Global Information Assurance Certification Paper

AUDITING YOUR DATA CENTER ACCESS CONTROL SYSTEM: AN INDEPENDENT AUDITORS PERSPECTIVE

Barry Cox
GSNA Practical Version 2.1

Abstract

A thorough audit of any system looks at the physical access to the server(s). In most cases the data center is where that system resides. The ability to properly control and monitor access to a corporate data center has become a large task. Gone are the days of key or code locked doors. Today electronic access control systems are required. Access control systems that use the very technology they are designed to protect. The ability to properly audit you access control system is the key first step to protecting all of the system that reside within any secure data facility.

TABLE OF CONTENTS

Assignment One

Company Overview

ABC Communication Inc. is a provider of a wide array of communications related products. It offers voice and data services to customers from a wide variety of industries. It deals at both the business and consumer level. In an effort to build new sources of revenue the company is diversifying itself and is looking towards its established data center as a new possibility.

ABC has spent a significant amount of money building a data center that was designed for just their internal needs. The facility is located within one of their main operational offices which is considered extremely secure and has state of the art environmental and safety controls. The building hosts internal employees and has no direct public access. Most of the employees do not work directly in the data center. There is a small group that handles that responsibility. The building also houses several contractors at various times throughout the year.

Strategically and financially there is considerable benefit to using the capital investment already made in this facility to promote it as an external hosted services environment. In consultation with various industry experts the plan was deemed acceptable with one recommendation. The majority of clients who host their data and key systems with outsourced data facilities expect high standards for physical access control to the data facility. This risk increases when external customers begin visiting the site to deal with their respective systems in the data center.

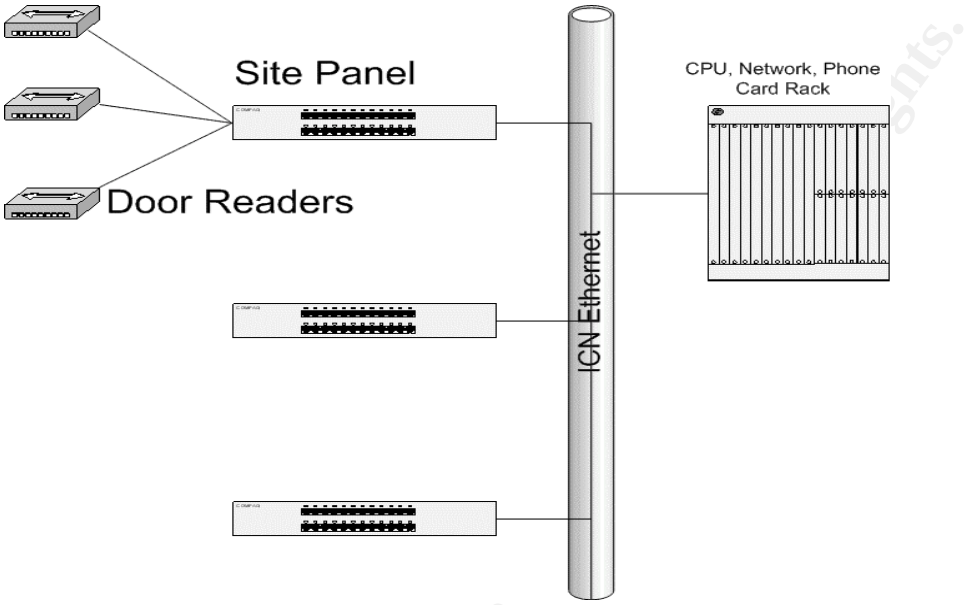
The building has a 24 hour guard at the street level. To enter the building you need to either have a visible ID that has access credentials on it or you need to be signed in. Through out the building code locked doors are used to restrict access. This was seen as unacceptable for a hosted data facility. There are a variety of minor reasons, but the two major ones are that logging is required and credentials can very easily be shared between people.

Previously ABC purchased an access control and alarm monitoring system. They bought the PACOM GMS32 product and installed in some buildings. They decided to expand it to the data center facility. It is used with proximity cards and readers on all doors located outside and inside of the facility. The system uses a client/server model across the company's IT network to manage secure access to this room and others within the company.

At the request of management, an independent audit of this system was called for to provide to customers reassurance that the system is being managed properly. It also will guide ABC in the hardware, software, policy and procedure decisions with the system.

The System

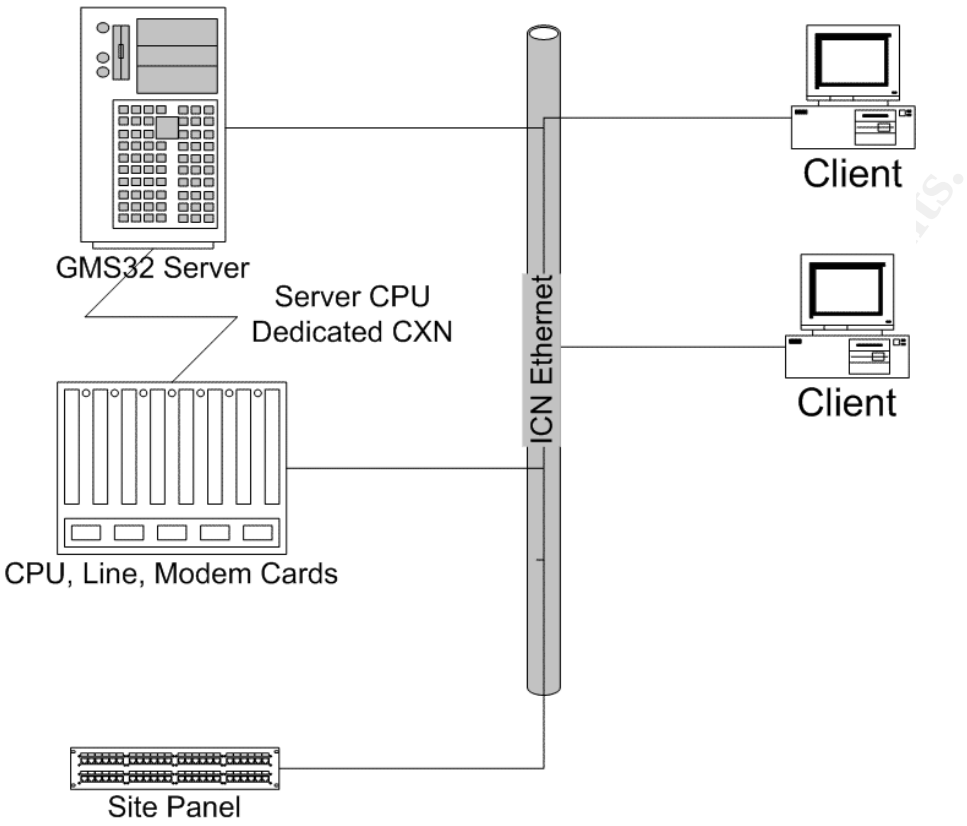
There are really two systems at work with this access control system. There is a networked infrastructure that facilitates the operation of the doors. The operational pieces are readers, panels, CPU cards, line cards, and dialup cards. The following diagram shows how these are connected:



A proximity card is presented to a reader which is hard wired to a panel. The panel can do localized processing of the request if it has a record stored locally in memory that verifies the card is valid. If not, it will communicate with the CPU card and download that record from the database. It communicates across the Ethernet network to the CPU card to updates the record using a proprietary security protocol which is encrypted. The panel will also communicate back all the events that it sees such as valid card swipes, invalid swipes, door ajar alarms, etc. The line card is the network intelligent interface that accepts communication from the panel and directs it to the CPU card. Some sites do not have LAN access so a modem line card is configured to get dialup connectivity when required. The whole system can convert to dialup between the CPU and panels anytime that network access is lost.

The second, and most important part of the system, is the server and client stations. They provide a GUI interface for the system to be programmed, database storage, alarms monitoring, logging and report generation. The server interfaces with the CPU card through a direct cable connection. The clients

connect to the server over the Ethernet network. The diagram below gives a high level overview:



The focus of this audit will be on the client/server (CS) portion to better evaluate the risks associated with the hardware, software, processes and procedures used to secure the data center. The CS portion is comprised of a Windows NT 4.0 Server running on Compaq Proliant 4500 server with a 10 gig HD and 256 megabytes of RAM. It runs the PACOM GMS32 version 1.0 server software. That software uses a Microsoft SQL database with a proprietary front end to deliver service. The server interfaces with client stations that are Compaq Deskpro P350's with 1 gig drives and 128 megabytes of RAM and running Windows NT 4.0 Workstation. These workstations are dedicated for only this purpose and run the GMS32 client software.

Evaluating System Risk

This system was chosen for audit primarily because failure to secure the system that controls physical access to your data center places every system in the center at an elevated level of risk. The complexity of this system also raises the probability of some known vulnerabilities being overlooked. In a layered security approach you need to assure that physical console access is covered before moving on to address other risks to your key servers. This system is a key layer in protecting the databases that hold your most critical information.

The high level risks associated with this system are listed in the table below:

Risk Item	Probability	Consequences
Poor authentication management on the server and application.	High	Unauthorized persons could enter the system through any of these points and change security parameters, add security levels or lock persons out of the system.
Weak disaster recovery or business continuity planning. You need assurance that the security system will maintain integrity in the event of an unforeseen incident.	High	System could go down and release doors exposing all systems in data center. Could also inhibit the ability to allow access to key areas to address the original event.
Insufficient logging and procedures for system events and alarms on the application and server	High	There could be a compromise of the system and the logs wouldn't be available to do proper forensics to determine the impact of the breach.
Limited or incomplete policy around system administration	High	The lack of policy and proper procedures is the primary cause of bad choices by people working with the system. These mistakes could lead to an erosion or elimination of the system controls.
Improper screening of people requesting access cards to the secure data center	Med	The goal is to keep people out of the data center that shouldn't be there or cannot be trusted in that area.
Poor configuration and management of key devices to protect them from known vulnerabilities	High	If the any part of the system can be attacked and thus disable the functionality of it that could be used to prevent alarm notifications or changes

and viruses.		to an individual card security clearance
Weak or non-existent change managment practices	High	Doors could be left unsecured because of poorly executed changes. Programming or configuration errors could flood the network and cause failures on other systems within the data center.
Poor physical security on the consoles and system components	Medium	All of the logical controls possible cannot overcome the risk of permitting physical access to the console for someone who should not be trusted with it.
Providing secure access to outside parties to service your system within your rules and policies.	High	All too often companies lock down their own people but totally ignore the threat of vendors having remote access to their network with little or no controls around their activities.

The focus of this audit is to understand the risks associated with the access control system that is protecting the data center from a higher level technical view combined with the policies and procedures the govern day to day operations. A detailed analysis of the any individual component such as Windows NT Server, Windows NT Workstation or Microsoft SQL will not be done. The pieces of each area that are key to evaluating the system as a whole will be looked at but a comprehensive security analysis of each is not in scope. The focus will be on the practice of managing the access control system as it pertains to the data center.

Current State of Practice

This audit is focused on a key physical control. This control is usually an essential layer in determining the overall security of any system residing in the data center it protects. It is covered in most information assurance audits. The system is responsible for physical events that are managed by a complex IT system. The processes and policies are as important as the components that make up system.

To successfully audit an access control system for a data center you need to separate it into two areas. The first is the processes and controls that are used to manage the system. The second is a high level evaluation of the key components that comprise the system. In this case that would be the hardware and software of the PACOM GMS32 installation combined with the Windows NT client/server environment is works on. To get bogged down in the details of the each particular element widens the scope and the cases the audit to be more complicated than required. Additionally the panels and readers offer little of value as they are nothing but dumb terminals on a wire. The server is the core.

There is very little research done on auditing access control systems. There are a lot of standards organizations that define criteria for these systems, and data centers, but few discuss auditing an existing system. They focus on design standards.

For the first phase of this analysis there are industry sources that define criteria for developing access control policy. These are some resources available for physical access control practices:

White Paper from Core Street
http://www.corestreet.com/whitepapers/SecurePhysAccess.pdf

Handbook of Information Security Management Web Book
http://www.cccure.org/Documents/HISM/ewtoc.html

Electronic Access Control – By Gerard Honey

Introduction to Security 6th Edition – Robert Fischer/Gion Green

Encyclopedia of Security Management : *Techniques and Technology* – John J. Fay

Protection of Assets: Volume 1 – POA Publishing

There is also some information available for data center controls:

Microsoft Solutions Paper
http://www.microsoft.com/solutions/msa/evaluation/overview/idc/archgoals.asp

Self Audit Checklist from Institute of Internal Auditors
http://www.theiia.org/ecm/guidance.cfm?doc_id=2670

SANS Reading Room Paper by Sean Heare
SANS Institute Information Security Reading Room - Data Center Physical Security Checklist

ABC Company also had the following documents that provided their standards and policies.

