ICS 35.040
L 80

中华人民共和国国家标准

GB/T 20273—2019
代替 GB/T 20273—2006

信息安全技术
数据库管理系统安全技术要求

Information security technology—
Security technical requirements for database management system

2019-08-30 发布　　2020-03-01 实施

国家市场监督管理总局
中国国家标准化管理委员会　发布

目　　次

前言 …… Ⅲ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语、定义和缩略语 …… 1
3.1　术语和定义 …… 1
3.2　缩略语 …… 1
4　评估对象描述 …… 2
4.1　评估对象概述 …… 2
4.2　评估对象安全特性 …… 2
4.3　评估对象部署方式说明 …… 3
5　安全问题定义 …… 3
5.1　数据资产 …… 3
5.2　威胁 …… 4
5.3　组织安全策略 …… 6
5.4　假设 …… 7
6　安全目的 …… 8
6.1　TOE 安全目的 …… 8
6.2　环境安全目的 …… 11
7　安全要求 …… 13
7.1　扩展组件定义 …… 13
7.2　安全功能要求 …… 14
7.3　安全保障要求 …… 26
8　基本原理 …… 39
8.1　安全目的基本原理 …… 39
8.2　安全要求基本原理 …… 47
8.3　组件依赖关系 …… 54
附录 A（资料性附录）　关于标准修订和使用说明 …… 57
参考文献 …… 60

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准代替 GB/T 20273—2006《信息安全技术　数据库管理系统安全技术要求》，与 GB/T 20273—2006 相比主要技术变化如下：

——修改了“术语和定义”，增加了“缩略语”中的内容（见 3.1 和 3.2，2006 年版的 3.1）；

——增加了安全问题定义、安全目的、扩展组件定义、基本原理（见第 5 章、第 6 章、第 7 章、第 8 章）；

——修改了评估对象描述（见第 4 章，2006 年版的第 4 章）；

——删除了“安全审计”安全功能中提供“潜在侵害分析”“基于异常检测”和“简单攻击探测”的要求（见 2006 年版的第 5 章）；

——删除了“SSODB 自身安全保护”安全功能中提供“SSF 物理安全保护”的要求（见 2006 年版的第 5 章）；

——删除了“SSF 运行安全保护”安全功能中关于与“不可旁路性”“域分离”和“可信恢复”相关的要求（见 2006 年版的第 5 章）；

——删除了安全功能中提供“推理控制”的要求（见 2006 年版的第 5 章）；

——增加了附录 A 关于标准修订和使用说明。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由全国信息安全标准化技术委员会（SAC/TC 260）提出并归口。

本标准起草单位：中国信息安全测评中心、清华大学、北京江南天安科技有限公司、公安部第三研究所、北京大学、武汉达梦数据库有限公司、天津南大通用数据技术股份有限公司。

本标准主要起草人：张宝峰、毕海英、叶晓俊、王峰、王建民、陈冠直、陆臻、沈亮、顾健、宋好好、赵玉洁、吉增瑞、刘昱函、刘学洋、胡文蕙、付铨、方红霞、冯源、李德军。

本标准所代替标准的历次版本发布情况为：

——GB/T 20273—2006。

信息安全技术
数据库管理系统安全技术要求

1 范围

本标准规定了数据库管理系统评估对象描述，不同评估保障级的数据库管理系统安全问题定义、安全目的和安全要求，安全问题定义与安全目的、安全目的与安全要求之间的基本原理。

本标准适用于数据库管理系统的测试、评估和采购，也可用于指导数据库管理系统的研发。

注：本标准规定的 EAL2、EAL3、EAL4 级的安全要求既适用于基于 GB/T 18336.1—2015、GB/T 18336.2—2015 和 GB/T 18336.3—2015 的数据库管理系统安全性测评，同样适用于基于 GB 17859—1999 的数据库第二级系统审计保护级、第三级安全标记保护级、第四级结构化保护级的数据库安全性测评，相关对应关系参见附录 A 的 A.1。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB/T 18336.1—2015 信息技术 安全技术 信息技术安全评估准则 第 1 部分：简介和一般模型

GB/T 18336.2—2015 信息技术 安全技术 信息技术安全评估准则 第 2 部分：安全功能组件

GB/T 18336.3—2015 信息技术 安全技术 信息技术安全评估准则 第 3 部分：安全保障组件

GB/T 25069—2010 信息安全技术 术语

GB/T 28821—2012 关系数据管理系统技术要求

3 术语、定义和缩略语

3.1 术语和定义

GB/T 25069—2010、GB/T 18336.1—2015 和 GB/T 28821—2012 界定的术语和定义适用于本文件。

3.2 缩略语

下列缩略语适用于本文件。

ACID：原子性、隔离性、一致性和持久性

CM：配置管理(Configuration Management)

DBMS：数据库管理系统(DataBase Management System)

EAL：评估保障级(Evaluation Assurance Level)

IT：信息技术(Information Technology)

JDBC：JAVA 数据库连接(Java DataBase Connectivity)

LBAC：基于标签的访问控制(Label Based Access Control)

ODBC：开放数据库连接(Open DataBase Connectivity)

PP：保护轮廓(Protection Profile)

RDBMS:关系数据库管理系统(Relational DataBase Management System)
SFP:安全功能策略(Security Function Policy)
SFR:安全功能要求(Security Functional Requirements)
SQL:结构化查询语言(Structured Query Language)
ST:安全目标(Security Target)
TOE:评估对象(Target Of Evaluation)
TSF:TOE 安全功能(TOE Security Functionality)
TSFI:TSF 接口(TSF Interface)
TSP:TOE 安全策略(TOE Security Policy)

4 评估对象描述

4.1 评估对象概述

本标准评估对象(TOE)是指数据库管理系统(DBMS)所包含的管理软件及其管理的数据库对象。

DBMS 所包含的管理软件应提供数据库语言对数据库对象进行定义、操作和管理;提供数据库控制语言,通过数据模型语义约束条件维护 DBMS 运行的数据完整性;提供数据库备份、还原与恢复机制,保证 DBMS 运行中出现故障时的数据库可用性。关系数据库管理系统(RDBMS)应提供事务管理机制,保证多用户数据库并发操作时事务的原子性、隔离性、一致性和持久性(ACID)。

DBMS 主要包括以下组成部分:

a) 数据库:存放用户数据和 TOE 安全功能(TSF)数据的数据文件、存放数据库事务处理过程的日志文件、维护 DBMS 运行完整性控制文件等物理文件组成。存储的数据库对象包括模式对象、非模式对象、数据库字典对象等。
b) 数据库实例:包括查询引擎、事务管理器、数据存储管理器等部件。实现对数据库对象的定义、管理、查询、更新、控制等基本功能。
c) 数据库语言及其访问接口:提供结构化查询语言(SQL)、开放数据库连接(ODBC)、JAVA 数据库连接(JDBC)等数据库语言和数据库开发接口规范,允许授权用户通过数据库开发接口定义数据库结构、访问和修改数据库对象数据、展现 DBMS 运行相关配置参数,以及对用户数据和 DBMS 运行相关数据执行各种维护操作。
d) DBMS 运行维护辅助工具:提供数据库实例的启动与关闭,数据库或数据文件的联机、脱机、打开与关闭,数据库检查点控制,数据库日志归档、外部数据导入等 DBMS 运行维护辅助工具或接口。

4.2 评估对象安全特性

DBMS 提供通过多种安全控制措施保证其管理数据资产安全。TOE 安全特性可由 DBMS 本身直接提供,也可通过 DBMS 运行的信息技术(IT)环境间接支持。

DBMS 安全特性主要包括:

a) 用户认证:用户标识只有通过身份鉴别后才能通过 TOE 的访问控制引擎控制授权用户对数据库对象的访问和操作。
b) 用户授权:每个授权用户有一组数据库安全域特性,可决定用户下列安全域特性内容:可用特权和授权角色、可用存储空间(如表空间)限额、可用系统资源(如共享缓存、数据读写容量、处理器使用)限制等安全属性。
c) 角色管理:提供安全管理员、安全审计员、数据库管理员等缺省的数据库角色。授权管理员也可以面向授权用户配置其访问控制策略、定义用户标识与鉴别方式、设置数据库审计策略等数

据库安全管理功能。

d) 访问控制：在确认授权用户与授权管理员身份以及他们安全域特性基础上，TSF 实施授权用户与授权管理员的授权策略，控制主体访问客体活动。例如：自主访问控制、基于角色的访问控制、基于标签的访问控制等。

e) 安全审计：提供与 TSF 相关的数据库操作是否被记录到数据库审计文件的机制。审计踪迹记录可以存储在 DBMS 审计表或外部 IT 环境的系统文件中。TSF 应提供审计记录的安全保护。

f) 备份恢复：DBMS 运行出现故障后，利用 TSF 数据库备份与恢复机制实现对备份数据的还原，在数据库还原的基础上利用数据库日志进行数据库恢复，重新建立一个完整的数据库。

g) 数据加密：提供对数据库中的数据进行加密存储、传输或处理，以及密钥管理服务接口功能，从而保证用户数据的保密性。

h) 资源限制：防止授权用户无控制地使用主机处理器(CPU)、共享缓存、数据库存储介质等数据库服务器资源，限制每个授权用户/授权管理员的并行会话数等功能。

注：DBMS 软件及其管理数据资产的安全性不是孤立的。在生产环境下，操作系统、网络系统与硬件等 DBMS 运行 IT 环境和 DBMS 一起共同构筑起 TOE 的安全体系。安全目标(ST)作者在描述 TOE 时明确说明和标识评估 DBMS 的体系结构与这些 IT 环境各个组件之间的相互关系。

