Oracle Database 12c Release 2 Enterprise Edition (with Database Vault and Multitenant) Security Target

Evaluation Assurance Level (EAL): EAL2+

Doc No: 2030-000-D102
Version: 1.4
13 December 2018

Oracle Corporation
5000 Oracle Parkway
Redwood Shores, California
94065

Prepared by:
EWA-Canada
1223 Michael Street
Ottawa, Ontario, Canada
K1J7T2

CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 SECURITY TARGET INTRODUCTION

This Security Target (ST) defines the scope of the evaluation in terms of the assumptions made, the intended environment for the TOE, the Information Technology (IT) security functional and assurance requirements to be met, and the level of confidence (evaluation assurance level) to which it is asserted that the TOE satisfies its IT security requirements. This document forms the baseline for the Common Criteria (CC) evaluation.

1.1 DOCUMENT ORGANIZATION

Section 1, ST Introduction, provides the Security Target (ST) reference, the Target of Evaluation (TOE) reference, the TOE overview and the TOE description.

Section 2, Conformance Claims, describes how the ST conforms to the Common Criteria, Protection Profile, and Assurance Packages.

Section 3, Security Problem Definition, describes the expected environment in which the TOE is to be used. This section defines the set of threats that are relevant to the secure operation of the TOE, organizational security policies with which the TOE must comply, and secure usage assumptions applicable to this analysis.

Section 4, Security Objectives, defines the set of security objectives to be satisfied by the TOE and by the TOE operating environment in response to the problem defined by the security problem definition.

Section 5, Extended Components Definition, defines the extended components which are then detailed in Section 6.

Section 6, Security Requirements, specifies the security functional and assurance requirements that must be satisfied by the TOE and the Information Technology (IT) environment.

Section 7, TOE Summary Specification, describes the security functions and assurance measures that are included in the TOE to enable it to meet the IT security functional and assurance requirements.

Section 8 Terminology and Acronyms, defines the acronyms and terminology used in this ST.

1.2 SECURITY TARGET REFERENCE

ST Title:	Oracle Database 12c Release 2 Enterprise Edition (with Database Vault and Multitenant) Security Target
ST Version:	1.4
ST Date:	13 December 2018

1.3 TOE REFERENCE

TOE Identification: Oracle Database 12cR2 (12.2.0.1) Enterprise Edition with Critical Patch Update (CPU) October 2018

TOE Developer: Oracle Corporation

TOE Type: Database Management System

1.4 TOE OVERVIEW

Oracle Database 12cR2 is a relational database management system (RDBMS) from the Oracle Corporation. The system is built around a relational database framework in which data objects may be directly accessed by users, or an application front end, through structured query language (SQL). Oracle is a fully scalable relational database architecture typically used by global enterprises to manage and process data across wide and local area networks.

The security functionality in Oracle Database 12cR2 includes:

- Configurable audit capture.
- Fine-grained access controls on database objects. Discretionary Access Control (DAC) is based on object and system privileges, as well as roles. Fine-grained access control may be implemented to allow access based on the information itself. For example, a user may be granted access to their own human resources details, but not the details of the other users contained in the same tables.
- User identification and authentication. Users are identified and authenticated before access to database objects is allowed. On login, the user identity is associated with role and privilege information that is used to make access control decisions.
- Security management functionality. The security functionality associated with audit, access control, and user accounts are provided through the SQL command line interface (CLI).
- Consistent replication. The content of a database may be replicated to another server, with assurances that the consistency of the data is maintained.
- Multitenant. Oracle Multitenant features maintain physical and logical separation and isolation between databases hosted on the same server.
- Database Vault. Database Vault functionality provides schemas and roles supporting separation of duties, and enhanced audit functionality in support of multitenant environments.

The TOE is a software only TOE.

1.5 TOE DESCRIPTION

1.5.1 Physical Scope

The TOE consists of the Oracle Database 12cR2 software in one of the four configurations shown in Figure 1.

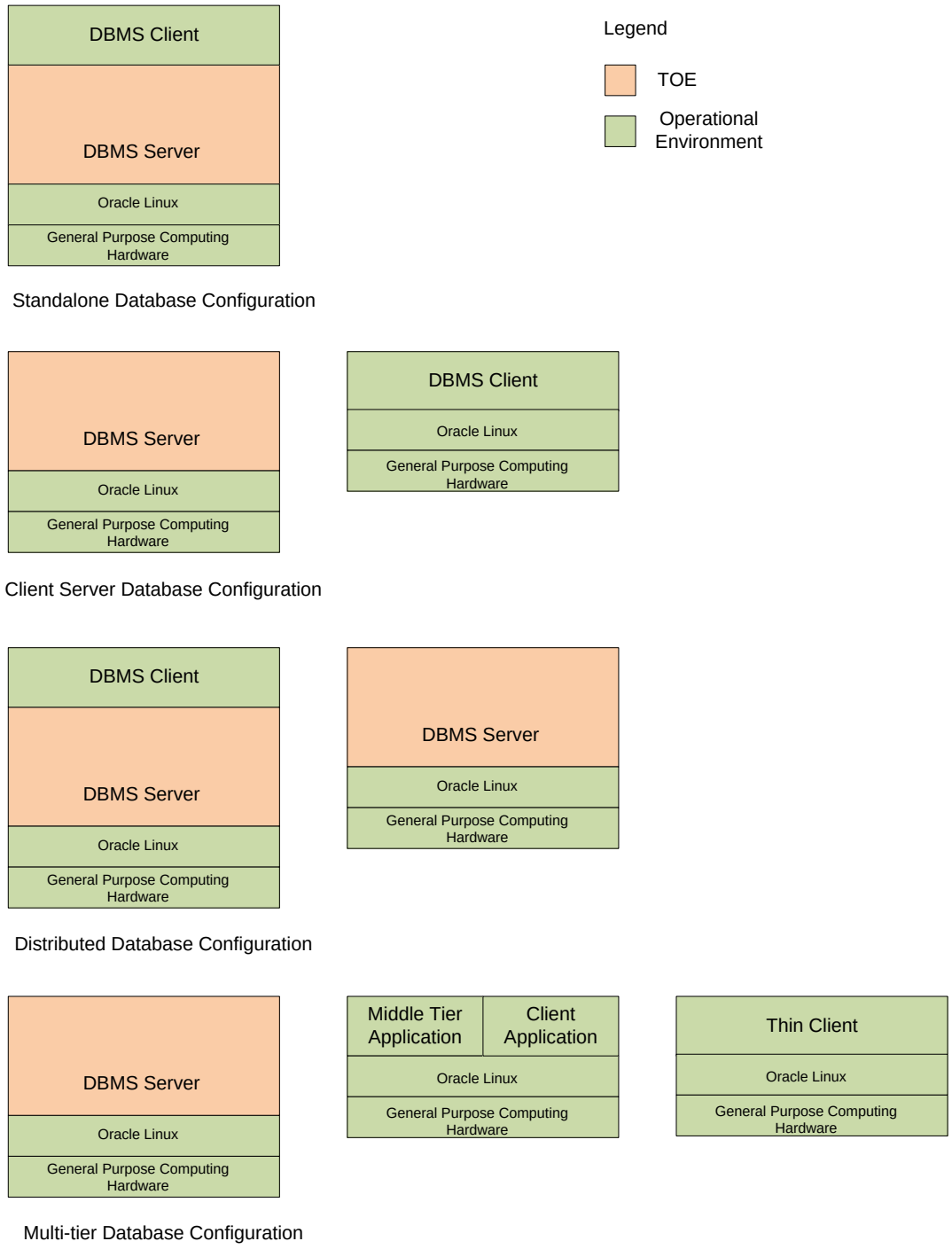

Figure 1 – Oracle Database 12cR2 Diagram

The configurations are:

a. the DBMS server operated with a co-located client;
b. the DBMS server operated with a remote client;
c. a primary DBMS server and a secondary DBMS server with replicated data; and
d. a DBMS server accessed by a thin client through a middle tier application proxy.

1.5.2 TOE Environment

The following operating system and hardware components are required for operation of the TOE in the evaluated configuration.

Component	Operating System	Hardware
Oracle Database 12cR2 (TOE component)	Oracle Linux 7	General Purpose Computing Hardware
Oracle Database 12cR2, second instance (TOE component)	Oracle Linux 7	General Purpose Computing Hardware
Database client (Non-TOE component)	Oracle Linux 7	General Purpose Computer Hardware

Table 1 – Operational Environment Operating System and Hardware Requirements

Note that the Database client refers to the presentation of the SQL commands at the TOE interface. These are the same whether they are entered on the database machine, from a client machine or from an application.

1.5.3 TOE Guidance

The TOE includes the following guidance documentation:

- Oracle® Database Installation Guide 12c Release 2 (12.2) for Linux E85758-02, January 2018
- Oracle® Database Administrator's Guide 12c Release 2 (12.2) E85760-06, March 2018
- Oracle® Database SQL Language Reference 12c Release 2 (12.2) E83703-01, April 2017
- Oracle® Database PL/SQL Language Reference 12c Release 2 (12.2) E85773-02, December 2017
- Oracle® Database Security Guide 12c Release 2 (12.2) E85682-02, December 2017
- Oracle® Data Guard Concepts and Administration 12c Release 2 (12.2) E85767-01, May 2017

- Oracle® Database Vault Administrator's Guide 12c Release 2 (12.2) E85657-02, March 2018
- Oracle Database 12c Release 2 Enterprise Edition (with Database Vault and Multitenant) Common Criteria Guidance Supplement, Version 1.3, 6 November 2018

1.5.4 Logical Scope

The logical boundary of the TOE includes all interfaces and functions within the physical boundary. The logical boundary of the TOE may be broken down by the security function classes described in Section 6. Table 2 summarizes the logical scope of the TOE.

Functional Classes	Description
Security Audit	Audit entries are generated for security related events. Audit policies may be created to generate logs based on details such as the user, the object being accessed, event type or success or failure of the operation.
User Data Protection	The TOE provides a discretionary access control policy to provide fine-grained access control between users and database objects. The TOE provides a Database Vault access control policy to enforce additional access controls to user data. In a multitenant environment, resources in pluggable databases are logically separate and inaccessible by local users in any other pluggable database or Container Database (CDB). Once data is allocated to a resource, the previous information content is no longer available.
Identification and Authentication	Users must identify and authenticate prior to gaining TOE access. Attributes are maintained to support the access control policy.

Functional Classes	Description
Security Management	The TOE provides management capabilities via SQL statements. Management functions allow the administrators to: • configure auditing and access control options (including granting and revoking privileges) • configure users (including the maximum number of concurrent sessions) and roles • configure replication options • configure Database Vault functions • configure separate domains for pluggable databases within a container database • assess roles and privileges in use at run-time Database Vault management capabilities are provided through designated PL/SQL procedures.
Protection of the TSF	Data may be consistently replicated to a secondary DBMS server.
TOE Access	The number of concurrent user sessions may be limited by policy. User login may be restricted based on user identity.

Table 2 – Logical Scope of the TOE

1.5.5 Functionality Excluded from the Evaluated Configuration

The following features are excluded from this evaluation:

- Authentication features
    - Although Oracle Database 12cR2 supports several authentication mechanisms, including Kerberos and Public Key Infrastructure, only Oracle password authentication was demonstrated for the purposes of this evaluation.
- Real Application Clusters (RAC)
- Oracle Label Security (OLS)
- External clients

2 CONFORMANCE CLAIMS

2.1 COMMON CRITERIA CONFORMANCE CLAIM

This Security Target claims to be conformant to Version 3.1 of Common Criteria for Information Technology Security Evaluation according to:

- Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model; CCMB-2017-04-001, Version 3.1, Revision 5, April 2017
- Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components; CCMB-2017-04-002, Version 3.1, Revision 5, April 2017
- Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements CCMB-2017-04-003, Version 3.1, Revision 5, April 2017

As follows:

- CC Part 2 extended
- CC Part 3 conformant

The Common Methodology for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017 (CEM) has to be taken into account.

2.2 ASSURANCE PACKAGE CLAIM

This Security Target claims conformance to Evaluation Assurance Level 2 augmented with ALC_FLR.2, Flaw Reporting Procedures.

2.3 PROTECTION PROFILE CONFORMANCE CLAIM

The TOE for this ST claims demonstrable conformance with the Base Protection Profile for Database Management Systems (DBMS PP) version 2.12, dated March 23, 2017 and with the DBMS PP Extended Package – Access History version 1.02, dated March 23, 2017.

This ST includes all of the mandatory Security Functional Requirements (SFRs) from the claimed Protection Profile (PP) and Extended Package (EP) and additional SFRs to address Database Vault and Multitenant functions in the TOE.

3 SECURITY PROBLEM DEFINITION

3.1 THREATS

Section 3 lists the threats addressed by the TOE. In accordance with the DBMS PP, a threat agent is defined as an entity that can adversely act on assets. Potential threat agents are authorized TOE users, unauthorized persons, and unauthorized processes. The level of expertise associated with these threat agents is assumed to be unsophisticated.

TOE users are assumed to have access to the TOE, extensive knowledge of TOE operations and to possess a level of skill commensurate with their responsibilities. They have moderate resources to alter TOE parameters, but are assumed not to be wilfully hostile.

Unauthorized persons have little knowledge of TOE operations, a low level of skill, limited resources to alter TOE parameters, and no physical access to the TOE. Unauthorized processes are assumed to be equivalent in sophistication to an attacker with a basic attack potential.

Mitigation to the threats is through the objectives identified in Section 4.1 Security Objectives.

Threat	Description
T.ACCESS_TSFDATA	A threat agent may read or modify TSF data using functions of the TOE without the proper authorization.
T.ACCESS_TSFFUNC	A threat agent may use or manage TSF, bypassing protection mechanisms of the TSF.
T.IA_MASQUERADE	A user or a process acting on behalf of a user may masquerade as an authorized entity in order to gain unauthorized access to user data, TSF data, or TOE resources.
T.IA_USER	A threat agent may gain access to user data, TSF data, or TOE resources with the exception of public objects without being identified and authenticated.
T.RESIDUAL_DATA	A user or a process acting on behalf of a user may gain unauthorized access to user or TSF data through reallocation of TOE resources from one user or process to another.
T.TSF_COMPROMISE	A user or a process acting on behalf of a user may cause configuration data to be inappropriately accessed (viewed, modified or deleted), or may compromise executable code within the TSF.

Threat	Description
T.UNAUTHORIZED_ACCESS	A threat agent may gain unauthorized access to user data for which they are not authorized according to the TOE security policy.

Table 3 – Threats

3.2 ORGANIZATIONAL SECURITY POLICIES

Organizational Security Policies (OSPs) are security rules, procedures, or guidelines imposed upon an organization in the operational environment. Table 4 lists the OSPs that are presumed to be imposed upon the TOE or its operational environment by an organization that implements the TOE in the Common Criteria evaluated configuration.

OSP	Description
P.ACCOUNTABILITY	The authorized users of the TOE shall be held accountable for their actions within the TOE.
P.ROLES	Administrative authority to TSF functionality shall be given to trusted personnel and be as restricted as possible supporting only the administrative duties the person has. This role shall be separate and distinct from other authorized users.
P.USER	Authority shall only be given to users who are trusted to perform the actions correctly.

Table 4 – Organizational Security Policies

3.3 ASSUMPTIONS

The assumptions required to ensure the security of the TOE are listed in Table 5.

Assumptions	Description
Physical aspects	
A.PHYSICAL	It is assumed that the IT environment provides the TOE with appropriate physical security, commensurate with the value of the IT assets protected by the TOE.

Assumptions	Description
Personnel aspects	
A.AUTHUSER	Authorized users possess the necessary authorization to access at least some of the information managed by the TOE.
A.MANAGE	The TOE security functionality is managed by one or more competent administrators. The system administrative personnel are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the guidance documentation.
A.TRAINEDUSER	Users are sufficiently trained and trusted to accomplish some task or group of tasks within a secure IT environment by exercising complete control over their user data.
Procedural aspects	
A.NO_GENERAL_PURPOSE	There are no general-purpose computing capabilities (e.g., compilers or user applications) available on DBMS servers, other than those services necessary for the operation, administration, and support of the DBMS.
A.PEER_FUNC_&_MGT	All remote trusted IT systems trusted by the TSF to provide TSF data or services to the TOE, or to support the TSF in the enforcement of security policy decisions are assumed to correctly implement the functionality used by the TSF consistent with the assumptions defined for this functionality and to be properly managed and operate under security policy constraints compatible with those of the TOE.
A.SUPPORT	Any information provided by a trusted entity in the IT environment and used to support the provision of time and date, information used in audit capture, user authentication, and authorization that is used by the TOE is correct and up to date.
Connectivity aspects	
A.CONNECT	All connections to and from remote trusted IT systems and between separate parts of the TSF are physically or logically protected within the TOE environment to ensure the integrity and confidentiality of the data transmitted and to ensure the authenticity of the communication end points.

