

Global Information Assurance Certification Paper

Copyright SANS Institute Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Auditing SunGard Zai*net An Independent Auditor's Perspective

GSNA Practical Version 2.1 – Option 1

Lane Boyd

November 2003

ABSTRACT RESEARCH IN AUDIT, MEASUREMENT PRACTICE, AND CONTROL Identify the system to be audited Evaluate the risk to the system What is the current state of practice, if any? CREATE AN AUDIT CHECKLIST CREATE AN AUDIT CHECKLIST Introduction Checklist Audit Step #1 Audit Step #2 Audit Step #3 Audit Step #4 Audit Step #5 Audit Step #6 Audit Step #7 Audit Step #8 Audit Step #1	liting SunGuard Zai*net	An Independent Auditor's Perspe
ABSTRACT RESEARCH IN AUDIT, MEASUREMENT PRACTICE, AND CONTROL Identify the system to be audited Evaluate the risk to the system What is the current state of practice, if any? CREATE AN AUDIT CHECKLIST CREATE AN AUDIT CHECKLIST Introduction Checklist Audit Step #1 Audit Step #2 Audit Step #3 Audit Step #4 Audit Step #5 Audit Step #6 Audit Step #7 Audit Step #8 Audit Step #1	TABLE OF C	ONTENTS
RESEARCH IN AUDIT, MEASUREMENT PRACTICE, AND CONTROL Identify the system to be audited Evaluate the risk to the system What is the current state of practice, if any? CREATE AN AUDIT CHECKLIST Introduction CREATE AN AUDIT CHECKLIST Introduction Checklist Audit Step #1 Audit Step #2 Audit Step #3 Audit Step #4 Audit Step #4 Audit Step #4 Audit Step #3 Audit Step #4 Audit Step #1 Audit Step #1 Audit Step #1 Audit Step #1 Audit Step #11 Audit Step #11 Audit Step #13 Audit Step #14 Audit Step #15 Audit Step #13 Audit Step #13 Audit Step #14 Audit Step #13 Audit Step #13 Audit	ABSTRACT	4
RESEARCH IN AUDIT, MEASUREMENT PRACTICE, AND CONTROL Identify the system to be audited Evaluate the risk to the system What is the current state of practice, if any? CREATE AN AUDIT CHECKLIST Introduction CREATE AN AUDIT CHECKLIST Introduction Checklist Audit Step #1 Audit Step #2 Audit Step #3 Audit Step #4 Audit Step #4 Audit Step #4 Audit Step #3 Audit Step #4 Audit Step #1 Audit Step #1 Audit Step #1 Audit Step #1 Audit Step #11 Audit Step #11 Audit Step #13 Audit Step #14 Audit Step #15 Audit Step #13 Audit Step #13 Audit Step #14 Audit Step #13 Audit Step #13 Audit		
Identify the system to be audited Evaluate the risk to the system What is the current state of practice, if any? CREATE AN AUDIT CHECKLIST Introduction Checklist Audit Step #1 Audit Step #3 Audit Step #4 Audit Step #5 Audit Step #6 Audit Step #7 Audit Step #8 Audit Step #1 Audit Step #11 Audit Step #12 Audit Step #13 Audit Step #14 Audit Step #15 Audit Step #16 Audit Step #18 Audit Step #18 Audit Step #19 Audit Step #18 Audit Step #19 Audit Step #18 Audit Step #19 Audit Step #19 Audit Step #18 Audit Step #19 Audit Step #19 Audit Step #10	ABSTRACT	4
Identify the system to be audited Evaluate the risk to the system What is the current state of practice, if any? CREATE AN AUDIT CHECKLIST Introduction Checklist Audit Step #1 Audit Step #3 Audit Step #4 Audit Step #5 Audit Step #6 Audit Step #7 Audit Step #8 Audit Step #1 Audit Step #11 Audit Step #12 Audit Step #13 Audit Step #14 Audit Step #15 Audit Step #16 Audit Step #18 Audit Step #18 Audit Step #19 Audit Step #18 Audit Step #19 Audit Step #18 Audit Step #19 Audit Step #19 Audit Step #18 Audit Step #19 Audit Step #19 Audit Step #10		
Evaluate the risk to the system What is the current state of practice, if any? CREATE AN AUDIT CHECKLIST	RESEARCH IN AUDIT, MEASUREMENT PR	ACTICE, AND CONTROL 4
Evaluate the risk to the system What is the current state of practice, if any? CREATE AN AUDIT CHECKLIST		50
What is the current state of practice, if any? CREATE AN AUDIT CHECKLIST Introduction Checklist Audit Step #1 Audit Step #2 Audit Step #3 Audit Step #4 Audit Step #5 Audit Step #6 Audit Step #7 Audit Step #8 Audit Step #8 Audit Step #1 Audit Step #6 Audit Step #1 Audit Step #14 Audit Step #15 Audit Step #18 Audit Step #18 Audit Step #19 Audit Step #20	Identify the system to be audited	4
CREATE AN AUDIT CHECKLIST Introduction Checklist Audit Step #1 Audit Step #2 Audit Step #3 Audit Step #4 Audit Step #5 Audit Step #6 Audit Step #7 Audit Step #8 Audit Step #1 Audit Step #14 Audit Step #15 Audit Step #16 Audit Step #18 Audit Step #19 Audit Step #19 Audit Step #19 Audit Step #20		7
Introduction Checklist Audit Step #1 Audit Step #2 Audit Step #3 Audit Step #4 Audit Step #5 Audit Step #6 Audit Step #8 Audit Step #9 Audit Step #10 Audit Step #11 Audit Step #12 Audit Step #14 Audit Step #13 Audit Step #14 Audit Step #14 Audit Step #15 Audit Step #16 Audit Step #18 Audit Step #18 Audit Step #19 Audit Step #19 Audit Step #18 Audit Step #19 Audit Step #18 Audit Step #20	what is the current state of practice, if any?	8
Checklist Audit Step #1 Audit Step #2 Audit Step #3 Audit Step #4 Audit Step #5 Audit Step #6 Audit Step #7 Audit Step #8 Audit Step #10 Audit Step #11 Audit Step #12 Audit Step #13 Audit Step #14 Audit Step #15 Audit Step #16 Audit Step #17 Audit Step #18 Audit Step #19 Audit Step #19 Audit Step #19 Audit Step #12	CREATE AN AUDIT CHECKLIST	10
Checklist Audit Step #1 Audit Step #2 Audit Step #3 Audit Step #4 Audit Step #5 Audit Step #6 Audit Step #7 Audit Step #8 Audit Step #10 Audit Step #11 Audit Step #12 Audit Step #13 Audit Step #14 Audit Step #15 Audit Step #16 Audit Step #17 Audit Step #18 Audit Step #19 Audit Step #19 Audit Step #19 Audit Step #12	Introduction	10
Audit Step #1 Audit Step #2 Audit Step #3 Audit Step #4 Audit Step #5 Audit Step #6 Audit Step #7 Audit Step #8 Audit Step #10 Audit Step #11 Audit Step #12 Audit Step #13 Audit Step #14 Audit Step #15 Audit Step #16 Audit Step #17 Audit Step #18 Audit Step #19 Audit Step #19 Audit Step #19 Audit Step #19 Audit Step #12	Checklist	10
Audit Step #2 Audit Step #3 Audit Step #4 Audit Step #5 Audit Step #6 Audit Step #7 Audit Step #7 Audit Step #8 Audit Step #9 Audit Step #10 Audit Step #11 Audit Step #12 Audit Step #13 Audit Step #14 Audit Step #15 Audit Step #16 Audit Step #17 Audit Step #18 Audit Step #18 Audit Step #19 Audit Step #19 Audit Step #12		
Audit Step #3 Audit Step #4 Audit Step #5 Audit Step #6 Audit Step #7 Audit Step #7 Audit Step #8 Audit Step #9 Audit Step #10 Audit Step #11 Audit Step #12 Audit Step #13 Audit Step #14 Audit Step #15 Audit Step #16 Audit Step #18 Audit Step #19 Audit Step #18 Audit Step #19 Audit Step #12		
Audit Step #4 Audit Step #5 Audit Step #6 Audit Step #7 Audit Step #8 Audit Step #9 Audit Step #10 Audit Step #11 Audit Step #12 Audit Step #13 Audit Step #14 Audit Step #15 Audit Step #16 Audit Step #17 Audit Step #18 Audit Step #19 Audit Step #19 Audit Step #12	Audit Step #3	 13
Audit Step #5 Audit Step #6 Audit Step #7 Audit Step #8 Audit Step #9 Audit Step #10 Audit Step #11 Audit Step #12 Audit Step #13 Audit Step #14 Audit Step #15 Audit Step #16 Audit Step #18 Audit Step #19 Audit Step #19 Audit Step #12	Audit Step #4	13
Audit Step #6 Audit Step #7 Audit Step #8 Audit Step #9 Audit Step #10 Audit Step #11 Audit Step #12 Audit Step #13 Audit Step #14 Audit Step #15 Audit Step #16 Audit Step #17 Audit Step #18 Audit Step #19 Audit Step #19 Audit Step #20	Audit Step #5	
Audit Step #/ Audit Step #8 Audit Step #10 Audit Step #11 Audit Step #12 Audit Step #13 Audit Step #14 Audit Step #15 Audit Step #16 Audit Step #17 Audit Step #18 Audit Step #19 Audit Step #20	Audit Step #6	14
Audit Step #8 Audit Step #10 Audit Step #11 Audit Step #12 Audit Step #13 Audit Step #14 Audit Step #15 Audit Step #16 Audit Step #17 Audit Step #18 Audit Step #19 Audit Step #20	Audit Step #7	15
Audit Step #9 Audit Step #10 Audit Step #11 Audit Step #12 Audit Step #13 Audit Step #13 Audit Step #14 Audit Step #15 Audit Step #16 Audit Step #17 Audit Step #18 Audit Step #19 Audit Step #12	Audit Step #8	15
Audit Step #10 Audit Step #11 Audit Step #12 Audit Step #13 Audit Step #13 Audit Step #14 Audit Step #15 Audit Step #16 Audit Step #17 Audit Step #18 Audit Step #19 Audit Step #19 Audit Step #20		16
Audit Step #11 Audit Step #12 Audit Step #13 Audit Step #14 Audit Step #15 Audit Step #16 Audit Step #17 Audit Step #18 Audit Step #19 Audit Step #20		16
Audit Step #12 Audit Step #13 Audit Step #14 Audit Step #15 Audit Step #16 Audit Step #16 Audit Step #17 Audit Step #18 Audit Step #19 Audit Step #20		17
Audit Step #13 Audit Step #14 Audit Step #15 Audit Step #16 Audit Step #16 Audit Step #17 Audit Step #17 Audit Step #18 Audit Step #19 Audit Step #20 AUDIT EVIDENCE		17
Audit Step #14 Audit Step #15 Audit Step #16 Audit Step #17 Audit Step #17 Audit Step #18 Audit Step #19 Audit Step #20 AUDIT EVIDENCE Conduct the audit		18
Audit Step #15 Audit Step #16 Audit Step #17 Audit Step #18 Audit Step #19 Audit Step #20 AUDIT EVIDENCE Conduct the audit	Audit Step #14	4.0
Audit Step #16 Audit Step #17 Audit Step #18 Audit Step #19 Audit Step #20 AUDIT EVIDENCE Conduct the audit	Audit Step #15	20
Audit Step #17 Audit Step #18 Audit Step #19 Audit Step #20 AUDIT EVIDENCE Conduct the audit	Audit Step #16	21
Audit Step #18	Audit Step #17	22
Audit Step #20	Audit Step #18	23
AUDIT EVIDENCE	Audit Step #19	24
Conduct the audit	Audit Step #20	24
		25
	Conduct the audit	25
Augit Step #1—Application User Security	Audit Step #1—Application User Security	2