4.3 评估对象部署方式说明

DBMS 的任何内部和外部实体若要获取 TOE 管理的数据资产，应首先满足与 TOE 及运行环境相应的安全策略。TOE 运行环境对象可能包括多个安全控制组件，涉及设备物理安全、环境物理安全、系统物理安全、人员安全管理等多种安全策略。这些运行环境安全策略使 DBMS 软件及其管理的数据库免受 DBMS 运行环境中的安全威胁。

本标准可用来评估多种部署结构的 DBMS 安全性，包括但不限于下列体系结构：

a) 集中式体系结构：DBMS 软件和数据库应用程序都安装运行在一个主机上，用户只能通过应用终端发出存取数据库访问请求或管理命令，由通信线路传输给主机，主机上的数据库实例响应并处理后，再将处理结果通过通信线路返回给用户终端。

b) 客户/服务器体系结构：客户端数据库应用和服务器端数据库实例通过网络连接进行通信，客户端发送数据库访问请求或管理命令，展示数据库实例返回的数据，服务器端安全地执行用户数据库访问请求或管理命令。前端应用可以是基于浏览器实现，通过远程 Web 服务器或应用服务器实现与数据库服务器的连接，由远程服务器负责与数据库服务器交互。

c) 分布式数据库体系结构：数据节点分别保存在多个物理上相互独立的站点数据库服务器上，这些站点之间的数据库服务器通过网络连接，协同提供分布式数据库数据访问服务。用户可以对本地服务器中的数据节点执行某些数据库访问请求或管理命令(局部应用)，也可以对其他站点上的数据节点执行某些数据库访问请求或管理命令(全局应用或分布应用)。

注：本标准定义了一个必要的数据库管理员角色(授权管理员)，并允许 ST 作者定义更多的授权管理员角色。当然对某些 DBMS，提供的管理角色数量和角色责任的能力，以及这些角色的分配能力在 TOE 实现中都预先存在。TSF 提供这些系统权限或角色建立、分配、撤销等授权管理功能。

5 安全问题定义

5.1 数据资产

DBMS 需要保护的数据资产包括：

a) TSF 数据：存储在 TOE 中数据库字典数据，面向数据库应用的数据库对象定义数据、DBMS

运行统计数据、数据库逻辑存储与物理存储管理数据等。

b) 用户数据：存储在 TOE 中的非 TSF 数据的数据，一般指与用户数据库应用相关的、存储在数据库中的各种数据库对象数据，如表数据、索引数据、物化视图数据、语义约束条件、业务过程等来自用户数据库应用程序的数据。

c) 安全运行数据：TOE 中的事务日志数据、安全审计数据等，包括存储在 DBMS 外部，但由 DBMS 维护的数据库实例、数据库配置等控制 TOE 安全运行相关参数配置数据。

5.2 威胁

5.2.1 概述

TOE 面临过度或合法的特权滥用、软件漏洞被利用和潜在应用安全攻击（如 SQL 注入、拒绝服务、特权提升等）等安全威胁。表 1 给出了 DBMS 评估保障级（EAL）2、3 和 4 面临的不同威胁。

表 1 评估对象威胁

序号	威胁	评估保障级		
		EAL2	EAL3	EAL4
T.1	管理员误操作 T.MISOPERATION_ADMIN	√	√	√
T.2	审计机制失效 T.AUDIT_FAILURE	√	√	√
T.3	密码攻击 T.CRYPTO_COMPROMISE	—	√	√
T.4	数据传输窃听 T.EAVESDROP	—	√	√
T.5	设计缺陷 T.FLAWED_DESIGN	—	√	√
T.6	实现缺陷 T.FLAWED_IMPLEMENTATION	—	√	√
T.7	标签数据失控 T.LBAC	—	—	√
T.8	假冒授权用户 T.MASQUERADE	√	√	√
T.9	测试缺陷 T.POOR_TEST	√	√	√
T.10	残余信息利用 T.RESIDUAL_DATA	—	√	√
T.11	安全功能失效 T.TSF_COMPROMISE	—	√	√
T.12	非授权访问 T.UNAUTHORIZED_ACCESS	√	√	√
T.13	服务失效 T.UNAVAILABILITY	√	√	√
T.14	未标识动作 T.UNIDENTIFIED_ACTIONS	—	√	√

注：√ 代表在该评估保障级下 DBMS 面临的威胁。
— 代表在该评估保障级下无需考虑的威胁。

5.2.2 管理员误操作（T.MISOPERATION_ADMIN）

管理员误操作主要有两种：一是授权管理员可能错误地安装或配置数据库实例组件或错误地设置数据库实例运行参数或数据库安全属性所造成 TSF 安全控制机制的失效；二是授权管理员恶意修改、删除 TSF 数据或安全运行数据导致 TSF 安全控制机制的失效。

5.2.3 审计机制失效（T.AUDIT_FAILURE）

恶意用户或进程可能修改安全审计策略，使数据库审计功能停用或失效、审计记录丢失或被篡改，

也有可能通过审计数据存储失效来阻止未来审计记录被存储，从而掩盖用户的数据库操作。

5.2.4 密码攻击(T.CRYPTO_COMPROMISE)

恶意用户或进程可能导致与数据库存储和通信加密功能相关的密钥、数据或密文服务组件可执行代码被不适当地浏览、修改或删除，从而破坏数据库加密机制和泄露加密机制所保护的数据。

5.2.5 数据传输窃听(T.EAVESDROP)

恶意用户或进程可能观察或修改 TOE 物理分离部件之间传递的用户数据或 TSF 数据(包括客户端和服务器之间用户请求及其响应、分布式数据库不同节点间传输数据等)。

5.2.6 设计缺陷(T.FLAWED_DESIGN)

TOE 需求规范或设计中的无意逻辑错误可能产生设计弱点或缺陷，恶意用户可能利用这些缺陷对 TOE 进行安全攻击。

5.2.7 实现缺陷(T.FLAWED_IMPLEMENTATION)

在 TOE 开发过程中的无意错误可能造成 TOE 实现弱点或缺陷，恶意用户可能利用这些未知漏洞对 TOE 进行攻击。

5.2.8 标签数据失控(T.LBAC)

恶意用户或进程可能非法浏览、修改或删除 TOE 的标签策略数据、受控主体分类标签数据与受控客体绑定标签数据。授权管理员非法访问基于标签管理的受控主体的数据资产。

5.2.9 假冒授权用户(T.MASQUERADE)

恶意用户或进程假冒授权管理员或授权用户访问数据库字典、系统安全配置参数、或 DBMS 保护的数据资产。

5.2.10 测试缺陷(T.POOR_TEST)

开发或测试人员对 TOE(包括数据库安全选件及其支撑环境)的测试不充分，导致 TOE 弱点(逻辑错误)未被发现，恶意用户可能利用这些未知漏洞对 TOE 进行攻击。

5.2.11 残余信息利用(T.RESIDUAL_DATA)

恶意用户或进程可能利用数据库实例共享缓存或磁盘上残留信息的处理缺陷，在数据库实例执行过程中对未删除的残留信息进行利用，以获取敏感信息或滥用 TOE 的安全功能。

5.2.12 安全功能失效(T.TSF_COMPROMISE)

恶意用户或进程通过安全攻击非法地浏览、修改或删除 TSF 数据或可执行代码。这可能让恶意用户或进程获得数据库实例和数据库的配置信息，或可能导致数据库实例的安全功能对于数据资产保护的安全机制不再正常工作。

5.2.13 未授权访问(T.UNAUTHORIZED_ACCESS)

恶意用户或进程可能未经授权地访问 TOE 和利用系统特权提升等方法来访问 TOE 的安全功能和数据，不适当地更改数据库实例和数据库配置数据及其安全功能机制。

5.2.14 服务失效(T.UNAVAILABILITY)

恶意用户或进程可能通过数据库服务器资源(CPU、RAM)的拒绝服务攻击来阻止其他用户获得TOE管理的数据资源,数据库实例核心功能/组件的故障可能会导致用户不能访问数据库,或TOE可能由合法授权用户的高并发服务请求,预防或延缓TSF被其他授权用户访问。

5.2.15 未标识动作(T.UNIDENTIFIED_ACTIONS)