Table 5 – Assumptions

4 SECURITY OBJECTIVES

The purpose of the security objectives is to address the security concerns and to show which security concerns are addressed by the TOE and which are addressed by the environment. Threats may be addressed by the TOE or the security environment or both. Therefore, the CC identifies two categories of security objectives:

- Security objectives for the TOE
- Security objectives for the environment

4.1 SECURITY OBJECTIVES FOR THE TOE

This section identifies and describes the security objectives that are to be addressed by the TOE.

Security Objective	Description
O.ACCESS_HISTORY	The TOE will store information related to previous attempts to establish a session and make that information available to the user.
O.ADMIN_ROLE	The TOE will provide a mechanism (e.g. a "role") by which the actions using administrative privileges may be restricted.
O.AUDIT _GENERATION	The TSF must be able to record defined security-relevant events (which usually include security-critical actions of users of the TOE). The information recorded for security-relevant events must contain the time and date the event happened and, if possible, the identification of the user that caused the event, and must be in sufficient detail to help the authorized user detect attempted security violations or potential misconfiguration of the TOE security features that would leave the IT assets open to compromise.
O.DISCRETIONARY _ACCESS	The TSF must control access of subjects and/or users to named resources based on identity of the object, subject, or user. The TSF must allow authorized users to specify for each access mode which users/subjects are allowed to access a specific named object in that access mode.
O.I&A	The TOE ensures that users are authenticated before the TOE processes any actions that require authentication.
O.MANAGE	The TSF must provide all the functions and facilities necessary to support the authorized users that are responsible for the management of TOE security mechanisms, must allow restricting such management actions to dedicated users, and must ensure that only such authorized users are able to access management functionality.
O.MEDIATE	The TOE must protect user data in accordance with its security policy, and must mediate all requests to access such

Security Objective	Description
	data.
O.RESIDUAL_INFORMATION	The TOE will ensure that any information contained in a protected resource within its Scope of Control is not inappropriately disclosed when the resource is reallocated.
O.TOE_ACCESS	The TOE will provide functionality that controls a user's logical access[1] to user data and to the TSF.

Table 6 – Security Objectives for the TOE

4.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

This section identifies and describes the security objectives that are to be addressed by non-technical or procedural means, and by the IT domain.

4.2.1 Operational Environment Security Objectives

The following table describes the operational environment security objectives.

Security Objective	Description
OE.ADMIN	Those responsible for the TOE are competent and trustworthy individuals, capable of managing the TOE and the security of the information it contains.
OE.INFO_PROTECT	Those responsible for the TOE must establish and implement procedures to ensure that information is protected in an appropriate manner. In particular: • All network and peripheral cabling must be approved for the transmittal of the most sensitive data transmitted over the link. Such physical links are assumed to be adequately protected against threats to the confidentiality and integrity of the data transmitted using appropriate physical and logical protection techniques. • DAC protections on security-relevant files (such as audit trails and authorization databases) shall always be set up correctly. • Users are authorized to access parts of the data managed by the TOE and are trained to exercise control over their own data.

[1] As noted in the DBMS PP, "logical access" is specified, since the control of "physical access" is outside the scope of the evaluation.

Security Objective	Description
OE.NO_GENERAL_PURPOSE	There will be no general-purpose computing capabilities (e.g., compilers or user applications) available on DBMS servers, other than those services necessary for the operation, administration, and support of the DBMS.
OE.PHYSICAL	Those responsible for the TOE must ensure that those parts of the TOE critical to enforcement of the security policy are protected from physical attack that might compromise IT security objectives. The protection must be commensurate with the value of the IT assets protected by the TOE.

Table 7 – Operational Environment Security Objectives

4.2.2 Operational Environment IT Domain Security Objectives

The following table describes the operational environment IT security objectives.

Security Objective	Description
OE.IT_I&A	Any information provided by a trusted entity in the environment and used to support user authentication and authorization used by the TOE is correct and up to date.
OE.IT_REMOTE	If the TOE relies on remote trusted IT systems to support the enforcement of its policy, those systems provide that the functions and any data used by the TOE in making policy decisions required by the TOE are sufficiently protected from any attack that may cause those functions to provide false results.
OE.IT_TRUSTED_SYSTEM	The remote trusted IT systems implement the protocols and mechanisms required by the TSF to support the enforcement of the security policy. These remote trusted IT systems are managed according to known, accepted, and trusted policies based on the same rules and policies applicable to the TOE, and are physically and logically protected equivalent to the TOE.

Table 8 – Operational Environment IT Security Objectives

4.3 SECURITY OBJECTIVES RATIONALE

The following table maps the security objectives to the assumptions, threats, and organisational policies identified for the TOE.

	T.ACCESS_TSFDATA	T.ACCESS_TSFFUNC	T.IA_MASQUERADE	T.IA_USER	T.RESIDUAL_DATA	T.TSF_COMPROMISE	T.UNAUTHORIZED_ACCESS	P.ACCOUNTABILITY	P.ROLES	P.USER	A.AUTHUSER	A.CONNECT	A.MANAGE	A.NO_GENERAL_PURPOSE	A.PEER_FUNC_&_MGT	A.PHYSICAL	A.SUPPORT	A.TRAINEDUSER
O.ACCESS_HISTORY	X		X			X												
O.ADMIN_ROLE		X						X	X									
O.AUDIT _GENERATION						X		X										
O.DISCRETIONARY _ACCESS				X			X											
O.I&A	X	X	X	X				X										
O.MANAGE	X	X					X			X								
O.MEDIATE			X	X			X											
O.RESIDUAL _INFORMATION	X	X			X													
O.TOE_ACCESS	X	X	X	X		X		X	X	X								
OE.ADMIN								X	X	X			X					
OE.INFO_PROTECT						X	X	X		X	X	X	X			X		X
OE.NO_GENERAL _PURPOSE			X			X								X				
OE.PHYSICAL						X						X				X		
OE.IT_I&A																	X	
OE.IT_REMOTE						X					X	X			X			
OE.IT_TRUSTED _SYSTEM						X					X	X			X			

Table 9 – Mapping Between Objectives, Threats, OSPs, and Assumptions

4.3.1 Security Objectives Rationale Related to Threats

The security objectives rationale related to threats traces the security objectives for the TOE and the Operational Environment back to the threats addressed by the TOE. The rationale tracing the threats to the security objectives for the TOE and to the Operational Environment have been separated to provide consistency with the claimed PP.

4.3.1.1 Threats Mapped to Security Objectives for the TOE

Threat: **T.ACCESS_TSFDATA**	A threat agent may read or modify TSF data using functions of the TOE without the proper authorization.	
Objectives:	O.ACCESS_HISTORY	The TOE will store information related to previous attempts to establish a session and make that information available to the user.
	O.I&A	The TOE ensures that users are authenticated before the TOE processes any actions that require authentication.
	O.MANAGE	The TSF must provide all the functions and facilities necessary to support the authorized users that are responsible for the management of TOE security mechanisms, must allow restricting such management actions to dedicated users, and must ensure that only such authorized users are able to access management functionality.
	O.RESIDUAL_INFORMATION	The TOE will ensure that any information contained in a protected resource within its Scope of Control is not inappropriately disclosed when the resource is reallocated.
	O.TOE_ACCESS	The TOE will provide mechanisms that control a user's logical access to user data and to the TSF.
Rationale:	O.ACCESS_HISTORY diminishes this threat because it ensures the TOE will store the information that is needed to advise the user of previous authentication attempts and allows this information to be retrieved. O.I&A supports this policy by requiring that each entity interacting with the TOE is properly identified and authenticated before allowing any action the TOE is defined to provide to authenticated users only. O.MANAGE diminishes this threat since it ensures that functions and facilities used to modify TSF data are not available to unauthorized users.	

	O.RESIDUAL_INFORMATION diminishes this threat since information contained in protected resources will not be easily available to the threat agent through reallocation attacks. O.TOE_ACCESS diminishes this threat since it makes it more unlikely that a threat agent has access to the TOE.

Threat: **T.ACCESS _TSFFUNC**	A threat agent may use or manage TSF, bypassing protection mechanisms of the TSF.	
Objectives:	O.ADMIN_ROLE	The TOE will provide a mechanism (e.g. a "role") by which the actions using administrative privileges may be restricted.
	O.I&A	The TOE ensures that users are authenticated before the TOE processes any actions that require authentication.
	O.MANAGE	The TSF must provide all the functions and facilities necessary to support the authorized users that are responsible for the management of TOE security mechanisms, must allow restricting such management actions to dedicated users, and must ensure that only such authorized users are able to access management functionality.
	O.RESIDUAL _INFORMATION	The TOE will ensure that any information contained in a protected resource within its Scope of Control is not inappropriately disclosed when the resource is reallocated.
	O.TOE_ACCESS	The TOE will provide mechanisms that control a user's logical access to user data and to the TSF.
Rationale:	O.ADMIN_ROLE diminishes this threat by providing isolation of privileged actions. O.I&A diminishes this threat since the TOE requires successful authentication to the TOE prior to gaining access to any controlled-access content. By implementing strong authentication to gain access to these services, an attacker's opportunity to masquerade as another entity in order to gain unauthorized access to data or TOE resources is reduced. O.MANAGE diminishes this threat because an access control policy is specified to control access to TSF data. This objective is used to dictate who is able to view and modify TSF data, as well as the behavior of TSF functions. O.RESIDUAL_INFORMATION diminishes this threat by ensuring that TSF data and user data is not persistent when resources are	

	released by one user/process and allocated to another user/process. O.TOE_ACCESS diminishes this threat since it makes it more unlikely that a threat agent has access to the TOE.

Threat: **T.IA _MASQUERADE**	A user or a process acting on behalf of a user may masquerade as an authorized entity in order to gain unauthorized access to user data, TSF data, or TOE resources.	
Objectives:	O.ACCESS _HISTORY	The TOE will store information related to previous attempts to establish a session and make that information available to the user.
	O.I&A	The TOE ensures that users are authenticated before the TOE processes any actions that require authentication.
	O.MEDIATE	The TOE must protect user data in accordance with its security policy, and must mediate all requests to access such data.
	O.TOE_ACCESS	The TOE will provide mechanisms that control a user's logical access to user data and to the TSF.
Rationale:	O.ACCESS_HISTORY diminishes this threat because it ensures the TOE will be able to store and retrieve the information that will advise the user of the last successful login attempt and performed actions without their knowledge. O.I&A diminishes this threat by requiring that each entity interacting with the TOE is properly identified and authenticated before allowing any action the TOE has defined to provide to authenticated users only. O.MEDIATE diminishes this threat by ensuring that all access to user data are subject to mediation, unless said data has been specifically identified as public data. The TOE requires successful authentication to the TOE prior to gaining access to any controlled-access content. By implementing strong authentication to gain access to these services, an attacker's opportunity to masquerade as another entity in order to gain unauthorized access to data or TOE resources is reduced. O.TOE_ACCESS diminishes this threat by controlling the logical access to the TOE and its resources. By constraining how and when authorized users can access the TOE, and by mandating the type and strength of the authentication mechanism this objective helps mitigate the possibility of a user attempting to login and masquerade as an authorized user. In addition, this objective provides the administrator the means to control the number of failed login attempts a user can generate before an account is	

	locked out, further reducing the possibility of a user gaining unauthorized access to the TOE.

Threat: **T.IA_USER**	A threat agent may gain access to user data, TSF data, or TOE resources with the exception of public objects without being identified and authenticated.	
Objectives:	O.DISCRETIONARY_ACCESS	The TSF must control access of subjects and/or users to named resources based on identity of the object, subject, or user. The TSF must allow authorized users to specify for each access mode which users/subjects are allowed to access a specific named object in that access mode.
	O.I&A	The TOE ensures that users are authenticated before the TOE processes any actions that require authentication.
	O.MEDIATE	The TOE must protect user data in accordance with its security policy, and must mediate all requests to access such data.
	O.TOE_ACCESS	The TOE will provide mechanisms that control a user's logical access to user data and to the TSF.
Rationale:	O.DISCRETIONARY_ACCESS diminishes this threat by requiring that data including user data stored with the TOE, have discretionary access control protection. O.I&A diminishes this threat by requiring that each entity interacting with the TOE is properly identified and authenticated before allowing any action the TOE is defined to provide to authenticated users only. O.MEDIATE diminishes this threat by ensuring that all access to user data are subject to mediation, unless said data has been specifically identified as public data. The TOE requires successful authentication to the TOE prior to gaining access to any controlled-access content. By implementing strong authentication to gain access to these services, an attacker's opportunity to masquerade as another entity in order to gain unauthorized access to data or TOE resources is reduced. O.TOE_ACCESS diminishes this threat by controlling logical access to user data, TSF data or TOE resources.	

Threat: **T.RESIDUAL_DATA**	A user or a process acting on behalf of a user may gain unauthorized access to user or TSF data through reallocation of TOE resources from one user or process to another.

Objectives:	O.RESIDUAL _INFORMATION	The TOE will ensure that any information contained in a protected resource within its Scope of Control is not inappropriately disclosed when the resource is reallocated.
Rationale:	O.RESIDUAL_INFORMATION diminishes this threat because even if the security mechanisms do not allow a user to view TSF data, if TSF data were to reside inappropriately in a resource that was made available to a user, that user would be able to view the TSF data without authorization.	

Threat: **T.TSF _COMPROMISE**	A user or a process acting on behalf of a user may cause configuration data to be inappropriately accessed (viewed, modified or deleted), or may compromise executable code within the TSF.	
Objectives:	O.ACCESS _HISTORY	The TOE will store information related to previous attempts to establish a session and make that information available to the user.
	O.AUDIT _GENERATION	The TOE will provide the capability to detect and create records of security relevant events associated with users.
	O.TOE_ACCESS	The TOE will provide mechanisms that control a user's logical access to user data and to the TSF.
Rationale:	O.ACCESS_HISTORY diminishes this threat because it ensures the TOE will be able to store and retrieve the information that will advise the user of the last successful login attempt and performed actions without their knowledge. O.AUDIT_GENERATION diminishes this threat by providing the authorized administrator with the appropriate audit records supporting the detection of compromise of the TSF. O.TOE_ACCESS diminishes this threat since controlled user's logical access to the TOE will reduce the opportunities for an attacker's access to configuration data.	

Threat: **T.UNAUTHOR-IZED_ACCESS**	A threat agent may gain unauthorized access to user data for which they are not authorized according to the TOE security policy.	
Objectives:	O.DISCRETIONARY _ACCESS	The TSF must control access of subjects and/or users to named resources based on identity of the object, subject or user. The TSF must allow authorized users to specify for each access mode which users/subjects are allowed to access a specific named

		object in that access mode.
	O.MANAGE	The TSF must provide all the functions and facilities necessary to support the authorized users that are responsible for the management of TOE security mechanisms, must allow restricting such management actions to dedicated users, and must ensure that only such authorized users are able to access management functionality.
	O.MEDIATE	The TOE must protect user data in accordance with its security policy, and must mediate all requests to access such data.
Rationale:	O.DISCRETIONARY_ACCESS diminishes this threat by requiring that data including TSF data stored with the TOE, have discretionary access control protection. O.MANAGE diminishes this threat by ensuring that the functions and facilities supporting that authorized users can be held accountable for their actions by authorized administrators are in place. O.MEDIATE diminishes this threat because it ensures that all access to user data are subject to mediation, unless said data has been specifically identified as public data. The TOE requires successful authentication to the TOE prior to gaining access to any controlled-access content. By implementing strong authentication to gain access to these services, an attacker's opportunity to conduct a man-in-the-middle and/or password guessing attack successfully is greatly reduced. Lastly, the TSF will ensure that all configured enforcement functions (authentication, access control rules, etc.) must be invoked prior to allowing a user to gain access to TOE or TOE mediated services. The TOE restricts the ability to modify the security attributes associated with access control rules, access to authenticated and unauthenticated services, etc. to the administrator. This feature ensures that no other user can modify the information flow policy to bypass the intended TOE security policy.	

