilities policy
        - Define roles and responsibilities for Information Security
- Policy Name: Acceptable Usage
    - Purpose:
        - Educate users in the stores about proper use of computing devices
    - Audience:
        - Users of the store information systems
    - Addressing:

        - Describe user responsibilities
        - Define proper account usage
        - Define password policy (ISO 17799, 9.3.1)
        - Define unattended system policy (ISO 17799, 9.3.2)
        - Define incident handling responsibilities
            - References to Incident Reporting procedure
- Policy Name: Administrative Responsibilities
    - Purpose:
        - Define responsibilities of Systems Administrators
    - Audience:
        - Store information systems Systems Administrators
    - Addressing:
        - Define scope of Information Security responsibilities
        - Protection against malicious software (ISO 17799, 8.3.1)
        - Compliance with regulatory, legislative, and contractual requirements
        - References to Incident Handling procedures
        - References to General Administrative Procedures procedure
            - Including reference to Account management procedure

Procedures

The following procedures will be defined. These procedures are referred to in the security policies.

- Procedure Name: System Access
    - Purpose:
        - Describe steps for accessing the store information systems with user accounts
        - Describe steps for managing passwords
- Procedure Name: Incident Reporting
    - Purpose:
        - Define steps that users are to take in the event of a security-related incident or weakness (ISO 17799, 6.3.1, 6.3.2)
    - Audience:
        - Users of the store information systems
    - Addressing:
        - Viruses
        - Other malicious software
        - System failures
        - Violations of policies by other persons
        - Potential security weakness
- Procedure Name: Incident Handling (ISO 17799, 6.3)
    - Purpose:
        - Define procedures for handling incidents related to the store information systems

    - Audience:
        - Systems Administrators of the store information systems
    - Addressing:
        - Proper handling of malicious software and viruses
            - Prevention, detection, and response
            - Steps to take once compromise is detected
- General Administrative Procedures
    - Purpose: Define general security-related procedures
    - Audience: System Administrators of the store information systems
    - Addressing:
        - Backups
        - System patching
        - Virus updates
        - Account management
            - User registration (ISO 17799, 9.2.1)
            - Privilege management (ISO 17799, 9.2.2)
            - Review of user access rights (ISO 17799, 9.2.4)
        - Change management

Risk Mitigation

Several major risks have been identified by the Design Forum. Each of these risks has the potential to compromise a significant portion of the store information systems infrastructure. Hence, the risks were identified, acknowledged, and mitigated through the application of controls. Four main risks are explained below. These risks are broken out into more detailed pieces in Figure 1 and its coinciding narratives. The FMECA risk model is used to analyze each risk.

Risk – Malicious software on any device connected to the network used for the store information systems

Again, since the computing devices can be accessed at over 5,000 locations, it is imperative that controls are put in place that will minimize the ability for a virus to infect the device.

Risk – Inappropriate system usage

Any unauthorized or inappropriate activity must be prevented and tracked.

Risk – Unauthorized access of a network device

If the network devices were to be compromised, they could be used to perform a variety of attacks on the VSAT network. The VSAT network is particularly vulnerable to Denial of Service attacks, because it already operates with very limited bandwidth.

Risk – Unauthorized access or use of computing device in the store

The computing devices in the stores are at risk of being accessed by unauthorized persons. This risk is high since there are over 5,000 devices in disparate locations.

FMECA Analysis

The System Defined

A computing device will be placed in each of the company's 5,000 stores. The store personnel will use the computing devices to communicate in real-time, transfer information, and participate in Computer-Based Training. The basic parts of the Store Information Systems Infrastructure include:

- A single computing device at each store
  - A single network interface connected to the network
  - Devices in stores cannot communicate with devices in other stores
- The computing devices communicate via a private VSAT network
  - The VSAT network connects the devices to the corporate Ethernet network
- Host systems (servers) are hosted at corporate
  - Hosted on the Ethernet network
    - Connected directly to VSAT network
    - A firewall separates these hosts, along with entire VSAT network, from all other corporate information systems
      - Access Control Lists are used to provide specific host to host (and port to port) communication
  - Provide the following services
    - Messaging services
    - File sharing services
    - Security mechanisms
      - Authentication
      - Authorization
      - Event Logging

The VSAT network currently in place is stable and reliable. Since cash registers at each store use this network to transfer important information, the continued dependability of the VSAT network is of critical importance.

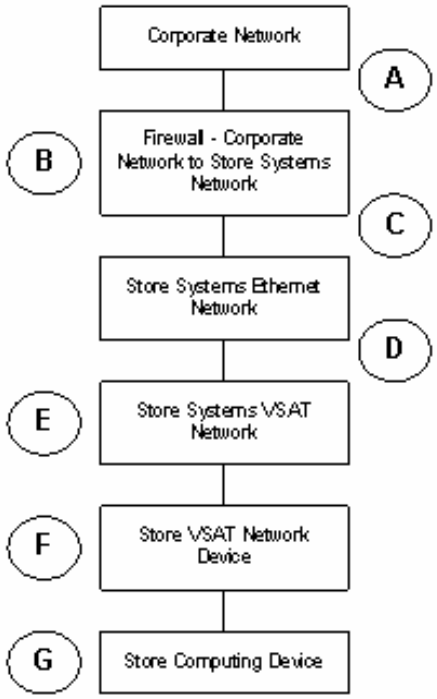
The computing device at each store, although important, is not required in order for the company's operations to continue. The expectation is that the devices will be reliable and available, but the criticality rating being assigned to the devices themselves has been defined as Low to Medium. This does not take into account the security aspects of these systems- if these devices are

compromised, from a security standpoint, these systems can dramatically affect other connected systems.

