

Interested in learning more about security?

SANS Institute Security Consensus Operational Readiness Evaluation This checklist is from the SCORE Checklist Project. Reposting is not permitted without express, written permission.

Oracle Database Security Checklist

Copyright SANS Institute Author Retains Full Rights

Oracle Database Checklist

Prepared by Pete Finnigan

References:

Oracle security step-by-step – A survival guide for Oracle security – Pete Finnigan - SANS Press – April 2004 (version 1.0 and version 2.0) Links to many useful papers and presentations about Oracle security – <u>http://www.petefinnigan.com/orasec.htm</u> Oracle security website <u>http://otn.oracle.com/deploy/security</u> Oracle Corporation main page <u>http://www.oracle.com</u> Customer support site <u>http://metalink.oracle.com</u> Security alerts http://otn.oracle.com/deploy/security/alerts.htm

Introduction:

This checklist is to be used to audit an Oracle database installation. This checklist is just that "a checklist" and does not contain any specific SQL or shell commands because it is intended to be just a list rather than a "how to" document otherwise. It is also important that the Oracle database is not checked in isolation and the surrounding elements such as the operating system used, the network configuration, web access, application servers and clients are considered.

Whilst every effort has been made to ensure that this checklist is as complete and comprehensive as possible new issues and vulnerabilities are found every day therefore don't rely on it to be all encompassing. Regularly check for updates of this list.

Elements to be considered prior to applying this checklist:

- Host Operating System Although this checklist includes items that specifically relate to the operating system hosting the Oracle installation they are included because they have a direct effect on Oracle. It is imperative that the host operating system is secured before any applications (in this case Oracle). The same applies to network components and other applications hosted on the same servers. Please consult other S.C.O.R.E documents (<u>http://www.sans.org/score</u>), center for internet security (CIS) benchmarks and tools (<u>http://cisecurity.org</u>) and SANS step-by-step guides (<u>http://sore.sans.org</u>) for more information.
- *Procedural* It is important to also consider physical security of the servers hosting the Oracle database and also to employ security procedures and policies and to develop standards for change and control.
- Findings and data sensitivity Establish the sensitivity of the data stored within the Oracle database and establish *rules* for reporting any security findings back to the organisation. This should take into account availability, confidentiality and the integrity of the data. This is important to be able to place any findings within the correct context when reporting back results of an audit.

- Practicality of the checklist This list is the culmination of the knowledge of many Oracle database security practitioners and as such includes every issue thought to be relevant to *somebody*. To some organisations some items are important to be fixed and to others not relevant because of mitigating circumstances. Oracle can be configured in many differing ways and this affects how it is secured. The list has been provided with severity levels to allow the audit to be conducted to a specified level and also includes OS and Oracle versions relevancies.
- Oracle database security standards This checklist could also be used to define a company standard for securing Oracle.

Before using this checklist to review an Oracle database installation it is important to understand the use to which the Oracle database and applications will be put. How the database is used can have a direct effect on how this list is read and interpreted. Oracle is a complicated beast to configure in any multitude of guises and checks and solutions that are relevant for one installation and type of application will conflict with another. Practicality is called for!

Checklist:

Before presenting the checklist a few words about what the columns mean. The *action* column indicates broad sections that checks are grouped into and also includes the action references indicated in the Oracle security step-by-step guide. The severity levels are set between 1 and 5 (1 indicating the highest level). These levels were reached by consensus during the writing of the *step-by-step*. The O/S column identifies whether *Unix* or *Windows* or both can be checked. The *Oracle version* column indicates the relevant Oracle installation and finally the *default install* column indicates whether the issue can be considered after a default installation. For ease of identification all of the highest severity issues are indicated by being greyed out.

Action	Description	Severity Level	O/S	Oracle Version	Default Install
0.	Planning and Risk assessment				
0.1	Identify and patch known and reported Vulnerabilities	1	ALL	ALL	YES
0.2	Identify and record software (Oracle and OS and Applications) versions and patch levels on the System	1	ALL	ALL	YES
0.3	Install only the database features that are needed	1	ALL	ALL	YES
0.4	Record database configuration and store securely	2	ALL	ALL	YES
0.5	Record database security configuration and store securely	2	ALL	ALL	YES
0.6	Review database security procedures and policies	2	ALL	ALL	YES
0.7	Store copies of the media used to build Oracle database off site	3	ALL	ALL	YES
0.8	Consider physical location of servers	2	ALL	ALL	YES
0.9	Define secure database / application architecture	3	ALL	ALL	YES
1.	Host Operating System security Issues				
1.1.1	Check owner of Oracle software owns all files in \$ORACLE_HOME/bin	1	ALL	ALL	YES
1.1.2	Lock Oracle software owner account	1	ALL	ALL	YES
1.1.3	Do not name Oracle software owner account oracle	2	ALL	ALL	YES
1.1.4	Limit access to software owner account	2	Unix	ALL	YES
1.1.5	Use separate owners for different components of Oracle such as listener, intelligent agent and database.	2	ALL	ALL	YES
1.2.1	Check file permissions in \$ORACLE_HOME/bin	1	Unix	ALL	YES
1.2.2	Check umask value	1	Unix	ALL	YES

1.2.3	Check owner and group for all files in \$ORACLE_HOME	1	Unix	ALL	YES
1.2.4	Set file system type, user name, group name and file permission issues for Windows	1	Win	ALL	YES
1.2.5	Location of temp directories pointed at by TMP_DIR and TMPDIR	1	Unix	ALL	YES
1.2.6	Check windows groups used for ORACLE_HOME and ORACLE_BASE	1	Win	ALL	YES
1.3.1	Review membership of OSDBA	1	ALL	ALL	YES
1.3.2	Ensure Oracle is not in root group	1	Unix	ALL	YES
1.3.3	Don't use the name <i>dba</i> for the OSDBA group	1	Unix	ALL	YES
1.3.4	Don't use the name ORA DBA for the OSDBA group on Windows	2	Win	ALL	YES
1.4.1	Check trace file permissions	3	ALL	ALL	0
1.4.2	Remove <i>tkprof</i> from production database	3	ALL	ALL	YES
1.4.3	Remove the <i>otrace</i> utility	2	ALL	ALL	YES
1.4.4	Check permissions of the datafiles	1	ALL	ALL	YES
1.4.5	Monitor Oracle log files	3	ALL	ALL	TLO
1.4.6	Check for sensitive temporary files	2	ALL	ALL	
1.4.7	Check for tertiary trace files	2	ALL	ALL	
1.4.7	Check for remote data access files (RDA)	3	ALL	ALL	
					VEC
1.4.9	Raw device permissions	1	Unix	ALL	YES
1.5.1	Usernames and passwords in process list	1	Unix	ALL	
1.5.2	Restrict the <i>ps</i> command	2	Unix	ALL	YES
1.5.3	Search shell history files for usernames and passwords	2	Unix	ALL	
1.6.1	Secure network transmissions	3	ALL	ALL	
1.6.2	Encrypt data transmissions	3	ALL	ALL	
1.6.3	Secure password transmission on the server	1	ALL	ALL	YES
1.6.4	Secure password transmission on the client	1	ALL	ALL	YES
1.6.5	JDBC thin driver transmissions – ensure minimum permissions of connections used	1	ALL	ALL	YES
1.7.1	Permissions on Oracle SUID and SGID files	3	Unix	ALL	YES
1.7.2	Check for non Oracle SUID and SGID files in \$ORACLE_HOME	3	Unix	ALL	
1.8.1	Audit environment variables for usernames and password	3	ALL	ALL	
1.8.2	Audit the machine for scripts containing usernames and passwords	2	ALL	ALL	
1.8.3	Audit cron for usernames and passwords	2	Unix	ALL	
1.8.4	Audit client machines for configuration files containing usernames and passwords	2	ALL	ALL	
1.8.5	Remove database creation scripts	2	ALL	ALL	YES
1.9.1	Utilize O/S auditing facilities	2	ALL	ALL	YES
1.9.2	Save log files to a separate server using Syslog or Windows event viewer	2	ALL	ALL	YES
1.9.3	Integrity check O/S files used by Oracle	2	Unix	ALL	YES
1.9.4	Consider using host based IDS	3	ALL	ALL	_
1.9.5	Review expected processes regularly	2	ALL	ALL	
1.10.1	Check control file permissions	2	ALL	ALL	YES
1.11.1	Confirm who is creating trace files	3	ALL	ALL	
1.11.2	Audit trace files for attempts to read database internal structures	3	ALL	ALL	
1.11.3	Ensure no user has ALTER SESSION and ALTER SYSTEM privileges	1	ALL	ALL	YES
1.12.1	Audit for export file existence	1	ALL	ALL	120
1.12.1	Changing database passwords after full import	1	ALL	ALL	
1.12.2	Locate archive log files and check no user except software owner can read them	2	ALL	ALL	
1.13.1	Save archive log files to disk and purge	2	ALL	ALL	
1.13.2	Audit external tables used	2	ALL	>= 9i	
1.14.1		2	ALL	>= 9i	YES
1.15.1	Restrict access to native PL/SQL compilation Be aware of key files containing hashes or passwords or other sensitive information	3	ALL	>= 9i ALL	YES
1.10		3	ALL	ALL	IES

1.17.1	Password protected listener can be shut down	3	Win	ALL	
2	Oracle Authentication				
2.1.1	Audit database users activities	3	ALL	ALL	
2.1.2	Audit application database logins	3	ALL	ALL	
2.1.3	Audit users database passwords	2	ALL	>= 8	YES
2.1.4	Establish a policy that prevents users from sharing account ID's	2	ALL	ALL	
2.1.5	Use proxy authentication to help resolve SSO issues	3	ALL	>= 8	
2.2.1	Audit default database accounts	1	ALL	ALL	YES
2.2.2	Add password management for default accounts	1	ALL	ALL	YES
2.2.3	Audit <i>internal</i> alias login	2	ALL	>= 8i	YES
2.2.4	Audit non database Oracle passwords	2	ALL	ALL	YES
2.2.5	Change sys password	1	ALL	ALL	YES
2.2.6	Change system password	1	ALL	ALL	YES
2.2.7	Create business process to audit default accounts regularly	2	ALL	ALL	
2.2.8	Disable remote login password file	2	ALL	ALL	YES
2.2.9	Check use of system tablespace as default	3	ALL	ALL	YES
2.2.10	Modify Oracle scripts for default accounts that are used	1	ALL	ALL	YES
2.2.10	Audit known default role passwords	1	ALL	ALL	YES
2.3.1	Audit users accounts for passwords same as username	2	ALL	ALL	120
2.3.1	Audit users accounts for weak passwords	2	ALL	ALL	
2.3.2	Lock dormant database accounts and remove after time delay	3	ALL	ALL	
2.3.3 2.3.4	Stop personal data exposure on users accounts	5	ALL	ALL	
2.3.4 2.3.5	Use obfuscated naming convention for users accounts	5	ALL	ALL	
2.3.5 2.3.6	Use LDAP for external authentication	5	ALL	>= 9i	
2.3.0 2.3.7		4	ALL	>= 9i ALL	
	Review database accounts, ensuring they belong to business users.				
2.4.1	Secure remote password login file	3	ALL	ALL	YES
2.5.1	Change SID and service name for third-party applications	4	ALL	ALL	YES
2.6.1	Audit third party and home grown applications authentication systems	3	ALL	ALL	
3.	Oracle Access Controls	<u> </u>	A.L.I.	A.I. I.)//50
3.1.1	Audit utl_file_dir parameter	3	ALL	ALL	YES
3.1.2	Audit dbms_backup_restore package permissions	3	ALL	ALL	YES
3.1.3	Audit Java access to the O/S	2	ALL	>= 8	YES
3.1.4	Be aware of how Java and Oracle interact	2	ALL	>= 8	YES
3.1.5	Secure Oracle Con Text	3	ALL	>= 8	YES
3.1.6	Remove oo4o if not needed	2	ALL	>= 7	YES
3.2.1	Secure ALL_USERS view	3	ALL	ALL	YES
			ALL	ALL	YES
3.2.2	Secure all ALL_% views	4			YES
3.2.2 3.3.1	Make extproc secure	2	ALL	>= 8	
3.2.2 3.3.1 3.4.1	Make <i>extproc</i> secure Understand Data Access Descriptor administration	2 4	ALL ALL	9iAS	YES
3.2.2 3.3.1 3.4.1 3.5.1	Make <i>extproc</i> secure Understand Data Access Descriptor administration Secure access to catalog roles	2 4 3	ALL ALL ALL	9iAS ALL	YES YES
3.2.2 3.3.1 3.4.1 3.5.1 3.5.2	Make <i>extproc</i> secure Understand Data Access Descriptor administration Secure access to catalog roles Secure access to dba role views	2 4	ALL ALL ALL ALL	9iAS ALL ALL	YES YES YES
3.2.2 3.3.1 3.4.1 3.5.1 3.5.2 3.5.3	Make <i>extproc</i> secure Understand Data Access Descriptor administration Secure access to catalog roles Secure access to dba role views Password protect admin roles	2 4 3	ALL ALL ALL	9iAS ALL ALL ALL	YES YES
3.2.2 3.3.1 3.4.1 3.5.1 3.5.2	Make <i>extproc</i> secure Understand Data Access Descriptor administration Secure access to catalog roles Secure access to dba role views	2 4 3 3	ALL ALL ALL ALL	9iAS ALL ALL	YES YES YES
3.2.2 3.3.1 3.4.1 3.5.1 3.5.2 3.5.3	Make <i>extproc</i> secure Understand Data Access Descriptor administration Secure access to catalog roles Secure access to dba role views Password protect admin roles Check role hierarchy depth	2 4 3 3 4	ALL ALL ALL ALL ALL	9iAS ALL ALL ALL	YES YES YES
3.2.2 3.3.1 3.4.1 3.5.1 3.5.2 3.5.3 3.5.4	Make <i>extproc</i> secure Understand Data Access Descriptor administration Secure access to catalog roles Secure access to dba role views Password protect admin roles Check role hierarchy depth Adopt role naming conventions	2 4 3 3 4 4	ALL ALL ALL ALL ALL ALL	9iAS ALL ALL ALL ALL	YES YES YES
3.2.2 3.3.1 3.4.1 3.5.1 3.5.2 3.5.3 3.5.4 3.5.5 3.5.6	Make <i>extproc</i> secure Understand Data Access Descriptor administration Secure access to catalog roles Secure access to dba role views Password protect admin roles Check role hierarchy depth Adopt role naming conventions Create a role to manage users accounts	2 4 3 3 4 4 5	ALL ALL ALL ALL ALL ALL ALL	9iAS ALL ALL ALL ALL ALL ALL	YES YES YES YES
3.2.2 3.3.1 3.4.1 3.5.1 3.5.2 3.5.3 3.5.4 3.5.5 3.5.6 3.5.6 3.6.1	Make <i>extproc</i> secure Understand Data Access Descriptor administration Secure access to catalog roles Secure access to dba role views Password protect admin roles Check role hierarchy depth Adopt role naming conventions Create a role to manage users accounts Check database in archivelog mode (if required)	2 4 3 4 4 5 5	ALL ALL ALL ALL ALL ALL ALL ALL ALL	9iAS ALL ALL ALL ALL ALL ALL ALL	YES YES YES YES YES
3.2.2 3.3.1 3.4.1 3.5.1 3.5.2 3.5.3 3.5.4 3.5.5 3.5.6	Make <i>extproc</i> secure Understand Data Access Descriptor administration Secure access to catalog roles Secure access to dba role views Password protect admin roles Check role hierarchy depth Adopt role naming conventions Create a role to manage users accounts	2 4 3 4 4 5 5 3	ALL ALL ALL ALL ALL ALL ALL ALL	9iAS ALL ALL ALL ALL ALL ALL ALL	YES YES YES YES