4.3.1.2 Threats Mapped to Security Objectives for the Operational Environment

Threat: **T.IA_MASQUERADE**	A user or process may masquerade as an authorized entity in order to gain unauthorized access to user data, TSF data, or TOE resources.	
Objectives:	OE.NO_GENERAL_PURPOSE	There will be no general-purpose computing capabilities (e.g., compilers or user

		applications) available on DMBS servers, other than those services necessary for the operation, administration, and support of the DBMS.
Rationale:	OE.NO_GENERAL_PURPOSE The DBMS server must not include any general-purpose computing or storage capabilities. This diminishes the threat of masquerade since only users with DBMS or related functions will be defined in the TOE environment.	

Threat: **T.TSF _COMPROMISE**	A user or process acting on behalf of a user may cause configuration data to be inappropriately accessed (viewed, modified or deleted), or may compromise executable code within the TSF.	
Objectives:	OE.INFO _PROTECT	Those responsible for the TOE must establish and implement procedures to ensure that information is protected in an appropriate manner. In particular: • All network and peripheral cabling must be approved for the transmittal of the most sensitive data transmitted over the link. Such physical links are assumed to be adequately protected against threats to the confidentiality and integrity of the data transmitted using appropriate physical and logical protection techniques. • DAC protections on security-relevant files (such as audit trails and authorization databases) shall always be set up correctly. • Users are authorized to access parts of the data managed by the TOE and are trained to exercise control over their own data.
	OE.IT_REMOTE	If the TOE relies on remote trusted IT systems to support the enforcement of its policy, those systems provide that the functions and any data used by the TOE in making policy decisions, required by the TOE are sufficiently protected from any attack that may cause those functions to provide false results.
	OE.IT_TRUSTED _SYSTEM	The remote trusted IT systems implement the protocols and mechanisms required by the TSF to support the enforcement of the

		security policy. These remote trusted IT systems are managed according to known, accepted, and trusted policies based on the same rules and policies applicable to the TOE, and are physically and logically protected equivalent to the TOE.
	OE.NO_GENERAL_PURPOSE	There will be no general-purpose computing capabilities (e.g., compilers or user applications) available on DMBS servers, other than those services necessary for the operation, administration, and support of the DBMS.
	OE.PHYSICAL	Those responsible for the TOE must ensure that those parts of the TOE critical to enforcement of the security policy are protected from physical attack that might compromise IT security objectives. The protection must be commensurate with the value of the IT assets protected by the TOE.
Rationale:	OE.INFO_PROTECT diminishes the threat by ensuring that all network and peripheral cabling must be approved for the transmittal of the most sensitive data transmitted over the link. Such physical links are assumed to be adequately protected against threats to the confidentiality and integrity of the data transmitted using appropriate physical and logical protection techniques. OE.IT_REMOTE diminishes the threat by ensuring that remote trusted IT systems are sufficiently protected. OE.IT_TRUSTED_SYSTEM diminishes the threat by ensuring that remote trusted IT systems are managed according to known, accepted and trusted policies based on the same rules and policies applicable to the TOE, and are physically and logically protected equivalent to the TOE. OE.NO_GENERAL_PURPOSE diminishes this threat by reducing the opportunities to subvert non TOE related capabilities in the TOE environment. OE.PHYSICAL diminishes the threat of a TSF compromise due to exploitation of physical weaknesses or vulnerabilities as a vector in an attack.	

Threat: **T.UNAUTHOR-IZED_ACCESS**	A threat agent may gain unauthorized access to user data for which they are not authorized according to the TOE security policy.	
Objectives:	OE.INFO	Those responsible for the TOE must establish and implement procedures to

	_PROTECT	ensure that information is protected in an appropriate manner. In particular: • All network and peripheral cabling must be approved for the transmittal of the most sensitive data transmitted over the link. Such physical links are assumed to be adequately protected against threats to the confidentiality and integrity of the data transmitted using appropriate physical and logical protection techniques. • DAC protections on security-relevant files (such as audit trails and authorization databases) shall always be set up correctly. • Users are authorized to access parts of the data managed by the TOE and are trained to exercise control over their own data.
Rationale:	OE.INFO_PROTECT diminishes the threat by ensuring that the logical and physical threats to network and peripheral cabling are appropriately protected. DAC protections if implemented correctly may support the identification of unauthorized accesses.	

4.3.2 Security Objectives Rationale Related to OSPs

The security objectives rationale related to OSPs traces the security objectives for the TOE and the Operational Environment back to the OSPs applicable to the TOE. The rationale tracing the OSPs to the security objectives for the TOE and to the Operational Environment have been separated to provide consistency with the claimed PP.

4.3.2.1 OSPs Mapped to Security Objectives for the TOE

Policy: **P.ACCOUNT-ABILITY**	The authorized users of the TOE shall be held accountable for their actions within the TOE.	
Objectives:	O.ADMIN_ROLE	The TOE will provide a mechanism (e.g. a "role") by which the actions using administrative privileges may be restricted.
	O.AUDIT _GENERATION	The TOE will provide the capability to detect and create records of security relevant events associated with users.
	O.I&A	The TOE ensures that users are authenticated before the TOE processes any actions that

		require authentication.
	O.TOE_ACCESS	The TOE will provide mechanisms that control a user's logical access to user data and to the TSF.
Rationale:	O.ADMIN_ROLE supports this policy by ensuring that the TOE has an objective to provide authorized administrators with the privileges needed for secure administration. O.AUDIT_GENERATION supports this policy by ensuring that audit records are generated. Having these records available enables accountability. O.I&A supports this policy by requiring that each entity interacting with the TOE is properly identified and authenticated before allowing any action the TOE is defined to provide to authenticated users only. O.TOE_ACCESS supports this policy by providing a mechanism for controlling access to authorized users.	

Policy: **P.ROLES**	Administrative authority to TSF functionality shall be given to trusted personnel and be as restricted as possible supporting only the administrative duties the person has. This role shall be separate and distinct from other authorized users.	
Objectives:	O.ADMIN_ROLE	The TOE will provide a mechanism (e.g. a "role") by which the actions using administrative privileges may be restricted.
	O.TOE_ACCESS	The TOE will provide mechanisms that control a user's logical access to user data and to the TSF.
Rationale:	O.ADMIN_ROLE The TOE has the objective of providing an authorized administrator role for secure administration. The TOE may provide other roles as well, but only the role of authorized administrator is required. O.TOE_ACCESS supports this policy by ensuring that an authorized administrator role can be distinguished from other authorized users.	

Policy: **P.USER**	Authority shall only be given to users who are trusted to perform the actions correctly.	
Objectives:	O.MANAGE	The TSF must provide all the functions and facilities necessary to support the authorized users that are responsible for the management of TOE security mechanisms,

		must allow restricting such management actions to dedicated users, and must ensure that only such authorized users are able to access management functionality.
	O.TOE_ACCESS	The TOE will provide mechanisms that control a user's logical access to user data and to the TSF.
	OE.ADMIN	Those responsible for the TOE are competent and trustworthy individuals, capable of managing the TOE and the security of information it contains.
Rationale:	O.MANAGE supports this policy by ensuring that the functions and facilities supporting the authorized administrator role are in place. O.TOE_ACCESS supports this policy by providing a mechanism for controlling access to authorized users. OE.ADMIN supports this policy by ensuring that the authorized administrator role is understood and used by competent administrators.	

4.3.2.2 OSPs Mapped to Security Objectives for the Operational Environment

Policy: **P.ACCOUNT-ABILITY**	The authorized users of the TOE shall be held accountable for their actions within the TOE.	
Objectives:	OE.ADMIN	Those responsible for the TOE are competent and trustworthy individuals, capable of managing the TOE and the security of information it contains.
	OE.INFO_PROTECT	Those responsible for the TOE must establish and implement procedures to ensure that information is protected in an appropriate manner. In particular: • All network and peripheral cabling must be approved for the transmittal of the most sensitive data transmitted over the link. Such physical links are assumed to be adequately protected against threats to the confidentiality and integrity of the data transmitted using appropriate physical and logical protection techniques. • DAC protections on security-relevant files (such as audit trails and authorization databases) shall always

		be set up correctly. Users are authorized to access parts of the data managed by the TOE and are trained to exercise control over their own data.
Rationale:	OE.ADMIN supports the policy that the authorized administrators are assumed competent in order to help ensure that all the tasks and responsibilities are performed effectively. OE.INFO_PROTECT supports the policy by ensuring that the authorized users are trained and have procedures available to support them and that the DAC protections function and are able to provide sufficient information to inform those pursuing accountability.	

Policy: **P.ROLES**	Administrative authority to TSF functionality shall be given to trusted personnel and be as restricted as possible supporting only the administrative duties the person has. This role shall be separate and distinct from other authorized users.	
Objectives:	OE.ADMIN	Those responsible for the TOE are competent and trustworthy individuals, capable of managing the TOE and the security of information it contains.
Rationale:	OE.ADMIN supports the policy by ensuring that an authorized administrator role for secure administration of the TOE is established.	

Policy: **P.USER**	Authority shall only be given to users who are trusted to perform the actions correctly.	
Objectives:	OE.ADMIN	Those responsible for the TOE are competent and trustworthy individuals, capable of managing the TOE and the security of information it contains.
	OE.INFO _PROTECT	Those responsible for the TOE must establish and implement procedures to ensure that information is protected in an appropriate manner. In particular: • All network and peripheral cabling must be approved for the transmittal of the most sensitive data transmitted over the link. Such physical links are assumed to be adequately protected against threats to the confidentiality and integrity of the data transmitted using appropriate physical and logical

		protection techniques. • DAC protections on security-relevant files (such as audit trails and authorization databases) shall always be set up correctly. • Users are authorized to access parts of the data managed by the TOE and are trained to exercise control over their own data.
Rationale:	OE.ADMIN supports the policy by ensuring that the authorized administrators, responsible for giving appropriate authorities to users, are trustworthy. OE.INFO_PROTECT supports the policy by ensuring that users are authorized to access parts of the data managed by the TOE and are trained to exercise control over their own data and that DAC protections on security-relevant files (such as audit trails and authorization databases) shall always be set up correctly.	

4.3.3 Security Objectives Rationale Related to Assumptions

The security objectives rationale related to assumptions traces the security objectives for the operational environment back to the assumptions for the TOE's operational environment.

Assumption: **A.AUTHUSER**	Authorized users possess the necessary authorization to access at least some of the information managed by the TOE.	
Objectives:	OE.INFO_PROTECT	Those responsible for the TOE must establish and implement procedures to ensure that information is protected in an appropriate manner. In particular: • All network and peripheral cabling must be approved for the transmittal of the most sensitive data transmitted over the link. Such physical links are assumed to be adequately protected against threats to the confidentiality and integrity of the data transmitted using appropriate physical and logical protection techniques. • DAC protections on security-relevant files (such as audit trails and authorization databases) shall always be set up correctly. • Users are authorized to access parts of the data managed by the TOE and are trained to exercise control over their own data.

	OE.IT_REMOTE	If the TOE relies on remote trusted IT systems to support the enforcement of its policy, those systems provide that the functions and any data used by the TOE in making policy decisions, required by the TOE are sufficiently protected from any attack that may cause those functions to provide false results.
	OE.IT_TRUSTED_SYSTEM	The remote trusted IT systems implement the protocols and mechanisms required by the TSF to support the enforcement of the security policy. These remote trusted IT systems are managed according to known, accepted, and trusted policies based on the same rules and policies applicable to the TOE, and are physically and logically protected equivalent to the TOE.
Rationale:	OE.INFO_PROTECT supports the assumption by ensuring that users are authorized to access parts of the data managed by the TOE and is trained to exercise control over their own data. Having trained, authorized users, who are provided with relevant procedures for information protection supports the assumption of co-operation. OE.IT_REMOTE supports this assumption by ensuring that remote systems that form part of the IT environment are protected. This gives confidence that the environment is benign. OE.IT_TRUSTED_SYSTEM supports this assumption by providing confidence that systems in the TOE IT environment contribute to a benign environment.	

Assumption: **A.CONNECT**	All connections to and from remote trusted IT systems and between separate parts of the TSF are physically or logically protected within the TOE environment to ensure the integrity and confidentiality of the data transmitted and to ensure the authenticity of the communication end points.	
Objectives:	OE.IT_REMOTE	If the TOE relies on remote trusted IT systems to support the enforcement of its policy, those systems provide that the functions and any data used by the TOE in making policy decisions, required by the TOE are sufficiently protected from any attack that may cause those functions to provide false results.
	OE.INFO_PROTECT	Those responsible for the TOE must establish and implement procedures to ensure that information is protected in an appropriate manner. In particular:

		• All network and peripheral cabling must be approved for the transmittal of the most sensitive data transmitted over the link. Such physical links are assumed to be adequately protected against threats to the confidentiality and integrity of the data transmitted using appropriate physical and logical protection techniques. • DAC protections on security-relevant files (such as audit trails and authorization databases) shall always be set up correctly. • Users are authorized to access parts of the data managed by the TOE and are trained to exercise control over their own data.
	OE.IT_TRUSTED_SYSTEM	The remote trusted IT systems implement the protocols and mechanisms required by the TSF to support the enforcement of the security policy. These remote trusted IT systems are managed according to known, accepted, and trusted policies based on the same rules and policies applicable to the TOE, and are physically and logically protected equivalent to the TOE.
	OE.PHYSICAL	Those responsible for the TOE must ensure that those parts of the TOE critical to enforcement of the security policy are protected from physical attack that might compromise IT security objectives. The protection must be commensurate with the value of the IT assets protected by the TOE.
Rationale:	OE.IT_REMOTE supports the assumption by levying a requirement in the environment that connections between trusted systems or physically separated parts of the TOE are sufficiently protected from any attack that may cause those functions to provide false results. OE.INFO_PROTECT supports the assumption by requiring that All network and peripheral cabling must be approved for the transmittal of the most sensitive data transmitted over the link. Such physical links are assumed to be adequately protected against threats to the confidentiality and integrity of the data transmitted using appropriate physical and logical protection techniques. OE.IT_TRUSTED_SYSTEM supports the assumption by ensuring that remote trusted IT systems implement the protocols and mechanisms required by the TSF to support the enforcement of the security policy.	

	OE.PHYSICAL supports the assumption by ensuring that appropriate physical security is provided within the domain.

Assumption: **A.MANAGE**	The TOE security functionality is managed by one or more competent administrators. The system administrative personnel are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the guidance documentation.	
Objectives:	OE.ADMIN	Those responsible for the TOE are competent and trustworthy individuals, capable of managing the TOE and the security of information it contains.
	OE.INFO_PROTECT	Those responsible for the TOE must establish and implement procedures to ensure that information is protected in an appropriate manner. In particular: • All network and peripheral cabling must be approved for the transmittal of the most sensitive data transmitted over the link. Such physical links are assumed to be adequately protected against threats to the confidentiality and integrity of the data transmitted using appropriate physical and logical protection techniques. • DAC protections on security-relevant files (such as audit trails and authorization databases) shall always be set up correctly. • Users are authorized to access parts of the data managed by the TOE and are trained to exercise control over their own data.
Rationale:	OE.ADMIN supports the assumption since the authorized administrators are assumed competent in order to help ensure that all the tasks and responsibilities are performed effectively. OE.INFO_PROTECT supports the assumption by ensuring that the information protection aspects of the TOE and the system(s) and relevant connectivity that form the platform for the TOE is vital to addressing the security problem, described in this ST and the PP. Managing these effectively using defined procedures is reliant on having competent administrators.	

Assumption: **A.NO_GENERAL**	There are no general-purpose computing capabilities (e.g., compilers or user applications) available on DBMS servers, other than those services necessary for the operation, administration,

_PURPOSE	and support of the DBMS.	
Objectives:	OE.NO_GENERAL_PURPOSE	There will be no general-purpose computing capabilities (e.g., compilers or user applications) available on DMBS servers, other than those services necessary for the operation, administration, and support of the DBMS.
Rationale:	OE.NO_GENERAL_PURPOSE The DBMS server must not include any general-purpose computing or storage capabilities. This will protect the TSF data from malicious processes. The environmental objective is tightly related to the assumption, which when fulfilled will address the assumption.	

