Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

Auditing SunGard Zai*net
An Independent Auditor's Perspective

GSNA Practical Version 2.1 – Option 1

Lane Boyd

November 2003

TABLE OF CONTENTS

2

3

ABSTRACT

The trading of energy and energy derivatives has come to the forefront of public knowledge over the last two years. With the scandals of Enron, Dynegy, and El Paso Energy, the public has begun to demand that organizations that conduct energy trading have security and controls in place to prevent individuals from performing unauthorized transactions. With this in mind, SunGard Zai*net, the energy trading application used by GIAC Power Trading, must meet Corporate Standards regarding confidentiality, integrity, and availability of trading information.

Research in Audit, Measurement Practice, and Control

Identify the system to be audited

I am auditing the production SunGard Zai*net energy trading application for GIAC Power Trading (herein referred to as "GPT"), an integrated utility that provides both generation and electrical distribution capabilities for over 5 million customers. The application acts as the primary means of trading energy for GPT. Because of the potential effects on the spot market (current trading price for energy), it is critical to maintain the highest level of confidentiality for trading information with their trading partners (counterparties). Integrity is also important because if a counterparty disputes a trade, the unaltered proof of a trade will corroborate GPT's version of any dispute in a court of law. Availability is critical to GPT. The loss of trading operations has been estimated by our Corporate Risk Control Group to potentially cost upwards of $50M per week of downtime. This makes GPT the most critical (in terms of revenue) network belonging to GIAC Power (GPT's parent company)

Besides energy trading, Zai*net also handles the settlement (payment) of trades and acts as the general ledger for GPT, making it a material target for Sarbanes Oxley compliance. Section 404 of the Sarbanes Oxley act requires Executive Management's assertion that the internal controls of key financial systems are effective. The company's external auditor will then attest as to the accuracy of this statement during the external audit process.

Through extensive research on the Internet and trade publications, there is absolutely no information regarding the audit of an energy trading application. I was able to locate standard application audit checklists on a variety of audit-related websites. I was also able to gather information regarding key control areas of the trading process. It is important to note that for auditing an energy trading application, as with any application, the auditor must have a clear understanding of the processes being supported. Lack of understanding of the process could lead the auditor to evaluate controls that are not applicable, or do not actually manage risk within the system.

Zai*net is a prominent player in the energy trading risk management market with a large number of Fortune 500 utilities employing this product.

4

Moreover, with Zai*net's "easy to administer" philosophy, we still have too administrators without the proper training and experience managing the security of Zai*net. Therefore, this paper gives back to the Systems Administrator, Auditing, and Security community a solid checklist to ensure that all administrators are properly securing Zai*net.

The methodology of auditing a Sungard Energy Systems Zai*net will be the result of Best Practices by technology leaders, energy trading experts, Sungard, and personal experience.

Due to the limited scope of this paper, the following audit areas will not be included: network devices (firewalls/routers/switches), operating systems and databases. Although, it is critical to note that without proper security steps taken on the network layer and on the host operating systems, Windows 2000 Server and Windows NT Server, all Zai*net auditing and security enhancements are nullified. This paper is meant to build upon a strong security foundation and auditing process already being completed on the network and Windows 2000/NT Server. Moreover, new vulnerabilities are discovered on a regular basis; therefore, it is important that administrators stay current with the new vulnerabilities/exploits and learn how to mitigate their risks.

Additionally, this audit will not cover the specific page access that is allowed through Zai*net keys (which will be explained later in the paper). There are over 500 keys within Zai*net and determination of what specific page access is required for every individual at GPT would require its own paper and the expertise of accounting and energy trading experts.

I'll briefly mention the major controls for Zai*net.

Controls

CONTROLS	Input (Prevention)	Processing (Detection)	Output (Correction)
Application User Security	X	X	X
Approved Counterparty Configuration	X	X	
Antivirus	X	X	
Archiving	X		
Auditing and Monitoring		X	X
Backup System, Process, & Tapes	X		
Change Management Policy and Procedures	X		X
Disaster Recovery Plan			X
OS Folder Level Security	X		
Intrusion Detection System		X	
MultiLayered Network & Security Design	X		

Offsite storage	X		
Operating System Security	X		
Password complexity	X		
Patch Management	X		
Physical Security	X		
Policies	X		
Price Lockdown	X	X	
Reports			X
Report Security		X	X
Retired Users	X		
Risk Control Document	X		
Stamping Process	X	X	
Source Code Escrow	X		
System Performance Monitoring			
Trader and Counterparty Limit Alerts		X	
User and Administrator Security Awareness	X		
WarnDays	X		

Figure 1

DIAGRAM OF CURRENT ZAI*NET INFRASTRUCTURE

Internal Router

Hub   Hub

Zainet1_App Server   Zainet2_App Server

Zainet3_DB Server

Servers

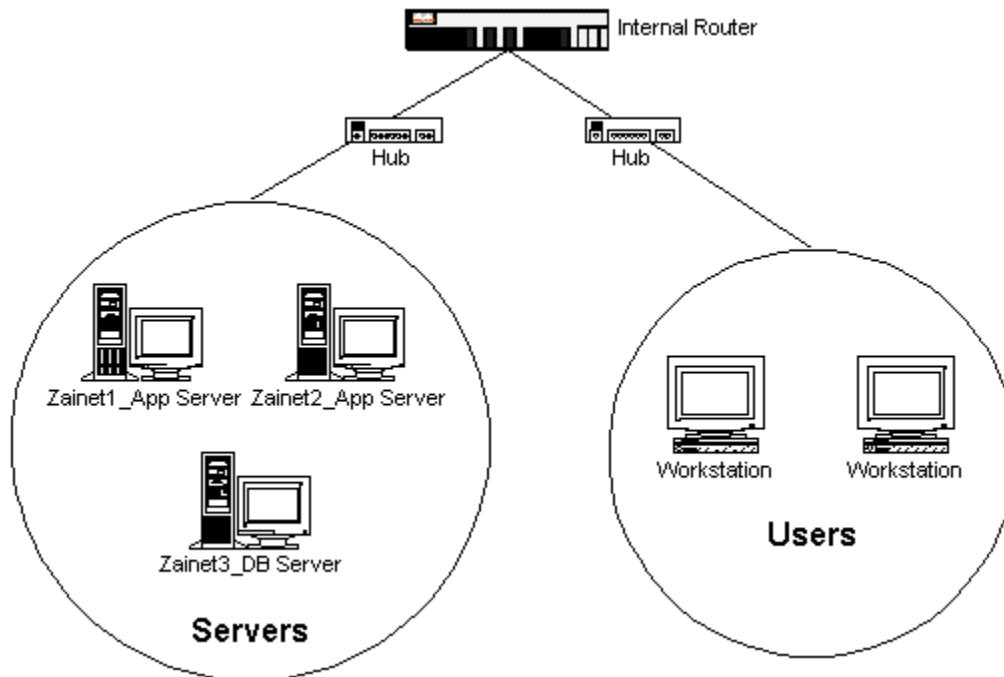Workstation   Workstation

Users

Figure 2

Evaluate the risk to the system

There are three fundamental risks to an energy trading risk management system like Zai*net. If a vulnerability, threat, and exploit are combined, we could potentially lose one or a combination of the following: confidentiality, integrity, and availability of the information stored within the Zai*net system.

A compromise of confidentially on the system is a very high risk to GPT, its customers, and its partners. The loss of confidentiality could cause fluctuations within energy trading markets, but also cause GPT to lose its reputation as a secure transactional partner and not be trusted by any energy trading companies, thereby affecting GPT's credit status, which is paramount in the energy trading industry. The likelihood of confidentiality being lost is high with the default configuration of Zai*net and the lack of a strong password policy. A few other specific risks to confidentiality are the misuse of privileges, intercepting the data, social engineering of a password, and identity theft. Taking corrective measures and proactive auditing can greatly reduce the chance of an exploit from happening.

After obtaining a password or some type of access to the Zai*net, it is possible to forge an energy trade, modify an existing energy trade, delete trades, and corrupt the database. Any loss of data integrity is a high risk to the company. However, after taking the necessary countermeasures to these threats, it would be unlikely and challenging for a hacker to do all but forge a trade. The consequences of comprised data integrity on Zai*net is very similar to those of compromised confidentiality. GPT

7

could go out of business. Other data integrity risks are viruses that manipulate the data, any malicious code, or a Trojan horse.

A Denial of Service (DOS) attack whether from a virus or misconfigured server, is a very likely problem that hasn't been contained as well as it could be.

The risk of compromised confidentiality, integrity, and/or availability is of the utmost importance with confidentiality being the top risk to the company's reputation and business status.

The security control objectives are to minimize risks while allowing proper operations of Zai*net. In general, we are ensuring that only authorized users can use the system and with the least privilege necessary, ensuring that the system maintains the highest availability, and ensuring that the proper design is minimizing their risks.

What is the current state of practice, if any?

I searched everywhere for an audit checklist for SunGard Zai*net, or for that matter, any energy trading application. I spoke with peers in the utility industry, not a single one of them had an auditing checklist for an energy trading application. I was able to locate generic checklists for auditing applications but energy trading applications are a completely different beast. Through my discussions with various energy trading experts, I was able to compile of list of "must have" controls to secure a trade.

The research consisted of attending searching the Internet for Zai*net auditing and security material, application auditing procedures, attending utilities specific internal audit training, SANS Reading Room, reading the system administration and security administration guides for Zai*net, and setting up a lab to test different configurations.

Articles
- Chris McCown, "Framework for Secure Application Design and Development," SANS Reading Room, http://www.sans.org/rr/paper.php?id=842, November 12, 2002.
- Jay Hollander, "What is a "Source-Code Escrow Agreement"?" Gigalaw.com, http://www.gigalaw.com/articles/2000-all/hollander-2000-08-all.html, August 2000.

Audit Checklists
- Dan Holt, "Auditing Microsoft Exchange 2000 Server, An Administrator's Perspective," http://www.giac.org/practical/GSNA/Dan_Holt_GSNA.pdf.
- Paul Hugenberg, "Application IT System Audit," http://www.auditnet.org/docs/ApplicationITSystemsAudit.doc.
- Harvey Siegal, "EDP General Controls Review Audit Program," http://www.auditnet.org/docs/itgeneral.txt.

Books

8

- Caminus Zai*net 6.3 System Administration Guide, 2002.
- Caminus Zai*net 63 User Guide, 2002.
- Peter Fusaro, "Energy Risk Management," 1998, McGraw-Hill.
- Frederick Gallegos, "Information Technology Control and Audit," 1999, Auerbach Publishing.

Conferences
- Edison Electric Institute Utility Internal Auditor's Training Course, September 22-24, New Orleans, LA.
- SANS Institute, <u>Track 7 – Auditing Networks, Perimeters and Systems</u>, The SANS Institute, 2003.

Since a specific audit checklist about auditing an energy trading application was not found, an audit checklist will be created from personal experience, conversations with energy trading experts, books, presentations, and articles about energy trading.

9

Create an Audit Checklist

Introduction

Where applicable, Corporate Standards for information technology will be used as the basis to evaluate the configuration of Zai*net.

It is important to note that for auditing an energy trading risk management system, the auditor must have a thorough understanding of the underlying processes that the ETRM system supports. While Zai*net is a major player in the energy trading risk management market, trading processes (and as a result how Zai*net is used) varies drastically from one trading organization to another.

The audit checklist I have created is based upon the process that GPT uses to trade energy. Many of the fundamentals are applicable for any Zai*net installation; however, certain checklists steps (such as Audit Step #1) are based solely on how GPT is organized and how responsibilities have been distributed. This is not to say that GPT is perfect in how it is organized, but to convey the message to the reader that the controls must secure the processes in use by the trading organization.

Checklist

Audit Step #1

Application User Security	
Reference	http://www.sans.org/rr/paper.php?id=842 Caminus Zai*net 6.3 System Administration Guide
Control Objective	Users should have the minimun necessary access to an application to perform their duties and nothing more.
Risk	Excessive access opens the door to users to utilize application functionality, outside of their area of expertise. As a result, users could, intentionally or unintentionally, adversely affect data residing in other areas of an application.
Compliance	Determine if users are restricted to application pages that are necessary for them to perform their jobs. Trade operations at GPT are divided into three distinct areas. There is a "Front Office" that consists of traders, who make trades and input them into Zai*net. A "Middle Office" consisting of risk analysts, who perform the duties of Zai*net administrator and oversight of the trade floor. Finally, there is a "Back Office" where financial personnel handle billing, credit, and legal issues within

10

Zai*net.

From the most basic perspective of segregation of duties, Front Office should have access to Zai*net trade entry pages, Back Office should have access to Zai*net billing, credit, and legal pages, and Middle Office should have access to pages that allow the editing and approval of pages used by the Front and Back Office.

Zai*net uses a security architecture that allows an administrator to assign "keys" to groups. Each key is configured to allow or deny access to pages within the Zai*net application. These keys are then put into a directory architecture for groups. For GPT, the following keys are in Production:

Front Office
FTRD—Fuels Trading
ANLY—Analysis
PTRD—Power Trading
FRNT—Front Office

Middle Office
RADM—Risk Administration
RISK—Risk Administration
MID—Middle Office
MID2—Middle Office 2

Back Office
INV—Invoicing
MA—Master Agreement
CRED--Credit
BACK—Back Office
BAK2—Back Office 2

Because the process of correctly setting up keys for Zai*net is so complex and trading organization specific that an entire paper could be dedicated to it, for the purposes of this audit, I will assume that each of the keys are configured correctly, in accordance with GPT's organization structure.

Personnel should be restricted from accessing areas of Zai*net that are not necessary for them to complete their jobs.

