



# ORACLE DATABASE 11*g* SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG) OVERVIEW

## Version 9, Release 1

## 27 October 2021

## Developed by DISA for the DoD

## Trademark Information

# TABLE OF CONTENTS

Page

# LIST OF TABLES

**Page**

# 1. INTRODUCTION

## 1.1 Executive Summary

The Oracle Database 11g Security Technical Implementation Guide (STIG) is published as a tool to improve the security of Department of Defense (DoD) information systems

The Oracle Database Security Readiness Review (SRR) targets conditions that undermine the integrity of security, contribute to inefficient security operations and administration, or may lead to interruption of production operations specific to databases. Additionally, the review ensures the site has properly installed and implemented the database environment and that it is being managed in a way that is secure. The items reviewed are derived from DOD policy documents, most notably, Department of Defense (DOD) Directive 8500.1 and DOD Instruction 8500.2 and the Information Assurance (IA) Controls defined therein as they apply to an Oracle Database Server installation.

Each security item to review is listed in this document with a procedure for measuring compliance with the security requirement. The result of the procedure is a status of compliance with the requirement. Results are assigned one of the following:

**O** = Open finding or non-compliance
**NF** = Not a Finding or in compliance
**NA** = Not Applicable or the item is not applicable to the database version, database use or host platform being reviewed
**NR** = Not Reviewed or the procedure was not completed so compliance is not determined
**MR** = Manual review. Can be the following check types:

1. Interview – Requires information found outside the DBMS
2. Manual – Requires information that cannot be automated
3. Verify – Requires verification of information found in the DBMS

DISA has assigned a level of urgency to each finding based on Chief Information Officer (CIO) established criteria for certification and accreditation. All findings are based on regulations and guidelines. All findings require correction by the host organization. Category 1 findings are any vulnerability that provides an attacker immediate access into a machine, super user access, or access that bypasses a firewall. Category II findings are any vulnerabilities that provide information that has a high potential of giving access to an intruder. Category III findings are any vulnerabilities that provide information that potentially could lead to compromise.

**Note**: Security patches required by the DOD IAVM process are reviewed during an operating system security review.

## 1.2 Authority

DoD Instruction (DoDI) 8500.01 requires that “all IT that receives, processes, stores, displays, or transmits DoD information will be […] configured […] consistent with applicable DoD

cybersecurity policies, standards, and architectures" and tasks that Defense Information Systems Agency (DISA) "develops and maintains control correlation identifiers (CCIs), security requirements guides (SRGs), security technical implementation guides (STIGs), and mobile code risk categories and usage guides that implement and are consistent with DoD cybersecurity policies, standards, architectures, security controls, and validation procedures, with the support of the NSA/CSS, using input from stakeholders, and using automation whenever possible." This document is provided under the authority of DoDI 8500.01.

Although the use of the principles and guidelines in these SRGs/STIGs provides an environment that contributes to the security requirements of DoD systems, applicable NIST SP 800-53 cybersecurity controls need to be applied to all systems and architectures based on the Committee on National Security Systems (CNSS) Instruction (CNSSI) 1253.

## 1.3 Vulnerability Severity Category Code Definitions

Severity Category Codes (referred to as CAT) are a measure of vulnerabilities used to assess a facility or system security posture. Each security policy specified in this document is assigned a Severity Category Code of CAT I, II, or III.

**Table 1-1: Vulnerability Severity Category Code Definitions**

| | DISA Category Code Guidelines |
|---|---|
| CAT I | Any vulnerability, the exploitation of which will **directly and immediately** result in loss of Confidentiality, Availability, or Integrity. |
| CAT II | Any vulnerability, the exploitation of which **has a potential** to result in loss of Confidentiality, Availability, or Integrity. |
| CAT III | Any vulnerability, the existence of which **degrades measures** to protect against loss of Confidentiality, Availability, or Integrity. |

## 1.4 STIG Distribution

Parties within the DoD and Federal Government's computing environments can obtain the applicable STIG from the Cyber Exchange website at https://cyber.mil/. This site contains the latest copies of STIGs, SRGs, and other related security information. Those without a Common Access Card (CAC) that has DoD Certificates can obtain the STIG from https://public.cyber.mil/.

## 1.5 Document Revisions

Comments or proposed revisions to this document should be sent via email to the following address: disa.stig_spt@mail.mil. DISA will coordinate all change requests with the relevant DoD organizations before inclusion in this document. Approved changes will be made in accordance with the DISA maintenance release schedule.

## 1.6 Other Considerations

DISA accepts no liability for the consequences of applying specific configuration settings made on the basis of the SRGs/STIGs. It must be noted that the configuration settings specified should be evaluated in a local, representative test environment before implementation in a production environment, especially within large user populations. The extensive variety of environments makes it impossible to test these configuration settings for all potential software configurations.

For some production environments, failure to test before implementation may lead to a loss of required functionality. Evaluating the risks and benefits to a system's particular circumstances and requirements is the system owner's responsibility. The evaluated risks resulting from not applying specified configuration settings must be approved by the responsible Authorizing Official. Furthermore, DISA implies no warranty that the application of all specified configurations will make a system 100 percent% secure.

Security guidance is provided for the Department of Defense. While other agencies and organizations are free to use it, care must be given to ensure that all applicable security guidance is applied both at the device hardening level as well as the architectural level due to the fact that some of the settings may not be able to be configured in environments outside the DoD architecture.