存在授权管理员不能标识的TOE中可能发生的数据库用户的非授权操作,包括提供采取必要行动以应对这些潜在未被授权访问操作的安全问责管理。

5.3 组织安全策略

5.3.1 概述

组织安全策略需要由DBMS或其IT运行环境或由两者一起实施。表2给出了DBMS评估保障级(EAL)2、3和4的组织安全策略。

表2 评估对象组织安全策略

序号	组织安全策略	评估保障级		
		EAL2	EAL3	EAL4
P.1	责任与义务 P.ACCOUNTABILITY	√	√	√
P.2	密码策略 P.CRYPTOGRAPHY	—	√	√
P.3	标签策略 P.LABEL	—		√
P.4	角色分离策略 P.ROLES	√	√	√
P.5	系统完整性 P.SYSTEM_INTEGRITY	—	√	√
P.6	脆弱性分析与测试 P.VULNERABILITY_ANALYSIS_TEST	—	—	√
注:√ 代表在该评估保障级下包括的组织安全策略。 — 代表在该评估保障级下未包括的组织安全策略。				

5.3.2 责任与义务(P.ACCOUNTABILITY)

组织应制定TOE的授权用户和授权管理员在应对DBMS中的数据库操作行为负责的程序与规范。

5.3.3 密码策略(P.CRYPTOGRAPHY)

组织应为TOE自身的应用提供数据加密存储和通信的密码策略,包括加密/解密和数字签名操作规范(ST作者提供的密码策略需符合国家、行业要求的相关标准,如是自己提供的密码算法(方法和实现),需提供用于密钥管理和密码服务的保障性证据。

5.3.4 标签策略(P.LABEL)

组织应定义适合细粒度访问控制机制的标签策略,包括安全分级数组、范围集合、或分组树等标签组成元素,并定义数据安全分级管理的数据标签和用户安全级别分类的用户标签。授权管理员应能正确地将标签与授权用户和存储在数据库表中的客体相关联。

5.3.5 角色分离策略(P.ROLES)

组织应为其 TOE 的不同级别、不同粒度的安全管理设置适当的授权管理员角色。授权管理员角色应提供诸如三权分立或其他授权角色区别和分离策略。

5.3.6 系统完整性(P.SYSTEM_INTEGRITY)

组织应提供能够定期验证其组织安全策略及其 IT 运行环境正确操作规范,并在授权管理员的帮助下能够提供数据库进程恢复、数据库实例恢复和数据库介质恢复等方法与技术,包括修正任何被检测到的错误操作修复指南(ST 作者提供 TOE 运行设施需提供的不可抵赖性安全元数据传输服务,包括生成和验证不可抵赖性的证据,证据的时间戳等 DBMS 运行完整性机制)。

5.3.7 脆弱性分析与测试(P.VULNERABILITY_ANALYSIS_TEST)

组织应保证 TOE 经过适当的渗透性测试和脆弱性分析,以证明其 TSF 组件实现的安全性。

5.4 假设

5.4.1 概述

依据 DBMS 的安全目的不断识别出更多的假设,ST 作者扩充表 3 列出的 DBMS 评估保障级(EAL)2、3 和 4 级的假设。

表 3 评估对象假设

序号	假设	评估保障级		
		EAL2	EAL3	EAL4
A.1	目录服务器保护 A.DIR_PROTECTION	—	—	√
A.2	安全域分离 A.DOMAIN_SEPARATION	—	√	√
A.3	角色分工管理 A.MANAGER	√	√	√
A.4	多层应用问责 A.MIDTIER	—	—	√
A.5	人员假设 A.NO_HARM	√	√	√
A.6	服务器专用 A.NO_GENERAL_PURPOSE	√	√	√
A.7	物理安全 A.PHYSICAL	√	√	√
A.8	通信安全 A.SECURE_COMMS	—	√	√

注:√ 代表在该评估保障级下包括的假设。
— 代表在该评估保障级下未包括的假设。

5.4.2 目录服务器保护(A.DIR_PROTECTION)

TOE 所使用的目录服务器(如 LDAP)能防御针对存储在目录中的 TSF 数据的非授权访问,包括存储在目录中的 TSF 数据被管理人员合理地使用,并且目录服务器及其网络连接从物理和逻辑上都免于非授权人员的访问和干扰。

5.4.3 安全域分离(A.DOMAIN_SEPARATION)

分布式数据库不同节点安全域之间传输的数据应通过各节点的 TSF 控制,DBMS 运行 IT 环境将

为 TOE 的分布式部署提供独立安全域，IT 环境应确保无法绕过 TSF 以获得对 TOE 数据的访问。

5.4.4 角色分工管理(A.MANAGER)

假定在 TOE 中将有一个或多个指定角色权限的授权管理员，他们之间依据最小特权、职责分离、深度防御等安全原则进行了角色分工(ST 作者需根据 DBMS 支持的系统权限及针对的具体应用解决方案解释“安全角色”的具体含义)。

5.4.5 多层应用问责(A.MIDTIER)

在多层应用环境中为了确保 TOE 的安全问责制，任意中间层次的 TOE 运行环境组件服务都应将原始的授权用户标识发送给 TSF(ST 作者应根据 DBMS 针对的具体应用解决方案解释“多层应用问责”的具体含义)。

5.4.6 管理员假设(A.NO_HARM)

使用数据库的授权用户和授权管理员具备基本的数据库安全防护知识并具有良好的使用习惯，他们训练有素且遵循 TOE 的管理员指南，并且以安全的方式使用数据库。

5.4.7 服务器专用(A.NO_GENERAL_PURPOSE)

在 DBMS 运行主机上没有安装其他获得通用的计算或存储能力的程序或服务(例如：编译器、编辑器或应用程序)。

5.4.8 物理安全(A.PHYSICAL)

DBMS 运行环境应提供与其所管理的数据价值相一致的物理安全。例如存储在数据库之外的 TOE 相关数据(如配置参数、归档日志等)以一种安全的方式存储和管理。

5.4.9 通信安全(A.SECURE_COMMS)

假定数据库服务器和应用终端之间、分布式数据库不同节点间的通信信道是安全可靠的(如满足私密性和完整性)。实现方式可通过共享密钥、公/私钥对，或者利用存储的其他密钥来产生会话密钥。

6 安全目的

6.1 TOE 安全目的

6.1.1 概述

本标准定义的安全目的可明确追溯到 TOE 相关威胁或组织安全策略。表 4 列出了 DBMS 评估保障级(EAL)2、3 和 4 的 TOE 安全目的。

表 4 评估对象的 TOE 安全目的

序号	TOE 安全目的	评估保障级		
		EAL2	EAL3	EAL4
O.1	访问历史 O.ACCESS_HISTORY	√	√	√
O.2	标签访问 O.ACCESS_LBAC	—	—	√
O.3	管理员指南 O.ADMIN_GUIDANCE	√	√	√

表 4（续）

序号	TOE 安全目的	评估保障级		
		EAL2	EAL3	EAL4
O.4	管理角色分离 O.ADMIN_ROLE	√	√	√
O.5	审计数据产生 O.AUDIT_GENERATION	√	√	√
O.6	审计数据保护 O.AUDIT_PROTECTION	√	√	√
O.7	数据库服务可用 O.AVAIL	√	√	√
O.8	配置标识 O.CONFIG	√	√	√
O.9	密码安全 O.CRYPTOGRAGHY	—	√	√
O.10	设计文档化 O.DOCUMENTED_DESIGN	√	√	√
O.11	功能测试 O.FUNCTIONAL_TEST	√	√	√
O.12	内部安全域 O.INTERNAL_TOE_DOMAINS	√	√	√
O.13	安全管理员 O.MANAGE	√	√	√
O.14	残留信息 O.RESIDUAL_INFORMATION	√	√	√
O.15	资源共享 O.RESOURCE_SHARING	—	√	√
O.16	TOE 访问控制 O.TOE_ACCESS	√	√	√
O.17	可信路径 O.TRUSTED_PATH	—	√	√
O.18	漏洞分析 O.VULNERABILITY_ANALYSIS	—	—	√
注：√ 代表在该评估保障级下包括的安全目的。 — 代表在该评估保障级下未包括的安全目的。				

6.1.2 访问历史（O.ACCESS_HISTORY）

TOE 应具备存储和检索授权用户和授权管理员先前连接数据库实例的会话信息，包括尝试建立数据库连接/会话的相关请求历史数据。

6.1.3 标签访问（O.ACCESS_LBAC）

TOE 应提供安全标签的数据分级、用户分类与分组的读/写权限安全策略设置，提供基于标签的访问控制机制，从而通过 DBMS 标签机制实现集中式或细粒度的数据访问控制。

6.1.4 管理员指南（O.ADMIN_GUIDANCE）

TOE 应为授权管理员提供 DBMS 产品安全分发、安装配置和运行管理必要的管理指南信息，应为授权用户提供数据库对象创建和使用相关的用户操作手册文档（ST 作者应依据其 TOE 的安全机制，解释预配置的数据库管理员角色，以实现职责分离的授权管理）。

6.1.5 管理角色分离（O.ADMIN_ROLE）

TOE 应提供与不同数据库管理操作相适应的授权管理员角色，以提供职责分离、角色约束等角色管理功能，并且这些管理功能可以在本地或以远程方式进行安全管理（ST 作者应依据其 TOE 的安全机制，解释预配置的数据库管理员角色，以实现职责分离的授权管理）。

6.1.6 审计数据产生(O.AUDIT_GENERATION)