Testing	Evaluate tree security to ensure that keys are assigned to appropriate groups, in accordance with GPT energy trading processes. Login to the New GUI Select "Configuration" Select "Security Administration Select "New" under "Users" Create a new user by inputing in a user ID and password Select "OK" Drag the newly created ID into each folder you want to test. The ID will inherit the permissions of the key(s) located in the folder.
Objective/Subjective	Objective

Audit Step #2

Report Security	
Reference	Caminus Zai*net 6.3 System Administration Guide
Control Objective	Ensure that the ability to create, edit, and/or view a report is restricted to appropriate personnel.
Risk	Reports used for performing energy trading monitoring functions may be edited or deleted. Additionally, users may utilize system resources for reports they do not require to perform their duties.
Compliance	Report security within Zai*net is enabled. Users have been segregated into groups that allow them the minimum level of access to perform their jobs.
Testing	Determine if report security is enabled Login to the New GUI Select "Configuration" Select "Security Administration" Select the "Report Security Screen" Button Verify that personnel have been segregated into different report screens Login to the Old GUI Select "Reports" Select "Report Design" Attempt to run/edit/delete reports

12

Objective/Subjective	Objective—Report security is enabled
	Subjective—Report access is restrictive enough

Audit Step #3

Price Lockdown	
Reference	Caminus Zai*net 6.3 System Administration Guide
	Personal Experience
Control Objective	Energy prices are "locked down" preventing alteration.
Risk	Alterations to actual energy prices could affect accounting of daily transactions.
Compliance	Lockdown of prices occurs on a daily basis. Users are unable to alter information in a day where the price has been locked down.
Testing	Login to the OLD GUI
	Select "Prices"
	Select "Close Day"
	Verify that all dates (except the current day) appear
	Randomly select one of the dates and attempt to alter the information
Objective/Subjective	Objective

Audit Step #4

Retired Users	
Reference	http://www.sans.org/rr/paper.php?id=842
Control Objective	Determine if users that are no longer with the company have had their access removed from Zai*net
Risk	Users that have left the company may attempt to gain access to Zai*net and make unauthorized transactions. The data structure of the Zai*net application prevents user IDs from being deleted from the system. In order to prevent alteration of Zai*net information by these individuals, their access to Zai*net pages must be removed. Normally, these users should be removed from an application when the ID is no longer being used. However, due to the way the Zai*net has been configured at GPT, these IDs cannot be removed without "orphaning" trade information.
Compliance	Former users will be placed into a "Retired" group, which has no privileges, whatsoever.
Testing	Compare users to a current employee list from HR.
	All users that are not current employees should be in the "RETR" list, which has no access.

13

	To View User IDs: Login to the New GUI Select "Configuration" Select "Security Administration" Create a user ID: Select "New" under "Users" in the "Security Administration" screen Create a new user by inputing in a user ID and password Select "OK" Place the User ID in the RETR and determine if any access is allowed
Objective/Subjective	Objective

Audit Step #5

Reports	
Reference	Corporate Risk Control Document Caminus Zai*net 6.3 System Administration Guide
Control Objective	Ensure all trades are being monitored for 1) not being approved in a timely manner 2) modification 3) canceling.
Risk	Trades are not approved in a timely manner or trades are being inappropriately altered or deleted.
Compliance	The following reports exist: Aged transaction Modified transaction Voided transaction report
Testing	Determine if reports exist: Login to the Old GUI Select "Reports" Select "Report Design" Look for reports that fit the above criteria
Objective/Subjective	Objective

Audit Step #6

"D" and "B" Stamps	
Reference	Caminus Zai*net 6.3 System Administration Guide Personal experience

14

Control Objective	Trades are approved by the "Dealer" and "Back Office" in a timely manner
Risk	Trades may not be reviewed by appropriate management personnel, and therefore not compliant with the Corporate Risk Control Document.
Compliance	All trades are stamped (approved) within 3 days by the "Dealer" and "Back Office."
Testing	Login to New GUI Select "Deal Entry" Select "Power Trades" Input random (Previously Selected) trades into "Trade Number" Verify that "D" and "B" stamps have been applied within 3 days
Objective/Subjective	Objective

Audit Step #7

Trader Limit Alerts	
Reference	Caminus Zai*net 6.3 System Administration Guide Personal experience
Control Objective	Ensure that traders do not exceed the trade limits for the trader.
Risk	Exceeding trader limits exposes GPT to the risk of a trader making errors that could adversely affect GPT.
Compliance	Trader limits are established in accordance with the Corporate Risk Document.
Testing	Login to the Old GUI Select "Master" Select "Limits" Select "Trader Limits" Verify that trader limits are configured in accordance with the Corporate Risk Document
Objective/Subjective	Objective

Audit Step #8

Approved Counterparty Configuration	
Reference	Caminus Zai*net 6.3 System Administration Guide Personal experience
Control Objective	Ensure that trades are only allowed to make trades (via drop down menus) with approved counterparties.

15

Risk	Trades could be made with unapproved counterparties, who may not have the ability to deliver energy or funds, for the trades that they make.
Compliance	Trades with unapproved counterparties cannot be made.
Testing	Identify an unapproved counterparty Login to the New GUI Select "Deal Entry" Select "Power Trades" Attempt to create a trade with the unapproved counterparty
Objective/Subjective	Objective

Audit Step #9

Auditing	
Reference	Information Technology Control and Audit
Control Objective	Auditing is enabled and management has the ability to identify unusual activity within the system.
Risk	An audit trail does not exist to allow management to determine who has made unusual transactions.
Compliance	Auditing is enabled on Zai*net to track the user, date, time, and activity of changes made to a trade.
Testing	Login to New GUI Select "Deal Entry" Enter a previously selected trade number into "Trade Number" Attempt to edit, delete, and add status Select the "Audit" tab and verify that auditing captured changes to ticket number, status flag, and individual responsible for the change and date and time of the change.
Objective/Subjective	Objective

Audit Step #10

Password Complexity – New GUI	
Reference	http://www.sans.org/rr/paper.php?id=842 Corporate Standards
Control Objective	Prevent unauthorized access Zai*net's New GUI.
Risk	Weak passwords increase the risk of an unauthorized user to gain access to the application.
Compliance	Password complexity settings are compliant with Corporate Standards. Zai*net's New GUI is primarily responsible for Zai*net security, as

16

	well as Front and Back Office operations. To secure information within Zai*net, passwords must comply with Corporate Standards of being at least 8 characters long.
Testing	Log into New GUI Select "Configuration" Select "Security Administration" Select "New User" under "Users" Create a user ID with a password with less than 8 characters
Objective/Subjective	Objective

Audit Step #11

Source Code Escrow	
Reference	http://www.gigalaw.com/articles/2000-all/hollander-2000-08-all.html
Control Objective	Ensure that GPT has access to the source code of Zai*net, should SunGard stop supporting Zai*net.
Risk	If SunGard became unable (or unwilling) to support Zai*net, GPT would not have the application source code to support Zai*net themselves. The original creator of Zai*net (Caminus), was recently purchased by SunGard Energy Systems. Prior to that Caminus was in financial difficulty and was expected to declare bankruptcy. Because of the critical nature of Zai*net's role at GPT, access to the source code, in the event Zai*net is no longer supported, is crucial to business operations for GPT.
Compliance	A source code escrow agreement will be in place between GPT and SunGard.
Testing	Obtain a copy of the current source code escrow document from SunGard. Verify that it is current.
Objective/Subjective	Objective

Audit Step #12

WarnDays	
Reference	Caminus Zai*net 6.3 System Administration Guide
Control Objective	Prevent putting in inaccurate dates for trades.
Risk	Traders may enter inaccurate dates for trade information.
Compliance	Warnday is enabled. Trades entered with previously occurring dates will receive a warning message.

17

Testing	Check Warnday configuration: Login to New GUI Select "Configuration" Select "Global Setup" Select "GLOI" under "View" Look for the WARNDAYS variable to be set to Y Enter a trade and try to input a historical date: Login to New GUI Select "Deal Entry" Enter a Trade with a "Delivery Date" in the past
Objective/Subjective	Objective

Audit Step #13

Security Awareness	
Reference	http://www.giac.org/practical/GSNA/Dan_Holt_GSNA.pdf Information Technology Control and Audit
Control Objective	Ensure that employees are aware of the importance of computer security, especially as it applies to Zai*net.
Risk	Users may create weak passwords, or worse yet, write down passwords and leave them in visible areas. Zai*net is a very critical system, in which hundreds of millions of dollars flow through annually. Users tend to consider computer security the responsibility of IT, and as such, remain unaware of the basics of security.
Compliance	A Corporate Standard for Security Awareness training exists. Meeting requests or a list of attendees available to prove the training happened.
Testing	Determine if a Corporate Standard governing Security Awareness training exists. Verify that training records are kept, documenting compliance with Corporate Standards.
Objective/Subjective	Objective-whether it was actually given or not Subjective-Content and effectiveness of the training

Audit Step #14

Physical Security	
Reference	Information Technology Control and Audit

Control Objective	Ensure that access to Zai*net systems is restricted to authorized personnel.
Risk	Unauthorized personnel could gain access to Zai*net systems and affect the confidentiality, integrity, and/or availability of the Zai*net system.
Compliance	Physical barriers restrict access to Zai*net systems. Security guards and a card reader system used to restrict access to the trade floor or the data center to authorized personnel.
Testing	Review the policies and procedures for restricting physical access to the processing center and other sensitive areas.
	Determine who is responsible for issuing access to the data center and how access is authorized.
	Review the policies and procedures for maintaining and monitoring the card-key system. Observe the card-key system in use.
	Verify that all personnel are required to present an identification card prior to entry into the data center.
	Review policies and procedures for controlling limited access visitor cards.
	Verify that visitors are required to sign a visitor log and wear a name tag indicating that they must be accompanied by authorized personnel at all times while in the data center.
	Verify that all valid and invalid attempts to enter the data center are logged. Obtain a copy of the violation logs that are reviewed periodically.
	Verify that security is notified after a number of invalid attempts to access the data center.
	Attempt to gain access to the data center, noting the approximate time. Review the security report, noting whether the unauthorized access attempt was recorded.
	Observe processing center activity to determine whether access appears to be limited to authorized individuals.
	Obtain a copy of all individuals that have access to the data center. Review the individuals with access to the data center and determine whether access is appropriate based on the individuals' job responsibilities.

Objective/Subjective	Objective

Audit Step #15

System Performance Monitoring	
Reference	Information Technology Control and Audit
Control Objective	Performance of the Zai*net system is monitored and a process is in place to address issues identified.
Risk	Poor Zai*net performance could affect GPT's ability to conduct energy trading operations and the ability to create back end reports in a timely manner. Proactive performance monitoring is often ignored by IT.
Compliance	A process is in place to monitor the performance of the Zai*net system. Performance issues that are identified are addressed in a timely and effective manner.
Testing	Obtain the Key Performance Indicators (KPIs) to gain an understanding of the system performance standards in place. Determine which tools are used to monitor system performance. Review operations policies and procedures for system monitoring and determine if the procedures appear appropriate. Verify that server volumes meet the established KPIs for system growth. Verify that memory statistics are reviewed periodically to ensure that adequate resources are available for the workload performed by a system. Verify that system log files are periodically reviewed. Verify that the integrity of each file server disk drive periodically reviewed.
Objective/Subjective	Objective—Standards are in place Subjective—Effectiveness of standards

20

Audit Step #16

Change Management	
Reference	Information Technology Control and Audit
Control Objective	Adequate measures are in place to allow only authorized and adequately tested and approved changes (both emergency and normal) implemented into production, and prevent implementation of changes that introduce unacceptable risks.
Risk	Changes that are not approved or inadequately tested could adversely impact energy trading operations by introducing changes to the Zai*net system that do not function as planned.
Compliance	A documented change management process is in place and evidence that this process is followed exists.
Testing	Business unit and IT department management approval is required before systems acquisition and/or change projects are undertaken. Verify that environments (either logical or physical) separate from production systems exist for development (or modification) and testing of IT solutions. Determine who has access to the Production and Test environments and why. • Obtain a list of individuals with access to the Production and Test environments and verify that access is appropriate based on job responsibilities. Determine who has access to the system directories. • Obtain a list of individuals with access to system directories and verify that access is appropriate based on job responsibility. Select a sample of 5 program changes, including emergency and requested changes, and complete the following: • Obtain the respective request/approval documents for each of the changes. • Verify that the changes are authorized by management, prior to implementation.

21

	• Verify that the change testing documentation and results are available.
	• Verify that the tested changes are approved for move to production by someone other than the programmer.
	• Verify that all relevant parties, including users are being notified of the changes and actual installation of the change.
	• Determine if all relevant parties are made aware of the business impact of the changes.
	• Review the testing process for the developers and obtain samples of the signoffs for the testing results.
	• Verify that audit trails are being maintained to track what has been changed in the production system, when, and why.
	• Verify that user and system documentation is updated for the changes, if needed.
	• Verify the contingency arrangement is in place to enable back out of installed changes if necessary.
	• Verify that the emergency changes are tracked for timely replacement by a permanent change.
Objective/Subjective	Objective

Audit Step #17

Backup Procedures	
Reference	Information Technology Control and Audit
Control Objective	GPT has the ability to restore files in the event of data loss.
Risk	Hard drive failure or accidental file deletion could cause the loss of critical business data. The loss of this data could potentially affect energy trading operations.
Compliance	Backups of data occur and backup procedures exist.

22

Testing	Determine who is responsible for the back-up process.
	Determine what documentation is kept for the back-up process.
	Verify that off-site storage is used for the back-up tapes.
	Determine how quickly can restoration take place when needed.
	Review and document the backup, rotation and retention procedures in place.
	Determine who is responsible for reviewing backup logs to help ensure that the backup has actually occurred.
	Determine if a process is in place to re-perform backups if there are problems with the initial back up.
Objective/Subjective	Objective

Audit Step #18

Disaster Recovery	
Reference	Information Technology Control and Audit
Control Objective	GPT has the ability to recover energy trading operations in the event that the primary trading floor becomes unusable.
Risk	GPT would not be able to conduct energy trading operations if the GPT building were to become unavailable.
Compliance	A tested disaster recovery plan exists and a process is in place to ensure it remains current.
Testing	Review the current disaster recovery plan for completeness.
	Examine copy of agreement in effect for hot-site emergency processing facility.
	Review the results of the testing performed during the review period including: ▪ Full system disaster recovery ▪ Power outage testing ▪ Fire alarm testing
Objective/Subjective	Subjective—Completeness of disaster recovery plan. Objective—Examination of hot-site agreement and testing

documentation.

Audit Step #19

Password Complexity – Old GUI	
Reference	http://www.sans.org/rr/paper.php?id=842 Corporate Standards
Control Objective	Prevent unauthorized access to Zai*net's Old GUI.
Risk	Weak passwords increase the risk of an unauthorized user gaining access to the application.
Compliance	Password complexity settings are compliant with Corporate Standards. Zai*net's Old GUI is primarily responsible for report writing within Zai*net. To secure information within Zai*net, passwords must comply with Corporate Standards of being 8 characters long.
Testing	Login to the Old GUI Select "User ID" from "Setup" Create a new user ID with a password of less than 8 characters
Objective/Subjective	Objective

Audit Step #20

Archiving	
Reference	Personal Experience
Control Objective	Unused Zai*net data is archived (removed from the database), enhancing Zai*net performance.
Risk	Unnecessary data will continue to collect within Zai*net, slowing system performance.
Compliance	A process is in place to identify unnecessary data and remove it from the production Zai*net database.
Testing	Determine if procedures or a process exists for database tables storing price data, volatility data, scheduling data, and transaction data to be archived (removed) from the production system.
Objective/Subjective	Objective—Data archiving occurs. Subjective—Determining what specific tables should be archived.