-ABC IT Security Policies
-GMS32 Access Control Operations Manual
-ABC Security Program Overview
-Security Guidelines for Developers
-ABC Policy for Removing Access Credential After Termination
-ABC Securing Windows NT Guidelines

There is very little information available that specifically discusses the GMS32 product outside that which is available on their website. They have since began using the newer name of Access32 which is two revisions ahead of the installed product at this location

http://www.bellgroupplc.com

There was a detailed manual that shipped with the product:

GMS-32 Card Access Training Manual

The Windows NT Server practices are easier to find. As are the Windows NT workstation practices.

SANS Reading Room Paper by Satnam Bhogal
FAQ for How to Secure Windows NT

The Center for Internet Security
The Center for Internet Security CIS Benchmarks and Scoring Tool for Windows 2000 and Windows NT

Nysecurity.nu web site

ntsecurity.nu - Toolbox

SANS Publication – Windows NT Security : Step by Step
www.sans.org

NSA Security Guides
http://nsa2.www.conxion.com/winnt/download.htm

Also the use of Internet search engines off great help.

www.google.com
www.yahoo.com

Assignment Two

Checklist Item One - SERVICE PACKS AND HOT FIXES FOR SERVER

Reference	http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/Tools/MBSAhome.asp
Control Objective	Mitigate the risk associated with improper patching of the server.
Risk	Each of the exploits fixed by the patches or hot fixes represents a vulnerability to the system that is publicly known. Failure to apply these in a timely manner leaves the server open to attack and possible compromise.
Compliance	A vulnerability scan of the system shows that all patches that can be applied have been.
Testing	1. Download a known good copy of Microsoft Baseline Security Analyzer. 2. Burn it to a CD and install it on a system running W2K or XP. 3. Run MBSA and review the results provided by the tool. 4. Ensure that "SQL vulnerabilities" is checked to ensure added protection for the database. 5. Save the results.
Objective/Subjective	Objective - It is easy to compare lists to decide if the patches have been applied or not.

Checklist Item Two - SERVER ACCOUNT PASSWORD POLICIES

Reference	-ABC Company Policy -FAQ for How To Secure Windows NT http://www.sans.org/rr/win/NT_FAQ.php
Control Objective	Assure that passwords for the user accounts on the server meet corporate security policy standards and aren't weak and easily compromised.
Risk	If the passwords for the clients are weak it is extremely easy to crack them and use that account for malicious purposes.
Compliance	Accounts meet the standards outlined in the corporate password security policy of 8-10 characters, alpha-numeric, and unique.
Testing	1. Gather the related policies for passwords for user accounts on domains. 2. Download a known good copy of Microsoft Baseline Security Analyzer.

	3. Connect to the server at an administrator level from an XP or 2000 workstation.(MBSA doesn't work on NT) 4. Input the IP address of the server and run MBSA against it. Review the results provided by the tool for password specific results. 5. Pick an administrator and basic user account and review the settings on it in the user manager. Assure they match the security policy requirements.
Objective/Subjective	Objective – Either the password is within policy guidelines or it is not strong enough.

Checklist Item Three - BACKUP PROCEDURES FOR WORKSTATIONS AND SERVER

Reference	Auditing Paper - Auditing a SQL Server 2000 Server – Graham Thompson
Control Objective	Verify that backups of these two systems will be available and useful if needed.
Risk	If these systems crash or are compromised "last known good" key files and databases are required to perform a timely rebuild. If they aren't available critical data may be lost.
Compliance	Retrieve a successful sample of restored files from a backup and having an acceptable backup policy with well documented procedures.
Testing	1. Take the most recent backup tape and load it in the tape drive. 2. Using the backup program, browse the contents of the backup and select a file or directory to restore that should not have changed. 3. Restore the selected item to another location and compare it to the copy in place on the server. 4. Review the corporate policies on backups. 5. Walk through the documented procedure for backups to verify process integrity.
Objective/Subjective	Object and Subjective – The file restore is objective because it either worked or didn't. The policy and procedure review is subjective.

Checklist Item Four - GENERAL SERVER VULNERABILITY CHECK

Reference	http://www.gfi.com/lannetscan/wplannetworkscanner.htm Auditing Novell iFolder Professional Edition V2.0 – Jerry Shenk

	http://www.giac.org/practical/GSNA/Jerry_Shenk_GSNA.pdf
Control Objective	Assure that the server is free of a wide range of known vulnerabilities
Risk	With known vulnerabilities or risky services running the system is at a significantly greater risk of being compromised.
Compliance	Scanning tool report should show no serious risks or issues present on server.
Testing	1. Run a vulnerability scanner against the server. 2. Review the report and analyze the findings.
Objective/Subjective	Objective – There are either high risk items present or not. There is a minor subjective component in determining if a risk is high but most scanners categorize the risks for you so it becomes primarily objective.

Checklist Item Five - REMOTE CONSOLE MANAGEMENT OF THE SERVER

Reference	Personal Experience
Control Objective	Assure that the remote management tool (PCAnywhere) used to administer the server is not causing risk
Risk	If the tool is improperly configured it will leave the server exposed. Another unauthorized party could connect to the server and compromise it.
Compliance	Assure that all settings outlined in the corporate policy "Securing PCAnywhere" are followed.
Testing	1. Go to the server and launch PCAnywhere. 2. Review all of the settings stated in the policy. 3. Go to a PCAnywhere client station and try to connect to the server to see if the challenges are working.
Objective/Subjective	Objective – The server is either configured properly or it isn't and the client station can either successfully connect or not.

Checklist Item Six - GMS32 APPLICATION ACCOUNT PASSWORD POLICIES

Reference	Personal Experience
Control Objective	Assure that passwords for the user accounts within the application are within corporate security policy standards.
Risk	Application passwords are your last line of defense against malicious attempts to break into the system. If the server is compromised a valid username and password for the application is still required. Once obtained unapproved access can be granted, controls changed or other

	malicious activities.
Compliance	Accounts meet the standards outlined in the corporate password security policy of 8-10 characters, alpha-numeric, and unique.
Testing	1. Review the system documentation and account management procedures for GMS32. 2. Have a new ID created for you on the system by the administrator and document all the steps of the process from this point forward. 3. Login into the application using that ID. 4. Try changing the password to 12345 which should not be allowed. 5. Logout and log back in and try the initial password given to you buy the support person with other user names to see if any still have the original password. 6. At the server console inspect the settings for your test account as they relate to passwords.
Objective/Subjective	Objective – Either the passwords standards of the system meet the policy or they don't. There is a subjective component in that some controls may not automatically force the settings outlined in the policy so the auditor is required to decide if this is actually being done.

Checklist Item Seven - APPLICATION PRIVILEGE ASSIGNMENT

Reference	Mosler GMS32 Training Manual
Control Objective	Excessive rights assigned to application level ID's
Risk	Someone with elevated rights and without proper training can unintentionally cause serious damage to the system. Also poorly assigned rights can provide high level abilities to someone who isn't properly screened to use them
Compliance	All accounts contain only the rights needed for the account owner to perform the functions they are required to do in their role.
Testing	1. Review the system documentation and operational procedures to understand the roles associated with the application. 2. Review the documentation that outlines which rights each role ID should have such as administrator or operator. 3. Review the administration accounts by entering the Operator Configuration section, selecting an admin ID and creating a printout of the privileges assigned to each. 4. Review the station operator accounts by entering

	the Operator Configuration section, selecting a station operator ID and creating a printout of the privileges assigned to each. 5. Review the printouts to determine if the rights follow the least privilege model.
Objective/Subjective	Objective – Either the rights assigned to an ID are correct or excessive. There is no subjectivity because the documentation should outline what is needed for each role.

Checklist Item Eight - BACKUP AND RESTORE PROCEDURES FOR THE APPLICATION

Reference	Auditing Paper - Auditing a SQL Server 2000 Server – Graham Thompson
Control Objective	Assure that proper procedures are in to restore the application.
Risk	The application database is the key file that holds the security details about access levels, groups and the assignment access to individuals. Also, the database references files from other directories that are required for proper operation. If these are lost or backups are not current partial or total loss of the system security configuration will result.
Compliance	There is an acceptable procedure and sufficient documentation for backing up the application is in place and used.
Testing	1. Obtain copies of the documentation and procedures for backing up this application and compare it to the corporate backup policy. 2. Review system operations documents and determine a recent failure where application files were restored from backup. 3. Review the steps taken and the outcome. 4. Obtain a copy of a recent backup and restore just a single directory. 5. Compare the contents the directory on the server.
Objective/Subjective	Objective – The previous backup restore either worked or did not and the test restore of the file is either successful or not.

Checklist Item Nine - SERVER CONFIGURED AND HARDENED DURING INSTALLATION

Reference	ABC Securing Windows NT Guidelines

Control Objective	Ensures that known and documented OS controls for server were done during installation as per the company requirements.
Risk	If the corporate checklist for installing and hardening a Windows NT server was not followed completely during the installation the server could have several known exploits or vulnerabilities on it. This would make it easy to compromise.
Compliance	All relevant items on the original checklist were addressed.
Testing	1. Obtain a copy of the current corporate checklist for installing and hardening Windows NT Server 4.0. 2. Gather any previous revisions of the document and isolate the one that would've been the most current during the installation of this server. 3. Compare the two documents and highlight any changes such as added steps or checklist items. 4. From that list of controls randomly pick an appropriate subset and verify that they have been applied to the server. 5. Pick an appropriate number of controls from the current checklist and test to see if they have been done as well. 6. Review output logs from vulnerability and baseline scans to provide evidence of checklist items that may have been missed.
Objective/Subjective	Objective – Either the tested items on the standardized configuration checklist for the server were done or they weren't. There is a small subjective judgment used in selecting which items will be tested.

Checklist Item Ten - PHYSICAL SECURITY OF THE SYSTEM CONSOLES

Reference	Microsoft Solutions Paper http://www.microsoft.com/solutions/msa/evaluation/overview/idc/archgoals.asp Self Audit Checklist from Institute of Internal Auditors http://www.theiia.org/ecm/guidance.cfm?doc_id=2670
Control Objective	Server and client consoles must be securely protected
Risk	If someone can get console access to the server or client station they have a much greater chance of getting unauthorized access to the system and change security access parameters for individuals or groups.
Compliance	Console security is available only to those who require it and have been approved.

Testing	1. Review the access list for people who can enter the rooms where both the server and clients reside. 2. Physically visit both locations and observe the behavior of persons entering and leaving the room to see if they hold doors open for people without passes etc. 3. At the server cabinet, check to assure the door is locked and that the mouse and keyboard used for the server are locked inside the cabinet. **Note that if a keyboard switching device is present make sure the security system has its' own mouse and keyboard. 4. Visit the client station sites and assure the systems are kept in offices locked from public access.
Objective/Subjective	Subjective – The overall security approach to protecting the consoles requires a judgment call at the end of the process to decide if it works. While some tests may be objective, the whole process isn't.

Checklist Item Eleven - BUSINESS CONTINUITY OR CONTINGENCY PLANNING

Reference	Auditing The Cisco AS5300 Remote Access Router – Cliff Ziarno http://www.giac.org/practical/GSNA/Cliff_Ziarno_GSNA.pdf
Control Objective	Assure that proper planning has been to done to facilitate continuity of access control service.
Risk	In the event of an unexpected event such, as a power failure, the ability to control access to the data center is crucial because the inside systems are also most likely impacted by the same event. You could find yourself in a situation where you are locked out of the facility or you may see locked doors suddenly open.
Compliance	There is a documented business continuity plan for this system which has been approved by the manager responsible for the area.
Testing	1. Get a copy of the business continuity plan that covers the Access Control System and review it. 2. Meet with the manager responsible for business continuity planning to determine if they have reviewed the plan and if so, do they endorse it. 3. Confirm that any physically verifiable items such as UPS, backup tapes, spare part, etc. are in fact in place as described in the policy. 4. Determine if any previous events have taken place when the system was unavailable and if so:

	-was the plan useful? -did the system respond as expected?
Objective\Subjective	Subjective – After gathering all of the evidence and information a judgment call has to be made to determine if the plan is acceptable or not.

Checklist Item Twelve - SYSTEM MODIFICATION\CHANGE MANAGEMENT

Reference	Personal Experience
Control Objective	Assurance that changes to the system are done in accordance with the guidelines of an acceptable change management process.
Risk	Allowing work to be done without approval could lead to changes in the security configuration management does not know about. Poorly tested changes could impact other systems on the same network if they are implemented without notification or review.
Compliance	All changes are approved, documented, tested prior to implementation, done during approved times and have proper back out procedures in the event of complications.
Testing	1. Obtain a copy of the corporate change management document. 2. Review a recent system change such as a service pack upgrade to the server, 3. Ensure that the corporate change management process was followed by reviewing: -change request form -approval or sign-off -activity log -back out plan
Objective/Subjective	Objective – Assuring that all areas of the current policy are followed is objective however reviewing them to make sure it delivers the right results is somewhat subjective.