Audit Step #2—Report Security	29
Audit Step #3—Price Lockdown Audit Step #4—Retired users	34 35
Andlit Otan #E Demanta	35 37
Audit Step #6—D&B Stamps	 38
Audit Step #7—Trader limit alerts	39
Audit Step #8—Unapproved Counterpart	
Audit Step #9—Auditing	43
Audit Step #10—New GUI Passwords	44
AUDIT REPORT	49
Executive Summary	49
Background / Risk	49 49
Audit Recommendations	50
Conclusion	 50
REFERENCES	52

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.

As part of GIAC practical repository.

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.

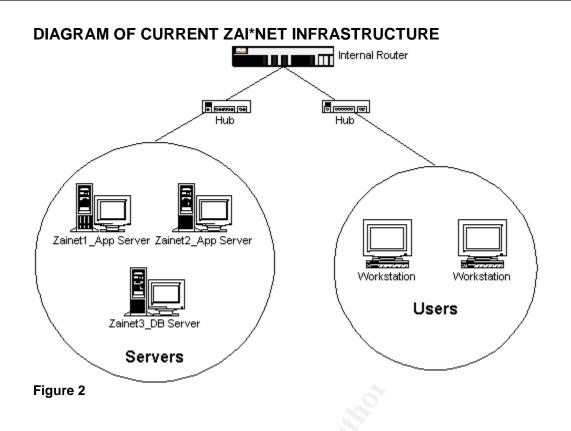
I'll briefly mention the major controls for Zai*net.

Controls

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

	Х		
Operating System Security	Х		
Password complexity	Х		
Patch Management	Х		
Physical Security	Х		
Policies	Х		
Price Lockdown	Х	Х	
Reports			X
Report Security		Х	X
Retired Users	Х	•	65
Risk Control Document	Х		
Stamping Process	Х	X	
Source Code Escrow	X		
System Performance Monitoring	5	7	
Trader and Counterparty Limit Alerts		Х	
User and Administrator Security Awareness	Х		
WarnDays	Х		
Figure 1			

©SANS Institute 2003



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	
	©SANS Institute 2003	As part of GIAC practical repository.	Author retains full rights.
©S	ANS Institute 2003,	As part of GIAC practical repository.	Author retains full rights.

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, <u>http://www.sans.org/rr/paper.php?id=842</u>, November 12, 2002.
- Jay Hollander, "What is a "Source-Code Escrow Agreement"?" Gigalaw.com, <u>http://www.gigalaw.com/articles/2000-all/hollander-2000-08-all.html</u>, August 2000.

Audit Checklists

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

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, <u>Track 7 Auditing Networks</u>, Perimeters and Systems, 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.