16.65 16.66Check that light and the period large start to true3ALLALLVES36.67Check that log, and the period large start of the period	3.6.4	Check core_dump_dest is valid	4	ALL	ALL	YES
5.6.6 Check that in G_ archive_start is set to thue 4 ALL YES 3.6.0 Check that os, authent is set to false 1 ALL ALL ALL YES 3.6.11 Check that remote, os, authent is set to false 1 ALL ALL ALL YES 3.6.12 Check that remote, os, authent is set to false 1 ALL ALL ALL YES 3.6.12 Check that remote, os, authent is set to false 1 ALL ALL ALL YES 3.6.13 Periodically confirm parameters in database are the same as the configuration file 3 ALL ALL ALL YES 3.6.11 Check that famole, jestemic is aution aread by the software owner. 2 ALL ALL ALL YES 3.6.11 Check for on on sys objects in system tablespace 1 ALL ALL YES 3.6.11 Check for on on sys objects in system tablespace 1 ALL AL						
5.6.7 Check that max_enabled_roles is set correctly 3 ALL <						
5.6.8 Check that os_authent_prefix is set to "(null string). 2 ALL ALL ALL YES 3.6.9 Check that or_dictionary_accessibility is set to false 1 ALL ALL YES 3.6.11 Check that remote, os_authent is set to false 3 ALL ALL YES 3.6.12 Check that remote, os_authent is set to false 1 ALL ALL YES 3.6.13 Periodically confirm parameters in database are the same as the configuration file 3 ALL ALL YES 3.6.14 Audit use of IFILE and the contents of files pointed to by IFILE 3 ALL YES 3.6.16 Check that remote, listener is null 3 ALL YES 3.6.16 Check that remote, listener is null 3 ALL YES 3.6.17 Check that seme access poicy privilege is revoked 2 ALL ALL YES 3.6.16 Check that seme access poicy privilege is revoked 2 ALL ALL YES 3.6.11 Check that seme access poicy privilege is revoked 1 ALL ALL YES 3.7.1 Check that seme access poicy pri						
36.9 Check that oz_roles is set to false 4 ALL ALL YES 36.10 Check that oz_roles is set to false 3 ALL ALL YES 36.11 Check that remote, os_authent is set to false 3 ALL ALL YES 36.12 Check that remote, os_roles is set to false 3 ALL ALL YES 36.13 Check that remote, isterer is null 3 ALL ALL YES 36.16 Check that file and splite can only be written to and read by the software owner. 2 ALL ALL YES 36.16 Check that file and splite can only be written to and read by the software owner. 2 ALL ALL YES 36.16 Check that pfile and parameters 3 ALL YES 3 3 ALL YES 36.17 Check that pfile and parameters 2 ALL ALL YES 3 3 ALL YES 37.1 Check for prology synchesin system tables 1 ALL YES 3 3 ALL YES 38.2 Check for priviloges granted 1 A						
5.6.10 Check that 07_dictionary_accessibility is set to false 1 ALL ALL ALL ALL YES 3.6.11 Check that remote, os_notes is set to false 1 ALL ALL ALL YES 3.6.12 Check that remote, os_notes is set to false 1 ALL ALL YES 3.6.13 Periodically confirm parameters in database are the same as the configuration file 3 ALL ALL ALL YES 3.6.16 Check that remote, listener is null 3 ALL YES 3 ALL YES 3.6.16 Check that exempt access policy privilege is revoked 2 ALL ALL YES 3.6.11 Check that exempt access policy privilege is revoked 2 ALL ALL YES 3.6.10 Check for sOurs work access policy privilege is revoked 1 ALL ALL YES 3.6.11 Check for users work access policy privilege is revoked 1 ALL ALL YES 3.6.11 Check for users or roles granted work access policy privilege is revoked 1 ALL ALL YES 3.8.2 Check for privileges granted						
3.6.11 Check that remote os. Joles is set to false 3 ALL ALL ALL ALL ALL YES 3.6.12 Check that remote, os. Joles is set to false 3 ALL >= 91 3.6.13 Periodically confirm parameters in database are the same as the configuration file 3 ALL >= 91 3.6.15 Check that remote, listener is null and the contents of files pointed to by IFILE 3 ALL >= 91 3.6.16 Check that remote, listener is null and remote pointed to by IFILE 3 ALL >= 91 3.6.16 Check that refine and splite can only be written to and read by the software owner. 2 ALL ALL YES 3.6.11 Check that remote, losing parameters 2 ALL ALL YES 3.6.12 Check for rousers, who have dba privilege 1 ALL YES 3.6.11 Check for rousers, who have dba privileges granted 1 ALL ALL YES 3.8.2 Check for privileges granted 1 ALL ALL YES 3.8.4 Check for or privileges granted 1 ALL ALL YES						
5.612Check that remote $\sum_{n=1}^{\infty} objects is set to false1ALLALLVES3.613Periodically confirm parameters in database are the same as the configuration file3ALL>= 9iYES3.614Audit use of IFILE and the contents of files pointed to by IFILE3ALL>= 9iYES3.615Check that remote jistener is null3ALL>= 9iYES3.616Check that remote provideg is revoked2ALLALLYES3.617Check that exempt access policy privileg is revoked2ALLALLYES3.618Check for const security standards2ALLALLYES3.619Check for on sys objects in system tablespace1ALLALLYES3.82Check for privileges granted ALL PRIVILEGES1ALLALLYES3.84Check for privileges granted WITH ADMIN2ALLALLYES3.85Check for privileges granted WITH ADMIN2ALLALLYES3.86Check for privileges granted WITH ADMIN2ALLALLYES3.87Check for privileges granted WITH ADMIN2ALLALLYES3.88Check for or Delests owned by privilege Users2ALLALLYES3.81Check for or SREATE LIBRARY* privilege3ALLALLYES3.81Audit access privileges on objects3ALLALLYES3.81Check for privileges on objects3ALL$						
3.1 Periodically confirm parameters in database are the same as the configuration file 3 ALL >= 9i 3.6.14 Audiu sed of IFLE and the contents of files pointed to by IFLE 3 ALL >= 9i 3.6.16 Check that remote_listener is null 3 ALL >= 9i YES 3.6.16 Check that exempt access policy privilege is revoked 2 ALL ALL YES 3.6.18 Check that exempt access policy privilege is revoked 2 ALL ALL YES 3.6.18 Check for on system tablespace 1 ALL ALL YES 3.8.1 Check for oursers who have dba privilege quanted 1 ALL ALL YES 3.8.2 Check for privileges granted "WITH ADMIN" 2 ALL ALL YES 3.8.3 Check for privileges granted "WITH ADMIN" 2 ALL ALL YES 3.8.4 Check for or privileges granted "WITH ADMIN" 2 ALL ALL YES 3.8.4 Check for privileges granted "WITH ADMIN" 2 ALL ALL YES 3.8.5 Check for oring atraneted 1 ALL						
3.6.14Audi use of IFILE and the contents of files pointed to by IFILE3ALL>= 9i3.6.15Check that pile and splite can only be written to and read by the software owner.2ALL>= 9iYES3.6.16Check that pile and splite can only be written to and read by the software owner.2ALL>= 9iYES3.6.17Check that zemery biologies is roycked2ALLALLYES3.6.18Check for on sys objects in system biolespace1ALLYES3.7.1Check for users or roles granted ALL PRIVILEGES1ALLYES3.8.2Check for privileges granted 'WITH ADMIN'2ALLALLYES3.8.3Check for privileges granted 'WITH GRANT'2ALLALLYES3.8.6Review system privileges granted 'WITH GRANT'2ALLALLYES3.8.7Check for privileges granted 'WITH GRANT'2ALLALLYES3.8.8Check for dipticipes owned by privileged users2ALLALLYES3.8.10Use roles to access granted data3ALLYES3.8.11Audi access privileges on objects3ALLALLYES3.8.11Audi access privileges on objects3ALLALLYES3.8.11Audi access privileges on objects3ALLALLYES3.8.11Audi access privileges on objects3ALLALLYES3.8.11Audi access privileges on objects3ALLA						IL3
3.6.16Check that remote, listener is null3ALL>= 9iYES3.6.16Check that prime and splite can only be written to and read by the software owner.2ALLALLYES3.6.17Check that exempt access policy privilege is revoked2ALLALLYES3.6.18Check ror SQL92 security standards2ALLALLYES3.6.19Check for SQL92 security standards2ALLALLYES3.6.11Check for users who have <i>dbe</i> privilege1ALLALLYES3.8.2Check for users or roles granted ALL PRIVILEGES1ALLALLYES3.8.4Check for privileges granted WITH ADMIN*2ALLALLYES3.8.5Check for privileges granted WITH AGANT*2ALLALLYES3.8.6Review system privileges granted WITH AGANT*2ALLALLYES3.8.7Check for direct access granted to tables and objects2ALLALLYES3.8.10Use roles to access underly in yikinged users3ALLALLYES3.8.11Audit access privileges onces2ALLALLYES3.8.12Use roles to access underlying database objects3ALLALLYES3.8.12Use roles to access underlying database objects3ALLALLYES3.8.12Use roles to access underlying database objects3ALLALLYES3.8.11Vidit access privileges on the XT pri						
3.6.16Check that pile and spile can only be written to and read by the software owner.2ALLALLYES3.6.17Check that zeemp taccess policy privilege is revoked2ALLALLYES3.6.18Check for cord locking parameters2ALLALLYES3.6.19Check for users who have dba privilege1ALLALLYES3.7.1Check for users or loles granted ALL PRIVILEGES1ALLALLYES3.8.2Check for users who have dba privilege1ALLALLYES3.8.3Check for privileges granted "WITH ADMIN"2ALLALLYES3.8.4Check for privileges granted "WITH APANT"2ALLALLYES3.8.5Check for privileges granted "WITH APANT"2ALLALLYES3.8.7Check for grivileges granted "WITH APANT"2ALLALLYES3.8.8Check for grivileges granted "WITH APANT"2ALLALLYES3.8.9Check for GREATE LIBRARY" privilege1ALLALLYES3.8.10Use roles to access underlying database objects33ALLALLYES3.8.11Audit access privileges on objects3ALLALLYES3.8.12Use ringers to insert critical data3ALLALLYES3.8.11Audit access privileges2ALLALLYES3.8.12Use ringers to insert critical data3ALLALLYES<					-	VEC
3.6.17Check that exempt access policy privilege is revoked2ALL>= 9iYES3.6.18Check record locking parameters2ALLALLALLYES3.6.19Check for SQL92 security standards2ALLALLYES3.6.11Check for or sy objects in system tablespace1ALLALLYES3.8.1Check for users who have <i>dta</i> privilege1ALLALLYES3.8.2Check for privileges granted 'WITH ADMIN'2ALLALLYES3.8.4Check for privileges granted 'WITH GRANT'2ALLALLYES3.8.5Check for privileges granted 'WITH GRANT'2ALLALLYES3.8.6Review system privileges granted out of the system tables and objects2ALLALLYES3.8.9Check for direct access granted to tables and objects3ALLALLYES3.8.11Audit access privileges objects3ALLALLYES3.8.12Use inderify constraints3ALLALLYES3.8.13Use it gers to one of a once2ALLALLYES3.8.14Reviter users to one role at once2ALLALLYES3.8.15Check for CREATE_ADD privilege2ALLALLYES3.8.14Restrict users to one role at once2ALLALLYES3.8.15Check for CREATE_ADD privilege2ALLALLYES3.8.16Check f			3			
3.6.18Check for SOL29 security standards2ALLALLYES37.11Check for non sys objects in system tablespace1ALLALLYES38.11Check for users who have dba privilege1ALLALLYES38.21Check for users or noles granted ALL PRIVILEGES1ALLALLYES38.32Check for privileges granted 'WITH ADMIN'2ALLALLYES38.43Check for privileges granted 'WITH ADMIN'2ALLALLYES38.55Check for privileges granted 'WITH ADMIN'2ALLALLYES38.6Review system privileges granted 'WITH ADMIN'2ALLALLYES38.7Check for privileges granted 'WITH ADMIN'2ALLALLYES38.7Check for application objects owned by privileged users2ALLALLYES38.8Check for 'CREATE LIBRAR'' privilege1ALLALLYES38.11Audt access privileges on objects2ALLALLYES38.12Use ringers to insert critical data3ALLALLYES38.13User togers to insert critical data3ALLALLYES38.14Restrict Users to insert critical data3ALLALLYES38.14Restrict Users to insert critical data3ALLALLYES38.14Restrict Users to insert critical data3ALLALLYES38.15Check for C		Check that pile and spile can only be written to and read by the software owner.	2			
36.19Check for SQL92 sciurity standards2ALLALLYES37.1Check for on sys objects mystem tablespace1ALLALLYES38.1Check for users or loises granted ALL PRIVILEGES1ALLALLYES38.2Check for privileges granted 'WITH GRANT''2ALLALLYES38.4Check for privileges granted 'WITH GRANT''2ALLALLYES38.5Check for privileges granted 'WITH GRANT''2ALLALLYES38.6Review system privileges granted of WITH GRANT''2ALLALLYES38.7Check for direct access granted to tables and objects2ALLALLYES38.8Check for direct access granted to tables and objects3ALLALLYES38.10Use roles to access underlying database objects3ALLALLYES38.11Audit access privileges on objects3ALLALLYES38.12Use integrity constraints3ALLALLYES38.14Ves integrity constraints3ALLALLYES38.15Check for CREATE AND NECTORY privilege2ALLALLALL38.14Ves integrity constraints3ALLALLYES38.17Check for creater and once2ALLALLYES38.11Juse integrity constraints3ALLALLALLYES38.14Addit Exercity Privilege2<			2			
3.7.1Check for non sys objects in system tablespace1ALLALLYES $3.8.1$ Check for users who have dba privilege1ALLALLYES $3.8.2$ Check for privileges granted ALL PRIVILEGES1ALLALLYES $3.8.3$ Check for privileges granted VITH ADMIN*2ALLALLYES $3.8.4$ Check for privileges granted VITH AGNAT*2ALLALLYES $3.8.5$ Check for privileges granted VITH AGNAT*2ALLALLYES $3.8.6$ Revew system privileges granted VITH AGNAT*2ALLALLYES $3.8.6$ Check for privileges granted to tables and objects2ALLALLYES $3.8.6$ Check for direct access granted to tables and objects2ALLALLYES $3.8.9$ Check for direct ATE LIBRARY* privilege1ALLALLYES $3.8.11$ Audit access privileges to objects3ALLALLYES $3.8.12$ Use integrity constraints3ALLALLYES $3.8.13$ Use triggers to insert critical data3ALLALLYES $3.8.16$ Check for CREATE JDRARY* privilege2ALLALLALL $3.8.11$ Audit access prive privilege for privilege2ALLALLYES $3.8.13$ Use triggers to insert critical data3ALLALLYES $3.8.16$ Check for CREATE ANY DRECTORY privilege2ALLALLYES </td <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>						
3.8.1Check for users who have <i>dba</i> privilege1ALLALLYES3.8.2Check for privileges with ANY keyword granted1ALLALLYES3.8.3Check for privileges granted 'WITH GRANT'2ALLALLYES3.8.4Check for privileges granted 'WITH GRANT'2ALLALLYES3.8.5Check for privileges granted 'WITH GRANT'2ALLALLYES3.8.6Review system privileges granted 'WITH GRANT'2ALLALLYES3.8.7Check for direct access granted to tables and objects2ALLALLYES3.8.8Check for direct access granted to tables and objects2ALLALLYES3.8.9Check for direct access granted to tables and objects3ALLALLYES3.8.10Use roles to access underlying database objects3ALLALLYES3.8.11Audit access privileges on objects3ALLALLYES3.8.12Use integrity constraints3ALLALLYES3.8.13Use integrity constraints3ALLALLYES3.8.14Acti access privilege2ALLALLYES3.8.15Check for CREATE LIBRANTPrivilege2ALLALLYES3.8.14Acti access with "BECOME USER" privilege2ALLALLYES3.8.15Check for or cREATE LINP INTECTORY privilege2ALLALLYES3.9.1				· ·==		
3.8.2Check for users or roles granted ALL PRIVILEGES1ALLALLYES3.8.3Check for privileges granted WITH ADMIN"2ALLALLYES3.8.4Check for privileges granted WITH GRANT2ALLALLYES3.8.5Check for privileges granted WITH GRANT2ALLALLYES3.8.6Review system privileges granted WITH GRANT2ALLALLYES3.8.7Check for application objects owned by privileged users2ALLALLYES3.8.7Check for application objects owned by privilege1ALLALLYES3.8.8Check for "CREATE LIBRARY" privilege1ALLALLYES3.8.9Check for "CREATE LIBRARY" privilege2ALLALLYES3.8.11Audit access privileges on objects2ALLALLYES3.8.12Use Integrity constraints3ALLALLYES3.8.13Use trigers to insert critical data3ALLALLYES3.8.15Check for CREATE ANY DIRECTORY privilege2ALLALLYES3.8.16Check for CREATE ANY DIRECTORY privilege2ALLALLYES3.8.17Check for CREATE ANY DIRECTORY privilege2ALLALLYES3.9.1Audit EXTERNAL users2ALLALLYES3.9.2Check for CREATE ANY DIRECTORY privileges possible2ALLALLYES3.9.3Check for creamal						
3.8.3Check for privileges with ANY keyword granted1ALLALLYES3.8.4Check for privileges granted 'WITH ADMIN''2ALLALLALLYES3.8.5Check for privileges granted 'WITH GRANT'2ALLALLYES3.8.6Review system privileges granted to tables and objects1ALLALLYES3.8.7Check for direct access granted to tables and objects2ALLALLYES3.8.8Check for 'CREATE LIBRARY'' privilege1ALLALLYES3.8.9Check for 'CREATE LIBRARY'' privilege3ALLALLYES3.8.10Use roles to access underlying database objects3ALLALLYES3.8.11Audit access privileges on objects3ALLALLYES3.8.12Use Integrity constraints3ALLALLYES3.8.13Use triggers to insert critical data3ALLALLYES3.8.14Restrict users to one role at once2ALLALLYES3.8.16Check for CREATE JOB privilege2ALLALLYES3.8.17Check for external users who are <i>dba</i> 1ALLYES3.9.3Check for external users have the least privileges possible2ALLALL3.9.4Ensure external users have the least privileges possible2ALLALL3.9.5Do not use remote host based authentication2ALLALLYES3.9.4						
3.8.4 Check for privileges granted "WITH ADMIN" 2 ALL ALL YES 3.8.5 Check for privileges granted "WITH GRANT" 2 ALL ALL YES 3.8.6 Review system privileges granted to ables and objects 1 ALL YES 3.8.7 Check for direct access granted to tables and objects 2 ALL ALL YES 3.8.8 Check for direct access granted to tables and objects 2 ALL ALL YES 3.8.9 Check for direct access granted to tables and objects 2 ALL ALL YES 3.8.11 Audit access privileges on objects 3 ALL ALL YES 3.8.11 Just intigen to insert critical data 3 ALL ALL YES 3.8.12 Use Integrity constraints 3 ALL ALL YES 3.8.12 Use Integrity constraints 3 ALL ALL YES 3.8.13 Use triggers to one role at once 2 ALL ALL YES 3.8.14 Restrict users to one role at once 2 ALL ALL YES <tr< td=""><td></td><td></td><td>-</td><td></td><td></td><td></td></tr<>			-			
3.8.5Check for privileges granted "WITH GRANT"2ALLALLYES3.8.6Review system privileges granted1ALLALLALLYES3.8.7Check for application objects owned by privileged users2ALLALLALLYES3.8.8Check for direct access granted to tables and objects2ALLALLYES3.8.9Check for GREATE LIBRARY" privilege1ALLALLYES3.8.10Use roles to access underlying database objects3ALLALLYES3.8.11Audit access privileges on objects2ALLALLYES3.8.12Use Integrity constraints3ALLALLYES3.8.13Use Integrity constraints3ALLALLYES3.8.14Restrict users to one role at once2ALLALLYES3.8.15Check for CREATE ANY DIRECTORY privilege2ALLALLYES3.8.16Check for external users who are <i>dba</i> 1ALL>=010 gressYES3.9.2Check for external users who are <i>dba</i> 1ALLALLYES3.9.4Ensure external users have the least privilege sposible2ALLALLYES3.9.4Ensure external users have SYSDBA or SYSOPER1ALLALLYES3.10.1Revoke public execute privilege on <i>ull_tfap</i> 1ALLALLYES3.10.2Revoke public execute privilege on <i>ull_tfap</i> 1ALLALL<						
38.6Review system privileges granted1ALLALLYES3.8.7Check for application objects owned by privileged users2ALLALLALLYES3.8.8Check for direct access granted to tables and objects2ALLALLYES3.8.9Check for "CREATE LIBRARY" privilege1ALLALLYES3.8.10Use roles to access underlying database objects3ALLALLYES3.8.11Audit access privileges on objects2ALLALLYES3.8.12Use Integrity constraints3ALLALLYES3.8.13Use triggers to insert critical data3ALLALLALL3.8.14Restrict users to one role at once2ALLALLALL3.8.15Check for CREATE JOB privilege2ALLALLYES3.8.17Check for CREATE JOB privilege2ALLALLYES3.9.2Check for creaternal users who are dba1ALLYES3.9.3Check for external users who are dba1ALLYES3.9.4Ensure external users have the least privileges possible2ALLALLYES3.9.4Ensure external users have SYSDBA or SYSOPER1ALLALLYES3.9.4Check that no external thereit privilege on utl_file1ALLALLYES3.9.4Check that no external users have SYSDBA or SYSOPER1ALLALLYES3.9.4Check t						
3.8.7Check for application objects owned by privileged users2ALLALLYES3.8.8Check for direct access granted to tables and objects2ALLALLALLYES3.8.9Check for CREATE LIBRARY" privilege1ALLALLYES3.8.10Use roles to access underlying database objects3ALLALLYES3.8.11Audit access privileges on objects3ALLALLYES3.8.12Use triggers to insert critical data3ALLALLYES3.8.13Use triggers to one role at once2ALLALLYES3.8.14Restrict users to one role at once2ALLALLYES3.8.15Check for CREATE LIBRECTORY privilege2ALLALLYES3.8.16Check for CREATE JOB privilege2ALLALLYES3.9.1Audit EXTERNAL users2ALLALLYES3.9.2Check for external users who are <i>dba</i> 1ALLYES3.9.3Check for external users have the least privileges possible2ALLALLYES3.9.4Ensure external users have SYSDBA or SYSOPER1ALLALLYES3.10.2Revoke public execute privilege on <i>utl_ftip</i> 1ALLYESS3.10.3Revoke public execute privilege on <i>utl_ftip</i> 1ALLYESS3.10.4Revoke public execute privilege on <i>utl_ftip</i> 1ALLYESS3.10.4						
38.8Check for direct access granted to tables and objects2ALLALLYES38.9Check for "CREATE LIBRARY" privilege1ALLALLYES38.10Use roles to access underlying database objects3ALLALLYES38.11Audit access privileges on objects2ALLALLYES38.12Use Integrity constraints3ALLALLYES38.13Use triggers to insert critical data3ALLALLALL38.14Restrict users to one role at once2ALLALLALL38.15Check for CREATE ANY DIRECTORY privilege2ALLALLYES38.17Check for CREATE JOB privilege2ALL>=9iYES3.9.1Audit EXTERNAL users2ALLALLYES3.9.2Check for external users who have "ALL PRIVILEGES"1ALLALLYES3.9.3Check for external users have the least privilege spossible2ALLALLYES3.9.4Lastread users have the SYSOPER1ALLALLYES3.9.5Do not use remote host based authentication2ALLALLYES3.9.6Check that no external users have SYSOPER1ALLALLYES3.10.1Revoke public execute privilege on <i>utl_fitp</i> 1ALLALLYES3.10.3Revoke public execute privilege on <i>utl_fitp</i> 1ALLALLYES3.10.4Revoke public exec						
38.9Check for "CREATE LIBRARY" privilege1ALLALLYES3.8.10Use roles to access underlying database objects3ALLALLYES3.8.11Audit access privileges on objects2ALLALLYES3.8.12Use Integrity constraints3ALLALLALLYES3.8.13Use triggers to insert critical data3ALLALLALLALLALL3.8.14Restrict users to one role at once2ALLALLALLYES3.8.15Check for users with "BECOME USER" privilege2ALLALLYES3.8.16Check for CREATE JOB privilege2ALL>=9iYES3.8.17Check for cREATE JOB privilege2ALLYES3.9.1Audit EXTERNAL users2ALLALLYES3.9.2Check for external users who are <i>dba</i> 1ALLYES3.9.3Check for external users have the least privileges possible2ALLALLYES3.9.4Ensure external users have SYSDBA or SYSOPER1ALLALLYES3.10.1Revoke public execute privilege on <i>utl_tpp</i> 1ALLYESSt.7YES3.10.2Revoke public execute privilege on <i>utl_tpp</i> 1ALL>=8.1.7YES3.10.3Revoke public execute privilege on <i>utl_tpp</i> 1ALLYESSt.7YES3.10.4Revoke public privilege on <i>utl_tpp</i> 1ALLYESSt.7						YES
38.10Use roles to access underlying database objects3ALLALLYES3.8.11Audit access privileges on objects2ALLALLALLYES3.8.12Use Integrity constraints3ALLALLALLYES3.8.13Use triggers to insert critical data3ALLALLALLALL3.8.14Restrict users to one role at once2ALLALLALLALL3.8.15Check for CREATE ANY DIRECTORY privilege2ALLALLYES3.8.17Check for CREATE JOB privilege2ALL>=0igYES3.9.1Audit EXTERNAL users2ALLALLYES3.9.2Check for external users who are <i>dba</i> 1ALLYES3.9.3Check for external users have the least privileges possible2ALLALLYES3.9.4Ensure external users have SYSDBA or SYSOPER1ALLALLYES3.10.1Revoke public execute privilege on <i>utl_file</i> 1ALL>=8YES3.10.2Revoke public execute privilege on <i>utl_tcp</i> 1ALL>=8.1.7YES3.10.4Revoke public execute privilege on <i>utl_smp</i> 1ALLALLYES3.10.5Audit public execute privilege on <i>db_s_random</i> 2ALLALLYES3.10.6Revoke the public execute privilege on <i>dbms_random</i> 2ALLALLYES3.10.6Revoke the public execute privilege on <i>dbms_random</i> 2ALL						
3.8.11Audit access privileges on objects2ALLALLYES3.8.12Use Integrity constraints3ALLALLALLALLALL3.8.13Use triggers to insert critical data3ALLALLALLALLALL3.8.14Restrict users to one role at once2ALLALLALLALLALLALL3.8.15Check for users with "BECOME USER" privilege2ALLALLYESS.8.16Check for CREATE ANY DIRECTORY privilege2ALL>=9iYES3.8.16Check for CREATE JOB privilege2ALL>=10gYESYES3.9.1Audit EXTERNAL users2ALLALLYES3.9.2Check for external users who are <i>dba</i> 1ALLYES3.9.4Ensure external users have the least privilege possible2ALLALLYES3.9.4Ensure external users have the least privileges possible2ALLALLYES3.9.5Do not use remote host based authentication2ALLALLYES3.10.1Revoke public execute privilege on <i>utl_tcp</i> 1ALLYESS3.10.2Revoke public execute privilege on <i>utl_tcp</i> 1ALL>=8.1.7YES3.10.4Revoke public privilege on <i>utl_tcp</i> 1ALL>=8.1.7YES3.10.5Audit public execute privilege on <i>utl_smp</i> 1ALL>=8.1.7YES3.10.6Revoke the public execute privilege on <i>dbms_t</i>						
38.12Use Integrity constraints3ALLALL38.13Use triggers to insert critical data3ALLALL38.14Restrict users to one role at once2ALLALL38.15Check for users with "BECOME USER" privilege2ALLALL38.16Check for CREATE ANY DIRECTORY privilege2ALLALL38.17Check for CREATE JOB privilege2ALL>=9i39.1Audit EXTERNAL users2ALLALLYES3.9.2Check for external users who are <i>dba</i> 1ALLYES3.9.3Check for external users have the least privileges possible2ALLALLYES3.9.4Ensure external users have the least privileges possible2ALLALLYES3.9.5Do not use remote host based authentication2ALLALLYES3.9.6Check that no external users have SYSDBA or SYSOPER1ALLALLYES3.10.1Revoke public execute privilege on <i>utl_file</i> 1ALL>=8YES3.10.2Revoke public execute privilege on <i>utl_file</i> 1ALL>=8.1.7YES3.10.4Revoke public execute privilege on <i>utl_fitp</i> 1ALL>=8.1.7YES3.10.4Revoke public execute privilege on <i>utl_fitp</i> 1ALLYES3.10.5Audit public execute privilege on <i>utl_fitp</i> 1ALLYES3.10.6Revoke the public execute privilege on <i>dbms_random</i> .2ALL						
3.8.13Use triggers to insert critical data3ALLALL3.8.14Restrict users to one role at once2ALLALLALL3.8.15Check for users with "BECOME USER" privilege2ALLALLYES3.8.16Check for CREATE ANY DIRECTORY privilege2ALLALL>=9YES3.8.17Check for CREATE JOB privilege2ALL>=10gYES3.9.1Audit EXTERNAL users2ALLALLYES3.9.2Check for external users who are <i>dba</i> 1ALLALLYES3.9.3Check for external users have the least privileges possible2ALLALLYES3.9.4Ensure external users have the least privileges possible2ALLALLYES3.9.5Do not use remote host based authentication2ALLALLYES3.9.6Check that no external users have SYSDBA or SYSOPER1ALLALLYES3.10.1Revoke public execute privilege on <i>utl_tcp</i> 1ALL>=8.1.7YES3.10.3Revoke public execute privilege on <i>utl_ttp</i> 1ALL>=8.1.7YES3.10.4Revoke public execute privilege on <i>dbms_random.</i> 2ALLALLYES3.10.6Revoke the public execute privilege on <i>dbms_random.</i> 2ALLALLYES3.10.7Revoke the public execute privilege on <i>dbms_random.</i> 2ALLALLYES3.10.7Revoke the public execute privilege on <i>dbms_random.</i>			2			YES
3.8.14Restrict users to one role at once2ALLALL3.8.15Check for users with "BECOME USER" privilege2ALLALLYES3.8.16Check for CREATE ANY DIRECTORY privilege2ALL>=9iYES3.8.17Check for CREATE JOB privilege2ALL>=10gYES3.8.17Check for CREATE JOB privilege2ALL>=10gYES3.9.1Audit EXTERNAL users2ALLALLYES3.9.2Check for external users who are <i>dba</i> 1ALLALLYES3.9.3Check for external users have the least privileges possible1ALLALLYES3.9.4Ensure external users have the least privileges possible2ALLALLYES3.9.5Do not use remote host based authentication2ALLALLYES3.9.6Check that no external users have SYSDBA or SYSOPER1ALLALLYES3.10.1Revoke public execute privilege on <i>ut_file</i> 1ALL>=8.1.7YES3.10.3Revoke public execute privilege on <i>ut_file</i> 1ALL>=8.1.7YES3.10.4Revoke public privilege on <i>sys</i> owned packages.1ALL>=8.1.7YES3.10.5Audit public execute privilege on <i>dbms_random</i> .2ALLALLYES3.10.7Revoke the public execute privilege on <i>dbms_random</i> .2ALLALLYES3.10.7Revoke the public execute privilege on <i>dbms_random</i> .2 <t< td=""><td></td><td></td><td></td><td></td><td></td><td></td></t<>						
38.15Check for users with "BECOME USER" privilege2ALLALLYES38.16Check for CREATE ANY DIRECTORY privilege2ALL>=9iYES38.17Check for CREATE JOB privilege2ALL>=10gYES3.9.1Audit EXTERNAL users2ALLALLYES3.9.2Check for external users who are <i>dba</i> 1ALLALLYES3.9.3Check for external users who have "ALL PRIVILEGES"1ALLALLYES3.9.4Ensure external users have the least privileges possible2ALLALLYES3.9.5Do not use remote host based authentication2ALLALLYES3.9.6Check that no external users have SYSDBA or SYSOPER1ALLYES3.10.1Revoke public execute privilege on <i>utl_file</i> 1ALL>=8YES3.10.4Revoke public execute privilege on <i>utl_http</i> 1ALL>=8.1.7YES3.10.5Audit public execute privilege on <i>sys</i> owned packages.1ALL>=8.1.7YES3.10.6Revoke public execute privilege on <i>dbms_random</i> .2ALLALLYES3.10.7Revoke the public execute privilege			3			
38.16Check for CREATE ANY DIRECTORY privilege2ALL>=9iYES38.17Check for CREATE JOB privilege2ALL>=10gYES3.9.1Audit EXTERNAL users2ALLALLYES3.9.2Check for external users who are <i>dba</i> 1ALLALLYES3.9.3Check for external users who have "ALL PRIVILEGES"1ALLALLYES3.9.4Ensure external users have the least privileges possible2ALLALLYES3.9.5Do not use remote host based authentication2ALLALLYES3.9.6Check that no external users have SYSDBA or SYSOPER1ALLALLYES3.10.1Revoke public execute privilege on <i>utl_file</i> 1ALL>=8YES3.10.2Revoke public execute privilege on <i>utl_file</i> 1ALL>=8.1.7YES3.10.3Revoke public execute privilege on <i>utl_smtp</i> 1ALL>=8.1.7YES3.10.4Revoke public execute privilege on <i>sys</i> owned packages.1ALLALLYES3.10.5Audit public execute privilege on <i>dbms_random</i> .2ALLALLYES3.10.7Revoke the public exec			2			
3.8.17Check for CREATE JOB privilege2ALL $\Rightarrow=10g$ YES3.9.1Audit EXTERNAL users2ALLALLYES3.9.2Check for external users who are <i>dba</i> 1ALLALLYES3.9.3Check for external users who have "ALL PRIVILEGES"1ALLALLYES3.9.4Ensure external users have the least privileges possible2ALLALLYES3.9.5Do not use remote host based authentication2ALLALLYES3.9.6Check that no external users have SYSDBA or SYSOPER1ALLALLYES3.10.1Revoke public execute privilege on <i>utl_file</i> 1ALL>= 8YES3.10.2Revoke public execute privilege on <i>utl_filp</i> 1ALL>= 8.1.7YES3.10.3Revoke public execute privilege on <i>utl_smtp</i> 1ALL>=8.1.7YES3.10.4Revoke public execute privilege on <i>utl_smtp</i> 1ALL>=8.1.7YES3.10.5Audit public execute privilege on <i>dbms_random</i> .2ALLALLYES3.10.6Revoke the public execute privilege on <i>dbms_random</i> .2ALLALLYES3.10.7Revoke the public execute privilege on <i>dbms_lob</i> 1ALL>= 8iYES			2			
3.9.1Audit EXTERNAL users2ALLALLYES3.9.2Check for external users who are dba1ALLALLYES3.9.3Check for external users who have "ALL PRIVILEGES"1ALLALLYES3.9.4Ensure external users have the least privileges possible2ALLALLYES3.9.5Do not use remote host based authentication2ALLALLYES3.9.6Check that no external users have SYSDBA or SYSOPER1ALLALLYES3.10.1Revoke public execute privilege on utl_file1ALL>= 8YES3.10.2Revoke public execute privilege on utl_tcp1ALL>=8.1.7YES3.10.3Revoke public privilege on utl_smtp1ALL>=8.1.7YES3.10.4Revoke public privilege on sys owned packages.1ALLALLYES3.10.5Audit public execute privilege on dbms_random.2ALLALLYES3.10.6Revoke the public execute privilege on dbms_random.2ALLALLYES3.10.7Revoke the public execute privilege on dbms_lob1ALLYES			2		-	
3.9.2Check for external users who are <i>dba</i> 1ALLALLYES3.9.3Check for external users who have "ALL PRIVILEGES"1ALLALLYES3.9.4Ensure external users have the least privileges possible2ALLALLYES3.9.5Do not use remote host based authentication2ALLALLYES3.9.6Check that no external users have SYSDBA or SYSOPER1ALLYES3.10.1Revoke public execute privilege on <i>utl_file</i> 1ALL>= 8YES3.10.2Revoke public execute privilege on <i>utl_tcp</i> 1ALL>= 8.1.7YES3.10.3Revoke public execute privilege on <i>utl_smtp</i> 1ALL>=8.1.7YES3.10.4Revoke public execute privilege on <i>sys</i> owned packages.1ALL>=8.1.7YES3.10.5Audit public execute privilege on <i>dbms_random</i> .2ALLALLYES3.10.7Revoke the public execute privilege on <i>dbms_lob</i> 1ALL>=8iYES			2			
3.9.3Check for external users who have "ALL PRIVILEGES"1ALLALLYES3.9.4Ensure external users have the least privileges possible2ALLALLALLYES3.9.5Do not use remote host based authentication2ALLALLYES3.9.6Check that no external users have SYSDBA or SYSOPER1ALLYES3.10.1Revoke public execute privilege on <i>utl_file</i> 1ALL>= 8YES3.10.2Revoke public execute privilege on <i>utl_tcp</i> 1ALL>= 8.1.7YES3.10.3Revoke public execute privilege on <i>utl_smtp</i> 1ALL>=8.1.7YES3.10.4Revoke public execute privilege on <i>utl_smtp</i> 1ALL>=8.1.7YES3.10.5Audit public execute privilege on <i>sys</i> owned packages.1ALLYES3.10.6Revoke the public execute privilege on <i>dbms_random</i> .2ALLALLYES3.10.7Revoke the public execute privilege on <i>dbms_lob</i> 1ALL>=8iYES						
3.9.4Ensure external users have the least privileges possible2ALLALL3.9.5Do not use remote host based authentication2ALLALLYES3.9.6Check that no external users have SYSDBA or SYSOPER1ALLALLYES3.10.1Revoke public execute privilege on utl_file1ALL>= 8YES3.10.2Revoke public execute privilege on utl_tcp1ALL>=8.1.7YES3.10.3Revoke public execute privilege on utl_smtp1ALL>=8.1.7YES3.10.4Revoke public execute privilege on sys owned packages.1ALL>=8.1.7YES3.10.5Audit public execute privilege on dbms_random.2ALLALLYES3.10.7Revoke the public execute privilege on dbms_lob1ALL>=8iYES						
3.9.5Do not use remote host based authentication2ALLALLYES3.9.6Check that no external users have SYSDBA or SYSOPER1ALLALLYES3.10.1Revoke public execute privilege on utl_file1ALL>= 8YES3.10.2Revoke public execute privilege on utl_tcp1ALL>=8.1.7YES3.10.3Revoke public execute privilege on utl_http1ALL>=8.1.7YES3.10.4Revoke public execute privilege on utl_smtp1ALL>=8.1.7YES3.10.5Audit public execute privilege on sys owned packages.1ALL>=8.1.7YES3.10.6Revoke the public execute privilege on dbms_random.2ALLALLYES3.10.7Revoke the public execute privilege on dbms_lob1ALL>=8iYES						YES
3.9.6 Check that no external users have SYSDBA or SYSOPER 1 ALL ALL YES 3.10.1 Revoke public execute privilege on utl_file 1 ALL >= 8 YES 3.10.2 Revoke public execute privilege on utl_tcp 1 ALL >=8.1.7 YES 3.10.3 Revoke public execute privilege on utl_http 1 ALL >=8.1.7 YES 3.10.4 Revoke public execute privilege on utl_smtp 1 ALL >=8.1.7 YES 3.10.5 Audit public execute privilege on sys owned packages. 1 ALL >=8.1.7 YES 3.10.6 Revoke the public execute privilege on dbms_random. 2 ALL ALL YES 3.10.7 Revoke the public execute privilege on dbms_lob 1 ALL >=8i YES						
3.10.1Revoke public execute privilege on ut_{file} 1ALL>= 8YES3.10.2Revoke public execute privilege on ut_{cp} 1ALL>=8.1.7YES3.10.3Revoke public execute privilege on ut_{cp} 1ALL>=8.1.7YES3.10.4Revoke public privilege on ut_{cm} 1ALL>=8.1.7YES3.10.5Audit public execute privilege on ut_{cm} 1ALL>=8.1.7YES3.10.6Revoke the public execute privilege on $dbms_{cm}$ 2ALLALLYES3.10.7Revoke the public execute privilege on $dbms_{cm}$ 1ALL>=8iYES						
3.10.2Revoke public execute privilege on ut_tcp 1ALL>=8.1.7YES3.10.3Revoke public execute privilege on ut_tpp 1ALL>=8.1.7YES3.10.4Revoke public privilege on ut_smtp 1ALL>=8.1.7YES3.10.5Audit public execute privileges on sys owned packages.1ALLALLYES3.10.6Revoke the public execute privilege on $dbms_random$.2ALLALLYES3.10.7Revoke the public execute privilege on $dbms_lob$ 1ALL>= 8iYES						
3.10.3 Revoke public execute privilege on utl_http 1 ALL >=8.1.7 YES 3.10.4 Revoke public privilege on utl_smtp 1 ALL >=8.1.7 YES 3.10.5 Audit public execute privileges on sys owned packages. 1 ALL ALL YES 3.10.6 Revoke the public execute privilege on dbms_random. 2 ALL ALL YES 3.10.7 Revoke the public execute privilege on dbms_lob 1 ALL >= 8i YES			1			
3.10.4Revoke public privilege on ut_smtp 1ALL>=8.1.7YES3.10.5Audit public execute privileges on sys owned packages.1ALLALLYES3.10.6Revoke the public execute privilege on dbms_random.2ALLALLYES3.10.7Revoke the public execute privilege on dbms_lob1ALL>= 8iYES			1		-	
3.10.5Audit public execute privileges on sys owned packages.1ALLYES3.10.6Revoke the public execute privilege on dbms_random.2ALLALLYES3.10.7Revoke the public execute privilege on dbms_lob1ALL>= 8iYES			· · ·		-	
3.10.6 Revoke the public execute privilege on dbms_random. 2 ALL ALL YES 3.10.7 Revoke the public execute privilege on dbms_lob 1 ALL >= 8i YES						
3.10.7 Revoke the public execute privilege on <i>dbms_lob</i> 1 ALL >= 8i YES						
3.10.8 Revoke any privileges on <i>dbms_sql</i> and <i>dbms_sys_sql granted</i> 1 ALL YES						
	3.10.8	Revoke any privileges on <i>dbms_sql</i> and <i>dbms_sys_sql granted</i>	1	ALL	ALL	YES