24

Audit Evidence

Conduct the audit

Audit Step #1—Application User Security
PASS

Determine if users are restricted to Zai*net keys that are necessary for them to perform their jobs.

To test Zai*net, a user ID was created and systematically placed into folders reserved for Front, Middle, and Back Office. While the user ID was in each of these folders, I attempted to gain access to functions that belonged to other offices.
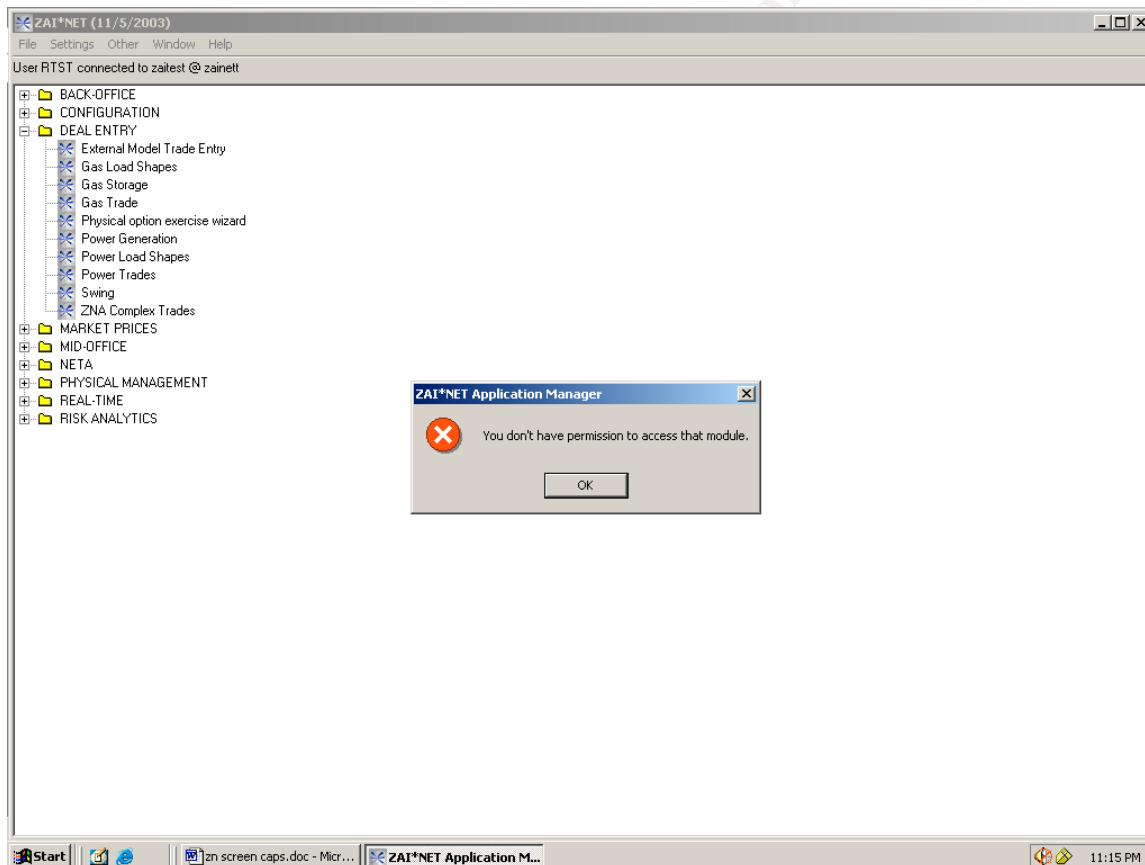
Figure 3

Figure 3 shows that as a member of the Middle Office, I attempted (unsuccessfully) to gain access to the "Power Trades" screen, which should be restricted to the Front Office.

25
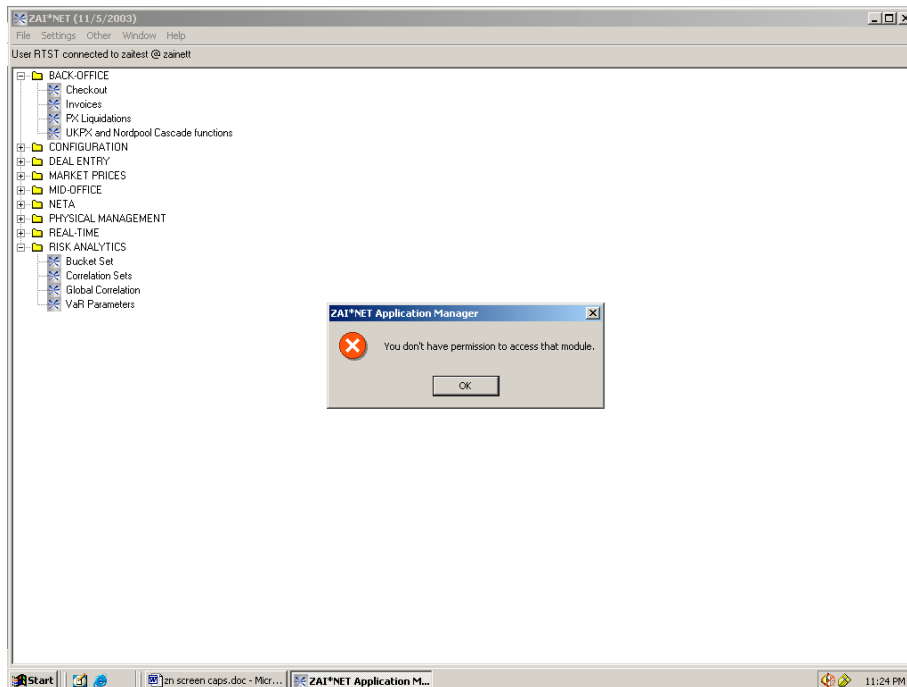
Figure 4

Figure 4 shows that as a member of the Middle Office, I attempted (unsuccessfully) to gain access to the "Checkout" screen, which should be restricted to the Back Office.

Figure 5

26
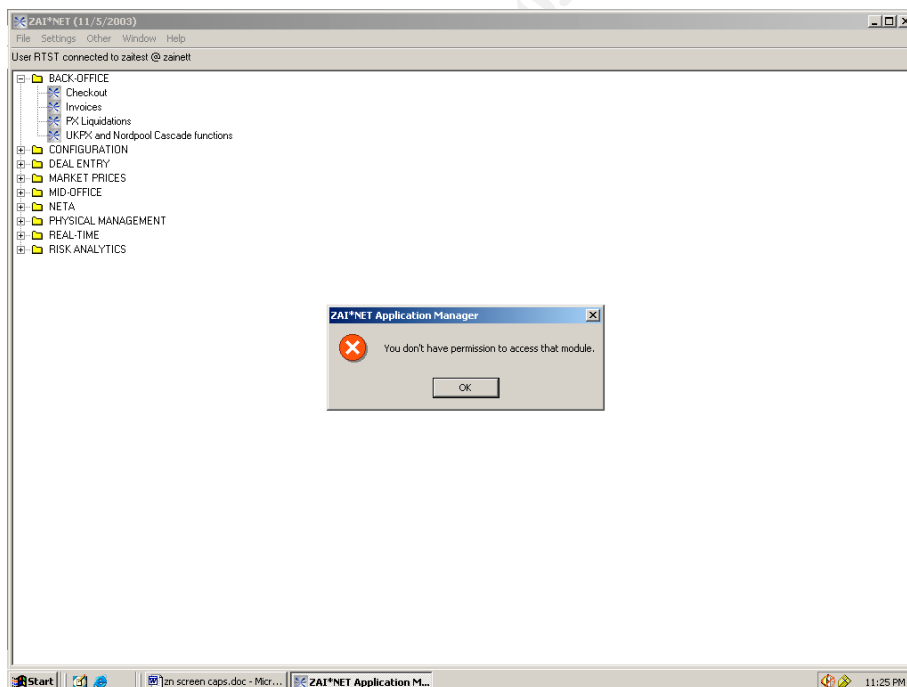
Figure 5 shows that as a member of the Front Office, I attempted (unsuccessfully) to gain access to the "Invoice" screen, which should be restricted to the Back Office.
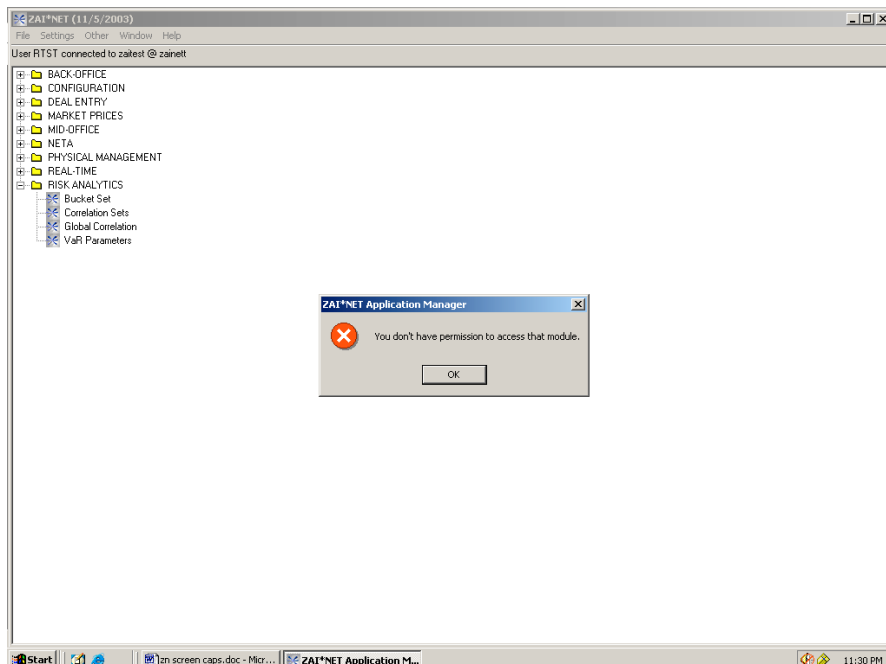
Figure 6

Figure 6 shows that as a member of the Front Office, I attempted (unsuccessfully) to gain access to the "Var" screen, which should be restricted to the Middle Office.
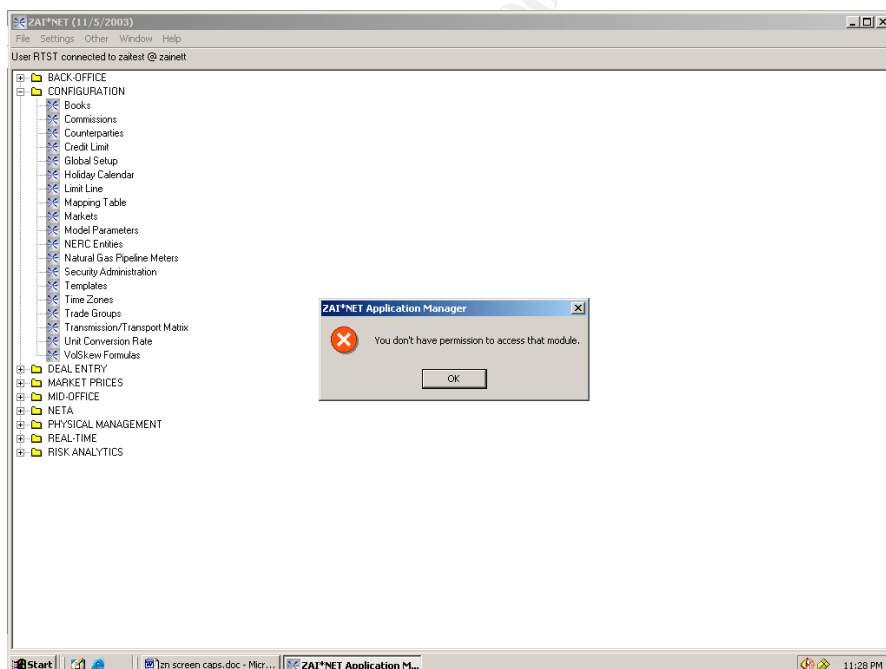
Figure 7

27

Figure 7 shows that as a member of the Middle Office, I attempted (unsuccessfully) to gain access to the "Credit Limit" screen, which should be restricted to the Back Office.
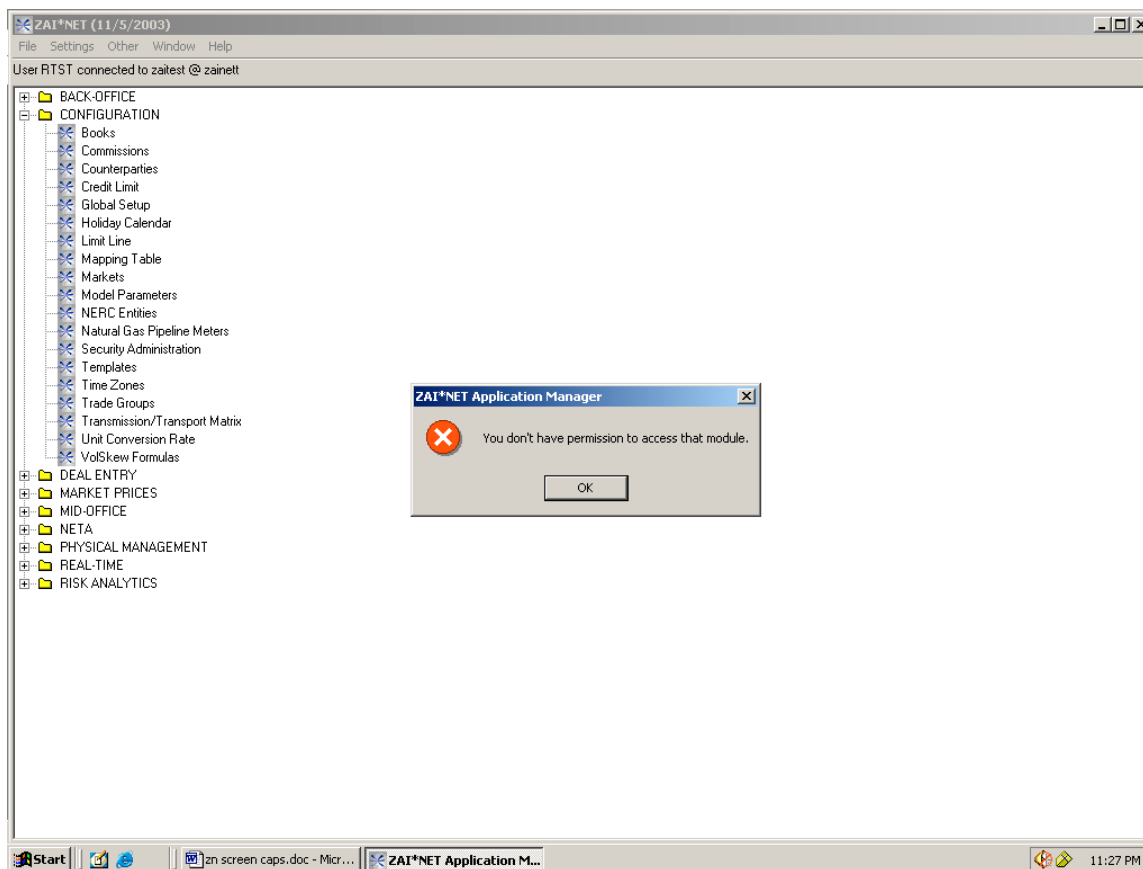
Figure 8

Figure 8 shows that as a member of the Middle Office, I attempted (unsuccessfully) to gain access to the "Credit Limit" screen, which should be restricted to the Back Office.