Checklist Item Thirteen - APPLICATION ALARM RESPONSE

Reference	GMS32 Access Control Operations Manual
Control Objective	To verify that higher risk alarms generated by the system are being acknowledged and answered.
Risk	The alarms signal a security violation or a system failure. If they are not acknowledged or answered to the risk associated with the alarm remains unattended and could lead to a compromise in security.

Compliance	High risk alarms are being logged acknowledged and properly addressed.
Testing	1. Review the alarm notification section of system documentation to understand what alarms are available. 2. Go to the server and review the system events log to find a previous system alarm event. 3. Check with the system operations documentation to see if anyone responded to the alarm. 4. Go the data center and hold the door open for around five minutes. 5. Wait to see if the alarm triggers a response. 6. Return to the server, or a client, and check to assure that the door ajar event showed up in the logs.
Objective/Subjective	Objective – Alarms are either being dealt with properly they are not. Logs and documentation will prove this.

Checklist Item Fourteen - TRAFFIC ENCRYPTION\INTERCEPTION

Reference	Personal Experience
Control Objective	Assure the integrity and security of network traffic for the system.
Risk	If traffic that can be captured with a sniffer can be read key passwords could be captured, packets could modified or a whole series of other attacks.
Compliance	Intercepted traffic does not reveal any useful information.
Testing	1. Setup a sniffer on the subnet a workstation is on. 2. Capture traffic on the wire. 3. Login and logout of the application several times. 4. Run a report query on the system. 5. Review the logs from the sniffer to look for traffic from the workstation and assess if the PACOM proprietary protocol reveals information.
Objective/Subjective	Objective – Either the packets are revealing or not.

Checklist Item Fifteen - ANTI-VIRUS PRACTICES FOR THE SERVER

Reference	http://www.nai.com/common/media/vil/pdf/free_AV_tips_techniques.pdf
Control Objective	Protect the server and workstations from being infected with viruses.
Risk	If a virus can make it onto the server it can wipe out the entire system, alter key files, or create vulnerabilities in the

	server configuration that can allow it to be easily compromised.
Compliance	The server is running approved virus scanning software with a process in place to install the latest definition files in a timely manner.
Testing	1. At the server console, go to program files and look for the anti-virus program. (In this case Network Associates) 2. Launch the virus scan console. Then go into the help section and 'About McAfee Virus Scan'. 3. Document the scan engine and virus definition settings. 4. Visit the product website and verify the scan engine is supported and if so validate the age of the definition files. 5. Consult the corporate anti-virus policy to ensure there is a procedure for timely definition file updates.
Objective/Subjective	Objective – This process has enough documented evidence that it is objective however there is a small area with some subjectivity. The decision on what constitutes a timely update for this particular system is somewhat subjective.

Checklist Item Sixteen - APPROVING REQUESTS FOR DATA CENTER ACCESS

Reference	Personal Experience
Control Objective	To allow only those requiring access to the data to have it.
Risk	If proper screening of requests is not done, and access can easily be obtained then, then risk increases. Primary concerns are persons of questionable trust getting access and people without proper training having the ability to access server consoles.
Compliance	Everyone on the access list has been properly screened from a security and operational perspective.
Testing	1. Option copies of the procedure for granting access to the data center. 2. Go to a client station with the client software for GMS32 active. 3. Go to the card holder search function and search on the site number (building), reader group (door) and all valid cards for the data center. 4. Review the list with the security clearance officer and the operations person responsible for approving data center access to understand if they

	are have records to verify the approvals. 5. Ask to view the usage and sign-off logs for any temporary passes in circulation and spot check that list by following up with users to see why there needed to be in the center.
Objective/Subjective	Objective – The people who have access have either been screened against the criteria for entering the data center or they haven't been.

Checklist Item Seventeen - PROCESS FOR REMOVAL/CHANGE OF ACCESS

Reference	Personal Experience
Control Objective	To assure that terminated employees, or employees changing job functions were data center access is needed, have those rights removed.
Risk	Disgruntled or malicious persons should not be allowed back into the data center after their access has been revoked or you face a huge sabotage or theft risk. If a persons' status changes the access must be addressed quickly to narrow the window of opportunity for these actions to take place.
Compliance	There is a process and procedure in place to effectively manage the removal of people who no longer are authorized to have it.
Testing	1. Obtain a copy of the documentation for terminating access to the data center. 2. Get access to the list of people who recently have had their access for the data revoked. 3. Go to the client station for the GMS32 and do a search for that person in card access configuration screen. 4. Review that status of their access card and if it is valid check their access levels to ensure they no longer have data center swipe access. 5. Review your checklist #16 list that shows valid access card holders for the data center. If there were ones that were on the list and not approved follow up to see if they were suppose to be removed and it hadn't been done. (However if the list does not contain unapproved names than it may support the idea that previously terminated employees were removed.)
Objective/Subjective	Objective – The access list either includes names of people who have been denied access to the data center or

	it doesn't. The policy and procedure are somewhat subjective but overall this analysis is objective.

Checklist Item Eighteen - SECURITY AWARENESS PROGRAM

Reference	Auditing The Cisco AS5300 Remote Access Router – Cliff Ziarno http://www.giac.org/practical/GSNA/Cliff_Ziarno_GSNA.pdf
Control Objective	Ensure that people are aware of the security policies and procedures of the company and are trained in their application within the data center.
Risk	If people do not have access to these documents and given the chance to review them they will likely not conduct their activities in accordance with them. Especially data center specific guidelines like testing fixes off of the production network.
Compliance	There is an opportunity and requirement for people to review security policies and ask questions about them.
Testing	1. Go to the corporate Intranet site and look for the security policies. 2. Review the content of the site to see if there is an email address or contact information to ask security questions. 3. Check with the Human Resource group to see if new employees are advised of policies. 4. Check to see if the security group provides awareness seminars for employees. 5. Visit the data center to see if the policies are posted anywhere. 6. Review sections of the policy that would apply to the data center and physically review some of them to see if they are being followed.
Objective/Subjective	Subjective – It is a subjective decision that has to be made as to whether the there is sufficient effort put into the awareness program to call if effective.

Checklist Item Nineteen - SERVER DIALUP SUPPORT MODEM CONTROL

Reference	Personal Experience
Control Objective	Assurance that the modem used as a backup to access the system is not causing risk.
Risk	If the modem is left plugged in and connected to the server a hacker could easily use it to dial into the server remotely and compromise it.

Compliance	The modem is disabled when not in use and poses no elevated risk to the system.
Testing	1. Physically inspect the server cabinet to verify the modem is not plugged into the phone line. 2. Inspect cabinet to ensure that the modem cannot be reached without open the locked door. 3. Check to see if the phone line is programmed to record the number of all incoming calls. If so review the log to see how has been calling. 4. Verify that the line is not programmed to allow outgoing calls from the server. 5. Try a social engineering activity by calling the support line for the data center and pretend to be the system vendor. Ask for the modem to be connected.
Objective/Subjective	Objective – The modem is either non-functional and poses no risk when not in use or it isn't. The items can be independently verified.

Checklist Item Twenty - RESTRICTED VPN ACCOUNT FOR VENDOR

Reference	Personal Experience
Control Objective	The VPN account provided to the vendor follows the least privilege model and requires notification to activate it.
Risk	If the account can be used whenever you want and isn't restricted someone at the vendor location who has the motivation could use the access to probe and scan the network. They could gather key system information and confidential data rather easily. They could also remotely perform changes to the system without approving them through change management and the customer may not know they've done the work.
Compliance	The account cannot be accessed without alerting the company that you want to use it. Also the access must only allow the vendor to reach their server IP only.
Testing	1. Obtain the username for the account and review the rights assigned to it on the VPN switch. 2. Verify those rights only allow direct access to the server required. 3. Check the procedure for logging into the account to determine: -under what condition is it used? -is their a requirement the vendor contact the customer fist? -can the vendor proceed without consulting the

	client?
Objective\Subjective	Objective – The test is easy to do and repeat. The account is restrictions can be tested to their minimal level and the authentication procedure either requires contact with the client first or it doesn't.

Assignment Three

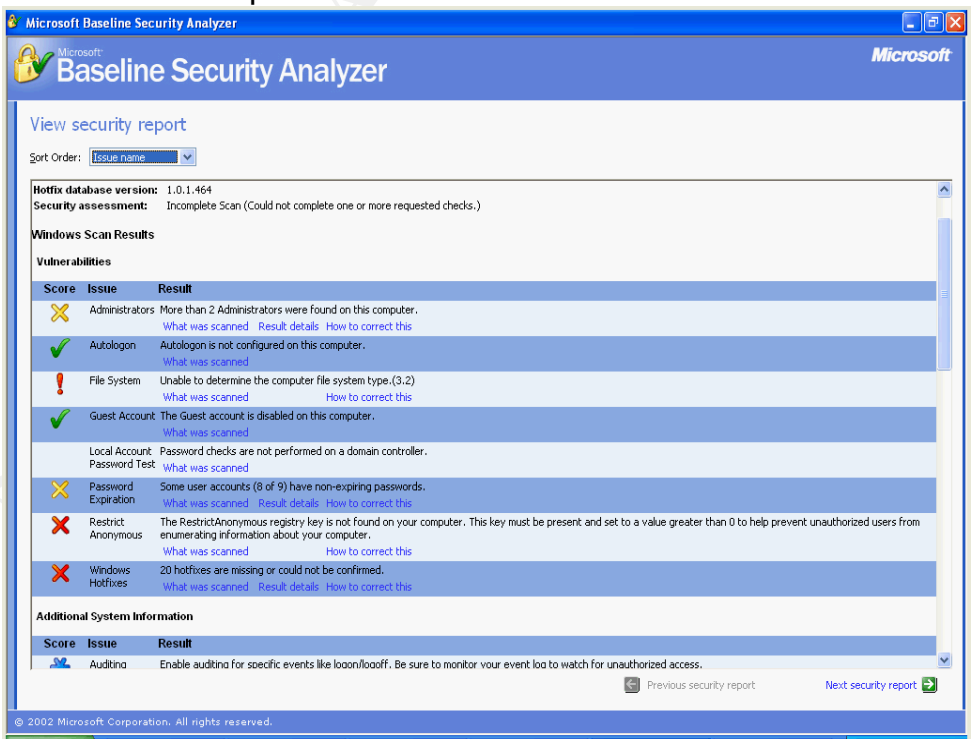
Decision Criteria for 10 Checklist Item to Be Performed

Item	Area	Risk Level	Probability	Include in Test	Comments
1	Patch/Fix	High	Very Possible	Yes	Key to server stability. Always changing and server cannot auto-update.
2	Server Accounts	Medium	Possible	Yes	The server accounts are important because if you can login and install a keystroke capturing tool you'd get everyone's credentials.
3	Backup W/S	Medium	Possible	No	Both OS could be rebuilt in the time it would take to restore them from backup.
4	Server Vulnerability Check	High	Very Possible	Yes	While considerable effort is made during installation to cover this off new risks are found daily.
5	Remote Server Console	High	Possible	Yes	Extremely important to review this. PCAnywhere needs to be configured properly or it is vulnerability.
6	App Accounts	High	Very Possible	Yes	System does not seem to have a lot of controls built in for this.
7	App Privileges	High	Possible	Yes	There needs to be a clear line between admin and operational rights.
8	App Backup	High	Possible	No	The database is critical to the long

					term viability of the system but several backups exist.
9	Server Configuration	High	Lower Possibility	No	All servers are screened prior to installation and checked thoroughly against the standard configuration.
10	Physical Console Control	Medium	Possible	No	There may be a remote time when the cabinet gets left open and unattended but you'd still need passwords to move forward
11	BCP	Medium	Possible	No	System has dial backup, battery power, UPS, etc. The formal plan is needed.
12	Change Mgt.	High	Lower Possibility	No	New work problems need an impact assessment done however most jobs won't start without a work order.
13	Alarms	High	Very Possible	Yes	Alarms get ignored or aren't setup right. Not responding to failures it big.
14	Traffic Analysis	Medium	Lower Possibility	No	PACOM has a propriety security protocol used within the system across certain points.
15	Virus Mgt.	High	Very Possible	Yes	Several pictures for ID's are supplied by disk or emailed to support staff. Server cannot auto update software.
16	Clearance	Medium	Possible	No	Security checks

					done on key employees.
17	Access Changes	High	Very Possible	Yes	Communication of terminations normally weak and pose great risk.
18	Security Awareness	Medium	Possible	No	Security awareness key for company's overall awareness level.
19	Modem	High	Possible	No	War dialing may uncover it but modem is always unplugged. Modems get mistakenly left plugged in but you would need cabinet access to do that.
20	VPN Account	High	Possible	Yes	Vendor controls are important. Normally they are only needed when you are in a bind and more apt to be less security focused.

