Global Information Assurance Certification Paper

Security Audit of an Oracle 8.1.7 Database Server: An Independent Auditor's Perspective

This paper is submitted to fulfill the requirements of the
Auditing Networks, Perimeters, and Systems GSNA Practical Assignment
Version 2.1, Option 1.

Prepared By: Steven Kallio, Jr.
Submitted In: December 2003
Location: SANSFire Washington D.C. July 2003
Track: 7 Auditing Networks, Perimeters and Systems

Table of Contents

Introduction

Purpose
The purpose of this paper is to fulfill the practical requirement of the GIAC Systems and Network Auditor (GSNA) certification.

Scope
This paper will walk through the steps / processes that were completed to perform an audit of an Oracle 8.1.7 database running on HP Tru64. The steps involved include: identifying the system to be audited, assessing the risks that the system is exposed to, researching the current state of auditing for an Oracle database, developing an audit checklist, executing the audit, and generating an audit report.

1 Research in Audit, Measurement Practice, and Control

1.1 System Identification

The Oracle database server to be audited throughout this paper (DBSRV1) is used by a small retail operation; SJK Corporation (SJK) located in Denver, Colorado. The databases stored on this server provide a number of different functions, to include: accounting, payroll, inventory management, timekeeping, and sales information.

All systems at SJK are required to pass a certification process prior to going into production. In addition, periodic security assessments are performed for all systems on an annual basis. Systems must also be reviewed for security considerations as part of the change management process. The audit for DBSRV1 is part of a periodic security assessment for all database (DB) servers.

1.2 System Details

1.2.1 Hardware

Compaq (HP) AlphaServer ES40

1.2.2 Software

HP Tru64 5.1A
Oracle 8.1.7

1.2.3 Location

The database server is located in the computer room on the third floor of SJK headquarters building in the Denver Technology Center. The computer room has a cardkey access system that limits access to authorized personnel only. Within the computer room, the database server is located in a rack that has a

physical key lock with only limited access to the key. This audit will not take into consideration any physical security requirements or environmental controls. It is assumed that these are adequate within the data center. It is also assumed that redundant power and telecommunications lines are in place.

1.2.4 Network Diagram:

The database server is on a network that is composed of only database servers. The database network is segmented from all other networks by a Symantec Enterprise Firewall with multiple interface cards. Connections to the database server must go through the firewall. An audit of the network configuration and firewall is not part of this assessment. Figure 1 is a graphical representation of the network architecture.

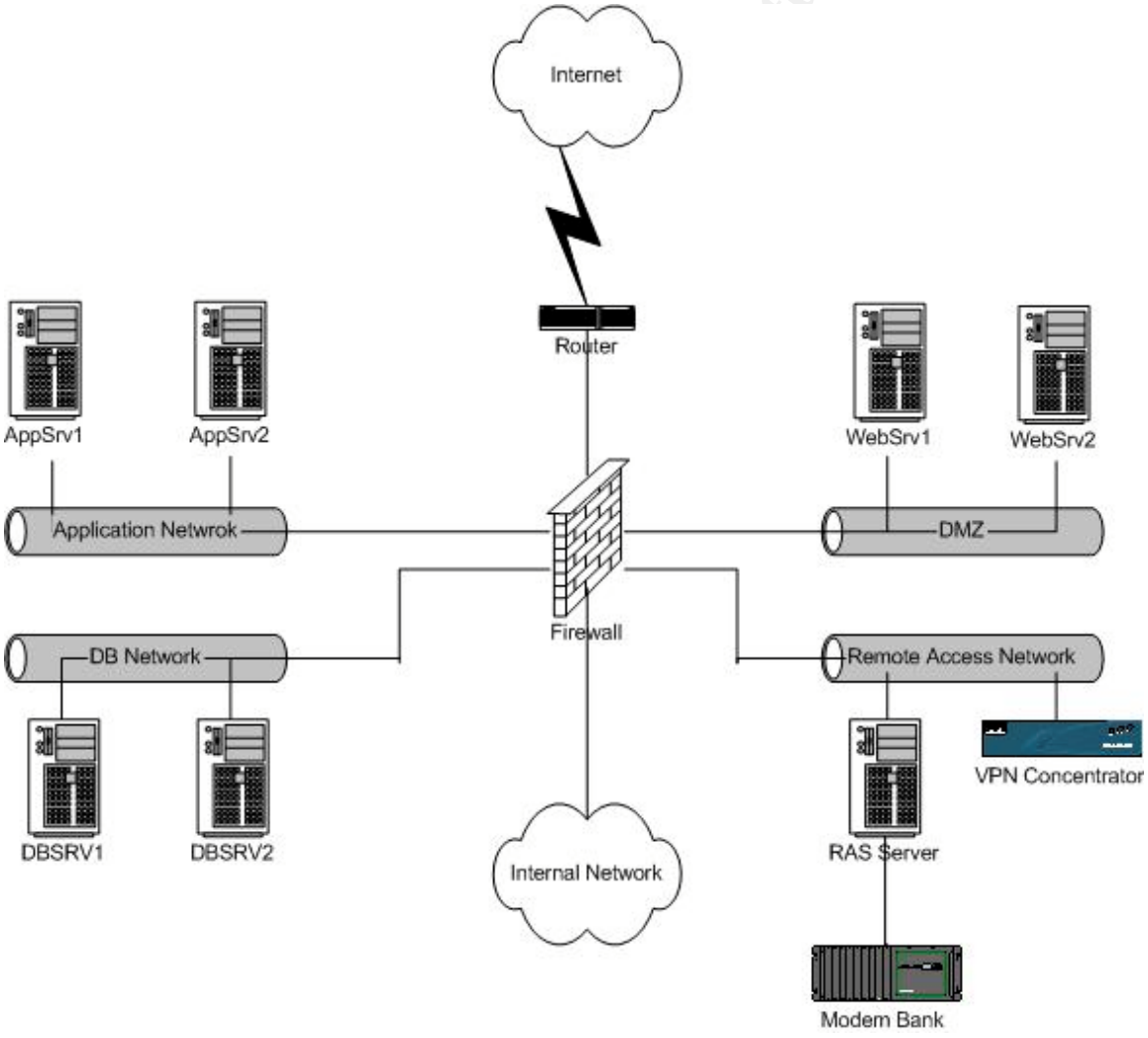

Figure 1: SJK Network Diagram

1.2.5 System Users and Communication Methods:

The database server is used by SJK employees located in the headquarters' building and point-of-sale applications (POS) in the retail stores. SJK employees' located in the headquarters' building access the database through custom developed Oracle forms applications using the local area network (LAN) and / or remote access connections (modem or VPN). Access from the retail stores is provided via a virtual private network (VPN) connection across the Internet. This audit is focused on the database server (DBSRV1) and will not include an audit of the applications, systems and networks located at the stores, nor will it include any other applications, servers, workstations, VPN concentrators, or networks that are located at SJK headquarters.

1.3 Risk Evaluation

The data stored within the individual databases on DBSRV1 vary in sensitivity from Low to High. While some of the information is considered "Public" knowledge, other information must be held "Strictly Confidential". As mentioned previously, this audit is part of a periodic security assessment of the DB server environment. Due to the information stored on DBSRV1, the server has been identified as being crucial to the business and therefore the overall risk level of the system has been evaluated as High.

In evaluating the risks that the database server is exposed to, potential vulnerabilities and the likelihood of their occurrence were analyzed to determine what the exposure would be and the level of severity of the exposure should it occur. The exposure can be a loss of one or more of the following:

- Confidentiality: Information can be / has been exposed to individuals without a need-to-know.
- Integrity: Information can be / has been modified and therefore cannot be verified or trusted to be accurate.
- Availability: Information is / may not be available when it is needed.

The severity level for the individual risks is a subjective measurement that takes into consideration each vulnerability, its' likelihood, and the exposure to the business.

Table 1 provides an evaluation of risks for DBSRV1. The list that is provided in Table 1 is not intended to be a complete risk assessment for DBSRV1 due to the limited scope of this audit. For example, the risk matrix does not include an item for SQL Injection Attacks that could expose the Confidentiality, Integrity, and Availability of the data in the database. The reason for this is that we are auditing the database itself and not the applications that are accessing it.

Risk #	Risk Evaluation	Exposure			Severity Level (High, Medium, Low)
		Confidentiality	Integrity	Availability	
1.3.1	A component of the servers' hardware goes bad and needs to be replaced. This could result in a complete loss of data. While the hardware has proven to be stable over the past couple of years, it is possible for a failure to occur at any time.	A			High
1.3.2	An unauthorized user obtains full control over the database server executables. This could result in a complete compromise of the data. The likelihood of this happening is low due to the: hardened operating system, segmentation of the network, limited number of operating system users, and file integrity monitoring software used.	CIA			Low
1.3.3	An unauthorized user obtains full control over the database files. This could result in a complete compromise of the data. The likelihood of this happening is low due to the: hardened operating system, segmentation of the network, limited number of operating system users, and file integrity monitoring software used.	CIA			Low
1.3.4	An unauthorized user obtains access to the database using default accounts and passwords. The level of access provided would be dependent on the account used. The likelihood of this happening is low due to the system certification process that a system must pass prior to being placed into production. The process requires all default user accounts to be deleted if they are not used, and the password changed on all accounts that are required.	CIA			Low

Risk #	Risk Evaluation	Exposure			Severity Level (High, Medium, Low)
		Confidentiality	Integrity	Availability	
1.3.5	Authorized database users share their passwords. It is likely that a percentage of users will share their passwords with one another, however the level of access provided would be dependent on the specific accounts shared.	CIA			Medium
1.3.6	The database listener is not configured securely. Improper listener configuration could lead to the database being unavailable. The likelihood of this happening is low due to the system certification process. This process requires a number of security configuration options be implemented for the listener.	A			Low
1.3.7	An unauthorized user is granted access to data they do not have a need-to-know. The severity of the risk depends on the level of information accessed. This is likely to happen due to the distributed administration provided to specific application owners, however an individual application administrator can only provide access to their application.	CIA			Medium
1.3.8	An unauthorized user gains access to the database by being able to perform a password guessing attack. The severity of this compromise depends on the account accessed. The likelihood of this happening is low due to the setting that locks out accounts after three failed logins.	CIA			Low

Risk #	Risk Evaluation	Exposure			Severity Level (High, Medium, Low)
		Confidentiality	Integrity	Availability	
1.3.9	A user inappropriately has the privilege to "SELECT ANY TABLE". This could lead to a full compromise of the data should the user become aware of these privileges. The likelihood of this happening is low due to the periodic review for these privileges by the database administrator. In addition, most users are not provided access (e.g. SQLPlus, ODBC Connections, etc) to the database outside of the Oracle forms applications.	CIA			Low
1.3.10	A user account exists in the database that has not been authorized appropriately. The severity depends on the permissions "roles" that have been granted to the account. This is likely to happen due to the number of people with the ability to create accounts, and the informal account creation procedures.	CIA			Medium
1.3.11	A database administrator makes an error and "accidentally" drops tables from the database that are still required. The likelihood of this happening is moderate given the number and training level of DBAs.	A			High

Table 1: Risk Evaluation

1.4 Current State of Oracle Audit Practices

To evaluate the current state of Oracle "security" audit practices available, I performed a thorough Internet search using many different combinations of related words (e.g. Oracle security audit, Oracle best practices, Oracle audit checklist, Oracle security guide). There is a considerable amount of information available related to securing Oracle databases, some are version specific, but I did not find many documents related to performing an Oracle Security Audit. The quality and detail of documents reviewed varied widely. A complete list of documents reviewed can be found in the References section of this report. Some of the documents were brief and only touched on one aspect of Oracle

security, while others provided an extensive amount of information on a number of topics. Below are the documents I found to be most valuable and a brief description of each.

- Oracle Database Listener Security Guide. Downloaded from http://www.integrigy.com/info/Integrigy_OracleDB_Listener_Security.pdf on December 15, 2003.
  - This paper "outlines the vulnerabilities in the Oracle TNS Listener and provide recommendations for properly securing it." (Oracle Database Listener Security Guide, p. 4)

- Oracle Database Security Benchmark v1.0. Downloaded from http://www.cisecurity.org/tools2/Oracle/OracleBenchmark.pdf on December 17, 2003.
  - "This guide provides high-level recommendations to secure an Oracle database." (Oracle Database Security Benchmark v1.0, p. 6)

- Exploiting and Protecting Oracle. Downloaded from http://www.pentest.co.uk/documents/Oracle-security.pdf on December 15, 2003.
  - "This paper attempts to cover the major security aspects of an Oracle RDBMS and applications installation, highlighting where there could be security issues." (Finnigan, p. 2)

In addition to the documents related to Oracle security, I found a few web sites that I felt were most valuable and should be shared with the audience of this paper. These were:

- http://www.auditnet.org
  - This web site provides an enormous amount of information for auditors (both financial and technical), including audit programs for a wide variety of systems.

- http://www.petefinnigan.com/orasec.htm
  - This web site provides links to a number of different resources about Oracle security, in addition to the papers written by Pete Finnigan himself. I would say this is the portal for Oracle security.

- http://www.securityfocus.com
  - This web site provides a wealth of knowledge related to information security. It has sections dedicated to security related news, vulnerabilities, viruses, security advisories, security books, and security tools.

2. Audit Checklist

This audit checklist has been developed in order to perform an audit of DBSRV1, an Oracle 8.1.7 database server used by SJK. In developing this checklist numerous white papers, security configuration guides, and other audit checklists were reviewed, but not all of the items in these documents were determined to be relevant for the audit of this database. As a result, this checklist could be used to perform an audit of other database servers, but it may need to be supplemented with additional checklist items. This checklist does not include items for performing an audit of the underlying Operating System (Tru64), but it does include some Oracle specific items that will need to be performed at the operating system level.

The checklist items have been divided up into two control categories, Policy and Procedure and Technical.

Within each category there are a number of different items. Each checklist item has the following details:

- Checklist # and Control Title = For referencing purposes. Number followed by a short description of the control.
- Control Objective = An explanation of what the control is expected to achieve.
- References = List of where the control objective was found.
- Objective / Subjective = Whether the control is based on hard evidence or judgement calls.
- Risk = A description of the potential threats, likelihood of occurrence and consequences to DBSRV1 should the control not be implemented.
- Risk Level = Level of risk to DBSRV1 based on a subjective analysis of the risk description. (High, Medium, or Low)
- Compliance Criteria = Details how to determine if a control passes or fails.
- Audit Procedure = Provides the steps (commands) to perform to obtain the information needed to make the compliance (pass / fail) decision. The convention used for the commands that need to be run is *10-point italics*.

2.1 Policy and Procedures

2.1.1 Change Management	
Control Objective	This control objective is designed to ensure that changes to the database in the production environment are performed in a controlled and consistent manner. To perform these changes in a consistent manner, change management procedures need to be documented and available to all database administrators.

References	♦ Personal Knowledge ♦ Newallis, p. 10. ♦ "Oracle Database Security Benchmark v1.0", p. 29.	Objective / Subjective	Subjective
Risk	Should change management procedures not exist, the DB may become unavailable or have degraded performance due to inconsistencies in the testing and change management process. If a documented policy does not exist, it is highly likely that a change will be made in the production environment without following the appropriate procedures.	Risk Level	Medium
Compliance Criteria	Having a documented change management policy and the associated procedures is objective, deciding that the policy and procedures are adequate (Whether they cover all the relevant areas of change management.) is subjective. Because this is an audit of Oracle and not the policies and procedures, the compliance criteria are subjective and will require the following to be true to obtain a "Pass" for this item: • A change management policy must exist. • Changes must be tested prior to being placed into production. • Changes and the test results need to be documented. • Changes must be approved.		
Audit Procedure	1. Obtain a copy of the change management policy from the DB administrator. 2. Obtain copies of completed change request documentation. 3. Review the documentation obtained to determine if it meets the compliance criteria.		