1010 Use involvers rights PL/SQL procedures 2 ALL >=8 YES 31011 Ault DRECTORY volveds 2 ALL >=8 YES 31011 Ault DRECTORY volveds 2 ALL ALL YES 31011 Revoke public execute privilege on dms. job of ms.	3.10.9	Audit packages available via a database link	1	ALL	ALL	
3.10.11Audit DIRECTÓRY objects'2ALL $\rightarrow = 8$ YES3.10.12Revoke public execute privilege on dbms, scheduler2ALLALLYES3.10.13Revoke public execute privilege on dbms, scheduler2ALLALLYES3.10.14Revoke public execute privilege on owa_util2ALLALLYES3.10.15Revoke public execute privilege on owa_util2ALLALLYES3.10.17Revoke public execute privilege on owa_util2ALLALLYES3.11.1Audit directly granted privileges2ALLALLYES3.11.2Change system uses default and temporary tablespaces2ALLALLYES3.12.2Change vistem uses default and temporary tablespaces2ALLALLYES3.13.3Revoke all non-essential rights from PUBLIC3ALLALLYES3.13.4Revoke all non-essential rights from PUBLIC3ALL>= 833.14.3Set password frace time to 33ALL>= 833.14.4Set password reve max to 203ALLALLYES3.14.5Set up general privile parameters3ALLALLYES3.14.6Set up general privile parameters3ALLALLYES3.14.6Set up general privile parameters3ALLALLYES3.14.6Set up general privile parameters3ALLALLYES3.14.7						
31.01.2Revoke excute privileges on sys.inflymaux2ALLALLYES31.01.3Revoke public execute privilege on dbms, bob1ALLs=10gYES31.01.4Revoke public execute privilege on own_util2ALLALLALLYES31.11.1Auctor dprivileges on roles.2ALLALLALLYES31.12Access tables fruque parkedges or roles.4ALLALLYES31.2.1Change users default tablespace.1ALLALLYES31.3.1Revoke the CONVector role from users1ALLALLYES31.3.1Revoke the RESOURCE role from users1ALLALLYES31.3.1Revoke the CONVector role from users3ALLALLYES31.3.1Revoke the CONVector role from users3ALLALLYES31.4.1Revoke the CONVector role from users3ALLALLYES31.4.1Revoke the CONVector						YES
310.13Revoke public execute privilege on odms, scheduler2ALLALLYES310.14Revoke public execute privilege on owa_util2ALLALLXES310.15Revoke public execute privilege on owa_util2ALLALLALLYES311.1Audit directly granted privileges2ALLALLALLYES311.2Access tables through packages or roles.4ALLALLYES312.2Change system users default tablespace.1ALLALLYES313.3Revoke the RESOURCE role from users2ALLALLYES313.4Revoke the RESOURCE role from users2ALLALLYES313.4Revoke the RESOURCE role from ousers3ALLALLYES313.4Revoke the RESOURCE role from ousers3ALLALLXES314.4Revoke all non-essential rights from PUBLIC3ALL>= 8314.3Set password rules max to 203ALL>= 8314.4Set taled login attempts to 53ALLALL315.1Set up general profile parameters3ALLALL316.2Rever halden initialisation parameters3ALLALL317.1Audit users database tugers fre3ALLALL318.3Rever halden intralisation parameters3ALLALL318.4Set up general profile parameters3ALLALL318.5Rever halden inta						
310.11 Revoke public execute privilege on owe_util 2 ALL YES 31.11.2 Access tables frundy packages or roles. 1 ALL ALL ALL YES 31.2.1 Change system users default tablespace. 1 ALL ALL YES 31.3.1 Revoke the CONKECT role from users 1 ALL ALL YES 31.3.1 Revoke all non-essemial nghts from PUBLC 3 ALL ALL ALL ALL Set apsilo for form some some some some some some some som						
3:10:15 Revoke public execute privilege on over, util 2 ALL ALL ALL ALL 3:11:1 Audit directly granted privileges 2 ALL ALL ALL 3:12:1 Change system users default ablespace. 1 ALL ALL YES 3:12:1 Change system users default ablespaces 2 ALL ALL YES 3:13:1 Revoke the RESOURCE role from suess 1 ALL ALL YES 3:13:1 Revoke the CONNECT role from suess 2 ALL ALL ALL 3:14:3 Revoke the CONNECT role from PUBLIC 3 ALL ALL ALL 3:14:4 Set password is users and to non-essential rights from PUBLIC 3 ALL >= 8 3:14:4 Set password reuse max to 20 3 ALL ALL ALL 3:14:5 Set up profiles for each class of database user 3 ALL ALL ALL 3:14:5 Set up profiles for each class of database user 3 ALL ALL ALL 3:15:1 Set rade_effiles_public to false 3 ALL ALL ALL <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>						
5.11.1Audit directly granted privilegésALLALLALL31.12Access tables trivuid packages or roles.1ALLALLALL31.21Change system users default tablespace.1ALLALLVFS31.31Revoke the RESOURCE role from users1ALLALLVFS31.31Revoke the CNNetC Trole from all users3ALLALLALLVFS31.33Revoke the CNNetC Trole from PUBLIC3ALLALLALLVFS31.34Revoke all non-escential rights from PUBLIC3ALLALLALLSet password is concentrative roles3ALLSet password is concentrative roles3ALLALLSet password is concentrative roles3ALLALLALLSet password is concentrative roles3ALLALLALLSet password is concentrative roles3ALLALLALLSet password is concentrative roles3ALLALLALLALLSet password is concentrative roles3ALLALLALLSet password is concentrative roles3ALLALLALL						
3.11.2 Access tables "through packages or roles. 4 ALL ALL ALL ALL ML 3.12.1 Change system uses default and temporary tablespaces 2 ALL ALL VFS 3.13.1 Revoke the CONNECT role from users 1 ALL ALL VFS 3.13.3 Add passwords to critical and administrative roles 3 ALL ALL VFS 3.13.3 Add passwords to critical and administrative roles 3 ALL ALL VFS 3.13.4 Revoke all non-essential rights from PUBLIC 3 ALL >= 8 14.4 Set password freques max to 20 3 ALL >= 8 3.14.4 Set password grace time to 3 ALL >= 8 14.4 Set failed login attempts to 5 3 ALL ALL ALL ALL ALL 3.14.5 Set up profiles for each class of database user 3 ALL ALL ALL ALL ALL 3.16.1 Objects in application tablespaces not owned by schema owner should be dropped 3 ALL ALL ALL 3.17.2 Estable different users for schema amagement and data management						120
5.12.1Change system users default and temporary tablespaces1ALLALLYES3.13.2Revoke the RESOURCE role from users1ALLALLYES3.13.3Revoke the RESOURCE role from all users2ALLALLYES3.13.4Revoke the CNNECT role from all users3ALLALLALLYES3.13.4Revoke the CNNECT role from all users3ALLALLALLYES3.13.3Revoke all non-essential rights from PUBLIC3ALLALL>= 83.14.1Set password receit the to 33ALL>= 83.14.3Set password receit the to 33ALL>= 83.14.4Set password receit the to 53ALLALL>= 83.14.5Set up general profile parameters3ALLALLALL3.15.5Review hidden initialisaton parameters3ALLALLALL3.16.1Objects in application tablespaces not owned by schema owner should be dropped1ALLALLYES3.17.2Establish different users for schema management and data management3ALLALLYES3.17.1Audi userd albabe triggers2ALLALLYES3.17.2Establish different users for schema owners and administrators and users5ALLALLYES3.17.2Establish different users for schema management3ALLALLYES3.17.1Audi userd albabe striggers2ALL		Access tables through nackages or roles				
3.12.2 Charge users default and temporary tablespaces 2 ALL ALL YES 3.13.1 Revoke the RESOURCE role from users 2 ALL ALL YES 3.13.1 Revoke the CONNECT role from all users 2 ALL ALL YES 3.13.3 Add passwords to ortical and administrative roles 3 ALL ALL ALL YES 3.13.1 Revoke all non-essential rights from PUBLIC 3 ALL ALL >= 8 3.14.2 Set password grace time to 3 ALL >= 8 3.14.4 Set password grace time to 3 ALL >= 8 3.14.4 Set password grace time to 3 ALL ALL >= 8 3.14.4 Set tablet login attempts to 5 3 ALL ALL 3.14.5 Set up profiles for each class of database user 3 ALL ALL 3.15.1 Set up fortile to tables 3 ALL ALL 3.14.5 Set up fortile to tables 3 ALL ALL 3.14.5 Set up fortile to tables 3 ALL ALL 3.14.5 Set up fortile to tables 3 ALL ALL 3.14.5 Set up fortile to tables 3 ALL ALL <t< td=""><td></td><td></td><td></td><td></td><td></td><td>VES</td></t<>						VES
13.1.1 Revoke the RESOURCE role from all users 1 ALL ALL ALL YES 31.3.2 Revoke the CONNECT role from all users 3 ALL ALL<						
13.12 Revoke the CONNECT role from all users 2 ALL ALL ALL ALL 13.13 Add passwords to critical and administrative roles 3 ALL ALL ALL 31.33 Add passwords word lifetime in profile to 60 3 ALL ALL ALL 31.41 Set password grace time to 3 3 ALL ALL >= 8 31.42. Set password grace time to 3 3 ALL >= 8 31.43. Set password grace time to 3 3 ALL ALL 31.44. Set tables login attempts to 5 3 ALL ALL 31.45. Set up general profile parameters 3 ALL ALL 31.51. Set transport ingars fire 3 ALL ALL 31.61. Objects in application tablespaces not owned by schema owner should be dropped 3 ALL ALL 31.71. Audit access to critical ays owned views like user\$, link\$ etc 1 ALL ALL 31.71. Audit access to critical ays owned views like user\$, link\$ etc 1 ALL ALL 31.71. Audit access to critical sys owned views						
3.13.3 Add passwords to critical and administrative roles 3 ALL ALL 3.13.4 Revoke all non-sesmital rights from PUBLC 3 ALL >= 8 3.14.1 Set password grace time to 3 3 ALL >= 8 3.14.2 Set password grace time to 3 3 ALL >= 8 3.14.4 Set password grace time to 3 3 ALL >= 8 3.14.4 Set laidel doign attempts to 5 3 ALL ALL 3.14.5 Set up profiles for each class of database user 3 ALL ALL 3.14.5 Set up profiles for each class of database user 3 ALL ALL 3.14.5 Set urace files public to false 3 ALL ALL 3.15.3 Ensure system triggers file 3 ALL ALL 3.15.3 Ensure system triggers for schema management and data management 3 ALL ALL 3.17.1 Audit access to critical sys owned views like user\$, link\$ etc 1 ALL ALL 3.20.1 Audit access to critical sys owned views 1 ALL ALL YES 3.20.20						
13.1.4Revoke all non-essential rights from PUBLIC3ALL> ALL> ALL31.4.1Set password itelation in profile to 603ALL> = 831.4.2Set password rause max to 202ALL> = 831.4.3Set password rause max to 202ALL> = 831.4.4Set laidel digan attempts to 53ALL> = 831.4.5Set up general profile parameters3ALLALL31.4.5Set up general profile parameters3ALLALL31.5.1Set up general profile parameters3ALLALL31.6.1Objects in application tablespaces not owned by schema owner should be dropped3ALLALL31.7.2Establish different users for schema anagement and data management3ALLALLYES31.7.1Audit users database triggers5ALLALLYES31.7.2Establish different users for schema owners and administrators and users5ALLALLYES31.9.1Audit access to critical sys owned views like user\$, link\$ etc1ALLALLYES32.0.1Audit access to critical sys owned views1ALLALLYES32.0.2Audit access to critical sys owned viewsand sys owned atabase2ALLALL32.0.1Audit access to critical sys owned viewsand sys owned atabase2ALLALL32.0.1Audit access to critical sys owned viewsand sys owned atabase2ALLALL<						TLS
3.14.1 Set password lifetime in profile to 60 3 ALL >= 8 3.14.2 Set password reuse max to 20 2 ALL >= 8 3.14.3 Set password reuse max to 20 2 ALL >= 8 3.14.4 Set ialied login attempts to 5 3 ALL ALL >= 8 3.14.5 Set up profiles for each class of database user 3 ALL ALL ALL 3.14.5 Set up profiles for each class of database user 3 ALL ALL ALL 3.14.5 Set up rofiles for each class of database user 3 ALL ALL ALL 3.15.1 Set urace, fliese public to false 3 ALL ALL ALL 3.15.3 Ensure system triggers fire 1 ALL ALL YES 3.16.1 Objects in application tablespaces not owned by schema owners should be dropped 3 ALL ALL YES 3.17.2 Establish different users for schema amagement and data management 3 ALL ALL YES 3.17.1 Audit access to critical sys owned views ike user5, link\$ etc 1 ALL ALL YES<						
1.14.2Set password grace time to 3ALL>= 83.14.3Set password reuse max to 20ALL>= 83.14.4Set tailed login attempts to 53ALL>= 83.14.5Set up general profile parameters3ALLALL3.15.5Set up general profile parameters3ALLALL3.15.1Set us general initialisation parameters3ALLALL3.15.2Review hidden initialisation parameters3ALLALL3.16.1Objects in application tablespaces not owned by schema owner should be dropped3ALLALL3.17.1Audit quota use per user3ALLALLYES3.17.2Establish different users for schema management and data management3ALLALLYES3.18.1Set up naming conventions for schema owners and administrators and users5ALLALLYES3.20.1Audit access to all dba and sys owned views1ALLALLYES3.20.2Audit access to all dba and sys owned views1ALLALLYES3.20.1Audit access to all dba and sys owned views2ALLALLYES3.21.1Revoke bELECT ANY TABLESel owned and seles2ALLALLYES3.21.2Ensure users can only see the objects they need2ALLALLYES3.21.1Revoke be chace of brute force attacks2ALLALLYES3.21.2Ensure users can only see the objects they need<						
13.14.3Set password reuse max to 202ALL>= 831.44.3Set tailed login attempts to 53ALLALLALL31.44.5Set up profiles for each class of database user3ALLALLALL31.45.1Set _race_files_public to false3ALLALLALL31.51.5Review hidden initialisation parameters3ALLALLALL31.52.7Review hidden initialisation parameters3ALLALLALL31.53.1Ensure system triggers fire1ALLSet up anditication tablespaces not owned by schema owner should be dropped3ALLALLYES31.61.1Objects in application tablespaces not owned by schema owner should be dropped3ALLALLYES31.71.1Audit quota users for schema management and data management3ALLALLYES31.71.1Audit users for schema owners and administrators and users5ALLALLYES31.20.2Audit access to critical sys owned views like users, link\$ etc1ALLALLYES32.01.1Audit access to critical sys owned views1ALLALLYES32.1.2Ensure users can only see the objects they need2ALLALLYES32.1.1Revoke object reation privileges from all but schema owners and DBA's2ALLALLYES32.1.1Revoke object oreation privileges from all but schema owners and DBA's2ALLALLYES32.1.1 <t< td=""><td></td><td></td><td></td><td></td><td>-</td><td></td></t<>					-	
3.14.4Set failed login attempts to 53ALL>= 83.14.5Set up pofiles for each class of database user3ALLALLALL3.14.5Set up general profile parameters3ALLALLALL3.15.1Set intrao_files, public to false3ALLALLALL3.15.2Review hidden initialisation parameters3ALLALLALL3.16.1Objects in application tablespaces not owned by schema owner should be dropped3ALLALLYES3.17.1Audit quota use per user3ALLALLYESYES3.17.1Audit quota use per user for schema management and data management3ALLALLYES3.17.1Audit quotes to critical sys owned views like user\$, link\$ etc3ALLALLYES3.18.1Set up naming conventions for schema owners and administrators and users5ALLALLYES3.20.1Audit access to critical sys owned views like user\$, link\$ etc1ALLALLYES3.20.2Audit access to all dha and sys owned views1ALLALLYES3.21.1Revoke SELECT ANY TABLE2ALLALLYES3.21.2Ensure users can only see the objects they need2ALLALLYES3.21.1Audit views to ensure only select access is allowed2ALLALLYES3.21.1Audit integration and server to server communications2ALLALLYES3.					-	
3.14.5Set up profiles for each class of database user3ALLALL3.14.6Set up general profile parameters2ALLALLALL3.15.1Set_trace_files_public to false3ALLALLALL3.15.2Review hidden initialisation parameters3ALLALLALL3.15.3Ensure system triggers fire1ALLALLYES3.16.1Objects in application tablespaces not owned by schema owner should be dropped3ALLALLYES3.17.2Establish different users for schema management and data management3ALLALLYES3.17.2Establish different users for schema owners and administrators and users5ALLALLYES3.18.1Set up naming conventions for schema owners and administrators and users5ALLALLYES3.20.1Audit access to attical sys owned views1ALLALLYES3.20.2Audit access to attical sys owned views1ALLYES3.20.3Revoke SELECT ANY TABLE1ALLYES3.21.1Revoke object creation privileges from all but schema owners and DBA's2ALLALLYES3.21.2Audit views to ensure only select access is allowed2ALLALLYES3.22.1Audit interest actors of brue force attacks2ALLALLYES3.22.1Audit interest actors of brue force attacks2ALLALLYES3.22.1Audit interes					-	
3.14.6Set up general profile parameters2ALLALLALL3.15.1Set trace, files_public to false3ALLALLALLALLALL3.15.2Review hidden initialisation parameters3ALLALLALLALLALL3.15.3Ensure system triggers fire3ALLALLALLYES3.16.1Objects in application tablespaces not owned by schema owner should be dropped3ALLALLYES3.17.1Audit quote use per user3ALLALLYES3.17.2Establish different users for schema management and data management3ALLALLYES3.18.1Set up naming conventions for schema owners and administrators and users5ALLALLYES3.20.2Audit access to critical sys owned views like user\$, link\$ etc1ALLALLYES3.20.2Audit access to all dba and sys owned views1ALLALLYES3.20.3Revoke object creation privileges from all but schema owners and DBA's2ALLALLYES3.21.1Revoke object rotation privileges from all but schema owners and DBA's2ALLALLYES3.22.1Audit views to ensure only selet access is allowed2ALLALLYES3.23.1Reduce the chance of brute force attacks2ALLALLYES3.24.1Prevent the dba reading system tables2ALLALLYES3.24.1Prevent the dba reading sy						
3.15.1Set trace files public to false3ALLALLALL3.15.2Review hidden initialisation parameters3ALLALLALL3.15.3Ensure system triggers fire1ALL>=8iYES3.16.1Objects in application tablespaces not owned by schema owner should be dropped3ALLALLALLYES3.17.1Audit quota use per user3ALLALLYESYES3.17.2Establish different users for schema management and data management3ALLALLYES3.18.1Set up naming conventions for schema owners and administrators and users5ALLALLYES3.20.2Audit access to all dba and sys owned views like user\$, link\$ etc1ALLALLYES3.20.2Audit access to all dba and sys owned views1ALLALLYES3.21.1Revoke object creation privileges from all but schema owners and DBA's2ALLALLYES3.22.1Audit views to ensure only seleta access is allowed2ALLALLYES3.22.1Revoke object creation privileges from all but schema owners and DBA's2ALLALLYES3.22.1Audit views to ensure only seleta access is allowed2ALLALLYES3.23.1Reduce the chance of brute force attacks2ALLALLYES3.24.1Prevent the dba reading system tables2ALLALLYES3.25.1Prevent the dba reading system tables <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>						
3.15.2Review hidden initialisation parameters3ALLALL3.15.3Ensure system triggers fire1ALL>=8i3.16.1Objects in application tablespaces not owned by schema owner should be dropped3ALLALLALL3.17.1Audit quota use per user3ALLALLALLYES3.17.2Establish different users for schema management and data management3ALLALLALLYES3.18.1Set up naming conventions for schema owners and administrators and users5ALLALLYES3.20.1Audit access to critical sys owned views like user\$, link\$ etc1ALLALLYES3.20.2Audit access to all dba and sys owned views1ALLALLYES3.20.3Revoke SELECT ANY TABLE1ALLALLYES3.21.1Revoke object creation privileges from all but schema owners and DBA's2ALLALLYES3.22.1Audit views to ensure only see the objects they need2ALLALLYES3.22.1Audit views to ensure only see the objects they need2ALLALLYES3.23.1Reduce the chance of brute force attacks2ALLALLYES3.24.1Prevent the dba from reading application data2ALLALLYES3.23.1Audit internet access to the Oracle database2ALLALLYES3.24.1Prevent the dba from reading application data2ALLALLYES			2			
3.15.3Ensure system triggers fire1ALL>=8iYES3.16.1Objects in application tablespaces not owned by schema owner should be dropped3ALLALLALLYES3.17.1Audit quota use per user3ALLALLYESYES3.17.2Establish different users for schema management and data management3ALLALLYES3.18.1Set up naming conventions for schema owners and administrators and users5ALLALLYES3.19.1Audit access to critical sys owned views like user\$, link\$ etc1ALLALLYES3.20.1Audit access to all dba and sys owned viewslike user\$, link\$ etc1ALLALLYES3.20.2Audit access to all dba and sys owned viewslike user\$, link\$ etc1ALLALLYES3.21.1Revoke object creation privileges from all but schema owners and DBA's2ALLALLYES3.21.1Revoke object creation privileges from all but schema owners and DBA's2ALLALLYES3.21.1Revoke object creation privileges from all but schema owners and DBA's2ALLALLYES3.21.1Revoke object creation privileges from all but schema owners and DBA's2ALLALLYES3.22.1Audit rives to ensure only selet access is allowed2ALLALLYES3.23.1Reduce the chance of brute force attacks2ALLALLYES3.25.1Prevent the dba from reading applicat						
3.16.1Objects in application tablespaces not owned by schema owner should be dropped3ALLALLALL3.17.1Audit quota use per user3ALLALLALLYES3.17.2Establish different users for schema management and data management3ALLALLYES3.18.1Set up naming conventions for schema owners and administrators and users5ALLALLYES3.19.1Audit users database triggers2ALLALLYES3.20.1Audit access to critical sys owned views like user\$, link\$ etc1ALLALLYES3.20.2Audit access to all dba and sys owned views1ALLALLYES3.20.3Revoke SELECT ANY TABLE1ALLYES3.21.1Revoke object creation privileges from all but schema owners and DBA's2ALLALLYES3.21.2Ensure users can only see the objects they need2ALLALLYES3.22.1Audit views to ensure only select access is allowed2ALLALLYES3.22.1Revoke object creation privileges from all but schema owners and DBA's2ALLALLYES3.22.1Revoke the chance of brute force attacks2ALLALLYES3.23.1Reduce the chance of brute force attacks2ALLALLYES3.24.1Prevent the dba reading system tables2ALLALLYES3.25.1Prevent the dba form reading application data4ALLA						
3.17.1Audit quota use per user3ALLALLYES3.17.2Establish different users for schema management and data management3ALLALLYES3.18.1Set up naming conventions for schema owners and administrators and users5ALLALLYES3.19.1Audit users database triggers2ALLALLYES3.20.1Audit access to critical sys owned views like user\$, link\$ etc1ALLALLYES3.20.2Audit access to all dba and sys owned views1ALLALLYES3.20.3Revoke SELECT ANY TABLE1ALLALLYES3.21.1Revoke object creation privileges from all but schema owners and DBA's2ALLALLYES3.22.1Audit views to ensure only see the objects they need2ALLALLYES3.22.1Audit views to ensure only see the object access is allowed2ALLALLYES3.23.1Reduce the chance of brute force attacks2ALLALLYES3.24.1Prevent the dba reading system tables2ALLALLYES3.25.1Prevent the dba reading system tables2ALLALLYES3.27.1Audit integration and server to sever communications2ALLALLYES3.27.1Audit integration and server to sever communications2ALLALLYES3.26.1Audit integration and server to sever communications2ALLALL>=8iYES						YES
3.17.2Establish different users for schema management and data management3ALLALLYES3.18.1Set up naming conventions for schema owners and administrators and users5ALLALLALLYES3.19.1Audit access to critical sys owned views like user\$, link\$ etc1ALLALLYES3.20.1Audit access to all dba and sys owned views1ALLALLYES3.20.2Audit access to all dba and sys owned views1ALLALLYES3.20.3Revoke SELECT ANY TABLE1ALLYES3.21.1Revoke object creation privileges from all but schema owners and DBA's2ALLALLYES3.21.2Ensure users can only see the objects they need2ALLALLYES3.22.1Audit views to ensure only select access is allowed2ALLALLYES3.23.1Reduce the chance of brute force attacks2ALLALLYES3.24.1Prevent the dba reading system tables2ALLALLYES3.25.1Prevent the dba from reading application data4ALLALLYES3.26.1Audit integration and server to sever communications2ALLALLYES3.27.1Audit integration and server to sever communications2ALLALLYES3.28.1Audit integration dat storage.2ALLALL>=9iR2YES3.28.1Audit integration distorage.2ALLALLYES </td <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>						
3.18.1Set up naming conventions for schema owners and administrators and users5ALLALLALL3.19.1Audit users database triggers2ALLALLALLYES3.20.1Audit access to critical sys owned views1ALLALLYES3.20.2Audit access to all dba and sys owned views1ALLALLYES3.20.3Revoke SELECT ANY TABLE1ALLALLYES3.21.1Revoke object creation privileges from all but schema owners and DBA's2ALLALLYES3.22.1Audit views to ensure only see the objects they need2ALLALLYES3.22.1Audit views to ensure only select access is allowed2ALLALLYES3.23.1Reduce the chance of brute force attacks2ALLALLYES3.24.1Prevent the dba reading system tables2ALLALLYES3.25.1Prevent the dba from reading application data4ALLALLYES3.26.1Audit integration and server to sever communications2ALLALLALL3.27.1Audit insert failures on critical objects2ALLALLYES3.28.1Audit and scure statspack2ALLALLYES3.28.1Audit insert failures on critical objects2ALLALLYES3.28.1Audit insert failures on critical objects2ALLALLYES4.2.1Audit insert failures on critical obje						
3.19.1Audit users database triggers2ALLYES3.20.1Audit access to critical sys owned views like user\$, link\$ etc1ALLYES3.20.2Audit access to all dba and sys owned views1ALLYES3.20.3Revoke SELECT ANY TABLE1ALLYES3.21.1Revoke object creation privileges from all but schema owners and DBA's2ALLALLYES3.21.2Ensure users can only see the objects they need2ALLALLYES3.22.1Reduce the chance of brute force attacks2ALLALLYES3.23.1Reduce the chance of brute force attacks2ALLALLYES3.24.1Prevent the dba reading system tables2ALLALLYES3.25.1Prevent the dba from reading application data4ALLALLYES3.26.1Audit integration and server to sever communications2ALLALLYES3.27.1Audit integration and server to sever communications2ALLALLYES3.28.1Audit integration and storage.2ALLXESYES3.28.1Audit insert failures on critical objects2ALLALLYES4.1.1Configure audit and storage.2ALLALLYES4.2.1Audit insert failures on critical objects2ALLALLYES4.3.1Audit use of all grant privileges.2ALLALLYES4.3.2Audit use						YES
3.20.1Audit access to critical sys owned views like user\$, link\$ etc1ALLALLALLYES3.20.2Audit access to all dba and sys owned views1ALLALLALLYES3.20.3Revoke SELECT ANY TABLE1ALLALLALLYES3.20.4Revoke object creation privileges from all but schema owners and DBA's2ALLALLALLYES3.21.2Ensure users can only see the objects they need2ALLALLYES3.22.1Audit views to ensure only select access is allowed2ALLALLYES3.23.1Reduce the chance of brute force attacks2ALLALLYES3.24.1Prevent the dba reading system tables2ALLALLYES3.25.1Prevent the dba reading application data4ALLALLYES3.26.1Audit integration and server to sever communications2ALLALLALL3.27.1Audit integration and server to sever communications2ALLALL>=9iR2YES3.28.1Audit and secure statspack2ALL>=0iYES4.1.1Configure audit and storage.2ALLALLALLYES4.1.1Configure such tables on critical objects2ALLALLALLYES4.2.1Audit insert failures on critical objects2ALLALLALLYES4.3.1Audit create session2ALLALLYESYES <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>						
3.20.2Audit access to all dba and sys owned views1ALLALLALLYES3.20.3Revoke SELECT ANY TABLE1ALLALLALLALLYES3.21.1Revoke object creation privileges from all but schema owners and DBA's2ALLALLALLYES3.21.2Ensure users can only see the objects they need2ALLALLALLYES3.22.1Audit views to ensure only select access is allowed2ALLALLYES3.23.1Reduce the chance of brute force attacks2ALLALLYES3.24.1Prevent the dba reading system tables2ALLALLYES3.25.1Prevent the dba reading application data4ALLYES3.26.1Audit integration and server to sever communications2ALLALLALL3.27.1Audit integration and server to sever communications2ALL>=9iR2YES3.28.1Audit and secure statspack2ALL>=8iYES4Audit insert failures on critical objects2ALLALLYES4.1.1Configure audit and storage.2ALLALLYES4.2.2Use triggers to capture login events2ALLALLYES4.3.1Audit use of all grant privileges.2ALLALLYES4.3.2Audit use of all grant privileges.2ALLALLYES						
3.20.3Revoke SELECT ANY TABLÉ1ALLALL3.21.1Revoke object creation privileges from all but schema owners and DBA's2ALLALLYES3.21.2Ensure users can only see the objects they need2ALLALLYES3.22.1Audit views to ensure only select access is allowed2ALLALLYES3.23.1Reduce the chance of brute force attacks2ALLALLALLYES3.24.1Prevent the dba reading system tables2ALLALLYES3.25.1Prevent the dba from reading application data4ALLALLYES3.26.1Audit integration and server to sever communications2ALLALLALL3.27.1Audit internet access to the Oracle database2ALLALL>=9iR2YES3.28.1Audit inger audit and storage.2ALL>= 8iYESYES4.1.1Configure audit and storage.2ALLALLYES4.1.1Audit insert failures on critical objects2ALLALLYES4.2.2Use triggers to capture login events2ALLALLYES4.3.2Audit use of all grant privileges.2ALLALLYES						
3.21.1Revoke object creation privileges from all but schema owners and DBA's2ALLALLYES3.21.2Ensure users can only see the objects they need2ALLALLYES3.22.1Audit views to ensure only select access is allowed2ALLALLYES3.23.1Reduce the chance of brute force attacks2ALLALLYES3.24.1Prevent the dba reading system tables2ALLALLYES3.25.1Prevent the dba reading system tables2ALLALLYES3.25.1Prevent the dba from reading application data4ALLALLYES3.26.1Audit integration and server to sever communications2ALLALLALL3.27.1Audit integration and server to sever communications2ALL>=8iYES3.28.1Audit integration and server to sever communications2ALL>=8iYES3.28.1Audit integration and storage.2ALL>=8iYES4.1.1Configure audit and storage.2ALLALLALL4.1.1Configure audit and storage.2ALLALLYES4.2.2Use triggers to capture login events2ALLALLYES4.3.2Audit inset failures on critical objects2ALLALLYES4.3.2Audit inset failures on critical objects2ALLALLYES4.3.2Audit use of all grant privileges.2ALLALL<						YES
3.21.2Ensure users can only see the objects they need2ALLALLYES3.22.1Audit views to ensure only select access is allowed2ALLALLYES3.23.1Reduce the chance of brute force attacks2ALLALLYES3.24.1Prevent the dba reading system tables2ALLALLYES3.25.1Prevent the dba reading application data4ALLALLYES3.26.1Audit integration and server to sever communications2ALLALLALL3.27.1Audit internet access to the Oracle database2ALLALL>=9iR2YES3.28.1Audit and secure statspack2ALL>=9iR2YESYES4.1.1Configure audit and storage.2ALLALLALL+ES4.1.1Configures to capture login events2ALLALLYES4.2.2Use triggers to capture login events2ALLALLYES4.3.1Audit create session2ALLALLYES4.3.2Audit use of all grant privileges.2ALLALLYES						
3.22.1Audit views to ensure only select access is allowed2ALLALLYES3.23.1Reduce the chance of brute force attacks2ALLALLALLYES3.24.1Prevent the dba reading system tables2ALLALLALLYES3.25.1Prevent the dba from reading application data4ALLALLALLYES3.26.1Audit integration and server to sever communications2ALLALLALLALL3.27.1Audit integration and server to sever communications2ALLALL>=9iR2YES3.28.1Audit and secure statspack2ALL>=8iYES4.1.1Configure audit and storage.2ALLALLALL4.2.1Audit insert failures on critical objects2ALLALLALL4.2.2Use triggers to capture login events2ALLALLYES4.3.1Audit use of all grant privileges.2ALLALLYES			2			
3.23.1Reduce the chance of brute force attacks2ALLALLALL3.24.1Prevent the dba reading system tables2ALLALLALLYES3.25.1Prevent the dba from reading application data4ALLALLALLALL3.26.1Audit integration and server to sever communications2ALLALLALL3.27.1Audit internet access to the Oracle database2ALLALL>=9iR2YES3.28.1Audit and secure statspack2ALL>=8iYES4.1.1Configure audit and storage.2ALLALLALL4.2.1Audit insert failures on critical objects2ALLALLALL4.2.2Use triggers to capture login events2ALLALLYES4.3.1Audit use of all grant privileges.2ALLALLYES						-
3.24.1Prevent the dba reading system tables2ALLALLYES3.25.1Prevent the dba from reading application data4ALLALLALLALL3.26.1Audit integration and server to sever communications2ALLALLALLALL3.27.1Audit integration and server to sever communications2ALLALL>=9iR2YES3.28.1Audit and secure statspack2ALL>=8iYES3.28.1Audit and secure statspack2ALL>=8iYES4.1.1Configure audit and storage.2ALLALLALL4.2.1Audit insert failures on critical objects2ALLALLALL4.2.2Use triggers to capture login events2ALLALLYES4.3.1Audit create session2ALLALLYES4.3.2Audit use of all grant privileges.2ALLALLYES						YES
3.25.1Prevent the dba from reading application data4ALLALL3.26.1Audit integration and server to sever communications2ALLALL3.27.1Audit internet access to the Oracle database2ALL>=9iR2YES3.28.1Audit and secure statspack2ALL>=8iYES4.Auditinger audit and storage.2ALLALLALL4.1.1Configure audit and storage.2ALLALLALL4.2.1Audit insert failures on critical objects2ALLALLALL4.2.2Use triggers to capture login events2ALLALLYES4.3.1Audit create session2ALLALLYES4.3.2Audit use of all grant privileges.2ALLALLYES		Reduce the chance of brute force attacks	2			
3.26.1Audit integration and server to sever communications2ALLALL3.27.1Audit internet access to the Oracle database2ALL>=9iR2YES3.28.1Audit and secure statspack2ALL>=8iYES4.Auditinger audit and storage.2ALLALLALL4.1.1Configure audit and storage.2ALLALLALL4.2.1Audit insert failures on critical objects2ALLALLALL4.2.2Use triggers to capture login events2ALLALLYES4.3.1Audit create session2ALLALLYES4.3.2Audit use of all grant privileges.2ALLALLYES			2			YES
3.27.1Audit internet access to the Oracle database2ALL>=9iR2YES3.28.1Audit and secure statspack2ALL>= 8iYES4.Auditing2ALLALLALL4.1.1Configure audit and storage.2ALLALLALL4.2.1Audit insert failures on critical objects2ALLALLALL4.2.2Use triggers to capture login events2ALLALLYES4.3.1Audit create session2ALLALLYES4.3.2Audit use of all grant privileges.2ALLALLYES	3.25.1	Prevent the dba from reading application data	4	ALL	ALL	
3.28.1Audit and secure statspack2ALL>= 8iYES4.Auditing2ALLALL4LL4.1.1Configure audit and storage.2ALLALLALL4.2.1Audit insert failures on critical objects2ALLALLALL4.2.2Use triggers to capture login events2ALLALLYES4.3.1Audit create session2ALLALLYES4.3.2Audit use of all grant privileges.2ALLALLYES	3.26.1	Audit integration and server to sever communications	2	ALL	ALL	
3.28.1Audit and secure statspack2ALL>= 8iYES4.Auditing2ALLALLALL4.1.1Configure audit and storage.2ALLALLALL4.2.1Audit insert failures on critical objects2ALLALLALL4.2.2Use triggers to capture login events2ALLALLYES4.3.1Audit create session2ALLALLYES4.3.2Audit use of all grant privileges.2ALLALLYES	3.27.1	Audit internet access to the Oracle database	2		>=9iR2	YES
4.1.1Configure audit and storage.2ALLALL4.2.1Audit insert failures on critical objects2ALLALLALL4.2.2Use triggers to capture login events2ALLALLYES4.3.1Audit create session2ALLALLYES4.3.2Audit use of all grant privileges.2ALLALLYES	3.28.1	Audit and secure statspack	2	ALL	>= 8i	YES
4.2.1Audit insert failures on critical objects2ALLALL4.2.2Use triggers to capture login events2ALLALLYES4.3.1Audit create session2ALLALLYES4.3.2Audit use of all grant privileges.2ALLALLYES	4.	Auditing				
4.2.1Audit insert failures on critical objects2ALLALL4.2.2Use triggers to capture login events2ALLALLYES4.3.1Audit create session2ALLALLYES4.3.2Audit use of all grant privileges.2ALLALLYES	4.1.1	Configure audit and storage.	2			
4.2.2Use triggers to capture login events2ALLYES4.3.1Audit create session2ALLALLYES4.3.2Audit use of all grant privileges.2ALLALLYES	4.2.1		2	ALL	ALL	
4.3.1Audit create session2ALLYES4.3.2Audit use of all grant privileges.2ALLALLYES			2	ALL	ALL	YES
4.3.2 Audit use of all grant privileges. 2 ALL ALL YES	4.3.1		2	ALL	ALL	YES
	4.3.2	Audit use of all grant privileges.	2	ALL		YES
	4.3.3	Audit the use of all drop statements		ALL	ALL	