## 1.7 Product Approval Disclaimer

The existence of a STIG does not equate to DoD approval for the procurement or use of a product.

STIGs provide configurable operational security guidance for products being used by the DoD. STIGs, along with vendor confidential documentation, also provide a basis for assessing compliance with Cybersecurity controls/control enhancements, which supports system Assessment and Authorization (A&A) under the DoD Risk Management Framework (RMF). DoD Authorizing Officials (AOs) may request available vendor confidential documentation for a product that has a STIG for product evaluation and RMF purposes from disa.stig_spt@mail.mil. This documentation is not published for general access to protect the vendor's proprietary information.

AOs have the purview to determine product use/approval IAW DoD policy and through RMF risk acceptance. Inputs into acquisition or pre-acquisition product selection include such processes as:

- National Information Assurance Partnership (NIAP) evaluation for National Security Systems (NSS) (http://www.niap-ccevs.org/) IAW CNSSP #11
- National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) (http://csrc.nist.gov/groups/STM/cmvp/) IAW Federal/DoD mandated standards
- DoD Unified Capabilities (UC) Approved Products List (APL) (http://www.disa.mil/network-services/ucco) IAW DoDI 8100.04

# 2. ASSESSMENT CONSIDERATIONS

## 2.1 Organization of the Checklist

The Database Security Checklist is composed of five major sections and four appendices. The organizational breakdown proceeds as follows:

| |
|---|
| Introduction |
| This section contains summary information about the sections and appendices that comprise the *Oracle Database Security Checklist* and defines its scope. Supporting documents consulted are listed in this section. |
| Oracle DBMS SRR Result Report |
| This section provides information for the reviewer to manually document review results of the Oracle DBMS SRR process for databases. |
| Oracle DBMS Security Review Procedures |
| This section documents the procedures that instruct the reviewer on how to determine security compliance with each security item for databases by following manual procedures. It includes a list of interfaces and tools required to complete the review. |
| Oracle DBMS Installation Check Procedures |
| This section includes the procedures to determine the final finding result for each check against Oracle DBMS Installations. |
| Oracle Database Check Procedures |
| This section includes the procedures to determine the final finding result for each check against Oracle Database Instances. |
| Appendix A: Information Assurance Vulnerability Management (IAVM) Bulletin Compliance |
| IAVMs issued against the Oracle DBMS product are assigned to the host platform. |
| Appendix B: Record of Changes |
| This appendix summarizes the changes made to this document |
| Appendix C: Checklist Discrepancy List |
| This appendix contains a list of general requirements that are not directly addressed in this checklist. |

## 2.2 Supported Versions

This checklist provides instructions for review of Oracle DBMS Server version 11.1.

## 2.3 Document Effective Date

This document is current as of the release date. Updates are made to support DoD policy, to correct errors, omissions and to clarify guidance.

## 2.4 Review Method

The goal is to perform a successful Security Readiness Review (SRR) of an Oracle DBMS. An SRR evaluation script that measures compliance for some check items listed in this document is available for supported versions of Oracle as listed in section 1.3.

## 2.5 Referenced Documents

The following table enumerates the documents and resources consulted:

**Table 2-1: Consulted Resources and Documents**

| Date | Document Description |
|---|---|
| 07 April 2008 | *JTF-GNO CTO 07-015 Revision 1, Public Key Infrastructure (PKI) Implementation, Phase 2* |
| 14 March 2007 | *Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, "DEFENSE-IN-DEPTH: INFORMATION ASSURANCE (IA) AND COMPUTER NETWORK DEFENSE (CND)" – Appendix* |
| 06 February 2003 | *Department of Defense (DOD) Instruction 8500.2, Information Assurance (IA) Implementation* |
| 24 October 2002 | *Department of Defense (DOD) Directive 8500.1, Information Assurance(IA) – Paragraph 4.18* |

## 3. ORACLE DBMS SRR RESULTS REPORT

Unclassified UNTIL FILLED IN

**CIRCLE ONE**
**FOR OFFICIAL USE ONLY** (mark each page)
**CONFIDENTIAL and SECRET** (mark each page and each finding)

**Classification is based on classification of system reviewed:**
Unclassified System = FOUO Checklist
Confidential System = CONFIDENTIAL
Checklist Secret System = SECRET Checklist
Top Secret System = SECRET Checklist (This checklist is effective as of **15 Jun 2008**.)

| | |
|---|---|
| Reviewer: | |
| System: | , Full): |
| **Finding Totals:** | **Comments:** |
| Category I: | |
| Category II: | |
| Category III: | |

### 3.1 Site Information

| |
|---|
| Site: |
| System Administrator Information:<br>Name: E-mail Address: |
| Phone # (Commercial): ( ) DSN: |
| ISSO Information:<br>Name: E-Mail Address<br>Phone # (Commercial) ( ) DSN: |

| DBA Information |
|---|
| E-mail Address: |
| Phone # (Commercial): ( ) DSN: |

## 3.2 System Information

| System Detail | |
|---|---|
| System ID or Host Name | |
| Hardware Platform | |
| Operating System | |
| Operating System Version | |
| Relational Database Management System | |
| Relational Database Management System Version | |
| RDBMS Software OS Owner Account Name | |
| Database Instance Identifier | |
| COTS/GOTS Application / Schema Name(s) | |
| Application Software OS Owner Account Name | |
| Instance IP Port Listening on | |
| Number/Name of Other Instances/RDBMS on this Host | |