2.1.2 Oracle Security Baseline			
Control Objective	This control objective is designed to ensure that all Oracle DB servers are configured in a consistent and secure fashion.		
References	♦ Personal Knowledge	Objective / Subjective	Objective
Risk	Failure to have a documented Oracle Security Baseline can lead to inconsistencies in the security configuration of Oracle DBs. Without a baseline, it is highly likely that the databases will be configured differently and without the appropriate security controls in place.	Risk Level	High

Compliance Criteria	Having a documented Oracle Security Baseline is objective, deciding that it is adequate (Whether they cover all the relevant areas of Oracle Security.) is subjective. Because this is an audit of Oracle and not the baseline, the compliance criteria will be objective based on whether or not a baseline exists. At the conclusion of the audit we will be able to determine if the baseline was adequate or not. Pass = Oracle Security Baseline exists. Fail = Oracle Security Baseline does not exist.
Audit Procedure	1. Obtain a copy of the Oracle Security Baseline.

2.1.3 Patch Management			
Control Objective	This control objective is designed to ensure that a patch management process has been implemented at SJK.		
References	♦ Personal Knowledge ♦ "Oracle Database Security Benchmark v1.0", p. 7, 25.	Objective / Subjective	Subjective
Risk	Failure to document and follow appropriate patch management procedures could lead to the Oracle DB being exposed to a security vulnerability due to a patch not being installed on the system in a timely manner. It is highly likely that a patch will be released and not be installed in a timely manner if patch management procedures are not followed.	Risk Level	High
Compliance Criteria	Having patch management procedures is objective, deciding that they are adequate (Whether they cover all the relevant areas of patch management.) is subjective. Because this is an audit of Oracle and not the procedures, the compliance criteria are subjective and will require the following to be true to obtain a "Pass" for this item: • Vendor patch releases will be monitored for new patches. • Patches should be evaluated to determine if they relevant to the SJK database environment. • Patches should be tested prior to being installed in production. • Systems shall be reviewed periodically to ensure they have the appropriate patches installed.		

Audit Procedure	1. Obtain a copy of the patch management procedures. 2. If documented procedures do not exist, interview the database administrator to determine the informal procedures being followed (if any). 3. Review the documented and informal procedures to determine if they meet the compliance criteria.

2.1.4 Account Creation / Termination			
Control Objective	This control objective is designed to ensure that account creation and termination procedures have been implemented.		
References	♦ Personal Knowledge ♦ Newallis, p. 7. ♦ "Oracle Database Security Benchmark v1.0", p. 28.	Objective / Subjective	Subjective
Risk	Failure to document and implement account creation and termination procedures could lead to unauthorized access to the Oracle DB. There is a good chance that an account will be left on the system if termination procedures do not exist. It is also likely that accounts will be created for users who don't have a need-to-know if account creation procedures do not exist.	Risk Level	High
Compliance Criteria	Having documented account creation and termination procedures is objective, deciding that they are adequate (Whether they cover all the relevant areas of account management.) is subjective. Because this is an audit of Oracle and not the policies and procedures, the compliance criteria are subjective and will require the following to be true to obtain a "Pass" for this item: • An account creation form must exist and be approved by an appropriate manager prior to account creation. • Termination procedures should include timely notification from Human Resources. • All accounts should be reviewed on a periodic basis.		
Audit Procedure	1. Obtain a copy of the documented account creation and termination procedures. 2. If documented procedures do not exist, interview the database administrator to determine the informal procedures being followed (if any). 3. Review the documented and informal procedures to determine if they meet the compliance criteria.		

2.1.5 Auditing / Logging / Monitoring			
Control Objective	This control objective is designed to ensure that auditing, logging and monitoring policies and procedures have been implemented.		
References	♦ Personal Knowledge	Objective / Subjective	Subjective
Risk	Failure to require auditing, logging, and monitoring can result in the lack of ability to identify and respond to security incidents. It is highly likely that auditing / logging / monitoring not be enabled or performed if there isn't a procedure stating its' requirement.	Risk Level	Medium

Compliance Criteria	Having auditing, logging, and monitoring procedures is objective, deciding that they are adequate (Whether they cover all the relevant areas.) is subjective. Because this is an audit of Oracle and not the policies and procedures, the compliance criteria are subjective and will require the following to be true to obtain a "Pass" for this item:
	• Auditing and logging is required to be enabled (at a minimum to log access attempts).
	• Log reviews are being performed on a periodic basis. The following logs need to be included in the review:
	  • Listener Logs
	  • Oracle Logs
	  • Operating System Logs		

Audit Procedure	1. Obtain a copy of the documented auditing, logging, and monitoring procedures. 2. If documented procedures do not exist, interview the database administrator to determine the informal procedures being followed (if any). 3. Review the documented and informal procedures to determine if they meet the compliance criteria.		

2.1.6 Backup Procedures			
Control Objective	This control objective is designed to ensure that backup procedures have been implemented.		
References	♦ Personal Knowledge ♦ Plusnina, p. 1, 13-15. ♦ "Oracle Audit Checklist", p. 1.	Objective / Subjective	Subjective

Risk	Failure to have adequate backup procedures can lead to a loss of information. Users frequently request information that they have deleted to be restored. In addition, DBAs have the permissions that allow them to drop tables from the database, sometimes accidentally. It is highly likely that backups not be performed if backup procedures are not implemented.	Risk Level	High
Compliance Criteria	Having backup procedures is objective, deciding that they are adequate (Whether they cover all the relevant areas.) is subjective. Because this is an audit of Oracle and not the policies and procedures, the compliance criteria are subjective and will require the following to be true to obtain a "Pass" for this item: • Backups must be performed on a schedule with at least one full backup weekly and nightly incremental backups. • Backups must include the database and operating system files. • Restore of backup tapes should be tested on a periodic basis.		
Audit Procedure	1. Obtain a copy of the documented backup procedures. 2. If documented procedures do not exist, interview the database administrator to determine the informal procedures being followed (if any). 3. Review the documented and informal procedures to determine if they meet the compliance criteria.		

2.1.7 Disaster Recovery Procedures			
Control Objective	This control objective is designed to ensure that disaster recovery procedures are documented, tested, and available to DB administrators.		
References	♦ Personal Knowledge ♦ Plusnina, p. 1, 13-15. ♦ "Oracle Database Security Benchmark v1.0", p. 29.	Objective / Subjective	Objective
Risk	Failure to have documented disaster recovery procedures could result in the inability to recover the database in the amount of time required to support the needs of the business. It is almost a certainty that people will not know (remember) the disaster recovery procedures if they are not documented.	Risk Level	Medium

Compliance Criteria	Having a documented Disaster Recovery Procedure is objective, deciding that it is adequate (Whether they cover all the relevant areas of Oracle Security.) is subjective. Because this is an audit of Oracle and not the disaster recovery procedures, the compliance criteria will be objective based on the following criteria: Pass = A Disaster Recovery document exists and has been tested in the previous 12 months. Fail = Any other scenario.
Audit Procedure	1. Obtain a copy of the documented disaster recovery procedures. 2. Obtain a copy of the most recent disaster recovery test results. 3. If documented test results do not exist, interview the database administrator to determine when the last test of the disaster recovery procedures was completed. 4. Review the documented procedures and test results to determine if they meet the compliance criteria.

2.1.8 Incident Response Procedures			
Control Objective	This control objective is designed to ensure that incident response procedures have been implemented.		
References	♦ Personal Knowledge	Objective / Subjective	Subjective
Risk	Failure to have documented incident response procedures can lead to an incident not being handled properly, potentially leading to further losses and / or lack of prosecution due to mishandled evidence. While it is highly likely that the appropriate procedures won't be followed if they aren't documented, it is not as likely that this will result in additional consequences.	Risk Level	Medium

Compliance Criteria	Having documented Incident Response procedures is objective, deciding that they are adequate (Whether they cover all the relevant areas of incident response.) is subjective. Because this is an audit of Oracle and not the incident response procedures, the compliance criteria will be objective based on the following criteria. Pass = Incident Response procedures have been documented. Fail = Incident response procedures have not been documented.
Audit Procedure	1. Obtain a copy of the incident response procedures.

2.1.9 Risk Assessment			
Control Objective	This control objective is designed to ensure that a risk assessment (including data classification) has been completed for the database server (DBSRV1).		
References	♦ Personal Knowledge ♦ Plusnina, p. 4	Objective / Subjective	Subjective
Risk	The results of the risk assessment should be used to guide the security architecture of the database environment. Failure to complete a risk assessment may create a situation where the data does not have the appropriate amount of security controls in place. For example, if the data is classified as high, it could be decided that encryption is a requirement. It is probable that the data wouldn't be secured appropriately if a risk assessment isn't completed.	Risk Level	Medium
Compliance Criteria	Having a completed risk assessment for DBSRV1 is objective, deciding that it was adequate is subjective. Because this is an audit of Oracle and not the risk assessment, the compliance criteria will be objective based on the following criteria. Pass = A risk assessment has been completed (and documented) for DBSRV1. Fail = A risk assessment has not been conducted (or documented).		
Audit Procedure	1. Obtain a copy of the risk assessment for DBSRV1.		

2.2 Technical

2.2.1 Access Controls

2.2.1.1 Authorization			
Control Objective	This control objective is designed to ensure that all the database user accounts have an account creation form completed for them.		
References	♦ Personal Knowledge ♦ "Oracle Audit Checklist", p. 1.	Objective / Subjective	Objective
Risk	If each of the accounts that exist in the database do not have a corresponding account creation form completed, the account creation procedures are not being followed. This could lead to an individual gaining access to information he/she does not have a need-to-know. In addition, the undocumented accounts could be evidence of a security incident. The probability that accounts exist without documentation is moderate in this environment.	Risk Level	Low
Compliance Criteria	There should be a one to one match of user accounts that exist in the database, and the documentation on file (could be electronic). Pass = All accounts have the appropriate documentation completed. Fail = User accounts exist that have not been documented.		
Audit Procedure	1. Obtain a list of all database user accounts by executing the following command via SQL*Plus: *select username from dba_users;* 2. Obtain all the account creation forms. 3. Depending on the number of accounts, select a sample to determine if all accounts have the appropriate documentation. (Note: If the list of users and the documentation is electronic it may be possible to compare all accounts in an efficient manner, instead of performing an audit of a sample).		

2.2.1.2 Default Accounts / Passwords	
Control Objective	This control objective is designed to ensure that all of the default accounts have been disabled / deleted if the account is not necessary, and that the password has been changed on all default accounts that are necessary.

References	♦ Personal Knowledge ♦ Plusnina, p. 9. ♦ Newallis, p. 7. ♦ "Oracle Audit Checklist", p. 1. ♦ Newman, p. 38. ♦ "Oracle Database Security Benchmark v1.0", p. 35.	Objective / Subjective	Objective
Risk	Leaving default accounts active and with default passwords provides an easy entry point for unauthorized access. It is highly likely that authorized users and attackers will attempt to log in to the database using the vendor supplied default accounts.	Risk Level	High
Compliance Criteria	A review of the database user accounts will determine if any vendor-supplied accounts are present. Once the list of vendor supplied accounts present has been determined, they can be reviewed to determine if the account is necessary, if it has been disabled, and if the password has been changed. Pass = If vendor supplied default accounts exist, they are either disabled, or do not have default passwords. Fail = Multiple scenarios. Examples below: 1. A vendor supplied default account is enabled, and the password is still set to the default. 2. If the default account is enabled and it is not necessary.		
Audit Procedure	1. Obtain a list of all database user accounts by executing the following command via SQL*Plus: *select username, password, profile from dba_users;* 2. Review the list of accounts to determine if any are vendor supplied. 3. For the vendor supplied accounts found in step 2, attempt to connect to the database with the default password (usually equals username). An extensive list of default username / password combinations can be found at: <http://www.cirt.net/cgi-bin/passwd.pl?method=showven&ven=Oracle>. Successful connections mean the default password has not been changed.		

2.2.1.3 Blank Passwords	
Control Objective	This control objective is designed to ensure that database accounts do not have blank passwords.

References	♦ Personal Knowledge	Objective / Subjective	Objective
Risk	Accounts with blank passwords provide an easy entry point into the database by unauthorized users. The level of exposure, should an account with blank password be exploited, is dependant on the permissions granted to the specific account. The likelihood of the account being found is moderate.	Risk Level	Medium
Compliance Criteria	Pass = No user accounts are found with blank passwords. Fail = At least one user account was found with a blank password.		
Audit Procedure	1. Execute the following command via SQL*Plus: select username, password from dba_users; 2. Review the password column to ensure that all users have a password assigned.		

2.2.1.4 Inactive Accounts			
Control Objective	This control objective is designed to ensure that database user accounts do not exist even though they are never used.		
References	♦ Personal Knowledge	Objective / Subjective	Objective
Risk	Accounts that are not needed provide an unnecessary entry point to the database. Should an inactive account be exploited, the level of exposure is dependent on the permissions granted to the specific account. The likelihood of an account being exploited is low provided the appropriate password controls are in place.	Risk Level	Low

Compliance Criteria	To comply with this item, a process needs to be in place to review database accounts for inactivity (not used for 60 days or more). In addition, a review of all database accounts must not find any that are enabled and not used for the past 60 days. Pass = Accounts are reviewed (manually or via tools) for inactivity duration. Accounts that have been inactive for 60 days are disabled / deleted. Fail = Inactive accounts are not reviewed. And / Or Fail = Inactive accounts are found enabled.
Audit Procedure	1. Ask the system administrator if there is a process in place to review inactive accounts. 2. Review a sample number of accounts for inactivity by checking the access log for each.

2.2.1.5 Shared Accounts			
Control Objective	This control objective is designed to ensure that user accounts are not shared.		
References	♦ Personal Knowledge ♦ Newallis, p. 7.	Objective / Subjective	Subjective
Risk	The use of shared accounts eliminates the ability to track the integrity of information, because there is no way to tell whom the last person to access the data was.	Risk Level	Medium
Compliance Criteria	Compliance will depend on interviews with DBAs and users to determine if accounts are being shared, which makes compliance subjective. Overall compliance will be binary based on the following: Pass: Accounts are being shared. Fail: No accounts are shared.		

Audit Procedure	1. Obtain a list of all database user accounts by executing the following command within SQL*Plus: *select username from dba_users;* 2. Review the output of the above statement for accounts that are not assigned to one particular individual (e.g. helpdesk, training, and test). 3. Ask the database administrator if the accounts found in step 2 are used by a group of individuals (e.g. shared password). 4. A log review can also be performed to determine if any user accounts are logging in from more than one terminal. Logging in from more than one terminal can be an indication of an account being shared. Obtain a list of accounts that have logged in from more than one terminal by executing the following within SQL*Plus. *select count(distinct(terminal)) Count, username* *from dba_audit_session* *having count(distinct(terminal))>1* *group by username;* 5. Review the output from step 4 to identify user accounts that appear to be shared by a number of users. 6. Interview the DBA and appropriate users to determine why an account is being used from more than one terminal.

2.2.1.6 "Public" Permissions			
Control Objective	This control objective is designed to ensure that the permissions granted to the user group "PUBLIC" are appropriate.		
References	♦ Personal Knowledge ♦ Newman, p. 38.	Objective / Subjective	Subjective
Risk	Permissions granted to the PUBLIC user group are provided to all database users because all database users are members of the PUBLIC user group. Permissions granted to PUBLIC should be limited to those that all users need to have. It is very likely that the permissions assigned to PUBLIC will be greater than necessary if they are not reviewed.	Risk Level	High

Compliance Criteria	Compliance will depend on the analysis of the permissions / roles / privileges granted to the PUBLIC user group. This review will need to be done in coordination with the DBA to determine what permissions are required of all users. Pass: The analysis has concluded that all permissions / roles / privileges granted to the PUBLIC user group are appropriate. Fail: PUBLIC has been granted permissions / roles / privileges that are not appropriate for all users to have. .
Audit Procedure	1. Obtain a list of all the objects where permissions have been granted to PUBLIC. *select table_name, privilege from dba_tab_privs where grantee='PUBLIC';* 2. Review the output of step 1 with the DBA to determine if the permissions are necessary for the PUBLIC user group. 3. Obtain a list of all roles that have been granted to PUBLIC. *select granted_role from dba_role_privs where grantee='PUBLIC';* 4. Review the output of step 3 with the DBA to determine if the roles are necessary for the PUBLIC user group. 5. Obtain a list of all system privileges that have been granted to PUBLIC. *select privilege from dba_sys_privs where grantee='PUBLIC';* 6. Review the output of step 3 with the DBA to determine if the roles are necessary for the PUBLIC user group.