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

Reference	http://www.sans.org/rr/paper.php?id=842		
Control Objective	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.		
	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 residin		
	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		
©SANS Institute 2003	As part of GIAC practical repository. Author retains full rigi		
titute 2003,	As part of GIAC practical repository. Author ret		

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:

<u>Front Office</u> FTRD—Fuels Trading ANLY—Analysis PTRD—Power Trading FRNT—Front Office

<u>Middle Office</u> 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.

diting Sun	Guard Zai*net	An Independent Auditor's Perspectiv
Testing		nsure that keys are assigned to ordance with GPT energy trading
	Login to the New GUI Select "Configuration" Select "Security Administra Select "New" under "Users Create a new user by inpu Select "OK"	
		into each folder you want to test. The ID of the key(s) located in the folder.
Objective/Sub	jectiveObjective	

Audit Step #2

A

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
	10
	12
©SANS Institute 2003	As part of GIAC practical repository. Author retains full rights
itute 2003.	As part of GIAC practical repository. Author reta

...

An Independent Auditor's Perspective

Objective/SubjectiveObjective—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/Subjectiv	/eObjective

•		
Retired Users		
Reference	http://www.sans.org/rr/paper.php?id=842	
Control Objective	Determine if users that are no longer with the their access removed from Zai*net	company have had
Risk	Users that have left the company may attemp Zai*net and make unauthorized transactions. the Zai*net application prevents user IDs from the system. In order to prevent alteration of Z these individuals, their access to Zai*net page Normally, these users should be removed fro when the ID is no longer being used. However Zai*net has been configured at GPT, these ID without "orphaning" trade information.	The data structure o n being deleted from Zai*net information by es must be removed. m an application er, due to the way the
Compliance	Former users will be placed into a "Retired" g privileges, whatsoever.	roup, which has no
Testing	Compare users to a current employee list from	m HR.
	All users that are not current employees shou list, which has no access.	Ild be in the "RETR"
	13	
©SANS Institute 2003	As part of GIAC practical repository.	Author retains full right

Auditing	Sun	Guard	Zai*net
11000000	N CHAI	o and a	Liui nee

	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	eObjective

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	eObjective

Reference	Reference Caminus Zai*net 6.3 System Administration Guide Personal experience	
	14	
©SANS Institute 2003	14 As part of GIAC practical repository.	Author retains full rights.

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/Subjectiv	veObjective

Audit Step #7

Trader Limit Alerts	S
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/Subjectiv	

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.

An Independent Auditor's Perspective

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	ctiveObjective

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/Subjectiv	eObjective

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	

Auditing	Sun	Guard	Zai*net
Auuning	Suir	Juaru	Lai IIci

	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/Subjec	tiveObjective

Audit Step #11

Source Code Escr	ow
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/Subjectiv	eObjective

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

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 Awarene	SS
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/Subjectiv	eObjective-whether it was actually given or not Subjective-Content and effectiveness of the training

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.
0	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.
	19
©SANS Institute 2003	As part of GIAC practical repository. Author retains full righ

Objective/Subjective

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/Subjectiv	eObjective—Standards are in place Subjective—Effectiveness of standards

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 system directories and verify that access is appropriate based on job responsibilities. Determine who has access to the system directories. 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. Obtain the changes are authorized by management, prior to implementation.	Change Managem	
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 is appropriate based on job responsibilities. Determine who has access to the system directories. Obtain a list of individuals with access is appropriate based on job responsibilities. Determine who has access to the system directories. Obtain a list of individuals with access is appropriate based on job responsibilities. Determine who has access to the system directories. Obtain a list of individuals with access is appropriate based on job responsibility. Select a sample of 5 program changes, including emergency and requested changes, and complete the following: Obtai	Reference	Information Technology Control and Audit
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. esting 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.	Control Objective	adequately tested and approved changes (both emergency and normal) implemented into production, and prevent implementation
evidence that this process is followed exists. resting 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.	Risk	adversely impact energy trading operations by introducing
esting 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 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.	Compliance	
 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 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. 	Testing	Business unit and IT department management approval is required before systems acquisition and/or change projects are
 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 are authorized by management, prior to implementation. 		production systems exist for development (or modification) and
 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. 		
 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. 		and Test environments and verify that access is
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.		Determine who has access to the system directories.
 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. 		directories and verify that access is appropriate based on
 each of the changes. Verify that the changes are authorized by management, prior to implementation. 		
prior to implementation.		
		 Prequested changes, and complete the following of the respective request/approviet ach of the changes. Verify that the changes are authorized prior to implementation.
		21 As part of GIAC practical repository. Author retains full rigit

Auditing SunGua	rd Zai*net	An Independent Auditor's Pers
	are available.Verify that the test	ange testing documentation and results sted changes are approved for move to meone other than the programmer.

Verify that all relevant parties, including users are being notified of the changes and actual installation of the change.

In Independent Auditor's Perspective

- 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/SubjectiveObjective

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.	

diting Sun	Guard Zai*net An Independent Auditor's Perspect
Testing	Determine who is responsible for the back-up process.
looung	
	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/Sub	jective Objective
Audit Step #	18
Audit Step #	

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/Subjectiv	eSubjective—Completeness of disaster recovery plan. Objective—Examination of hot-site agreement and testing
	23
©SANS Institute 2003	As part of GIAC practical repository. Author retains full right
tituto 2003	As part of GIAC practical repository

ve

An Independent Auditor's Perspective

documentation.

Audit Step #19

Password Comple	xity – 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	eObjective

Archiving	
Reference	Personal Experience
-	Unused Zai*net data is archived (removed from the database), enhancing Zai*net performance.
	Unnecessary data will continue to collect within Zai*net, slowing system performance.
	A process is in place to identify unnecessary data and remove it from the production Zai*net database.
	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—Data archiving occurs. Subjective—Determining what specific tables should be archived.

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.

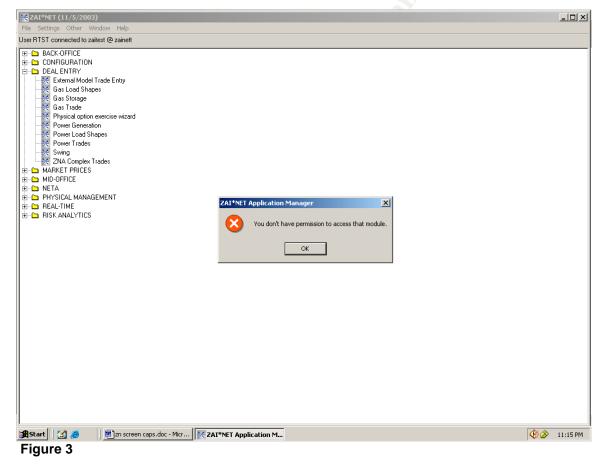


Figure 3 shows that as a member of the Middle Office, I attempted (unsuccessfully) to gain access to the "Power Trades" screen, which should be restricted to the Front Office.

	©SA	٩NS	In	IS	titute	2003	

2AI*NET (11/5/2003)		_ _ ×
File Settings Other Window Help		
User RTST connected to zaitest @ zainett		
BackOFFICE BackOFFICE BackOFFICE Contributer and the second second functions Contributer Prices Microsoft Second Second Functions Discrete Prices Microsoft Second Second Second Functions Discrete Prices Microsoft Second	Vou don't have permission to access that module.	11:24 FM
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.