1 4 9 4					i i
4.3.4	Audit the use of all alter statements	2	ALL	ALL	
4.3.5	Audit the use of create user	3	ALL	ALL	YES
4.3.6	Audit use of create role	3	ALL	ALL	
4.3.7	Audit all create statements	3	ALL	ALL	
4.3.8	Establish procedures to review audit logs	3	ALL	ALL	YES
4.3.9	Use Log Miner to audit in the case of forensics	4	ALL	ALL	
4.4.1	Configure basic audit	2	ALL	ALL	
4.4.2	Limit users who can change the audit trail	2	ALL	ALL	YES
4.4.3	Protect the audit trail	2	ALL	ALL	YES
4.4.4	Backup the audit trail	3	ALL	ALL	YES
4.4.5	Purge the audit trail	4	ALL	ALL	YES
4.4.6	Audit all SYS operations	1	ALL	>=9iR2	YES
4.4.0	Check date / time stamps on database objects		ALL	ALL	TEO
4.5.1	Check date / time stamps on database objects	3 3	ALL	ALL	YES
	Ensure reports and alerts are in place to deal with irregularities found through audit				TES
4.7.1	Use triggers for row level auditing	3	ALL	ALL	
4.7.2	Use VPD, RLS and label security for full data protection	3	ALL	>= 8	
4.8.1	Be aware of possible failure to be alerted of suspicious activities	2	ALL	ALL	YES
4.9.1	Be aware of possible failure to audit the security profile.	2	ALL	ALL	
4.10.1	Audit and review the Oracle generated log files	2	ALL	ALL	
5.	Networking				
5.1.1	Prevent set commands on the listener	1	ALL	ALL	YES
5.1.2	Prevent remote dba access on sql*net v1	4	ALL	ALL	
5.1.3	Audit the listener.ora file	5	ALL	ALL	
5.1.4	Enable shared sockets	3	win	ALL	
5.1.5	Force the MTS dispatcher to use specific ports	4	ALL	ALL	
5.1.6	Do not use the standard listener ports 1521, 1526	2	ALL	ALL	YES
5.1.7	Do not use known SID or service names such as ORCL	2	ALL	ALL	YES
5.1.8	In small environments do not use hostnames in listener.ora.	2	ALL	ALL	
5.1.9	Use a personal firewall on database administrator computers	2	ALL	ALL	YES
5.1.10	Secure listener or at the O/S level	2	ALL	ALL	YES
5.1.11	Ensure that listener logging is enabled	2	ALL	ALL	YES
5.2.1	Restrict sources of database connections	3	ALL	ALL	120
5.2.2	Use connection manager and Oracle names to restrict connections by source	2	ALL	ALL	
5.3.1	Set the listener password	1	ALL	ALL	YES
5.4.1	Restrict listener banner information	3	ALL	ALL	TL3
5.4.1			ALL	ALL	
5.5.1	Use a firewall to protect the Oracle server.	2			
5.6.1	Audit Oracle client file permissions	4	ALL	ALL	
5.6.2	Audit client configuration file contents	5	ALL	ALL	
5.6.3	Audit the listener	2	ALL	ALL	YES
5.7.1	Audit database links for hard clear text passwords	1	ALL	ALL	YES
5.7.2	Discover what objects can be seen in the linked database	2	ALL	ALL	YES
5.7.3	Create a policy to manage database links	1	ALL	ALL	YES
5.7.4	Database link user should not be a dba	1	ALL	ALL	YES
5.7.5	Audit what links exist into and from the database	1	ALL	ALL	YES
5.8.1	Confirm the file permissions in the network admin directory	2	ALL	ALL	YES
5.8.2	Add only minimum configuration files to all clients	2	ALL	ALL	
5.9.1	Keep up to date with Oracle listener vulnerabilities and patch	2	ALL	ALL	
					1
5.10.1	Secure remote dba access to the server	1	ALL	ALL	