2.2.1.7 Remote OS Authentication			
Control Objective	This control objective is designed to ensure that authentication via a remote Operating System is not trusted.		
References	♦ "Oracle Database Security Benchmark v1.0", p. 10, 35.	Objective / Subjective	Objective
Risk	An attacker could gain access to the database without having to supply a password. If this setting were enabled, the attacker would only need a valid username that is trusted for remote authentication. The likelihood of this happening is low due to the limited number of operating system users and the parameter having been checked during system certification.	Risk Level	Low

Compliance Criteria	This item either passes or fails compliance based on a binary setting of this parameter. Pass: remote_os_authent must be set equal to FALSE. Fail: remote_os_authent is set equal to TRUE.
Audit Procedure	1. Obtain a copy of the init.ora file from the database administrator. 2. Perform a find in the file for the parameter "remote_os_authent=". 3. Review the value assigned to the parameter to see if it meets the compliance criteria.

2.2.1.8 Password Settings			
Control Objective	This control objective is designed to ensure that database user accounts have password settings enforced upon them.		
References	♦ Personal Knowledge ♦ Newallis, p. 9. ♦ "Oracle Audit Checklist", p. 1. ♦ "Oracle Database Security Benchmark v1.0", p. 19-20, 36.	Objective / Subjective	Objective
Risk	Users will not follow password guidelines if they are not forced to comply via technical measures. The likelihood that users not change their password appropriately is almost a certainty.	Risk Level	High

Compliance Criteria	Password settings are made at the Profile level within oracle. For each database profile used, review for the following information. To PASS, all of the following must be true: • password_life_time must be < 60: This sets the parameter that controls how often a password must be changed. • password_reuse_max must be > 10: This parameter controls how many times a password must change before it can be reset to a previous password. • password_lock_time > 30: This parameter controls how long an account is locked if the number of failed logins is exceeded. • password_grace_time < 5: This parameter controls the number of days an account can be logged into after the password has expired. • password_verify_function = a valid function (meaning it is not null or unlimited): This parameter sets the function to be used when a password is being changed. The function identified verifies the composition of the password to ensure that weak passwords are not allowed.

Audit Procedure	1. Obtain a copy of the password_life_time setting for each profile by issuing the following statement within SQL*Plus: *select profile, limit from dba_profiles where resource_name='PASSWORD_LIFE_TIME';* 2. Review this setting against the compliance criteria 3. Obtain a copy of the password_reuse_max setting for each profile by issuing the following statement within SQL*Plus: *select profile, limit from dba_profiles where resource_name='PASSWORD_REUSE_MAX';* 4. Review this setting against the compliance criteria. 5. Obtain a copy of the password_lock_time setting for each profile by issuing the following statement within SQL*Plus: *select profile, limit from dba_profiles where resource_name='PASSWORD_LOCK_TIME';* 6. Review this setting against the compliance criteria. 7. Obtain a copy of the password_grace_time setting for each profile by issuing the following statement within SQL*Plus: *select profile, limit from dba_profiles where resource_name='PASSWORD_GRACE_TIME';* 8. Review this setting against the compliance criteria. 9. Obtain a copy of the password_verify_function setting for each profile by issuing the following statement within SQL*Plus: *select profile, limit from dba_profiles where resource_name='PASSWORD_VERIFY_FUNCTION';* 10. Review this setting against the compliance criteria.

2.2.1.9 Account Lockout			
Control Objective	This control objective is designed to ensure that database user accounts lockout after a specified number of failed login attempts.		
References	♦ Personal Knowledge ♦ "Oracle Database Security Benchmark v1.0", p. 19	Objective / Subjective	Objective
Risk	Failure to lockout accounts after a number of failed login attempts increases the chance that an account will be compromised due to a brute force password guessing attack. The likelihood of a password guessing attack is moderate. The impact of a compromise of this nature would depend on the permissions granted to the account that is compromised.	Risk Level	High

Compliance Criteria	Account lockout settings are made at the Profile level within Oracle. For each database profile used, review the failed login attempt parameter to ensure that it meets the following: This parameter can have a range of values assigned to it. Following SJK policy, the number of attempts shall be limited to 5 or less. This parameter needs to be verified for all profiles that are assigned to user accounts. PASS = failed_login_attempts ≤ 5 FAIL = failed_login_attempts > 5
Audit Procedure	1. Obtain a copy of the failed_login_attempts setting for each profile by issuing the following statement within SQL*Plus: *select profile, limit from dba_profiles where resource_name='FAILED_LOGIN_ATTEMPTS';* 2. Review this setting against the compliance criteria. 3. In addition to checking the setting, test to ensure that the setting is effective by attempting to login using an invalid password six times in a row. a. First display the account status for an account. b. Next attempt to connect as the account six times. c. Finally, display the account status again to show that the account is now locked.

2.2.2 Network Listener

2.2.2.1 Listener Patches			
Control Objective	This control objective is designed to ensure that all the security patches related to the Oracle TNS Listener have been applied.		
References	♦ Personal Knowledge ♦ "Oracle Database Listener Security Guide", p. 9-10.	Objective / Subjective	Objective
Risk	Failure to apply a security patch to the network listener could leave the system vulnerable to attack. The likelihood of an attacker attempting to exploit the listener using known vulnerabilities is high.	Risk Level	High

Compliance Criteria	This item either passes or fails compliance based on a binary setting of this parameter. Pass = All relevant patches have been applied. Fail = Not all patches have been applied.
Audit Procedure	1. Obtain a list of all Oracle security patches (from the Oracle web site) related to the network listener. 2. Obtain a list of all the Oracle security patches that have been installed on the server from the database administrator. 3. Compare the two lists to ensure that all relevant patches have been applied.

2.2.2.2 TNS Listener Password			
Control Objective	This control objective is designed to ensure that the Listener is password protected.		
References	♦ "Oracle Database Listener Security Guide", p. 7-9. ♦ Newman, p. 11.	Objective / Subjective	Objective
Risk	Failure to password protect the Oracle Listener provides anyone who can communicate with it the ability to create a denial of service to the database, as well as obtain detailed configuration information. The likelihood of anyone trying to exploit the listener is low due to the complexity of the attack and the filtering at the firewall.	Risk Level	Medium
Compliance Criteria	This item either passes or fails compliance based on a binary setting of this parameter. Pass = The TNS Listener requires a password. Fail = A password is not required.		

Audit Procedure	1. Obtain a copy of the listener.ora file off of DBSRV1 from the administrator. *cat /u01/app/oracle/product/8.1.7/network/admin/listener.ora* 2. Review the file for the parameter "PASSWORDS_LISTENER=". 3. Another way to check is to execute the tnscmd perl script and run the services command. *perl tnscmd services --indent -h dbsrv1* 4. Review the output of the tnscmd services command to determine if a password has been configured. Output will be limited if a password is required. 5. A third way to verify the password requirement is to execute the tnscmd perl script and run the status command. *perl tnscmd status --indent -h dbsrv1* *6.* Review the output of the script for the parameter SECURITY. If the value for this parameter is ON, a password has been set.

2.2.2.3 Listener Admin Restrictions			
Control Objective	This control objective is designed to ensure that changes to the listener cannot be made dynamically.		
References	♦ "Oracle Database Security Benchmark v1.0", p. 15.	Objective / Subjective	Objective
Risk	Without this parameter turned on, changes can be made to the listener settings without having to reload it. Exploiting this would be rather difficult and likelihood low since the listener is required to have a password.	Risk Level	Low
Compliance Criteria	This item either passes or fails compliance based on a binary setting of this parameter. Pass: admin_restrictions_*listener_name* must be set equal to "on". Fail: If admin_restrictions_*listener_name* is set equal to "off".		
Audit Procedure	1. Obtain a copy of the listener.ora file from the database administrator. 2. Perform a find in the file for the parameter "admin_restrictions_*listener_name*=". 3. Review the value assigned to the parameter to see if it meets the compliance criteria.		

2.2.2.4 Listener Audit Settings			
Control Objective	This control objective is designed to ensure that auditing has been enabled on the Oracle network listener.		
References	♦ "Oracle Database Listener Security Guide", p. 11,25.	Objective / Subjective	Objective
Risk	Failure to enable auditing on the network listener would make it difficult to identify and track down a security incident.	Risk Level	Medium
Compliance Criteria	This item either passes or fails compliance based on a binary setting of this parameter. Pass = Auditing is enabled and working (the log file has data in it). Fail = Auditing is not enabled.		
Audit Procedure	1. Obtain a copy of the listener.ora file from the database administrator. This file can be found in the "$ORACLE_HOME/network/admin/" directory. 2. Review the file for the "LOG_STATUS=ON" or "LOG_STATUS=OFF". 3. Review the contents of the listener log file. The location and name of the listener log file can be found in the listener.ora file. 4. Review the information obtained to see if the compliance criteria has been met.		

2.2.2.5 Unused Listener Services			
Control Objective	This control objective is designed to ensure that only necessary listener services are installed.		
References	♦ "Oracle Database Listener Security Guide", p. 13-14. ♦ Newman, p. 22. ♦ "Oracle Database Security Benchmark v1.0", p. 31.	Objective / Subjective	Subjective
Risk	"ExtProc (PLSExtProc) functionality allows external C and Java functions to be called from within PL/SQL." (Oracle Database Security Benchmark v1.0, p. 31).	Risk Level	Low

Compliance Criteria	Compliance of this item is subjective based on the analysis and determination made by the database administrator. Pass: ExtProc (PLSExtProc) is not started, or it is started and required. Fail: ExtProc (PLSExtProc) is started, but not required.
Audit Procedure	1. Obtain a copy of the listener.ora file from the database administrator. This file can be found in the "$ORACLE_HOME/network/admin/" directory. 2. Review the file for the services configured by looking for the lines with Service "ExtProc" or Service "PLSExtProc". 3. If either of these lines are found, ask the database administrator if the service is required as they are generally enabled by default.

2.2.2.6 Listener Ports			
Control Objective	This control objective is designed to ensure that the Oracle TNS listener is not running on the default ports of 1521 or 1526.		
References	♦ "Oracle Database Security Benchmark v1.0", p. 31.	Objective / Subjective	Objective
Risk	The default ports are well known by attackers. Running the listener on a non-default port will make it more difficult for an attacker to determine the location of critical database resources. The likelihood that an attacker would attempt to connect to the default port is high, but the risk of not changing the value from the default is low because a determined attacker would only be slowed down by this change.	Risk Level	Low
Compliance Criteria	This item either passes or fails compliance based on a binary setting of this parameter. Pass = The listener port is neither 1521 nor 1526. Fail = The listener port is 1521 or 1526.		

Audit Procedure	1. Obtain a copy of the listener.ora file off of DBSRV1 from the administrator. *cat /u01/app/oracle/product/8.1.7/network/admin/listener.ora* 2. Review the file for the listener port setting. 3. Run the tnscmd perl script and run the status command. *perl tnscmd status --indent -h dbsrv1* 4. Review the output of the script for the listener port. 5. Execute an nmap scan of the database server. *nmap -sS -O -p 1-65535 -v -oN dbsrv1.txt dbsrv1* 6. Review the output of the nmap scan to determine if the default listener port (1521) is used.

2.2.3 Tru64

2.2.3.1 Tru64 Patches			
Control Objective	This control objective is designed to ensure that all the Tru64 security related patches have been applied.		
References	♦ Personal Knowledge	Objective / Subjective	Objective
Risk	Failure to install security patches in a timely manner will leave the system exposed to a known vulnerability. The longer a system is exposed to a known vulnerability, the more likely an exploit for that vulnerability will be run against the system.	Risk Level	High
Compliance Criteria	This item either passes or fails compliance based on a binary setting of this parameter. Pass: All Tru64 security patches have been installed. Fail: At least one Tru64 security patch has not been installed.		
Audit Procedure	1. Obtain a list of all security patches that have been installed from the system administrator. 2. Obtain a list of all Tru64 security patches available from HP for the version of Tru64 installed. 3. Compare what is installed on the system to what is available.		

2.2.3.2 Tru64 Audit Settings			
Control Objective	This control objective is designed to ensure that auditing is enabled on Tru64 and that at a minimum logon and logoffs are being recorded.		
References	♦ Personal Knowledge	Objective / Subjective	Subjective

Risk	Failure to record audit data leads to the inability to identify and respond to security incidents.	Risk Level	Medium
Compliance Criteria	Compliance with this item is subjective because there is a wide array of potential audit requirements. For the purpose of this audit, the following criteria have been set: Pass: Auditing is enabled for at a minimum logon and logoff attempts. The audit log must be reviewed on a regular basis. Fail: Auditing is not enabled.		
Audit Procedure	1. Interview the system administrator and inquire if auditing is enabled. Also, ask what the procedures are for monitoring the logs. 2. Have the administrator display the current audit log as evidence.		

2.2.3.3 Oracle Account & Group			
Control Objective	This control objective is designed to ensure that only authorized personnel have access to the Oracle account and / or are members of the Oracle groups.		
References	♦ Personal Knowledge ♦ Plusnina, p. 8. ♦ "Oracle Database Security Benchmark v1.0", p. 26.	Objective / Subjective	Subjective
Risk	Having access to the Oracle account, or being a member of the Oracle group provides privileges to access files in the Oracle home directory and therefore sensitive information.	Risk Level	High
Compliance Criteria	Determining who has access to the Oracle account and who is a member of the Oracle group is objective. Deciding that they need that level of access is subjective. The following criteria will be used to base compliance for this item: Pass: Only authorized users are members of the Oracle DBA group and only authorized individuals know the Oracle account password. Fail: Any other scenario		

Audit Procedure	1. Obtain a copy of the Tru64 password file to get a list of user accounts on the system. (*cat /etc/passwd*) 2. Obtain a copy of the Tru64 group file from the system administrator. (*cat /etc/group*) 3. Review the files with the database administrator to determine that Oracle group membership is appropriate. 4. Ask the DBA to tell you who knows the Oracle password. 5. Review the people who know the Oracle password and decide if they have a need-to-know.

2.2.3.4 Database file permissions.			
Control Objective	This control objective is designed to ensure that the Oracle database files have the appropriate file permissions. This should include reviewing the Oracle home directory, Oracle temporary directories and all of their subdirectories and files.		
References	♦ Personal Knowledge ♦ Plusnina, p. 7 ♦ "Oracle Database Listener Security Guide", p. 13. ♦ Newman, p. 11. ♦ "Oracle Database Security Benchmark v1.0", p. 9,13.	Objective / Subjective	Subjective
Risk	Access to Oracle files should be controlled to prevent an unauthorized user from gaining access to sensitive information. Due to the limited number of operating system users, the likelihood of someone gaining access to any Oracle files is limited.	Risk Level	Low
Compliance Criteria	Compliance with this item is subjective based on the analysis performed with the system and database administrators. Pass: The administrators determine that the Oracle file permissions are appropriate. Fail: File permissions are not appropriate.		
Audit Procedure	1. Obtain a list of all Oracle related files (showing the file permissions) from the system administrator. 2. Review the list of files with the system and database administrators to determine that the permissions are appropriate.		

2.2.3.5 Database File Integrity			
Control Objective	This control objective is designed to ensure that file integrity monitoring is in place for the Oracle installation. This should include reviewing Oracle scripts and executables in the Oracle home directory.		
References	♦ Personal Knowledge	Objective / Subjective	Objective
Risk	Changes to Oracle executables and scripts can be indication that the system has been penetrated and the files replaced with Trojaned versions. The likelihood of this happening is low due to the limited number of users who can log into the operating system.	Risk Level	Low
Compliance Criteria	File integrity monitoring needs to be in place, this can be either a manual process or automated tool. The automated tool option is preferred. Pass: File integrity software (e.g. Tripwire) is configured to monitor the integrity of database executables and scripts. Pass: A manual process is in place to monitor the integrity of database executables and scripts on a regular basis. Fail: File integrity monitoring is not being completed.		
Audit Procedure	1. Interview the database administrator (system administrator) to determine if file integrity is being monitored, and if so is being completed through a manual process or an automated tool. 2. Obtain documented procedures from the DBA that describes the process / tool being used and which database files are being monitored.		