Test Item #1

Checklist Item #1	SERVICE PACKS AND HOT FIXES FOR SERVER AND CLIENTS
Control Objective	Mitigate the risk associated with improperly patching the server.
Risk	Each of the exploits fixed by the patches or hot fixes represents a vulnerability to the system that is publicly known. Failure to apply these in a timely manner leaves the server open to attack and possible compromise.
Compliance	A vulnerability scan of the system shows that all patches that can be applied have been.
Testing	-Download a known good copy of Microsoft Baseline Security Analyzer. -Connect to the server at an administrator level from an XP or 2000 workstation.(MBSA doesn't work on NT) -Input the IP address of the server and run MBSA against it. Review the results provided by the tool. -For the server ensure that SQL vulnerabilities are checked to ensure potential database vulnerabilities are tested. -Save the results
Actions	-Connected to the server and ran MSBA with all SQL vulnerabilities checked. -Got the follow report back  - Major concerns around the outdated hot fixes. Checked the list of missing patches. Appears it hasn't been getting done

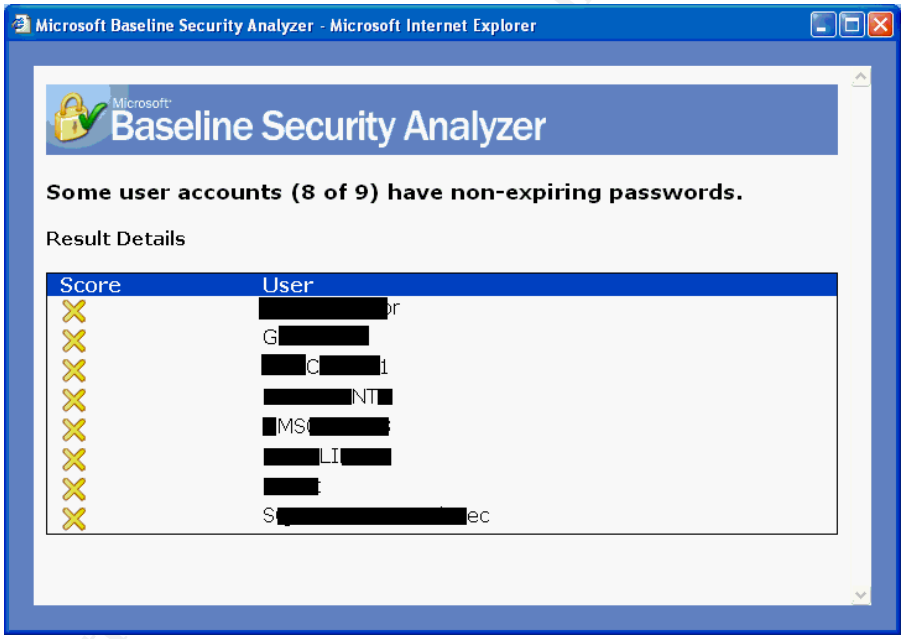
	since early last year. - Found that 3 accounts have administrator access. One was the renamed administrator account and the other two were for two technical support people. It was listed as a policy violation for them to share an administrator account so these are acceptable. - It appears only one account had a password that expires. - Restricted anonymous registry key is also missing. - Appears that checklist items during installation were done as no unneeded services were on other thing such as disabling guest, etc were also done.
Result	Failed

Test Item #2

Checklist Item#2	SERVER ACCOUNT PASSWORD POLICIES
Control Objective	Assure that passwords for the user accounts on the server meet corporate security policy standards and aren't weak and easily compromised.
Risk	If the passwords for the clients are weak it is extremely easy to crack them and use that account for malicious purposes.
Compliance	Accounts meet the standards outlined in the corporate password security policy of 8-10 characters, alpha-numeric, and unique.
Testing	1. Gather the related policies for passwords for user accounts on domains. 2. Download a known good copy of Microsoft Baseline Security Analyzer. 3. Connect to the server at an administrator level from an XP or 2000 workstation.(MBSA doesn't work on NT) 4. Input the IP address of the server and run MBSA against it. Review the results provided by the tool. 5. Pick an administrator and basic user account and review the settings on it in the user manager. Assure they match the security policy requirements.
Actions	-Reviewed the policies for passwords and here are the main points: Passwords are required for all systems. ▪ Users must be able to change their own passwords. ▪ Account IDs and passwords must ***not*** be shared. ▪ Minimum password length is eight alphanumeric characters. ▪ Maximum password life must ***not*** exceed 90 days.

- Minimum password reuse checks should be set at three.
- Common or trivial passwords must ***not*** be used.
- Passwords must be encrypted when transmitted over a public network.
- Password files must be in an encrypted format and physically and logically secured.
- All default vendor account passwords shipped with the application must be changed.

-Ran a scan with MBSA and the password specific results showed that the expiration of passwords option was not set on most accounts:



-Checked the account settings for an administrator and user and their expiration options were not set. Also no policies applied to force some of the other settings.

Stimulus\Response

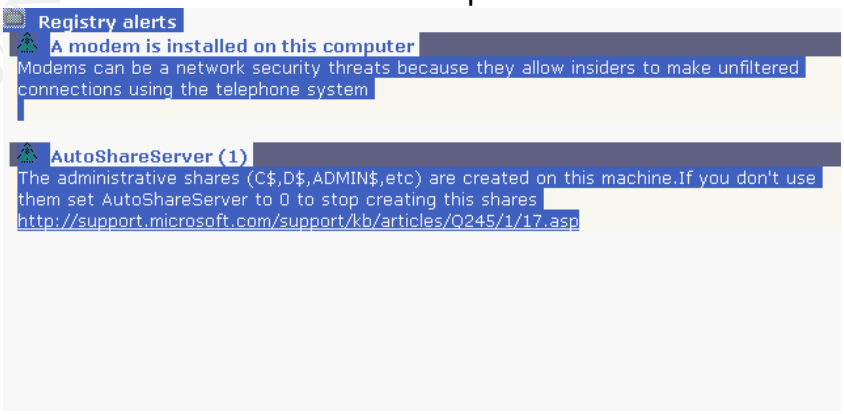
-The results of a LANguard scan confirmed the password age.

(Removed by Author)

FullName : (removed by author)
Privilege : User
Last Logon : 27 Feb, 2003, 9:59:28
Password age : 1404 days, 12 hours, 39 seconds
Logons : 10

	Bad Passwords Count : 0 **(Removed by Author)** FullName : (remove by author) Privilege : Administrator (*) Last Logon : 27 Feb, 2003, 6:48:8 Password age : 73 days, 4 hours, 49 minutes, 46 seconds # Logons : 54 Bad Passwords Count : 0 -Had a test account created and logged in with the password provided. I wasn't prompted to change it on first login. I was able to change it to 12345.
Results	Failed

Test Item #3

Checklist Item#4	GENERAL SERVER VULNERABILITY CHECK
Control Objective	Assure that server is free of a wide range of known vulnerabilities
Risk	With known vulnerabilities or risky services running the system is at a significantly greater risk of being compromised.
Compliance	Scanning tool report should show no serious risks or issues present on server.
Testing	-Run a vulnerability scanner against the server. -Review the report and analyze the findings.
Actions	-Performed a LANguard scan of the server. -The report showed some interesting results in a few areas: - It identified that the modem was connected to the server and that the administrative shares were open. 

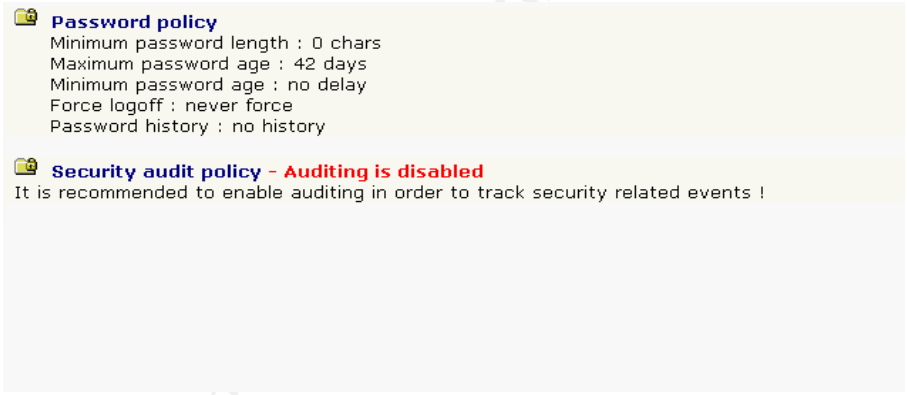
-The scan also showed that some other shares are open:

Shares

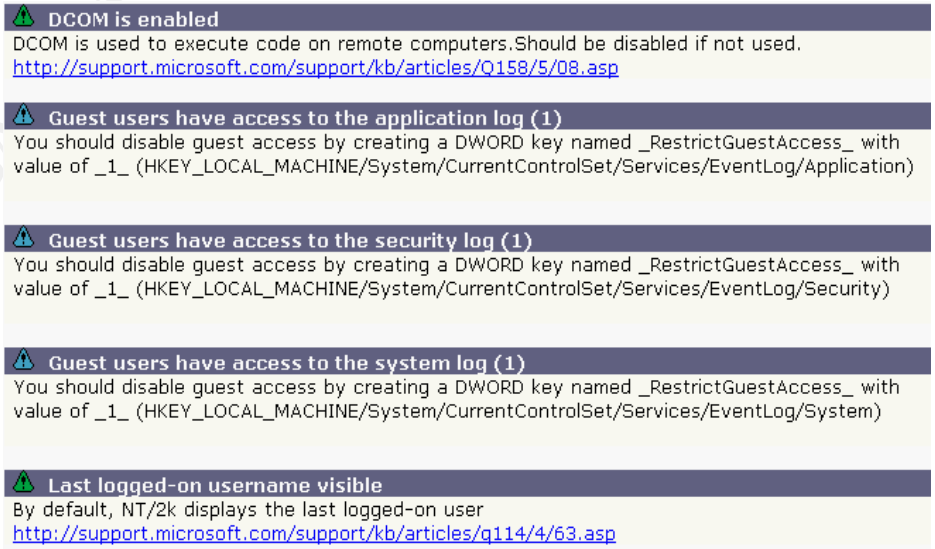
IPC$ - Remote IPC
C$ - Default share
F$ - Default share
GMS32Bbackuplog - Log files
G$ - Default share
ServerGms32 –

-These shares are the ones listed for which there doesn't seem to be any understanding of why they are there or any processes that require them to be available.

- The password policy, as pointed out above created vulnerability in the server. Also security auditing is disabled on the server. The installation checklist shows it was active when it was installed.



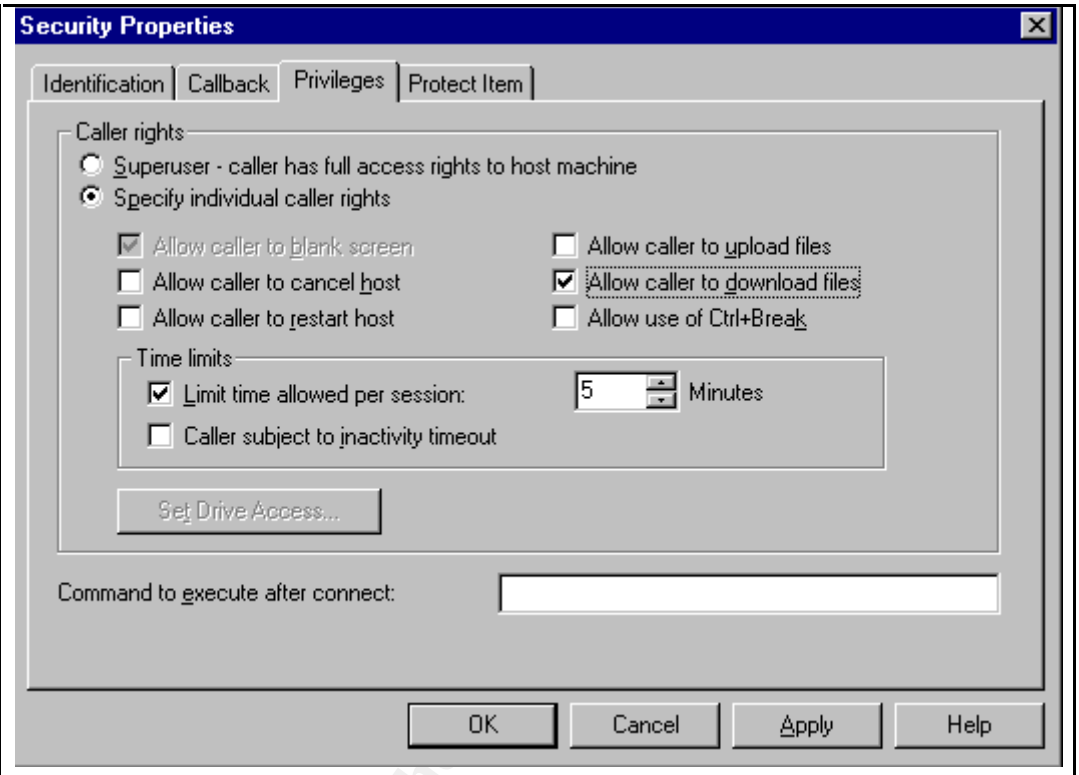
- The following alerts were also found. DCOM is enabled and the Guest account has some permissions it shouldn't. The account is disabled. The ability to view the last logged on username is also turned on which was checked off during the initial installation.