The host systems at corporate that support the devices in the stores are critical. These systems capture security events, process logins, etc; therefore, they must be available at all times. Additionally, although a firewall will separate these systems from the corporate systems, “one-to-one” and “port-to-port” connections will exist; thereby making it possible for a compromised host on the Store Information Systems network to affect a host on the corporate network.

Diagrams of System Interfaces

Below, two diagrams are shown. Firstly, a block diagram pictures the flow of information between the corporate network and the store’s computing device. Comments for each point of failure are described at the bottom of the page. Secondly, the basic networks and systems are shown for further understanding of the infrastructure.



A. The corporate network is connected to a firewall that separates it from the Store Information Systems network. This is intended to protect each network from the other network. Only one-to-one and port-to-port connections will be established between the two networks. Points of failure: malicious software could traverse the firewall and infect either network; if a system on either network is compromised, that system may be used to spawn attacks on other systems (on the same or the other network).
B. It is possible for the firewall operating system to be compromised, which would jeopordize both networks and the systems hosted on them.
C. See point A
D. The Store Systems Ethernet network is directly connected to the Store Systems VSAT network (I.E. There is no firewall protection; however, they are on separate network segments.)
E. The Store Systems VSAT network is particularly vulnerable to Denial of Service activity because of its low bandwidth.
F. The Store VSAT network device may be vulnerable to tampering, both physically and logically.
G. The computing device may be vulnerable to tampering if it is not properly secured.

Figure 1

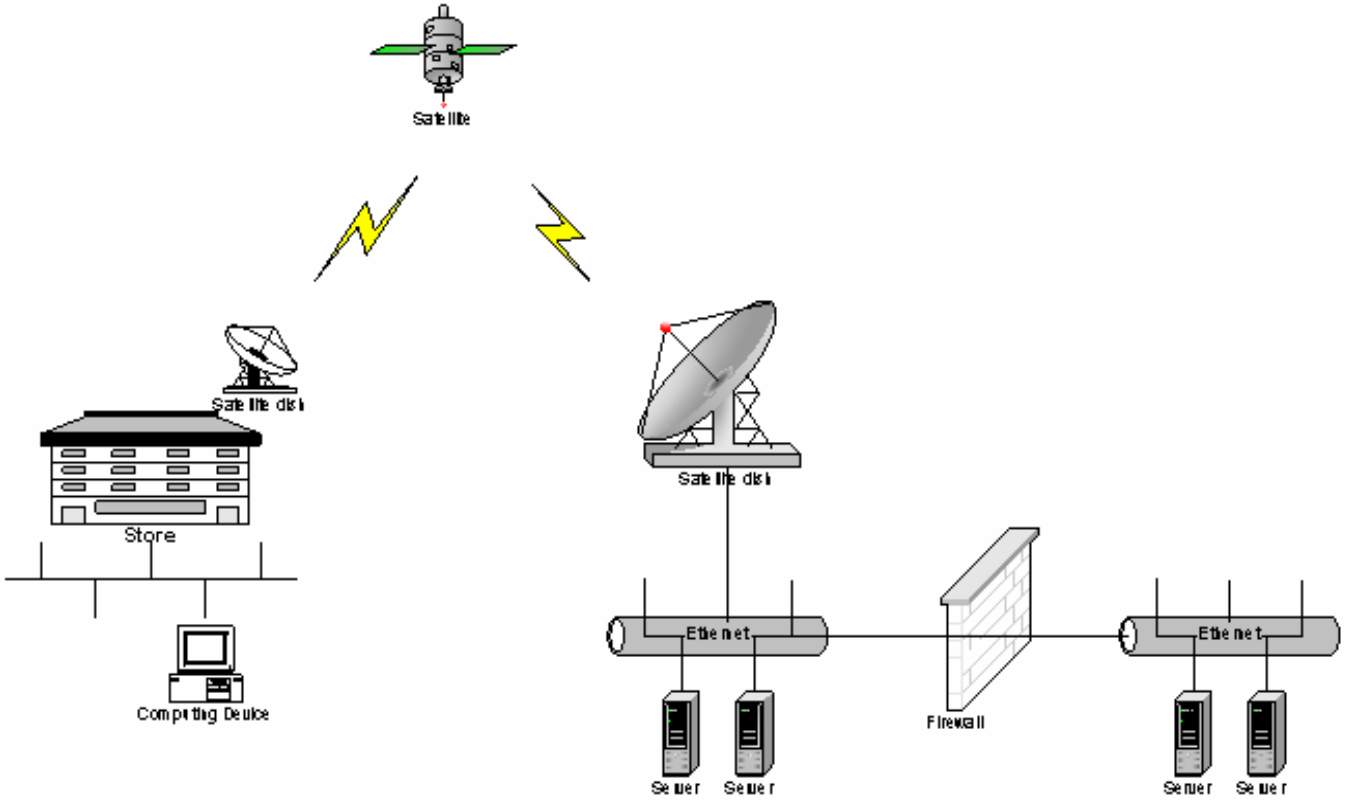


Figure 2

Impacts of Failures and Severity Level Ratings

The expected impacts of each of the failures shown in Figure 1 above are explained below. Each worst-case scenario detailed below is followed by a Severity rating for the potential failure(s). The Severity ratings are: Category 1 – Catastrophic; Category 2 – Critical; Category 3 – Marginal; Category 4 – Minor.