**Table 3-1: Summary of Database SRR Findings By Category**

| Summary of Database SRR Findings By Category | | |
|---|---|---|
| **Category** | **Total Possible Findings** | **Actual Finding** |
| Category I | 9 | |
| Category II | 147 | |
| Category III | 24 | |
| Total Findings | 180 | |

# 4. ORACLE DBMS SECURITY REVIEW PROCEDURES

## 4.1 Review Process Notes

A security review of an Oracle Database DBMS may be completed by following the procedures in this section. Each security compliance item of interest is listed with procedures for determining whether the Oracle DBMS is configured to be compliant with the requirement or not. Each security item procedure is referred to as a "check". A security item is also referred to as "vulnerability".

There may be more than one installation of the Oracle DBMS software on a single host platform. There may be multiple Oracle Database Instances (SID) defined for a single Oracle DBMS software installation.

The checks are categorized into the following two categories and four types:

### 4.1.1 Categories:

**Oracle Home Checks** – These checks are applicable once per each Oracle DBMS software installation. Oracle refers to each installation as an Oracle Home and assigns an identifier to each. Some of these checks refer to the Oracle network communication configuration which in some cases occur only once per database host server.

**Oracle Database Checks** – These checks are applicable once per each Oracle Database Instance (SID). Each Oracle Database Instance (SID) must be checked, as there are significant security configurations that can be exploited per instance.

### 4.1.2 Types:

**Manual checks** – The reviewer must complete a technical procedure using SQL*Plus or a similar SQL interface to the Oracle database or another tool to determine the compliance status.

**Interview checks** – The procedure requires a review of available documentation and interviews of the ISSO, DBA or other database points-of-contact to determine the compliance status.

**Verify checks** – If the SRR evaluation script is used, it may or may not be able to determine a final finding result without action by the reviewer. If it is unable to provide a final finding result, it may provide information to help complete the manual procedures provided.

**Automated checks** – If the SRR evaluation script is used, it is able to determine the final finding result without action by the reviewer. Manual procedures are provided for manual review of compliance if desired.

The checks are ordered sequentially by STIGID number.

The checks are associated to either a DBMS (or installation) level or the database level. Installation checks are applicable to a single occurrence of an installation. This security level is meant to include operating system (OS) security configurations that affect the DBMS process and related services that are configured or controlled by security controls outside or beyond DBMS controls and those DBMS security controls that occur only once per installation and affect one or more occurrences at other security levels.

Database checks are controls configured by the DBMS that may occur more than once per DBMS installation. Therefore, a complete review of a single DBMS installation may include one status for each installation check and one status of each database check *per defined database*.

The purpose of this separation of checks is to ensure that all multiple occurrences of security controls are reviewed individually and to avoid duplication of control reviews that affect other security levels.

## 4.2 IAVM Compliance

Security patches required by the DoD IAVM process are reviewed during an operating system security review. Information for security patch compliance for Oracle DBMS is available in Appendix A of this Database Security Checklist.

## 4.3 Review Tools and Interfaces

You should run the review procedures and utilities listed below from the Oracle DBMS host system. In addition to the operating system tools listed below, some checks also refer to SQL commands that may be submitted to the database using Oracle's SQL*Plus command line utility. Other tools with the same capability as SQL*Plus may be used.

An SRR evaluation script is also available for use to complete the Oracle DBMS security review. The script provides results for all checks designated as being "automated". It also provides results for SQL commands specified to complete a manual review. These checks are indicated as "verify" checks. Checks for which the script provides no results are marked "Interview" or "Manual". The SRR script is run locally from the host prompt. The script is not tested for access to remote databases.

Windows platform tools:

**Windows explorer** – review file directory permissions and disk partition information
**Windows registry editor** – review registry values and permissions
**Windows Microsoft Management Console (MMC)** – review various Windows items including users, groups, and services

UNIX platform shell commands and tools:

vi, gedit or other text editor

The procedures also assume a familiarity with the Structured Query Language (SQL). Most DBMS provide a utility to connect to the DBMS and issue SQL commands directly to the DBMS.

This document does not provide instruction for use of any tools referenced. Please refer to vendor documentation for access to and use of the required vendor tools.

### 4.4 System Security Plan Overview

Some procedures within this checklist refer to the System Security Plan (SSP). The System Security Plan is referenced in the DoD Instruction 8500.2 in the following IA control as:

DCSD-1 IA Documentation

All appointments to required IA roles (e.g., AO and ISSM/ISSO) are established in writing, to include assigned duties and appointment criteria such as training, security clearance, and IT designation. A System Security Plan is established that describes the technical, administrative, and procedural IA program and policies that govern the DOD information system and identifies all IA personnel and specific IA requirements and objectives (e.g., requirements for data handling or dissemination, system redundancy, and backup or emergency response).