5.10.2	Use an application gateway firewall	2	ALL	ALL	1 1
5.11.1	Set server to dedicated in the tnsnames ora file	1	ALL	ALL	YES
5.11.2	Disable Oracle ports that are not needed.	3	ALL	ALL	YES
5.12.1	Audit the intelligent agent	2	ALL	ALL	YES
5.12.2	Protect clear text passwords for SNMP	2	ALL	ALL	YES
5.13.1	Use Oracle advance security to encrypt data transfer	3	ALL	ALL	
5.13.2	Enable SSL to protect client transmissions	3	ALL	ALL	
6.	Availability / backup / Recovery				
6.1.1	Review and document backup and restore procedures	3	ALL	ALL	YES
6.1.2	Review and document recovery procedures	3	ALL	ALL	YES
6.1.3	Store backup media off site	3	ALL	ALL	YES
6.1.4	Schedule cold backups	3	ALL	ALL	YES
6.1.5	Validate the backup media regularly	3	ALL	ALL	YES
6.1.6	Do not allow backups to be available on-line	2	ALL	ALL	
6.1.7	Create and use media retrieval procedures	2	ALL	ALL	
6.2.1	Mirror the on line redo logs	2	ALL	ALL	YES
6.3.1	Ensure the database is in archive log mode	2	ALL	ALL	YES
6.3.2	Ensure archive log directories exist and are protected	2	ALL	ALL	YES
6.3.3	Ensure archive logs are written to backup and are purged	3	ALL	ALL	YES
6.4.1	Separate the Oracle software from data and from on-line redo and archive	3	ALL	ALL	YES
6.4.2	Keep Oracle data files on separate disks	3	ALL	ALL	YES
6.4.3	Use OFA	5	ALL	ALL	
6.4.4	Use striping and mirroring or RAID for Oracle data	4	ALL	ALL	
6.5.1	Magnetically wipe old disks that have contained database data.	2	ALL	ALL	
6.6.1	Document and review disaster recovery procedures	4	ALL	ALL	YES
6.6.2	Include business users in disaster recovery planning	4	ALL	ALL	YES
7.	Application Development				
7.1.1	Identify and wrap all PL/SQL code in the database	2	ALL	ALL	YES
7.1.2	Checksum all PL/SQL objects in the database	3	ALL	ALL	
7.1.3	Audit PL/SQL code for hard coded usernames and passwords	3	ALL	ALL	
7.1.4	Audit PL/SQL code for possible SQL injection attacks				
		2	ALL	ALL	
7.1.5	Ensure as little information as possible about schema structure is available from the code in Oracle	3	ALL	ALL	
7.1.6	Ensure as little information as possible about schema structure is available from the code in Oracle Pre-compile Java code before loading into the database	3 3	ALL ALL	ALL ALL	YES
7.1.6 7.2.1	Ensure as little information as possible about schema structure is available from the code in Oracle Pre-compile Java code before loading into the database Review which applications access the database and how and from where	3 3 2	ALL ALL ALL	ALL ALL ALL	YES
7.1.6 7.2.1 7.2.2	Ensure as little information as possible about schema structure is available from the code in Oracle Pre-compile Java code before loading into the database Review which applications access the database and how and from where Implement procedures to limit which applications can access the database and from where	3 3 2 2	ALL ALL ALL ALL	ALL ALL ALL ALL	YES
7.1.6 7.2.1 7.2.2 7.2.3	Ensure as little information as possible about schema structure is available from the code in Oracle Pre-compile Java code before loading into the database Review which applications access the database and how and from where Implement procedures to limit which applications can access the database and from where Limit administration tools from accessing the database	3 3 2 2 3	ALL ALL ALL ALL ALL	ALL ALL ALL ALL ALL	YES
7.1.6 7.2.1 7.2.2 7.2.3 7.3.1	Ensure as little information as possible about schema structure is available from the code in Oracle Pre-compile Java code before loading into the database Review which applications access the database and how and from where Implement procedures to limit which applications can access the database and from where Limit administration tools from accessing the database When decommissioning old applications remove all binaries and files	3 2 2 3 4	ALL ALL ALL ALL ALL ALL	ALL ALL ALL ALL ALL ALL	YES
7.1.6 7.2.1 7.2.2 7.2.3 7.3.1 7.4.1	Ensure as little information as possible about schema structure is available from the code in Oracle Pre-compile Java code before loading into the database Review which applications access the database and how and from where Implement procedures to limit which applications can access the database and from where Limit administration tools from accessing the database When decommissioning old applications remove all binaries and files Review procedures for adding new applications	3 2 2 3 4 4	ALL ALL ALL ALL ALL ALL ALL	ALL ALL ALL ALL ALL ALL ALL	YES
7.1.6 7.2.1 7.2.2 7.2.3 7.3.1	Ensure as little information as possible about schema structure is available from the code in Oracle Pre-compile Java code before loading into the database Review which applications access the database and how and from where Implement procedures to limit which applications can access the database and from where Limit administration tools from accessing the database When decommissioning old applications remove all binaries and files Review procedures for adding new applications Establish procedures for movers, leavers and joiners	3 2 2 3 4 4 2	ALL ALL ALL ALL ALL ALL ALL ALL	ALL ALL ALL ALL ALL ALL ALL ALL	YES
7.1.6 7.2.1 7.2.2 7.2.3 7.3.1 7.4.1 7.5.1 7.6.1	Ensure as little information as possible about schema structure is available from the code in Oracle Pre-compile Java code before loading into the database Review which applications access the database and how and from where Implement procedures to limit which applications can access the database and from where Limit administration tools from accessing the database When decommissioning old applications remove all binaries and files Review procedures for adding new applications Establish procedures for movers, leavers and joiners Audit application file permissions	3 2 2 3 4 4 2 3	ALL ALL ALL ALL ALL ALL ALL ALL ALL	ALL ALL ALL ALL ALL ALL ALL ALL ALL	YES
7.1.6 7.2.1 7.2.2 7.2.3 7.3.1 7.4.1 7.5.1 7.6.1 7.7.1	Ensure as little information as possible about schema structure is available from the code in Oracle Pre-compile Java code before loading into the database Review which applications access the database and how and from where Implement procedures to limit which applications can access the database and from where Limit administration tools from accessing the database When decommissioning old applications remove all binaries and files Review procedures for adding new applications Establish procedures for movers, leavers and joiners Audit application file permissions Check for evidence of development on production databases	3 3 2 3 4 4 2 3 3 3	ALL ALL ALL ALL ALL ALL ALL ALL ALL ALL	ALL ALL ALL ALL ALL ALL ALL ALL ALL ALL	YES
7.1.6 7.2.1 7.2.2 7.2.3 7.3.1 7.4.1 7.5.1 7.6.1 7.7.1 7.8.1	Ensure as little information as possible about schema structure is available from the code in Oracle Pre-compile Java code before loading into the database Review which applications access the database and how and from where Implement procedures to limit which applications can access the database and from where Limit administration tools from accessing the database When decommissioning old applications remove all binaries and files Review procedures for adding new applications Establish procedures for movers, leavers and joiners Audit application file permissions Check for evidence of development on production databases Restrict ad-hoc queries against production database	3 3 2 2 3 4 4 2 3 3 3 3	ALL ALL ALL ALL ALL ALL ALL ALL ALL ALL	ALL ALL ALL ALL ALL ALL ALL ALL ALL ALL	YES
7.1.6 7.2.1 7.2.2 7.2.3 7.3.1 7.4.1 7.5.1 7.6.1 7.7.1 7.8.1 7.8.1 7.9.1	Ensure as little information as possible about schema structure is available from the code in Oracle Pre-compile Java code before loading into the database Review which applications access the database and how and from where Implement procedures to limit which applications can access the database and from where Limit administration tools from accessing the database When decommissioning old applications remove all binaries and files Review procedures for adding new applications Establish procedures for movers, leavers and joiners Audit application file permissions Check for evidence of development on production database Restrict ad-hoc queries against production database Review users permissions in test and development databases	3 3 2 2 3 4 4 2 3 3 3 2	ALL ALL ALL ALL ALL ALL ALL ALL ALL ALL	ALL ALL ALL ALL ALL ALL ALL ALL ALL ALL	YES
7.1.6 7.2.1 7.2.2 7.2.3 7.3.1 7.4.1 7.5.1 7.6.1 7.6.1 7.8.1 7.8.1 7.9.1 7.9.2	Ensure as little information as possible about schema structure is available from the code in Oracle Pre-compile Java code before loading into the database Review which applications access the database and how and from where Implement procedures to limit which applications can access the database and from where Limit administration tools from accessing the database When decommissioning old applications remove all binaries and files Review procedures for adding new applications Establish procedures for movers, leavers and joiners Audit application file permissions Check for evidence of development on production database Review users permissions in test and development databases Check for database links with access to production databases from development or test systems	3 3 2 3 4 4 2 3 3 3 2 2	ALL ALL ALL ALL ALL ALL ALL ALL ALL ALL	ALL ALL ALL ALL ALL ALL ALL ALL ALL ALL	YES
7.1.6 7.2.1 7.2.2 7.2.3 7.3.1 7.4.1 7.5.1 7.6.1 7.7.1 7.8.1 7.9.1 7.9.2 7.9.3	Ensure as little information as possible about schema structure is available from the code in Oracle Pre-compile Java code before loading into the database Review which applications access the database and how and from where Implement procedures to limit which applications can access the database and from where Limit administration tools from accessing the database When decommissioning old applications remove all binaries and files Review procedures for adding new applications Establish procedures for movers, leavers and joiners Audit application file permissions Check for evidence of development on production databases Restrict ad-hoc queries against production database Review users permissions in test and development databases Check for database links with access to production databases from development or test systems Ensure "live" data held in test or development is mangled or obfuscated.	3 3 2 2 3 4 4 2 3 3 3 2 2 2	ALL ALL ALL ALL ALL ALL ALL ALL ALL ALL	ALL ALL ALL ALL ALL ALL ALL ALL ALL ALL	YES
7.1.6 7.2.1 7.2.2 7.2.3 7.3.1 7.4.1 7.5.1 7.5.1 7.5.1 7.6.1 7.7.1 7.8.1 7.9.1 7.9.2 7.9.3 7.9.4	Ensure as little information as possible about schema structure is available from the code in Oracle Pre-compile Java code before loading into the database Review which applications access the database and how and from where Implement procedures to limit which applications can access the database and from where Limit administration tools from accessing the database When decommissioning old applications remove all binaries and files Review procedures for adding new applications Establish procedures for movers, leavers and joiners Audit application file permissions Check for evidence of development on production database Review users permissions in test and development databases Check for database links with access to production databases from development or test systems	3 2 2 3 4 4 2 3 3 2 2 2 2 2 2 2	ALL ALL ALL ALL ALL ALL ALL ALL ALL ALL	ALL ALL ALL ALL ALL ALL ALL ALL ALL ALL	YES
7.1.6 7.2.1 7.2.2 7.2.3 7.3.1 7.4.1 7.5.1 7.6.1 7.7.1 7.8.1 7.9.1 7.9.2 7.9.3	Ensure as little information as possible about schema structure is available from the code in Oracle Pre-compile Java code before loading into the database Review which applications access the database and how and from where Implement procedures to limit which applications can access the database and from where Limit administration tools from accessing the database When decommissioning old applications remove all binaries and files Review procedures for adding new applications Establish procedures for movers, leavers and joiners Audit application file permissions Check for evidence of development on production databases Restrict ad-hoc queries against production database Review users permissions in test and development databases Check for database links with access to production databases from development or test systems Ensure "live" data held in test or development is mangled or obfuscated.	3 3 2 2 3 4 4 2 3 3 3 2 2 2	ALL ALL ALL ALL ALL ALL ALL ALL ALL ALL	ALL ALL ALL ALL ALL ALL ALL ALL ALL ALL	YES