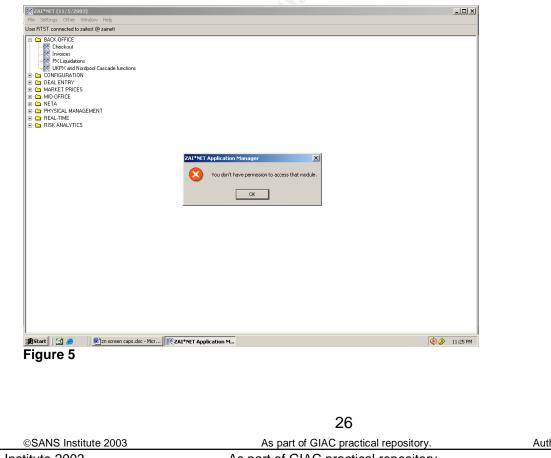
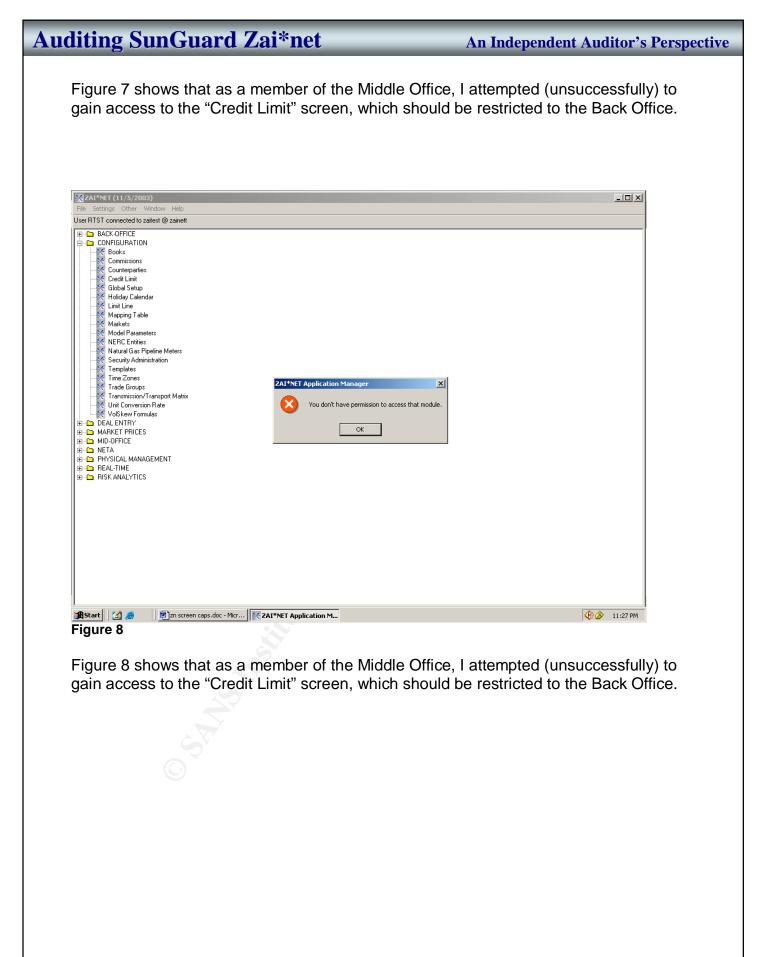


Figure 5 shows that as a member of the Front Office, I attempted (unsuccessfully) to gain access to the "Invoice" screen, which should be restricted to the Back Office.

ZAI*NET (11/5/2003)		X
File Settings Other Window Help		
BACK-OFFICE CONFIGURATION DEALE NIRY MARKET FRICES MID-OFFICE DE PHO-OFFICE DE DE D	ZAL*NET Application Manager	
	ZALTINE I Application M	49 🖉 11:30 PM
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.

ZAI*NET (11/5/2003)	× □_	
File Settings Other Window Help User RTST connected to zaitest @ zainett		
Urer RTST connected to zatest @ zamet ■ DAC-OFFICE ■ COMFIGURATION © Connected to zatest @ zamet © Connected to zatest @ zatest © Connected to zatest © Conne	ZATINET Application Manager X You don't have permission to access that module.	
🎉 Start 🛛 🏹 🥔 🗍 🖻 zn screen caps.doc - Micr 🕅 🏹 Zf	AI*NET Application M 😢 🇞 11:28 PM	
Figure 7		
	27	
©SANS Institute 2003	As part of GIAC practical repository.	Author retains full rights.
© SANS Institute 2003,	As part of GIAC practical repository.	Author retain



As part of GIAC practical repository.

Audit Step #2—Report Security

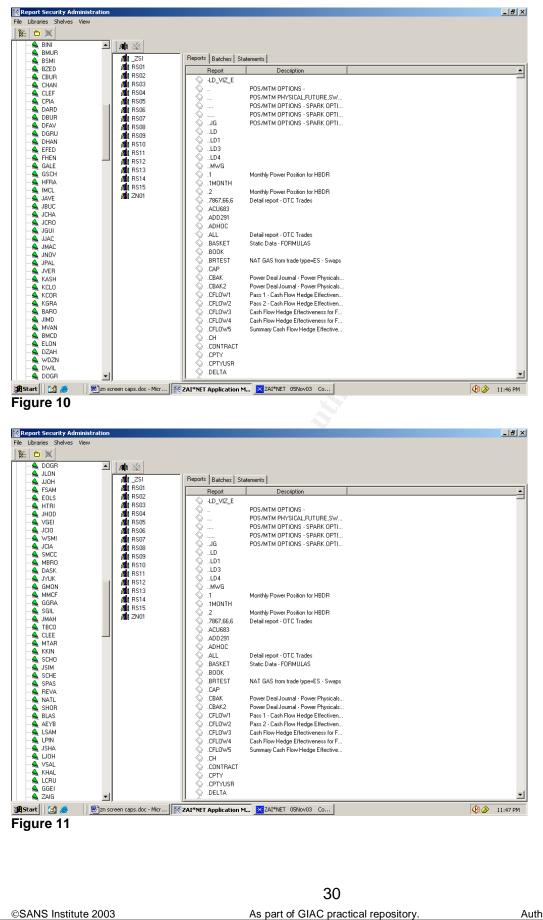
FAIL

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.