Result	Fail

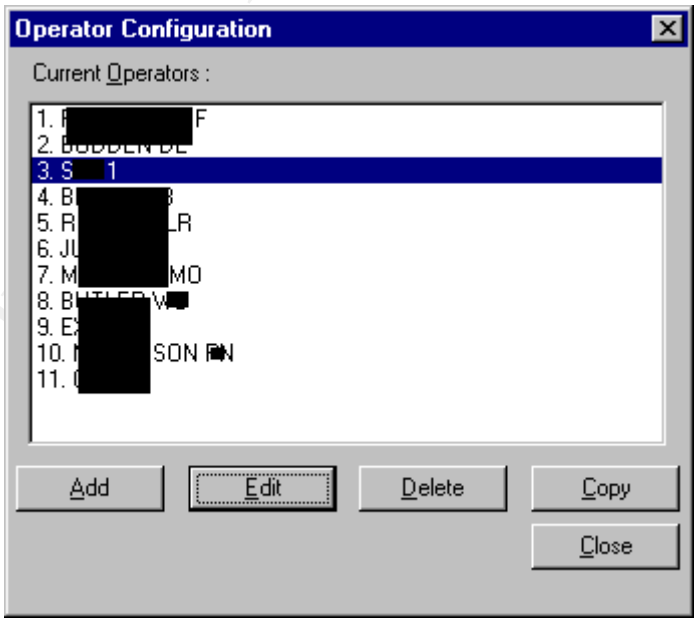
Test Item #4

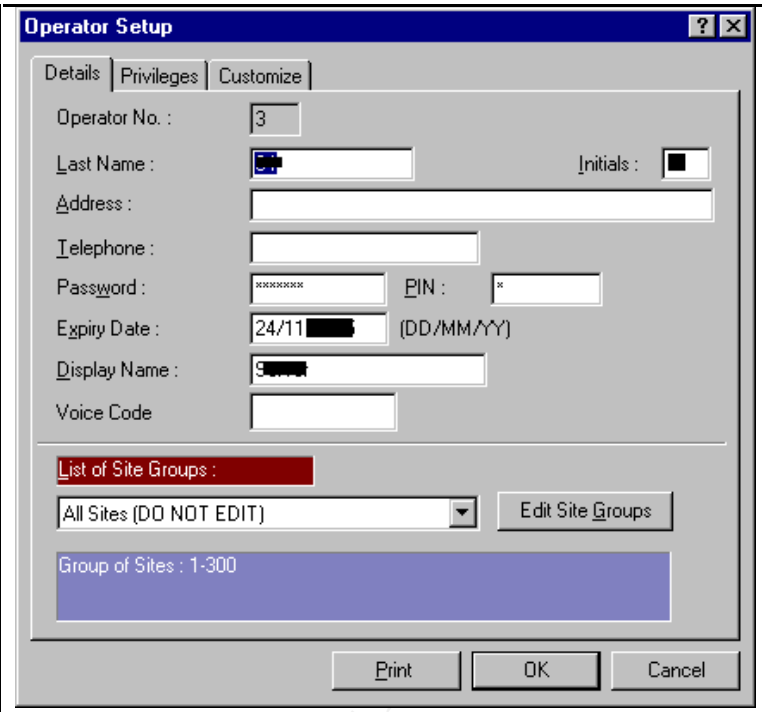
Checklist Item#5	REMOTE CONSOLE MANAGEMENT OF THE SERVER
Control Objective	Assure that the remote management tool (PCAnywhere) used to administer the server is not causing risk
Risk	If the tool is improperly configured it will leave the server exposed. Another unauthorized party could connect to the server and compromise it.
Compliance	Assure that all settings outlined in the corporate policy "Securing PCAnywhere" are followed.
Testing	-Go to the server and launch PCAnywhere. -Review all of the settings stated in the policy. -Go to a PCAnywhere client station and try to connect to the server to see if the challenges are working.
Action	-Went to the server console and launched the PCAnywhere console. Then I selected the "Be a Host Screen" and right clicked on the GMS network icon and entered the properties to review the Host settings as per the corporate policy for securing the tool. -Noted these exceptions from the policy: 1. Policy requires each caller to have their own caller ID but only one was present for everyone to use. 2. "Blank PC screen after connection" was not turned on. 3. Login attempts for a session were not limited to three but set at 5. -Then the caller icon was selected and right clicked to review the properties. -Noted no exceptions from policy. Most items were set at more secure settings than required.

	
Results	Fail

Test Item #5

Checklist Item#6	GMS32 APPLICATION ACCOUNT PASSWORD POLICIES
Control Objective	Assure that passwords for the user accounts within the application are within corporate security policy standards.
Risk	Application passwords are your last line of defense against malicious attempts to break into the system. If the server is compromised a valid username and password for the application is still required. Once obtained unapproved access can be granted, controls changed or other malicious activities.
Compliance	Accounts meet the standards outlined in the corporate password security policy of 8-10 characters, alpha-numeric, and unique.
Testing	-Review the system documentation and account management procedures for GMS32. -Have a new ID created for you on the system by the support person and document all the steps of the process from this point forward. -Login into the application using that ID.

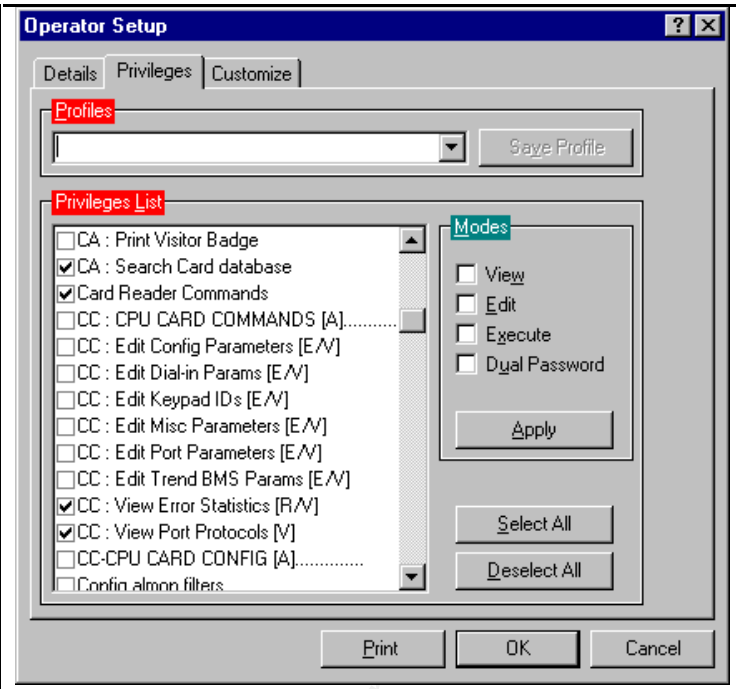
	-Try changing the password to 12345 which should not be allowed. -Logout and log back in and try the initial password given to you buy the support person with other user names to see if any still have the original password. -At the server console inspect the settings for your test account as they relate to passwords.
Actions	-Reviewed the documentation and operations manual. The account management instructions reference the password policies listed in checklist item #2. -A new ID was created on the system. At a client station that was already logged in I tried to log myself on by entering going into the "login" console. I couldn't login until the operator already logged in logged out. -Entered the username given to me and the password supplied. All usernames are two characters and the password was "summer". -There were no prompts to change the password on first login. -Entered the operator screen and went and reviewed the number of accounts. There were 11 including mine yet there are less than 9 people who are active users of this system.  -I selected the #3 account I was told to use and clicked on edit to see the properties.

	 -Account details not fully filled out. The account does have an expiration date but no other settings are configurable. Documentation says the passwords are cases sensitive. -PIN field is available as a secondary type of password to use at a PIN pad station. -Max password length is 8 characters. -I changed the password to 12345 and selected okay. I then logged out and logged back in. It accepted the change and was using 12345. I then changed the password to "TEST". **Stimulus\Response** -Tried logging in with the id and "TeSt" for a password. Wouldn't take it. Tried "TEST" and it worked. It is case sensitive. Then tried setting is to 123456789. Wouldn't take it. The tried 12345678 and it was accepted. -Tried the original password given to me against the other 10 accounts. It worked on one of them.
Result	Fail

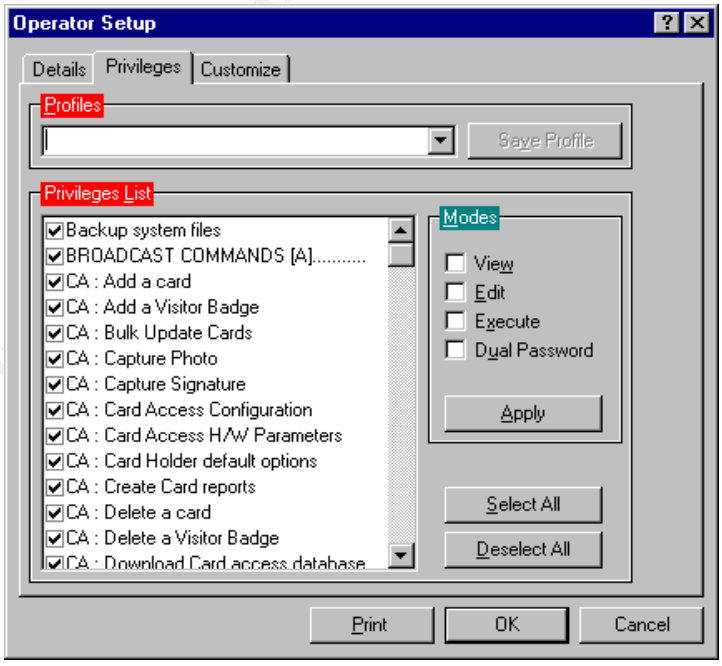
Test Item #6

Checklist Item#7	APPLICATION PRIVILEGE ASSIGNMENT
Control Objective	Eliminate excessive rights assigned to application level ID's

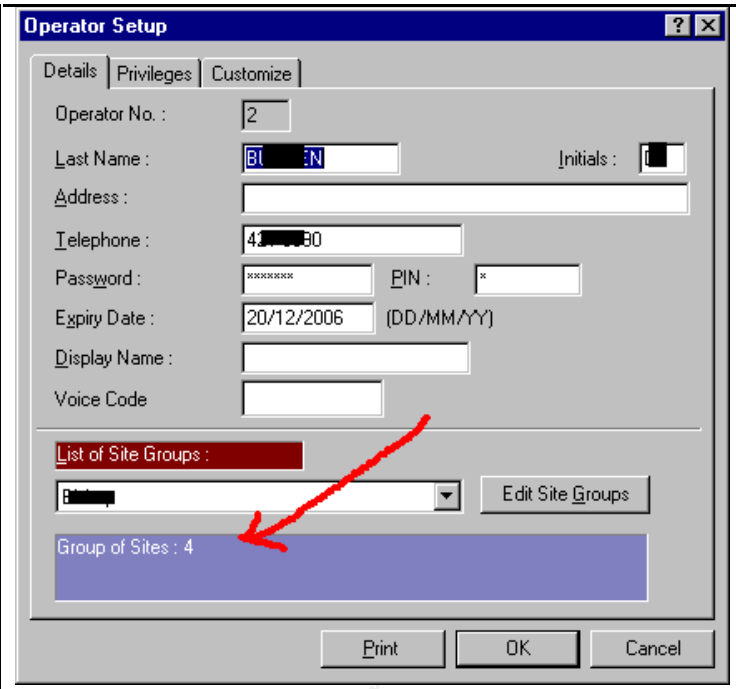
Risk	Someone with elevated rights and without proper training can unintentionally cause serious damage to the system. Also poorly assigned rights can provide high level abilities to someone who isn't properly screened to use them
Compliance	All accounts contain only the rights needed for the account owner to perform the functions they are required to do in their role.
Testing	-Review the system documentation and operational procedures to understand the roles associated with the application. -Review the documentation that outlines which rights each role should have such as administrator or operator. -Review the administration accounts by entering the Operator Configuration section, selecting an admin ID and creating a printout of the privileges assigned to each. -Review the station operator accounts by entering the Operator Configuration section, selecting a station operator ID and creating a printout of the privileges assigned to each. -Review the printouts to determine if it is following the least privilege model for rights assignment.
Actions	-The operations manual points out there are three roles for the system -Administrator – administers system. Full Access. -Operator – Functional account required to operate system -Monitor – System requires one client to be logged in for monitoring alarms at all time so this account is very restricted and used for just receiving alarm data. -Reviewed the possible settings for privileges. -Picked a basic operator account and reviewed the privileges. They were not excessive based on documentation.