Audit Step #2—Report Security
FAIL
Ensure that the ability to create, edit, and/or view a report is restricted to appropriate personnel.

Figures 9-12, below show that all user IDs have been place into a single folder. This grants all report access to all users. As evidenced in the middle column in these Figures, report security folders have been established, but users have not been placed into them.
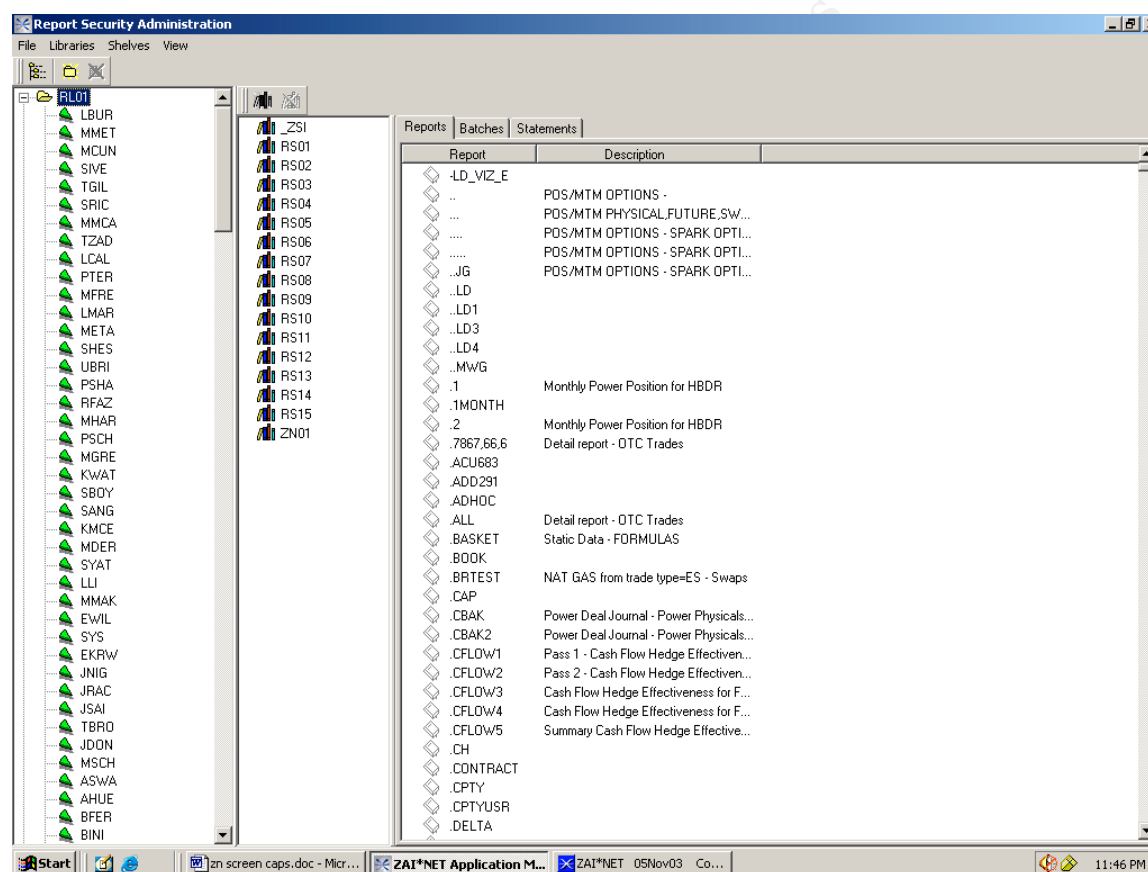
Figure 9

29
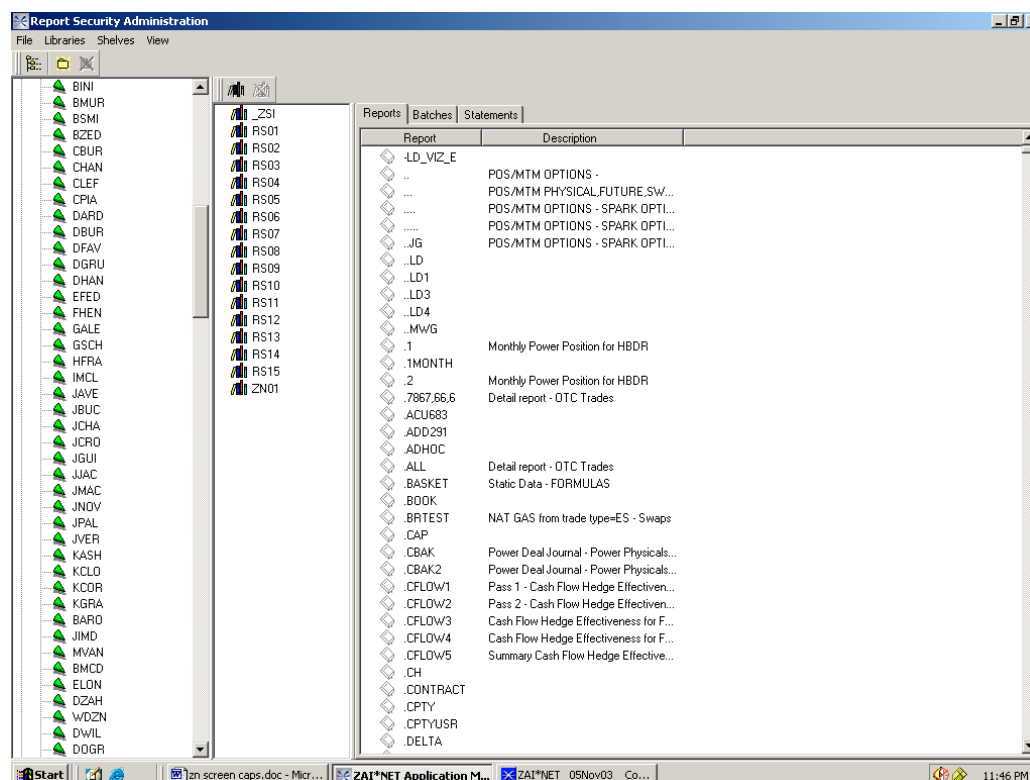
Figure 10

Figure 11

30
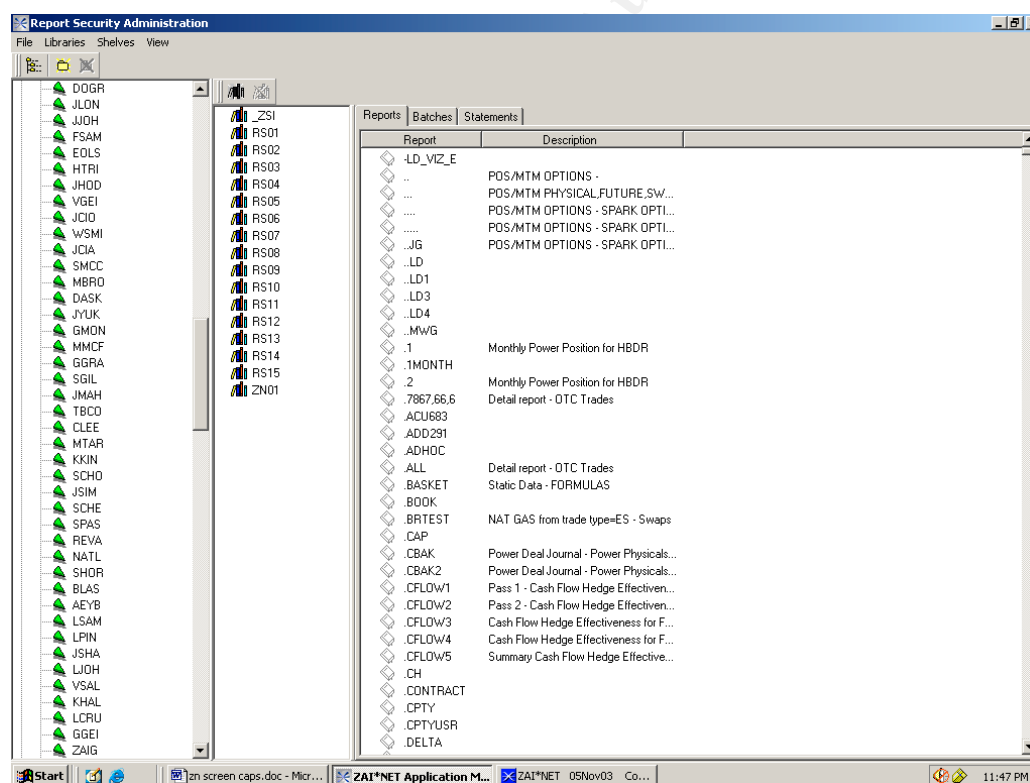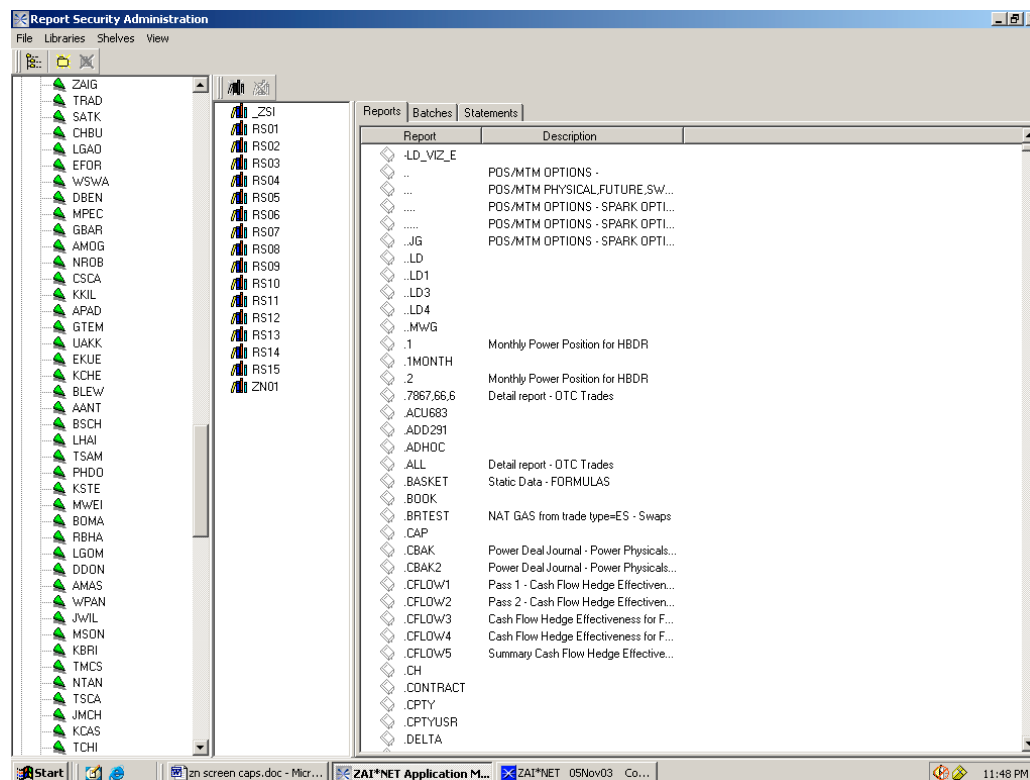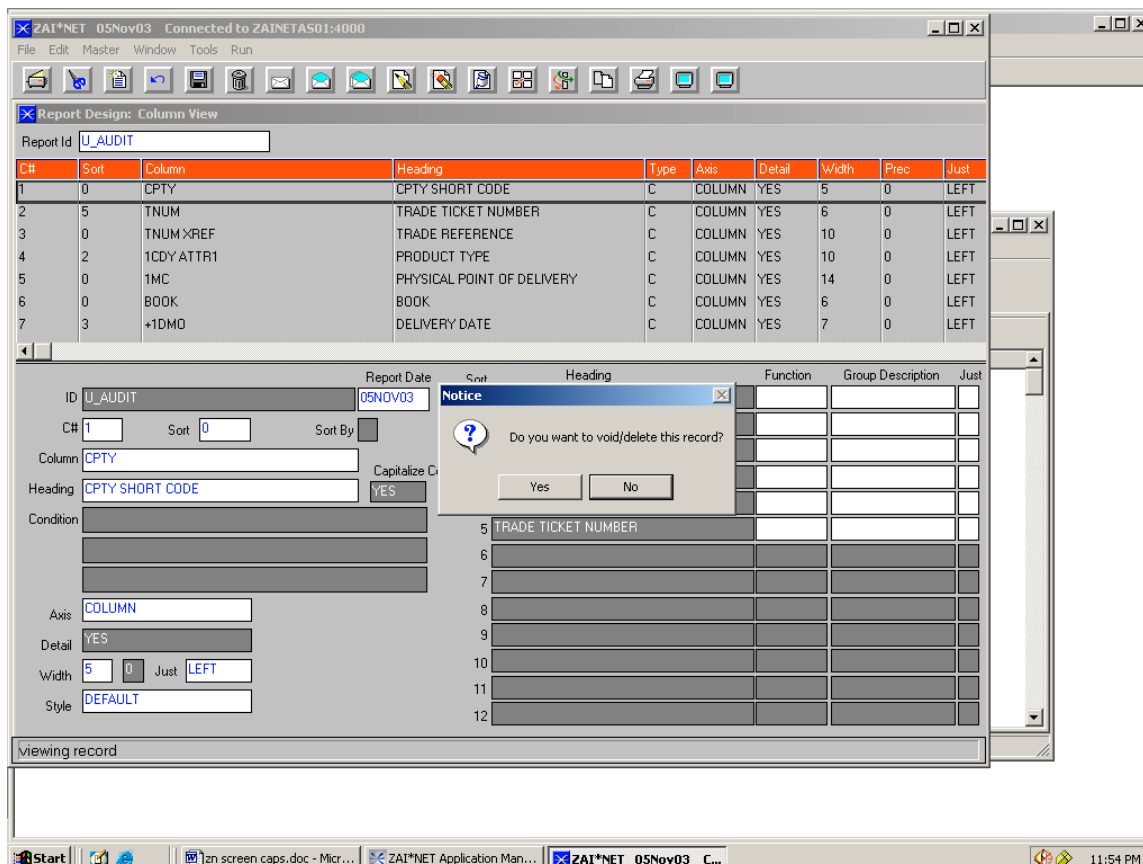
Figure 12