(**A**)The corporate network is connected to a firewall that separates it from the Store Information Systems network. This is intended to protect each network from the other network. Only one-to-one and port-to-port connections will be established between the two networks. Points of failure: malicious software could traverse the firewall and infect either network. If a system on either network is compromised, that system may be used to spawn attacks on other systems (on the same or the other network).

In the event that a system is infected with malicious software or is hacked, the expectation is that all other systems on the network – and connected networks – will be at risk. The result of such an infection on one or more systems would likely include the loss of production data, loss of productivity, and disclosure of confidential data.

Additionally, the network routing devices and network bandwidth would be at risk. A compromised network routing device could be used to spawn other attacks- on other network devices or operating systems. Again, a loss of production data, productivity, and the possible loss of confidentiality are all likely results of such activity.

Should bandwidth be consumed as a result of a compromise, the result would be a loss of productivity, and the possibility of other vulnerabilities being taken advantage of.

Severity Rating: Category 1 – Catastrophic

(**B**) It is possible for the firewall operating system to be compromised, which would jeopardize both networks and the systems hosted on them.

The firewall separating the corporate and store networks is a hardware-based solution. If an attacker could gain access to the firewall, he could potentially capture confidential data, not to mention the ability to launch attacks. Also, in the event that this firewall is compromised, either network may be harmed by activities on the other connected network since the barrier would be weakened.

In a worst-case scenario, the integrity of all systems connected to each of the networks is at stake.

Severity Rating: Category 1 – Catastrophic

(**C**) The Store Information Systems network is connected to a firewall that separates it from the corporate network. However, the firewall alone cannot fully protect the systems from malicious software. See item A for risks.

Severity Rating: Category 1 – Catastrophic

(**D**) The Store Information Systems Ethernet network is directly connected to the Store Information Systems VSAT network (I.E. There is no firewall protection; however, they are on separate network segments.)

Without a packet-monitoring, a firewall, or Access Control Lists regulating traffic between the two networks, data can flow between the networks unchecked and without regulation. Packets containing malicious content may be passed between the networks, which are particularly threatening to the VSAT network. Traffic on the Ethernet network must be managed and throttled, or it can easily overload the VSAT network.

The result of these threats in a worst-case scenario would be the loss of bandwidth availability in the VSAT network. This would interrupt the flow of critical sales and payroll data; therefore, the business would be seriously impacted negatively.

Severity Rating: Category 1 – Critical

(**E**) The Store Information Systems VSAT network is particularly vulnerable to Denial of Service activity because of its low bandwidth.

If the VSAT network is unavailable, critical sales and payroll data cannot be captured; hence, the company's financial information cannot be processed. This scenario could occur as a result of the other items in this list (A-D, F and G).

Severity Rating: Category 1 – Critical

(**F**) The stores' VSAT network devices may be vulnerable to tampering, both physically and logically.

Each store has a VSAT network device that is used to route packets. This device, if not protected, is vulnerable to improper handling: physical abuse, theft of the device, hacking of the operating system.

The physical destruction of the device, although undesirable, would likely have a minimal impact on the overall integrity of the network. However, if an unauthorized person was able to reach the device, he may also be able to access the network ports the device attaches to. These ports could be used to plug in another computing device in order to launch attacks.

If a device is stolen, a hacker could use it as a test system for cracking passwords and determining routes; information which could then be used to compromise a live device in another store. If an attacker could compromise one of the network devices, he could use the device to attack other devices on the network, launch Denial of Service attacks, etc.

The result of these activities could result in the loss of data integrity, loss of critical network bandwidth, and so forth, which could significantly impact the company's ability to process its financial information.

Severity Rating: Category 1 - Critical

(**G**) The computing device may be vulnerable to tampering if it is not properly secured.

The computing devices in the stores, if unsecured, are subject to theft, physical destruction, and hacking. No confidential information will be stored on the devices; however, the devices have access to the VSAT network, and, therefore, they have the potential of impacting other systems. Hence, the VSAT network may be put at risk, the computing devices in the other stores may be at risk, and the systems at corporate may be at risk as well.

The physical destruction of the device, although undesirable, would likely have a minimal impact on the overall integrity of the network. However, if an unauthorized person was able to reach the device, he may also be able to access the network ports the device attaches to. These ports could be used to plug in another computing device in order to launch attacks.

If a device is stolen, a hacker could use it as a test system for cracking passwords and determining routes; information which could then be used to compromise a live device in another store. If an attacker could compromise one of the network devices, he could use the device to attack other devices on the network, launch Denial of Service attacks, etc.

The result of these activities could result in the loss of data integrity, loss of critical network bandwidth, and so forth, which could significantly impact the company's ability to process its financial information.

Severity Rating: Category 1 - Critical

Controls to Prevent, Detect, and React

The members of the Design Forum determined that controls could be implemented to mitigate all of the risks that were identified. (As risks are

discovered in the future – and as new ones are introduced through change – they will be reviewed using the appropriate risk models.)

(**A**) A firewall is in place between the corporate and Store Information Systems networks. However, a firewall will not totally prevent malicious software from passing from one network to another. To protect the systems on each network from malicious software, anti-virus software will run on the systems (ISO 17799, 8.3.1). The anti-virus pattern files will be updated hourly on every network-connected device running an operating system (e.g. printers would not run anti-virus).