TOE 应提供数据库审计策略定义、审计功能启停管理、数据库管理操作、用户数据库对象操作等检测和创建与用户关联的安全相关事件的记录能力(ST 作者应依据 TOE 的审计记录的组成和存储机制,说明审计数据保存方式(数据库内部、数据库外部),以及审计数据安全管理机制)。

6.1.7 审计数据保护(O.AUDIT_PROTECTION)

TOE 应安全存储审计数据,并对存储的审计事件进行保护能力。

6.1.8 数据库服务可用(O.AVAIL)

TOE 应提供事务、数据库实例和存储介质故障的数据恢复机制,提供 DBMS 升级中数据库存储结构的自动维护能力,保证 TOE 管理数据资产的可恢复性。

TOE 应提供主数据库服务器与备用服务器 TSF 控制转移和数据库实例故障切换机制,以支持分布式数据库服务高可用管理需求的分布式组件部署。

6.1.9 配置标识(O.CONFIG)

TOE 应对产品组件配置及其文档的评估配置项进行标识,以便 DBMS 被重新分发和纠正执行错误时提供修改和跟踪他们的方法。

注:配置标识一般是指在 TOE 组装与系统测试阶段结束时,交付给外部顾客的发行基线,它包括软件产品的全部配置项的规格说明。

6.1.10 密码安全(O.CRYPTOGRAGHY)

TOE 应提供密钥管理和密码运算功能的调用机制,以维护 TOE 中数据资产在存储和传输过程中的加密保护需求(ST 编制中 TOE 使用的密码算法应符合国家、行业或组织要求的密码管理相关标准或规范)。

6.1.11 设计文档化(O.DOCUMENTED_DESIGN)

TOE 的设计、实现等软件研发工作应被充分、准确地文档化,包括在设计及其在研发过程中的所有变更证据都应被分析、追踪和控制。这些过程性设计与开发文档应贯穿于 TOE 的整个开发过程。

6.1.12 功能测试(O.FUNCTIONAL_TEST)

TOE 应进行合适的安全功能测试以证明 DBMS 的 TSF 满足安全功能设计要求。

6.1.13 内部安全域(O.INTERNAL_TOE_DOMAINS)

在多用户并发事务执行过程中,数据库查询引擎中的 TSF 应为不同并发用户请求维护一个私有的数据查询和数据处理安全域,保证多用户并发访问数据的隔离性和一致性。

6.1.14 安全管理员(O.MANAGE)

TOE 应提供系统管理、安全管理、安全审计等安全管理员角色管理 DBMS 安全性所必需的功能和设施,并防止这些管理功能和管理设施被未授权用户使用。

6.1.15 残留信息(O.RESIDUAL_INFORMATION)

TOE 应确保数据库服务器共享缓存、磁盘存储等服务器资源中重要的数据在使用完成或意外掉电

后会被删除或被安全处理，从而保证不会留下可被攻击者利用的残留数据信息。

6.1.16 资源共享(O.RESOURCE_SHARING)

TOE 应提供数据库服务器资源(即共享缓存、CPU 使用、存储空间等共享资源)使用的控制机制，以避免耗尽数据库服务器资源的安全威胁。

6.1.17 TOE 访问控制(O.TOE_ACCESS)

TOE 应对在数据字典数据、用户数据、运行日志数据和数据库安全功能组件实施访问控制措施，防止在未授权情况下被访问、修改或删除。

6.1.18 可信路径(O.TRUSTED_PATH)

TOE 应提供方法保证用户提供标识和授权数据时，与其通信的不是伪装成 DBMS 的其他 IT 实体。例如针对用户/程序与数据库服务器之间的通信，TOE 提供合适的数据加密传输控制机制，保护数据库实例运行过程中与外部用户/程序交换的数据库通信安全。

6.1.19 漏洞分析(O.VULNERABILITY_ANALYSIS)

TOE 应进行合适的独立渗透性测试和脆弱性分析以证明其设计和实现不存在安全弱点或缺陷，能阻止违反数据库安全策略的数据库攻击行为。

6.2 环境安全目的

6.2.1 概述

表 5 列出了 DBMS 评估保障级(EAL)2、3 和 4 的运行环境安全目的。

表 5 评估对象运行环境安全目的

序号	环境安全目的	评估保障级		
		EAL2	EAL3	EAL4
OE.1	运行环境安全审计保护 OE.AUDIT_PROTECTION	√	√	√
OE.2	运行环境审计信息查看 OE.AUDIT_REVIEW	√	√	√
OE.3	运行环境管理 OE.CONFIG	—	√	√
OE.4	目录访问控制保护 OE.DIR_CONTROL	—	—	√
OE.5	IT 域分离 OE.DOMAIN_SEPARATION	—	√	√
OE.6	管理员诚信 OE.NO_HARM	√	√	√
OE.7	数据库服务器专用 OE.NO_GENERAL_PURPOSE	√	√	√
OE.8	物理安全一致性 OE.PHYSICAL	√	√	√
OE.9	通信安全环境 OE.SECURE_COMMS	—	√	√
OE.10	IT 环境自我保护 OE.SELF_PROTECTION	—	√	√
OE.11	IT 时间戳 OE.TIME_STAMPS	√	√	√
OE.12	IT 环境访问控制 OE.TOE_ACCESS	√	√	√
OE.13	IT 环境无旁路 OE.TOE_NO_BYPASS	√	√	√
OE.14	可信 IT 环境 OE.TRUST_IT	—	√	√
注：√ 代表在该评估保障级下包括的环境安全目的。 — 代表在该评估保障级下未包括的环境安全目的。				

6.2.2 运行环境安全审计保护(OE.AUDIT_PROTECTION)

TOE 运行环境应提供保护数据库安全审计信息和用户鉴别证书的能力。数据库服务器应维护一个保护自身及其审计痕迹资源免受外部干扰、破坏或通过自身接口未授权泄漏的执行域。

6.2.3 运行环境审计信息查看(OE.AUDIT_REVIEW)

TOE 运行环境应提供选择性查看 DBMS 与运行环境安全审计信息的能力。

6.2.4 运行环境管理(OE.CONFIG)

TOE 运行环境应具备数据库管理员组或角色,提供管理与配置 DBMS 运行安全所需的功能和设施,并防止这些功能和设施被未授权使用。

6.2.5 目录访问控制保护(OE.DIR_CONTROL)

支持目录服务(如 LDAP 服务器)的 DBMS 运行环境应提供用户标识、身份验证、访问控制等机制,以阻止非法用户访问目录服务保存的 TSF 数据。目录服务的访问控制机制应提供 TSF 控制数据的导入/导出的安全保护措施。

6.2.6 IT 域分离(OE.DOMAIN_SEPARATION)

分布式部署 TOE 的运行环境应为 TOE 运行节点提供一个可分离的安全执行域,不同 DBMS 节点间应以一种安全方式进行通信。

6.2.7 管理员诚信(OE.NO_HARM)

使用 TOE 的组织应保证其授权管理员是可信的,训练有素且遵循组织安全策略和相关的数据库管理员使用指南。

6.2.8 数据库服务器专用(OE.NO_GENERAL_PURPOSE)

数据库服务器除了提供 TOE 运行、管理和支持的必要服务组件外,不存在与数据库实例运行无关的计算或存储功能组件(如编译器、编辑器或应用程序)。

6.2.9 物理安全一致性(OE.PHYSICAL)

TOE 运行环境应提供与 DBMS 及其管理数据资产价值相一致的物理安全。

6.2.10 通信安全环境(OE.SECURE_COMMS)

TOE 运行环境应在远程用户/程序和数据库服务器之间提供安全的通信线路。

6.2.11 IT 环境自我保护(OE.SELF_PROTECTION)

TOE 运行环境应维护一个保护 DBMS 及其运行环境资源免受外部干扰、破坏或未授权泄漏的执行域。

6.2.12 IT 时间戳(OE.TIME_STAMPS)

TOE 运行环境应为 DBMS 提供可靠的时间戳。

6.2.13 IT 环境访问控制(OE.TOE_ACCESS)

TOE 运行环境应提供有助于 DBMS 控制其运行环境用户对 TOE 进行逻辑访问的机制。

6.2.14 IT 环境无旁路(OE.TOE_NO_BYPASS)

DBMS 客户端与数据库服务器或多数据库服务器主机(分布式数据库)之间传输的数据应通过 TOE 的安全控制引擎来实现。

6.2.15 可信 IT 环境(OE.TRUST_IT)

TOE 运行所依赖的 IT 环境实体应正确地安装、配置、管理和维护,并与 DBMS 安全策略和 IT 环境安全策略之间的关系保持一致性。

7 安全要求

7.1 扩展组件定义

7.1.1 概述

表 6 列出了本标准中基于 GB/T 18336.2—2015 安全功能要求扩展组件的基本原理,扩展组件在 GB/T 18336.2—2015 标准组件名称后加上"_EXT"表示。在组件元素描述中,方括号【】中的宋体加粗字内容表示已经完成的操作,粗斜体字内容表示还需在安全目标中由 ST 作者确定赋值及选择项。