Figure 13

Figure 13 shows that I have the ability to edit/delete a report, which I should not be able to do as a "user."
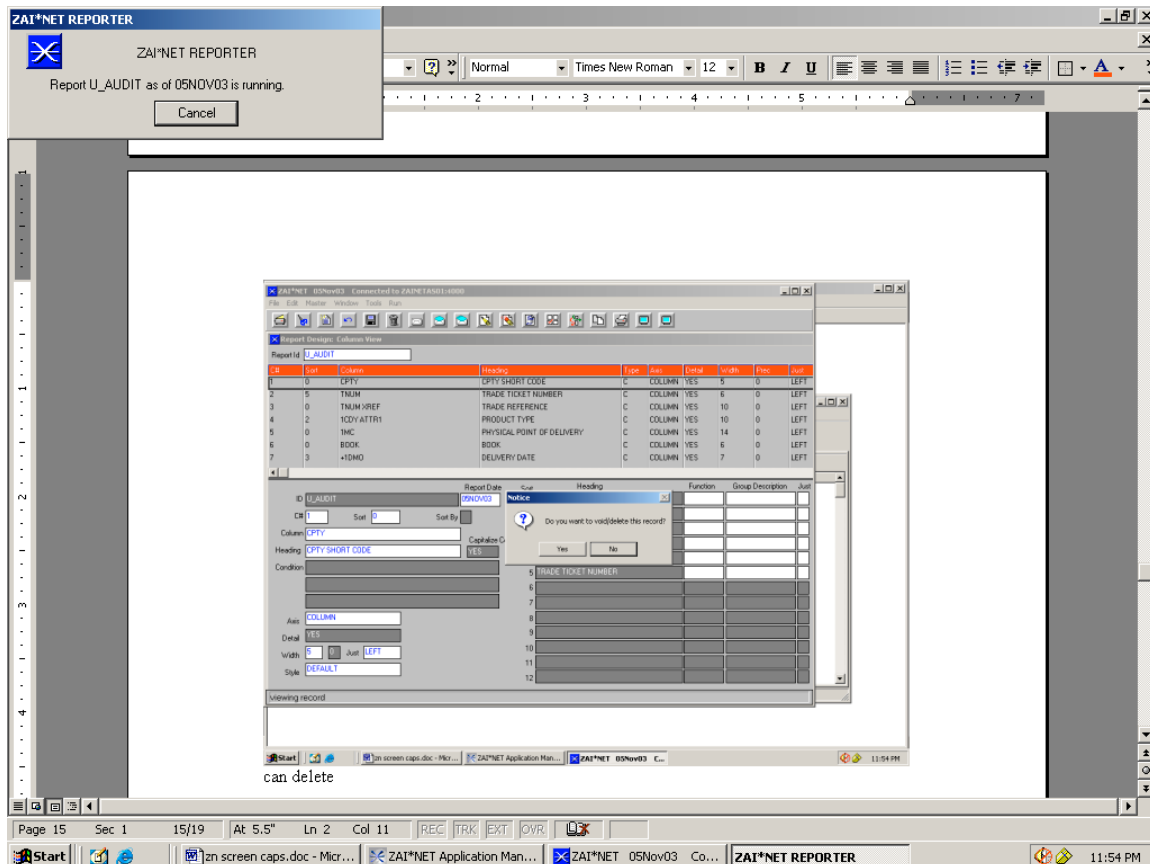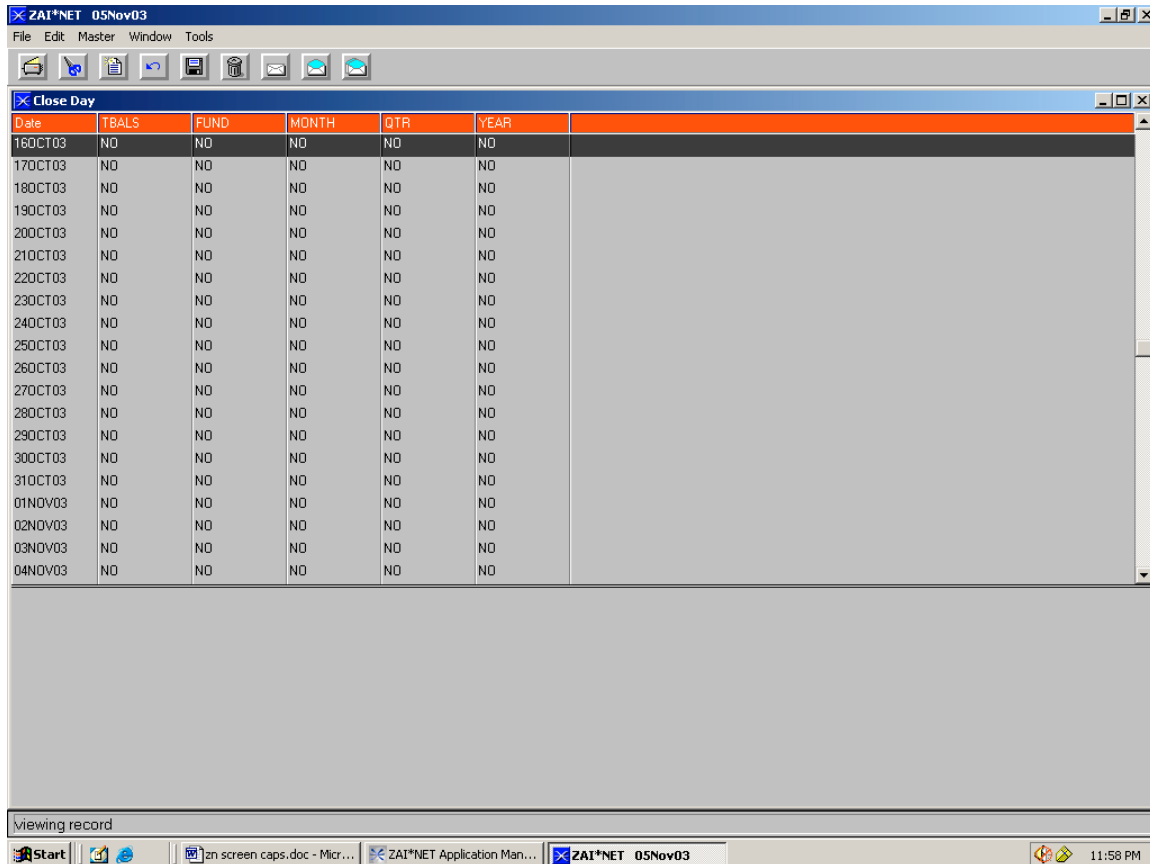
Figure 14

Figure 14 shows that I have the ability to run a report. While users will be able to run some reports, this should be restricted to prevent inexperienced users from tying up application resources by running query intensive reports. Additionally, certain reports divulge sensitive information such as earnings per share or profit and loss statements. The ability to run these reports should be restricted to authorized personnel.

Audit Step #3—Price Lockdown
PASS
Ensure that trade prices are locked down on a daily basis.

Figure 15

Figure 15 shows that as of November 5, 2003 (the day this screen shot was taken), all prior days have had Price Lockdown applied.

Audit Step #4—Retired users
PASS
Ensure that traders that have left the company no longer have access to Zai*net.
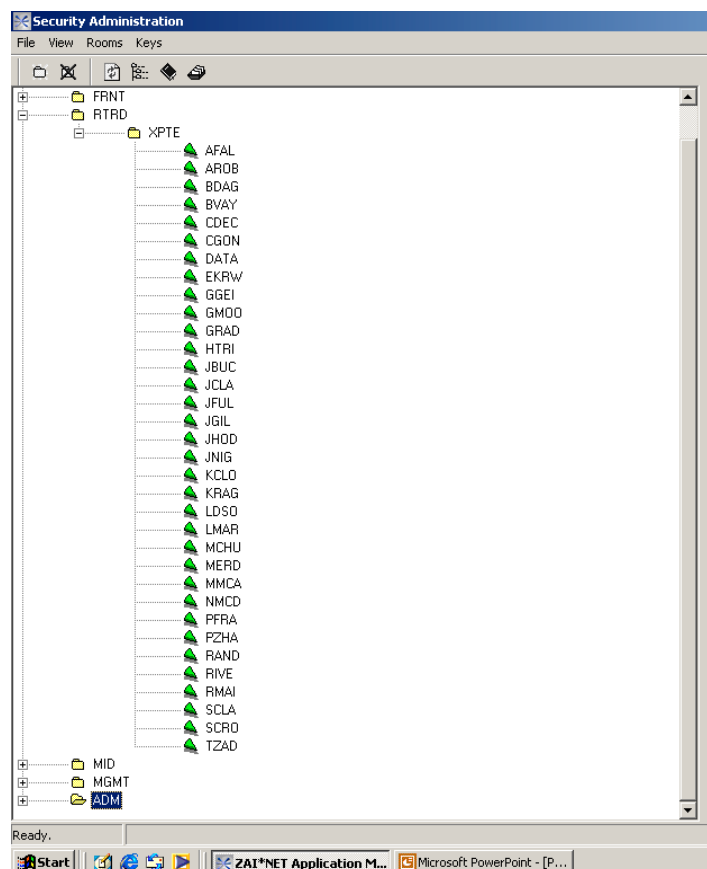
Figure 16

Figure 16, shown above is the XPTE "X-Power Trading Employees" group. Note that no key is assigned to their group. Even if a former employee were able to login to the Zai*net, he or she would not have the ability to access any pages. As a side note, when employees leave GPT, their passwords are changed by a Zai*net system administrator.
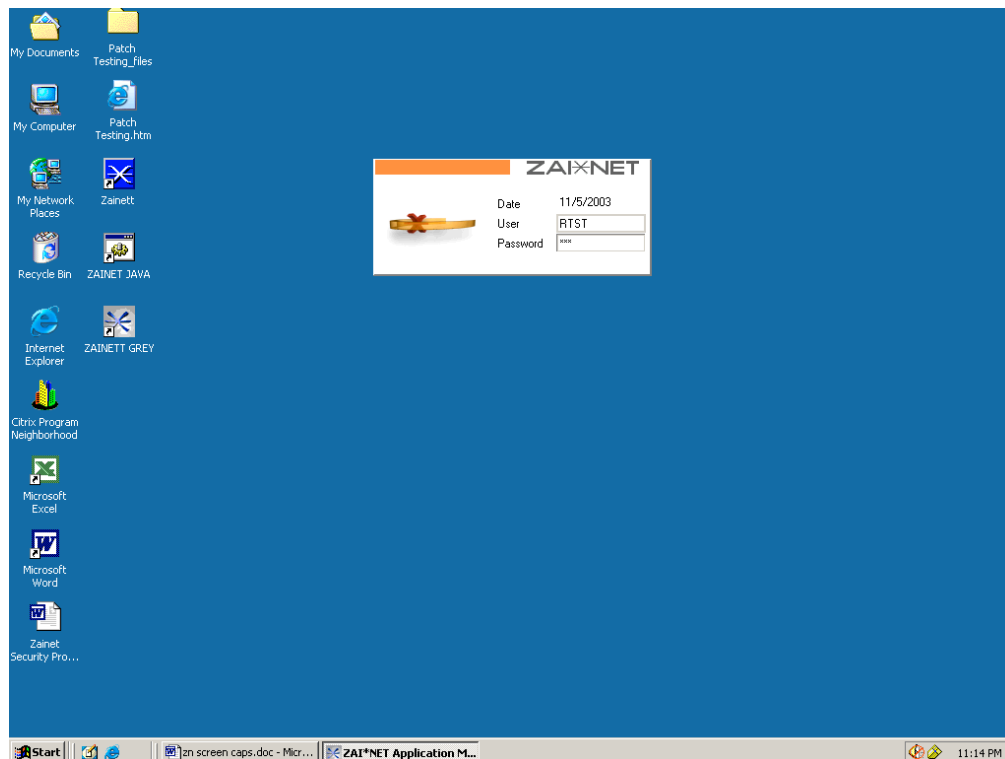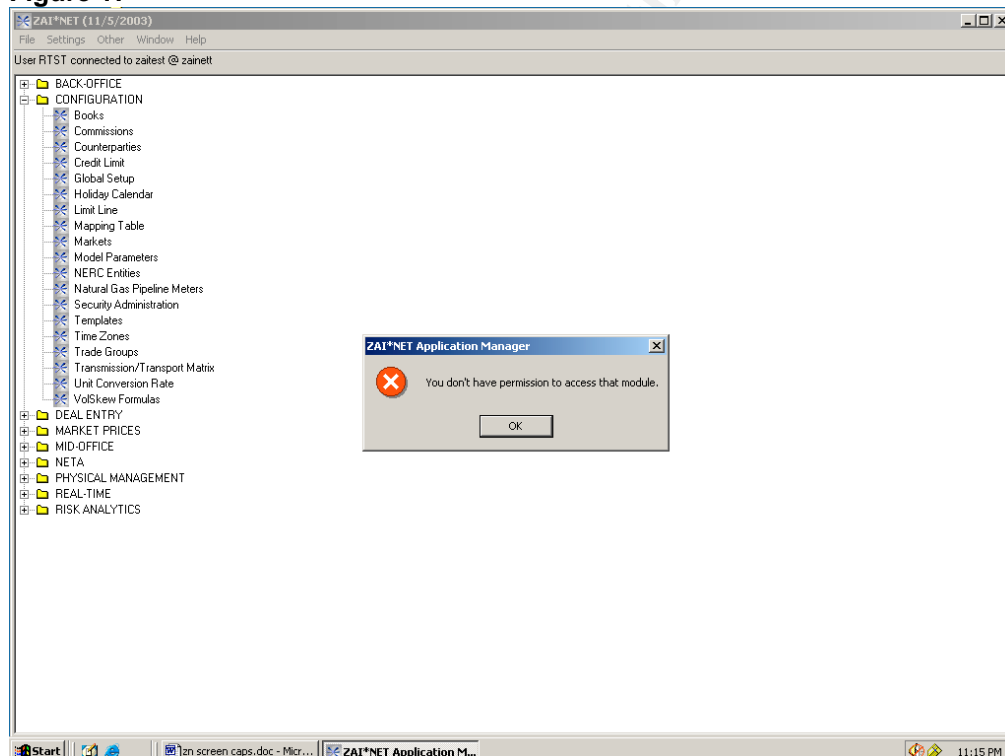
Figure 17

Figure 18

Figure 17 and 18 show me logging in as a user who has been placed in the XPTE folder and attempting (unsuccessfully) to access a submenu within "Configuration."