Furthermore, any system that will be connected through the firewall to another system will require a host-based Intrusion Detection System (IDS) and a host-based firewall (I.E. a one-to-one connection between a host on the corporate network and a host on the Store Information Systems network). The host-based IDS will provide real-time reporting and analysis for the host. The host-based firewall will restrict inbound and outbound traffic to specific ports. (ISO 17799, 9.4.6)

Likelihood of Occurrence: Medium

Significance of Impact (Severity Rating): Category 1 - Critical

Risk Level before Controls (Low, Medium, High): High

Risk Level after Controls: (Low, Medium, High): Low

(**B**) The firewall separating the corporate and Store Information Systems networks will run a hardened operating system with a minimum set of services. Only the administrators of the firewall will retain user and password credentials. The firewall device will reside in a physically secure location (ISO 17799, 7.2.1). Also, network cables and ports for routing devices and the firewall will reside in a secure location (ISO 17799, 7.2.3, 9.4.6).

Likelihood of Occurrence: Medium

Significance of Impact (Severity Rating): Category 1 - Critical

Risk Level before Controls (Low, Medium, High): High

Risk Level after Controls: (Low, Medium, High): Low

(**C**) The Store Information Systems network is connected to a firewall that separates it from the corporate network. However, the firewall alone cannot fully protect the systems from malicious software. See item A for controls.

Likelihood of Occurrence: Medium

Significance of Impact (Severity Rating): Category 1 - Critical

Risk Level before Controls (Low, Medium, High): High

Risk Level after Controls: (Low, Medium, High): Low

(**D**) The Store Information Systems Ethernet and VSAT networks are not separated by a firewall device; thus, without added protection, malicious packets may route freely between the networks. To mitigate this risk, each system on the Store Information Systems Ethernet network will run a host-based IDS and host-based firewall. The purpose of these security tools is: have immediate logging and reporting of unusual activity, limit the inbound and outbound ports that can communicate.

Likelihood of Occurrence: Medium

Significance of Impact (Severity Rating): Category 1 - Critical

Risk Level before Controls (Low, Medium, High): High

Risk Level after Controls: (Low, Medium, High): Low

(**E**) The VSAT network has limited bandwidth availability; thus, it is vulnerable to Denial of Service attacks. A Denial of Service attack would make it difficult or impossible to communicate with the computing and VSAT network devices in the stores. The controls defined in “D” above will help mitigate this risk.

Additionally, the VSAT network devices in the stores will have strict routing rules, which will only route data to specific systems. The purpose of these routing lists is to prevent the stores’ computing devices from sending data to any IP address that is not specifically allowed. Only a device with a specific IP address in the store would be allowed to communicate beyond the VSAT network device. In essence, a device could not plugged into the network at the store and communicate beyond the VSAT network device unless it had the proper IP address. (ISO 17799, 9.4.2, 9.4.4, 9.4.8)

Likelihood of Occurrence: Medium

Significance of Impact (Severity Rating): Category 1 - Critical

Risk Level before Controls (Low, Medium, High): High

Risk Level after Controls: (Low, Medium, High): Low

(**F**) The VSAT network device, without security measures, is vulnerable to tampering, both logically and physically. To mitigate this risk, the device is to be secured in a locked room in the stores' back rooms. Only specific personnel will have access to the room (ISO 17799, 7.2.1).

Since the device would not be accessible by unauthorized personnel, it could not be easily accessed directly (considering that the room is properly secured and monitored); however, the device would still be subject to logical tampering. For example, if someone were to unplug the cable from the store's computing device (or the network hub) and plug in another device, that device could communicate with the VSAT network device (assuming the IP address was discovered and the new device also had the single IP address that could communicate with the VSAT network device). This risk is noted. The CIO and Manager of Information Security deem this risk as acceptable.

Likelihood of Occurrence: Medium

Significance of Impact (Severity Rating): Category 1 - Critical

Risk Level before Controls (Low, Medium, High): High

Risk Level after Controls: (Low, Medium, High): Low

(**G**) The computing device may be vulnerable to physical and logical tampering without further controls. The computing device is to be secured in a locked room. Only authorized personnel are granted access to this area. (ISO 17799, 7.2.1)

In order to prevent an attacker from loading a rogue operating system onto the computing devices, the ability to boot from the floppy, CDROM, and USB devices is to be disabled in the BIOS of the device. The BIOS is to be password protected with a strong password.

Each device will require users to provide a username and password combination in order to access the device's operating system. All users in the stores will have unique username/password combinations.

All requests for new user accounts (or changes to existing accounts) must be handled by the District Managers of the store, and the request must have originated under that manager's user account. The District Manager must use his/her credentials to request new accounts. Store Manager's and District Managers are placed in security classes, which enable them to access an account management interface.

The usernames and passwords for new accounts are sent to the District Manager- under his/her secured session on the store's computing device. The

District Manager then communicates this information to the Store Managers. The Store Managers are required to change their passwords when they first login into the system. (ISO 17799, 9.2.1, 9.2.2, 9.2.3)

Activity for security-related functions on the device is logged to a central location- an Event Collection Server on the Store Information Systems Ethernet network. The Event Collection Server provides real-time reporting and communication to the administrative staff. This information is used to monitor, track, and react to security and other important events. (ISO 17799, 8.4.3 9.7.1, 9.7.2)

Likelihood of Occurrence: Medium

Significance of Impact (Severity Rating): Category 1 - Critical

Risk Level before Controls (Low, Medium, High): High

Risk Level after Controls: (Low, Medium, High): Low

Additional Controls and Their Effects

The members of the Design Forum agreed that the controls put in place are sufficient to mitigate the risks identified. As new risks are discovered or introduced, they will be evaluated and mitigated.