Assumption: **A.PEER_FUNC_&_MGT**	All remote trusted IT systems trusted by the TSF to provide TSF data or services to the TOE, or to support the TSF in the enforcement of security policy decisions are assumed to correctly implement the functionality used by the TSF consistent with the assumptions defined for this functionality and to be properly managed and operate under security policy constraints compatible with those of the TOE.	
Objectives:	OE.IT_REMOTE	If the TOE relies on remote trusted IT systems to support the enforcement of its policy, those systems provide that the functions and any data used by the TOE in making policy decisions, required by the TOE are sufficiently protected from any attack that may cause those functions to provide false results.
	OE.IT_TRUSTED_SYSTEM	The remote trusted IT systems implement the protocols and mechanisms required by the TSF to support the enforcement of the security policy. These remote trusted IT systems are managed according to known, accepted, and trusted policies based on the same rules and policies applicable to the TOE, and are physically and logically protected equivalent to the TOE.
Rationale:	OE.IT_REMOTE The assumption that connections between trusted systems or physically separated parts of the TOE is addressed by the objective specifying that such systems are sufficiently protected from any attack that may cause those functions to provide false results. OE.IT_TRUSTED_SYSTEM The assumption on all remote trusted IT systems to implement correctly the functionality used by the TSF consistent with the	

	assumptions defined for this functionality is supported by physical and logical protections and the application of trusted policies commensurate with those applied to the TOE.

Assumption: **A.PHYSICAL**	It is assumed that the IT environment provides the TOE with appropriate physical security, commensurate with the value of the IT assets protected by the TOE.	
Objectives:	OE.PHYSICAL	Those responsible for the TOE must ensure that those parts of the TOE critical to enforcement of the security policy are protected from physical attack that might compromise IT security objectives. The protection must be commensurate with the value of the IT assets protected by the TOE.
	OE.INFO _PROTECT	Those responsible for the TOE must establish and implement procedures to ensure that information is protected in an appropriate manner. In particular: • All network and peripheral cabling must be approved for the transmittal of the most sensitive data transmitted over the link. Such physical links are assumed to be adequately protected against threats to the confidentiality and integrity of the data transmitted using appropriate physical and logical protection techniques. • DAC protections on security-relevant files (such as audit trails and authorization databases) shall always be set up correctly. • Users are authorized to access parts of the data managed by the TOE and are trained to exercise control over their own data.
Rationale:	OE.PHYSICAL The TOE, the TSF data, and protected user data is assumed to be protected from physical attack (e.g., theft, modification, destruction, or eavesdropping). Physical attack could include unauthorized intruders into the TOE environment, but it does not include physical destructive actions that might be taken by an individual that is authorized to access the TOE environment. OE.INFO_PROTECT supports the assumption by requiring that all network and peripheral cabling must be approved for the transmittal of the most sensitive data transmitted over the link. Such physical links are assumed to be adequately protected against threats to the confidentiality and integrity of the data transmitted	

	using appropriate physical and logical protection techniques.

Assumption: **A.SUPPORT**	Any information provided by a trusted entity in the IT environment and used to support the provision of time and date, information used in audit capture, user authentication, and authorization that is used by the TOE is correct and up to date.	
Objectives:	OE.IT_I&A	Any information provided by a trusted entity in the environment and used to support user authentication and authorization used by the TOE is correct and up to date.
Rationale:	OE.IT_I&A supports the assumption implicitly.	

Assumption: **A.TRAINED-USER**	Users are sufficiently trained and trusted to accomplish some task or group of tasks within a secure IT environment by exercising complete control over their user data.	
Objectives:	OE.INFO_PROTECT	Those responsible for the TOE must establish and implement procedures to ensure that information is protected in an appropriate manner. In particular: • All network and peripheral cabling must be approved for the transmittal of the most sensitive data transmitted over the link. Such physical links are assumed to be adequately protected against threats to the confidentiality and integrity of the data transmitted using appropriate physical and logical protection techniques. • DAC protections on security-relevant files (such as audit trails and authorization databases) shall always be set up correctly. Users are authorized to access parts of the data managed by the TOE and are trained to exercise control over their own data.
Rationale:	OE.INFO_PROTECT supports the assumption by ensuring that users are authorized to access parts of the data managed by the TOE and is trained to exercise control over their own data.	

5 EXTENDED COMPONENTS DEFINITION

This section specifies the extended Security Functional Requirements (SFRs) used in this ST. One extended SFR is included from the DBMS PP (FIA_USB_(EXT).2) and one extended SFR is included from the DBMS PP EP – Access History (FTA_TAH_(EXT).1). Four additional extended SFRs have been created to address additional security features of the TOE (FDP_ISO_(EXT).1, FDP_LDP_(EXT).1, FDP_SER_(EXT).1, and FMT_PRA_(EXT).1). The SFRs and the rationale for their inclusion are as follows:

a. Isolation of resources (FDP_ISO_(EXT).1)
   Database resources protected in one database instance are logically separate and inaccessible by users in another database instance when both databases are hosted on the same root database;

b. Lockdown Profiles for pluggable databases (FDP_LDP_(EXT).1)
   Privileges of database users may be restricted through the use of Lockdown Profiles;

c. Dedicated services for pluggable databases (FDP_SER_(EXT).1)
   Pluggable databases may only be accessed through dedicated services.

d. Enhanced user-subject binding (FIA_USB_(EXT).2)
   A DBMS may derive subject security attributes from other TSF data that are not directly user security attributes. An example is the point-of-entry the user has used to establish the connection. An access control policy may also use this subject security attribute within its access control policy, allowing access to critical objects only when the user has connected through specific ports-of-entry; and

e. Privilege Analysis (FMT_PRA_(EXT).1)
   Authorized administrators are able to identify the privileges and roles in use, thereby allowing unused privileges to be removed or reduced, and unused roles to be removed in order to mitigate the risk of potential attacks on the associated accounts.

f. TOE access information (FTA_TAH_(EXT).1)
   This PP [the DBMS PP] does not require the TOE to contain a client. Therefore, the PP cannot require the client to display a message. This requirement has been modified to require the TOE to store and retrieve the access history instead of displaying it.

5.1 FDP_ISO ISOLATION OF RESOURCES

Family Behaviour

FDP_ISO_(EXT) is a new family that defines requirements to maintain separate domains for user data. As it addresses separation requirements primarily for user data, it is included in the User data protection class.

FDP_ISO_(EXT).1 is an extended SFR modelled after FPT_SEP.1.2 (from CC 2.3) and is added to this new family.

Component Levelling

FDP_ISO_(EXT).1 is not hierarchical to any other components.

Figure 2 – FDP_ISO_(EXT): Isolation of Resources Component Levelling

Management: FDP_ISO_(EXT).1

The following actions could be considered for the management functions in FMT:

a. an authorized administrator can define separate domains for tenant databases.

Audit: FDP_ISO_(EXT).1

There are no auditable events foreseen.

FDP_ISO_EXT.1 Isolation of Resources

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_ISO_(EXT).1.1 The TSF shall enforce separation between the security domains of subjects.

5.2 FDP_LDP LOCKDOWN PROFILES

Family Behaviour

FDP_LDP_(EXT) is a new family that defines requirements for restricting the privileges of PDB common users.

FDP_LDP_(EXT).1 is an extended SFR modelled after FDP_IFF.1.5 and is added to this new family.

Component Levelling

FDP_LDP_(EXT).1 is not hierarchical to any other components.

Figure 3 – FDP_LDP_(EXT): Lockdown Profiles Component Levelling

Management: FDP_LDP_(EXT).1

The following actions could be considered for the management functions in FMT:

a. an authorized administrator can define lockdown profiles.

b. an authorized administrator can assign lockdown profiles to PDBs.

Audit: FDP_LDP_(EXT).1

There are no auditable events foreseen.

FDP_LDP_(EXT).1 Lockdown Profiles for pluggable databases

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_LDP_(EXT).1.1 Lockdown profiles may be implemented to enable or disable the statements [*assignment: list of statements*]..

FDP_LDP_(EXT).1.2 Lockdown profiles may be implemented to enable or disable the features [*assignment: list of features*].

5.3 FDP_SER DEDICATED SERVICES

Family Behaviour

FDP_SER_(EXT) is a new family that defines requirements to ensure that connections to a pluggable database may only be through one or more dedicated services.

FDP_SER_(EXT).1 is an extended SFR modelled after FPT_SEP.1.2 (from CC 2.3) and is added to this new family.

Component Levelling

FDP_SER_(EXT).1 is not hierarchical to any other components.

Figure 4 – FDP_SER_(EXT): Dedicated Services Component Levelling

Management: FDP_SER_(EXT).1

The following actions could be considered for the management functions in FMT:

a. an authorized administrator can create dedicated services for a PDB.

Audit: FDP_SER_(EXT).1

There are no auditable events foreseen.

FDP_SER_(EXT).1 Dedicated services for pluggable databases

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_SER_(EXT).1.1 Each pluggable database has one or more dedicated services and a connection to a pluggable database can only be made through one of these services.

5.4 FIA_USB USER-SUBJECT BINDING

Family Behaviour

An authenticated user, in order to use the TOE, typically activates a subject. The user's security attributes are associated (totally or partially) with this subject. This family defines requirements to create and maintain the association of the user's security attributes to a subject acting on the user's behalf.

FIA_USB_(EXT).2 is an extended SFR modelled after FIA_USB.1 and added to this existing family. FIA_USB_(EXT).2 is analogous to FIA_USB.1 except that it adds the possibility to specify rules whereby subject security attributes are also derived from TSF data other than user security attributes.

Component Levelling

FIA_USB_(EXT).2 is hierarchical to FIA_USB.1.

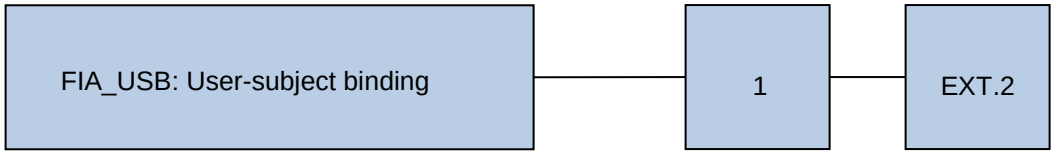

Figure 5 – FIA_USB_(EXT): User-subject binding Component Levelling

Management: FIA_USB_(EXT).2

The following actions could be considered for the management functions in FMT:

a. an authorized administrator can define default subject security attributes.

b. an authorized administrator can change subject security attributes.

Audit: FIA_USB_(EXT).2

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

a. Minimal: Unsuccessful binding of user security attributes to a subject (e.g. creation of a subject).

b. Basic: Success and failure of binding of user security attributes to a subject (e.g. success or failure to create a subject).

FIA_USB_(EXT).2 Enhanced user-subject binding

Hierarchical to: FIA_USB.1

Dependencies: FIA_ATD.1 User attribute definition

FIA_USB_(EXT).2.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [assignment: list of user security attributes].

FIA_USB_(EXT).2.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [assignment: rules for the initial association of attributes].

FIA_USB_(EXT).2.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [assignment: rules for the changing of attributes].

FIA_USB_(EXT).2.4 The TSF shall enforce the following rules for the assignment of subject security attributes not derived from user security attributes when a subject is created: [assignment: rules for the initial association of the subject security attributes not derived from user security attributes].

5.5 FMT_PRA PRIVILEGE ANALYSIS

Family Behaviour

FMT_PRA_(EXT) is a new family that defines requirements to identify the privileges and roles used at runtime. Identifying the privileges and roles in use allows administrators to remove unused privileges and roles which could be subject to attack.

FMT_PRA_(EXT).1 is an extended SFR modelled after FMT_SMR.2 and is added to this new family.

Component Levelling

FMT_PRA_(EXT).1 is not hierarchical to any other components.

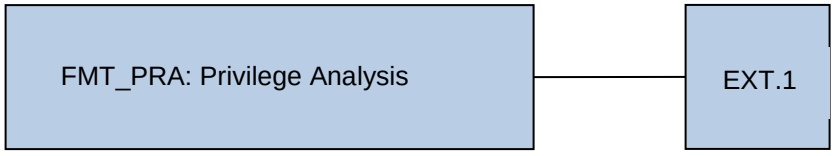

Figure 6 – FMT_PRA_(EXT): Privilege Analysis Component Levelling

Management: FMT_PRA_(EXT).1

The following actions could be considered for the management functions in FMT:

a. an authorized administrator can create, enable and disable a capture policy.

b. an authorized administrator can generate an analysis report from the captured result.

Audit: FMT_PRA_(EXT).1

There are no auditable events foreseen.

FMT_PRA_(EXT).1 Privilege Analysis

Hierarchical to:	No other components.
Dependencies:	No other components.

FMT_PRA_(EXT).1.1 The TSF shall assess the roles and privileges in use at run-time.

5.6 FTA_TAH TOE ACCESS HISTORY

Family Behaviour

This family defines requirements for the TSF to display to a user, upon successful session establishment, a history of successful and unsuccessful attempts to access the user's account.

FTA_TAH_(EXT).1 is an extended SFR modelled after FTA_TAH.1 and added to this existing family. FTA_TAH_(EXT).1 TOE access information provides the requirement for a TOE to make available information related to attempts to establish a session.

Component Levelling

FTA_TAH_(EXT).1 is not hierarchical to any other components.

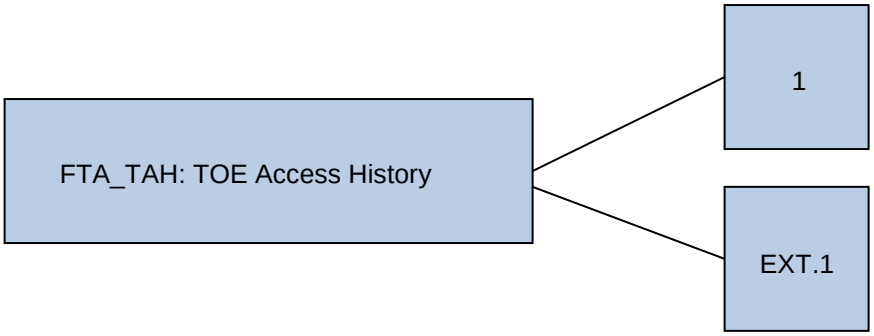

Figure 7 – FTA_TAH_(EXT): TOE Access History Component Levelling

Management: FTA_TAH_(EXT).1

There are no management activities foreseen.

Audit: FTA_TAH_(EXT).1

There are no auditable events foreseen.

FTA_TAH_(EXT).1 TOE access information

Hierarchical to: No other components.

Dependencies: No dependencies

FTA_TAH_(EXT).1.1 Upon a session establishment attempt, the TSF shall store

a. the [date and time] of the session establishment attempt of the user.

b. the incremental count of successive unsuccessful session establishment attempt(s).

FTA_TAH_(EXT).1.2 Upon successful session establishment, the TSF shall allow the [date and time] of

a. the previous last successful session establishment, and

b. the last unsuccessful attempt to session establishment and the number of unsuccessful attempts since the previous last successful session establishment

to be retrieved by the user.

5.7 SECURITY ASSURANCE REQUIREMENTS

This ST does not include extended Security Assurance Requirements.

6 SECURITY REQUIREMENTS

Section 6 provides security functional and assurance requirements that must be satisfied by a compliant TOE. These requirements consist of functional components from Part 2 of the CC, extended requirements, and an Evaluation Assurance Level (EAL) that contains assurance components from Part 3 of the CC.

6.1 CONVENTIONS

The CC permits four types of operations to be performed on functional requirements: selection, assignment, refinement, and iteration. These operations, when performed on requirements that derive from CC Part 2 are identified in this ST in the following manner:

- Selection: Indicated by surrounding brackets, e.g., [selected item].
- Assignment: Indicated by surrounding brackets and italics, e.g., [*assigned item*].
- Refinement: Refined components are identified by using **bold** for additional information, or ~~strikeout~~ for deleted text.
- Iteration: Indicated by assigning a number in parenthesis to the end of the functional component identifier as well as by modifying the functional component title to distinguish between iterations, e.g., 'FDP_ACC.1(1), Subset access control (administrators)' and 'FDP_ACC.1(2) Subset access control (devices)'.