表 6 扩展组件的基本原理

序号	组件名称	基本原理
1	FMT_MSA_EXT.1 安全属性的管理	DBMS 一般提供多种访问控制机制,其中最主要的是自主访问控制和标签机制,这两种机制的属性管理权限不同,需从这两个角度对 TOE 安全属性管理给出相应的要求
2	FMT_MTD_EXT.1TSF 数据的管理	本标准对 TSF 数据细化为系统权限、实例权限、数据库权限、对象权限和数据权限,授权管理员细化为系统管理员、安全管理员和安全审计员。组件元素由 GB/T 18336.2—2015 一个增加到 5 个
3	FMT_MSA_EXT.3 静态属性初始化	GB/T 18336.2—2015 并不允许 PP/ST 编制者指定不可修改的限制值,因此本标准从组件 FMT_MSA_EXT.3 中取消了元素 FMT_MSA_EXT.3.2,而且通过要求对象的安全属性在创建时受到限制使得这个组件更加安全,而且并不允许用户能够覆盖这个限制的默认值
4	FPT_OVR_EXT.1TSF 故障切换/转移	在 GB/T 18336.2—2015 中没有组件来指定主备用数据库实例控制切换和故障转移的功能。FPT_OVR_EXT.1 组件定义了备用服务器数据库可用性功能中内部 TSF 一致性功能的及时性

7.1.2 TSF 保护(FPT 类)

TSF 控制切换/故障转移(FPT_OVR_EXT.1)

FPT_OVR_EXT.1.1 TSF 应提供从正在运行数据库实例【选择:**主节点**,【***赋值:指定节点***】】切换到另外一个数据库实例【选择:**备用节点**,【***赋值:指定节点***】】故障转移的能力,即一旦授权管理员发起 TSF 故障切换命令,在不丢失分布式事务处理数据的情况下,两个节点的 TSF 控制都能够保证在切换

时事务继续正常的执行。

FPT_OVR_EXT.1.2 TSF 应提供从正在运行数据库实例【选择：**主节点**，【***赋值：指定节点***】】切换到另外一个数据库实例【选择：***备用节点***，【***赋值：指定节点***】】故障转移的能力，即一旦授权管理员发起故障转移，仅仅会丢失已经被提交到正在运行数据库实例节点上的事务，而不会影响到转移节点上的数据库事务。

7.1.3 安全管理（FMT 类）

7.1.3.1 安全属性的管理[FMT_MSA_EXT.1(1)]

FMT_MSA_EXT.1.1TSF 应实施【选择：***基于用户控制策略***、***基于角色控制策略***、***基于用户组控制策略***、【***赋值：ST 作者定义的自主访问控制***】】，以仅限于【选择：***授权管理员***、***授权用户***】能够对安全属性【选择：***数据库对象访问权限***、***安全角色***】进行【选择：***改变默认值***、***查询***、***修改***、***删除***、【***赋值：其他操作***】】。

FMT_MSA_EXT.1.2TSF 应实施【选择：***基于标签访问控制安全策略***、【***赋值：ST 作者指定机制的信息流控制策略***】】，以仅限于【选择：***LBAC 授权的用户***、【***赋值：ST 作者指定授权管理员***】】能够【【赋值：***安全属性***】以【赋值：***安全标签***】】。

注：该要求适用于 EAL3 评估保障级。

7.1.3.2 安全属性的管理[FMT_MSA_EXT.1(2)]

FMT_MSA_EXT.1.1TSF 应实施【选择：***基于用户控制策略***、***基于角色控制策略***、***基于用户组控制策略***、【***赋值：ST 作者定义的强制访问控制***】】，以仅限于【选择：***授权管理员***、***授权用户***】能够对安全属性【选择：***数据库对象访问权限***、***安全角色***】进行【选择：***改变默认值***、***查询***、***修改***、***删除***、【***赋值：其他操作***】】。

FMT_MSA_EXT.1.2TSF 应实施【选择：***基于标签访问控制安全策略***、【***赋值：ST 作者指定机制的信息流控制策略***】】，以仅限于【选择：***LBAC 授权的用户***、【***赋值：ST 作者指定授权管理员***】】能够【【赋值：***安全属性***】以【赋值：***安全标签***】】。

注：该要求适用于 EAL4 评估保障级。

7.1.3.3 静态属性初始化（FMT_MSA_EXT.3）

FMT_MSA_EXT.3.1 TSF 应执行【选择：***基于用户控制策略***、***基于角色控制策略***、***基于用户组控制策略***、【***赋值：ST 作者定义的自主访问控制***】】，以便为用于执行 SFP 的安全属性提供【选择，从中选取一个：***受限的***、***许可的***、【***赋值：其他特性***】】默认值。

7.2 安全功能要求

7.2.1 概述

表 7 列出了 DBMS 评估保障级（EAL）2、3 和 4 的 TOE 安全功能组件。在安全功能组件元素描述中，方括号【】中的粗体字内容表示已经完成的操作，粗斜体字内容表示还需在安全目标中由 ST 作者确定赋值及选择项。

表 7 安全功能组件

功能类	功能组件	评估保障级		
		EAL2	EAL3	EAL4
安全审计	FAU_GEN.1 审计数据产生	√	√	√
	FAU_GEN.2 用户身份关联	√	√	√

表 7（续）

功能类	功能组件	评估保障级		
		EAL2	EAL3	EAL4
安全审计	FAU_SAR.1 安全审计查阅	√	√	√
	FAU_SAR.2 限制审计查阅	—	√	√
	FAU_SAR.3 可选审计查阅	—	√	√
	FAU_SEL.1 选择性审计	√	√	√
	FAU_STG.2 审计数据可用性保证	√	√	√
	FAU_STG.4 防止审计数据丢失	—	√	√
密码支持	FCS_CKM.1 密钥生成	—	√	√
	FCS_CKM.4 密钥销毁	—	√	√
	FCS_COP.1 密码运算	—	√	√
用户数据保护	FDP_ACC.1 子集访问控制	√	√	—
	FDP_ACF.1 基于安全属性的访问控制	√	√	√
	FDP_IFC.1 子集信息流控制	—	—	√
	FDP_IFF.2 分级安全属性	—	√	√
	FDP_ETC.2 带有安全属性的用户数据输出	√	√	√
	FDP_ITC.1 不带安全属性的用户数据输入	√	√	√
	FDP_ITT.1 基本内部传送保护	√	√	√
	FDP_RIP.1 子集残余信息保护	√	√	√
	FDP_ROL.1 基本回退	√	√	√
	FDP_SDI.2 存储数据完整性监视和行动	—	√	√
标识和鉴别	FIA_AFL.1 鉴别失败处理	√	√	√
	FIA_ATD.1 用户属性定义	√	√	√
	FIA_SOS.1 秘密的验证		√	√
	FIA_UAU.1 鉴别的时机	√	√	√
	FIA_UAU.5 多重鉴别机制	—	√	√
	FIA_UAU.7 受保护的鉴别反馈	√	√	√
	FIA_UID.1 标识的时机	√	√	√
	FIA_USB.1 用户-主体绑定	√	√	√
安全管理	FMT_MOF.1 安全功能行为的管理	√	√	√
	FMT_MSA_EXT.1 (1)安全属性的管理	√	√	—
	FMT_MSA_EXT.1 (2)安全属性的管理	—	—	√
	FMT_MSA_EXT.3 静态属性初始化	√	√	√
	FMT_MTD.1 TSF 数据的管理	√	√	√
	FMT_REV.1 撤销	√	√	√

表 7（续）

功能类	功能组件	评估保障级		
		EAL2	EAL3	EAL4
安全管理	FMT_SMF.1 管理功能规范	√	√	√
	FMT_SMR.1 安全角色	—	√	—
	FMT_SMR.2 安全角色限制	—	—	√
TSF 保护	FPT_FLS.1 失效即保持安全状态	√	√	√
	FPT_ITT.2 TSF 数据传送的分离	√	√	√
	FPT_RCV.3 无过度损失的自动恢复	√	√	√
	FPT_TRC.1 内部 TSF 的一致性	√	√	√
	FPT_OVR_EXT.1 TSF 控制切换/故障转移	—	√	√
资源利用	FRU_FLT.1 降级容错	√	√	√
	FRU_RSA.2 最低最高配额	√	√	√
TOE 访问	FTA_LSA.1 可选属性范围限定	√	√	√
	FTA_MCS.1 多重并发会话的基本限定	√	√	√
	FTA_SSL.3 TSF 原发会话终止	—	√	√
	FTA_TAH.1 TOE 访问历史	√	√	√
	FTA_TSE.1 TOE 会话建立	√	√	√
可信路径/信道	FTP_ITC.1 TSF 间可信信道	—	—	√
注：√ 代表在该评估保障级下包括的安全功能组件。 — 代表在该评估保障级下未包括的安全功能组件。				