A template for creating an SSP may be found on the DIACAP Knowledge Service (https://diacap.iaportal.navy.mil/), DIACAP Resources, DIACAP Reference Library, Sample Documents, *ISP_Sample.doc (zipped)* or the National Institute of Standards and Technology (NIST), Special Publication (SP) 800-18, *Guide for Developing Security Plans for Federal Information Systems*. This document may be found at http://csrc.nist.gov/publications/PubsSPs.html. The DIACAP Knowledge Service also provides a matrix of documentation requirements for the IA Controls to those required under the previous DITSCAP System Security Authorization Agreement (SSAA). The matrix may be found under IA Controls, Information on the IA Controls Matrix of IA Controls to Documentation.

Information required and verified by the procedures in this checklist should be contained in the SSP under the IA control referenced. However, this document concerns itself only with the specific controls referenced in it and does not review and verify the entirety of the SSP.

### 4.5 Automated Information System (AIS) Functional Architecture Document

The DoDI 8500.2 defines an AIS functional architecture document under IA control DCFA as:

DCFA-1 Functional Architecture for AIS Applications

For AIS applications, a functional architecture that identifies the following has been developed and is maintained:

All external interfaces, the information being exchanged, and the protection mechanisms associated with each interface - user roles required for access control and the access privileges assigned to each role (See ECAN)
Unique security requirements (e.g., encryption of key data elements at rest)
Categories of sensitive information processed or stored by the AIS application, and their specific protection plans (e.g., Privacy Act, HIPAA)
Restoration priority of subsystems, processes, or information (See COEF)

Additional information may be obtained for this IA control from the DIACAP Knowledge Service.

## 4.6 Sensitive Data Protection and Definition

Databases, as frequent repositories for sensitive data, are often relied upon for providing an additional layer of protection for such data. The responsibility for determining what protections should be employed for sensitive data falls to the Information Owner as the person that best understands the purpose, function, and the possible impact of unauthorized release of the data. Most commonly, authentication and authorizations are sufficient to protect data against unauthorized release. However, in some cases encryption may be used to assist in protecting against disclosure where authorizations do not provide needed restrictions. For example, the access provided to DBAs to administer the DBMS provides them with access to all data stored within the database.

The DoDD 8500.1 provides the following definition for sensitive data:

Information, the loss, misuse, or unauthorized access to or modification of, could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of title 5, United States Code, "The Privacy Act", but which has not been specifically authorized under criteria established by Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy (Section 278g-3 of title 15, United States Code, "The Computer Security Act of 1987"). Examples of sensitive information include, but are not limited to information in DOD payroll, finance, logistics and personnel management systems. Sensitive information sub-categories include, but are not limited to, the following:

For Official Use Only (FOUO) - In accordance with DOD 5400.7-R (reference (ab)), DOD information exempted from mandatory public disclosure under the Freedom of Information Act (FOIA) Privacy Data. Any record that is contained in a system of records as defined in the Privacy Act of 1974 (5 U.S.C. 552a) (reference (z)) and information the disclosure of which would constitute an unwarranted invasion of personal privacy.

DoD Unclassified Controlled Nuclear Information (DoD UCNI) - Unclassified Information on security measures (including security plans, procedures, and equipment) for the physical protection of DoD Special Nuclear Material (SNM), equipment, or facilities in accordance with DoD Directive 5210.83. Information is Designated DoD UCNI only when it is determined that its unauthorized disclosure could reasonably be expected to have a significant adverse effect on the health and safety of the public or the common defense and security by increasing significantly the likelihood of the illegal production of nuclear weapons or the theft, diversion, or sabotage of DoD SNM, equipment, or facilities.

Unclassified Technical Data - Data that is not classified but is subject to export control and is withheld from public disclosure according to DoD Directive 5230.25.

Proprietary Information - Information that is provided by a source or sources under the condition that it not be released to other sources.

Foreign Government Information - Information that originated from a foreign government and that is not classified CONFIDENTIAL or higher, but must be protected in accordance with DOD 5200.1-R.

Department of State Sensitive But Unclassified (DoS SBU) - Information that originated from the Department of State (DoS) that has been determined to be SBU under appropriate DoS information security policies.

Drug Enforcement Administration (DEA) Sensitive Information - Information that is originated by the Drug Enforcement Administration and requires protection against unauthorized disclosure to protect sources and methods of investigative activity, evidence, and the integrity of pretrial investigative reports.

## 4.7 Process Notes

The SRR evaluation script and many manual procedures require Oracle DBA privileges to the database and host platform. Some operating system commands require Root or Administrator privileges to the host operating system. This will vary based on the permissions assigned to the OS account used. It is recommended the account used for installation of the Oracle software be used to process the security review as this account is expected to have the access required. An authorized DBA or the ISSO should log and monitor the use of this account.

The SRR script also creates temporary tables in the Oracle Database. Definitions for the tables are included in the script file "dbsrr-oracle-tables.sql". The tables are created in the USERS tablespace by default, however, if tables currently exist, the script will use those tables. This allows the DBA to control which tablespace and storage is used by the SRR script. This should be reviewed and considered as part of configuration management especially on production systems. Please see the readme and release notes of the script for additional information.

## 4.8 Check Reference Numbering Scheme

The checks use two different reference numbers: the STIGID and GroupID. The STIGID is a manually assigned reference number. The database STIGID assignments including those for Oracle are prefixed with two letters that indicate the following:

**DG** – Identifies a general database check and the fundamental requirement is specified for any DBMS product where available. The Oracle-specific checks and fixes are listed in the rule STIGID for these DG checks
**DO** – Identifies an Oracle specific check and does not apply as written to any other DBMS product.