2.2.4 Oracle

2.2.4.1 Oracle Patches			
Control Objective	This control objective is designed to ensure that Oracle related security patches are installed on the system.		
References	♦ Personal Knowledge ♦ "Oracle Database Security Benchmark v1.0", p. 7.	Objective / Subjective	Objective

Risk	Failure to install security patches in a timely manner will leave the system exposed to a known vulnerability. The longer a system is exposed to a known vulnerability, the more likely an exploit for that vulnerability will be run against the system.	Risk Level	High
Compliance Criteria	This item either passes or fails compliance based on a binary setting of this parameter. Pass: All relevant Oracle security patches have been installed. Fail: At least one relevant Oracle security patch has not been installed.		
Audit Procedure	1. Obtain a list of all security patches that have been installed from the database administrator. 2. Obtain a list of all Oracle security patches available that are relevant to Oracle version 8.1.7. 3. Compare what is installed on the system to what is available.		

2.2.4.2 Oracle Audit Settings			
Control Objective	This control objective is designed to ensure that Oracle auditing has been enabled for a predetermined set of events.		
References	♦ Personal Knowledge ♦ Finnigan, Pete. "Introduction to Simple Oracle Auditing", p. 4	Objective / Subjective	Objective
Risk	Failure to record audit data leads to the inability to identify and respond to security incidents.	Risk Level	Medium

Compliance Criteria	Check the audit settings to determine that the following are being audited: • ALTER USER • Any CREATE statement. • Any DROP statement. • GRANT ANY PRIVILEGE • GRANT ANY ROLE • INSERT failures • LOGON and LOGOFF Pass: Auditing is enabled and configured to record at a minimum the above events. Fail: Auditing is not enabled, or does not record the minimum events above.
Audit Procedure	1. Obtain a copy of the init.ora file from the DBA. 2. Review the file for the parameter, audit_trail =, to determine if auditing is enabled. 3. Another check to see if auditing is enabled would be to execute the following within SQL*Plus: *select name, value from v$parameter where name like 'audit%';* 4. Next, check to see what privilege audit options are enabled by executing the following within SQL*Plus: *select * from dba_priv_audit_opts;* 5. Check to see what statement audit options are enabled by executing the following within SQL*Plus: *select * from dba_stmt_audit_opts;*

2.2.4.3 Database Link Settings			
Control Objective	This control objective is designed to ensure that database links do not have usernames and passwords stored.		
References	♦ Personal Knowledge ♦ "Oracle Audit Checklist", p. 1. ♦ "Oracle Database Security Benchmark v1.0", p. 24. ♦ Finnigan, "Exploiting and Protecting Oracle", p. 11.	Objective / Subjective	Objective

Risk	Database links that store the username and password in the database do so in clear text. Should users gain access to the table that maintains this information, the information in the database being linked to could be compromised. The level of severity depends on the user account privileges associated with the account compromised.	Risk Level	Medium
Compliance Criteria	Compliance with this item is objective based on a review of all database links. Pass: There are no database links that have usernames and passwords hardcoded. Fail: At least one database link has a hardcoded username and password.		
Audit Procedure	1. Obtain a list of all database links by executing the following within SQL*Plus: *select * from all_db_links;* 2. Review the output of this statement to determine if any hardcoded usernames and passwords are found.		

2.2.4.4 Trace Files			
Control Objective	This control objective is designed to ensure that "users do not have the ability to read trace files". (Oracle Database Security Benchmark v1.0, p. 9)		
References	♦ "Oracle Database Security Benchmark v1.0", p. 9.	Objective / Subjective	Objective
Risk	Public access to trace files could reveal sensitive information to people who do not have a need to know. The likelihood of this happening is low due to the limited number of people who have access to the database outside of the application interfaces and host operating system.	Risk Level	Low
Compliance Criteria	This item either passes or fails compliance based on a binary setting of this parameter. Pass: _trace_files_public must be set equal to FALSE. Fail: _trace_files_public is set equal to TRUE.		

Audit Procedure	1. Obtain a copy of the init.ora file from the database administrator. 2. Perform a find in the file for the parameter "_trace_files_public=". 3. Review the value assigned to the parameter to see if it meets the compliance criteria.

2.2.4.5 SQL92 Security			
Control Objective	This control objective is designed to ensure that SELECT privileges are required to execute an update or delete on table values.		
References	♦ "Oracle Database Security Benchmark v1.0", p. 12.	Objective / Subjective	Objective
Risk	"This parameter will enforce the requirement that a user must have SELECT privilege on a table in order to be able to execute UPDATE and DELETE statements using WHERE clauses on a given table." (Oracle Database Security Benchmark v1.0, p. 12) Users could gain access to information they don't have a need to know should this setting not be set. Users are not likely to take advantage should this not be configured appropriately.	Risk Level	Low
Compliance Criteria	This item either passes or fails compliance based on a binary setting of this parameter. Pass: sql92_security must be set equal to TRUE. Fail: sql92_security is set equal to FALSE.		
Audit Procedure	1. Obtain a copy of the init.ora file from the database administrator. 2. Perform a find in the file for the parameter "sql92_security=". 3. Review the value assigned to the parameter to see if it meets the compliance criteria.		

2.2.4.6 Views			
Control Objective	This control objective is designed to ensure that access to sensitive views is appropriate.		
References	♦ "Oracle Database Security Benchmark v1.0", p. 21-22,37.	Objective / Subjective	Subjective

Risk	There are a number of database views that contain sensitive information. Users who have permission to access these views can use this information in an attempt to compromise application data. The likelihood of this happening is low due to the restriction on users to only access the database from within applications.	Risk Level	Medium
Compliance Criteria	Review the permissions that users have to the following database views: • DBA_% ; this represents a wildcard for all views that begin with DBA_. • V$_% ; this represents a wildcard for all views that begin with V$_. • ALL_% ; this represents a wildcard for all views that begin with ALL_. • ROLE_ROLE_PRIVS • USER_TAB_PRIVS • USER_ROLE_PRIVS Compliance for this item is subjective based on the different views and who the database administrator feels should have access to them. Pass: The permissions set on all sensitive views listed above are appropriate. Fail: The permissions are not appropriate on all sensitive views listed above.		
Audit Procedure	1. Execute the following SQL*Plus statement: *select grantee, privilege, table_name from dba_tab_privs where (owner='SYS' or table_name like 'DBA_%' or table_name like 'V$_%' or table_name like 'ALL_%' or table_name='ROLE_ROLE_PRIVS' or table_name='USER_TAB_PRIVS' or table_name='USER_ROLE_PRIVS');* 2. Review the output from step 1 with the DBA to determine if access to all the views are appropriate.		

2.2.4.7 With Admin			
Control Objective	This control objective is designed to ensure that privileges and roles have not been granted with the administrator option turned on.		
References	♦ "Oracle Database Security Benchmark v1.0", p. 23.	Objective / Subjective	Subjective

Risk	Granting privileges / roles with the admin option set allows the user to act as an administrator for that privilege / role. The likelihood of a user taking advantage of this ability is minimized due to the restriction of accessing the database via the application.	Risk Level	Medium
Compliance Criteria	Compliance with this item is subjective because certain users may require this capability and the identification of these users is at the discretion of the database administrator. Pass: All users who have been granted privileges / roles with admin option are appropriate. Fail: Users have been granted privileges / roles with admin option inappropriately.		
Audit Procedure	1. Obtain a list of all users that have been granted privileges with the admin option set by executing the following within SQL*Plus: *select grantee, privilege from dba_sys_privs where grantee not in ('SYS', 'SYSTEM', 'DBA') and admin_option='YES';* 2. Review the list with the database administrator to verify whether all the users require the privilege with admin option set. 3. Obtain a list of all users that have been granted roles with the admin option set by executing the following within SQL*Plus: *select grantee, granted_role from dba_role_privs where grantee not in ('SYS', 'SYSTEM', 'DBA') and admin_option='YES';* 4. Review the list with the database administrator to verify whether all the users require the role with admin option set.		

2.2.4.8 With Grant Privileges			
Control Objective	This control objective is designed to ensure that privileges have not been granted with the with grant option enabled.		
References	♦ "Oracle Database Security Benchmark v1.0", p. 23.	Objective / Subjective	Subjective
Risk	Users that have privileges to objects with the "with grant" option set are able to grant access to those same objects to other users. This risk is minimized by the inability of users to access the database outside of the application interface.	Risk Level	Medium

Compliance Criteria	Compliance with this item is subjective because certain users may require this capability and the identification of these users is at the discretion of the database administrator. Pass: All users who have been granted privileges with grant option are appropriate. Fail: Users have been granted privileges with grant option inappropriately.
Audit Procedure	1. Obtain a list of all users that have been granted privileges with the with grant option set by executing the following within SQL*Plus: *select owner, grantee, table_name from dba_tab_privs where grantable='YES' and owner not in ('SYS', 'SYSTEM', 'DBA') order by grantee;* 2. Review the list with the database administrator to verify whether all the users require the privilege with admin option set.

2.2.4.9 Select Any Table Privilege			
Control Objective	This control objective is designed to ensure that users do not have the ability to SELECT ANY TABLE.		
References	♦ "Oracle Database Security Benchmark v1.0", p. 23.	Objective / Subjective	Objective
Risk	Users with the privilege to SELECT ANY TABLE can view all the data in any table within the database and essentially bypass the permissions granted to them via roles. The likelihood that a user would attempt to select data from tables the don't have access to is low due to the fact that users are restricted from accessing the database via tools such as SQL*PLUS.	Risk Level	Low
Compliance Criteria	This item either passes or fails compliance based on a binary setting for each user account. Each user account either has this privilege or it doesn't so a simple review of all user accounts will provide the information necessary to assess this item. PASS = No users have been granted the privilege SELECT ANY TABLE. FAIL = Users have been granted the privilege SELECT ANY TABLE.		

Audit Procedure	1. Obtain a list of all users who have the privilege assigned to them by submitting the following from within SQL*PLUS. *select * from dba_sys_privs where privilege='SELECT ANY TABLE';* 2. Review the output of this command to determine if the compliance criteria is met.

2.2.4.10 Audit System Privilege			
Control Objective	This control objective is designed to ensure that only authorized users have audit privileges.		
References	♦ "Oracle Database Security Benchmark v1.0", p. 23.	Objective / Subjective	Subjective
Risk	As the audit trail has sensitive information in it, a user that has audit privileges may gain access to information they don't have a need-to-know. It is not likely that a user would use these privileges due to a lack of knowledge and the restriction of connecting through the application interface.	Risk Level	Low
Compliance Criteria	Determining whether a person has audit privileges or not is objective. Deciding that the person needs audit privileges is subjective. This item is therefore subjective based on the decision of the DBA as to who can have audit privileges. Pass: All users with audit privileges are appropriate. Fail: Users have audit privileges inappropriately.		
Audit Procedure	1. Execute the following statement within SQL*Plus: *select * from dba_sys_privs where privilege like '%AUDIT%';* 2. Review the output of step 1 with the DBA to decide if the privileges are appropriate.		

2.2.4.11 Package Access			
Control Objective	This control objective is designed to ensure that the access to packages that provide additional capabilities have not been granted to PUBLIC.		
References	♦ "Oracle Database Security Benchmark v1.0", p. 24.	Objective / Subjective	Subjective

Risk	Access to the packages provides users with additional privileges that may or may not be necessary for their job function. Unnecessary access to these packages provides privileges that are not required and could be exploited. Use of these packages is complex and the ability to work outside of the application interface is limited, therefore the likelihood of exploitation is low.	Risk Level	Medium
Compliance Criteria	Compliance for this item is objective based on the PUBLIC user group being granted access to the following packages. • UTL_FILE • UTL_TCP • UTL_HTTP • UTL_SMTP • DBMS_LOB • DBMS_SYS_SQL • DBMS_JOB Pass: None of the packages have been granted to the PUBLIC user group. Fail: At least one of the packages has been granted to the PUBLIC user group.		
Audit Procedure	1. Execute the following SQL*Plus statement to find packages that have been granted to PUBLIC with execute privileges. *select table_name from dba_tab_privs where grantee='PUBLIC' and privilege='EXECUTE' and table_name in ('UTL_FILE','UTL_TCP','UTL_HTTP','UTL_SMTP','DBMS_LOB','DBMS_SYS_SQL','DBMS_JOB');* 2. Review the results of step 1, if any are provided then this item fails compliance.		

2.2.4.12 Data Dictionary			
Control Objective	This control objective is designed to ensure that users with the privilege SELECT ANY TABLE cannot access the data dictionary.		
References	♦ "Oracle Database Security Benchmark v1.0", p. 30.	Objective / Subjective	Objective

Risk	The data dictionary contains sensitive information about the database and should not be accessible by users. It is not very likely that users have the privilege to SELECT ANY TABLE, however this control will reduce the risk should a user get this privilege.	Risk Level	Low
Compliance Criteria	This item either passes or fails compliance based on a binary setting of this parameter. PASS = The parameter O7_dictionary_accessibility is set to FALSE. FAIL = The parameter O7_dictionary_accessibility is set to TRUE.		
Audit Procedure	1. Obtain a copy of the init.ora file from the database administrator. 2. Review this file for value assigned to the parameter O7_dictionary_accessibility.		

3 Audit Evidence

Using the customized audit checklist, it was time to perform the audit of DBSRV1. Because I (the independent auditor) didn't have access to the system being audited, completing the audit required the involvement of the database administrator and the Tru64 system administrator. These administrators reviewed all the commands / scripts and then executed them on my behalf, providing the results in a text file. In order to demonstrate the execution of the audit, I selected ten checklist items to provide detailed audit results.

3.1 Audit Results

The results of the ten checklist items include the checklist item details with the additional audit evidence information (results of the commands / tests), a pass / fail determination based on the compliance criteria, and reference information to the discussion of the item in the audit report.

3.1.1 Default Account / Passwords

Reference: Checklist #: 2.2.1.2 Default Accounts / Passwords on page 19 Analysis in final report on page 73.	
Control Objective	This control objective is designed to ensure that all of the default accounts have been disabled / deleted if the account is not necessary, and that the password has been changed on all default accounts that are necessary.

References	♦ Personal Knowledge ♦ Plusnina, p. 9. ♦ Newallis, p. 7. ♦ "Oracle Audit Checklist", p. 1. ♦ Newman, p. 38. ♦ "Oracle Database Security Benchmark v1.0", p. 35.	Objective / Subjective	Objective
Risk	Leaving default accounts active and with default passwords provides an easy entry point for unauthorized access. It is highly likely that authorized users and attackers will attempt to log in to the database using the vendor supplied default accounts.	Risk Level	High
Compliance Criteria	A review of the database user accounts will determine if any vendor supplied accounts are present. Once the list of vendor supplied accounts present has been determined, they can be reviewed to determine if the account is necessary, if it has been disabled, and if the password has been changed. Pass = If vendor supplied default accounts exist, they are either disabled, or do not have default passwords. Fail = Multiple scenarios. Examples below: 1. A vendor supplied default account is enabled, and the password is still set to the default. 2. If the default account is enabled and it is not necessary.		
Audit Procedure	1. Obtain a list of all database user accounts by executing the following command via SQL*Plus: *select username, password, profile from dba_users;* 2. Review the list of accounts to determine if any are vendor supplied. 3. For the vendor supplied accounts found in step 2, attempt to connect to the database with the default password (usually equals username). An extensive list of default username / password combinations can be found at: <http://www.cirt.net/cgi-bin/passwd.pl?method=showven&ven=Oracle>. Successful connections mean the default password has not been changed.		
Audit Results	1. Output from step 1 in the audit procedures, scrubbed for sensitive information.		