II Reports Batches 11 Report Report 12 ↓ LD_VIZ_E 13 ↓ ↓ 15 ↓	Description POS/MTM OPTIONS - POS/MTM PHYSICAL,FUTURE,SW POS/MTM OPTIONS - SPARK OPTI POS/MTM OPTIONS - SPARK OPTI		<u>.</u>
Image: style	Description P0S/MTM OPTIONS - P0S/MTM OPTIONS - SPARK OPTI P0S/MTM OPTIONS - SPARK OPTI		
Image: style	Description P0S/MTM OPTIONS - P0S/MTM OPTIONS - SPARK OPTI P0S/MTM OPTIONS - SPARK OPTI		
Image: style	Description P0S/MTM OPTIONS - P0S/MTM OPTIONS - SPARK OPTI P0S/MTM OPTIONS - SPARK OPTI		
Image: style	Description P0S/MTM OPTIONS - P0S/MTM OPTIONS - SPARK OPTI P0S/MTM OPTIONS - SPARK OPTI		
11 1 12 0 13 ↓ 14 ↓ 15 ↓ 16 ↓ 17 ↓ 18 ↓ 19 ↓ 10 ↓ 10 ↓ 11 ↓ 12 ↓ 13 ↓ 14 ↓ 15 ↓ 16 ↓ 17 ↓ 18 ↓ 10 ↓ 11 ↓ 12 ↓ 14 ↓ 15 ↓ 20 7867.66.6 △ △DD231 ↓ △ △ △DD231 ↓ △ △ △DD40C △ △LL	Description P0S/MTM OPTIONS - P0S/MTM OPTIONS - SPARK OPTI P0S/MTM OPTIONS - SPARK OPTI		
12 rteput 13 ↓ LD_VIZ_E 14 ↓ 15 ↓ 16 ↓ 17 ↓ 18 ↓ 19 ↓ 10 ↓ 11 ↓ 12 ↓ 14 ↓ 15 ↓ 14 ↓ 15 ↓ 14 ↓ 15 ↓ △ ACU6833 △ ADD231 △ ADL	POS/MTM OPTIONS - POS/MTM PHYSICAL,FUTURE,SW POS/MTM OPTIONS - SPARK OPTI POS/MTM OPTIONS - SPARK OPTI POS/MTM OPTIONS - SPARK OPTI Monthly Power Position for HBDR Monthly Power Position for HBDR		
33 → ↓□_VL_E 34 → … 35 → … 36 → … 37 → … 38 → … 39 → … 10 … … 11 → … 12 → … 13 → … 14 → … 15 → … 16 → … 17 → .2 18 → … 19 … … 10 … … 11 → … 12 … … 14 → … 15 → … 10 … 2 11 → … 12 … … 13 → … 14 … … 15 … … 10 … … 11 … … 15 … … 16 … … 17 … … 18	POS/MTM PHYSICAL, FUTURE, SW POS/MTM OPTIONS - SPARK OPTI POS/MTM OPTIONS - SPARK OPTI POS/MTM OPTIONS - SPARK OPTI Monthly Power Position for HBDR Monthly Power Position for HBDR		
13.3 ↓ 135 ↓ 136 ↓ 137 ↓ 138 ↓ 100 ↓ 111 ↓ 123 ↓ 14 ↓ 15 ↓ 14 ↓ 15 ↓ 14 ↓ 11 ↓ 12 ↓ 14 ↓ 11 ↓ 12 ↓ 13 ↓ 14 ↓ 11 ↓ 12 ↓ 13 ↓ 14 ↓	POS/MTM PHYSICAL, FUTURE, SW POS/MTM OPTIONS - SPARK OPTI POS/MTM OPTIONS - SPARK OPTI POS/MTM OPTIONS - SPARK OPTI Monthly Power Position for HBDR Monthly Power Position for HBDR		
14	POS/MTM PHYSICAL, FUTURE, SW POS/MTM OPTIONS - SPARK OPTI POS/MTM OPTIONS - SPARK OPTI POS/MTM OPTIONS - SPARK OPTI Monthly Power Position for HBDR Monthly Power Position for HBDR		
JD Similar Similar J7 Similar Similar J8 JG JG J0 LD LD 10 LD3 LD3 11 Similar LD4 J3 JMWG 1 14 Similar 1000000000000000000000000000000000000	POS/MTM OPTIONS - SPARK OPTI POS/MTM OPTIONS - SPARK OPTI POS/MTM OPTIONS - SPARK OPTI Monthly Power Position for HBDR Monthly Power Position for HBDR		
J6	POS/MTM OPTIONS - SPARK OPTI POS/MTM OPTIONS - SPARK OPTI Monthly Power Position for HBDR Monthly Power Position for HBDR		
1/2	POS/MTM OPTIONS - SPARK OPTI Monthly Power Position for HBDR Monthly Power Position for HBDR		
10 .LD 10 .LD1 11 .LD3 12 .LD4 13 .LD4 14 .INONTH 15 .ACU683 ADD291 .AD0291 AD1021 .AD0291 AD102 .AD1040	Monthly Power Position for HBDR Monthly Power Position for HBDR		
19 U 10 LD1 11 LD4 12 LD4 13 LD4 14 LD4 15 LD4 16 LD4 17 LD4 18 LD4 19 LD4 10 LD4 11 LD4 12 LD4 13 LD4 14 LD4 15 LD4 10 LD4 11 LD4 12 LD4 14 LD4 15 LD4 16 LD4 17 LD4 18 LD4 19 LD4 11 LD4 10 LD4 11 LD4 11 LD4 11 LD4 11 LA4 12 LA4 <tr< td=""><td>Monthly Power Position for HBDR</td><td></td><td></td></tr<>	Monthly Power Position for HBDR		
10	Monthly Power Position for HBDR		
11	Monthly Power Position for HBDR		
12 13 14 15 14 15 10 10 10 10 10 10 10 10 10 10	Monthly Power Position for HBDR		
12 13 14 15 11 15 11 11 11 12 13 14 15 11 10 10 10 10 10 10 10 10 10	Monthly Power Position for HBDR		
13 14 15 15 11 15 11 15 11 14 15 10 11 10 11 10 10 11 10 10 10	Monthly Power Position for HBDR		
14 15 16 17 18 19 19 10 10 10 10 10 10 10 10 10 10	Monthly Power Position for HBDR		
13 11 12 13 13 14 15 17 16 16 17 16 16 16 16 16 16 16 16 16 16			
,7867.66,6 ↓ ACU683 ↓ ADD291 ↓ ADHOC ↓ ALL			
 ↓ ACU683 ↓ ADD291 ↓ ADHOC ↓ ALL 	e courreport or e mades		
 ADD291 ADHOC ALL 			
ADHOC			
ALL			
	Detail report - OTC Trades		
.BASKET	Static Data - FORMULAS		
💮 .ВООК			
.BRTEST	NAT GAS from trade type=ES - Swaps		
.CAP			
🚫 .СВАК	Power Deal Journal - Power Physicals		
🚫 .СВАК2	Power Deal Journal - Power Physicals		
CFLOW1	Pass 1 - Cash Flow Hedge Effectiven		
CFLOW2	Pass 2 - Cash Flow Hedge Effectiven		
	Summary Cash Flow Hedge Effective		
💭 .CPTY			
.CPTYUSR			
.DELTA			
11 I I I I I I I I I I I I I I I I I I	M ZAI*NET 05Nov03 Co		🛞 🏈 🔢 11:46 Pi
oc - Micr 🗨 ZAI*NET Application			
oc - Micr			v u 11.101
	CPTY CPTYUSR	Image: Second system CFLOW4 Cash Flow Hedge Effectiveness for F Image: CFLOW5 Summary Cash Flow Hedge Effective Image: CONTRACT CONTRACT Image: CPTY CPTYUSR Image: CPTA DELTA	.CFL0W4 Cash Flow Hedge Effectiveness for F .CFL0W5 Summary Cash Flow Hedge Effective .CH .CINTRACT .CPTY .CPTYUSR .DELTA

As part of GIAC practical repository.



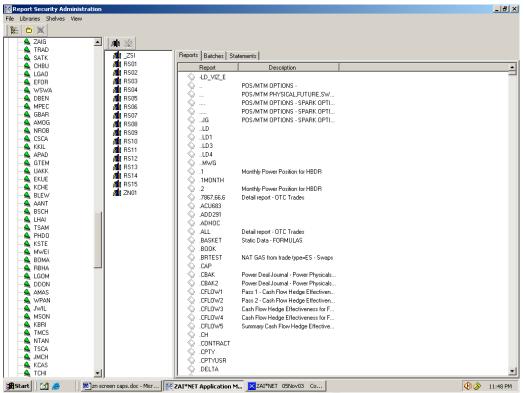


Figure 12

©SANS Institute 2003

As part of GIAC practical repository.