7.2.2 安全审计（FAU 类）

7.2.2.1 审计数据产生（FAU_GEN.1）

FAU_GEN.1.1 TSF 应能够为下述可审计事件产生审计记录：

a） 数据库审计功能的启动和关闭；

b） 数据库实例及其组件服务的启动和关闭；

c） 数据库安全功能【选择：***最小级***、***基本级***、***未规定***】审计级别的所有可审计事件；

d） 其他面向数据库安全审计员的，并且是可绕过访问控制策略的特殊定义【赋值：***ST 作者定义的 DBMS 审计事件***】的可审计事件；

e） 未指定审计级别（例如数据库对象数据操作级）的所有可审计事件。

FAU_GEN.1.2 TSF 应在每个审计记录中至少记录下列信息：

a） 事件的日期和时间、事件类型、主体身份和关联组或角色、事件结果（成功或失败）；

b） 对于每个审计事件类型，基于本标准定义的安全功能组件的可审计事件定义，表 8 列出了最小审计级别的数据库安全功能可审计事件。

表 8　可审计安全事件类型

安全功能要求	可审计事件
FAU_GEN.1	无审计事件
FAU_SAR.1	无审计事件
FAU_SAR.2	无审计事件
FAU_SAR.3	无审计事件
FAU_SEL.1	当审计选项开启，数据采集功能正在运行时，所有因审计配置修改而产生的事件
FAU_STG.2	无审计事件
FAU_STG.4	因审计存储失效而采取的动作
FCS_CKM.1	密钥生成操作成功和失败
FCS_CKM.4	密钥销毁操作成功和失败
FCS_COP.1	成功和失败，以及密码运算的类型
FDP_ACC.1	无审计事件
FDP_ACF.1	在安全功能策略覆盖的数据库对象上执行某个操作的成功请求
FDP_IFC.1	无审计事件
FDP_IFF.2	允许请求的信息流动的决定
FDP_ETC.2	输出信息的所有尝试
FDP_ITC.1	授权用户提供的用于输入的用户数据的安全属性规范
FDP_ITT.1	用户数据传送的所有尝试，包括所用的保护方法和出现的任何错误
FDP_RIP.1	无审计事件
FDP_ROL.1	所有成功的回退操作
FDP_SDI.2	检测到完整性错误时所采取的行动
FIA_AFL.1	未成功鉴别尝试达到阈值、达到阈值后所采取的动作（如，锁定账户），及后来（适当时）还原到正常状态（如，解锁）
FIA_ATD.1	无审计事件
FIA_SOS.1	试图修改用户密码的成功或失败的尝试
FIA_UAU.1	所有数据库鉴别机制的使用，包括鉴别成功或失败的尝试
FIA_UAU.5	鉴别的最终裁决
FIA_UAU.7	尚无预见的可审计事件
FIA_UID.1	未成功用户标识机制的使用，包括所提供的用户身份
FIA_USB.1	用户安全属性和数据库主体的成功或失败的绑定
FMT_MOF.1	无审计事件
FMT_MSA_EXT.1	所有对安全属性值的改动
FMT_MSA_EXT.3	对允许或限制规则默认设置的修改
FMT_MTD_1	无审计事件
FMT_REV.1	安全属性的未成功撤消

表 8（续）

安全功能要求	可审计事件
FMT_SMF.1	对充当某个角色的某用户/用户组的修改
FMT_SMR.1	对属于某个角色某用户/用户组的修改
FMT_SMR.2	对属于某个角色某用户/用户组的修改；由于对角色的限制条件，而导致使用某个角色时的未成功尝试
FPT_RCV.3	失效或服务中断的发生，正常运行的恢复
FPT_FLS.1	要求 TSF 当确定的失效出现时保持一种安全状态
FPT_ITT.2	无审计事件
FPT_TRC_.1	重新连接时恢复数据一致性
FPT_OVR_EXT.1	控制切换开始/完成、故障转移/切换开始/完成
FRU_FLT.1	TSF 检测出的任何失效
FRU_RSA.2	由于数据库服务器资源的限制导致分配操作的拒绝，确保用户可用资源
FTA_LSA.1	选择某种会话安全属性时的所有失败尝试
FTA_MCS.1	基于多重并发会话限定对新会话的拒绝
FTA_SSL.3	利用会话锁定机制对交互式会话的锁定
FTA_TAH.1	无审计事件
FTA_TSE.1	依据会话建立机制拒绝一个会话的建立
FTA_ITC.1	可信信道功能的失效，失效的可信信道功能的发起者和目标端的标识

7.2.2.2 用户身份关联（FAU_GEN.2）

FAU_GEN.2.1 对于已标识用户行为所产生的审计事件，TSF 应能将每个审计事件和引起该审计事件的用户身份关联起来。

7.2.2.3 安全审计查阅（FAU_SAR.1）

FAU_SAR.1.1 TSF 应为【赋值：***授权管理员***】提供从审计记录中阅读和获取下面所列出的审计信息的权力：

a） 用户、用户组或角色标识；

b） 审计事件类型；

c） 数据库对象标识；

d） 【选择：***主体标识***、***主机标识***、***无***】；

e） 【选择：***成功可审计安全事件***、***失败可审计安全事件***、和【选择：【***赋值：基于其他选择条件的选择性审计事件清单***】、***没有任何附加条件***】】；

f） 数据库权限【选择：***系统权限***、***实例权限***、***数据库权限***、***模式对象权限***、***细粒度数据权限***】。

FAU_SAR.1.2 TSF 应以使用授权用户理解的方式提供审计记录。

7.2.2.4 限制审计查阅（FAU_SAR.2）

FAU_SAR.2.1 除了授权管理员具有明确的阅读访问审计数据的权限外，TSF 应禁止所有授权用

户对审计记录进行读访问。

7.2.2.5 可选审计查阅(FAU_SAR.3)

FAU_SAR.3.1 TSF 应根据【**审计数据字段中的值的搜索与分类条件**】提供对查阅的审计数据进行【**搜索和排序**】的能力。

7.2.2.6 选择性审计(FAU_SEL.1)

FAU_SEL.1.1 TSF 应能根据以下属性从审计事件集中选择可审计事件:

a) 用户身份【选择:***客体身份***、***用户身份***、***组身份***、***主体身份***、***主机身份***】;

b) 操作类型【选择:***定义语句***、***查询语句***、***更新语句***、***控制语句***】;

c) 权限级别【选择:***系统权限***、***实例权限***、***数据库权限***、***模式对象级审计***、***细粒度数据权限***,【***赋值:ST 作者指定的权限列表***】】;

d) 可审计安全事件【选择:***成功***、***失败***、***二者***】;

e) 【赋值:***审计选择所依据的附加属性表***】;

f) 【选择:【***赋值:审计选择额外的标准列表***】、***没有额外标准***】】。

注:该功能目的是为了捕获充分的审计数据以允许授权管理员执行任务,ST 作者在细化时可依据审计目的给出更多的审计数据。

7.2.2.7 审计数据可用性保证(FAU_STG.2)

FAU_STG.2.1 TSF 应保护审计迹中所存储的审计记录,以避免未授权的删除。

FAU_STG.2.2 TSF 应能防止对审计迹中所存审计记录的未授权修改。

FAU_STG.2.3 当下列情况发生时:【选择:***审计存储耗尽***、***失效***、***受攻击***】,TSF 应能确保【赋值:***保存审计记录的度量***】审计记录将维持有效。

7.2.2.8 防止审计数据丢失(FAU_STG.4)

FAU_STG.4.1 如果审计记录数据已满,系统应【选择,选取一个:***忽略可审计事件***、***"阻止可审计事件,除非具有特权的授权用户产生的审计事件"***、***覆盖所存储的最早的审计记录***】和【赋值:***审计存储失效时所采取的其他动作***】。

7.2.3 密码支持(FCS 类)

7.2.3.1 密钥生成(FCS_CKM.1)

FCS_CKM.1.1TSF 应根据符合下列标准【赋值:***国家、行业要求的密码管理相关标准或规范***】的一个特定的密钥生成算法【赋值:***密钥生成算法***】和规定的密钥长度【赋值:***密钥长度***】来生成密钥。

注:若密钥由外部环境生成,可以不选择此组件。该组件仅适用于由 DBMS 本身完成的情况,此时 ST 作者可根据密码算法的具体情况,赋值 TOE 用户单位主管部门认可的相关标准及参数。

7.2.3.2 密钥销毁(FCS_CKM.4)

FCS_CKM.4.1 TSF 应根据符合下列标准【赋值:***国家、行业要求的密码管理相关标准或规范***】的一个特定的密钥销毁方法【赋值:***密钥销毁方法***】来销毁密钥。

7.2.3.3 密码运算(FCS_COP.1)

FCS_COP.1.1TSF 应根据符合下列标准【赋值:***国家、行业要求的密码管理相关标准或规范***】的特定的密码算法【赋值:***密码算法***】和密钥长度【赋值:***密钥长度***】来执行【赋值:***密码运算列表***】。

7.2.4 用户数据保护(FDP 类)

7.2.4.1 子集访问控制(FDP_ACC.1)

FDP_ACC.1.1 TSF 应对授权的数据库对象操作列表执行主体(系统和用户)定义的下列访问控制策略:【选择:*基于用户控制策略*、*基于角色控制策略*、*基于用户组控制策略*、【*赋值:ST 作者定义的自主访问控制策略*】】。

7.2.4.2 基于安全属性的访问控制(FDP_ACF.1)