36

Audit Step #5—Reports

PASS

Ensure all trades are being monitored for 1) not being approved in a timely manner 2) modification 3) canceling.
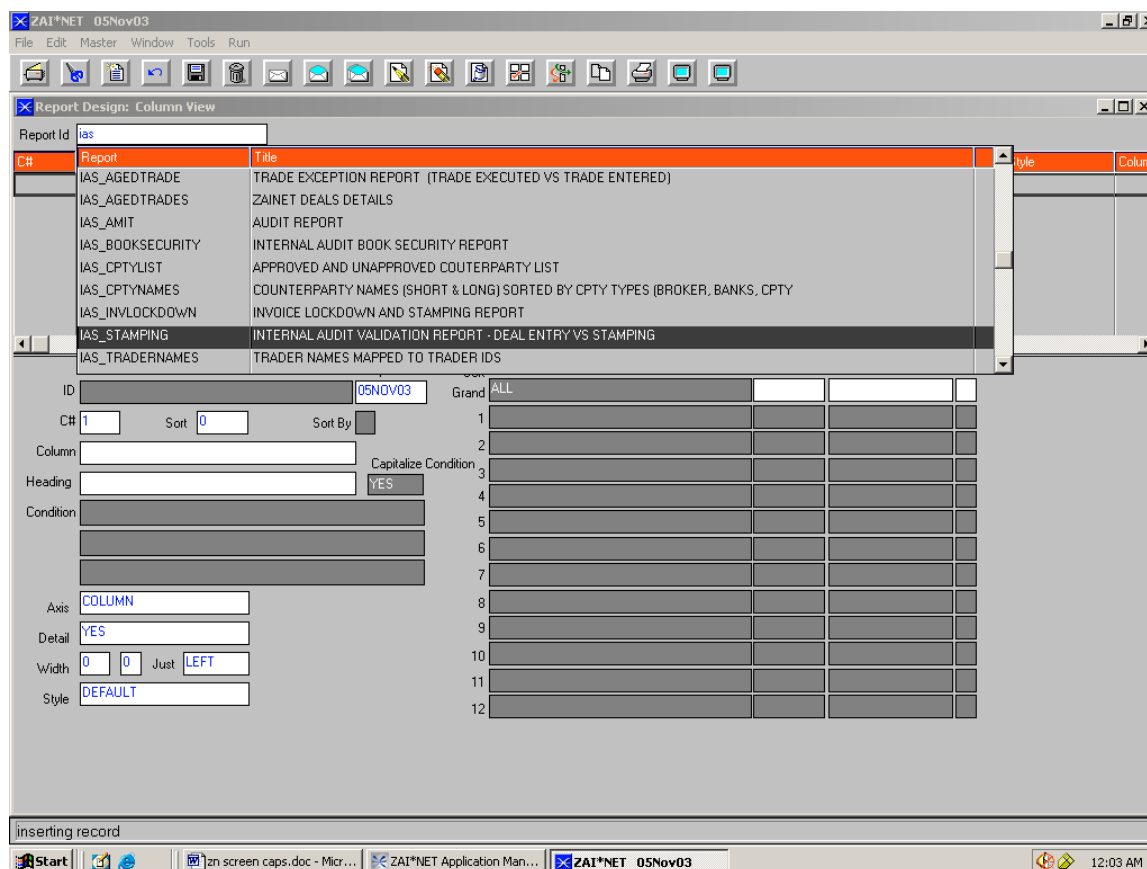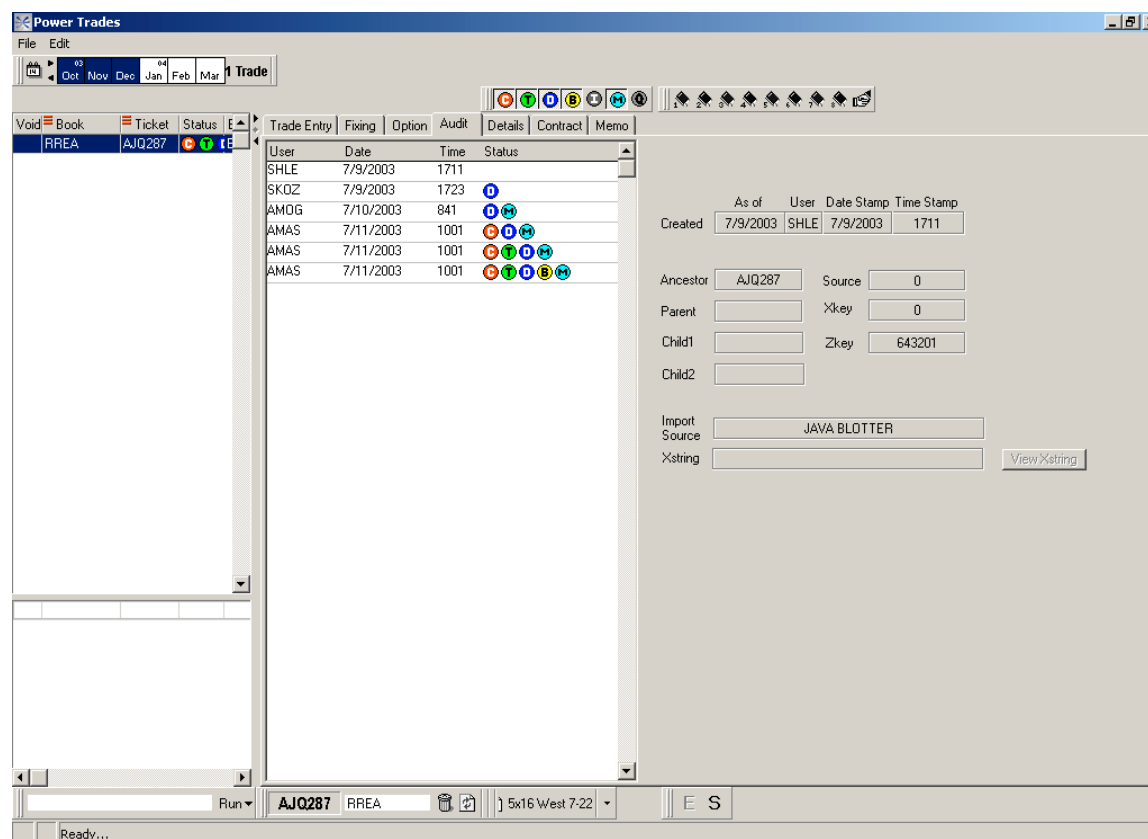

Figure 19

Figure 19 shows the three reports within the Report Design screen. These include IAS_AGEDTRADE, IAS_AGEDTRADES, and IAS_STAMPING.

Audit Step #6—D&B Stamps

PASS

Ensure that trades are only allowed to make trades (via drop down menus) with approved counterparties.

Figure 20

Figure 20 shows the stamping process for the randomly selected trade. In the middle column, the Audit Tab shows the trade being created on 7/9/2003, the D Stamp being applied on 7/9/2003, and the B Stamp being applied 7/11/2003.

Audit Step #7—Trader limit alerts

FAIL

Ensure that trader limits are set to alert appropriate personnel.

Figure 21

Figure 22

39

Figures 21 and 22 show 2 randomly selected traders that do not have limits set (Amount is set to $1.00) to alert Middle Office personnel if the traders exceed their pre-established limits.

Audit Step #8—Unapproved Counterparties

PASS

Ensure that traders are only allowed to make trades (via drop down menus) with approved counterparties.

On the Zai*net application, confirm that the GLOC table has the CPTYAPP variable set to "Y":

- Log into the new GUI
- Expand "Configuration"
- Go to "Global Setup"
- Select "GLOC" in the "View" dropdown menu
- Locate "CPTYAPP" and confirm "Y" setting
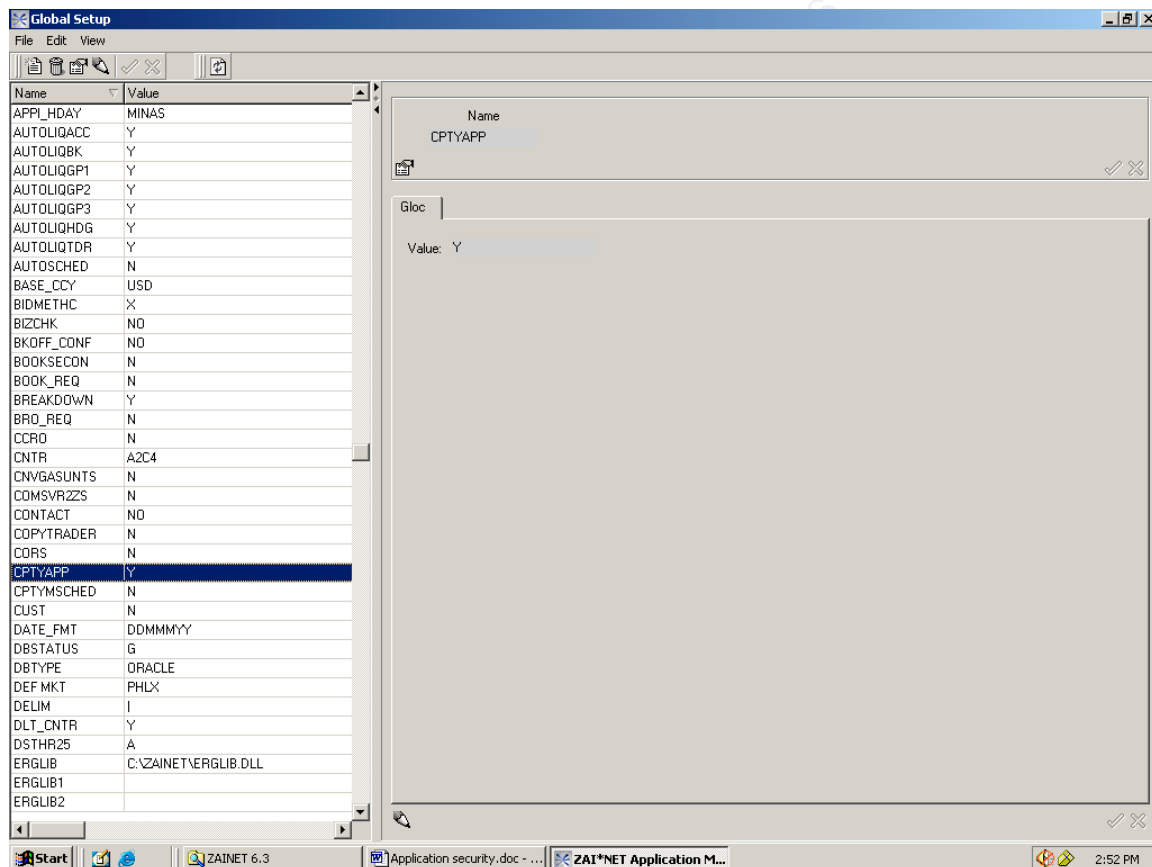
Figure 23

Figure 23 shows that the Zai*net configuration file "CPTAPP = Y" requires that traders select an approved counterparty from a drop-down list. Within the Zai*net application, this can be confirmed by simulating a trade.
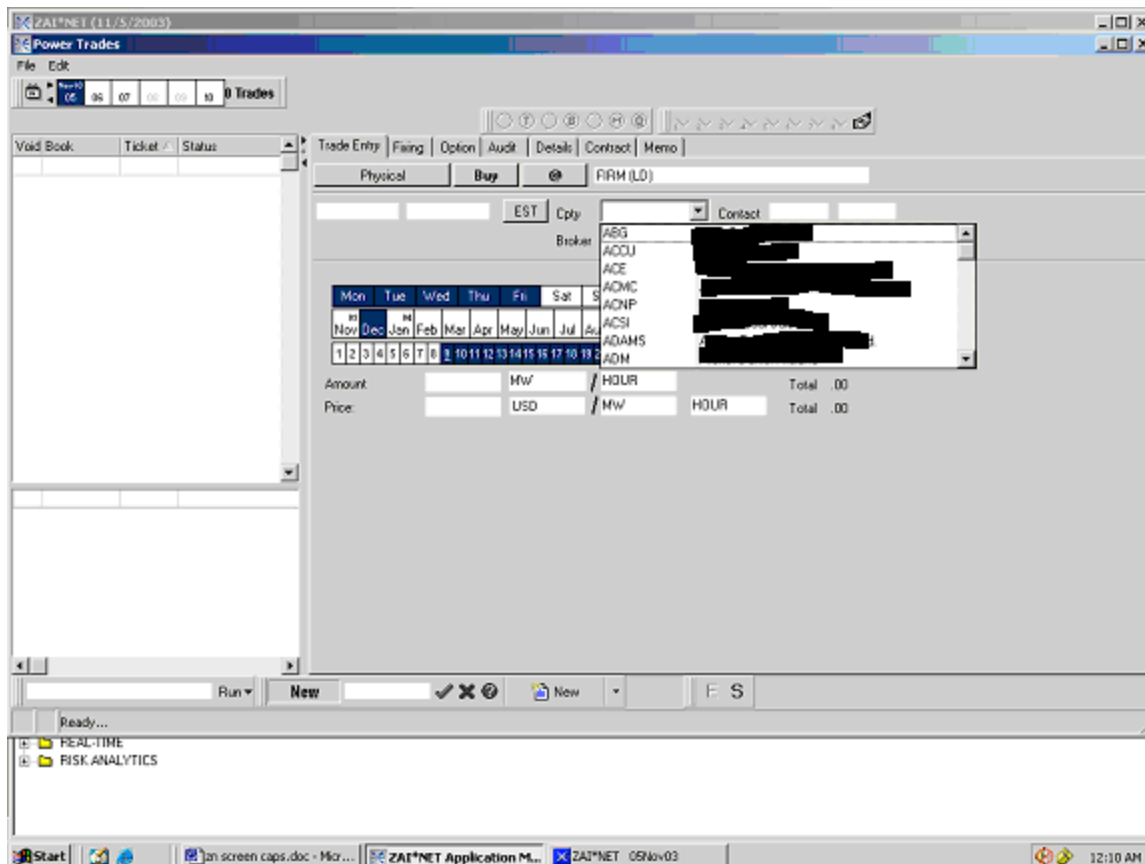
41

Figure 24

Figure 24 shows an attempt to make a trade with an unapproved counterparty, and that counterparties can only be selected through the use of a drop down menu. Attempts to type in a counterparty were unsuccessful.