7.9.7	No developer database accounts should exist on production database	2	ALL	ALL	
7.9.8	Backups and exports copy passwords to test and development – ensure they are not the same	2	ALL	ALL	
7.9.9	Place development and test on different network segment to production	2	ALL	ALL	
7.10.1	Move all non application objects from application tablespaces	2	ALL	ALL	
7.10.2	Ensure no privileged user owns application objects	2	ALL	ALL	
7.11.1	Audit resources used by the database	2	ALL	ALL	
7.12.1	Do not duplicate Oracle authentication	1	ALL	ALL	
7.12.2	Do not use one database login to authenticate all other users	2	ALL	ALL	
7.13.1	Do not use schema owners for administration tasks	2	ALL	ALL	
7.13.2	Ensure the schema owner is not a dba	2	ALL	ALL	
7.13.3	Lock schema owner accounts	2	ALL	ALL	
7.14.1	Audit public synonyms	5	ALL	ALL	
7.15.1	Do not hard code usernames and passwords in application source code	2	ALL	ALL	
7.15.2	Consider not using Java	2	ALL	>= 8	
7.15.3	Do not allow applications to change the schema	2	ALL	ALL	
7.16.1	Batch processes should access the database through one designed account	1	ALL	ALL	
7.16.2	Do not use external accounts for batch processes	1	ALL	ALL	
7.16.3	Consider password retrieval and use in schedulers	1	ALL	ALL	
7.16.4	Enable batch database accounts only when needed	1	ALL	ALL	
7.17.1	Use product user profile to secure SQL*Plus	4	ALL	ALL	
7.17.2	Audit query tool privileges	3	ALL	ALL	
7.18.1	Encrypt critical data	2	ALL	ALL	
7.19.1	Audit generated applications for known weaknesses	2	ALL	ALL	
7.19.2	Audit public libraries used for know vulnerabilities	2	ALL	ALL	
7.20.1	Use change control	2	ALL	ALL	
7.21.1	Audit use of advance queues	2	ALL	ALL	
7.22.1	Audit tools used for password leakage	2	ALL	ALL	
7.23.1	Ensure no tool offers better access to the database than the application	2	ALL	ALL	
7.24.1	Checksum application files for Trojans	2	ALL	ALL	
7.25.1	Start the Oracle HTTP Server as a non privileged user	1	ALL	>= 9i	YES
7.25.2	Configure HTTPS and secure the listener	3	ALL	>= 9i	YES
7.25.3	Add authentication for users	2	ALL	>= 9i	YES
7.25.4	Set HTTP passwords	2	ALL	>= 9i	YES
7.25.5	Configure product user profile for iSQL*Plus	3	ALL	>= 9i	YES
7.25.6	Restrict databases that can be accessed	2	ALL	>= 9i	YES
7.25.7	Disable iSQL*Plus on production servers	1	ALL	>= 9i	YES
7.26.1	Review how to enable and disable various database access features e.g.: IFS	2	ALL	ALL	
7.27.1	Protect debugger interfaces	2	ALL	ALL	
7.28.1	Do not divulge system information to the public	2	ALL	ALL	YES
8.	Application Servers and the Middle Tier				
	Oracle Portal				
8.1.1	Secure the portal DAD admin page	2	ALL	9iAS	YES
8.1.2	Encryption of the DAD password	1	ALL	9iAS	YES
8.1.3	Secure the portal users passwords in the database	1	ALL	9iAS	YES
8.1.4	Restrict the portal gateway URL	2	ALL	9iAS	YES
8.1.5	Remove the portal example programs	1	ALL	9iAS	YES
8.1.6	Revoke DBA from portal admin database users	1	ALL	9iAS 9iAS	YES YES
8.1.7	Restrict access to OWA UTL and other PL/SQL packages	1	ALL		