Only checks of type "DG" and "DO" are included in this checklist. All checks provide a mapping to General security requirements. Note that some CAT findings may be higher for the DO checks than their mapped General checks due to the potential ability to be exploited and access to elevated privileges.

## 4.9 Version Specific Checks

Any security checks or options applicable to a specific version or versions of the DBMS product should be performed in accordance with vendor-provided security guidance and best practices.

## 4.10 Documentation Conventions

Conventions used in this document:

The "\" character – This character is used to separate selection items. For example, registry folders and predefined keys and key values are listed as HKLM\Software\Microsoft where HKLM represents the top registry folder HKEY_LOCAL_MACHINE, Software is a folder under HKLM, etc. In addition, Start\ All Programs means click on the Start button in the Windows task bar and then select the All Programs icon.

The "[ ]" characters are used to indicate that a replacement value provided by the reviewer is required. For example, the [partial] SQL query command, "alter user [username]" where [username] should be replaced by the reviewer with the appropriate user name, (e.g., "alter user SYS"). The "[]" characters should not be included in the command.

## 4.11 Procedure Table Data Information Assurance (IA) Control

Each check is derived and associated with an IA Control from the DOD Instruction 8500.2. These are listed in the enclosures for the instruction and are applicable to the DBMS based on the Mission Assurance Category (MAC) determined for the system. Where the IA breakdown based on MAC is not listed in the table in this document, the check requirement

applies to all level systems or the IA control does not have breakdowns. Where a check applies to only one IA control and MAC level, the level is specified in the table.

### 4.11.1 Vulnerability Key:

This is the check reference number.

### 4.11.2 STIG ID:

This is the STIG reference number.

### 4.11.3 Short Name:

This is the title for the check reference.

### 4.11.4 Long Name:

This is a long name (or short description) for the check reference number.

### 4.11.5 IA Controls:

This is the check reference mapping in DoDI 8500.2.

### 4.11.6 Condition:

This indicates whether the check is performed once per defined database installation (Oracle Home) or once per Oracle Database Instance (Oracle Database).

### 4.11.7 Policy:

Each check is assigned a Gold, Platinum or All Policies (both) designation based on implementation difficulty. Gold requirements are those whose implementation is unlikely to interrupt system operation. Platinum requirements require consideration that is more careful and testing prior to implementation. Please note that no changes to the DBMS should be made without a careful review or test of potential impact.

### 4.11.8 Mission Assurance Category (MAC)/Confidentiality Grid:

This field shows the applicability of the check based on the mission criticality and confidentiality of the system under review. The DODI 8500.2 defines three levels of mission criticality where a MAC level of one requires the highest level of integrity and availability protection and a level three requires the lowest. The confidentiality levels are Public, Sensitive, and Classified. Please see DODI 8500.2 for more information on determining the MAC and Confidentiality for your DBMS system.

### 4.11.9 Severity:

This is the severity code assignment for this check. Severity code definitions are documented in Section 1.1 – Overview in this document.

### 4.11.10 Severity Override Guidance:

If populated, either provides an exception to DoD requirement for this check or a reduction of category level based on reported findings.

### 4.11.11 Vulnerability Discussion:

This field contains a brief discussion of the vulnerability.

### 4.11.12 Documentable:

This field indicates whether the check is documentable (Yes) or not (No).

### 4.11.13 Documentable Explanation:

This field contains the explanation for a documentable check.

### 4.11.14 Responsibility:

This field indicates the role or position responsible for ensuring compliance of this check.

### 4.11.15 Mitigations:

This field contains any documented as allowable vulnerability mitigations for the check.

### 4.11.16 References:

This field contains references to documentation for the check.

### 4.11.17 Checks:

Consist of these three fields:

#### 4.11.17.1 Check ID:

Check ID contains the check reference identifier, usually in the form "DB-STIGID- Product", where DB = Database, STIGID = the STIG identifier and, optionally, Product = DBMS product or product version (i.e. Generic, SQLServer8, ORACLE10, etc.).

#### 4.11.17.2 Check Type (in parenthesis):

This indicates the method available for determining the compliance to the check. A check type of *interview* means that the check does not require any technical or system hands- on actions. Rather it requires a review of documentation and in some cases verbal confirmation by the DBA or ISSO. A check type of *manual* indicates the check procedure requires hands-on technical review of the security configuration item.

#### 4.11.17.3 Check Text:

Check Text contains the required methods, processes, or procedures used to determine compliance for the check.

### 4.11.18 Fixes:

Consist of these three fields:

#### 4.11.18.1 Fix ID:

Fix ID contains the fix reference identifier, usually in the form "DB-STIGID-Product", where DB = Database, STIGID = the STIG identifier and, optionally, Product = DBMS product or product version (i.e. Generic, SQLServer8, ORACLE10, etc.).

#### 4.11.18.2 Fix Type (in parenthesis):

A fix type of *Manual* is the default.

#### 4.11.18.3 Fix Text:

Fix Text contains the required methods, processes or procedures for obtaining check compliance and may contain recommendations for consideration.

# APPENDIX A: INFORMATION ASSURANCE VULNERABILITY MANAGEMENT (IAVM) BULLETIN COMPLIANCE

Please check the IAVM - USCYBERCOM website (requires .mil or .gov address and/or PKI certificate for access) to confirm whether the DBMS under review has any specific vulnerability bulletins published against it.

https://iavm.csd.disa.mil

## APPENDIX B: RECORD OF CHANGES

Following is a list of significant changes to this document from the previous release of Oracle:

| CHANGE |
|---|
| Updated Appendix B – Record of Changes |

Following is a list of checks that were modified from the previous release:

**Table B-1: Checks Modified from Previous Version**

| STIGID | TITLE | CHANGE |
|---|---|---|
| DG0001 | DBMS version support | No Changes |
| DG0002 | DBMS version upgrade plan | No Changes |
| DG0003 | DBMS security patch level | No Changes |
| DG0004 | DBMS application object owner accounts | No Changes |
| DG0005 | DBMS administration OS accounts | No Changes |
| DG0007 | DBMS security compliance | No Changes |
| DG0008 | DBMS application object ownership | No Changes |
| DG0009 | DBMS software library permissions | No Changes |
| DG0010 | DBMS software monitoring | No Changes |
| DG0011 | DBMS Configuration Management | No Changes |
| DG0012 | DBMS software storage location | No Changes |
| DG0013 | Database backup procedures | No Changes |
| DG0014 | DBMS demonstration and sample databases | No Changes |
| DG0015 | DBMS data definition language use | No Changes |
| DG0016 | DBMS unused components | Reworded |
| DG0017 | DBMS shared production/development use | No Changes |
| DG0019 | DBMS software ownership | No Changes |
| DG0020 | DBMS backup and recovery testing | No Changes |
| DG0021 | DBMS software and configuration baseline | No Changes |
| DG0025 | DBMS encryption compliance | No Changes |
| DG0029 | Database auditing | No Changes |
| DG0030 | DBMS audit data maintenance | No Changes |
| DG0031 | DBMS audit of changes to data | No Changes |
| DG0032 | DBMS audit record access | No Changes |
| DG0040 | DBMS software owner account access | Reworded |
| DG0041 | DBMS installation account use logging | No Changes |
| DG0042 | DBMS software installation account use | No Changes |
| DG0050 | DBMS software and configuration file monitoring | No Changes |
| DG0051 | Database job/batch queue monitoring | No Changes |
| DG0052 | DBMS software access audit | No Changes |
| DG0053 | DBMS client connection definition file | No Changes |

| STIGID | TITLE | CHANGE |
|---|---|---|
| DG0054 | DBMS software access audit review | No Changes |
| DG0060 | DBMS shared account authorization | No Changes |
| DG0063 | DBMS restore permissions | Reworded |
| DG0064 | DBMS backup and restoration file protection | No Changes |
| DG0065 | DBMS PKI authentication | No Changes |
| DG0066 | DBMS temporary password procedures | No Changes |
| DG0067 | DBMS account password external storage | No Changes |
| DG0068 | DBMS application password display | No Changes |
| DG0069 | Production data import to development DBMS | No Changes |
| DG0070 | DBMS user account authorization | No Changes |
| DG0071 | DBMS password change variance | No Changes |
| DG0073 | DBMS failed login account lock | No Changes |
| DG0074 | DBMS inactive accounts | No Changes |
| DG0075 | DBMS links to external databases | No Changes |
| DG0076 | Sensitive data import to development DBMS | No Changes |
| DG0077 | Production data protection on a shared system | No Changes |
| DG0078 | DBMS individual accounts | No Changes |
| DG0079 | DBMS password complexity | No Changes |
| DG0080 | DBMS application user privilege assignment review | No Changes |
| DG0083 | DBMS audit report automation | No Changes |
| DG0085 | Minimum DBA privilege assignment | No Changes |
| DG0086 | DBMS DBA role privilege monitoring | No Changes |
| DG0087 | DBMS sensitive data labeling | No Changes |
| DG0088 | DBMS vulnerability mgmt and IA compliance testing | No Changes |
| DG0089 | Developer DBMS privileges on production databases | No Changes |
| DG0090 | DBMS sensitive data identification and | No Changes |
| DG0091 | DBMS source code encoding or encryption | No Changes |
| DG0092 | DBMS data file encryption | No Changes |
| DG0093 | Remote administrative connection encryption | No Changes |
| DG0095 | DBMS audit trail data review | No Changes |
| DG0096 | DBMS IA policy and procedure review | No Changes |
| DG0097 | DBMS testing plans and procedures | No Changes |
| DG0098 | DBMS access to external local objects | No Changes |
| DG0099 | DBMS access to external local executables | No Changes |
| DG0100 | DBMS replication account privileges | No Changes |
| DG0101 | DBMS external procedure OS account privileges | No Changes |
| DG0102 | DBMS services dedicated custom account | No Changes |

| STIGID | TITLE | CHANGE |
|---|---|---|
| DG0103 | DBMS Listener network restrictions | Updated Long Name, Updated Vulnerability Discussion |
| DG0104 | DBMS service identification | No Changes |
| DG0105 | DBMS application user role privilege assignment | No Changes |
| DG0106 | Database data encryption configuration | No Changes |
| DG0107 | DBMS sensitive data identification | No Changes |
| DG0108 | DBMS restoration priority | No Changes |
| DG0109 | DBMS dedicated host | No Changes |
| DG0110 | DBMS host shared with a security service | No Changes |

| STIGID | TITLE | CHANGE |
|---|---|---|
| DG0111 | DBMS dedicated software directory and partition | Replaced in STIG release V1R12 by DG7001, 2, 3. |
| DG0112 | DBMS system data file protection | No Changes |
| DG0113 | DBMS dedicated data files | No Changes |
| DG0115 | DBMS trusted recovery | No Changes |
| DG0116 | DBMS privileged role assignments | No Changes |
| DG0117 | DBMS administrative privilege assignment | No Changes |
| DG0118 | ISSM review of change in DBA assignments | No Changes |
| DG0119 | DBMS application user role privileges | No Changes |
| DG0120 | DBMS application user access to external objects | No Changes |
| DG0121 | DBMS application user privilege assignment | No Changes |
| DG0122 | Sensitive data access | No Changes |
| DG0123 | DBMS Administrative data access | No Changes |
| DG0124 | DBA account use | No Changes |
| DG0125 | DBMS account password expiration | No Changes |
| DG0126 | DBMS account password reuse | No Changes |
| DG0127 | DBMS account password easily guessed | No Changes |
| DG0128 | DBMS default passwords | Code corrected |
| DG0129 | DBMS passwords in transit | No Changes |
| DG0130 | DBMS passwords in executables | No Changes |
| DG0133 | DBMS Account lock time | No Changes |
| DG0135 | DBMS connection alert | No Changes |
| DG0138 | DBMS access to sensitive data | No Changes |
| DG0140 | DBMS security data access | No Changes |
| DG0141 | DBMS access control bypass | No Changes |
| DG0142 | DBMS Privileged action audit | No Changes |
| DG0145 | DBMS audit record content | No Changes |
| DG0146 | DBMS connection block audit | No Changes |
| DG0152 | DBMS network port, protocol and services (PPS) use | No Changes |
| DG0153 | DBMS DBA roles assignment approval | No Changes |
| DG0154 | DBMS System Security Plan | No Changes |
| DG0155 | DBMS trusted startup | No Changes |
| DG0157 | DBMS remote administration | No Changes |
| DG0158 | DBMS remote administration audit | No Changes |
| DG0159 | Review of DBMS remote administrative access | No Changes |
| DG0161 | DBMS Audit Tool | No Changes |
| DG0165 | DBMS symmetric key management | No Changes |
| DG0166 | Protection of DBMS asymmetric encryption keys | No Changes |
| DG0167 | Encryption of DBMS sensitive data in transit | No Changes |
| DG0171 | DBMS interconnections | No Changes |

| STIGID | TITLE | CHANGE |
|---|---|---|
| DG0172 | DBMS classification level audit | No Changes |
| DG0175 | DBMS host and component STIG compliancy | No Changes |
| DG0176 | DBMS audit log backups | No Changes |
| DG0179 | DBMS warning banner | No Changes |
| DG0186 | DBMS network perimeter protection | No Changes |
| DG0187 | DBMS software file backups | No Changes |
| DG0190 | DBMS remote system credential use and access | No Changes |
| DG0191 | DBMS credential protection | No Changes |
| DG0192 | DBMS fully-qualified name for remote access | No Changes |
| DG0194 | DBMS developer privilege monitoring on shared DBMS | No Changes |
| DG0195 | DBMS host file privileges assigned to developers | No Changes |
| DG0198 | DBMS remote administration encryption | No Changes |
| DG7001 | Dedicated directory for DBMS audit files | Replaces DG0111 in STIG release V1R12 |
| DG7002 | Dedicated directories for DBMS control files | Replaces DG0111 in STIG release V1R12 |
| DG7003 | Dedicated directories for DBMS redo log | Replaces DG0111 in STIG release V1R12 |
| DO0100 | Oracle version support | No Changes |
| DO0120 | Oracle process account host system privileges | No Changes |
| DO0140 | Oracle default account access | No Changes |
| DO0145 | Oracle SYSDBA OS group membership | No Changes |
| DO0155 | Oracle default tablespace assignment | Code modified |
| DO0157 | Oracle storage use privileges | No Changes |
| DO0190 | Oracle audit table ownership | No Changes |
| DO0210 | Oracle shared replication account access | No Changes |
| DO0220 | Oracle instance names | No Changes |
| DO0221 | Oracle default SID name | No Changes |
| DO0231 | Oracle application object owner tablespaces | No Changes |
| DO0234 | Oracle AUDIT_FILE_DEST parameter | No Changes |
| DO0235 | Oracle USER_DUMP_DEST parameter | No Changes |
| DO0236 | Oracle BACKGROUND_DUMP_DEST parameter | No Changes |
| DO0237 | Oracle CORE_DUMP_DEST parameter | No Changes |
| DO0238 | Oracle LOG_ARCHIVE_DEST parameter | No Changes |
| DO0240 | Oracle OS_ROLES parameter | No Changes |
| DO0243 | Oracle _TRACE_FILES_PUBLIC parameter | No Changes |
| DO0250 | Oracle database link usage | No Changes |
| DO0260 | Oracle control file availability | No Changes |
| DO0270 | Oracle redo log file availability | No Changes |

| STIGID | TITLE | CHANGE |
|---|---|---|
| DO0286 | Oracle connection timeout parameter | No Changes |
| DO0287 | Oracle SQLNET.EXPIRE_TIME parameter | No Changes |
| DO0320 | Oracle PUBLIC role privileges | No Changes |
| DO0340 | Oracle application administration roles enablement | No Changes |
| DO0350 | Oracle system privilege assignment | No Changes |
| DO0360 | DBMS mid-tier application account access | No Changes |
| DO0420 | Oracle XML DB | No Changes |
| DO0430 | Oracle management agent use | No Changes |
| DO3440 | Oracle DBA role assignment | No Changes |
| DO3447 | Oracle OS_AUTHENT_PREFIX parameter | No Changes |
| DO3451 | WITH GRANT OPTION privileges | No Changes |
| DO3475 | Oracle PUBLIC access to restricted packages | No Changes |
| DO3536 | Oracle IDLE_TIME profile parameter | No Changes |
| DO3538 | Oracle REMOTE_OS_AUTHENT parameter | No Changes |
| DO3539 | Oracle REMOTE_OS_ROLES parameter | No Changes |
| DO3540 | Oracle SQL92_SECURITY parameter | No Changes |
| DO3546 | Oracle REMOTE_LOGIN_PASSWORDFILE parameter | No Changes |
| DO3609 | System privileges granted WITH ADMIN OPTION | No Changes |
| DO3610 | Oracle minimum object auditing | No Changes |
| DO3612 | Oracle system privilege assignment | No Changes |
| DO3622 | Oracle roles granted WITH ADMIN OPTION | No Changes |
| DO3630 | Oracle listener authentication | No Changes |
| DO3685 | Oracle O7_DICTIONARY_ACCESSIBILITY parameter | No Changes |
| DO3686 | Oracle SYS.LINK$ table access | No Changes |
| DO3689 | Oracle object permission assignment to PUBLIC | No Changes |
| DO3696 | Oracle RESOURCE_LIMIT parameter | No Changes |
| DO5037 | Oracle SQLNet and listener log files protection | No Changes |
| DO6740 | Oracle listener ADMIN_RESTRICTIONS parameter | No Changes |
| DO6746 | Oracle Listener host references | No Changes |
| DO6747 | Connection Manager remote administration | No Changes |
| DO6749 | SEC_MAX_FAILED_LOGIN_ATTEMPTS | Reinstated in STIG Release V1R12 |
| DO6750 | SEC_PROTOCOL_ERROR_FURTHER_ACTION | Reinstated in STIG Release V1R12 |
| DO6751 | SQLNET.ALLOWED_LOGON_VERSION | No Changes |
| DO6753 | Oracle Application Express | No Changes |
| DO6754 | Oracle Configuration Manager | No Changes |

## APPENDIX C: CHECKLIST DISCREPANCY LIST

Below is a list of general requirements that are not directly addressed in this checklist:

**Table C-1: General Requirements Not Addressed**

| General Database Requirement | Disposition |
|---|---|
| *(DG0072: CAT II) The DBA will ensure users are not allowed to change their database account passwords more than once every 24 hours without ISSO approval where supported by the DBMS. (This requirement does not apply to password changes after password reset actions initiated by the DBA or application administrator).* | This check was removed due to the inability to develop a programmatic solution in Oracle 10.1 and Oracle 10.2 to support this requirement. |
| *(DG0084: CAT III) The DBA will ensure DBMS resource controls are enabled to clear residual data from released object stores.* | This feature is not configurable in Oracle 10.1 and Oracle 10.2. It is included by default. |
| *(DG0114: CAT II) The DBA will ensure files critical to database recovery are protected by employment of database and OS high-availability options such as storage on RAID devices.* | This is included under checks DO0260 and DO0270. |
| *(DG0131: CAT III) The DBA will change or delete default account usernames where supported.* | Oracle 10.1 and 10.2 do not support changing default user names. |
| *(DG0134: CAT II) The DBA will configure where supported by the DBMS a limit of concurrent connections by a single database account to the limit specified in the System Security Plan, a number determined by testing or review of logs to be appropriate for the application. The limit will not be set to unlimited except where operationally required and documented in the System Security Plan.* | Oracle 10.1 and 10.2 do not recommend limiting user connections. |
| *(DG0151: CAT II) The SA/DBA will ensure random port assignment to network connections is disabled when traversing network firewalls.* | This is included under DG0152. |
| *(DG0156: CAT III) The ISSM will assign and authorize ISSO responsibilities for the DBMS.* | This is checked under an Enclave review. The ISSM is not expected to be available for a DB review. |

| General Database Requirement | Disposition |
|---|---|
| *(DG0160: CAT III) The DBA will ensure database connection attempts are limited to a specific number of times within a specific time as specified in the System Security Plan. The limit will not be set to unlimited.* | This is covered under separate Oracle checks. |
| *(DG0170: CAT II) The DBA will configure the DBMS to enable transaction rollback and transaction journaling or their technical equivalent to maintain data consistency and recovery during operational cancellations, failures, or other interruptions.* | This is not configurable in Oracle 10.1 and 10.2. It is operational by default. |
| *(DG0193: CAT II) The DBA will set expiration times for non-interactive database application account passwords to 365 days or less where supported by the DBMS.* | This is included under check DG0125. |