-Next I selected an administrator command and reviewed the settings. Basically everything selected. That is not excessive given the role performed by the administrator.

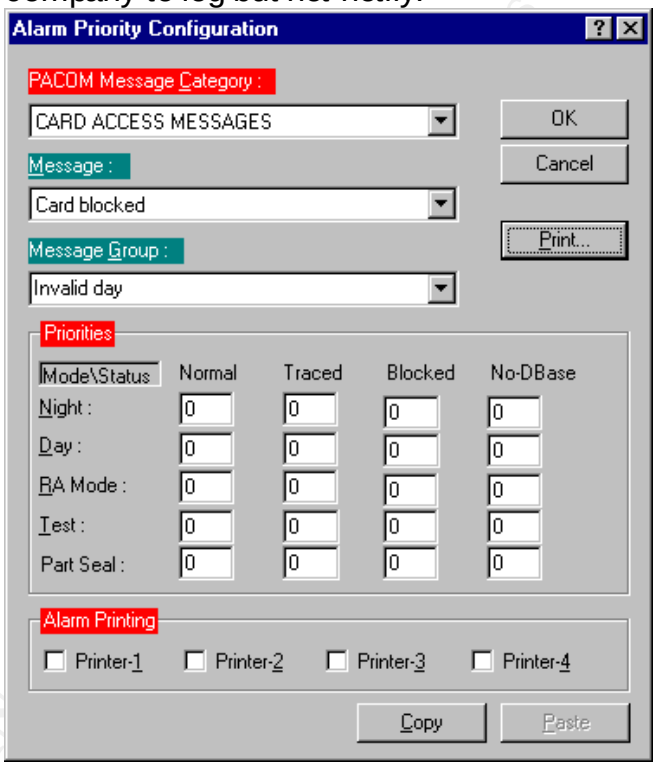


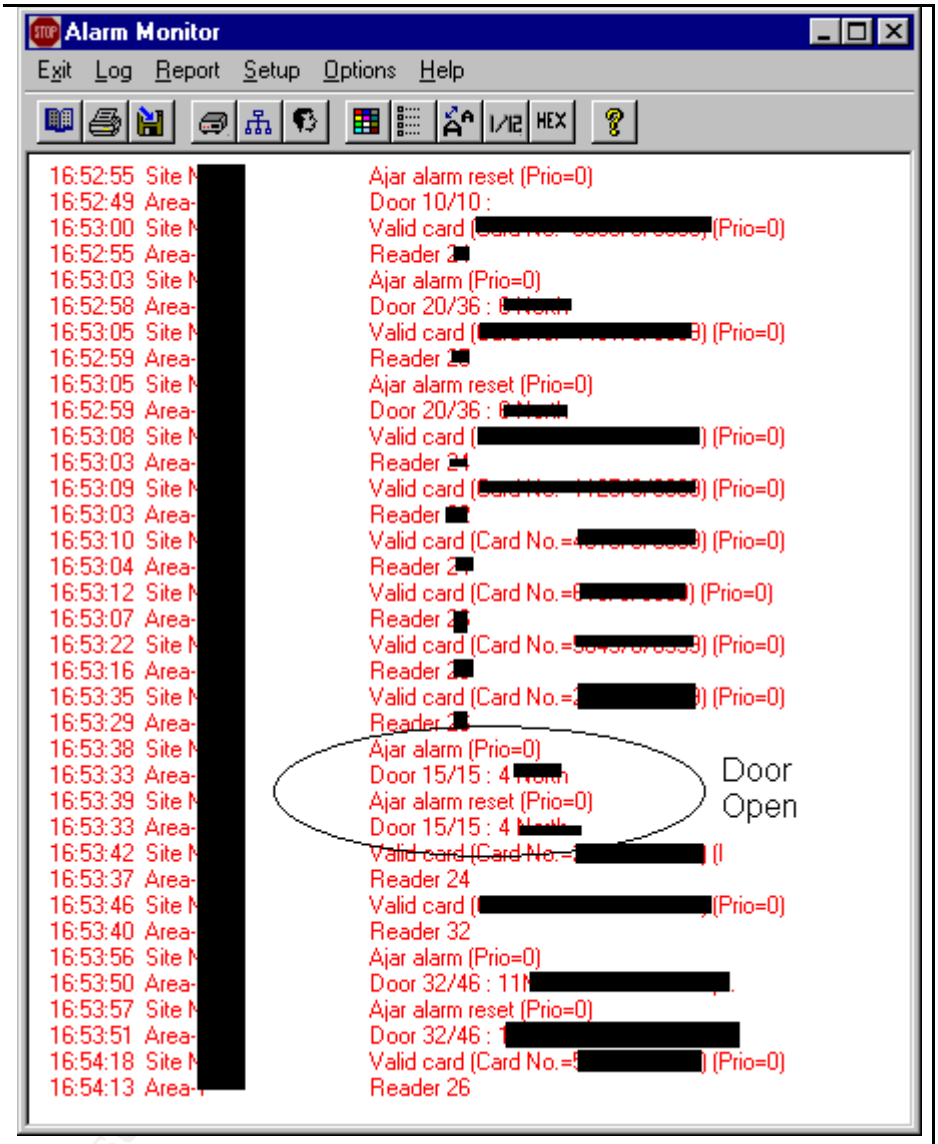
-The administrator account could edit these rights at all sites or buildings. As shown below, it was interesting to see that the operator account chosen was restricted to only one building as was required for their position.

	 **Stimulus\Response** -Had an account setup to allow me to change access at one site (site 4) which wasn't the building the data center is in (site 9). -Logged into the account and tried to change the time zone on the data center door. I could not.
Result	Pass

Test Item #7

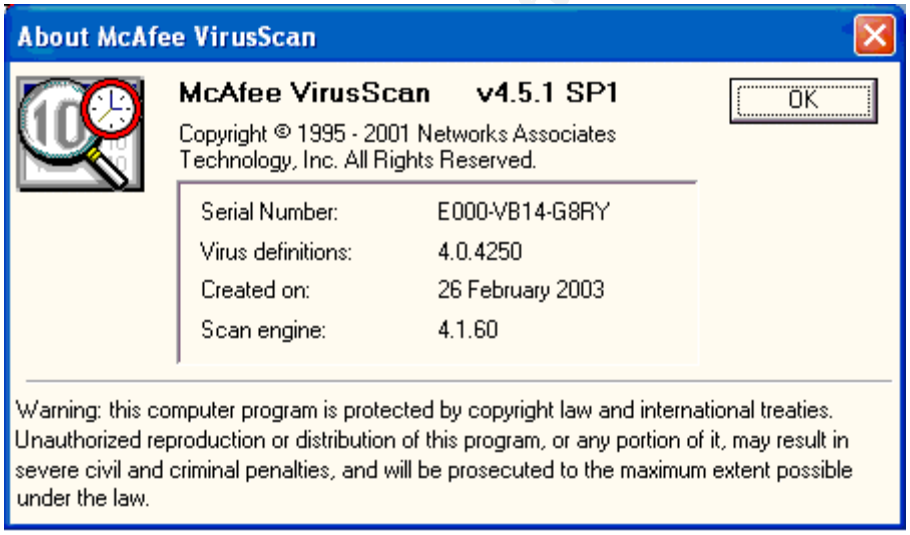
Checklist Item#13	APPLICATION ALARM RESPONSE
Control Objective	To verify that higher risk alarms generated by the system are being acknowledged and answered.
Risk	The alarms signal a security violation or a system failure. If they are not acknowledged or answered to the risk associated with the alarm remains unattended and could lead to a compromise in security.
Compliance	High risk alarms are being logged acknowledged, and responded to.
Testing	-Review the alarm notification section of system documentation to understand what alarms are available. -Go to the server and review the system events log to find a previous system alarm event.

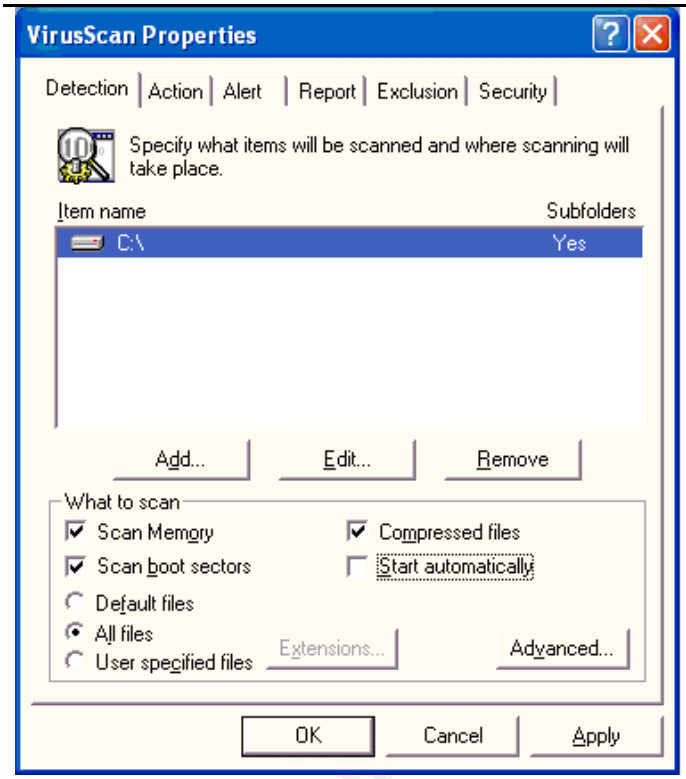
	-Check with the system operations documentation to see if anyone responded to the alarm. -Go the data center and hold the door open for around five minutes. -Wait to see if the alarm triggers a response. -Return to the server or a client and check to assure the door ajar event showed up in the logs.
Actions	-Reviewed documentation and there appears to be very little that the system will not report an alarm on. -There appears to be several alarms all day, every day in the alarm monitor logs. However, the priority of all the alarms is set to zero which according the documentation means it will register but isn't being given any importance. -The screen below shows that the alarms are configured by the company to log but not notify.  -In the alarm logs I picked several CPU alarms. There is no documentation or confirmation they were acknowledged. **Stimulus\Response** -Had the data center manager hold the door open for five minutes. Door ajar alarm showed up for the event. Alarm did not produce any other response or inquiries.

	
Result	Fail

Test Item #8

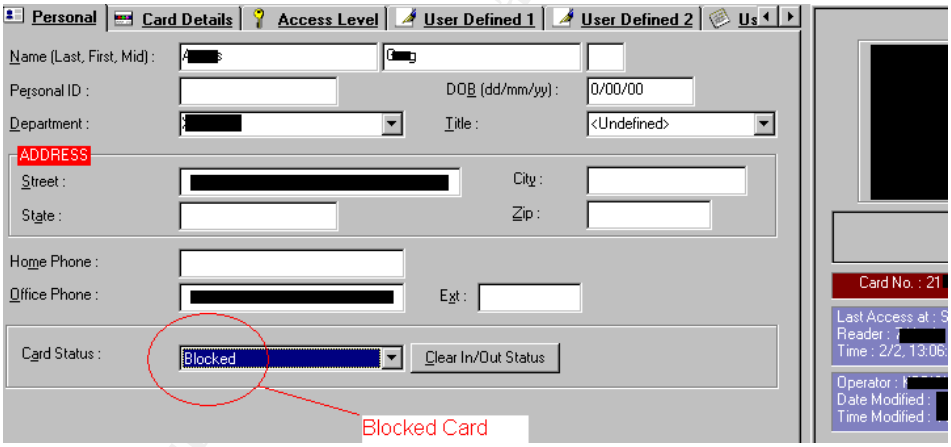
Checklist Item#15	ANTI-VIRUS PRACTICES FOR SERVER
Control Objective	Protect the server from being infected with viruses.
Risk	If a virus can make it onto the server it can wipe out the entire system, alter key files, or create vulnerabilities in the server configuration that can allow it to be easily compromised.
Compliance	Server is running approved virus scanning software with a process in place to install the latest definition files in a timely manner.

Testing	-At the server console, go to program files and look for the anti-virus program. (In this case Network Associates) -Launch the virus scan console, go into the help section and 'About McAfee Virus Scan'. -Document the scan engine and virus definition settings. -Review what is actually being scanned on the server. -Visit the product website and verify the scan engine is supported. Validated that the definition files are the most recent. -Consult the corporate anti-virus policy to ensure there is a procedure for timely definition file updates.
Actions	-Launched the AV console for McAfee. -Recorded the DAT files and Scan Engine versions.  -The DAT files were checked and found to be a current. The scan engine is older but still supported. -In the virus scan properties window the settings show that C:\ is being scanned and all files are selected. Heuristics scanning is turned on. Boot sectors and compressed files are also being looked at.

	 -The policy calls for regular updates and it appears that this procedure is being followed as the signatures are up to date.
Results	Pass

Test Item #9

Checklist Item#17	VALIDATION OF THE PROCESS FOR REMOVAL OF ACCESS OR CHANGES TO ACCESS
Control Objective	To assure that terminated employees, or employees changing job functions where data center access is not needed, have those rights removed.
Risk	Disgruntled or malicious persons should not be allowed back into the data center after their access has been revoked or you face a huge sabotage or theft risk. If a persons' status changes the access must be addressed quickly to narrow the window of opportunity for these actions to take place.
Compliance	There is a process and procedure in place to effectively manage the removal of people who no longer are authorized to have it.
Testing	-Obtain a copy of the documentation for terminating access to the data center. -Get access to the list of people who recently have had their access for the data revoked. -Go to the client station for the GMS32 and do a search for that

	person in card access configuration screen. -Review that status of their access card and if it is valid check their access levels to ensure they no longer have data center swipe access. -Review your checklist #16 list that shows valid access card holders for the data center. If there were ones that were on the list and not approved follow up to see if they were suppose to be removed and it hadn't been done.(However if the does not continue names that are not currently suppose to be in the data center than it may indicate that previously terminated employees were removed.)
Actions	-Obtained a listing of all employees who left the company for the past 12 months -I Found a server operations person on it and searched the card database for his name. -Screen showed the card was listed as blocked.  -Went to the reporting tool and ran a query on the card number assigned to the person. -Card not used since two weeks before the persons last date of employment.
Result	Pass

Test Item #10

Checklist Item#20	RESTRICTED VPN ACCOUNT FOR VENDOR
Control Objective	The VPN account provided to the vendor follows the least privilege model and requires notification to the client when they want to activate it.
Risk	If the account can be used whenever you want and isn't restricted someone at the vendor location who has the motivation could use the

	access to probe and scan the network. They could gather key system information and confidential data rather easily. They could also remotely perform changes to the system without approving them though change management and the vendor may not know they did it.
Compliance	The account cannot be accessed without alerting the company you want to use it. Also the access must only allow the vendor to reach their server IP only.
Testing	-Obtain the username for the account and review the rights assigned to it on the VPN switch. -Verify those rights only allow direct access to the server required. -Check the procedure for logging into the account to determine: -under what condition is it used? -is their a requirement for the vendor to contact the customer fist? -can the vendor proceed without contacting employer?
	-Username for the account was the original vendor's name. -Went to see the VPN administrator and verified that the rules. The account is restricted to access only the IP address of the server.  -Vendor has to call the company and get the token off of the SecureID card used to authenticate the account on login. Inactivity timeout is set to 5 minutes. **Stimulus\Response** -Called support desk and obtained a PIN. Logged in using the username and PIN of the vendor. Tried pinging several systems at differing IP's including the server. The server was the only one responding.
Result	Pass

Residual Risk

A zero risk environment is extremely hard to achieve and many say impossible. That is why many organizations have switched their "Security Department" to a "Risk Management" group. The whole idea is to determine what level of risk you feel comfortable operating at and to apply your resources in the areas that will help you achieve that level.

This system is very secure but there are areas of residual risk that remain. Below are items that were noted during the system audit:

Item #1	
Residual Risk	The valid access cards can still be passed to another person. There are no guarantees that a properly assigned and configured card is being swiped by the person who is allowed in the data center.
Threat	A card could be stolen and used to enter the data center by someone who has intentions to misuse the access to disrupt operations of compromise data.
Recommendation	A simple fix is to make sure you have a CCTV camera on the door that records events so you can see who came in. That is reactive and may be too late. The best method is to switch away from cards at the data center and use biometric authentication such as fingerprint, iris or facial recognition.
Potential Cost	A quality camera and digital recorder will cost over $4000. A biometric reader can be installed on that single point for around $2500.

Item #2	
Residual Risk	Alarming monitoring is not being done for anything. We realized is works and that the system functions well but the risk is that no one notices the alarms.
Threat	System violations, failures and other events are not being responded to and thus if something did happen that required a response it will go unnoticed. Just like the door being propped open with no response to the

	ajar alarm.
Recommendation	Configure and set suitable priorities on the alarm points. Have those alarms monitored and responded to.
Potential Cost	$5000 to setup and $10,000 annually to pay for the service at an existing guard stations.

Item #3	
Residual Risk	There is no way to formally give 100% assurance the passwords are strong enough on both the application and client\server authentication.
Threat	There really is no way to prevent someone from writing down a password because it is getting too confusing to remember them or keep track of them. People will write it down and find an easy way to keep it handy. Also if the system cannot be configured to force all of the policy requirements for passwords then you are left trusting that people will follow the rules. These weaker passwords can be used to compromise the entire system. Even with a tool such as passprop.exe installed to force complex passwords system administrators can reset them to whatever value they want.
Recommendation	Eventually go to a Biometric single sign-on solution for all systems. For now configure and use "Account Policies" for users in the domain and have a system administrator manually configure the application passwords.
Potential Cost	To plug this system into a corporate wide initiative would be less than $7500 including the biometric readers.

Item #4	
Residual Risk	The termination or resignation process for removing access is reactive. They get a list after the event.
Threat	The person who is leaving and disgruntled may go directly from their desk to the data center to cause a

	disruption or express their displeasure in leaving on one of your systems.
Recommendation	The process needs to move towards a more timely notification of the activity just before the event happens.
Potential Cost	Nothing unless the access is removed too early and the person notices. Then the cost to the organization my increase in other areas.

Item #5	
Residual Risk	VPN account allows access to the just the server IP.
Threat	The vendor has administrative rights and could reconfigure the server to defeat any attempts to limit access that were installed on the box. (such as disabling telnet)
Recommendation	It will be extremely difficult if not impossible to totally restrict the server from the network to prevent this and at the same time open up enough communication to make it functional. Also, anything applied to the server could be removed because the person will likely have administrative rights. The only reasonable measure is to install a small firewalling appliance with logging between the server and the other devices and make sure you review the logs.
Potential Cost	$3000 and up.

Item #6	
Residual Risk	Lag time between the patches and virus updates.
Threat	Even with auto update there is an exposure time between when a virus or vulnerability is active and when the update is available. This device isn't externally facing but does sit on a network which has several connections to the internet. The threat of exposure is real.
Recommendation	The threat cannot be eliminated but

	can be managed effectively. By enhancing corporate security policies and having a strong security awareness campaign the challenge is lessened. Also assigning the duties of patching and virus updates to a specific person will make it a priority within the organization. You can also pay for advanced services with your virus software vendor and buy a host based intrusion detection tool for your system to mitigate the risks.
Potential Cost	$0-$150,000

These residual risks remain but overall the control objectives were achieved as originally stated. These risks can be mitigated with the application of resources.

Is the System Auditable?

The world of access control is growing steadily. Previous implementations of access control systems all required a "hard wired" two tier network. Today most are moving towards a client\server model that takes advantage of the huge capital investment in your corporate IP network. Most of these newer systems follow the same basic design reviewed here. While the scope is wide, the system is extremely auditable if you focus on process and policy as well. The pieces of these systems are all very simple but as a combined entity it is extremely complex.

These systems are not cheap. Any company that invests this type of capital will undoubtedly need policy and procedure to accompany it. If there is no policy to accompany this system the ability to audit it decreases. Each piece could be audited according to industry best practices but the requirement is to audit the sum of the parts and not the pieces.

Procedures also play a big role in the auditability of this system. The policy tells you what the rules are but the procedure is the roadmap. If procedures are incomplete or absent then you are limited in how complete your audit will be. If you follow fives steps of a procedure and the sixth is missing then you lose direction. A wrong choice made when guessing the sixth step of the procedure may negate the entire previous steps and place the system at risk. That is why without procedures an auditor is limited in how sure they can be with what they have reviewed.

Security is about planning, policy and procedure and because this is a key piece of the security infrastructure for any company there will undoubtedly be all three of those elements in place. If they aren't in place, your audit will need to go much deeper than the access control system. With the procedures and policies in place the evaluation of the access control system becomes extremely objective. Data center standards are also very easily measured because there are many standardized tests and certifications available to develop best practices. These two facts make the whole process of reviewing the access control system very objective.

This specific system is auditable. It is a security system and with that comes considerable focus on logging. The logging that exists is very involved. It is made up of common pieces of architecture that as individual systems are auditable. Packaged together it uses some proprietary components. If you wanted to audit at the source code level you may end up with problems for copyright or confidentiality reasons. Other than that there is little reason this audit cannot be repeated for this system, or slightly modified and applied to a similar type of access control system.

Assignment Four

Executive Summary

The purpose of this audit was to assess the risks associated with the GMS32 card access system that protects the corporate data center. The system was tested for the suitability of the GMS32 application controls, the accompanying Windows NT client/server environment and the related policies and procedures. Generally the system is suitable for this purpose. This installation is facing some challenges which limit the ability to manage all the risks.

It was extremely positive to see such well documented policies and procedures. The system is impressive and is a very capable access control and alarm monitoring product. A good job is being done managing the risk of virus exposure. Privilege management within the GMS32 application also seems to be sound. The process for removing access seems to be effective and the controls that are in place to manage remote access for vendors are acceptable.

Unfortunately there are some areas were risk is not being managed properly. Patches and fixes are not being applied to the server in a suitable fashion. There were several missing. Password management for both the client\server and application accounts is not as strong as it should be for a system of this nature. A vulnerability scan also showed that some known exploits are open on the server. The use of PCAnywhere to remotely manage the server console is acceptable but results show that in this case there are some deviations from corporate policy that need to be addressed. There is also a huge area of exposure caused by not using the full functionality of the system to monitor alarms. The value of properly classifying and addressing these alarms is critical to the overall success of this system

Observation #1 Checklist Item #1 – Patches and Fixes

Background\Risk- The patching and hot fixes are not being applied to the server. A full service pack (SP 6a) is missing and all incremental patches are not applied. This creates a huge risk for the organization. An unpatched server is extremely dangerous to an access control system. With a simple free tool, even the most novice internal corporate hacker can scan the server and find vulnerabilities. The damage covers a wide range of possibilities. On the low end would be a server crash as the result of testing the exploit to a full undetected compromise of the server which could be used to harvest passwords and make system changes that will go completely undetected.

Recommendation – Patch the server to get it up to date and organize a program to assure it will be kept up to date. Ideally the solution is to have the server (and other key components) isolated in a private space on the network which is firewalled. The firewall rules should be configured as to allow only the access required to facilitate operation of the system. This will lessen the risk of being scanned and further restrict any attempts to run exploits. Logging should be turned on and the firewall alarmed to notify the appropriate person should any suspicious activity occur. There should also be a host based intrusion detection system in place for the server.

Cost – The cost associated with this will vary depending on the organization. If a firewall program already exists then there is the opportunity to simply add an interface to an under utilized box. You cold also add the firewall feature set to a screening router and place this behind it. Cost ranges from $2000-$50000 depending on the resources that are already in place.

Compensating Controls – In the meantime the controls that can reduce risk right away are the patches and fixes that are missing. A small personal software firewall will also serve a limited purpose by improving the logging of traffic and providing administrators the ability to review what is happening.

Observation #2 Checklist Item #2 – Server Account Password Policies

Background\Risk - The policy related to account passwords was available and appropriate. There is concern that these standards are not being followed. The Microsoft Baseline Security Analyzer revealed that the server accounts had no expiration. This was backed up by the LANguard scan which showed the password age was well beyond the 90 days limit outlined in the policy. This has a huge risk associated with it. If the password is compromised once it will always be available. If someone who is not authorized wishes to sneak onto the server on a regular basis there is nothing to stop them once thy have the password. They will continue to be able to use this password for that purpose. If an administrative password has been compromised this way the intruder will have administrative powers for the life of that password. They could do a variety of things which range from erasing logs to locking everyone else out of the server. Also on the test account no password changed was forced on the first login. Only the person holding the account should know their password. If others know it there is a risk that someone with malicious intent could use an account to carry out activities for which tier would be nothing to suggest they did it. While there is no specific evidence to suggest that all of the other password policy items are not being followed, it is clear that as the password policy is written there are examples where it isn't being followed. Without the benefit of the controls outlined in the policy the passwords are weaker. A simple cracking tool downloaded for free off the Internet could be used to break the weaker password quickly. The overall impact is that account security, and the rights assigned to the accounts, is virtually non-existent. It should be noted that do to the potential issues with the cracking tool being loaded on the server and possibly over taxing the server, and the concern of removing the SAM from the server, the current password database was not tested with such a tool. The results would have provided even further documentation to backup the already proven fact that work needs to be done in this area.

Recommendation – Immediately reset all passwords on the server. Invest in biometric fingerprint readers for the clients and server. Use the software supplied to authenticate to the domain using just a finger print. Most readers are accompanied with authentication software that does this. Use these to authenticate each person. Turn on all logging on the server. Configure all passwords to expire.