31

An Independent Auditor's Perspective

ZAI*NET 05Nov03 Connected to ZAINETA501:4000 File Edit Master Window Tools Run				<u>_</u> D×	[IX
		3 🛛 🗖				
🔀 Report Design: Column View						
Report Id U_AUDIT						
C# Sort Column	Heading	Type Axis	Detail Width	Prec Just		
1 0 CPTY	CPTY SHORT CODE	C COLUMN	YES 5	0 LEFT		
2 5 TNUM	TRADE TICKET NUMBER	C COLUMN		0 LEFT	- - ×	
3 0 TNUM XREF	TRADE REFERENCE	C COLUMN	YES 10	0 LEFT		
4 2 1CDY ATTR1	PRODUCT TYPE	C COLUMN	YES 10	0 LEFT		
5 0 1MC	PHYSICAL POINT OF DELIVERY	C COLUMN	YES 14	0 LEFT		
6 0 BOOK	BOOK	C COLUMN	YES 6	0 LEFT	I	
7 3 +1DMO	DELIVERY DATE	C COLUMN	YES 7	0 LEFT		
	eport Date Sort Heading		Function Group	Description Just		
ID U_AUDIT 05	NOV03 Notice	X				
C# 1 Sort 0 Sort By	Po you want to void/	delete this record?				
Column CPTY	Υ.					
	Capitalize Ci YES Yes	No				
		<u> </u>				
Condition	5 TRADE TICKET NUMBE	:R				
	6					
	7					
Axis	8					
Detail YES	9					
Width 5 0 Just LEFT	10					
	11					
Style DEPAGET	12					
viewing record						
Line migrooolia					111	
	ZAI*NET Application Man	05Nov03 C			🚯 🄗 11:54	PM
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."

As part of GIAC practical repository.

As part of GIAC practical repository.

ZAI*NET REPORTER	_ 8 ×
ZAI*NET REPORTER	▼②?"Normal ▼Times New Roman ▼ 12 ▼ B / U ■ 冨 冨 田 田 伊 伊 □ ▼▲ ▼ "
Report U_AUDIT as of 05N0V03 is running.	
Cancel	
1	
i	
► 2A1*NET 05Nov03 Connect File Edit Master Window Tool	i Run
-	
Reported U_AUDIT CH Soft Column	Heading Type Awar Detail width Piec Jour
1 0 CPTY 2 5 TNUM 3 0 TNUM/XPET	CPY Select CODE C COLLINY NS5 0 LEFT TPAGE TIOLET HANGER C COLLINY NS5 0 LEFT TAGGE REFERENCE C COLLINY NS5 10 0 LEFT
4 2 100VATE 5 0 1MC	PRODUCT TYPE C COLUMN YES 10 0 LEFT PHYSICAL POINT OF DELIVERY C COLUMN YES 14 0 LEFT
6 0 BDDK 7 3 +10MO	BODK C CDLUMM YES 6 0 LEFT PELMERY DATE C CDLUMM YES 7 0 LEFT
	Report Date Cue Heading Function Group Decogition Juar
CH Sort D	Sint By Do you want to vacijdelet tils record
- Column (PPY) - Heading (PPY SHORT CODE	Copider C Yes No
Candition	S TRACE TOXET NUMBER
Asis COLLMN	
Detail VES Wath 5 0 June LEFT	
Style DEFAULT	
- Viewing record	
:	some nac de . He. 19 201967 Accision No. 19 201967 a travel f
∭≋∞∞ [3] ∂ ∂ ∭∞ can delete	
	T T T T T T T T T T T T T T T T T T T
Page 15 Sec 1 15/19 At 5.5" Ln 2 Col 1	
	ZAI*NET Application Man ZAI*NET 05Nov03 Co ZAI*NET REPORTER
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.

©SANS Institute 2003

33 As part of GIAC practical repository.

Audit Step #3—Price Lockdown

PASS

Ensure that trade prices are locked down on a daily basis.

ate 60CT03		FUND	MONTH	QTR	YEAR	_ [
200200	TBALS NO	NO	NO	NO	NO	
70CT03	NO	NO	NO	NO	NO	
80CT03	NO	NO	NO	NO	NO	
90CT03	NO	NO	NO	NO	NO	
00CT03	NO	NO	NO	NO	NO	
10CT03	NO	NO	NO	NO	NO	
20CT03	NO	NO	NO	NO	NO	
30CT03	NO	NO	NO	NO	NO	
40CT03	NO	NO	NO	NO	NO	
50CT03	NO	NO	NO	NO	NO	
60CT03	NO	NO	NO	NO	NO	
70CT03	NO	NO	NO	NO	NO	
80CT03	NO	NO	NO	NO	NO	
90CT03	NO	NO	NO	NO	NO	
00CT03	NO	NO	NO	NO	NO	
10CT03	NO	NO	NO	NO	NO	
11NOV03	NO	NO	NO	NO	NO	
	NO	NO	NO	NO	NO	
I3NOV03	NO	NO	NO	NO	NO	
14NOV03	NO	NO	NO	NO	NO	

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.

≝ ⊠ X 0	۰ ک	
🗂 FRNT		-
🛱 RTRD		
ė 🖨 >		_
	🔍 AFAL	
	AROB	
	BDAG	
	BVAY	
	🕰 CDEC 🛳 CGON	
	EKRW	
	GGEI	
	GMOO	
	GRAD	
	👗 HTRI	
	🔦 JBUC	
	🛋 JCLA	
	🕰 JFUL	
	🕰 JGIL	
	🔦 JHOD	
	🕰 JNIG	
	🕰 KCLO	
	🔍 KRAG	
	ዿ LDSO	
	ALMAR	
	A MCHU	
	MERD	
	🔩 MMCA ዿ NMCD	
	PFRA	
	PZHA	
	A RAND	
	A RIVE	
	A RMAI	
	SCLA	
	SCRO	
	TZAD	
🛅 MID	-	
🛅 MGMT		
ADM		-
eady.		
🗚 Start 🔢 📶 🖉 🖆	🕽 💽 🛛 🔀 ZAI*NET Application M 🕒 Micros	soft PowerPoint - [P

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.

A 🗎			
ly Documents Patch Testing_files			
Ay Computer Patch Testing.htm			
	ZAIXNET		
My Network Zainett Places	Date 11/5/2003		
Recycle Bin ZAINET JAVA	Password m		
<i>6</i> ×			
Internet ZAINETT GREY Explorer			
itrix Program leighborhood			
Microsoft Excel			
Mirrosoft			
Microsoft Word			
Zainet scurity Pro			
俄Start 🛛 🚮 🚙 🚽 國]zn screen caps.doc - Micr.		🚱 🎓 11:14 PM	
Figure 17		,	
ZAI*NET (11/5/2003) File Settings Other Window Help			
Jser RTST connected to zaitest @ zainett B-C BACK-OFFICE CONFIGURATION			
Global Setup Global Setup Mapping Table Mapping Table Matchas Model Parameters Natural Gas Pipeline Meters Security Administration Time Zones Transmission/Transport Matrix Unit Conversion Rate Unit Conversion Rate DeAL ENTRY DeAL ENTRY DeAL ENTRY DeAL ENTRY DeAL ENTRY MID-OFFICE De MARKET PRICES De MID-OFFICE De MISK ANALYTICS	ZAI*NET Application Manager X Vou don't have permission to access that module. OK		
	J 🔣 ZAI*NET Application M	🛞 🖉 11:15 PM	
Figure 18			
Figure 17 and 18 sho	ow me logging in as a user who has bee	en placed in	the XPTE folde
	ccessfully) to access a submenu within		
	36		
SANS Institute 2003	As part of GIAC practical repository		Author retains full right

Audit Step #5—Reports

PASS

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

ZAI*NET 05Nov03 File Edit Master Window Tools RI	un	_ 8 ×					
Report Design: Column View		_ 🗆 🗵					
Report Id ias							
CH Report As_AGEDTRADE As_AGEDTRADE As_AGEDTRADE As_GETVLIST As_CPTVLIST As_CPTVLIST As_CPTVLIST AS_TADERNAMES ID CH Style CDLUMN CH CH CH CH CH CH CH CH CH C	THe The TRADE EXCEPTION REPORT (TRADE EXECUTED VS TRADE ENTERED) ZAINET DEALS DETAILS AUDIT REPORT INTERNAL AUDIT BOOK SECURITY REPORT APPROVED AND UNAPPROVED COUTERPARTY LIST COUNTERPARTY NAMES (SHORT & LONG) SORTED BY CPTY TYPES (BROKER, BANKS, CPTY INVOICE LOCKDOWN AND STAMPING REPORT INTERNAL AUDIT VALIDATION REPORT - DEAL ENTRY VS STAMPING TRADER NAMES MAPPED TO TRADER IDS OPNOV03 Grand ALL	Colum					
inserting record							
😹 Start 🛛 🖄 🥭 👘 🗍 🕅 zn scr	een caps.doc - Micr K ZAI*NET Application Man	🚯 🏈 12:03 AM					
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.

Rower Trade	es					
File Edit						
<u>AA</u> ► 03	Dec Jan Feb Mar 1 Trad					
Oct Nov	Dec Jan Feb Mar I IIau	e				
Void [≡] Book	Ticket Status E	Trade Entry Fixi	ing Option A	udit	Details Contract Memo	
RREA	AJQ287 🛛 😯 🕇 🖬	User Dai	te Ti	ime	Status 🔺	
		SHLE 7/9	1/2003 17	711		
		SKOZ 7/9	1/2003 17	23	0	
		AMOG 7/1	0/2003 84	11	00	As of User Date Stamp Time Stamp
					000	Created 7/9/2003 SHLE 7/9/2003 1711
			1/2003 10		0000	
		AMAS 7/1	1/2003 10	001	00080	Ancestor AJQ287 Source 0
						Parent Xkey 0
						Child1 Zkey 643201
						Child2
						Import JAVA BLOTTER
						Xstring View Xstring
	•					
•	Þ	<u> </u>				
	Run ▼	AJQ287 BF	REA	1) 5x16 West 7-22 🔹	ES
Ready	I					

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.

As part of GIAC practical repository.

Audit Step #7—Trader limit alerts

FAIL

Ensure that trader limits are set to alert appropriate personnel.

Category TRADER Name UCRO SubCategory Function Expiry Date Amount	Alf Ohm Lnum	
Category SubCategory Type TRADER " Funct	Line	
Name JCR0 Expiry D	Date	
Amo Refere		
inserting record		
Figure 21 ZAI*NET 270ct03 Connected to ZAINETAS01:4000 - [Limit Scr	reen]	_ D ×
🔀 File Edit Master Window Tools		
Category TRADER Name SSWA SubCategory	* SubName *	
Function Expiry Date Amount	Alf Ohm Lnum	
Category SubCategory	Line	
Type TRADER * Funct	tion	
Name ASWA Expiry D	Date	
Referen		
incorting record		
inserting record		
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 preestablished 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

ile Edit View				
11660				
Name	✓ Value			
APPI_HDAY	MINAS	•	Name	
UTOLIQACC	Y		CPTYAPP	
UTOLIQBK	Y		GINAN	
UTOLIQGP1	Y		r 🗗	1 %
UTOLIQGP2	Y			
UTOLIQGP3	Y		Gloc	
AUTOLIQHDG	Y			
AUTOLIQTOR	Y		Value: Y	
UTOSCHED	N		Yauc. I	
BASE_CCY	USD			
BIDMETHC	X			
BIZCHK	NO			
SIZCHK SKOFF_CONF	NO			
BOOKSECON	N			
BOOK_REQ	N			
BREAKDOWN	Y			
BRO_REQ	N			
CCRO	N			
ONTR	A2C4			
CNVGASUNTS	N			
COMSVR2ZS	N			
CONTACT	NO			
COPYTRADER	N			
CORS	N			
CPTYAPP	Y			
CPTYMSCHED	N			
CUST	N			
DATE_FMT	DDMMMYY			
DBSTATUS	G			
DBTYPE	ORACLE			
DEFINKT	PHLX			
DELIM	1			
DLT_CNTR	Y			
DSTHR25	A			
ERGLIB	C:\ZAINET\ERGLIB.DLL			
RGLIB1	C. ZAMET CHUED.DEE			
ERGLIB2				
INULIDZ			Ø	
•			N Contraction of the second se	
🔏 Start 🛛 🧭	8 🗍 🔍 ZAINET 6.3	<u></u>	Application security.doc	🛞 🌽 2:52 PM

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.

ZAI*NET (11/5/2003)							_ I I X
Power Trades							LO X
File Edit							
🛱 🕻 🚾 📾 🐼 🕲	0 Trades						
		000	@ () () @ () ()	~~~~~	マンショ		
/oid Book Ticket A Status	Trade Entry	Fixing Option Audit Deta	ils Contract Mem	0]			
	Physic Physic	al Buy @	FIRM (LD)				
		EST C	iply	Contact			
			LADO.	Loniaci	_	-	
		b	ACCU ACCU			_	
	_		ACE ACMC				
	Mon Ti		ACNP				
	Nov Dec J		AL ACSI ADAMS	4			
	12345	6 7 8 2 10 11 12 13 14 15 15 17	10 13 Z ADM	í		*	
	Amount	HW	/ HOUR		Total .00		
	Price:	USD	/ww	HOUR	Total .00		
	-1						
	-						
R	un • New	🗸 🗙 🥝 🗋 N	ew *	ES			
Ready							
E 🛅 FEAL-TIME							10
EISK ANALYTICS							
🏨 Start 🛛 🎦 🍎 🛛 😤 an s	creen caps.doc - Micr 🗮 🔀	AI*NET Application M.	ZAJ*NET OSNovO	a (🔄 🌛 12:10 AM

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.

Ma						
File Edit	es					
Oct Nov	v Dec Jan Feb Mar 1 Tra	de				
Void [≡] Book	🗏 Ticket Status E 🔺		Fixing Option	Audit	Details Contract Memo	
RREA	AJQ287 🛛 🕑 🗊 🕻 🖻 📃	 User 	Date	Time	Status 🔺	
		SHLE	7/9/2003	1711		
		SKOZ	7/9/2003	1723	0	
		AMOG	7/10/2003	841	00	As of User Date Stamp Time Stamp
		AMAS	7/11/2003	1001	000	Created 7/9/2003 SHLE 7/9/2003 1711
		AMAS	7/11/2003	1001	0100	
		AMAS	7/11/2003	1001	01080	Ancestor AJQ287 Source 0
						Parent Xkey 0
						Child1 Zkey 643201
						Child2
						lucat
						Import Source JAVA BLOTTER
						Xstring View Xstring
	-					
•	Þ				•	
	Run 🔻	AJQ287	RREA	8) 5x16 West 7-22 🔹	ES
Ready						
Keady	•					

Figure 25

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

As part of GIAC practical repository.

Auditing SunGuard Zai*net An Independent

Audit Step #10—New GUI Passwords

FAIL

Password complexity settings are compliant with Corporate Standards.