FDP_ACF.1.1TSF 应基于【选择:*基于用户控制策略*、*基于角色控制策略*、*基于用户组控制策略*、【*赋值:ST 作者定义的自主访问控制*】】对数据库对象的操作执行访问控制,具体应包括:

a) 与主体相关的授权用户身份和/或角色和/或组成员关系;
b) 受控数据库对象可实施的访问操作和/或角色/组权限;
c) 受控数据库对象标识;
d) 对数据库对象执行【选择:*基于用户控制策略*、*基于角色控制策略*、*基于用户组控制策略*、【*赋值:ST 作者定义的自主访问控制策略*】】。

FDP_ACF.1.2TSF 应执行【赋值:*在受控主体和受控数据库对象间,通过对受控数据库对象采取受控操作来管理访问的规则*】,以确定授权用户、授权管理员与数据库对象间的一个操作是否被允许。

FDP_ACF.1.3TSF 应基于附加规则:【选择:【*赋值:安全属性、明确授权用户访问数据库对象的规则*】、*无附加显式授权规则*】,明确授权用户访问 DBMS 控制的数据库对象。

FDP_ACF.1.4TSF 应基于【选择:【*赋值:安全属性,明确拒绝主体访问客体的规则*】、*无附加的显式拒绝规则*】,明确拒绝授权用户访问 DBMS 控制的数据库对象。

7.2.4.3 子集信息流控制(FDP_IFC.1)

FDP_IFC.1.1TSF 应对【**授权用户对受基于标签访问控制(LBAC)的数据库数据对象的读、写操作**】应用【选择:*LBAC 安全功能策略*、【*赋值:ST 作者附加的信息流控制 SFP 规则*】】。

7.2.4.4 分级安全属性(FDP_IFF.2)

FDP_IFF.2.1TSF 应基于授权用户和数据库对象安全属性:【**主体安全标签和数据库对象(关系行、列或单元)安全标签的**【选择:*数组*、*集合*、*树*、【*赋值:ST 作者定义的标签元素*】】】执行【选择:*LBAC 安全功能策略*、【*赋值:ST 作者附加的信息流控制 SFP 规则*】】。

FDP_IFF.2.2 如果满足【赋值:*规则列表*】规则,TSF 应允许通过授权用户和受控数据库对象(如关系表行、列、单元)之间的读写操作。

FDP_IFF.2.3TSF 应执行以下规则【只有【选择:*安全管理员*、【*赋值:ST 作者指定的授权管理员*】】能够改变用户的安全标签,具有适当权限的授权用户/授权管理员能够改变受 LBAC 保护的数据表的行、列或单元的安全标签】。

FDP_IFF.2.4TSF 应基于以下规则:【赋值:*ST 作者指定的一个拥有相应豁免的用户能够忽略对读数组、读集合、读树、写数组、写集合、写树的检查*】,明确地授权一个信息流。

FDP_IFF.2.5TSF 应基于以下规则:【赋值:*基于安全属性、明确拒绝信息流的规则*】明确拒绝一个信息流。

FDP_IFF.2.6TSF 应对任意两个【选择:*标签*、【*赋值:ST 作者定义的信息流控制*】】安全属性判定下列关系:

a) 存在一个有序函数,对于给定的两个有效的安全属性,函数能够判定他们是否相等,是否其中

一个大于另一个，还是两者不可比较；

b) 在安全属性集合中存在一个“最小上界”，对于给定的两个有效的安全属性，存在一个有效的安全属性大于或者等于这两个安全属性；

c) 在安全属性集合中存在一个“最大下界”，对于给定的两个有效的安全属性，存在一个有效的安全属性不大于这两个属性。

7.2.4.5 带有安全属性的用户数据输出(FDP_ETC.2)

FDP_ETC.2.1 在 SFP 控制下将用户数据输出到 TOE 之外时，TSF 应执行【赋值：***访问控制 SFP 和(/或)信息流控制 SFP***】。

FDP_ETC.2.2TSF 应输出用户数据且带有用户数据关联的安全属性。

FDP_ETC.2.3TSF 应确保输出安全属性到 TOE 之外时，与所输出的用户数据确切关联。

FDP_ETC.2.4 当从 TOE 输出用户数据时，TSF 应执行下列规则【赋值：***附加的输出控制规则***】。

7.2.4.6 不带安全属性的用户数据输入(FDP_ITC.1)

FDP_ITC.1.1 在 SFP 控制下从 TOE 之外输入用户数据时，TSF 应执行【赋值：***访问控制 SFP 和(/或)信息流控制 SFP***】。

FDP_ITC.1.2 从 TOE 外部输入用户数据时，TSF 应忽略任何与用户数据相关的安全属性。

FDP_ITC.1.3 在 SPF 控制下从 TOE 之外输入用户数据时，TSF 应执行下面的规则：【赋值：***附加的输入控制规则***】。

7.2.4.7 基本内部传送保护(FDP_ITT.1)

FDP_ITT.1.1 在 TOE 物理上分隔的部分间传递用户数据时，TSF 应执行【赋值：***访问控制 SFP 和(/或)信息流控制 SFP***】，以防止用户数据的【选择：***泄露、篡改、丧失可用性***】。

7.2.4.8 子集残余信息保护(FDP_RIP.1)

FDP_RIP.1.1TSF 应确保数据库服务器共享内存和存储空间等服务器资源的任何先前的信息内容，在资源释放或资源被重新分配给其他模式对象之后是不再可用的。

7.2.4.9 基本回退(FDP_ROL.1)

FDP_ROL.1.1TSF 应【选择：***子集访问控制、子集信息流控制、【赋值：ST 作者定义的访问控制***】】策略，以允许对【选择：***数据库、模式、表空间、数据表、视图、约束、存储过程、存储函数、【赋值：其他数据库对象***】】用【SQL **表达的数据库操作**】执行回退操作。

FDP_ROL.1.2TSF 允许对数据库实例重启中实例恢复事务中【**用户事务请求集合中未提交 SQL 语句**】进行回退操作。

7.2.4.10 存储数据的完整性监视和行动(FDP_SDI.2)

FDP_SDI.2.1 TSF 应基于下列属性：【赋值：***用户数据属性***】，对所有客体，监视存储在由 TSF 控制的载体内的用户数据的【赋值：***完整性错误***】。

FDP_SDI.2.1 检测到数据完整性错误时，TSF 应【赋值：***采取的动作***】。

7.2.5 标识和鉴别(FIA 类)

7.2.5.1 鉴别失败处理(FIA_AFL.1)

FIA_AFL.1.1 TSF 应对【赋值：***登录 DBMS 用户***】不满足授权管理员定义的口令策略【选择：***达到***

鉴别尝试次数、达到口令有效期、达到口令重用次数、【赋值：可接受值的范围】加以检测，与【选择：***授权用户鉴别、授权管理员鉴别、【赋值：其他鉴别事件列表】***】相关的未成功鉴别尝试进行处理。

FIA_AFL.1.2 当不成功鉴别尝试的指定次数已达到或超出【赋值：***可接受值的范围***】，TSF 应阻止受控主体的登录，直到安全管理员采取行动或直到安全管理员配置的时间【赋值：***可接受值的范围***】已经到达。

7.2.5.2 用户属性定义（FIA_ATD.1）

FIA_ATD.1.1TSF 应维护属于每个数据库用户下列安全属性：

a) 数据库用户标识，验证数据（秘密）；
b) 安全相关的角色或用户组；
c) 用户口令策略；
d) 服务器资源限制；
e) 数据库对象访问权限；
f) 数据库管理权限；
g) 【赋值：***任何附加的授权管理员安全属性***】。

7.2.5.3 秘密的验证（FIA_SOS.1）

FIA_SOS.1.1 TSF 应提供一种机制以验证秘密满足【赋值：***一个既定的质量度量***】。例如用户口令验证需满足：

a) 被限制在最小和最大数量的字符长度之间；
b) 包含一个大写和小写字符的组合；
c) 至少包含一个数字字符；
d) 至少包含一个特殊字符；
e) 不能是用户标识或用户名称；
f) 被限制在一个有效期内；
g) 以前使用的口令需在多少天数内无法再度使用等。

7.2.5.4 鉴别的时机（FIA_UAU.1）

FIA_UAU.1.1 在数据库用户身份被鉴别之前，TSF 应允许代表用户的【赋值：***TSF 促成的行动列表***】被执行。例如

a) 获取当前 DBMS 版本信息；
b) 建立数据库连接；
c) 如果不成功，返回错误信息。

FIA_UAU.1.2 在允许任何数据库用户的数据库请求行动执行前，TSF 应要求该用户已被成功鉴别。

注：本组件针对 TOE 本地鉴别的用户，不包括鉴别以前应在客户端和服务 DBMS 之间传输的管理和控制数据包。

7.2.5.5 多重鉴别机制（FIA_UAU.5）

FIA_UAU.5.1 TSF 应提供【选择：***口令、证书、【赋值：ST 作者提供的多重鉴别机制】***】多重鉴别机制，以支持数据库用户鉴别。

FIA_UAU.5.2 TSF 应依据选择【选择：***数据库鉴别、操作系统鉴别、第三方鉴别、【赋值：ST 作者提供的工作规则】***】为授权管理员和授权用户鉴别任何用户所声称的身份。