Implementation (Do)

Problem Identification and Actions

The following section describes the implementation of the controls that were chosen through the risk identification and analysis exercises. In this section, the specific problems are described, the actions to be taken are explained, and the steps for implementing the controls are detailed. In most cases, the "action taken" involves the application of an ISO 17799 control.

Problem: A firewall is in place between the corporate and Store Information Systems networks. However, a firewall will not totally prevent malicious software from passing from one network to another.

Action: To protect the systems on each network from malicious software, anti-virus software (ISO 17799, 8.3.1) and host-based IDS will run on the systems.

Steps:

- The anti-virus pattern files will be updated hourly on every network-connected device running an operating system (e.g. printers would not run anti-virus).
- Any system that will be connected through the firewall to another system will require a host-based Intrusion Detection System (IDS) and a host-based firewall (I.E. a one-to-one connection between a host on the corporate network and a host on the Store Information Systems network)
- The host-based IDS will provide real-time reporting and analysis for the host.
- The host-based firewall will restrict inbound and outbound traffic to specific ports.
- The Operations team will monitor the status of IDS reporting
    - Operations will follow appropriate procedures for handling incidents
        - ISO 17799, 8.1.1.c – instructions for handling errors or other exceptional conditions, which might arise during job execution, including restrictions on the use of system utilities
        - ISO 17799, 8.1.1.d – support contacts in the event of unexpected operational or technical difficulties

Problem: Without the application of security controls, the firewall may be vulnerable to tampering.

Action: A secure, enterprise-level firewall will be used to filter traffic and protect the networks.

Steps:

- The firewall separating the corporate and Store Information Systems networks will run a hardened operating system with a minimum set of services.
- Only the administrators of the firewall will retain user and password credentials.
- The firewall device will reside in a physically secure location (ISO 17799, 7.2.1).
- Network cables and ports for routing devices and the firewall will reside in a secure location (ISO 17799, 7.2.3, 9.4.6).

Problem: The Store Information Systems Ethernet and VSAT networks are not separated by a firewall device; thus, without added protection, malicious packets may route freely between the networks.

Action: To mitigate this risk, each system on the Store Information Systems Ethernet network will run a host-based IDS and host-based firewall.

Steps:

- The host-based IDS will provide immediate logging and reporting of unusual activity.

- The host-based firewall will limit the inbound and outbound ports that can communicate.
- The Operations team will monitor the status of IDS reporting
    - Operations will follow appropriate procedures for handling incidents
        - ISO 17799, 8.1.1.c – instructions for handling errors or other exceptional conditions, which might arise during job execution, including restrictions on the use of system utilities
        - ISO 17799, 8.1.1.d – support contacts in the event of unexpected operational or technical difficulties

Problem: The VSAT network has limited bandwidth availability; thus, it is vulnerable to Denial of Service attacks. A Denial of Service attack would make it difficult or impossible to communicate with the computing and VSAT network devices in the stores.

Action: Measures to protect the VSAT network will be implemented.

Steps:

- To mitigate this risk, each system on the Store Information Systems Ethernet network will run a host-based IDS and host-based firewall.
    - The host-based IDS will provide immediate logging and reporting of unusual activity.
        - The Operations team will monitor the status of IDS reporting
            - Operations will follow appropriate procedures for handling incidents
                - ISO 17799, 8.1.1.c – instructions for handling errors or other exceptional conditions, which might arise during job execution, including restrictions on the use of system utilities
                - ISO 17799, 8.1.1.d – support contacts in the event of unexpected operational or technical difficulties
    - The host-based firewall will limit the inbound and outbound ports that can communicate.
- The VSAT network devices in the stores will have strict routing rules, which will only route data to specific systems. (ISO 17799, 9.4.2, 9.4.4, 9.4.7, 9.4.8)
    - The purpose of these routing lists is to prevent the stores' computing devices from sending data to any IP address that is not specifically allowed.
    - Only a device with a specific IP address in the store would be allowed to communicate beyond the VSAT network device.
    - A device could not plugged into the network at the store and communicate beyond the VSAT network device unless it had the proper IP address.

Problem: The VSAT network device, without security measures, is vulnerable to tampering, both logically and physically.

Action: To mitigate this risk, the device is to be secured in a locked room in the stores' back rooms.

- Only specific personnel will have access to the room (ISO 17799, 7.2.1).
- Since the device would not be accessible by unauthorized personnel, it could not be easily accessed directly (considering that the room is properly secured and monitored); however, the device would still be subject to logical tampering.
    - For example, if someone were to unplug the cable from the store's computing device (or the network hub) and plug in another device, that device could communicate with the VSAT network device (assuming the IP address was discovered and the new device also had the single IP address that could communicate with the VSAT network device).
        - This risk is noted.
        - The CIO and Manager of Information Security deem this risk as acceptable.

Problem: The computing device may be vulnerable to physical and logical tampering without further controls.

Action: The computing device is to be secured in a locked room, the hardware will be secured, the operating system will be secured, and the device will record and report events.

Steps:

- Only authorized personnel are granted access to the locked room. (ISO 17799, 7.2.1)
- In order to prevent an attacker from loading a rogue operating system onto the computing devices, the ability to boot from the floppy, CDROM, and USB devices is to be disabled in the BIOS of the device.
    - The BIOS is to be password protected with a strong password.
- Each device will require users to provide a username and password combination in order to access the device's operating system.
    - All users in the stores will have unique username/password combinations.
- All requests for new user accounts (or changes to existing accounts) must be handled by the District Managers of the store, and the request must have originated under that manager's user account.
    - The District Manager must use his/her credentials to request new accounts.
- Store Manager's and District Managers are placed in security classes, which enable them to access an account management interface.

- The usernames and passwords for new accounts are sent to the District Manager- under his/her secured session on the store's computing device.
    - The District Manager then communicates this information to the Store Managers.
    - The Store Managers are required to change their passwords when they first login into the system. (ISO 17799, 9.2.1, 9.2.2, 9.2.3)
- Activity for security-related functions on the device is logged to a central location- an Event Collection Server on the Store Information Systems Ethernet network.
    - The Event Collection Server provides real-time reporting and communication to the administrative staff.
    - This information is used to monitor, track, and react to security and other important events. (ISO 17799, 8.4.3 9.7.1, 9.7.2)

Statements of Applicability

Dozens of controls were included in the ISMS. A few examples are shown below, along with explanations as to why some controls were and were not implemented.

Control: 7.x – Physical and Environmental Security

Having a computing device and network access in the stores is most significant risk this infrastructure introduces. This opens many opportunities for an attacker to take advantage of weak or nonexistent controls.

The rooms that house the computing devices and network equipment will be tightly controlled. Physical access to the room will be restricted to authorized personnel. All of the equipment and cabling will be kept in the secure, controlled rooms. The controls applied to this risk are considered the first line of defense (in the store) for the infrastructure.

Control: 9.4.8 - Network Routing Control

Strictly controlling the routing of packets for the VSAT network devices is a critical component of the ISMS for the project. Without this control in place, the administrative staff would be unable to prevent Denial of Service attacks on the VSAT network in the even that other controls were compromised. Also, this control helps limit traffic to the appropriate systems. For example, a store's computing device cannot communicate to another store due to the routing rules; thereby, eliminating unnecessary, undesirable traffic.

Controlling the network routing is, in actuality, part of a multi-layered approach to security. For instance, the controls applied to the computing device are intended to be one level of defense. Should an attacker compromise the device or go

around the device, the network routing controls (I.E. Access Control Lists) will help prevent the device from freely accessing the VSAT network.

Control: 10.3 – Cryptographic Controls
(Not selected)

The decision was made to not use cryptographic techniques to secure data in transit between the stores' computing devices and the systems at corporate. The CIO of Information Systems, the Manager of Information Systems, and the various technology owners agree that the controls put into place at the store – secure rooms, secure operating systems, secure and controlled network devices – provide enough security to mitigate the risks of unauthorized data transfers.

AUDIT PROCESS (CHECK)

The Information Security department will periodically audit the ISMS during the implementation of the infrastructure to ensure that controls are working effectively. Once the implementation phases have been completed, audits of manually selected controls will be performed quarterly. Exhaustive audits of the ISMS will be performed annually. The auditing checklist that Information Security will use is described in the table below.

The checklist will be used to test each control in the ISMS. When weaknesses are found, the results will be recorded and reported in the functioning security forum. The appropriate teams will remedy weak controls, using the auditing checklist as a guideline to ensure compliance.

Additionally, the Internal Audit department will perform quarterly and annual reviews to: (1) audit checklists and documentation produced by Information Security (2) audit the effectiveness of randomly selected controls to verify that the controls are functioning properly, and to ensure that the results Information Security is reporting are accurate.

ISO 17799 Control	ISO 17799 Section	ISO 17799 Audit Question	Reason for Control	Testing Process
3.1.1	Information Security policy document	Whether there exists an Information Security policy, which is approved by the management, published and communicated as appropriate to all employees. Whether it states the management commitment and set out the organizational approach to managing Information Security.	Information Security policies define acceptable use of the company's information facilities and processes, and help user community understand that security is "everyone's" job, and describe repercussions for noncompliance.	A) Gather existing security policies, if they exist B) Do policies state management's commitment to Information Security? C) Locate evidence of management's approval of policies (I.E. signed documents, etc.) D) Determine how policies are communicated to employees (e.g. Employee Handbooks) and determine whether employees are required to sign agreement/acceptance forms for policies
3.1.2	Review and evaluation	Whether the security policy has an owner, who is responsible for its maintenance and review according to a defined review process. Whether the process ensures that a review takes place in response to any changes affecting the basis of the original assessment, example: significant security incidents, new vulnerabilities, or changes to organizational or technical infrastructure.	The security policies should be treated as "living documents" and, therefore, should be updated by the owner as often as is necessary to ensure they are relevant.	A) Determine whether a policy owner is defined B) Obtain documentation regarding policy review procedures; Interview owner about review processes
4.1.1	Management Information Security forum	Whether there is a management forum to ensure there is a clear direction and visible management support for security initiatives within the organization.	The security forum is to provide leadership for security issues.	A) Interview person responsible for leading forum B) Obtain documentation or create documentation regarding forum's structure, membership, and purposes
4.1.2	Information Security coordination	Whether there is a cross-functional forum of management representatives from relevant parts of the organization to coordinate the implementation of Information Security controls.	The cross-functional forum should include members from multiple disciplines/departments and should address security issues.	A) Interview person responsible for leading forum B) Obtain documentation or create documentation regarding forum's structure, membership, and purposes
4.1.3	Allocation of Information Security responsibilities	Whether responsibilities for the protection of individual assets and for carrying out specific security processes were clearly defined.	Roles and responsibilities must be assigned to clarify and ensure: accountability, ownership, etc.	A) Obtain documentation describing roles and responsibilities B) Interview persons listed in documentation to determine if their understanding matches the documentation

4.1.5	Specialist Information Security advise	Whether specialist Information Security advice is obtained where appropriate.A specific individual may be identified to coordinate in-house knowledge and experiences to ensure consistency, and provide help in security decision making.	Critical decisions should be made with input from experts. This expertise may be available in-house, but should be sought externally, otherwise.	A) Interview technology owners to determine, specifying events if possible, what procedures are used to obtain advice B) If in-house expertise if used, determine whether it is sufficient- through interviews, certification, etc.
4.1.7	Independent review of Information Security	Whether the implementation of security policy is reviewed independently on regular basis. This is to provide assurance that organizational practices properly reflect the policy, and that it is feasible and effective.	The security policy's effectiveness should be reviewed by an external party to eliminate bias and provide outside expertise.	A) Interview policy owners and/or management to determine review processes B) Obtain feedback from past external party reviews
6.1.3	Confidentiality agreements	Whether employees are asked to sign Confidentiality or non-disclosure agreement as a part of their initial terms and conditions of the employment. Whether this agreement covers the security of the information processing facility and organization assets.	Since employees will have access to confidential information, they must be required to agree in writing that they will not disclose company information.	A) Obtain signed agreements: confidentiality and non-disclosure
6.3.1	Reporting security incidents	Whether a formal reporting procedure exists to report security incidents through appropriate management channels as quickly as possible.	Expediting the reporting of security incidents can greatly reduce the level of exposure the company incurs.	A) Obtain incident-reporting procedures B) Obtain evidence that procedures are communicated to appropriate personnel
6.3.2	Reporting security weaknesses	Whether a formal reporting procedure or guideline exists for users to report security weaknesses in, or threats to, systems or services.	Information regarding security weaknesses should be reported only to defined persons to avoid increased exposure (I.E. more users knowing)	A) Obtain reporting procedures for weaknesses, threats, etc. B) Obtain evidence that procedures are communicated to appropriate personnel
6.3.3	Reporting software malfunctions	Whether procedures were established to report any software malfunctions.	Software malfunctions may expose other weaknesses (I.E. security). This information should be reported immediately.	A) Obtain reporting procedures for software malfunctions. B) Obtain evidence that procedures are communicated to appropriate personnel

7.2.1	Equipment siting protection	Whether the equipment was located in appropriate place to minimize unnecessary access into work areas.Whether the items requiring special protection were isolated to reduce the general level of protection required.	Computer - and related - equipment should be protected from abuse, misuse, and damage. In this infrastructure, 5,000 computing devices are vulnerable to misuse, etc; thus, the physical devices should be protected, thereby providing another level of security.	A) Obtain configurations, schematics, etc. of building, rooms, and other relevant locations B) Inspect subset of locations for compliance
7.2.3	Cabling security	Whether the power and telecommunications cable carrying data or supporting information services are protected from interception or damage.	Cabling, if not properly secured, may be used to: tap in and capture data; or plug in foreign devices, which can then be used maliciously.	A) Obtain configurations, schematics, etc. of buildings, rooms, and the associated cabling configurations B) Inspect subset of locations for compliance
8.1.1.c,d	Documented operating procedures	Whether the security policy has identified any operating procedures such as backup, equipment maintenance, etc.	Operating procedures must be documented in order to be properly communicated and enforced.	A) Obtain operating procedures
8.3.1	Control against malicious software	Whether there exists any control against malicious software usage.	Anti-virus programs, firewalls, etc. must be used to minimize the possibility of the systems being compromised.	A) Determine products/methods of protecting systems and networks against malicious software. B) Ensure proper configurations and up-to-date programs (e.g. antivirus pattern files) C) Obtain firewall configuration documents
8.4.3	Fault logging	Whether faults are reported and well managed. This includes corrective action being taken, review of the fault logs and checking the actions taken.	Security and Event logging must be enabled and logs must be reviewed regularly so that corrective action can be taken quickly.	A) Obtain Security and Event Log settings from systems (document and inspect) B) Obtain procedures for reviewing logs and handling events
9.2.1	User registration	Whether there is any formal user registration and deregistration procedure for granting access to multi-user information systems and services.	User account management must be formally handled and action must be timely to ensure account creations, changes, and deletions do not expose the company's system to harm or misuse.	A) Obtain user account handling procedures B) Audit user account management process through observation and documentation review