Audit Step #9—Auditing

PASS
Ensure that auditing of trade information is enabled.
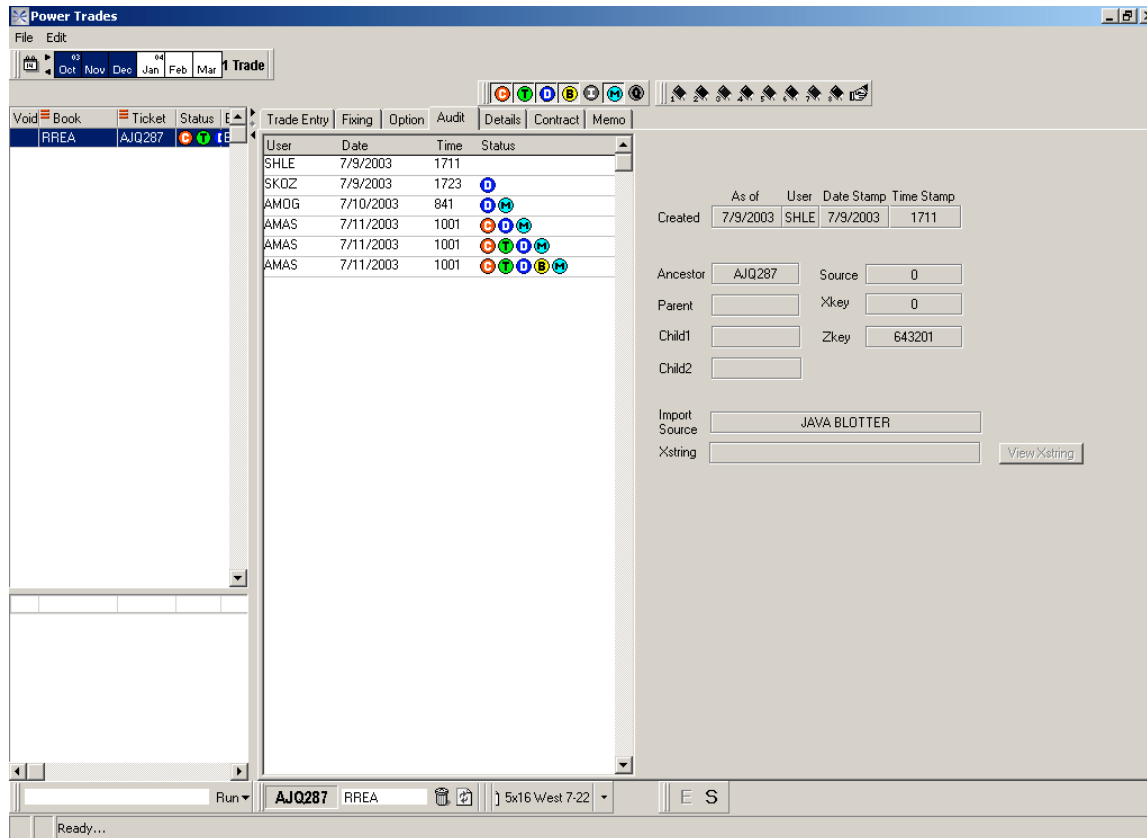
Figure 25

Figure 25 shows that auditing is enabled and tracking changes (by trader, date, time, and activity) are made to trade information.

Audit Step #10—New GUI Passwords
FAIL
Password complexity settings are compliant with Corporate Standards.
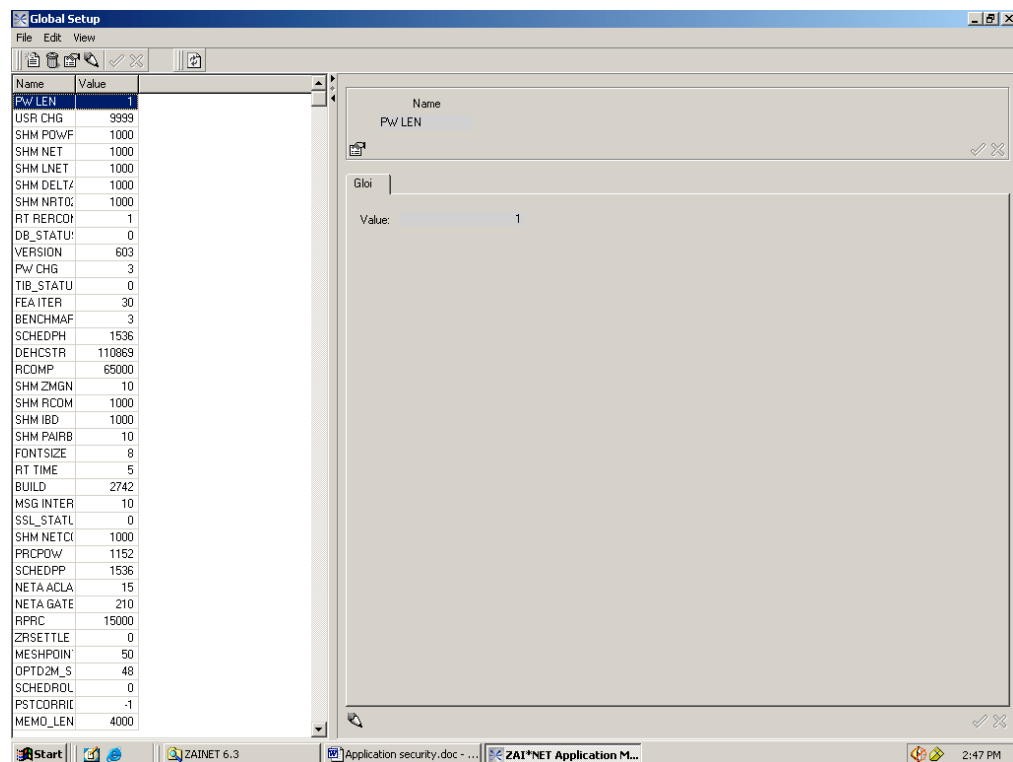
Figure 26

Figure 26 shows the "GLOI" table of "Global Setup."　Highlighted is PWLEN = 1 – This means that the minimum password length is set to 1, allowing a 1 character password.
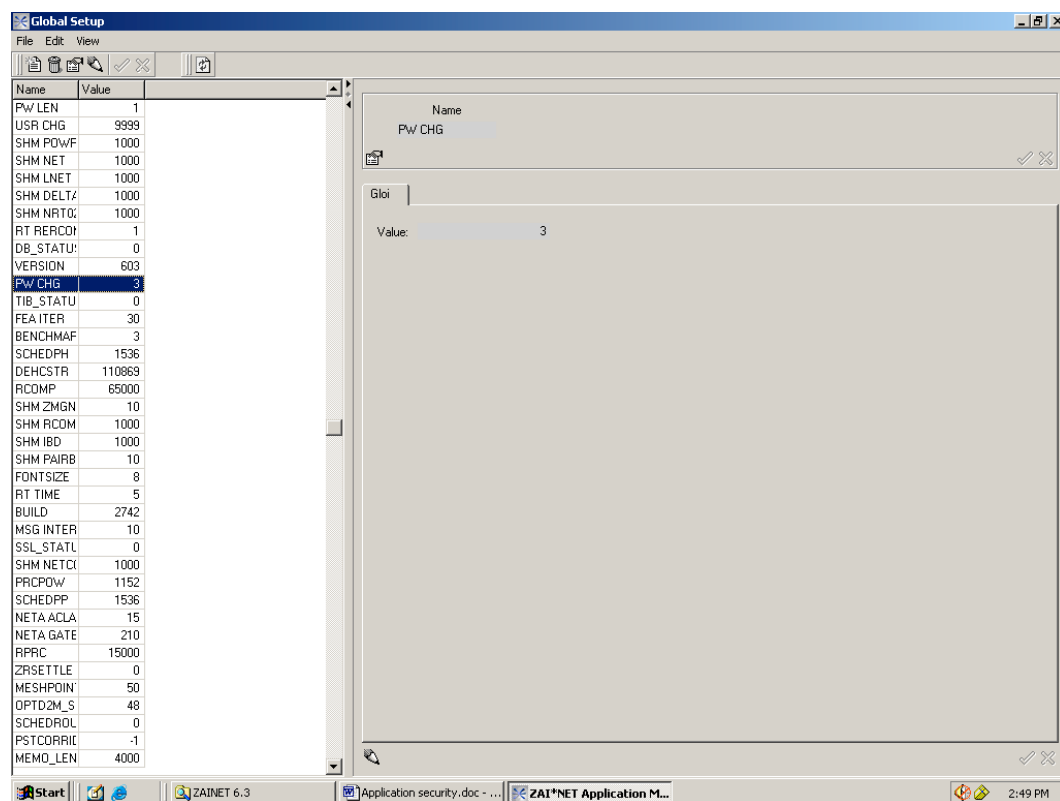
Global Setup

File Edit View

Name	Value
PW LEN	1
USR CHG	9999
SHM POWF	1000
SHM NET	1000
SHM LNET	1000
SHM DELT/	1000
SHM NRT0.	1000
RT RERCOI	1
DB_STATU:	0
VERSION	603
PW CHG	3
TIB_STATU	0
FEA ITER	30
BENCHMAF	3
SCHEDPH	1536
DEHCSTR	110869
RCOMP	65000
SHM ZMGN	10
SHM RCOM	1000
SHM IBD	1000
SHM PAIRB	10
FONTSIZE	8
RT TIME	5
BUILD	2742
MSG INTER	10
SSL_STATL	0
SHM NETC(	1000
PRCPOW	1152
SCHEDPP	1536
NETA ACLA	15
NETA GATE	210
RPRC	15000
ZRSETTLE	0
MESHPOIN'	50
OPTD2M_S	48
SCHEDROL	0
PSTCORRII	-1
MEMO_LEN	4000

Name
PW CHG

Gloi

Value: 3

Start | ZAINET 6.3 | Application security.doc - ... | ZAI*NET Application M... | 2:49 PM

Figure 27

Figure 27 shows the "GLOI" table of the "Global Setup." Highlighted is PW CHG = 3, which sets the number of times a user may enter an incorrect password before the password dialogue box closes and terminates the login session. When used in conjunction with the VOID_PW setting (which should be configured to "Y") shown in Figure 28, a user ID is disabled after 3 failed login attempts. As currently configured, 3 failed login attempts "kicks" you out of the application, but allows you to attempt to login as the same user, since the ID has not been disabled.
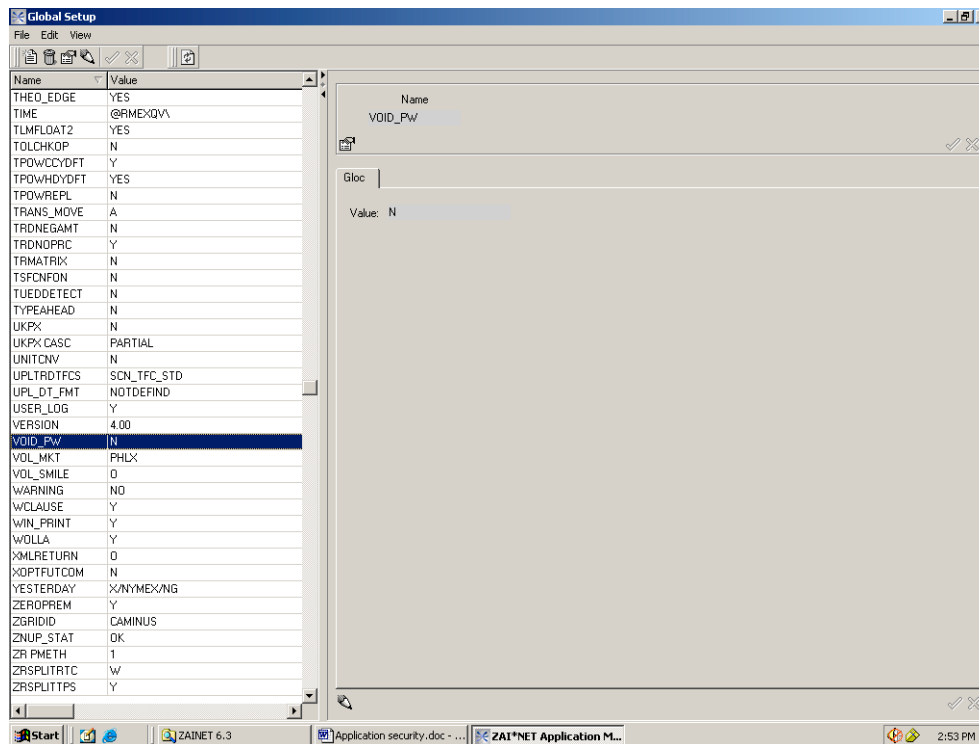
45

Figure 28

Figures 29-32 show the testing process of creating a "test" ID with only a 7 character password, which was allowed, as well as attempting to login with 3 bad passwords.
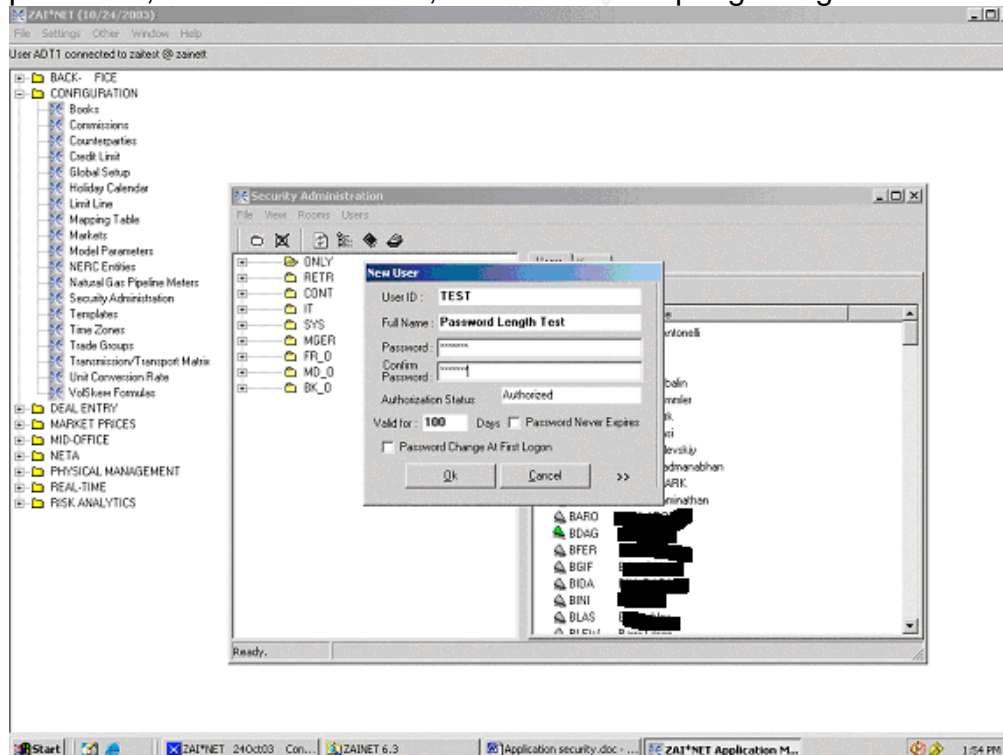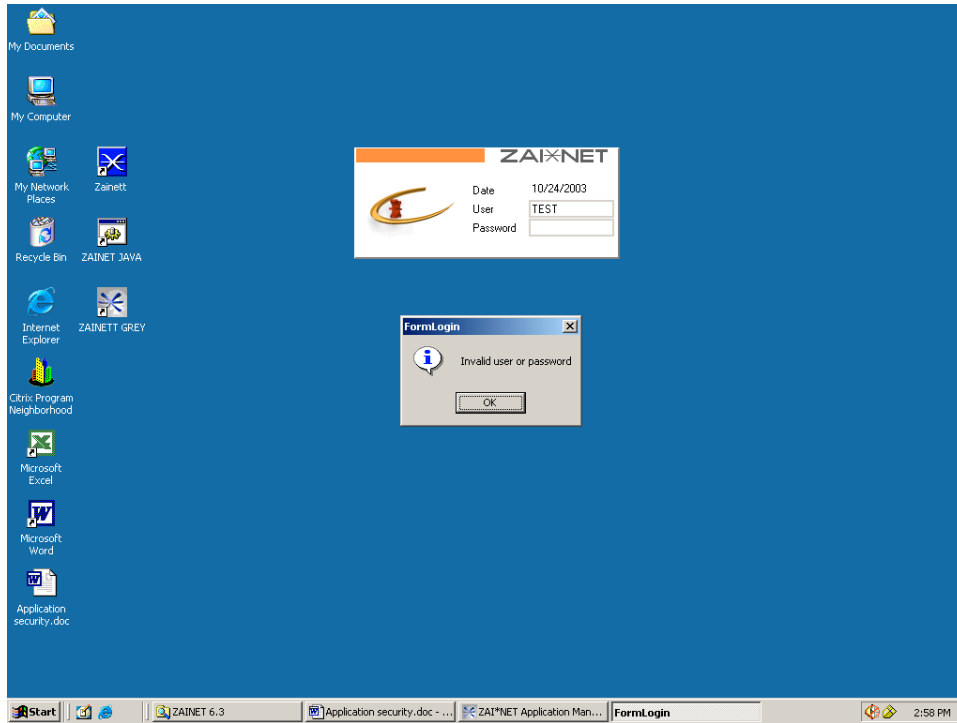

Figure 29

46

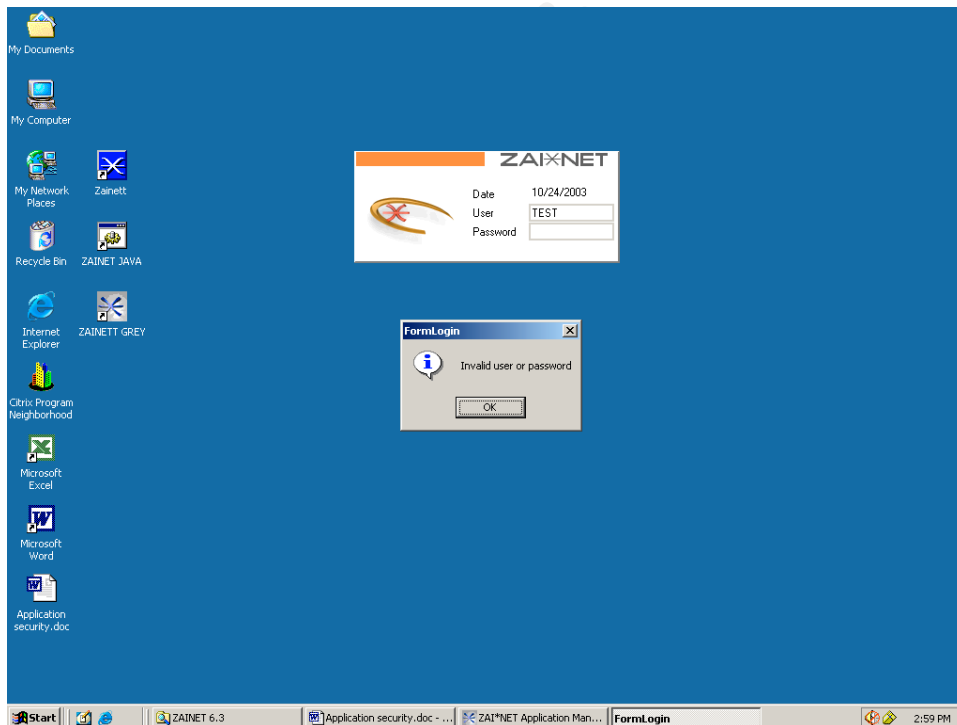Three "bad" login attempts
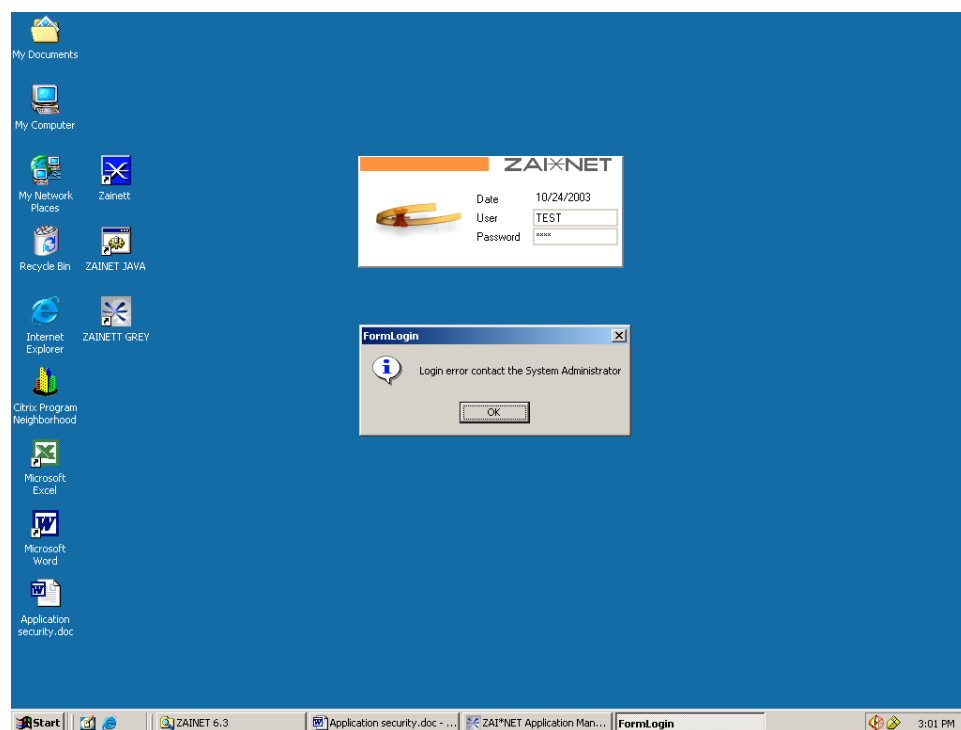

Figure 30

Figure 31

47

Figure 32

Measure residual risk

Based on the security needs of the system and the results from the conducted audit, little residual risk exists. Strong general controls (security admin/change management/ DR/etc) are in place to support the system. Additionally, many application specific controls that I was looking for in the audit were in place. The three audit findings uncovered in this report are configuration issues that can be addressed easily, with little cost to GPT. Based on the audit results, I believe that all the control objectives were achieved.

Is the system auditable?

The Zai*net application is auditable using the control objectives and checklist items. Most are considered to be stimulus and response checklist items that are truly objective. However, it is debatable whether the "Subjective" checklist items are auditable. Depending upon what processes are in place and how duties are established within an energy trading organization, there is no absolute right or wrong on segregation of duties.

Any audit of an energy trading risk management system cannot stand upon IT work alone. The process of energy trading must be completely understood in order to ensure that the controls within an application, such as Zai*net, are effectively protecting the established processes within the trading organization.

48

Overall, the system is auditable with a consolidation of best practices into 20 well-defined steps.

Audit Report

Executive Summary

For this engagement, I performed an assessment to determine if controls, both application and general IT, were adequate within Zai*net. This audit was designed to identify possible security weaknesses and/or vulnerabilities that exist within Zai*net. In order to do this, it was necessary to understand the energy trading process (as it is established at GPT). The following are the items that were defined as the scope for this audit:

- Zai*net application controls
- Security administration
- Change management
- System Performance Monitoring and Security Monitoring
- System Availability

Out of scope for this review were network devices (firewalls/routers/switches), operating systems, and databases.

Overall, there is good application security and controls for Zai*net. The only significant area of improvement revolves around password complexity enforcement. This is not to to say that Zai*net passwords do not meet Corporate Standards (due to the proprietary encryption of passwords stored within Zai*net, we were unable to test this), but that the ability to create weak passwords within Zai*net exists.

All results were discussed with GPT IT management. Management agrees with the audit issues identified and is committed to improving the control environment.

We appreciate the assistance of GPT IT personnel and management in completion of this review.

Background / Risk
Audit Step #2—Report Security
End of day reports used for daily business decisions have been created and secured, to prevent users from editing these reports. However, access to create and run ad-hoc Zai*net reports is not restricted. As a result, GPT personnel that do not have the need or necessary skills to accurately create a Zai*net report can do so. The accumulation of these reports has the potential to affect performance of the system.

Audit Step #7—Trader Limit Alerts

Zai*net trader limit alerts have not been configured to notify Middle Office personnel, in the event a trader exceeds his pre-established trading limit. As a result, a trader could expose GPT to more financial risk than allowed by the Corporate Risk Policy.

Audit Step #10—Password Complexity Settings

Zai*Net password complexity settings do not comply with Corporate Standards. Specifically, settings concerning minimum password length and ID lockout are not properly configured. Non-compliance with Corporate Standards on passwords could lead to an individual gaining access to the GPT's trading system.

Audit Recommendations

Listed below are my recommendations for addressing the identified issues:

Report Security

Develop a structure that restricts access to Zai*net reports based upon user roles (create/edit/run/delet). Once that has been created, implement this security for Zai*net reports.

Trader Limit Alerts

Activate Zai*net trader limit alerts and fill in the information regarding specific trader limits for each trader. Ensure appropriate Middle Office personnel are notified if a trader exceeds his limit.

Password Complexity Settings

Password Complexity Settings should be configured to enforce Corporate Standards to fullest extent that Zai*net is capable. This would include increasing the minimum password length to 8 and configuring Zai*net to automatically disable a user ID if a user 3 bad passwords.

Costs

The costs associated with addressing these issues would be minimal, since no additional hardware/software costs would be required. Working with the Zai*net administrator, we estimate that these corrections would take fewer than 40 hours to address.

Compensating Controls

This is not applicable since the costs to address the identified issues will be minimal, consisting only of personnel costs.

Conclusion

This audit entailed performing detailed testing on all components of GPT's Zai*net energy trading system. After completing this audit, I determined that Zai*net is configured in a secure manner. While there is some room for improvement, I would rate

50

the issues in the medium to low range of importance. Addressing the issues identified
will only enhance the security of Zai*net.

References

Articles
- Chris McCown, "Framework for Secure Application Design and Development," SANS Reading Room, http://www.sans.org/rr/paper.php?id=842, November 12, 2002.
- Jay Hollander, "What is a "Source-Code Escrow Agreement"?" Gigalaw.com, http://www.gigalaw.com/articles/2000-all/hollander-2000-08-all.html, August 2000.

Audit Checklists
- Dan Holt, "Auditing Microsoft Exchange 2000, An Administrator's Perspective," http://www.giac.org/practical/GSNA/Dan_Holt_GSNA.pdf.
- Paul Hugenberg, "Application IT System Audit," http://www.auditnet.org/docs/ApplicationITSystemsAudit.doc.
- Harvey Siegal, "EDP General Controls Review Audit Program," http://www.auditnet.org/docs/itgeneral.txt.

Books
- Caminus Zai*net 6.3 System Administration Guide, 2002.
- Caminus Zai*net 63 User Guide, 2002.
- Peter Fusaro, "Energy Risk Management," 1998, McGraw-Hill.
- Frederick Gallegos, "Information Technology Control and Audit," 1999, Auerbach Publishing.

Conferences
- Edison Electric Institute Utility Internal Auditor's Training Course, September 22-24, New Orleans, LA.
- SANS Institute, Track 7 – Auditing Networks, Perimeters and Systems, The SANS Institute, 2003.