1	Oracle Wireless Portal		I		
8.2.1	Create secure wireless user and password	3	ALL	9iAS	YES
	Oracle Web Cache				
8.3.1	Check permissions on file containing Webcache admin password	1	ALL	9iAS	YES
8.3.2	Check permissions on Webcache.xml	1	ALL	9iAS	YES
	Oracle iCache				
8.4.1	Reset default account passwords in database cache database	1	ALL	9iAS	YES
8.4.2	Check permissions for export files used to create database cache	2	ALL	9iAS	YES
	Apache				
8.5.1	Protect Apache	2	ALL	9iAS	YES
8.5.2	SYSTEM password appears in Apache install window title	3	ALL	9iAS	YES
8.5.3	Change default port numbers	3	ALL	9iAS	YES
8.5.4	Apply security patches to web server	1	ALL	9iAS	YES
8.5.5	Run nessus against 9iAS	4	ALL	9iAS	YES
8.5.6	Protect httpd.conf file	1	ALL	9iAS	YES
8.5.7	Remove OJSP example programs	1	ALL	9iAS	YES
8.5.8	Protect against an attacker reading JSP class files	1	ALL	9iAS	YES
8.5.9	Restrict dynamic monitoring services	1	ALL	9iAS	YES
	Oracle Internet File Server				
8.6.1	Change IFS password	1	ALL	9iAS	YES
	Oracle Reports Server				
8.7.1	Secure the reports sever	1	ALL	9iAS	YES
8.7.2	Use only compiled reports	2	ALL	9iAS	YES
8.7.3	Rename <i>rwcgi60</i> executable	3	ALL	9iAS	YES
	XML/XSL and the XSQL Servlet				
8.8.1	Protect XMLConfig.xml	3	ALL	9iAS	YES
8.8.2	Delete servlet class files	2	ALL	9iAS	YES
8.8.3	Disable servlet URL	3	ALL	9iAS	YES
8.8.4	Delete XSQL examples	3	ALL	9iAS	YES
8.8.5	In XSQL use bind variables	3	ALL	9iAS	YES
8.8.6	Set allow-client-style=no in XMLConfig.xml	3	ALL	9iAS	YES
8.8.7	Delete the XSQL XDK from production databases	2	ALL	9iAS	YES
8.8.8	Restrict the XSQL status URL	3	ALL	9iAS	YES
8.8.9	Change the mapping for the servlet URL	3	ALL	9iAS	YES