User Accounts, passwords, profile, and owner on prd

Username	PASSWORD	PROFILE	OWNER
ADMN	6376D30E4EB575A4	DEFAULT	
AJJJEEE	3EF9038440AB16AC	DEFAULT	
ARRRRRR	5C24E1D83817511A	DEFAULT	
ASSSSSSS	EFB49CC14DE72FC6	DEFAULT	
AZZZZZZ	SQLCQR_DORMANT	DEFAULT	
AUUUUU	97671BF1B68B8D27	DEFAULT	
AVVVVVV	3F155D06629E7FB3	DEFAULT	
BBBBB	98B716B9C56CCF0F	DEFAULT	
CCC	6680F90D9146233F	DEFAULT	
CCD	E90B20F9A44CFDCC	DEFAULT	
CCE	E70CE40EAC4D28E6	DEFAULT	
CCF	SQLCQR_DORMANT	DEFAULT	
CCG	0BDF7ED9F2121522	DEFAULT	
CCH	SQLCQR_DORMANT	DEFAULT	
DBSNMP	4B206F502565E28D	DEFAULT	
DDD	SQLCQR_DORMANT	DEFAULT	
DDE	SQLCQR_DORMANT	DEFAULT	
DDF	6A21EFAA1B16DCA1	DEFAULT	
DDG	B07CED2B5242ECF7	DEFAULT	
EEE	71BA501619B5A0C4	DEFAULT	
EEG	D97C9B88DAF00843	DEFAULT	
EEF	1CED4754B7751750	DEFAULT	
EEC	647B48A0CA8F13E6	DEFAULT	
EXX	432DE0E7F06E730C	DEFAULT	
FFF	E6F19F9975978204	DEFAULT	
FFB	08AF9455773E4AA1	DEFAULT	
FED	A19B4FC124764887	DEFAULT	
FTE	8CA985B8A4DBE1ED	DEFAULT	
FAAAA	1DB08E3D9B25405C	DEFAULT	
III	D81479E6F9FB2519	DEFAULT	
IIIIII	SQLCQR_DORMANT	DEFAULT	
IKKK	1CB4E995DE15C2D9	DEFAULT	
ILLLLL	E2C0B4E91A55E62D	DEFAULT	
IPPPPP	C50CC9CEA77D0E27	DEFAULT	
ISSSSS	F82503F31B82A19B	DEFAULT	
IYYYYY	0BB7B9963E0B3CC4	DEFAULT	
IUUUUUU	SQLCQR_DORMANT	DEFAULT	
OUTLN	C3B2A1D4C3B2A1D4	DEFAULT	
SA	SQLCQR_DORMANT	DEFAULT	
SAAAAAAC	C3B2A1D4C3B2A1D4	DEFAULT	
SCC	SQLCQR_DORMANT	DEFAULT	
SCO	C3B2A1D4C3B2A1D4	DEFAULT	
SQLCQR	C3B2A1D4C3B2A1D4	DEFAULT	
SQLCQR_VSM_AGENT	C3B2A1D4C3B2A1D4	DEFAULT	
SYS	C3B2A1D4C3B2A1D4	DEFAULT	
SYSTEM	C3B2A1D4C3B2A1D4	DEFAULT	

2. A review of the accounts reveals that the following are vendor supplied:
   - DBSNMP
   - OUTLN

	• SYS • SYSTEM 3. A connection attempt was made to determine if the default username password combination was still set. The following was found: • DBSNMP / DBSNMP = Did not work. • OUTLN / OUTLN = Got connected. • SYS / CHANGE_ON_INSTALL = Did not work. • SYSTEM / MANAGER = Did not work.
Compliance Determination	Fail

3.1.2 TNS Listener Password

Reference: Checklist #: 2.2.2.2 TNS Listener Password on page 29			
Control Objective	This control objective is designed to ensure that the Listener is password protected.		
References	♦ "Oracle Database Listener Security Guide", p. 7-9. ♦ Newman, p. 11.	Objective / Subjective	Objective
Risk	Failure to password protect the Oracle Listener provides anyone who can communicate with it the ability to create a denial of service to the database, as well as obtain detailed configuration information. The likelihood of anyone trying to exploit the listener is low due to the complexity of the attack and the filtering at the firewall.	Risk Level	Medium
Compliance Criteria	This item either passes or fails compliance based on a binary setting of this parameter. Pass = The TNS Listener requires a password. Fail = A password is not required.		

Audit Procedure	1. Obtain a copy of the listener.ora file off of DBSRV1 from the administrator. *cat /u01/app/oracle/product/8.1.7/network/admin/listener.ora* 2. Review the file for the parameter "PASSWORDS_LISTENER=". 3. Another way to check is to execute the tnscmd perl script and run the services command. *perl tnscmd services --indent -h dbsrv1* 4. Review the output of the tnscmd services command to determine if a password has been configured. Output will be limited if a password is required. 5. A third way to verify the password requirement is to execute the tnscmd perl script and run the status command. *perl tnscmd status --indent -h dbsrv1* *6.* Review the output of the script for the parameter SECURITY. If the value for this parameter is ON, a password has been set.
Audit Results	1. Copy of the listener.ora file. # LISTENER.ORA Network Configuration File: /u01/app/oracle/product/8.1.7/network/admin/listener.ora # Generated by Oracle configuration tools. LISTENER = (DESCRIPTION_LIST = (DESCRIPTION = (ADDRESS_LIST = (ADDRESS = (PROTOCOL = TCP)(HOST = dbsrv1)(PORT = 1521))))) SID_LIST_LISTENER = (SID_LIST = (SID_DESC = (GLOBAL_DBNAME = prd) (ORACLE_HOME = /u01/app/oracle/product/8.1.7) (SID_NAME = prd))) PASSWORDS_LISTENER=(k3h8vy6w) 2. A review of the listener.ora file reveals that a password has been set. 3. Output from the tnscmd command. perl tnscmd services -h dbsrv1 sending (CONNECT_DATA=(COMMAND=services)) to dbsrv1:1521 writing 91 bytes reading .e.....''..Y(DESCRIPTION=(TMP=)(VSNNUM=135295744)(ERR=1169)(ERROR_STACK=(ERROR=(CODE=1169)(EMFI=4)))) 4. Review of the output from the tnscmd command reveals that a password has been applied to the listener because

we received error code 1169. Error code 1169 is for invalid password, and since we didn't supply a password, we can deduce that a password has been applied to the listener.

5. Output from the tnscmd status command.

```
Perl tnscmd status --indent -h dbsrv1
sending (CONNECT_DATA=(COMMAND=status)) to dbsrv1:1521
writing 89 bytes
reading
. .....6.....a. .....k.....
  DESCRIPTION=
    TMP=
    VSNNUM=135295744
    ERR=0
    ALIAS=LISTENER
    SECURITY=ON
    VERSION=TNSLSNR for DEC OSF/1 AXP: Version 8.1.7.3.0 -
Production
    START_DATE=15-OCT-2003 23:47:05
    SIDNUM=1
    LOGFILE=/u01/app/oracle/product/8.1.7/network/log/listener.log
    PRMFILE=/u01/app/oracle/product/8.1.7/network/admin/listener.ora
    TRACING=off
    UPTIME=2974532
    SNMP=OFF

."......
  ENDPOINT=
    HANDLER=
      STA=ready
      HANDLER_MAXLOAD=0
      HANDLER_LOAD=0
      ESTABLISHED=0
      REFUSED=0
      HANDLER_ID=C9C868DC8123-5CE8-E030-348CFDA7C274
      PRE=ttc
      SESSION=NS
      DESCRIPTION=
        ADDRESS=
          PROTOCOL=tcp
          HOST=dbsrv1
          PORT=1521
,,
  ENDPOINT=
    HANDLER=
      STA=ready
      HANDLER_MAXLOAD=0
      HANDLER_LOAD=0
      ESTABLISHED=0
      REFUSED=0
      HANDLER_ID=C9C868DC8124-5CE8-E030-348CFDA7C274
      PRE=ttc
      SESSION=NS
      DESCRIPTION=
        ADDRESS=
          PROTOCOL=ipc
```

	KEY=EXTPROC ,, SERVICE= SERVICE_NAME=prd INSTANCE= INSTANCE_NAME=prd NUM=2 INSTANCE_CLASS=ORACLE NUMREL=2 , SERVICE= SERVICE_NAME=prd05 INSTANCE= INSTANCE_NAME=prd05 NUM=2 INSTANCE_CLASS=ORACLE NUMREL=2 ,,.....@ 6. A review the output of the tnscmd status command reveals that the parameter SECURITY is set to ON. This means that a password has been set.
Compliance Determination	Pass P

3.1.3 Data Dictionary

Reference: Checklist #: 2.2.4.12 Data Dictionary on page 45.			
Control Objective	This control objective is designed to ensure that users with the privilege SELECT ANY TABLE cannot access the data dictionary.		
References	♦ "Oracle Database Security Benchmark v1.0", p. 30.	Objective / Subjective	Objective
Risk	The data dictionary contains sensitive information about the database and should not be accessible by users. It is not very likely that users have the privilege to SELECT ANY TABLE, however this control will reduce the risk should a user get this privilege.	Risk Level	Low

Compliance Criteria	This item either passes or fails compliance based on a binary setting of this parameter. PASS = The parameter O7_dictionary_accessibility is set to FALSE. FAIL = The parameter O7_dictionary_accessibility is set to TRUE.
Audit Procedure	1. Obtain a copy of the init.ora file from the database administrator. 2. Review this file for value assigned to the parameter O7_dictionary_accessibility.
Audit Results	1. A copy of the init.ora file can be found in Appendix A. 2. A review of the init.ora file reveals that the O7_DICTIONARY_ACCESSIBILITY parameter has been set to FALSE.
Compliance Determination	Pass P

3.1.4 Account Lockout

Reference: Checklist #: 2.2.1.9 Account Lockout on page 27			
Control Objective	This control objective is designed to ensure that database user accounts lockout after a specified number of failed login attempts.		
References	♦ Personal Knowledge ♦ "Oracle Database Security Benchmark v1.0", p. 19	Objective / Subjective	Objective
Risk	Failure to lockout accounts after a number of failed login attempts increases the chance that an account will be compromised due to a brute force password guessing attack. The likelihood of a password guessing attack is moderate. The impact of a compromise of this nature would depend on the permissions granted to the account that is compromised.	Risk Level	High

Compliance Criteria	Account lockout settings are made at the Profile level within Oracle. For each database profile used, review the failed login attempt parameter to ensure that it meets the following: This parameter can have a range of values assigned to it. Following SJK policy, the number of attempts shall be limited to 5 or less. This parameter needs to be verified for all profiles that are assigned to user accounts. PASS = failed_login_attempts ≤ 5 FAIL = failed_login_attempts > 5
Audit Procedure	1. Obtain a copy of the failed_login_attempts setting for each profile by issuing the following statement within SQL*Plus: *select profile, limit from dba_profiles where resource_name='FAILED_LOGIN_ATTEMPTS';* 2. Review this setting against the compliance criteria. 3. In addition to checking the setting, test to ensure that the setting is effective by attempting to login using an invalid password six times in a row. a. First display the account status for an account. b. Next attempt to connect as the account six times. c. Finally, display the account status again to show that the account is now locked.

Audit Results	1. Output from the SQL*Plus statement: PROFILE LIMIT ---------- ---------- DEFAULT 3 2. This setting meets the compliance critteria. 3.a. select username, account_status from dba_users where username='SCOTT'; USERNAME ACCOUNT_STATUS ---------- ---------- SCOTT OPEN 3.b. Attempt to login six times with a bad password. Connect scott/garbage@prd ERROR: ORA-01017: invalid username/password; logon denied Repeat six times 3.c. select username, account_status from dba_users where username='SCOTT'; USERNAME ACCOUNT_STATUS ---------- ---------- SCOTT LOCKED
Compliance Determination	Pass P

3.1.5 Oracle Audit Settings

Reference: Checklist #: 2.2.4.2 Oracle Audit Settings on page 37. Analysis in final report on page 79.			
Control Objective	This control objective is designed to ensure that Oracle auditing has been enabled for a predetermined set of events.		
References	♦ Personal Knowledge ♦ Finnigan, Pete. "Introduction to Simple Oracle Auditing", p. 4	Objective / Subjective	Objective
Risk	Failure to record audit data leads to the inability to identify and respond to security incidents.	Risk Level	Medium

Compliance Criteria	Check the audit settings to determine that the following are being audited: • ALTER USER • Any CREATE statement. • Any DROP statement. • GRANT ANY PRIVILEGE • GRANT ANY ROLE • INSERT failures • CREATE SESSION Pass: Auditing is enabled and configured to record at a minimum the above events. Fail: Auditing is not enabled, or does not record the minimum events above.
Audit Procedure	1. Obtain a copy of the init.ora file from the DBA. 2. Review the file for the parameter, audit_trail =, to determine if auditing is enabled. 3. Another check to see if auditing is enabled would be to execute the following within SQL*Plus: *select name, value from v$parameter where name like 'audit%';* 4. Next, check to see what privilege audit options are enabled by executing the following within SQL*Plus: *select * from dba_priv_audit_opts;* 5. Check to see what statement audit options are enabled by executing the following within SQL*Plus: *select * from dba_stmt_audit_opts;*

Audit Results	1. A copy of the init.ora file can be found in Appendix A. 2. Review of the file reveals that the audit_trial is set to true. 3. Output from SQL*Plus NAME VALUE ---------- ---------- audit_sys_operations FALSE audit_file_dest ?/rdbms/audit audit_trail TRUE 4. Output from SQL*Plus USER_NAME PROXY_NAME ---------- ---------- PRIVILEGE SUCCESS FAILURE ---------- ---------- ---------- CREATE SESSION BY ACCESS BY ACCESS 5. Output from SQL*Plus USER_NAME PROXY_NAME ---------- ---------- PRIVILEGE SUCCESS FAILURE ---------- ---------- ---------- CREATE SESSION BY ACCESS BY ACCESS
Compliance Determination	Fail 

3.1.6 With Admin Privileges

Reference: Checklist #: 2.2.4.7 With Admin Privileges on page 41.			
Control Objective	This control objective is designed to ensure that privileges and roles have not been granted with the administrator option turned on.		
References	♦ "Oracle Database Security Benchmark v1.0", p. 23.	Objective / Subjective	Subjective
Risk	Granting privileges / roles with the admin option set allows the user to act as an administrator for that privilege / role. The likelihood of a user taking advantage of this ability is minimized due to the restriction of accessing the database via the application.	Risk Level	Medium

Compliance Criteria	Compliance with this item is subjective because certain users may require this capability and the identification of these users is at the discretion of the database administrator. Pass: All users who have been granted privileges / roles with admin option are appropriate. Fail: Users have been granted privileges / roles with admin option inappropriately.
Audit Procedure	1. Obtain a list of all users that have been granted privileges with the admin option set by executing the following within SQL*Plus: *select grantee, privilege from dba_sys_privs where grantee not in ('SYS', 'SYSTEM', 'DBA') and admin_option='YES';* 2. Review the list with the database administrator to verify whether all the users require the privilege with admin option set. 3. Obtain a list of all users that have been granted roles with the admin option set by executing the following within SQL*Plus: *select grantee, granted_role from dba_role_privs where grantee not in ('SYS', 'SYSTEM', 'DBA') and admin_option='YES';* 4. Review the list with the database administrator to verify whether all the users require the role with admin option set.
Audit Results	1. The output from SQL*Plus revealed that no users were granted privileges with the admin option set. 2. Nothing to review. 3. The output from SQL*Plus revealed that no users were granted roles with the admin option set. 4. Nothing to review.
Compliance Determination	Pass P

3.1.7 Select Any Table Privilege

Reference: Checklist #: 2.2.4.9 Select Any Table Privilege on page 43.			
Control Objective	This control objective is designed to ensure that users do not have the ability to SELECT ANY TABLE.		
References	♦ "Oracle Database Security Benchmark v1.0", p. 23.	Objective / Subjective	Objective