6.2 TOE SECURITY FUNCTIONAL REQUIREMENTS

The security functional requirements for this ST consist of the following components from Part 2 of the CC and extended components defined in Section 5, summarized in Table 10 - Summary of Security Functional Requirements.

Class	Identifier	Name
Security Audit (FAU)	FAU_GEN.1	Audit data generation
	FAU_GEN.2	User identity association
	FAU_SEL.1	Selective audit
User Data Protection (FDP)	FDP_ACC.1(1)	Subset access control
	FDP_ACC.1(2)	Subset access control (Database Vault)
	FDP_ACF.1(1)	Security attribute based access control
	FDP_ACF.1(2)	Security attribute based access control (Database Vault)
	FDP_ISO_(EXT).1	Isolation of resources
	FDP_LDP_(EXT).1	Lockdown Profiles for pluggable databases
	FDP_RIP.1	Subset residual information protection
	FDP_SER_(EXT).1	Dedicated services for pluggable databases
Identification and Authentication (FIA)	FIA_ATD.1	User attribute definition
	FIA_UAU.1	Timing of authentication
	FIA_UID.1	Timing of identification
	FIA_USB_(EXT).2	Enhanced user-subject binding
Security Management (FMT)	FMT_MOF.1	Management of security functions behaviour
	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialisation
	FMT_MTD.1	Management of TSF data

Class	Identifier	Name
	FMT_REV.1(1)	Revocation (user attributes)
	FMT_REV.1(2)	Revocation (subject, object attributes)
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1(1)	Security roles
	FMT_SMR.1(2)	Security roles (Database Vault)
	FMT_SMR.1(3)	Security roles (Multitenant)
	FMT_PRA_(EXT).1	Privilege Analysis
Protection of the TSF (FPT)	FPT_TRC.1	Internal TSF consistency
TOE Access (FTA)	FTA_MCS.1	Basic limitation on multiple concurrent sessions
	FTA_TAH_(EXT).1	TOE access information
	FTA_TSE.1	TOE session establishment

Table 10 – Summary of Security Functional Requirements

6.2.1 Security Audit (FAU)

6.2.1.1 FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;
b) All auditable events for the [minimum] level of audit **listed in Table 11: Auditable Events**; and
c) [Start-up and shutdown of the DBMS;
d) Use of special permissions (e.g., those often used by authorized administrators to circumvent access control policies); and
e) [[*Use of access control functions enforced by Database Vault*]]].

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [*information specified in column three of Table 11: Auditable Events, below*].

Column 1: **Security Functional Requirement**	**Column 2:** **Auditable Event(s)**	**Column 3:** **Additional Audit Record Contents**
FAU_GEN.1	None	None
FAU_GEN.2	None	None
FAU_SEL.1	All modifications to the audit configuration that occur while the audit collection functions are operating	The identity of the authorized administrator that made the change to the audit configuration
FDP_ACC.1(1)	None	None
FDP_ACC.1(2)	None	None
FDP_ACF.1(1)	Successful requests to perform an operation on an object covered by the SFP	The identity of the subject performing the operation
FDP_ACF.1(2)	Successful requests to perform an operation on an object covered by the SFP	The identity of the subject performing the operation
FDP_ISO_(EXT).1	None	None
FDP_LDP_(EXT).1	None	None
FDP_RIP.1	None	None
FDP_SER_(EXT).1	None	None
FIA_ATD.1	None	None
FIA_UAU.1	Unsuccessful use of the authentication mechanism	None
FIA_UID.1	Unsuccessful use of the user identification mechanism, including the user identity provided	None
FIA_USB_(EXT).2	Unsuccessful binding of user security attributes to a subject (e.g. creation of a subject)	None
FMT_MOF.1	None	None
FMT_MSA.1	None	None

Column 1: Security Functional Requirement	Column 2: Auditable Event(s)	Column 3: Additional Audit Record Contents
FMT_MSA.3	None	None
FMT_MTD.1	None	None
FMT_REV.1(1)	Unsuccessful revocation of security attributes	Identity of individual attempting to revoke security attributes
FMT_REV.1(2)	Unsuccessful revocation of security attributes	Identity of individual attempting to revoke security attributes
FMT_SMF.1	Use of the management functions	Identity of the administrator performing these functions
FMT_SMR.1(1)	Modifications to the group of users that are part of a role	Identity of authorized administrator modifying the role definition
FMT_SMR.1(2)	Modifications to the group of users that are part of a role	Identity of authorized administrator modifying the role definition
FMT_SMR.1(3)	Modifications to the group of users that are part of a role	Identity of authorized administrator modifying the role definition
FMT_PRA_(EXT).1	None	None
FPT_TRC.1	Restoring consistency	None
FTA_MCS.1	Rejection of a new session based on the limitation of multiple concurrent sessions	None
FTA_TAH_(EXT).1	None	None
FTA_TSE.1	Denial of a session establishment due to the session establishment mechanism	Identity of the individual attempting to establish a session

Table 11 – Auditable Events

6.2.1.2 FAU_GEN.2 User identity association

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation
FIA_UID.1 Timing of identification

FAU_GEN.2.1 For audit events resulting from actions of identified users **and any identified groups**, the TSF shall be able to associate each auditable event with the identity of the **[**user**]** that caused the event.

6.2.1.3 FAU_SEL.1 Selective audit

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit data generation
FMT_MTD.1 Management of TSF data

FAU_SEL.1.1 The TSF shall be able to select the set of events to be audited from the set of all auditable events based on the following attributes:

a) [object identity,
b) user identity,
c) [**no other identities**];
d) event type;]
e) [*success of auditable security events;*
f) *failure of auditable security events; and*
g) [[*no additional attributes*]].]

Application Note: The audit functionality may be configured to audit specified operations. 'Event type' is defined to be these specified operations for the purposes of FAU_SEL.1.

6.2.2 User Data Protection (FDP)

6.2.2.1 FDP_ACC.1(1) Subset access control

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1(1) The TSF shall enforce the [*Discretionary Access Control Policy*] on [*all subjects, all DBMS-controlled objects, and all operations among them*].

6.2.2.2 FDP_ACC.1(2) Subset access control (Database Vault)

Hierarchical to: No other components.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1(2) The TSF shall enforce the [*DBVault Access Control Policy*] on [*all subjects, all DB Vault-controlled objects, and all operations among them*].

6.2.2.3 FDP_ACF.1(1) Security attribute based access control

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1(1) The TSF shall enforce the [*Discretionary Access Control Policy*] to objects based on the following: [

Subjects: Database Users
Subject attributes: database role, system privileges
Objects: Database object
Object attributes: object privileges, any attribute].

FDP_ACF.1.2(1) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [*A user may access an object if:*

a. *the user is the owner of the object or has been granted specific object privileges;*
b. *the user has been granted specific system privileges allowing access to the object;*
c. *the user is a member of a role that has been granted specific object and/or system privileges;*
d. *a policy allows the user access based on the value of a specified attribute;*
e. *the object is accessible by 'PUBLIC'.*].

FDP_ACF.1.3(1) The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*no additional rules*].

FDP_ACF.1.4(1) The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*no additional rules*].

Application Note: A database object is an object in the database that may be manipulated with SQL. These include tables, cases, files, and views. An attribute is a property or detail associated with an object. 'Any attribute' refers to any property or detail associated with a database object.

Application Note: 'PUBLIC' is a special role granted to all users.

6.2.2.4 FDP_ACF.1(2) Security attribute based access control (Database Vault)

Hierarchical to: No other components.

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1(2) The TSF shall enforce the [*DBVault Access Control Policy*] to objects based on the following: [

Subjects: Database Users
Subject attributes: ownership, realm authorization, system privilege
Objects: Database object protected by DB Vault
Object attributes: object privilege, realm, command rules].

FDP_ACF.1.2(2) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [*A user may access an object if:*

a. *When an object is protected by a regular realm, a user can access the object if:*
    1. *The user is the owner of the object or has been granted the specific object privilege, or*
    2. *The user has been granted specific system privileges and has been authorized for the realm;*
b. *When an object is protected by a mandatory realm, a user can access the object if:*
    1. *The user is the owner of the object or has been granted the specific object or system privilege, and*
    2. *The user has been authorized for the realm;*

c. *When an object is protected by a command rule, a user can access the object if all the rules in the rule set associated with the command rule evaluate to true*].

FDP_ACF.1.3(2) The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*no additional rules*].

FDP_ACF.1.4(2) The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*no additional rules*].

Application Note: For objects protected by Database Vault, both the DBVault Access Control Policy and the Discretionary Access Control Policy must allow access to the object. Otherwise, access will be denied.

6.2.2.5 FDP_ISO_(EXT).1 Isolation of resources

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_ISO_(EXT).1.1 The TSF shall enforce separation between the security domains of subjects.

6.2.2.6 FDP_LDP_(EXT).1 Lockdown Profiles for pluggable databases

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_LDP_(EXT).1.1 Lockdown profiles may be implemented to enable or disable the statements [*ALTER DATABASE, ALTER PLUGGABLE DATABASES, ALTER SESSION, ALTER SYSTEM*].

FDP_LDP_(EXT).1.2 Lockdown profiles may be implemented to enable or disable the features [*AWR_ACCESS, COMMON_USER_LOCAL_SCHEMA_ACCESS, LOCAL_USER_COMMON_SCHEMA_ACCESS, SECURITY_POLICIES, COMMON_USER_CONNECT, LOCAL_SYSOPER_RESTRICTED_MODE_CONNECT, CTX_LOGGING, JAVA, JAVA_RUNTIME, AQ_PROTOCOLS, CTX_PROTOCOLS, DBMS_DEBUG_JDWP, UTL_HTTP, UTL_INADDR, UTL_SMTP, UTL_TCP, XDB_PROTOCOLS, DROP_TABLESPACE_KEEP_DATAFILES, EXTERNAL_AND_GLOBAL_AUTHENTICATION, EXTERNAL_FILE_ACCESS, EXTERNAL_PROCEDURES, FILE_TRANSFER, JAVA_OS_ACCESS, LOB_FILE_ACCESS, TRACE_VIEW_ACCESS, UTL_FILE*].

6.2.2.7 FDP_RIP.1 Subset residual information protection

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_RIP.1.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [allocation of the resource to] the following objects: [*table, row*].

6.2.2.8 FDP_SER_(EXT).1 Dedicated services for pluggable databases

Hierarchical to: No other components.

Dependencies: No dependencies.

FDP_SER_(EXT).1.1 Each pluggable database has one or more dedicated services and a connection to a pluggable database can only be made through one of these services.

6.2.3 Identification and Authentication (FIA)

6.2.3.1 FIA_ATD.1 User attribute definition

Hierarchical to: No other components.

Dependencies: No dependencies.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:

a) [*Database user identifier and any associated group memberships;*
b) *Security-relevant database roles; and*
c) [*object privileges, system privileges, any attribute*]].

Application Note: The intent of this requirement, as described in the DBMS PP, is to specify the TOE security attributes that the TOE utilizes to determine access. However, it should be noted that the object privileges, system privileges and attributes, although used in the access control decision, are not specifically associated with individual users.

Application Note: An attribute is a property or detail associated with an object. 'Any attribute' refers to any property or detail associated with a database object.

6.2.3.2 FIA_UAU.1 Timing of authentication

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.1.1 The TSF shall allow [*no TSF mediated actions*] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.2.3.3 FIA_UID.1 Timing of identification

Hierarchical to: No other components.
Dependencies: No dependencies.

FIA_UID.1.1 The TSF shall allow [*no TSF mediated actions*] on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.2.3.4 FIA_USB_(EXT).2 Enhanced user-subject binding

Hierarchical to: FIA_USB.1 User-subject binding

Dependencies: FIA_ATD.1 User attribute definition

FIA_USB_(EXT).2.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [*Database user identifier*, *roles, privileges*].

FIA_USB_(EXT).2.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of

users: [*an authorized administrator may allow a proxy user to perform database operations on behalf on another user*].

FIA_USB_(EXT).2.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [

a. granting and revoking of directly assigned privileges are effective immediately;
b. granting and revoking of indirectly assigned privileges are effective at the next log in].

FIA_USB_(EXT).2.4 The TSF shall enforce the following rules for the assignment of subject security attributes not derived from user security attributes when a subject is created: [*the proxy may be limited to the privileges of a particular role when acting on behalf of another user*].

6.2.4 Security Management (FMT)

6.2.4.1 FMT_MOF.1 Management of security functions behaviour

Hierarchical to: No other components.

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of management functions

FMT_MOF.1.1 The TSF shall restrict the ability to [disable and enable] the functions [*relating to the specification of events to be audited*] to [*authorised administrators*].

6.2.4.2 FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of management functions

FMT_MSA.1.1 The TSF shall enforce the [*Discretionary Access Control Policy and DBVault Access Control Policy*] to restrict the ability to [[*manage*]] [*all*] the security attributes to [*authorised administrators*].

Application Note: The security attribute assignment has been moved to enhance readability, and for consistency with the PP.

6.2.4.3 FMT_MSA.3 Static attribute initialisation

Hierarchical to: No other components.

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the [*Discretionary Access Control Policy and DBVault Access Control Policy*] to provide [restrictive] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow ~~the~~ [*no user*] to specify alternative initial values to override the default values when an object or information is created.

6.2.4.4 FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.
Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of management functions

FMT_MTD.1.1 The TSF shall restrict the ability to [[*include or exclude*]] the [*auditable events*] to [*authorized administrators*].

6.2.4.5 FMT_REV.1(1) Revocation

Hierarchical to: No other components.
Dependencies: FMT_SMR.1 Security roles

FMT_REV.1(1).1 The TSF shall restrict the ability to revoke [*system privileges, roles*] associated with the [users] under the control of the TSF to [*the authorised administrator*].

FMT_REV.1(1).2 The TSF shall enforce the rules [

a. granting and revoking of directly assigned privileges are effective immediately; and
b. granting and revoking of indirectly assigned privileges are effective at the next log in].

6.2.4.6 FMT_REV.1(2) Revocation

Hierarchical to: No other components.
Dependencies: FMT_SMR.1 Security roles

FMT_REV.1(2).1 The TSF shall restrict the ability to revoke [*object privileges*] associated with the [objects] under the control of the TSF to [*the authorized administrator*] **and database users with sufficient privileges as allowed by the Discretionary Access Control Policy**.

FMT_REV.1(2).2 The TSF shall enforce the rules [

a. authorized administrators and object owners may revoke object privileges; and

b. object owners may grant other users privileges to grant and revoke object privileges].

6.2.4.7 FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.
Dependencies: No dependencies.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [

a. management of the events to be audited;

b. granting or revoking of system privileges;

c. granting or revoking of object privileges;

d. changes to user accounts (including authentication) and roles;

e. configuration of Active Data Guard replication options;

f. configuration of the maximum number of concurrent sessions for an individual user;

g. configuration of Database Vault functions;

h. configuration of separate domains for pluggable databases within a container database;

i. *creation, enabling and disabling of capture policies*;

j. *generation of an analysis report from a capture result*;

k. *definition of lockdown profiles*;

l. *assignment of lockdown profiles to PDBs*;

m. *creation of dedicated services for a PDB*].

6.2.4.8 FMT_SMR.1(1) Security roles

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1(1) The TSF shall maintain the roles [*authorized administrator and[database user and other roles defined by authorized administrators]*].

FMT_SMR.1.2(1) The TSF shall be able to associate users with roles.

6.2.4.9 FMT_SMR.1(2) Security roles (Database Vault)

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1(2) The TSF shall maintain the roles [*DV_OWNER, DV_ADMIN, DV_ACCTMGR*, *DV_SECANALYST, CAPTURE_ADMIN*].

FMT_SMR.1.2(2) The TSF shall be able to associate users with roles.

6.2.4.10 FMT_SMR.1(3) Security roles (Multitenant)

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1(3) The TSF shall maintain the roles [*local users, common users*].

FMT_SMR.1.2(3) The TSF shall be able to associate users with roles.

6.2.4.11 FMT_PRA_(EXT).1 Privilege Analysis

Hierarchical to: No other components.

Dependencies: No other components.

FMT_PRA_(EXT).1.1 The TSF shall assess the roles and privileges in use at run-time.

6.2.5 Protection of the TSF (FPT)

6.2.5.1 FPT_TRC.1 Internal TSF consistency

Hierarchical to: No other components.

Dependencies: FPT_ITT.1 Basic internal TSF data transfer protection

FPT_TRC.1.1 The TSF shall ensure that TSF data is consistent when replicated between parts of the TOE.

FPT_TRC.1.2 When parts of the TOE containing replicated TSF data are disconnected, the TSF shall ensure the consistency of the replicated TSF data upon reconnection before processing any requests for [*queries*].

6.2.6 TOE Access (FTA)

6.2.6.1 FTA_MCS.1 Basic limitation on multiple concurrent sessions

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification

FTA_MCS.1.1 The TSF shall restrict the maximum number of concurrent sessions that belong to the same user.

FTA_MCS.1.2 The TSF shall enforce, by default, a limit of [*an administrator configurable number of*] sessions per user.

6.2.6.2 FTA_TAH_(EXT).1 TOE access information

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_TAH_(EXT).1.1 Upon a session establishment attempt, the TSF shall store

a. the [date and time] of the session establishment attempt of the user.

b. the incremental count of successive unsuccessful session establishment attempt(s).

FTA_TAH_(EXT).1.2 Upon successful session establishment, the TSF shall allow the [date and time] of

a. the previous last successful session establishment, and

b. the last unsuccessful attempt to session establishment and the number of unsuccessful attempts since the previous last successful session establishment

to be retrieved by the user.

6.2.6.3 FTA_TSE.1 TOE session establishment

Hierarchical to: No other components.

Dependencies: No dependencies.

FTA_TSE.1.1 The TSF shall be able to deny session establishment based on [*[attributes that can be set explicitly by authorized administrator(s), including user identity, and [[no additional attributes]]*].

6.3 SECURITY FUNCTIONAL REQUIREMENTS RATIONALE

The following Table provides a mapping between the SFRs and Security Objectives.

	O.ACCESS_HISTORY	O.ADMIN_ROLE	O.AUDIT_GENERATION	O.DISCRETIONARY_ACCESS	O.I&A	O.MANAGE	O.MEDIATE	O.RESIDUAL_INFORMATION	O.TOE_ACCESS
FAU_GEN.1			X						
FAU_GEN.2			X						
FAU_SEL.1			X						
FDP_ACC.1(1)				X			X		X
FDP_ACC.1(2)				X			X		X
FDP_ACF.1(1)				X			X		X
FDP_ACF.1(2)				X			X		X
FDP_ISO_(EXT).1									X
FDP_LDP_(EXT).1									X
FDP_RIP.1								X	
FDP_SER_(EXT).1									X
FIA_ATD.1					X				X
FIA_UAU.1					X				
FIA_UID.1					X				
FIA_USB_(EXT).2					X				
FMT_MOF.1						X			

	O.ACCESS_HISTORY	O.ADMIN_ROLE	O.AUDIT_GENERATION	O.DISCRETIONARY_ACCESS	O.I&A	O.MANAGE	O.MEDIATE	O.RESIDUAL_INFORMATION	O.TOE_ACCESS
FMT_MSA.1						X			
FMT_MSA.3						X			
FMT_MTD.1						X			
FMT_REV.1(1)						X			
FMT_REV.1(2)						X			
FMT_SMF.1						X			
FMT_SMR.1(1)		X				X			
FMT_SMR.1(2)		X				X			
FMT_SMR.1(3)		X				X			
FMT_PRA_(EXT).1						X			
FPT_TRC.1							X		
FTA_MCS.1									X
FTA_TAH_(EXT).1	X								
FTA_TSE.1									X

Table 12 – Mapping of SFRs to Security Objectives

6.3.1 SFR Rationale Related to Security Objectives

The following rationale traces each SFR back to the Security Objectives for the TOE.

Objective: **O.ACCESS_HISTORY**	The TOE will store information related to previous attempts to establish a session and make that information available to the user.

Security Functional Requirements:	FTA_TAH_(EXT).1	TOE access information
Rationale:	The TOE must be able to store and retrieve information about previous unauthorized login attempts and the number of times the login was attempted every time the user logs into their account. The TOE must also store the last successful authorized login. This information will include the date, time, method, and location of the attempts. When appropriately displayed, this will allow the user to detect if another user is attempting to access their account. These records should not be deleted until after the user has been notified of his/her access history. [FTA_TAH_(EXT).1]	

Objective: **O.ADMIN_ROLE**	The TOE will provide a mechanism (e.g. a "role") by which the actions using administrative privileges may be restricted.	
Security Functional Requirements:	FMT_SMR.1(1)	Security roles
	FMT_SMR.1(2)	Security roles (Database Vault)
	FMT_SMR.1(3)	Security roles (Multitenant)
Rationale:	The TOE will establish, at least, an authorized administrator role. The ST writer may choose to specify more roles. The authorized administrator will be given privileges to perform certain tasks that other users will not be able to perform. These privileges include, but are not limited to, access to audit information and security functions. [FMT_SMR.1(1)] Additional roles are established specifically for enforcement of the DBVault Access Control Policy. [FMT_SMR.1(2)] The multitenant implementation utilizes two classes of users, local users and common users. These user types are used to restrict administrative privileges. [FMT_SMR.1(3)]	

Objective: **O.AUDIT _GENERATION**	The TSF must be able to record defined security-relevant events (which usually include security-critical actions of users of the TOE). The information recorded for security-relevant events must contain the time and date the event happened and, if possible, the identification of the user that caused the event, and must be in sufficient detail to help the authorized user detect attempted security violations or potential misconfiguration of the TOE security features that would leave the IT assets open to compromise.	
Security Functional Requirements:	FAU_GEN.1	Audit data generation
	FAU_GEN.2	User identity association

	FAU_SEL.1	Selective audit
Rationale:	FAU_GEN.1 defines the set of events that the TOE must be capable of recording. This requirement ensures that the administrator has the ability to audit any security relevant events that takes place in the TOE. This requirement also defines the information that must be contained in the audit record for each auditable event. This requirement also places a requirement on the level of detail that is recorded on any additional security functional requirements a ST author adds to the ST. [FAU_GEN.1] FAU_GEN.2 ensures that the audit records associate a user and any associated group identity with the auditable event. In the case of authorized users, the association is accomplished with the user ID. In the case of authorized groups, the association is accomplished with the group ID. [FAU_GEN.2] FAU_SEL.1 allows the administrator to configure which auditable events will be recorded in the audit trail. This provides the administrator with the flexibility in recording only those events that are deemed necessary by site policy, thus reducing the amount of resources consumed by the audit mechanism. [FAU_SEL.1]	

Objective: **O.DISCRETION-ARY_ACCESS**	The TSF must control access of subjects and/or users to named resources based on identity of the object, subject, or user. The TSF must allow authorized users to specify for each access mode which users/subjects are allowed to access a specific named object in that access mode.	
Security Functional Requirements:	FDP_ACC.1(1)	Subset access control
	FDP_ACF.1(1)	Security attribute based access control
	FDP_ACC.1(2)	Subset access control (Database Vault)
	FDP_ACF.1(2)	Security attribute based access control (Database Vault)
Rationale:	The TSF must control access to resources based on the identity of users that are allowed to specify which resources they want to access for storing their data. The access control policy must have a defined scope of control [FDP_ACC.1(1)]. The rules for the access control policy are defined [FDP_ACF.1(1)]. Use of the Database Vault Access Control Policy allows additional control of which users are allowed to access a specific named object. [FDP_ACC.1(2), FDP_ACF.1(2)]	

Objective: **O.I&A**	The TOE ensures that users are authenticated before the TOE processes any actions that require authentication.	
Security Functional Requirements:	FIA_ATD.1	User attribute definition
	FIA_UAU.1	Timing of authentication
	FIA_UID.1	Timing of identification
	FIA_USB_(EXT).2	Enhanced user-subject binding
Rationale:	The TSF must ensure that only authorized users gain access to the TOE and its resources. Users authorized to access the TOE must use an identification and authentication process [FIA_UID.1, FIA_UAU.1]. To ensure that the security attributes used to determine access are defined and available to the support authentication decisions. [FIA_ATD.1]. Proper authorization for subjects acting on behalf of users is also ensured [FIA_USB_(EXT).2]. The appropriate strength of the authentication mechanism is ensured.	

Objective: **O.MANAGE**	The TSF must provide all the functions and facilities necessary to support the authorized users that are responsible for the management of TOE security mechanisms, must allow restricting such management actions to dedicated users, and must ensure that only such authorized users are able to access management functionality.	
Security Functional Requirements:	FMT_MOF.1	Management of security functions behaviour
	FMT_MSA.1	Management of security attributes
	FMT_MSA.3	Static attribute initialisation
	FMT_MTD.1	Management of TSF data
	FMT_REV.1(1)	Revocation (user attributes)
	FMT_REV.1(2)	Revocation (subject, object attributes)
	FMT_SMF.1	Specification of management functions
	FMT_SMR.1(1)	Security roles
	FMT_SMR.1(2)	Security roles (Database Vault)
	FMT_SMR.1(3)	Security roles (Multitenant)

	FMT_PRA_(EXT).1	Privilege Analysis
Rationale:	FMT_MOF.1 requires that the ability to use particular TOE capabilities be restricted to the administrator. [FMT_MOF.1] FMT_MSA.1 requires that the ability to perform operations on security attributes be restricted to particular roles. [FMT_MSA.1] FMT_MSA.3 requires that default values used for security attributes are restrictive. [FMT_MSA.3] FMT_MTD.1 requires that the ability to manipulate TOE content is restricted to administrators. [FMT_MTD.1] FMT_REV.1 restricts the ability to revoke attributes to the administrator. [FMT_REV.1(1), FMT_REV.1(2)] FMT_SMF.1 identifies the management functions that are available to the authorized administrator. [FMT_SMF.1] FMT_SMR.1(1) defines the specific security roles to be supported. [FMT_SMR.1(1)] FMT_SMR.1(2) defines additional security roles supported to facilitate the DBVault Access Control Policy. [FMT_SMR.1(2)] FMT_SMR.1(3) defines the security roles supported by multitenant implementations to control access. [FMT_SMR.1(3)] FMT_PRA_(EXT).1 provides security management functions to determine the roles and privileges in active use. [FMT_PRA_(EXT).1]	

Objective: **O.MEDIATE**	The TOE must protect user data in accordance with its security policy, and must mediate all requests to access such data.	
Security Functional Requirements:	FDP_ACC.1(1)	Subset access control
	FDP_ACF.1(1)	Security attribute based access control
	FDP_ACC.1(2)	Subset access control (Database Vault)
	FDP_ACF.1(2)	Security attribute based access control (Database Vault)
	FPT_TRC.1	Internal TSF consistency
Rationale:	The FDP requirements were chosen to define the policies, the subjects, objects, and operations for how and when mediation takes place in the TOE. FDP_ACC.1(1) defines the Access Control policy that will be enforced on a list of subjects acting on the behalf of users attempting to gain access to a list of named objects. All the operations between subject and object covered are defined by the	

	TOE's policy. [FDP_ACC.1(1)] FDP_ACF.1(1) defines the security attribute used to provide access control to objects based on the TOE's access control policy. [FDP_ACF.1(1)] FDP_ACC.1(2) defines an additional level of Access Control policy that can be used to further restrict the ability of users with system permission to gain access to named objects. [FDP_ACC.1(1)] FDP_ACF.1(2) defines the security attributes used to provide access control to objects based on the DBVault access control policy. [FDP_ACF.1(2)] FPT_TRC.1 ensures replicated TSF data that specifies attributes for access control must be consistent across distributed components of the TOE. The requirement is to maintain consistency of replicated TSF data. [FPT_TRC.1]

Objective: **O.RESIDUAL_INFORMATION**	The TOE will ensure that any information contained in a protected resource within its Scope of Control is not inappropriately disclosed when the resource is reallocated.	
Security Functional Requirements:	FDP_RIP.1	Subset residual information protection
Rationale:	FDP_RIP.1 is used to ensure the contents of resources are not available to subjects other than those explicitly granted access to the data. [FDP_RIP.1]	

Objective: **O.TOE_ACCESS**	The TOE will provide mechanisms that control a user's logical access to user data and to the TSF.	
Security Functional Requirements:	FDP_ACC.1(1)	Subset access control
	FDP_ACF.1(1)	Security attribute based access control
	FDP_ACC.1(2)	Subset access control (Database Vault)
	FDP_ACF.1(2)	Security attribute based access control (Database Vault)
	FDP_ISO_(EXT).1	Isolation of resources
	FDP_LDP_(EXT).1	Lockdown Profiles for pluggable databases
	FDP_SER_(EXT).1	Dedicated services for pluggable databases
	FIA_ATD.1	User attribute definition

	FTA_MCS.1	Basic limitation on multiple concurrent sessions
	FTA_TSE.1	TOE session establishment
Rationale:	FDP_ACC.1(1) requires that each identified access control SFP be in place for a subset of the possible operations on a subset of the objects in the TOE. [FDP_ACC.1(1)] FDP_ACF.1(1) allows the TSF to enforce access based upon security attributes and named groups of attributes. Furthermore, the TSF may have the ability to explicitly authorize or deny access to an object based upon security attributes. [FDP_ACF.1(1)] FDP_ACC.1(2) defines the DBVault access control policy which may be used to restrict access to user data. [FDP_ACC.1(2)] FDP_ACF.1(2) allows the TSF to enforce access based upon DBVault security attributes. [FDP_ACF.1(2)] FDP_ISO_(EXT).1 ensures that users of one pluggable database do not have access to resources held in another pluggable database. [FDP_ISO_(EXT).1] FDP_LDP_(EXT).1 ensures that access by common users to user data in pluggable databases is restricted using lockdown profiles. [FDP_LDP_(EXT).1] FDP_SER_(EXT).1 ensures that pluggable databases are only accessible through dedicated services. [FDP_SER_(EXT).1] FIA_ATD.1 defines the security attributes for individual users including the user's identifier and any associated group memberships. Security relevant roles and other identity security attributes. [FIA_ATD.1] FTA_MCS.1 ensures that users may only have a maximum of a specified number of active sessions open at any given time. [FTA_MCS.1] FTA_TSE.1 allows the TOE to restrict access to the TOE based on certain criteria. [FTA_TSE.1]	

6.4 DEPENDENCY RATIONALE

Table 13 identifies the Security Functional Requirements from Part 2 of the CC and their associated dependencies. It also indicates whether the ST explicitly addresses each dependency.

SFR	Dependency	Rationale
FAU_GEN.1	FPT_STM.1	This requirement is satisfied by the assumption on the IT environment, given in A.SUPPORT.
FAU_GEN.2	FAU_GEN.1	satisfied by FAU_GEN.1
	FIA_UID.1	satisfied by FIA_UID.1
FAU_SEL.1	FAU_GEN.1	satisfied by FAU_GEN.1
	FAU_MTD.1	satisfied by FAU_MTD.1
FDP_ACC.1(1)	FDP_ACF.1	satisfied by FDP_ACF.1(1)
FDP_ACC.1(2)	FDP_ACF.1	satisfied by FDP_ACF.1(2)
FDP_ACF.1(1)	FDP_ACC.1	satisfied by FDP_ACC.1(1)
	FMT_MSA.3	satisfied by FMT_MSA.3
FDP_ACF.1(2)	FDP_ACC.1	satisfied by FDP_ACC.1(2)
	FMT_MSA.3	satisfied by FMT_MSA.3
FDP_ISO_(EXT).1	None	N/A
FDP_LDP_(EXT).1	None	N/A
FDP_RIP.1	None	N/A
FDP_SER_(EXT).1	None	N/A
FIA_ATD.1	None	N/A
FIA_UAU.1	FIA_UID.1	satisfied by FIA_UID.1
FIA_UID.1	None	N/A
FIA_USB_(EXT).2	FIA_ATD.1	satisfied by FIA_ATD.1
FMT_MOF.1	FMT_SMR.1	satisfied by FMT_SMR.1(1)
	FMT_SMF.1	satisfied by FMT_SMF.1
FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1	satisfied by FDP_ACC.1
	FMT_SMR.1	satisfied by FMT_SMR.1(1) and FMT_SMR.1(2)
	FMT_SMF.1	satisfied by FMT_SMF.1(1) and FMT_SMR.1(2)

SFR	Dependency	Rationale
FMT_MSA.3	FMT_MSA.1	satisfied by FMT_MSA.1
	FMT_SMR.1	satisfied by FMT_SMR.1(1) and FMT_SMR.1(2)
FMT_MTD.1	FMT_SMR.1	satisfied by FMT_SMR.1(1)
	FMT_SMF.1	satisfied by FMT_SMF.1
FMT_REV.1(1)	FMT_SMR.1	satisfied by FMT_SMR.1(1) and FMT_SMR.1(2)
FMT_REV.1(2)	FMT_SMR.1	satisfied by FMT_SMR.1(1)
FMT_SMF.1	None	N/A
FMT_SMR.1(1)	FIA_UID.1	satisfied by FIA_UID.1
FMT_SMR.1(2)	FIA_UID.1	satisfied by FIA_UID.1
FMT_SMR.1(3)	FIA_UID.1	satisfied by FIA_UID.1
FMT_PRA_(EXT).1	None	N/A
FPT_TRC.1	FPT_ITT.1	FPT_ITT.1 is not applicable. For a distributed TOE, the dependency is satisfied through the assumption on the environment, A.CONNECT, that assures the confidentiality and integrity of the transmitted data.
FTA_MCS.1	FIA_UID.1	satisfied by FIA_UID.1
FTA_TAH_(EXT).1	None	N/A
FTA_TSE.1	None	N/A

Table 13 – Functional Requirement Dependencies

6.5 TOE SECURITY ASSURANCE REQUIREMENTS

The TOE assurance requirements for this ST consist of the requirements corresponding to the EAL 2 level of assurance, as defined in the CC Part 3, augmented by the inclusion of Flaw reporting procedures (ALC_FLR.2). This is the assurance level described in the claimed PP.

6.5.1 Security Assurance Requirements Rationale

The DBMS PP was developed for use by commercial DBMS security software developers. Since the PP will be applied to commercial DBMS products that are used internationally the EAL 2 assurance package was selected by the PP writers to meet the maximum level of assurance that is recognized internationally through the Common Criteria Recognition Arrangement (CCRA).

Flaw Remediation is the only requirement not included in any EAL level because it does not add any assurance to the current system, but to subsequent releases. Therefore, the DBMS WG/TC decided to augment EAL2 with ALC_FLR.2 to instruct the vendors on proper flaw remediation techniques.

The dependencies for security assurance requirements are all fulfilled based on the following facts:

- EAL2 is completely self-sufficient with all dependencies being fulfilled with the package of EAL2.
- The security assurance requirement of ALC_FLR.2, which is in addition to EAL2, does not have any dependencies.

The assurance requirements are summarized in the Table 14.

Assurance Class	Assurance Components	
	Identifier	**Name**
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	Basic design
Guidance Documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-cycle support	ALC_CMC.2	Use of a CM[2] system
	ALC_CMS.2	Parts of the TOE CM coverage

[2] Configuration Management

Assurance Class	Assurance Components	
	Identifier	**Name**
	ALC_DEL.1	Delivery procedures
	ALC_FLR.2	Flaw reporting procedures
Security Target Evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing - sample
Vulnerability Assessment	AVA_VAN.2	Vulnerability analysis

Table 14 – Security Assurance Requirements

7 TOE SUMMARY SPECIFICATION

This section provides a description of the security functions and assurance measures of the TOE that meet the TOE security requirements.

A description of each of the TOE security functions follows.

7.1 SECURITY AUDIT

Oracle Database 12cR2 supports two auditing mechanisms: traditional auditing and unified auditing. For the purposes of meeting the auditing requirements of the DBMS PP, either method, or a combination of both methods may be used.

The AUDIT statement is used to track the issuance of specific SQL statements, or all SQL statements authorized by a particular system privilege. It may also be used to track operations on a specific schema object. The AUDIT_TRAIL system parameter may be used to determine the format and location of the audit entries. Entries for start-up and shutdown events are sent to the operating system for logging.

Audit policies may be created (using the CREATE AUDIT POLICY statement) to determine exactly which events are audited, based on numerous criteria including use of particular roles or privileges. Each record includes the date and time of the event (EVENT_TIMESTAMP), type of event (ACTION_NAME), subject identity (DBUSERNAME, if applicable), and outcome (RETURN_CODE).

The policies required to capture the auditable events detailed in Column 2 of Table 11 are generally established through the Audit policy. However, the following details should be noted:

a. For the auditing requirements of FPT_TRC.1, restoring consistency, the actions are recorded on the primary database. The secondary database is an exact replica of the primary and therefore does not include platform specific audit records; and

b. For the auditing requirements for FTA_MCS.1, rejection of a new session based on the limitation of multiple concurrent sessions, the audit record appears as a failed login. However, the error code indicates the reason for failure (SESSION_PER_USER).

All activities in Oracle Database Vault can be audited, including Database Vault administrator activities. Optionally, auditing can be established for individual policies created for realms, rule sets, and factors. The audit indicates if the user's action succeeded or if the user's action failed. These actions are written to audit logs.

All configuration changes made to Database Vault are mandatorily audited, including actions of unprivileged users who attempt to modify Database Vault policies. When a new database is installed and configured to use Oracle Database Vault, then by default it uses a combination of unified auditing and traditional auditing.

TOE Security Functional Requirements addressed: FAU_GEN.1, FAU_GEN.2, FAU_SEL.1.

7.2 USER DATA PROTECTION

7.2.1 Database Functionality

FDP_ACC.1 and FDP_ACF.1 are used to describe how database users are granted access to database objects. Database objects are defined as any object in the database that may be manipulated with SQL. This includes, but is not limited to tables, rows, columns, cases, files, and views.

Access may be granted in one of several ways:

a. An object privilege is a system-defined privilege that controls access to a specific object. A database user has access to an object if the user is the owner of the object. In this case, the user has object privileges for the object. Object privileges may be granted to other users, as well. These privileges may be limited to certain operations. For example, the owner may be able to perform any operation (e.g. read, write, etc.), but another user may have read only access to the object;

b. A system privilege may be granted to or revoked from a user by an administrator. These privileges allow users to perform specific database operations. For example, a user with the CREATE TABLE system privilege may create a table within that user's schema;

c. A role is a collection of privileges and other roles. Some system-defined roles exist, but most are created by administrators to provide the least privilege required to perform the assigned tasks. Roles group together privileges and other roles, which facilitates the granting of multiple privileges and roles to users. Roles may be granted object privileges and system privileges in much the same way that users may be granted these privileges. A user in a role would have the ability to perform actions permitted by the privileges;

d. Users may be granted access to objects based on any attribute. A policy rule must be created to allow this access. For example, in a table of human resources data, a user may be granted access to his or her own information by creating a rule that provides access to a row in a table if the database user account name matches a username field in that row; and

e. An object privilege may grant access to users in the 'PUBLIC' role. The PUBLIC role is a special role automatically provided to every database account. By default, it has no privileges assigned to it, but it is granted access to many objects. The PUBLIC role may not be granted or revoked because the user account will always assume this role. Because all database user accounts assume the PUBLIC role, it does not appear in any list of roles.

Once a resource is allocated to a table, row or other database object, the previous content of that resource is no longer available.

TOE Security Functional Requirements addressed: FDP_ACC.1(1), FDP_ACF.1(1), FDP_RIP.1.

7.2.2 Database Vault Functionality

Oracle Database Vault implements a set of components to manage security of the database instance.

These components are as follows:

- Realms. A realm is a protection zone inside the database where database schemas, objects, and roles can be secured. For example, an organization can secure a set of schemas, objects, and roles that are related to accounting, sales, or human resources. After these have been secured into a realm, the realm is used to control the use of system and object privileges to specific accounts or roles. This enables the organization to provide fine-grained access controls to schemas, objects, and roles. Oracle Database Vault provides two types of realms: regular and mandatory. A regular realm controls system privilege-based access and a mandatory realm controls both object privilege-based access and system privilege-based access. Therefore, even an object owner cannot access his or her own objects without proper realm authorization if the objects are protected by mandatory realms.
- Command rules. A command rule is a special security policy that is created to control how users can execute almost any SQL statement, database definition language (DDL), and data manipulation language (DML) statements. Command rules must work with rule sets to determine whether the statement is allowed.
- Factors. A factor is a named variable or attribute, such as a user location, database IP address, or session user, which Oracle Database Vault can recognize and use to create filtering logic. Factors can be used in rules to control activities such as authorizing database accounts to connect to the database, or the execution of a specific database command to restrict the visibility and manageability of data.
- Rule sets. A rule set is a collection of one or more rules that can be associated with a realm authorization, command rule, factor assignment, or secure application role. The rule set evaluates to true or false based on the evaluation of each rule it contains and the evaluation type (All True or Any True). The rule within a rule set is a Procedural Language Extension to Structured Query Language PL/SQL expression that evaluates to true or false.
- Database Vault roles. The Database Vault functionality provides additional roles to manage the Database Vault configuration. In the evaluated configuration, the DV_OWNER, DV_ADMIN, DV_ACCMGR, DV_SECANALYST and CAPTURE_ADMIN roles are used.

An object may be protected by regular realm, a mandatory realm, and a command rule in combination. In this case, access is only allowed if all

conditions are met. An object may be protected by a realm and a command rule in combination. In that case, access is only allowed if all conditions are met.

In order to implement the Database Vault functionality, an organization would first create multiple realms composed of selected database schemas or database objects and authorize selected users to access the resources in different ways to enforce separation of duties. The organization may create rules, rule sets and command rules to harden the security of the entire database.

Evaluation of the Database Vault access controls does not supplant evaluation of the Discretionary Access Control Policy. Users will not be permitted to access objects unless permitted by both policies.

TOE Security Functional Requirements addressed: FDP_ACC.1(2), FDP_ACF.1(2).

7.2.3 Multitenant

The Oracle Multitenant features are provided by the DB12.2 architecture. This architecture allows a multitenant container database (CDB) to hold many pluggable databases (PDBs), thereby providing a number of performance and ease-of-management benefits. Figure 8 shows a multitenant container database made up of a root database with three pluggable databases.

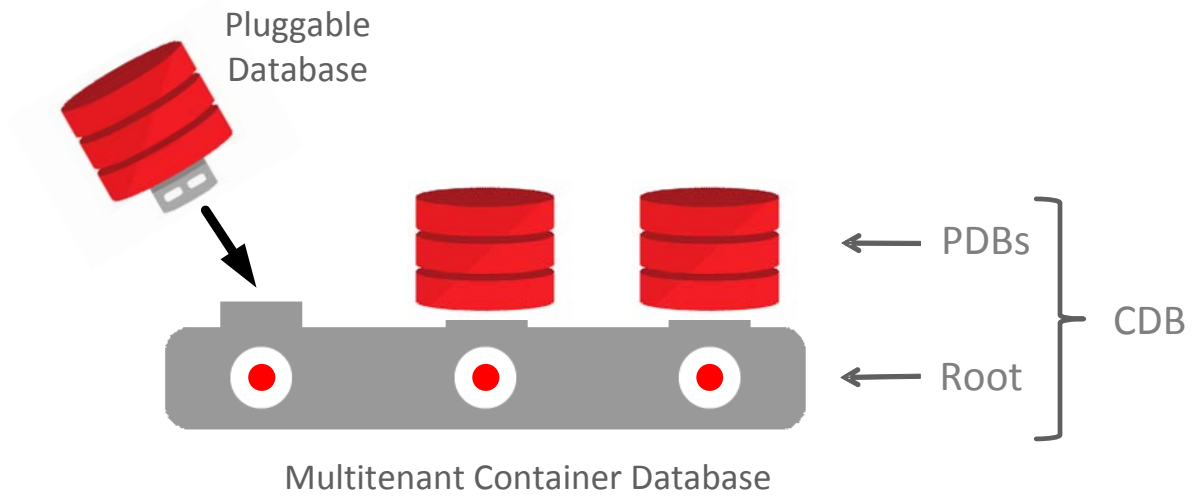

Figure 8 – Multitenant Architecture

7.2.3.1 Isolation of Resources

In order to maintain security in the multitenant architecture, isolation is provided between the resources of the pluggable databases. Database resources protected in a pluggable database are physically and logically separate and inaccessible by users in another pluggable database on the same container database. The user data is separated into self-contained pluggable databases which contain both the user tables and data.

Each PDB is self-contained with its own set of tablespaces including System, SysAux and User tablespaces, each with their own data files. In this way, at the storage level, each is physically and logically isolated from all other PDBs. Additionally, parameters can be defined to ensure that the files associated with each PDB are placed in a dedicated mount point within the underlying storage.

This architecture effectively provides the pluggable database with a data dictionary containing the definition of the user schema. The root database contains only the database application data dictionary tables, containing the application level metadata. This provides isolation of the resources in the pluggable databases. Only authorized users of a PDB, and authorized system users of the root database have access to the resources of that PDB.

TOE Security Functional Requirements addressed: FDP_ISO_(EXT).1.

7.2.3.2 Dedicated Services

Each PDB has one or more dedicated services, and a connection to the PDB must be made through one of these services.

In order to connect to a pluggable database, the user must present the listener location, the listener port, service name, username and password. The user session will only be established if the service name matches a service registered for that PDB. Services may be added to a PDB using the SRVCTL command with the parameter '-pdb' to specify the PDB for which the service is to be added.

TOE Security Functional Requirements addressed: FDP_SER_(EXT).1.

7.2.3.3 Lockdown Profiles

In the Multitenant architecture, key infrastructure and memory components are shared. Additionally, PDBs share the OS, network, and common objects. Lockdown profiles may be implemented in order to enhance isolation by preventing database users from performing cross-PDB operations. System administrators may enable or disable statements and features to achieve the required isolation between pluggable databases. The statements and features that may be disabled in the evaluated configuration are described in Table 15 and Table 16.

Statement	Description of Restrictions
ALTER DATABASE	This feature may be used to prevent users from using the ALTER DATABASE system privilege which allows users to modify, maintain or recover an existing database.
ALTER PLUGGABLE DATABASE	This feature may be used to prevent users from unplugging, modifying, modifying the state of a PDB, or multiple PDBs. It may also be used to prevent backup and recovery of a PDB.
ALTER SESSION	This feature may be used to prevent users from modifying any of the conditions or parameters that affect

Statement	Description of Restrictions
	the connection to the database.
ALTER SYSTEM	This feature may be used to prevent users from dynamically altering the Oracle Database instance.

Table 15 – Lockdown Profile Statements

Feature	Description of Restrictions
AWR_ACCESS	This feature may be used to prevent the PDB from taking manual and automatic Automatic Workload Repository (AWR) snapshots
COMMON_USER_LOCAL _SCHEMA_ACCESS	This feature may be used to prevent a common user from invoking an invoker's rights code unit or accessing a BEQUEATH CURRENT_USER view owned by any local user in the PDB
LOCAL_USER_COMMON _SCHEMA_ACCESS	Any of the following may be prevented using this feature: • A local user with an ANY system privilege (for example, CREATE ANY TABLE) creating or accessing objects in a common user's schema for which the privilege applies. • A local user with the BECOME USER system privilege becoming a common user • A local user altering a common user by issuing an ALTER USER statement • A local user using a common user for proxy connections
SECURITY_POLICIES	This feature may be used to prevent creation of certain security policies by a local user on a common object, including: • Data Redaction • Fine Grained Auditing (FGA) • Real Application Security (RAS) • Virtual Private Database (VPD)
COMMON_USER_CONNECT	This feature may be used to prevent a common user from connecting to the PDB directly. If this feature is disabled, a common user must first connect to the CDB root and then switch to the desired PDB using the ALTER SESSION SET CONTAINER statement in order to connect to the PDB.

Feature	Description of Restrictions
LOCAL_SYSOPER_RESTRICTED_MODE_CONNECT	This feature may be used to prevent a local user with the SYSOPER privilege from connecting to a PDB that is open in RESTRICTED mode.
CTX_LOGGING	This feature may be used to prevent use of logging in Oracle Text PL/SQL procedures such as CTX_OUTPUT.START_LOG and CTX_OUTPUT.START_QUERY_LOG.
JAVA	This feature may be used to prevent use of Java as a whole. If this feature is disabled, then all options and features of the database that depend on Java will be disabled.
JAVA_RUNTIME	This feature may be used to prevent use of operations through Java that require java.lang.RuntimePermission.
AQ_PROTOCOLS	This feature may be used to block use of HTTP, SMTP, and OCI notification features through Oracle Streams Advanced Queuing (AQ).
CTX_PROTOCOLS	Any of the following may be prevented using this feature: • Operations that access the Oracle Text datastore types FILE_DATASTORE and URL_DATASTORE • Printing tokens as part of CTX logging with events EVENT_INDEX_PRINT_TOKEN and EVENT_OPT_PRINT_TOKEN
DBMS_DEBUG_JDWP	This feature may be used to prevent use of the DBMS_DEBUG_JDWP PL/SQL package.
UTL_HTTP	This feature may be used to prevent PDB users from running procedures that access the network
UTL_INADDR	This feature may be used to prevent use of the UTL_INADDR PL/SQL package
UTL_SMTP	This feature may be used to prevent PDB users from running procedures that access the network
UTL_TCP	This feature may be used to prevent use of the UTL_TCP PL/SQL package
XDB_PROTOCOLS	This feature may be used to prevent use of HTTP, FTP, and other network protocols through XDB
DROP_TABLESPACE	This feature may be used to prevent the dropping of a

Feature	Description of Restrictions
_KEEP_DATAFILES	tablespace in the PDB without specifying the INCLUDING CONTENTS AND DATAFILES clause in DROP TABLESPACE statement
EXTERNAL_AND_GLOBAL _AUTHENTICATION	Any of the following may be prevented using this feature: • Creating external and global users in the PDB • Creating external and global roles in the PDB
EXTERNAL_FILE_ACCESS	This feature may be used to prevent use of external files or directory objects in the PDB when PATH_PREFIX is not set for the PDB
EXTERNAL_PROCEDURES	This feature may be used to prevent use of the external procedure agent extproc in the PDB
FILE_TRANSFER	This feature may be used to prevent use of the DBMS_FILE_TRANSFER package
JAVA_OS_ACCESS	This feature may be used to prevent use of java.io.FilePermission from Java
LOB_FILE_ACCESS	This feature may be used to prevent use of BFILE and CFILE data types
TRACE_VIEW_ACCESS	This feature may be used to prevent use of the following trace views: • [G]V$DIAG_OPT_TRACE_RECORDS • [G]V$DIAG_SQL_TRACE_RECORDS • [G]V$DIAG_TRACE_FILE_CONTENTS • V$DIAG_SESS_OPT_TRACE_RECORDS • V$DIAG_SESS_SQL_TRACE_RECORDS
UTL_FILE	This feature may be used to prevent use of UTL_FILE. If this feature is disabled, then the database blocks use of the UTL_FILE.FOPEN function.

Table 16 – Lockdown Profile Features

TOE Security Functional Requirements addressed: FDP_LDP_(EXT).1.

7.3 IDENTIFICATION AND AUTHENTICATION

To create a user, the administrator must provide a user account name and a password, and limitations on the resources available to the user. These limitations are in the form of defined tablespace and profile information. The tablespace assignment limits the number of resources available to the user and is measured in bytes. The profile associates the user with session limitations,

such as number of concurrent sessions allowed, and password parameters, such as the number of failed login attempts allowed before the account is locked.

Users are granted privileges, such as the right to run a particular type of SQL statement, or the right to access an object that belongs to another user. Roles are created to group together privileges and other roles, making it easier to grant multiple privileges to a new user. A role must first be created by identifying the role, and then adding privileges. Once the role is defined, it may be granted to a user.

In addition to granting object and system privileges to users through roles, these privileges may also be granted to users individually.

Users may be granted access to database objects based on any attribute. When configured, the policy appends a WHERE clause to queries to control access at the row and column level. This could be used to allow users to query a human resources table, but only see their own information, or only certain columns associated with the employees who report to these users. This policy (and therefore, this attribute) is not directly associated with the database user's account. Please note that these users must also have object or system privileges to access the database objects. Attributes may be used to provide a more fine-grained access control to data within accessible objects.

Oracle Database 12cR2 ensures that users are identified and authenticated prior to being allowed access to database objects or resources. Although several authentication mechanisms are supported, only local username and password authentication is examined for the purposes of this evaluation.

One database user may act with the privileges of another as a proxy user. To enable this, the user must be granted permission to access the database through a proxy. This grant operation may specify which roles (and therefore which privileges) are enabled for this access. In this way, the proxy access may be limited to a specific set of required privileges, rather than all of the primary user's privileges. This is typically used in cases where the proxy user is an application server or middle tier entity.

When a directly assigned privilege is granted or revoked, this takes effect immediately. This includes granting or revoking object privileges or system privileges, or granting or revoking object or system privileges from a role. When an indirectly assigned privilege is granted or revoked, this is effective at the next login. This includes adding or removing a role from a user account.

TOE Security Functional Requirements addressed: FIA_ATD.1, FIA_UAU.1, FIA_UID.1, FIA_USB_(EXT).2.

7.4 SECURITY MANAGEMENT

An audit policy determines which events are to be audited. The privileges required to specify this policy are only available to authorized administrators.

The access control decision for the Discretionary Access Control Policy is made based on object privileges, system privileges, roles and any attribute. All of these attributes may be managed by authorized administrators. Object

privileges and attributes may also be managed by their owners, or users to whom the owner has granted that privilege. In this case, the owner or delegated user is considered to be an authorized administrator of the object or attribute. The default values for these attributes are restrictive. System privileges, object privileges and roles must be specifically granted to users. Attribute values do not permit access until a policy granting that access has been created by an authorized administrator.

Only authorized administrators may revoke system privileges and roles. Revocation of directly assigned system privileges (i.e. system privileges granted directly to a user or a role) takes effect immediately. Revocation of a role from a user account is effective at the next login.

Authorized administrators and object owners may revoke object privileges. The ability to grant and revoke object privileges may also be granted to other users by an authorized administrator, or the object owner.

The TOE is managed by submitting SQL statements to the database using the SQL *Plus command line interface. The commands allow authorized administrators to perform all of the security management functionality required to manage the claimed security features of the TOE including:

a. management of the events to be audited;
b. changes to the system privileges;
c. changes to the object privileges;
d. changes to user accounts (including changes to authentication options) and roles;
e. configuration of Data Guard options in support of the replication requirements;
f. configuration of the maximum number of concurrent sessions for an individual user;
g. configuration of separate domains for pluggable databases within a container database;
h. creation, enabling and disabling of capture policies; and
i. generation of an analysis report from a capture result.

Database Vault administrative activities, such as create realms and create command rules are performed through designated PL/SQL procedures.

Each database requires at least one user in the database administrator role. (This role is described as ‘authorized administrator’ in the SFRs.) Other administrative roles may be created by authorized administrators with the unique set of system and object privileges required to perform assigned tasks. Database users make use of the database, but do not typically have administrative system privileges.

TOE Security Functional Requirements addressed: FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_MTD.1, FMT_REV.1(1), FMT_REV.1(2), FMT_SMF.1, FMT_SMR.1(1).

7.4.1 Privilege Analysis

A system administrator can create a capture policy to record the roles and privileges being used. The administrator then runs the capture for a determined period of time to record the privileges and roles in use. This will generate a capture report. The administrator can then analyze this report to determine which roles can be removed and which privileges can be removed or reduced. Removing excess roles and privileges reduces the attack surface available to potential threats.

TOE Security Functional Requirements addressed: FMT_PRA_(EXT).1

7.4.2 Security Roles for Database Vault

Both the DV_OWNER and DV_ADMIN roles provide the functionality to create and manage Database Vault policies. The DV_OWNER role has all the privileges of the DV_ADMIN role, such that users assigned the DV_OWNER role can perform any tasks available to users in the DV_ADMIN role. Users assigned the DV_OWNER role are also able to enable/disable Database Vault and grant or revoke Database Vault roles, with the exception of the DV_ACCTMGR role. The DV_ACCTMGR role provides functionality to manage user accounts. The DV_SECANALYST role provides privileges required to run Database Vault reports and monitor Database Vault. The CAPTURE_ADMIN role provides the privileges necessary to manage the Privilege Analysis functionality.

The users who are to be assigned the DV_OWNER and DV_ACCTMGR roles must exist prior to registration of an Oracle Database Vault instance.

TOE Security Functional Requirements addressed: FMT_SMR.1(2)

7.4.3 Security Roles for Multitenant

For a multitenant implementation, there are two types of users:

- Local Users. Local users are defined within a PDB and constrained purely to that PDB. They may not connect to any other PDB
- Common Users. Common users are defined within a Root Container (either CDB Root or an Application Root) and may be able to access one or more PDBs associated with that Root. To access a PDB associated with a Root, a common user requires either the ‘create session’ or ‘set container’ privilege in that PDB, which may be granted locally or commonly.

The Root Container may be a CDB Root or an Application Root. An Application Root is a special Pluggable Database where database Applications are installed. Developers maintain the relevant objects and data in the Pluggable Databases and may then synchronize the Application PDBs with these objects and data. There may be only one Application Root per Application Container. The

Application Container model is used by developers to create Applications, where every Application can have its own data and version, and Developers can control the version of the application within the Application Pluggable Database, and when to refresh the data.

TOE Security Functional Requirements addressed: FMT_SMR.1(3).

7.5 PROTECTION OF THE TSF

The TOE provides replication of data using the Data Guard feature. Primary database transactions generate redo records. A redo record is made up of a group of change vectors, each of which is a description of a change made to a single block in the database. For example, if a value is changed in a table, a redo record containing change vectors that describe changes to the data segment block for the table, the undo segment data block and the transaction table of the undo segments is generated. Data Guard works by shipping the redo to the replicated database and then applying that redo.

Redo records contain all the information needed to reconstruct changes made to the database. During media recovery, the database will read change vectors in the redo records and apply the changes to the relevant blocks. When configured to use the Synchronous transport method (also called the "zero data loss" method), the commit operation will not be confirmed until it is written to both the local and the remote database. If the connection between the databases is lost, updates to the primary database are halted until the secondary database is reconnected, thereby assuring consistency of the replicated data.

TOE Security Functional Requirements addressed: FPT_TRC.1.

7.6 TOE ACCESS

The TSF may restrict the maximum number of concurrent sessions for a user. This is configured using the SESSIONS_PER_USER option in the resource parameters of a profile assigned to a user. Although the default value is unlimited, in the evaluated configuration, an authorized administrator must select a finite number for this limit.

Upon user login, the date and time of the successful or unsuccessful login attempt is saved in the audit records. The audit records also maintain a count of successive unsuccessful login attempts. In order to maintain the date and time of the last successful login, the last unsuccessful login attempt and the number of unsuccessful attempts since the previous last successful login, and make that data accessible to the user, a custom query must be used. This custom SQL script is run to retrieve the required information, which may then be viewed by the user.

The TOE is able to deny session establishment based on user identity by dropping the user account.

TOE Security Functional Requirements addressed: FTA_MCS.1, FTA_TAH_(EXT).1, FTA_TSE.1.

8 TERMINOLOGY AND ACRONYMS

8.1 TERMINOLOGY

The following terminology from the DBMS PP is relevant to this ST. This table also includes terms relevant to the descriptions of Oracle Database 12c Release 2.

Term	Description
Access	Interaction between an entity and an object that results in the flow or modification of data.
Access Control	Security service that controls the use of resources[3] and the disclosure and modification of data[4].
Accountability	Property that allows activities in an IT system to be traced to the entity responsible for the activity.
Administrator	A user who has been specifically granted the authority to manage some portion or the entire TOE and whose actions may affect the TOE security policy. Administrators may possess special privileges that provide capabilities to override portions of the TOE security policy.
Assurance	A measure of confidence that the security features of an IT system are sufficient to enforce its security policy.
Attack	An intentional act attempting to violate the security policy of an IT system.
Attribute	An attribute is a property or detail associated with an object.
Authentication	Security measure that verifies a claimed identity.
Authentication data	Information used to verify a claimed identity.
Authorization	Permission, granted by an entity authorized to do so, to perform functions and access data.
Authorized Administrator	The authorized person in contact with the Target of Evaluation who is responsible for maintaining its operational capability.
Authorized user	An authenticated user who may, in accordance with the

[3] Hardware and software

[4] Stored or communicated

Term	Description
	TOE security policy, perform an operation.
Availability	Timely[5], reliable access to IT resources.
Compromise	Violation of a security policy.
Confidentiality	A security policy pertaining to the disclosure of data.
Configuration data	Data this is used in configuring the TOE.
Conformant Product	A Target of Evaluation that satisfied all the functional security requirements and satisfies all the TOE security assurance requirements.
Database Management System (DBMS)	A suite of programs that typically manage large structured sets of persistent data, offering ad hoc query facilities to many users. They are widely used in business applications.
Discretionary Access Control (DAC)	A means of restricting access to objects based on the identity of subjects and/or groups to which they belong. Those controls are discretionary in the sense that a subject with certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject.
Enclave	A collection of entities under the control of a single authority and having a homogeneous security policy. They may be logical, or may be based on physical location and proximity.
Entity	A subject, object, user or another IT device, which interacts with TOE objects, data, or resources.
Executable code within the TSF	The software that makes up the TSF which is in a form that can be run by the computer.
External IT entity	Any trusted Information Technology (IT) product or system, outside of the TOE, which may, in accordance with the TOE security policy, perform an operation.
Identity	A representation (e.g., a string) uniquely identifying an authorized user, which can either be the full or abbreviated name of that user or a pseudonym.
Integrity	A security policy pertaining to the corruption of data and TSF mechanisms.

[5] According to a defined metric

Term	Description
Named Object	An object that exhibits all of the following characteristics: • The object may be used to transfer information between subjects of differing user and/or group identities within the TSF. • Subjects in the TOE must be able to require a specific instance of the object. • The name used to refer to a specific instance of the object must exist in a context that potentially allows subjects with different user and/or group identities to require the same instance of the object.
Object	An entity within the TOE scope of control that contains or receives information and upon which subjects perform operations.
Operating Environment	The total environment in which a TOE operates. It includes the physical facility and any physical, procedural, administrative and personnel controls.
Public Object	An object for which the TSF unconditionally permits all entities “read” access. Only the TSF or authorized administrators may create, delete, or modify the public objects.
Resource	The term ‘resources’ is used to describe data resources such as database objects.
Secure State	Condition in which all TOE security policies are enforced.
Security attributes	TSF data associated with subjects, objects, and users that are used for the enforcement of the TOE security policy.
Security level	The combination of a hierarchical classification and a set of non-hierarchical categories that represent the sensitivity of the information.
Sensitive information	Information that, as determined by a competent authority, must be protected because its unauthorized disclosure, alteration, loss, or destruction will at least cause perceivable damage to someone or something.
Subject	An entity within the TOE scope of control that causes operation to be performed.
Threat	Capabilities, intentions and attack methods of

Term	Description
	adversaries, or any circumstance or event, with the potential to violate the TOE security policy.
TOE resources	Anything useable or consumable in the TOE.
Unauthorized user	A user who may obtain access only to system provided public objects if any exist.
User	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.
Vulnerability	A weakness that can be exploited to violate the TOE security policy.

Table 17 – Terminology

8.2 ACRONYMS

The following acronyms are used in this ST:

Acronym	Definition
CC	Common Criteria
CCRA	Common Criteria Recognition Agreement
CDB	Container Database
CEM	Common Methodology for Information Technology Security Evaluation
CLI	Command Line Interface
CM	Configuration Management
CPU	Critical Patch Update
DAC	Discretionary Access Control
DBMS	Database Management System
DBMS PP	Base Protection Profile for Database Management Systems
DDL	Data Definition Language
DML	Data Manipulation Language
EAL	Evaluation Assurance Level
I&A	Identification and Authentication
IP	Internet Protocol
IT	Information Technology

Acronym	Definition
OLS	Oracle Label Security
OSP	Organizational Security Policy
PDB	Pluggable Database
PL/SQL	Procedural Language Extension to Structured Query Language
PP	Protection Profile
RAC	Real Application Clusters
RDBMS	Relational Database Management System
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SQL	Structured Query Language
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
WG/TC	Working Group/Technical Community

Table 18 – Acronyms