Upcoming SANS Training Click Here for a full list of all Upcoming SANS Events by Location

SANS Riyadh May 2025	Riyadh, SA	May 10, 2025 - May 22, 2025	Live Event
SANS Amsterdam May 2025	Amsterdam, NL	May 12, 2025 - May 24, 2025	Live Event
SANS Abu Dhabi May 2025	Abu Dhabi, AE	May 18, 2025 - May 23, 2025	Live Event
SANS Security Leadership Nashville 2025	Nashville, TNUS	May 19, 2025 - May 23, 2025	Live Event
SANS Thailand May 2025	Bangkok, TH	May 19, 2025 - May 24, 2025	Live Event
SANS Philippines SEC504 2025	Manila, PH	May 19, 2025 - May 24, 2025	Live Event
SANS ICS418 Live Online May	Gold Coast, QLD, AU	May 19, 2025 - May 20, 2025	Live Event
SANS Dubai May 2025	Dubai, AE	May 25, 2025 - May 30, 2025	Live Event
SANS Madrid June 2025	Madrid, ES	Jun 02, 2025 - Jun 07, 2025	Live Event
SANS Baltimore Spring 2025	Baltimore, MDUS	Jun 02, 2025 - Jun 07, 2025	Live Event
SANS Zurich June 2025	Zurich, CH	Jun 02, 2025 - Jun 07, 2025	Live Event
SANS Cyber Defense Miami 2025	Coral Gables, FLUS	Jun 02, 2025 - Jun 07, 2025	Live Event
SANS Offensive Operations East 2025	Baltimore, MDUS	Jun 08, 2025 - Jun 14, 2025	Live Event
SANS London June 2025	London, GB	Jun 09, 2025 - Jun 14, 2025	Live Event
SANS OO East 2025: SEC535 Beta-2	Baltimore, MDUS	Jun 12, 2025 - Jun 14, 2025	Live Event
SANS ICS Security Summit & Training 2025	Lake Buena Vista, FLUS	Jun 15, 2025 - Jun 23, 2025	Live Event
SANS Amsterdam June 2025	Amsterdam, NL	Jun 16, 2025 - Jun 21, 2025	Live Event
SANS Cyber Defence Japan 2025	Tokyo, JP	Jun 16, 2025 - Jun 28, 2025	Live Event
SANS Paris June 2025	Paris, FR	Jun 23, 2025 - Jun 28, 2025	Live Event
SANS Cyber Defence Canberra 2025	Canberra, ACT, AU	Jun 23, 2025 - Jul 05, 2025	Live Event
SANS Rocky Mountain 2025	Denver, COUS	Jun 23, 2025 - Jun 28, 2025	Live Event
SANS Riyadh June 2025	Riyadh, SA	Jun 28, 2025 - Jul 03, 2025	Live Event
SANS Cloud Singapore June 2025	Singapore, SG	Jun 30, 2025 - Jul 05, 2025	Live Event
SANS Munich June 2025	Munich, DE	Jun 30, 2025 - Jul 05, 2025	Live Event
SANS Human Risk London July 2025	London, GB	Jul 07, 2025 - Jul 09, 2025	Live Event
SANS London July 2025	London, GB	Jul 07, 2025 - Jul 12, 2025	Live Event
SANS Riyadh July 2025	Riyadh, SA	Jul 12, 2025 - Jul 17, 2025	Live Event
SANSFIRE 2025	Washington, DCUS	Jul 14, 2025 - Jul 19, 2025	Live Event
SANS Amsterdam July 2025	Amsterdam, NL	Jul 14, 2025 - Jul 26, 2025	Live Event
SANS Anaheim 2025	Anaheim, CAUS	Jul 21, 2025 - Jul 26, 2025	Live Event
SANS DFIR Summit & Training 2025	Salt Lake City, UTUS	Jul 24, 2025 - Jul 31, 2025	Live Event
SANS Huntsville 2025	Huntsville, ALUS	Jul 28, 2025 - Aug 02, 2025	Live Event
SANS Doha May 2025	OnlineQA	May 10, 2025 - May 15, 2025	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced