Omega DB Security Reporter ™

For Oracle Database

July 2024 | Version 2.4

Compliance with CIS Benchmark for Oracle

Omega DB Security Reporter
support for
CIS Compliance

www.dataplus-al.com

TABLE OF CONTENTS

1. Overview

This document describes the support of:

Omega DB Security Reporter, version 2.4 - by DATAPLUS

for

CIS Oracle Database 19c Benchmark, version 1.2.0, by Center for Internet Security (CIS), published on December 2023.

Document Information:

Document Author:	Altin Karaulli – DATAPLUS
Document Date:	July-2024

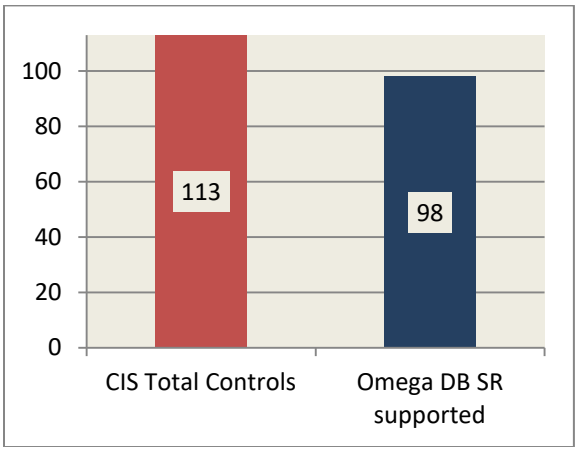
2. Summary Executive

Summary support for CIS Oracle Database 19c Benchmark

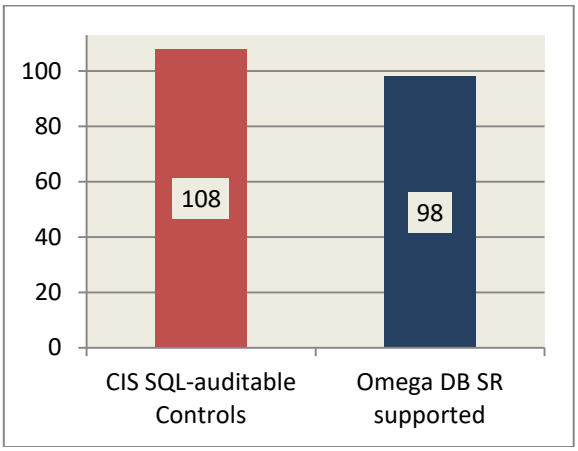
The CIS Oracle Database 19c Benchmark version 1.2.0 has:

CIS Total controls	113
CIS SQL-auditable controls	108

SQL-auditable controls comprise almost all (95.6%) of the CIS Benchmark. Omega DB Security Reporter is a network PL/SQL Scanner. It assesses CIS controls that are auditable by SQL commands. Omega DB Security Reporter supports 98 such controls.



CIS controls and Omega DB SR

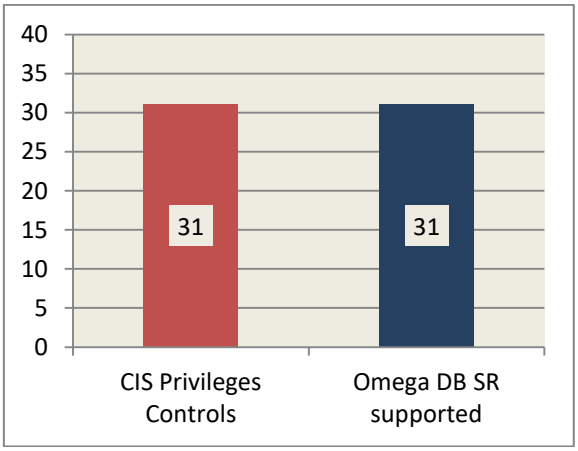


CIS SQL-auditable controls and Omega DB SR

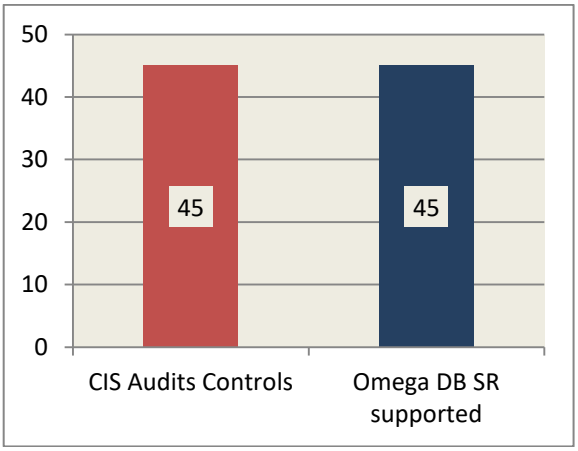
Omega DB Security Reporter support details for controls of the CIS Oracle Database 19c Benchmark are found in the next Chapter 3 "CIS Compliance".

CIS Privileges and Audits controls

31 Privilege controls and 45 Audit ones comprise 76 of the 108 SQL-auditable controls; they are subject of frequent changes in real-life environments!



CIS Privileges Controls



CIS Audit Controls

Omega DB Security Reporter supports 100% of them – and in a very advanced mode, as described in Chapter 4 "Advanced Compliance".

3. CIS Compliance

CIS Oracle Database 19c Benchmark topics and Omega DB Security Reporter support

CIS Benchmark Topic	Controls	SQL Control	Omega DB SR	Notes
1 Oracle Database Installation and Patching Requirements	1	0	0	**1)**
2 Oracle Parameter Settings				
2.1 Listener Settings	2	0	0	**1)**
2.2 Database Settings	17	17	14	**2)**
2.3 SQLNET.ORA Settings	2	0	0	**1)**
3 Oracle Connection and Login Restrictions	9	9	8	**3)**
4 Users	6	6	0	**4)**
5 Privileges & Grants & ACLs				
5.1 Excessive Table, View and Package Privileges				
5.1.1 Public Privileges	7	7	7	**5)**
5.1.2 Non-Default Privileges	1	1	1	**5)**
5.1.3 Other Privileges	3	3	3	**5)**
5.2 Excessive System Privileges	16	16	16	**5)**
5.3 Excessive Role Privileges	4	4	4	**5)**
6 Audit/Logging Policies and Procedures				
6.1 Traditional Auditing	18	18	18	**5)**
6.2 Unified Auditing	27	27	27	**5)**
	113	**108**	**98**	

Notes:

1. Omega DB Security Reporter is a network PL/SQL Scanner. SQL-auditable controls only are supported.

2. All parameters supported, except for: _trace_files_public, RESOURCE_LIMIT, PDB_OS_CREDENTIAL.

3. All restrictions supported, except for SESSIONS_PER_USER.

4. CIS Benchmark's topic User contains individual controls either not considered by Omega DB Security Reporter, or that represent one-time tasks.

5. All supported!

Unsupported SQL-auditable controls in this version will be subject of next releases of Omega DB Security Reporter.

4. Advanced Compliance

Advanced assessment for Compliance with Omega DB Security Reporter

4.1 Importance of Privileges

Everything a user can do in an Oracle Database, it can do because it is being granted a privilege, either as a direct grant, or an indirect grant (through a role/roles), granted to PUBLIC, or because it is acting on an object whose owner it is.

Even those controls that on a first glance seem not related directly to privileges, once they are set to the correct values, depend on the status of the privileges for later eventual changes.

CIS Topic	Required Privileges
2.2 Database Settings	System Privilege ALTER SYSTEM
3 Oracle Connection and Login Restrictions	System Privileges CREATE/ALTER USER and ALTER PROFILE
6.1 Traditional Auditing	System Privileges AUDIT SYSTEM and AUDIT ANY
6.2 Unified Auditing	System Privilege AUDIT SYSTEM

Thus, System Privileges do interfere with almost all of the Benchmark's controls! Of same importance are the Object Privileges – for both Oracle objects and user application objects.

4.2 Importance of Audits

"Ensure <Privilege> is revoked from <unauthorized grantee>" – this you will see on every item of the Privileges topics in the CIS Benchmark. While a top requirement – this is not enough. Revoking privileges from grantees that do not require them for their tasks is the easy part.

What about grantees that do need them for their tasks? The answer is: Audit is the remediation!

Assessment of Audit must include user application objects.

4.3 Privileges vs Audits

Assessing privileges and audits separately is also not enough. An in-depth assessment must confront privileges vs audits for every couple of assessed item and user.

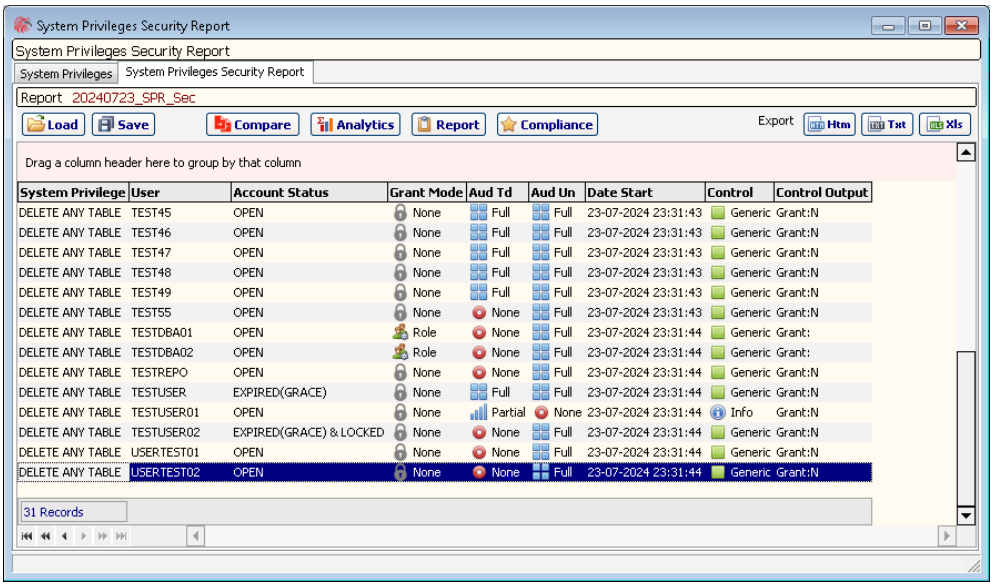
Omega DB Security Reporter addresses this top importance topic via its two advanced reports:

- System Privileges Security
- Object Operations Security

4.4 System Privileges Security

Omega DB Security Reporter features an advanced security report on System Privileges:

System Privilege Security Report combines system privilege grant status with traditional/unified audit status for each assessed system privilege and user.



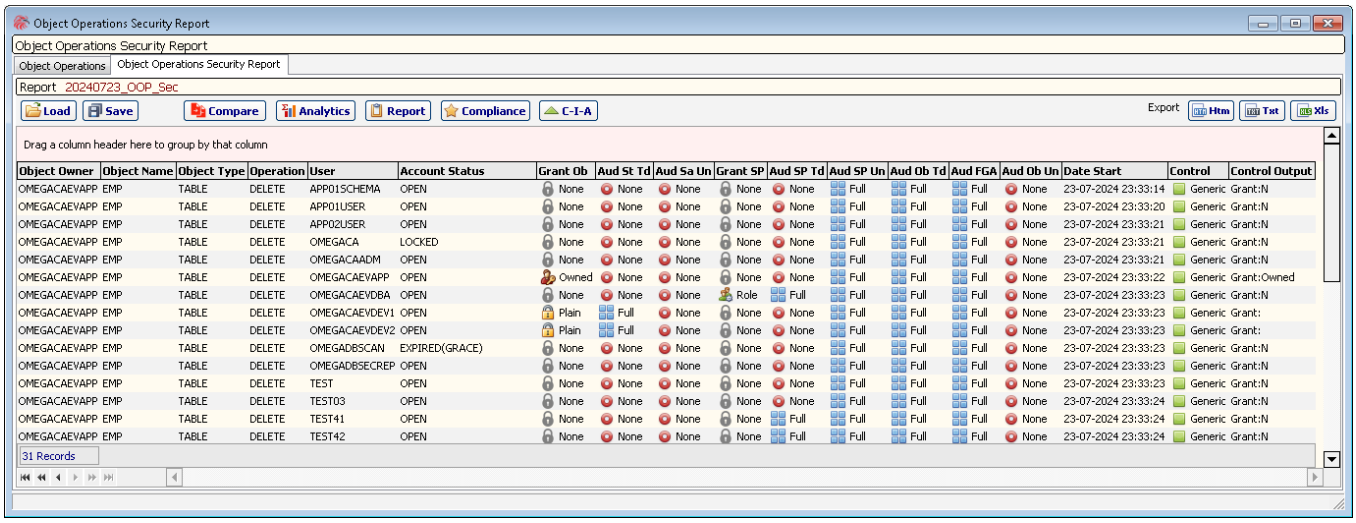
The evaluation result for every assessed couple of System Privilege – User is calculated on behalf of:

- User account status
- Grant Status
- Traditional Audit
- Unified Audit

4.5 Object Operations Security

Omega DB Security Reporter features an advanced security report on Object Operations:

Object Operations Security Report combines system/object privilege grants status with system/statement/object audit status (for traditional and unified) for each assessed object operation and user.



Object Owner	Object Name	Object Type	Operation	User	Account Status	Grant Ob	Aud St Td	Aud Sa Un	Grant SP	Aud SP Td	Aud SP Un	Aud Ob Td	Aud FGA	Aud Ob Un	Date Start	Control	Control Output
OMEGACAEVAPP	EMP	TABLE	DELETE	APP01SCHEMA	OPEN	None	None	None	None	None	Full	Full	Full	None	23-07-2024 23:33:14	Generic	Grant:N
OMEGACAEVAPP	EMP	TABLE	DELETE	APP01USER	OPEN	None	None	None	None	None	Full	Full	Full	None	23-07-2024 23:33:20	Generic	Grant:N
OMEGACAEVAPP	EMP	TABLE	DELETE	APP02USER	OPEN	None	None	None	None	None	Full	Full	Full	None	23-07-2024 23:33:21	Generic	Grant:N
OMEGACAEVAPP	EMP	TABLE	DELETE	OMEGACA	LOCKED	None	None	None	None	None	Full	Full	Full	None	23-07-2024 23:33:21	Generic	Grant:N
OMEGACAEVAPP	EMP	TABLE	DELETE	OMEGACAADM	OPEN	None	None	None	None	None	Full	Full	Full	None	23-07-2024 23:33:21	Generic	Grant:N
OMEGACAEVAPP	EMP	TABLE	DELETE	OMEGACAEVAPP	OPEN	Owned	None	None	None	None	Full	Full	Full	None	23-07-2024 23:33:22	Generic	Grant:Owned
OMEGACAEVAPP	EMP	TABLE	DELETE	OMEGACAEVDBA	OPEN	None	None	None	Role	Full	Full	Full	Full	None	23-07-2024 23:33:23	Generic	Grant:N
OMEGACAEVAPP	EMP	TABLE	DELETE	OMEGACAEVDEV1	OPEN	Plain	Full	None	None	None	Full	Full	Full	None	23-07-2024 23:33:23	Generic	Grant:
OMEGACAEVAPP	EMP	TABLE	DELETE	OMEGACAEVDEV2	OPEN	Plain	Full	None	None	None	Full	Full	Full	None	23-07-2024 23:33:23	Generic	Grant:
OMEGACAEVAPP	EMP	TABLE	DELETE	OMEGADBSCAN	EXPIRED(GRACE)	None	None	None	None	None	Full	Full	Full	None	23-07-2024 23:33:23	Generic	Grant:N
OMEGACAEVAPP	EMP	TABLE	DELETE	OMEGADBSECREP	OPEN	None	None	None	None	None	Full	Full	Full	None	23-07-2024 23:33:23	Generic	Grant:N
OMEGACAEVAPP	EMP	TABLE	DELETE	TEST	OPEN	None	None	None	None	None	Full	Full	Full	None	23-07-2024 23:33:23	Generic	Grant:N
OMEGACAEVAPP	EMP	TABLE	DELETE	TEST03	OPEN	None	None	None	None	None	Full	Full	Full	None	23-07-2024 23:33:24	Generic	Grant:N
OMEGACAEVAPP	EMP	TABLE	DELETE	TEST41	OPEN	None	None	None	None	Full	Full	Full	Full	None	23-07-2024 23:33:24	Generic	Grant:N
OMEGACAEVAPP	EMP	TABLE	DELETE	TEST42	OPEN	None	None	None	None	Full	Full	Full	Full	None	23-07-2024 23:33:24	Generic	Grant:N

The evaluation result for every assessed couple of Object Operation – User is calculated on behalf of:

- User account status
- Object grant status
- Traditional Audit for Statement
- Unified Audit for System Action
- System Privilege grant status
- Traditional Audit for System Privilege
- Unified Audit for System Privilege
- Traditional Object Audit
- FGA Object Audit
- Unified Object Audit

This report enables the very important assessment of user application objects!

4.6 Application – the final Compliance

The triangle of Security is CIA:

C – Confidentiality
I – Integrity
A - Availability

Your application's data stored inside and Oracle database are the final price of a malicious intruder.

These data must be assessed for:

Confidentiality	SELECT
Integrity	INSERT, DELETE, UPDATE, DROP, …
Availability	DELETE, DROP, TRUNCATE, …

Omega DB Security Reporter enables assessment and full visibility on user application objects, users and roles.