Risk	Users with the privilege to SELECT ANY TABLE can view all the data in any table within the database and essentially bypass the permissions granted to them via roles. The likelihood that a user would attempt to select data from tables the don't have access to is low due to the fact that users are restricted from accessing the database via tools such as SQL*PLUS.	Risk Level	Low
Compliance Criteria	This item either passes or fails compliance based on a binary setting for each user account. Each user account either has this privilege or it doesn't so a simple review of all user accounts will provide the information necessary to assess this item. PASS = No users have been granted the privilege SELECT ANY TABLE. FAIL = Users have been granted the privilege SELECT ANY TABLE.		
Audit Procedure	1. Obtain a list of all users who have the privilege assigned to them by submitting the following from within SQL*PLUS. *select * from dba_sys_privs where privilege='SELECT ANY TABLE';* 2. Review the output of this command to determine if the compliance criteria is met.		
Audit Results	1. Output from SQL*Plus No rows selected.		
Compliance Determination	Pass P		

3.1.8 Listener Ports

Reference: Checklist #: 2.2.2.6 Listener Ports on page 32. Analysis in final report on page 77.			
Control Objective	This control objective is designed to ensure that the Oracle TNS listener is not running on the default ports of 1521 or 1526.		
References	♦ "Oracle Database Security Benchmark v1.0", p. 31.	Objective / Subjective	Objective

Risk	The default ports are well known by attackers. Running the listener on a non-default port will make it more difficult for an attacker to determine the location of critical database resources. The likelihood that an attacker would attempt to connect to the default port is high, but the risk of not changing the value from the default is low because a determined attacker would only be slowed down by this change.	Risk Level	Low
Compliance Criteria	This item either passes or fails compliance based on a binary setting of this parameter. Pass = The listener port is neither 1521 or 1526. Fail = The listener port is 1521 or 1526.		
Audit Procedure	1. Obtain a copy of the listener.ora file off of DBSRV1 from the administrator. *cat /u01/app/oracle/product/8.1.7/network/admin/listener.ora* 2. Review the file for the listener port setting. 3. Run the tnscmd perl script and run the status command. *perl tnscmd status --indent -h dbsrv1* 4. Review the output of the script for the listener port. 5. Execute an nmap scan of the database server. *nmap -sS -O -p 1-65535 -v -oN dbsrv1.txt dbsrv1* 6. Review the output of the nmap scan to determine if the default listener port (1521) is used.		
Audit Results	1. Copy of the listener.ora file. # LISTENER.ORA Network Configuration File: /u01/app/oracle/product/8.1.7/network/admin/listener.ora # Generated by Oracle configuration tools. LISTENER = (DESCRIPTION_LIST = (DESCRIPTION = (ADDRESS_LIST = (ADDRESS = (PROTOCOL = TCP)(HOST = dbsrv1)(PORT = 1521))))) SID_LIST_LISTENER = (SID_LIST = (SID_DESC = (GLOBAL_DBNAME = prd) (ORACLE_HOME = /u01/app/oracle/product/8.1.7) (SID_NAME = prd)		

)
)

PASSWORDS_LISTENER=(k3h8vy6w)

2. A review of the file reveals that the listener port is the default of 1521.
3. Output from the tnscmd status command.

```
Perl tnscmd status --indent -h dbsrv1
sending (CONNECT_DATA=(COMMAND=status)) to dbsrv1:1521
writing 89 bytes
reading
. .....6.....a. .....k.....
  DESCRIPTION=
    TMP=
    VSNNUM=135295744
    ERR=0
    ALIAS=LISTENER
    SECURITY=ON
    VERSION=TNSLSNR for DEC OSF/1 AXP: Version 8.1.7.3.0 -
Production
    START_DATE=15-OCT-2003 23:47:05
    SIDNUM=1
    LOGFILE=/u01/app/oracle/product/8.1.7/network/log/listener.log
    PRMFILE=/u01/app/oracle/product/8.1.7/network/admin/listener.ora
    TRACING=off
    UPTIME=2974532
    SNMP=OFF

."......
  ENDPOINT=
    HANDLER=
      STA=ready
      HANDLER_MAXLOAD=0
      HANDLER_LOAD=0
      ESTABLISHED=0
      REFUSED=0
      HANDLER_ID=C9C868DC8123-5CE8-E030-348CFDA7C274
      PRE=ttc
      SESSION=NS
      DESCRIPTION=
        ADDRESS=
          PROTOCOL=tcp
          HOST=dbsrv1
          PORT=1521

,,
  ENDPOINT=
    HANDLER=
      STA=ready
      HANDLER_MAXLOAD=0
      HANDLER_LOAD=0
      ESTABLISHED=0
      REFUSED=0
      HANDLER_ID=C9C868DC8124-5CE8-E030-348CFDA7C274
      PRE=ttc
```

```
     SESSION=NS
     DESCRIPTION=
      ADDRESS=
        PROTOCOL=ipc
        KEY=EXTPROC
,,
  SERVICE=
    SERVICE_NAME=prd
    INSTANCE=
      INSTANCE_NAME=prd
      NUM=2
      INSTANCE_CLASS=ORACLE
      NUMREL=2
,
  SERVICE=
    SERVICE_NAME=prd05
    INSTANCE=
      INSTANCE_NAME=prd05
      NUM=2
      INSTANCE_CLASS=ORACLE
      NUMREL=2

,,.........@
```

4. A review the output of the tnscmd status command reveals the listener is running on port 1521.
5. Output from an nmap scan of DBSRV1.

Interesting ports on dbsrv1 (10.11.12.13):
(The 65493 ports scanned but not shown below are in state: closed)

Port	State	Service
21/tcp	open	ftp
22/tcp	open	ssh
25/tcp	open	smtp
110/tcp	open	pop-3
111/tcp	open	sunrpc
143/tcp	open	imap2
316/tcp	open	decauth
515/tcp	open	printer
596/tcp	open	smsd
619/tcp	open	unknown
886/tcp	open	unknown
1024/tcp	open	kdm
1025/tcp	open	NFS-or-IIS
1026/tcp	open	LSA-or-nterm
1028/tcp	open	unknown
1521/tcp	open	oracle
2121/tcp	open	unknown
2481/tcp	open	unknown
2793/tcp	open	unknown
3354/tcp	open	unknown
6000/tcp	open	X11
6112/tcp	open	dtspc
7150/tcp	open	unknown
7152/tcp	open	unknown
7153/tcp	open	unknown

	7650/tcp open unknown 7651/tcp open unknown 7652/tcp open unknown 9150/tcp open unknown 9151/tcp open unknown 9152/tcp open ms-sql2000 9153/tcp open unknown 9154/tcp open unknown 9155/tcp open unknown 9650/tcp open unknown 9651/tcp open unknown 9652/tcp open unknown 9653/tcp open unknown 9654/tcp open unknown 9655/tcp open unknown 10401/tcp open unknown 10402/tcp open unknown Device type: general purpose Running: Compaq Tru64 UNIX 5.X OS details: Compaq Tru64 UNIX V5.1A (Rev. 1885) TCP Sequence Prediction: Class=truly random Difficulty=9999999 (Good luck!) IPID Sequence Generation: Incremental 6. Reviewing the output of the nmap scan finds the Oracle listener running on port 1521.
Compliance Determination	Fail

3.1.9 Package Access

Reference: Checklist #: 2.2.4.11 Package Access on page 44. Analysis in final report on page 80.			
Control Objective	This control objective is designed to ensure that the access to packages that provide additional capabilities have not been granted to PUBLIC.		
References	♦ "Oracle Database Security Benchmark v1.0", p. 24.	Objective / Subjective	Subjective
Risk	Access to the packages provides users with additional privileges that may or may not be necessary for their job function. Unnecessary access to these packages provides privileges that are not required and could be exploited. Use of these packages is complex and the ability to work outside of the application interface is limited, therefore the likelihood of exploitation is low.	Risk Level	Medium

Compliance Criteria	Compliance for this item is objective based on the PUBLIC user group being granted access to the following packages. • UTL_FILE • UTL_TCP • UTL_HTTP • UTL_SMTP • DBMS_LOB • DBMS_SYS_SQL • DBMS_JOB Pass: None of the packages have been granted to the PUBLIC user group. Fail: At least one of the packages has been granted to the PUBLIC user group.
Audit Procedure	1. Execute the following SQL*Plus statement to find packages that have been granted to PUBLIC with execute privileges. *select table_name from dba_tab_privs where grantee='PUBLIC' and privilege='EXECUTE' and table_name in ('UTL_FILE','UTL_TCP','UTL_HTTP','UTL_SMTP','DBMS_LOB','DBMS_SYS_SQL','DBMS_JOB');* 2. Review the results of step 1, if any are provided then this item fails compliance.
Audit Results	1. Output from SQL*Plus: UTL_FILE 2. After review, this item fails because one of the packages provides public execute privileges.
Compliance Determination	Fail

3.1.10 "Public" Permissions

Reference: Checklist #: 2.2.1.6 "Public" Permissions on page 23. Analysis in final report on page 74.			
Control Objective	This control objective is designed to ensure that the permissions granted to the user group "PUBLIC" are appropriate.		
References	♦ Personal Knowledge ♦ Newman, p. 38.	Objective / Subjective	Subjective
Risk	Permissions granted to the PUBLIC user group are provided to all database users because all	Risk Level	High

	database users are members of the PUBLIC user group. Permissions granted to PUBLIC should be limited to those that all users need to have. It is very likely that the permissions assigned to PUBLIC will be greater than necessary if they are not reviewed.		
Compliance Criteria	Compliance will depend on the analysis of the permissions / roles / privileges granted to the PUBLIC user group. This review will need to be done in coordination with the DBA to determine what permissions are required of all users. Pass: The analysis has concluded that all permissions / roles / privileges granted to the PUBLIC user group are appropriate. Fail: PUBLIC has been granted permissions / roles / privileges that are not appropriate for all users to have. .		
Audit Procedure	1. Obtain a list of all the objects where permissions have been granted to PUBLIC. *select table_name, privilege from dba_tab_privs where grantee='PUBLIC';* 2. Review the output of step 1 with the DBA to determine if the permissions are necessary for the PUBLIC user group. 3. Obtain a list of all roles that have been granted to PUBLIC. *select granted_role from dba_role_privs where grantee='PUBLIC';* 4. Review the output of step 3 with the DBA to determine if the roles are necessary for the PUBLIC user group. 5. Obtain a list of all system privileges that have been granted to PUBLIC. *Select privilege from dba_sys_privs where grantee='PUBLIC';* 6. Review the output of step 3 with the DBA to determine if the roles are necessary for the PUBLIC user group.		
Audit Results	1. Output from SQL*Plus: BAT.NTUSERS: SELECT BAT.BATT_ACTIVE_USERS: SELECT BAT.BATT_APPLICATIONS: SELECT BAT.BATT_NONR_EMP: SELECT BAT.BATT_PUBLIC_READ_USAGE: SELECT BAT.BATT_USER_ROLES: SELECT DKAT.DKATT_USERS: SELECT CIRWS.TMP_WSRT_BUILDING: SELECT CIRWS.TMP_WSRT_OUTPUT: SELECT CIRWS.TMP_WSRT_OUTPUT_CCC: SELECT CIRWS.TMP_WSRT_OUTPUT_EPACODES: SELECT CIRWS.TMP_WSRT_OUTPUT_LDR_SUBCAT: SELECT CIRWS.TMP_WSRT_PROCESS: SELECT		

	BAT.BATV_PRD_USERS: SELECT SQLCQR.SQLCQRV_PWDSTATS: SELECT BAT.BATV_ACTIVE_USERS: SELECT BAT.ROLE_STRINGS: EXECUTE SQLCQR.SQLCQR_PWD: EXECUTE BAT.BATT_DB_SERVER: SELECT PRD.IMPORTCONTAINERBINDINGTAB2: SELECT BAT.BATT_APP_DB: SELECT TMS.TOOLT_USERS: SELECT SPARCS.SPARCSP_SECURITY: EXECUTE SPARCS.SPARCSP_SYSTEM: EXECUTE BAT.BATT_ALL_EMP: SELECT CUE.CUET_PHONES: SELECT CWEF.CWEFT_D_NAMES: SELECT CWEF.CWEFT_D_JOB: SELECT CWEF.CWEFT_D_HISTORY: SELECT FCW.FCWS_EMP_SEQ: SELECT FCW.FCWS_EQUIP_SEQ: SELECT FCW.FCWS_LOCATION: SELECT FCW.FCW_SEQ_NO: SELECT FCW.FCWT_ARCH_ADM: SELECT FCW.FCWT_ARCH_EQU: SELECT FCW.FCWT_ARCH_ORI: SELECT FCW.FCWT_ARCH_PRO: SELECT FCW.FCWT_ARCH_RES: SELECT FCW.FCWT_ARCH_SHI: SELECT FCW.FCWT_ARCH_SOU: SELECT FCW.FCWT_DAVIS_BACON: SELECT FCW.FCWT_FACTOR: SELECT FCW.FCWT_MEQ: SELECT FCW.FCWT_MINOR: SELECT FCW.FCWT_MINOR_CRAFT: SELECT FCW.FCWT_RANK: SELECT FCW.FCWT_REPORT: SELECT FCW.FCWT_RISK: SELECT FCW.FCWT_RPT_COLUMN: SELECT FCW.FCWT_SM_ACCESS: SELECT FCW.FCWT_SM_BLDG_CODE: SELECT FCW.FCWT_SM_CLOSE_CODE: SELECT FCW.FCWT_SM_CLUSTER: SELECT FCW.FCWT_SM_DAVIS_BACON: SELECT FCW.FCWT_SM_DESIGNEE: SELECT FCW.FCWT_SM_EMPLOYEE: SELECT FCW.FCWT_SM_EQUIP_MASTER: SELECT FCW.FCWT_SM_OPS_AREA: SELECT FCW.FCWT_SM_ORG_CODE: SELECT FCW.FCWT_SM_PRIORITY_CODE: SELECT FCW.FCWT_SM_PROG: SELECT FCW.FCWT_SM_RESPONSE_CODE: SELECT FCW.FCWT_SM_RISK: SELECT FCW.FCWT_SM_ROLE: SELECT FCW.FCWT_SM_SAFETY_CODE: SELECT FCW.FCWT_SM_SHIFT_PEOPLE: SELECT FCW.FCWT_SM_SOURCE_CODE: SELECT FCW.FCWT_SM_SYS_CATEGORY: SELECT FCW.FCWT_SM_VSS_BLDG: SELECT

	FCW.FCWT_SM_VSS_DSGNR: SELECT FCW.FCWT_SM_VSS_TCOMP: SELECT FCW.FCWT_SM_WBS_CODE: SELECT FCW.FCWT_SM_WORK_DSC: SELECT FCW.FCWT_SOURCE: SELECT FCW.FCWT_STATUS_MMS: SELECT FCW.FCWT_SYS_EQU: SELECT FCW.FCWT_SYS_NEWS: SELECT FCW.FCWT_SYS_OPS_WBS: SELECT FCW.FCWT_TRANS_LOG: SELECT FCW.FCWT_XFER: SELECT FCW.FCWV_DAVIS_BACON: SELECT FCW.FCWV_FCWS_CUET_PHONES: SELECT FCW.FCWV_CLUSTERS: SELECT FCW.FCWV_CWBST_CHARGES: SELECT FCW.FCWV_SM_EQUIP_MASTER: SELECT FCW.FCWV_CRAFT: SELECT FCW.FCWP_UTILITY: EXECUTE FCS.FCSP_CALCS: EXECUTE SMP.MMST_CLUSTERS: SELECT SMP.FCWV_SM_EQUIP_MASTER: SELECT CMEW.NUM_VARRAY: EXECUTE CMEW.STR_VARRAY: EXECUTE 2. After review with the DBA it has been determined that PUBLIC does not need privileges to the majority of the above tables. 3. Output from SQL*Plus: FCW_READ 4. After review with the DBA it has been determined that PUBLIC does not need the FCW_READ role. 5. The output from SQL*Plus did not contain any rows. This means that there are no system privileges granted to PUBLIC. 6. Nothing to review.
Compliance Determination	Fail ✗

3.2 Residual Risk

Given the number of items that failed the audit (15 out of 41), you could expect a fair amount of residual risk. However, most of the items that failed can be fixed relatively easily without a large impact to the system and its' associated business processes. The following table is a summary of all the failed items, with an

estimate of how difficult it would be to correct the problem, and what investment in time / money will be needed to become compliant.

Checklist #	Control Title	Compliance (Pass / Fail)	Difficulty	Investment
2.1.2	Oracle Security Baseline	Fail	Medium	80 hours
2.1.5	Auditing / Logging / Monitoring Policy and Procedures	Fail	Medium	80 hours
2.1.8	Incident Response Procedures	Fail	Medium	80 hours
2.1.9	Risk Assessment	Fail	Medium	80 hours
2.2.1.2	Default Accounts / Passwords	Fail	Low	2 hours
2.2.1.6	"Public" Permissions	Fail	High	20 hours
2.2.2.3	Listener Admin Restrictions	Fail	Low	2 hours
2.2.2.4	Listener Audit Settings	Fail	Low	2 hours
2.2.2.5	Unused Listener Services	Fail	Low	16 hours
2.2.2.6	Listener Ports	Fail	Medium	40 hours
2.2.3.4	Database file permissions.	Fail	Medium	40 hours
2.2.3.5	Database file Integrity	Fail	Medium	20 hours / $2000 for integrity software
2.2.4.2	Oracle Audit	Fail	Medium	16 hours
2.2.4.5	SQL92 Security	Fail	Low	2 hours
2.2.4.11	Package Access	Fail	Medium	24 hours

Table 2: Remediation Estimates

Due to the sensitivity level of a lot of the data that is stored in the databases on the system, I feel that it is well worth the investment to correct all the items found. The policy and procedure items will not only benefit this database server, but they will also benefit the entire company. The number of hours needed to complete all of the items is estimated to be around 488, although I feel like this is a rather high estimate. Equating these hours to dollars I used a fully burdened rate of $60 /hour for either a DBA or security professional. This would make the cost to fix all findings, $29,280 for labor and approximately $2,000 for software, for a total price of $31,280. While this cost appears pretty steep, it is assumed that it will really be absorbed by the DBA and security personnel fixing the problems as part of their regular duties and not an extra expense. The only real expense will be the $2,000 for file integrity software.

3.3 Audit Evaluation

An evaluation of the applicability and completeness of this audit reveals that this audit was thorough in identifying weaknesses and strengths in the security surrounding the database server. In addition, the audit was able to identify a number of items that if corrected would improve the security surrounding all systems used by SJK and not just this particular database server.

While it is best to be objective when performing an audit, the nature of Oracle leads itself to a number of subjective audit steps. While these subjective audit steps are not the ideal way to perform an audit, it is not possible for the independent auditor to know enough about the system and SJK's business processes to make an objective determination.

In addition, a number of audit steps performed only took into consideration a limited number of requirements as opposed to performing a detailed audit of the item in question. For example, the Disaster Recovery audit step only looked at whether or not a plan exists and if it is tested. A full audit of a Disaster Recovery plan would include many dozens of additional items.

4 Audit Report

4.1 Executive Summary

In December 2003, ABC Consulting group performed an independent audit of DBSRV1 at the request of SJK management. The audit performed was a periodic assessment of the security controls in place surrounding the Oracle 8.1.7 database server. The results of the audit point out that although the security of the system is pretty solid overall, a number of items can be implemented to improve the security of the server with little or no cost to SJK, and minimal impact to the business processes.

Table 3 contains a summary of the audit results broken down by the risk level and pass / fail mark.

	High	Medium	Low	Total
Pass	9	10	7	26
Fail	3	6	6	15
Total	12	16	13	41

Table 3: Finding Summary

A high level overview of the findings reveals that SJK should perform an assessment to determine that all the necessary security policies and procedures are in place. Documenting and implementing policies and procedures would mitigate the risks for the high rated findings. In addition, SJK should create security baselines for each platform (Operating System, Database, Application) used. These baselines would mitigate the majority of the medium and low rated findings. Section 4.2 of this report will go into detail for each audit checklist item that was found to be in non-compliance.

It is important to understand that this review was conducted as a point in time analysis. Since Information Technology (IT) infrastructures are continuously

changing, this security assessment should be used to report the status of security controls at this particular time. This review is not intended to act as a warranty against future threats or new vulnerabilities.

4.2 Audit Findings

We took a phased approach to complete this review. The planning phase consisted of research of industry best practice for Oracle, along with scheduling and requesting documentation from SJK personnel. The second phase was the actual performance of the audit, where both technical and interview processes were completed. The final phase consisted of data analysis and documentation (report generation).

The following tables contain the detailed Audit Findings, the Risk they pose to SJK, recommendations on how they can be remediated, an estimated cost for remediation, and compensating controls if required.

Finding 1: An Oracle security baseline document does not exist.	**Risk Level**	High
	Checklist #	2.1.2
	Page References	12-13, 68, 85
Control Objective	This control objective is designed to ensure that all Oracle DB servers are configured in a consistent and secure fashion.	
Risk	Not having a documented Oracle security baseline can lead to inconsistencies in the configuration of Oracle database servers that may leave them vulnerable to being compromised. A compromise of DBSRV1 could be critical to the business because all of the companies' financial, payroll, and customer information is stored in the database. Should the database be compromised, the attacker could steal customer credit card numbers, among other things, this would result in a loss of customer confidence in SJK.	
Recommendations	We recommend creating an Oracle Security Baseline. In addition, it is recommended that each database server be reviewed to ensure that it complies with the new baseline once the baseline has been completed.	

Cost Analysis	It is estimated that it will take 80 staff hours to research, create, and gain approval for an Oracle security baseline. This estimate is a combination of hours from a security staff member and a database administrator. Using a fully burdened rate of $60 / hour for each, the cost to create the baseline is estimated to be $4,800. The costs to implement the baseline on all database servers has not been estimated because it will be based on how insecure the servers currently are.
Compensating Controls	Compensating controls are not necessary because it is reasonable to implement the recommendation that addresses this finding.

Finding 2: Auditing / Logging / Monitoring policies and procedures do not exist.	**Risk Level**	Medium
	Checklist #	2.1.5
	Page References	15, 68, 85
Control Objective	This control objective is designed to ensure that auditing, logging and monitoring policies and procedures have been implemented.	
Risk	Failure to require auditing, logging, and monitoring can result in the lack of ability to identify and respond to security incidents. Probably the biggest risk to SJK would be the inability to recognize a security incident which would allow the attack to continue unimpeded.	
Recommendations	We recommend developing auditing, logging, and monitoring procedures that detail what auditing needs to be enabled, how often the logs need to be reviewed, and provides some examples of how to identify a security incident.	
Cost Analysis	It has been estimated that it will take 80 staff hours to develop the procedures. This estimate is a combination of hours from a security staff member and a database administrator. Using a fully burdened rate of $60 / hour for each, the cost to create the baseline is estimated to be $4,800. The cost to implement auditing has not been estimated because it will depend on factors that are unknown at this time. In addition, the ongoing costs have not been estimated. These include: the number of servers auditing will need to be configured on, the frequency and time it will take to monitor the logs, and the hourly rate of the staff that will perform the auditing.	
Compensating Controls	Compensating controls are not necessary because it is reasonable to implement the recommendation that addresses this finding.	

Finding 3: Incident Response Procedures do not exist.		**Risk Level**	Medium
		Checklist #	2.1.8
		Page References	17-18, 68, 85
Control Objective	This control objective is designed to ensure that incident response procedures have been implemented.		
Risk	Failure to have documented incident response procedures can lead to an incident not being handled properly, potentially leading to further losses and / or lack of prosecution due to mishandled evidence.		
Recommendations	Develop incident response procedures to follow in the case of a security incident. In addition, a security incident response team should be created and trained on the procedures. An annual test of the procedures should also be conducted.		
Cost Analysis	It is estimated that it will take 80 staff hours to research, create, and gain approval for the Incident Response Procedures. This estimate is a combination of hours from a security staff member and a database administrator. Using a fully burdened rate of $60 / hour for each, the cost to create the procedures is estimated to be $4,800. The ongoing costs to train and test the procedures have not been estimated, but will be a result of the number of individuals involved, their hourly rate, and the number of hours required of each.		
Compensating Controls	Compensating controls are not necessary because it is reasonable to implement the recommendation that addresses this finding.		

Finding 4: Risk Assessment	**Risk Level**	Medium
	Checklist #	2.1.9
	Page References	18, 68, 85

Control Objective	This control objective is designed to ensure that a risk assessment (including data classification) has been completed for the database server (DBSRV1).
Risk	The results of the risk assessment should be used to guide the security architecture of the database environment. Failure to complete a risk assessment may create a situation where the data does not have the appropriate amount of security controls in place. For example, if the data is classified as high, it could be decided that encryption is a requirement. It is probable that the data wouldn't be secured appropriately if a risk assessment isn't completed. Inadequate controls could lead to the public disclosure of sensitive information such as financial, payroll, and customer information.
Recommendations	We recommend that a thorough risk assessment be completed for DBSRV1. In addition, a formal risk assessment process should be created and a risk assessment completed for all systems at SJK.
Cost Analysis	It is estimated that it will take 80 staff hours to perform a thorough risk assessment for DBSRV1. This estimate is a combination of hours from a security staff member, a system administrator, and a database administrator. Using a fully burdened rate of $60 / hour for each, the cost to create the procedures is estimated to be $4,800. The cost to develop a formal risk assessment process was not included in the cost for this finding, but would be estimated at $4,800 as well. The cost to perform a risk assessment of every system at SJK has not been estimated due to a lack of knowledge of the number and size of the systems involved.
Compensating Controls	Compensating controls are not necessary because it is reasonable to implement the recommendation that addresses this finding.

Finding 5: Default user accounts have been found with the default password still enabled.	**Risk Level**	High
	Checklist #	2.2.1.2
	Page References	19-20, 46, 68, 85

Control Objective	This control objective is designed to ensure that all of the default accounts have been disabled / deleted if the account is not necessary, and that the password has been changed on all default accounts that are necessary.
Risk	Leaving default accounts active and with default passwords provides an easy entry point for unauthorized access. The amount of information available to an attacker will depend on the account accessed. Failure to change the default passwords could lead to the public disclosure of sensitive information such as financial, payroll, and customer information.
Recommendations	We recommend changing the password on all default system accounts. In addition, we recommend deleting / disabling all default accounts that are not necessary. Finally, a process should be developed to require that passwords be changed for all accounts on a periodic basis.
Cost Analysis	It is estimated that it will take two staff hours for a database administrator to identify and change all the default account passwords on DBSRV1. Using a fully burdened rate of $60 / hours, the cost to create the procedures is estimated to be $120. The cost to review all accounts for necessity has not been estimated due to a lack of knowledge on how default accounts are used at SJK. In addition, the cost to change all the default account passwords on other database servers has not been considered. There will also be an ongoing cost to change all default account passwords on a periodic basis, however this has not been estimated due to the unknown number of accounts and servers that need to be dealt with.
Compensating Controls	Compensating controls are not necessary because it is reasonable to implement the recommendation that addresses this finding.

Finding 6: Permissions granted to the PUBLIC user group are not set appropriately.	**Risk Level**	High
	Checklist #	2.2.1.6
	Page References	23-24, 64, 68, 85

Control Objective	This control objective is designed to ensure that the permissions granted to the user group "PUBLIC" are appropriate.
Risk	Permissions granted to the PUBLIC user group are provided to all database users because all database users are members of the PUBLIC user group. Permissions granted to PUBLIC should be limited to those that all users need to have. The risk is hard to estimate due to the lack of knowledge as to what the specific objects are that PUBLIC has access to. It is assumed that some of the data is at least moderately sensitive and would therefore result in a Medium risk rating.
Recommendations	We recommend that all permissions granted to the PUBLIC user account be reviewed for appropriateness. In addition, a process should be developed to review the permissions granted to PUBLIC on a periodic basis for each server, as they may change over time due to configuration changes to the database.
Cost Analysis	It is estimated that it will take 20 staff hours for a database administrator to review and correct the permissions granted to PUBLIC on DBSRV1. Using a fully burdened rate of $60 / hours, the cost to create the procedures is estimated to be $1,200. The cost to develop and implement a process on an ongoing basis has not been estimated due to the unknown number of database servers in question.
Compensating Controls	Compensating controls are not necessary because it is reasonable to implement the recommendation that addresses this finding.

Finding 7: Restrictions on the network listener are not configured appropriately.	**Risk Level**	Low
	Checklist #	2.2.2.3
	Page References	30, 68, 85
Control Objective	This control objective is designed to ensure that changes to the listener cannot be made dynamically.	
Risk	Without this parameter turned on, changes can be made to the listener settings without having to reload it.	
Recommendations	We recommend that the network listener be configured with admin restrictions turned on. In addition, this setting should be part of the Oracle Security baseline.	
Cost Analysis	The cost to implement this item has been estimated to be $120 based on two hours of the database administrators' time. The cost of adding this to the Oracle Security baseline has already been included in Finding #1.	

Compensating Controls	Compensating controls are not necessary because it is reasonable to implement the recommendation that addresses this finding.

Finding 8: Auditing is not enabled on the network listener.	**Risk Level**	Medium
	Checklist #	2.2.2.4
	Page References	31, 68, 85
Control Objective	This control objective is designed to ensure that auditing has been enabled on the Oracle network listener.	
Risk	Failure to enable auditing on the network listener would make it difficult to identify and track down a security incident.	
Recommendations	We recommend that auditing be enable on the network listener. In addition, as mentioned in Finding #2, procedures should be developed that detail what should be logged and how often the logs should be reviewed.	
Cost Analysis	The cost to implement this item has been estimated to be $120 based on two hours of the database administrators' time. The cost of updating the procedures has already been included in Finding #2.	
Compensating Controls	Compensating controls are not necessary because it is reasonable to implement the recommendation that addresses this finding.	

Finding 9: The network listener has unnecessary services enabled.	**Risk Level**	Low
	Checklist #	2.2.2.5
	Page References	31-32, 68, 85
Control Objective	This control objective is designed to ensure that only necessary listener services are installed.	
Risk	"ExtProc (PLSExtProc) functionality allows external C and Java functions to be called from within PL/SQL." (Oracle Database Security Benchmark v1.0, p. 31). The ability to call external programs could lead to a user having greater privileges than he / she needs to have.	
Recommendations	We recommend that ExtProc functionality be disabled if it is not required. In addition, this setting should be included in the Oracle security baseline.	
Cost Analysis	The cost to review the implications and implement this item has been estimated to be $960 based on 16 hours of the database administrators' time. The cost of adding this to the Oracle Security baseline has already been included in Finding #1.	

Compensating Controls	Compensating controls are not necessary because it is reasonable to implement the recommendation that addresses this finding.

Finding 10: The network listener is configured to use the default ports.	**Risk Level**	Low
	Checklist #	2.2.2.6
	Page References	32-33, 59-60, 68, 85
Control Objective	This control objective is designed to ensure that the Oracle TNS listener is not running on the default ports of 1521 or 1526.	
Risk	The default ports are well known by attackers. Running the listener on a non-default port will make it more difficult for an attacker to determine the location of critical database resources. The likelihood that an attacker would attempt to connect to the default port is high, but the risk of not changing the value from the default is low because a determined attacker would only be slowed down by this change.	
Recommendations	We recommend changing the port that the network listener uses to something other than default. In addition, this setting should be added to the Oracle security baseline.	
Cost Analysis	The cost to review the implications of making this change and implementing this item has been estimated to be $2,400 based on 40 hours of the database administrators time. The cost of adding this to the Oracle Security baseline has already been included in Finding #1.	
Compensating Controls	Compensating controls are not necessary because it is reasonable to implement the recommendation that addresses this finding.	

Finding 11: The database files do not have the appropriate access controls at the operating system level.	**Risk Level**	Low
	Checklist #	2.2.3.4
	Page References	35, 68, 85

Control Objective	This control objective is designed to ensure that the Oracle database files have the appropriate file permissions. This should include reviewing the Oracle home directory, Oracle temporary directories and all of their subdirectories and files.
Risk	Access to Oracle files should be controlled to prevent an unauthorized user from gaining access to sensitive information. Due to the limited number of operating system users, the likelihood of someone gaining access to any Oracle files is limited.
Recommendations	We recommend a thorough review of all database files to ensure they have the appropriate operating system access controls. In addition, a standard set of access control permissions should be added to the Oracle Security Baseline.
Cost Analysis	The cost to review the implications of making this change and implementing this item has been estimated to be $2,400 based on 40 hours of the database administrators time. The cost of adding this to the Oracle Security baseline has already been included in Finding #1.
Compensating Controls	Compensating controls are not necessary because it is reasonable to implement the recommendation that addresses this finding.

Finding 12: The database server executables and script files are not being monitored for file integrity.	**Risk Level**	Low
	Checklist #	2.2.3.5
	Page References	36, 68, 85
Control Objective	This control objective is designed to ensure that file integrity monitoring is in place for the Oracle installation. This should include reviewing Oracle scripts and executables in the Oracle home directory.	
Risk	Changes to Oracle executables and scripts can be indication that the system has been penetrated and the files replaced with Trojaned versions. The likelihood of this happening is low due to the limited number of users who can log into the operating system.	
Recommendations	We recommend implementing procedures to monitor the integrity of database scripts and executables. In addition, file integrity software (e.g. Tripwire) should be purchased to automate the process of file integrity monitoring. Finally, the files to be monitored should be added to the Oracle security baseline.	

Cost Analysis	The cost to review the implications of making this change and implementing this item has been estimated to be $3,200 based on 20 hours of the database administrators time and $2,000 to purchase a license for file integrity software. The cost of adding this to the Oracle Security baseline has already been included in Finding #1.
Compensating Controls	Compensating controls are not necessary because it is reasonable to implement the recommendation that addresses this finding.

Finding 13: Oracle Audit Settings have not been configured appropriately.	**Risk Level**	Medium
	Checklist #	2.2.4.2
	Page References	37-38, 55-56, 68, 85
Control Objective	This control objective is designed to ensure that Oracle auditing has been enabled for a predetermined set of events.	
Risk	Failure to record audit data leads to the inability to identify and respond to security incidents.	
Recommendations	We recommend enabling auditing within Oracle. In addition, the audit settings used should be added to the Oracle security baseline.	
Cost Analysis	The cost to review the implications of making this change and implementing this item has been estimated to be $960 based on 16 hours of the database administrators time. The cost of adding this to the Oracle Security baseline has already been included in Finding #1.	
Compensating Controls	Compensating controls are not necessary because it is reasonable to implement the recommendation that addresses this finding.	

Finding 14: A database configuration parameter, SQL92 Security, has not been enabled.	**Risk Level**	Low
	Checklist #	2.2.4.5
	Page References	40, 68, 85

Control Objective	This control objective is designed to ensure that SELECT privileges are required to execute an update or delete on table values.
Risk	"This parameter will enforce the requirement that a user must have SELECT privilege on a table in order to be able to execute UPDATE and DELETE statements using WHERE clauses on a given table." (Oracle Database Security Benchmark v1.0, p. 12) Users could gain access to information they don't have a need to know should this setting not be set. Users are not likely to take advantage should this not be configured appropriately.
Recommendations	We recommend that the database configuration parameter SQL92_Security be configured on DBSRV1. In addition, this setting should be added to the Oracle security baseline.
Cost Analysis	The cost to implement this item has been estimated to be $120 based on two hours of the database administrators' time. The cost of adding this to the Oracle Security baseline has already been included in Finding #1.
Compensating Controls	Compensating controls are not necessary because it is reasonable to implement the recommendation that addresses this finding.

Finding 15: Permissions to access database packages are not configured appropriately.	**Risk Level**	Medium
	Checklist #	2.2.4.11
	Page References	44-45, 63-64, 68, 86
Control Objective	This control objective is designed to ensure that the access to packages that provide additional capabilities have not been granted to PUBLIC.	
Risk	Access to the packages provides users with additional privileges that may or may not be necessary for their job function. Unnecessary access to these packages provides privileges that are not required and could be exploited. Use of these packages is complex and the ability to work outside of the application interface is limited, therefore the likelihood of exploitation is low.	
Recommendations	We recommend revoking execute privileges from PUBLIC to the packages identified in the checklist. In addition, this setting should be part of the Oracle security checklist.	

Cost Analysis	The cost to review the implications and implement this item has been estimated to be $1,440 based on 24 hours of the database administrators' time. The cost of adding this to the Oracle Security baseline has already been included in Finding #1.
Compensating Controls	Compensating controls are not necessary because it is reasonable to implement the recommendation that addresses this finding.

5 Appendix A – Init.ora File

```
#
# $Header: initx.orc 12-jun-97.09:14:56 hpiao Exp $ Copyr (c) 1992 Oracle
#

# include database configuration parameters
ifile                           = /u01/app/oracle/admin/prd/pfile/configprd.ora

rollback_segments               = (r01,r02,r03,r04,r05,r06,r07,r08,r09,r10)
# rollback_segments             = (r01,r02,r03,r04)

###########################################################################
#
# Example INIT.ORA file
#
# This file is provided by Oracle Corporation to help you customize
# your RDBMS installation for your site.  Important system parameters
# are discussed, and example settings given.
#
# Some parameter settings are generic to any size installation.
# For parameters that require different values in different size
# installations, three scenarios have been provided: SMALL, MEDIUM
# and LARGE.  Any parameter that needs to be tuned according to
# installation size will have three settings, each one commented
# according to installation size.
#
# Use the following table to approximate the SGA size needed for the
# three scenarious provided in this file:
#
#                -------Installation/Database Size------
#                 SMALL         MEDIUM         LARGE
#  Block        2K    4500K          6800K          17000K
#  Size         4K    5500K          8800K          21000K
#
# To set up a database that multiple instances will be using, place
# all instance-specific parameters in one file, and then have all
# of these files point to a master file using the IFILE command.
# This way, when you change a public
# parameter, it will automatically change on all instances.  This is
# necessary, since all instances must run with the same value for many
# parameters. For example, if you choose to use private rollback segments,
# these must be specified in different files, but since all gc_*
# parameters must be the same on all instances, they should be in one file.
#
# INSTRUCTIONS: Edit this file and the other INIT files it calls for
# your site, either by using the values provided here or by providing
# your own.  Then place an IFILE= line into each instance-specific
# INIT file that points at this file.
###########################################################################
##
# Disable system triggers for the duration of the maintenance operation.
# _system_trig_enabled=false
# job_queue_processes = 0
```

```
# aq_tm_processes = 0

# Following is fix for ORA-600 [729] [1968] [space leak] error.
event = "10262 trace name context forever, level 102400"
O7_dictionary_accessibility = false
resource_limit = true                    # 17-May-1999
dblink_encrypt_login = true
remote_dependencies_mode = signature                    # 12-Jan-2003

optimizer_mode = choose
remote_login_passwordfile = none
db_domain = .sjk.com

#accessible directories for utl_file
utl_file_dir = /u01/app/oracle/local/batch/logs

job_queue_processes = 4
job_queue_interval = 60

# tuning parameters

sql92_security = true
db_files = 200
open_cursors = 150
max_enabled_roles = 120
open_links = 15
disk_asynch_io = false
dbwr_io_slaves = 2
compatible = 8.1.7.0.0


# db_file_multiblock_read_count = 8                    # SMALL
# db_file_multiblock_read_count = 16                   # MEDIUM
db_file_multiblock_read_count = 32                     # LARGE

# db_block_buffers = 200                               # SMALL
# db_block_buffers = 550                               # MEDIUM
# db_block_buffers = 3200                              # LARGE
# db_block_buffers = 4000       78.5 cache hit ration
# db_block_buffers = 8000       82% cache hit ration
# db_block_buffers = 10000      73.5 % 04-Nov-02
# db_block_buffers = 12000      79.53 % 06-May-03
# db_block_buffers = 20000      81.6  % 22-May-03
# db_block_buffers = 30000      87.5% 19-Jun-03
db_block_buffers = 40000

# shared_pool_size = 3500000                           # SMALL
# shared_pool_size = 6000000                           # MEDIUM
# shared_pool_size = 9000000                           # LARGE
# shared_pool_size = 65000000
shared_pool_size = 100000000
# shared_pool_size = 250000000       # For Java Install


java_pool_size = 65000000
# java_pool_size = 100000000         # For Java Install
```

```
log_checkpoint_interval = 10000
log_checkpoints_to_alert = YES

# processes = 50                                    # SMALL
# processes = 200                                   # LARGE
# processes = 300               # Upped from 200 on 02/12/02 due to ORA-00018
processes = 400                         # Upped from 300 on 10/21/03 due to ORA-00018

# dml_locks = 100                                   # SMALL
# dml_locks = 200                                   # MEDIUM
# dml_locks = 350               # ora-0055 error with 200
dml_locks = 500                                     # LARGE

log_buffer = 8192                                   # SMALL
# log_buffer = 32768                                # MEDIUM
# log_buffer = 163840                               # LARGE

# Obsolete with 8.1.7 upgrade
# sequence_cache_entries = 10                       # SMALL
# sequence_cache_entries = 30                       # MEDIUM
# sequence_cache_entries = 100                      # LARGE

# Obsolete with 8.1.7 upgrade
# sequence_cache_hash_buckets = 10                  # SMALL
# sequence_cache_hash_buckets = 23                  # MEDIUM
# sequence_cache_hash_buckets = 89                  # LARGE

audit_trail = true          # if you want auditing
timed_statistics = true     # if you want timed statistics
max_dump_file_size = 10240      # limit trace file size to 5 Meg each

log_archive_start = true      # if you want automatic archiving

# global_names = TRUE

# mts_dispatchers="ipc,1"
# mts_max_dispatchers=10
# mts_servers=1
# mts_max_servers=10
# mts_service=prd
# mts_listener_address="(ADDRESS=(PROTOCOL=ipc)(KEY=PNPKEY))"

# needed if running OPS
#
# PARALLEL_SERVER=TRUE

#Parameter added by Data Migration Assistant
SERVICE_NAMES = "prd.sjk.com" , prd
```

6 Compliance Table

Checklist #	Control Title	Compliance (Pass / Fail)	Risk Level
2.1.1	Change Management	Pass P	Medium
2.1.2	Oracle Security Baseline	Fail	High
2.1.3	Patch Management	Pass P	High
2.1.4	Account Creation / Termination	Pass P	High
2.1.5	Auditing / Logging / Monitoring	Fail	Medium
2.1.6	Backup Procedures	Pass P	High
2.1.7	Disaster Recovery Procedures	Pass P	Medium
2.1.8	Incident Response Procedures	Fail	Medium
2.1.9	Risk Assessment	Fail	Medium
2.2.1.1	Authorization	Pass P	Low
2.2.1.2	Default Accounts / Passwords	Fail	High
2.2.1.3	Blank Passwords	Pass P	Medium
2.2.1.4	Inactive Accounts	Pass P	Low
2.2.1.5	Shared Accounts	Pass P	Medium
2.2.1.6	“Public” Permissions	Fail	High
2.2.1.7	Remote OS Authentication	Pass P	Low
2.2.1.8	Password Settings	Pass P	High
2.2.1.9	Account Lockout	Pass P	High
2.2.2.1	Listener Patches	Pass P	High
2.2.2.2	TNS Listener Password	Pass P	Medium
2.2.2.3	Listener Admin Restrictions	Fail	Low
2.2.2.4	Listener Audit Settings	Fail	Medium
2.2.2.5	Unused Listener Services	Fail	Low
2.2.2.6	Listener Ports	Fail	Low
2.2.3.1	Tru64 Patches	Pass P	High
2.2.3.2	Tru64 Audit Settings	Pass P	Medium
2.2.3.3	Oracle Account & Group	Pass P	High
2.2.3.4	Database file permissions.	Fail	Low
2.2.3.5	Database file Integrity	Fail	Low
2.2.4.1	Oracle Patches	Pass P	High
2.2.4.2	Oracle Audit Settings	Fail	Medium
2.2.4.3	Database Link Settings	Pass P	Medium
2.2.4.4	Trace Files	Pass P	Low
2.2.4.5	SQL92 Security	Fail	Low
2.2.4.6	Views	Pass P	Medium

Checklist #	Control Title	Compliance (Pass / Fail)	Risk Level
2.2.4.7	With Admin	Pass P	Medium
2.2.4.8	With Grant Privileges	Pass P	Medium
2.2.4.9	Select Any Table Privilege	Pass P	Low
2.2.4.10	Audit System Privilege	Pass P	Low
2.2.4.11	Package Access	Fail	Medium
2.2.4.12	Data Dictionary	Pass P	Low

7 References

"Oracle Audit Checklist". <http://www.auditnet.org/docs/Oracle%20Audit%20Checklist.pdf> (15 December 2003).

"Oracle DB Technical Audit Program". <http://www.auditnet.org/docs/Oracle%20DB%20Technical%20Audit%20Program.pdf> (17 December 2003).

"Oracle Database Security Benchmark v1.0". 2003. <http://www.cisecurity.org/tools2/Oracle/OracleBenchmark.pdf> (17 December 2003).

"Oracle Database Listener Security Guide". March 2003. <http://www.integrigy.com/info/Integrigy_OracleDB_Listener_Security.pdf> (15 December 2003).

"A Security Checklist for Oracle 9i". <http://otn.Oracle.com/deploy/security/Oracle9i/pdf/9i_checklist.pdf> (15 December 2003).

"Database Security in Oracle 8i". 1999. <http://technet.Oracle.com/deploy/security/pdf/oow99/dbswp86.pdf> (15 December 2003).

"Oracle 8i Administrator's Reference Release 3 (8.1.7) Compaq Tru64 Unix". August 2001. <http://download.Oracle.com/docs/pdf/A85347_01.pdf> (15 December 2003).

"Oracle Advanced Security Administrator's Guide Release 8.1.7". Sept. 2001. <http://otn.Oracle.com/docs/deploy/security/pdf/a85430_01.pdf> (15 December 2003).

"Oracle 8i Installation Guide Release 3 (8.1.7) for Compaq Tru64 Unix". August 2001. <http://download.Oracle.com/docs/pdf/A85472_01.pdf> (15 December 2003).

Finnigan, Pete. "A Simple Oracle Host-Based Scanner". December 2001. <http://www.securityfocus.com/infocus/1522> (23 December 2003).

Finnigan, Pete. "Exploiting and Protecting Oracle". August 2001. <http://www.pentest.co.uk/documents/Oracle-security.pdf> (15 December 2003).

Finnigan, Pete. "Introduction to Simple Oracle Auditing". April 2003. <http://www.securityfocus.com/infocus/1689> (23 December 2003).

Finnigan, Pete. "Oracle Database Checklist". <http://www.sans.org/score/checklists/Oracle_Database_Checklist.pdf> (17 December 2003).

Newallis, Richard. "Database Security 101: Preventing Espionage and Sabotage". <http://www.geocities.com/ckempster/wpapers/Oracle/databasesecurity101.pdf> (15 December 2003).

Newman, Aaron. "Hack Proofing Oracle Databases". <http://www.appsecinc.com/presentations/Oracle_security.pdf> (15 December 2003).

Plusnina, Svetlana. "Oracle Database Audit Program". January 2000. <http://www.auditnet.org/docs/Oracle%20Database%20Audit%20Program.doc> (15 December 2003).

Smith, Howard. "Hack Proofing Oracle". <http://archives.neohapsis.com/archives/ntbugtraq/2002-q3/0095.html> (15 December 2003).

Last Updated: September 21st, 2017

Upcoming Training

Community SANS Virginia Beach AUD507 **	**Virginia Beach, VA**	**Nov 27, 2017 - Dec 01, 2017**	**Community SANS**
SANS London February 2018	**London, United Kingdom**	**Feb 05, 2018 - Feb 10, 2018**	**Live Event**
SANS 2018	**Orlando, FL**	**Apr 03, 2018 - Apr 10, 2018**	**Live Event**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**