Cost - These devices can be as low as $300 per system. For this application your costs would not exceed $2000.

Compensating Controls – Assure that passprop.exe is loaded. Apply "NT account policies" and force as many settings from the corporate password policy as possible. Also educate each person involved on the requirement to adhere to the policy.

Observation #3 Checklist Item #4 – General Server Vulnerabilities

Background\Risk - A scan conducted with the LANguard tool showed some positive results and some areas for concern. Several of the configuration changes done during installation limited the scan results and hid much of the data collected during scans. There is a modem connected to the system but it was documented and configured securely as an emergency backup. A physical review showed that the modem is unplugged and cannot be re-activated without entering the locked cabinet. The auto shares were also turned on. These were not required. There were also other shares reported. There is no system documentation or notes to suggest these are required or even who set them up. Most are auto shares but the "GMSBackuplog" and GMS32Server are there as well. Having open shares that are not in use creates a risk. Data within these shares could be compromised. A malicious file could also be placed in them. Auditing is also disabled. This creates a huge risk. It was turned off to conserve space but a review of the drive showed space was available. Without this enabled security related events are being missed. A person could violate several security controls on the server and there would be no indication that it happened and no forensic evidence to use in an investigation. There are enhanced privileges for the guest account but because the account has been disabled that is not a risk. DCOM is enabled. With this active there is a risk of a remote attacker executing code on the server. DCOM is normally used to do this. The last login username is available. This should have been disabled during the installation checklist and in fact it was. After the administrator account was renamed to a more difficult value it was difficult for support staff to remember so they changed the value. The risk with doing that is once you have a valid username you only need the password to compromise the server.

Recommendation – The shares listed should all be reviewed thoroughly with the vendor to determine if eliminating any of them will have adverse effects on the system operation. If not then they should be removed. Full auditing should be turned on immediately. Hard disk storage capacity should be increased so that these space issues do not resurface. DCOM should be disabled if it will not adversely effect the operation of the GMS32 application. The registry should be edited to prevent the last username from being displayed.

Cost – The only incremental costs associated with carrying this out would be the new drive space. Less than $1000.

Compensating Controls – The controls provided in the recommendation could all be applied immediately if desired.

Observation #4 Checklist Item #5 – Remote Console Management

Background\Risk - The use of PCAnywhere to remotely manage the server is an accepted practice within the corporation. Remote management tools are not without risk but they are a required evil. If configured properly the risk is minimal. Upon review there were three items uncovered that deviated from the policy as it applies to this tool. The first was that all remote users are using the same account. That creates risk because if someone using it makes a mistake and causes a system problem it is harder to trace. Since all remote users appear the same in the logs the time required to trace back the person who made the change that caused the problem is greater. This increases the time you are exposed to the risk. The "Blank PC Screen After Connecting" option was not selected. This allows someone looking at the console to see all the activity of the person working remotely. This would allow an unauthorized by stander to see routines and procedures that may reveal sensitive or restricted processes being performed on the server. That would make it that much easier for them to repeat these steps should they get access. Also login attempts per session should be set at 3 but it was at 5. By increasing the number of times you allow a potential intruder to try a username and password during a given session you increase the speed at which they can try to penetrate the system. It takes time to re-establish a session and limiting connection attempts to 3 acts as a speed bump.

Recommendation – The PCAnywhere authentication should be switched to authentication using the NT authentication once the biometric authentication practice is put into place. The "Blank PC Screen After Connecting" setting should be switched on and the login attempts per session need to be reduced to three.

Cost – Only cost would be that which is assigned above to establishing the biometric NT authentication.

Compensating Controls – Until a decision has been made about using biometric authentication a separate user account should be created for each individual who uses this tool.

Observation #5 Checklist Item #6 – Application Passwords

Background\Risk - The application has operator accounts which use username and password for authentication. The usernames are all 2 characters. A longer username would give a wider range of possibilities and make them harder to guess. However, that is a limitation of the system and cannot be altered. When the test account was created the administrator setup the password. On my first login I wasn't prompted to change it. There is no place within the account details to force that setting. Without that option passwords usually do not get changed to values known by only the account holder. This means that there is an opportunity for others to use the account without the knowledge or permission of the owner. That is a principle method of concealment for anyone who wishes to conduct malicious activity. This was tested and proven positive for at least one account which retained the originally assigned password. The review showed that there are one or possibly two extra operator accounts. Having an account that isn't in use by someone is a risk. That account could have the password compromised and then be used to change system parameters, an individuals' access or a host of other serious violations with no ability to trace it back to the person who actually did it. The logs will show an unassigned account performed the changes. It does appear that case sensitive passwords are forced by the system and there are appropriate expiration dates assigned to all accounts. The system does not seem to require unique passwords. The minimum password length (8 characters) allowed by policy appears to be the maximum length permitted by the system.

Recommendation – The technical feasibility of using the biometric single sign-on with this application needs to be explored. There is also an updated version of this software (version 3.0) which lists improved account security and biometric integration as selling features. That upgrade should be strongly considered. The current password policy needs to be clearly explained and re-enforced with everyone holding accounts on the application. The inability to force password settings can be overcome with manual compliance. A list of all accounts needs to be reviewed and any that are unassigned removed.

Cost – The cost of going to the newer software version is expensive. Some pieces of system hardware are not compliant. The whole cost of doing this has been estimated at $15,000 - $25,000. The biometric costs would be minimal as they are part of other initiatives that are going on. However, true project costing would raise the biometric figure to $2000-$5000.

Compensating Controls – The system offers little flexibility other than what is outlined above. One control that could be done put in place is for a system administrator to be chosen to manually reset passwords in line with the policy and distribute them. While that person would know other's passwords the other policy items would be covered off.

Observation #6 Checklist Item #13 – Alarm Response

Background\Risk - This system has a phenomenal ability to monitor all sorts of alarms. It even has a voice notification component. However, in this particular installation alarm monitoring has been, for the most part, disabled. By setting the priority on the alarms to zero they are recorded but no one is prompted to respond to them. This was done because there were no agreements in place at the time of installation to have these alarms monitored. Operating like this is a huge risk. From an operational perspective you are ignoring alarms that tell you when someone is trying to enter a door they are not allowed to, when doors are propped open and a whole host of other serious infractions. This allows a potential intruder to test the system and see what response they get from security. If nothing occurs it tells them they aren't being watched and to go forward with their plans. From a technical perspective you miss alarms that inform you of hardware problems, systems failure or network connectivity issues. If these are ignored you will undoubtedly find yourself in the position of needing to change system settings in an emergency and just then finding out the system cannot perform the task because of a hardware failure.

Recommendation – Immediately start monitoring the technical and operation based alarms. The priority of these alarms should be reviewed and set. There should be 24X7 monitoring of the alarms chosen to be serious enough to warrant such activity. The functionality of the system that creates an alarm "event" needs to be activated. This procedure needs to enforce that a response must be documented inside the event window of the system software. These events need to be reviewed by the manager in charge to assure they are being dealt with properly

Cost – It would take between $5000-$20000 in consulting fees to address all of the alarms and set the correct priorities on them. The ongoing costs to add this assignment at a guard station or outsource it range from $5000-$25000 annually.

Compensating Controls – Immediately the key technical alarms, such as CPU failures, need to be set to notify the system administrator. Also the alarm monitor logs need to be reviewed daily to spot more serious events until such time that full alarm monitoring gets turned on.

Bibliography

"Designing a Data Center" – Justin Newton
About.com http--www.webtechniques.com-archives-1999-08-newton-

"Developing the Network Operations Center in Support of the NT 4.0 Wide Area Network"-David C. Peterson
Developing the Network Operations Center in Support of the NT 4.0 Wide Area Network

"Disaster Recovery Plan Testing: Cycle the Plan, Plan the Cycle" - Guy Krocker
Disaster Recovery Plan Testing Cycle the Plan, Plan the Cycle

"FAQ for How to Secure Windows NT" - Satnam Bhogal
FAQ for How to Secure Windows NT

"How to Check Compliance with your Security Policy" - Krishni Naidu
How to Develop Your Company's First Security Baseline Standard

"Ensuring Password Quality on NT Networks" – Frank O'Dwyer
http--www.brd.ie-ntsecurity-password.pdf

"The Canadian Handbook On Information Technology Security" – Canadian Government Publication
http--www.cse-cst.gc.ca-en-documents-knowledge_centre-publications-manuals-mg9e.pdf

"Auditing a Distributed Intrusion Detection System: An Auditors Perspective – Darrin Wassom"
http--www.giac.org-practical-Darrin_Wassom_GSNA.doc

"Auditing The Cisco AS5300 Remote Access Router" – Cliff Ziarno
http--www.giac.org-practical-GSNA-Cliff_Ziarno_GSNA.pdf

"Auditing a SQL Server 2000 Server: An Independent Auditor's Perspective" – Graham Thompson
http--www.giac.org-practical-GSNA-Graham_Thompson_GSNA.pdf

"Auditing Novell iFolder Professional Edition V2.0" – Jerry Shenk
http://www.giac.org/practical/GSNA/Jerry_Shenk_GSNA.pdf

"Implementing Remote Access: Security, Usability and Management" - John Torello
http--www.sans.org-rr-encryption-remote_access.php

"Securing Remote Users VPN Access to Your Company LAN" - Klavs Klavsen
http--www.sans.org-rr-encryption-sec_remote.php

"Protecting Computer Managed Assets" – Larstan Business Reports – Copyright 2002
http--www.sans.org-rr-practice-BLWpaper.pdf

"Internal Threat – Risks and Countermeasures" - Jarvis Robinson
Internal Threat – Risks and Countermeasures

"Microsoft Windows Security Patches" - Dan B Rolsma
Microsoft Windows Security Patches

Utility Source for NT - Arne Vidstrom
ntsecurity.nu - Toolbox

"Biometric Selection: Body Parts Online" - Steven M. Walker
SANS Institute Information Security Reading Room - Biometric Selection Body Parts Online

"Building a Secure Internet Data Center Network Infrastructure" - Chang Boon Tee
SANS Institute Information Security Reading Room - Building a Secure Internet Data Center Network Infrastructure

"Data Center Physical Security Checklist" - Sean Heare
SANS Institute Information Security Reading Room - Data Center Physical Security Checklist

"Iris Recognition Technology for Improved Authentication" - Penny Khaw
SANS Institute Information Security Reading Room - Iris Recognition Technology for Improved Authentication

"Is Single Sign on a Security Risk?" - Michael Kelly
SANS Institute Information Security Reading Room - Is Single Sign on a Security Risk

"Password Auditing and Password Filtering to Improve Network Security" - Tina MacGregor
SANS Institute Information Security Reading Room - Password Auditing and Password Filtering to Improve Network Security

"Password Protection: Is This the Best We Can Do?" - Jason Mortensen
SANS Institute Information Security Reading Room - Password Protection Is This the Best We Can Do

"Securing Access: Making Passwords a Legitimate Corporate Defense" - David H Sherrod
SANS Institute Information Security Reading Room - Securing Access Making Passwords a Legitimate Corporate Defense

"Center for Internet Security Benchmarks and Scoring Tool for Windows 2000 and Windows NT" – Center for Internet Security
The Center for Internet Security CIS Benchmarks and Scoring Tool for Windows 2000 and Windows NT

"Three Defenses to a Secure System: Virus Scanning, Applying Patches and System Monitoring" - Angelina Lucero
Three Defenses to a Secure System Virus Scanning, Applying Patches and System Monitoring

"You Can't Hack What You Can't Access" - Wamala Paul Mubanda
You Can't Hack What You Can't Access

"Free Anti-Virus Tips and Technique" – Chengi Jimmy Kuo
http://www.nai.com/common/media/vil/pdf/free_AV_tips_techniques.pdf

Manageable Secure Physical Access – Core Street Limited 2002
http://www.corestreet.com/whitepapers/SecurePhysAccess.pdf

Handbook of Information Security Management Web Book
http://www.cccure.org/Documents/HISM/ewtoc.html

Honey, Gerard - Electronic Access Control – Newnes 2000

Fischer, Robert / Green, Gion - Introduction to Security 6th Edition – Butterworth-Henemann - 1998

Fay, John J. - Encyclopedia of Security Management :*Techniques and Technology* – Butterworth-Henemann - 1993

Williams, Timothy L. - Protection of Assets: Volume 1 – POA Publishing -1999

"Microsoft System Architecture – Internet Data Center Overview" – Microsoft Publication - Posted: January 22, 2002
http://www.microsoft.com/solutions/msa/evaluation/overview/idc/archgoals.asp

"Self Audit Checklist from Institute of Internal Auditors" - The Institute of Internal Auditors, Inc
http://www.theiia.org/ecm/guidance.cfm?doc_id=2670

Mosler Inc. Publishing - GMS-32 Card Access Training Manual – Revision 1.0 - 1999