🔀 Global S	etup			_ 8
File Edit				
1266				
Name	Value	Name		
PW LEN	1	Name		
USR CHG	9999	PW LEN		
SHM POWF	1000			
SHM NET	1000			
SHM LNET	1000			
SHM DELT#		Gloi		
SHM NRTO:				
RT RERCON		Value: 1		
DB_STATU:				
VERSION	603			
PW CHG	3			
TIB_STATU				
FEA ITER	30			
BENCHMAF				
SCHEDPH	1536			
DEHCSTR	110869			
RCOMP	65000			
SHM ZMGN				
SHM RCOM				
SHM IBD	1000			
SHM PAIRB				
FONTSIZE	8			
RT TIME	5			
BUILD	2742			
MSG INTER				
SSL_STATU				
SHM NETCI PRCPOW	1000 1152			
SCHEDPP	1152			
NETA ACLA				
NETA GATE				
RPRC	15000			
ZRSETTLE	0			
MESHPOIN	50			
OPTD2M_S				
SCHEDROL				
PSTCORRIE				
MEMO_LEN				
Start] 🖸 🥭	Application security.doc 🔣 ZAI*NET Application M	()	2:47 PM

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 Sel ile Edit Vi			_ @
1166	N 10 10		
	Value		
W LEN	1	Name	
SR CHG	9999	PW CHG	
HM POWF	1000		
HM NET	1000		
HM LNET	1000		
HM DELT/	1000	Gloi	
HM NRTO:	1000		
T RERCOL	1	Value: 3	
B_STATU:	0		
ERSION	603		
w Chg 📋	3		
B_STATU	0		
EAITER	30		
ENCHMAF	3		
CHEDPH	1536		
EHCSTR	110869		
COMP	65000		
HM ZMGN	10		
IM RCOM	1000		
HM IBD	1000	-	
HM PAIRB	10		
ONTSIZE	8		
T TIME	5		
UILD	2742		
SG INTER	10		
SL_STATU	0		
HM NETC(1000		
RCPOW	1152		
CHEDPP	1536		
ETA ACLA	15		
ETA GATE	210		
PRC	15000		
RSETTLE	0		
ESHPOIN'	50		
PTD2M_S	48		
CHEDROL	0		
STCORRIE	-1		
EMO_LEN	4000	- I N	
n a . III	-		
Start	יין 🧶 🖸 סיי בי	Application security.doc K 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.

As part of GIAC practical repository.

Global Setup					_ 8 >
ile Edit View					
1 C 🗗 🔌	I I I I I I I I I I I I I I I I I I I				
lame 🤊	Value				
HEO_EDGE	YES		Name		
IME	@RMEXQV\		V0ID_PW		
LMFLOAT2	YES				
OLCHKOP	N		9		
POWCCYDFT	Y				
POWHDYDFT	YES		Gloc		
POWREPL	N				
RANS_MOVE	A		Value: N		
RDNEGAMT	N				
RDNOPRC	Y				
RMATRIX	N				
SECNEON	N				
UEDDETECT	N				
YPEAHEAD	N				
KPX	N				
KPX CASC	PARTIAL				
NITCNV	N				
PLTRDTFCS	SCN_TFC_STD				
PL_DT_FMT	NOTDEFIND				
SER_LOG	Y				
ERSION	4.00				
DID_PW	N				
DL_MKT	PHLX				
DL_SMILE	0				
ARNING	NO				
CLAUSE	Y				
IN_PRINT	Y				
OLLA	Y				
MLRETURN	0				
OPTFUTCOM	N				
ESTERDAY	X/NYMEX/NG				
EROPREM	Y				
GRIDID	CAMINUS				
NUP_STAT	OK				
R PMETH	1				
RSPLITRTC	W				
RSPLITTPS	Y				
			0		1 %
			N		
🛱 Start 📗 🚮	S ZAINET 6.3	[@1	pplication security.doc K ZAI*NET Application M	()	2:53 PM
					210011

Figure 28

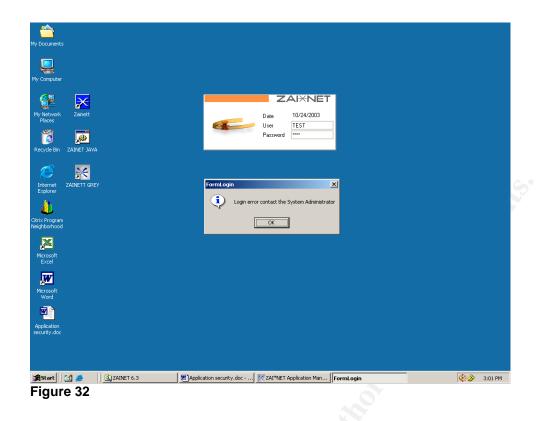
Figures 29-32 show the testing process of creating a "test" ID with only a 7 character password, which was allowed, as well as attempting to login with 3 bad passwords.

Jser ADT1 connected to zaitest @ zainett		
ACK FICE CONFIGURATION Seds Construints Construint Con	Security Administration The View Rooms Users The ONLY The ONLY	
∰व्यस्] ⊠ .≜ । । ⊠व्याप्रधा Figure 29	Pandy.	
	46	

An Independent Auditor's Perspective

Three "bad" login attempts

<complex-block></complex-block>	My Documents Wy Computer My Computer My Documents My Computer My Documents My Documents My Computer My Documents My Documents My Documents My Computer My Documents My Documents My Documents Zenett My Documents Zenett Schriefter Recordt Schriefter Recordt Recordt Recordt Zenett Recordt Recordt Recordt Recordt Recordt Recordt <th>Date 10/24/2003 User TEST Password TST Trynkid user or password Trynkid user or password Trynkid user or password Trynkid user or password</th> <th></th> <th></th>	Date 10/24/2003 User TEST Password TST Trynkid user or password Trynkid user or password Trynkid user or password Trynkid user or password		
<complex-block> Vry Concurrent Vry</complex-block>	Application security.doc	图]Application security.doc 至己 ZAITNET Application Man FormLogin	🕀 🏈 2:58 PM	
Application security.doc Restart M. Restart M. Restart Application security.doc Restart Application Man FormLogin	Hy Documents My Computer My Computer My Network Places Recycle Bin ZAINETT GREY Chitric Program Chitric Program Chitric Program Chitric Program Chitric Program Chitric Program	Dale 10/24/2003 User Password		
©SANS Institute 2003 As part of GIAC practical repository. Author retains full right	Application security.doc	47		Author retains full rights.



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		
	©SANS Institute 2003	As part of GIAC practical repository.	Author retains full rights.
© S	ANS Institute 2003,	As part of GIAC practical repository.	Author retains full rights.

Overall, the system is auditable with a consolidation of best practices into 20 welldefined 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 <u>ability</u> 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

©SANS	Institute	2003

An Independent Auditor's Perspective

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, <u>http://www.sans.org/rr/paper.php?id=842</u>, November 12, 2002.
- Jay Hollander, "What is a "Source-Code Escrow Agreement"?" Gigalaw.com, <u>http://www.gigalaw.com/articles/2000-all/hollander-2000-08-all.html</u>, August 2000.

Audit Checklists

- Dan Holt, "Auditing Microsoft Exchange 2000, An Administrator's Perspective," <u>http://www.giac.org/practical/GSNA/Dan_Holt_GSNA.pdf</u>.
- Paul Hugenberg, "Application IT System Audit," <u>http://www.auditnet.org/docs/ApplicationITSystemsAudit.doc</u>.
- 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, <u>Track 7 Auditing Networks</u>, Perimeters and Systems, The SANS Institute, 2003.