9.2.2	Privilege management	Whether the allocation and use of any privileges in multi-user information system environment is restricted and controlled.	When multiple user accounts are available, these accounts must be tightly controlled to restrict their use to legitimate users and uses.	A) Obtain user account handling procedures B) Audit user account management process through observation and documentation review
9.2.3	User password management	The allocation and reallocation of passwords should be controlled through a formal management process.	Passwords should be tightly controlled (I.E. strong passwords, confidentiality of passwords, appropriate controls for resetting passwords)	A) Obtain user account handling procedures B) Audit user account management process through observation and documentation review
9.4.2	Enforced path	Whether there is any control that restricts the route between the user terminal and the designated computer services the user is authorized to access. Example: enforced path to reduce risk	Where possible and necessary, network communication should be restricted to specified routes to avoid unnecessary exposure of network packets.	A) Obtain network configurations B) Interview administrators C) Inspect network device configurations to verify accurate documentation
9.4.4	Node authentication	Whether connections to remote computer systems that are outside organization's security management are authenticated. Node authentication can serve as an alternate means of authenticating groups of remote users where they are connected to a secure, shared computer facility.	Node communication will be restricted to specified IP addresses for this infrastructure as a means to authenticate this node (an added layer of protection), even though other controls will be used to provide additional security.	A) Obtain network configurations B) Interview administrators C) Inspect network device configurations to verify accurate documentation
9.4.6	Segregation in networks	Whether the network is segregated using perimeter security mechanisms such as firewalls.	Firewalls, ACLs, and other network restriction mechanisms are used to limit: where traffic can originate from, which ports data can be traversed, the direction packets can travel, and where data can be routed.	A) Obtain firewall/network configurations B) Interview administrators C) Inspect firewall and network device configurations to verify accurate documentation

9.4.8	Network routing control	Whether there exists any network control to ensure that computer connections and information flows do not breach the access control policy of the business applications. This is often essential for networks shared with non-organization users.	Network restriction mechanisms are used to limit: where traffic can originate from, which ports data can be traversed, the direction packets can travel, and where data can be routed.	A) Obtain network configurations B) Interview administrators C) Inspect network device configurations to verify accurate documentation
9.7.1	Event logging	Whether audit logs recording exceptions and other security relevant events are produced and kept for an agreed period to assist in future investigations and access control monitoring.	Security and Event logging must be enabled and logs must be reviewed regularly so that corrective action can be taken quickly.	A) Obtain Security and Event Log settings from systems (document and inspect) B) Obtain procedures for reviewing logs and handling events

MANAGEMENT AND REMEDIATION (ACT)

The Information Security Management System implementation will be continually monitored and updated as needed. As noted in the Project Teams section above, the Design Forum will continue addressing security issues for one year after the implementation of the infrastructure. This forum will meet weekly. The company's primary Security Forum will address security issues related to the infrastructure after the year is completed.

As described previously, the Operations group, the Systems Administrators, Information Security personnel, etc. will continuously monitor security controls to ensure their effectiveness. Event logs from stores' computing devices, the network devices, firewalls, and Intrusion Detection Systems will be reviewed daily. Additionally, when critical events occur, each system is designed to flag the event as such. The Operations group monitors critical events. These events are immediately reviewed by the appropriate system owner and a member of the Information Security group.

If a critical event is reviewed and the system owner and Information Security respondent determine it is necessary, an emergency meeting of the functioning security forum (Design or Security) will be called. The team will take the appropriate measures to ensure that the weakness will be corrected or controlled.

When the Design Forum – and, later, the Security Forum – meets each week, security and design weaknesses will be addressed. Any and all security issues related to the infrastructure may be addressed in this forum (low priority to critical issues). The forum retains the authority to implement controls to mitigate risks; however, the CIO of Information Systems and the Manager of Information Security must agree and sign-off on any proposed changes.

Documents related to the ISMS are considered "living" documents; hence, they are subject to ongoing scrutiny and changes. Changes are not, however, made without first going through a review process. The functioning security forum will review changes before they are implemented. The Manager of Information Security owns the documents that relate to the ISMS. The CIO of Information Systems and the Manager of Information Security are responsible for approving the security documents (policies, procedures, etc.).

The ISMS will also be reviewed periodically by two external parties. Firstly, the company's Internal Audit department will perform a quarterly analysis of the ISMS. When weaknesses are found, the Senior IT Auditor will present his findings to the functioning security forum. The members of the functioning security forum will respond to the findings in the appropriate manner- applying new controls, remedying weaknesses, creating/modifying policies and procedures, etc.

Internal Audit's quarterly reviews serve several purposes; including, locating weaknesses that the technical and security teams may not identify, preparing the teams for the annual audit of the ISMS that is performed by the external auditors; etc.

An outside auditing firm will perform annual audits of the infrastructure. This audit will help XYZ ensure that its controls are sufficient to protect the enterprise from security-related incidents. The results will be presented to the Executive Management team, as well as all other teams involved in the ISMS's maintenance.

Final Comments

The stability and security of information systems is of the utmost importance to XYZ. The company's Information Security team, along with members of Executive Management and the CIO of Information Systems, collectively made the decision to use ISO 17799 as a guideline for building the Information Security Management System for the computing infrastructure in the stores.

The security of the infrastructure cannot ultimately be guaranteed by the use of the ISMS; however, the process of building and maintaining the ISMS provides the means necessary to effectively identify and mitigate risks associated with infrastructure. The consensus amongst the teams involved with this implementation is that the ISO 17799 controls that were selected and applied have mitigated all known risks to an acceptable level.

WORKS CITED

International Organization for Standardization. *Information technology – Code of practice for information security management.* 1st ed. Geneva, Switzerland: International Organization for Standardization, 2000.

SANS Institute. Track 11 – SANS 17799 Security & Audit Framework: Risk Management, Security Compliance and Audit Controls. 2004.

FMECA. FMECA.COM. 14 Jan. 2003. Kinetic, LLC. 08 Aug. 2004. <www.fmeca.org>.