注：本标准规定外部鉴别是 TOE 通过 IT 环境提供的鉴别服务器对用户身份进行的鉴别（如操作系统鉴别、第三方鉴别）。

7.2.5.6 受保护的鉴别反馈(FIA_UAU.7)

FIA_UAU.7.1 鉴别进行时,TSF 应仅向用户提供【*赋值:反馈列表*】。

7.2.5.7 标识的时机(FIA_UID.1)

FIA_UID.1.1 在允许任何其他代表用户的 TSF 促成的行动执行前,TSF 应要求该用户已被成功标识。

7.2.5.8 用户-主体绑定(FIA_USB.1)

FIA_USB.1.1TSF 应将合适的用户安全属性与代表用户活动的主体相关联:【赋值:*用户安全属性的列表*】。

FIA_USB.1.2 TSF 在最初关联用户安全属性和代表用户活动的主体时应实施下面的规则:【赋值:*最初属性关联规则*】。

FIA_USB.1.3 在管理与代表用户活动的主体相关联的用户安全属性的变化时应实施下面的规则:【赋值:*属性变化的规则*】。

7.2.6 安全管理(FMT 类)

7.2.6.1 安全功能行为的管理(FMT_MOF.1)

FMT_MOF.1.1TSF 应仅限于【赋值:*已识别授权角色*】对安全管理功能【赋值:*功能列表*】具有【选择:*确定其行为、禁止、允许、修改其行为*】的能力。例如:

a) 管理【赋值:数据库实例安全功能组件配置参数】;
b) 限定启动/禁用授权管理员的安全功能【赋值:*有关事件审计规范*】;
c) 在安全告警事件中配置要【赋值:*执行行为*】的管理;
d) 在鉴别失败事件中要【赋值:*采取行为*】的管理;
e) 在用户成功被鉴别之前所能【赋值:*采取行为*】的管理;
f) 授权管理员如果能改变用户被识别之前所能采取的行为列表,应对授权管理员的此种【赋值:*行为*】进行管理;
g) DBMS 管理的数据及运行完整性自检发生【选择:*初始化启动、定期间隔、其他特定条件*】时的条件的管理;
h) ST 中附加【赋值:*安全功能列表*】的管理。

7.2.6.2 TSF 数据的管理(FMT_MTD.1)

FMT_MTD_EXT.1.1TSF 应仅限于具有【选择:*系统管理员、安全管理员、【赋值:授权安全管理官员】*】角色的授权管理员能够【赋值:*改变默认值、查询、修改、删除、【或添加】*】【选择:*用户标识、用户组成员、安全角色*】。

FMT_MTD_EXT.1.2TSF 应仅限于具有【选择:*系统管理员、安全管理员、【赋值:授权安全管理官员】*】角色的授权管理员能够【赋值:*改变默认值、修改、删除、【或添加】*】授权用户的【认证数据】。

FMT_MTD_EXT.1.3TSF 应仅限于具有【选择:*系统管理员、安全管理员、【赋值:授权安全管理官员】*】角色的授权管理员能够【赋值:*包括或排除可审计策略*】。

FMT_MTD_EXT.1.4TSF 应仅限于具有【选择:*系统管理员、安全管理员、【赋值:授权安全管理官员】*】角色的授权管理员能够【删除和【查看】】【审计踪迹中的审计事件集】。

FMT_MTD_EXT.1.5TSF 应根据【赋值:*ST 作者定义的安全元数据列表*】仅限于【选择:*系统管理*

*员、安全管理员、【赋值：授权安全管理官员】*能够在系统数据上执行操作【选择：*改变默认值、查询、修改、删除、清除、【赋值：其他操作】*】。

7.2.6.3 撤销(FMT_REV.1)

FMT_REV.1.1TSF 应仅限于【赋值：*已标识的授权角色*】能够撤消在 TSF 控制下的与【选择：*用户、主体、客体、【赋值：其他额外资源】*】相关联的所有可管理的安全属性【选择：*口令策略、资源限制、角色和权限、【赋值：ST 作者定义的安全属性】*】。

FMT_REV.1.2TSF 应执行规则【选择：*撤销数据库管理权限应在数据库用户开始下一个数据库会话前生效*、或【*赋值：撤消规则的详细说明*】】。

7.2.6.4 管理功能规范(FMT_SMF.1)

FMT_SMF.1.1 TSF 应能够执行如下安全管理功能：【赋值：*ST 作者提供的安全管理功能列表*】。例如下列数据库安全管理功能：

a) 添加和删除数据库用户；
b) 改变用户登录数据库实例状态；
c) 在数据库实例(服务器)级别和数据库级别配置数据库角色权限及其成员用户；
d) 创建和删除数据库实例(服务器)级别和数据库级别的用户组；
e) 定义数据库用户认证模式(操作系统验证、数据库验证、第三方验证)；
f) 管理连接数据库用户会话的属性；
g) 使能和禁用数据库加密功能；
h) 管理数据库加密密码；
i) 创建和销毁加密密钥；
j) 启动和停止审计；
k) 选择审计事件；
l) 创建、删除和查阅审计记录数据；
m) 定义当审计文件填满时采取的行动；
n) 创建和删除基于标签的访问控制(LBAC)策略和标签；
o) 授权和撤销 LBAC 安全标签与受控主体与受控客体的绑定；
p) 创建、删除、授权和撤销数据库角色；
q) 授权、撤销数据库管理员访问属性；
r) 管理数据库用户口令策略；
s) 管理数据库用户对系统资源使用的最大限额等。

7.2.6.5 安全角色(FMT_SMR.1)

FMT_SMR.1.1TSF 应维护角色【赋值：*已标识的授权角色或组*】。例如下列数据库安全管理角色或组：

a) 安全管理员；
b) 审计管理员；
c) 数据库管理员；
d) 系统管理员；
e) 由授权的安全管理员定义的安全角色或组。

FMT_SMR.2.2TSF 应能够把用户和角色或组关联起来。

7.2.6.6 安全角色限制(FMT_SMR.2)

FMT_SMR.2.1TSF 应维护角色【赋值:*已标识的授权角色或组*】。例如下列数据库安全管理角色或组:

a) 安全管理员;
b) 审计管理员;
c) 数据库管理员;
d) 系统管理员;
e) 由授权的安全管理员定义的安全角色或组。

FMT_SMR.2.2TSF 应能够把用户和角色或组关联起来。

FMT_SMR.2.3TSF 应确保条件【赋值:*不同角色或组的条件*】得到满足。

7.2.7 TSF 保护(FPT 类)

7.2.7.1 失效即保持安全状态(FPT_FLS.1)

FPT_FLS.1.1 TSF 在下列失效发生时应保持一种安全状态:【赋值:*TSF 的失效类型列表*】。

7.2.7.2 TSF 数据传送的分离(FPT_ITT.2)

FPT_ITT.2.1 TSF 应在 TOE 分布式部署时保护不同节点 TSF 数据在传送时不被【选择:*泄漏,篡改,丢失*】。

FPT_ITT.2.2 当数据在 TOE 分布式部署的不同部分间传送时,TSF 应将用户数据从 TSF 数据中分离出来。

7.2.7.3 无过度损失的自动恢复(FPT_RCV.3)

FPT_RCV.3.1TSF 应保证不能从【选择:*数据库服务器进程失效、数据库实例失效、数据库存储介质失效,【赋值:ST 作者定义失效或服务中断列表】*】自动恢复时,TSF 应进入一种维护模式,该模式提供将数据库服务器返回到一个安全状态的能力。

FPT_RCV.3.2TSF 应保证对【选择:*数据库服务器进程失效、数据库实例失效、数据库存储介质失效,【赋值:ST 作者定义失效或服务中断列表】*】,TSF 应确保通过数据库恢复服务自动化过程使 TOE 返回到一个安全状态。

FPT_RCV.3.3TSF 应保证 TSF 提供的从服务中断或失效状态数据库恢复的功能,应确保在 TSF 的控制内 TSF 数据或用户数据不超出【赋值:*数据库完整性约束条件*】的情况下,保证数据库数据一致性。

FPT_RCV.3.4TSF 应保证数据库实例失效情况下数据库恢复进程提供【选择:*恢复到指定时间点、恢复到指定事务、恢复到实例失效点、【赋值:ST 作者定义的恢复策略】*】的能力。

7.2.7.4 内部 TSF 的一致性(FPT_TRC.1)

FPT_TRC_EXT.1.1TSF 应保证 TSF 数据在【选择:*共享内容、磁盘、【赋值:分布式部署节点】*】间出现不一致时,提供某种机制使不一致的 TSF 数据及时的达到一种一致的状态。

7.2.8 资源利用(FRU 类)

7.2.8.1 降级容错 (FRU_FLT.1)

FRU_FLT.1.1 TSF 应确保当以下失效:【赋值:*失效类型列表*】发生时,【赋值:*TOE 能力列表*】能正常发挥。

7.2.8.2 最低最高配额(FRU_RSA.2)

FRU_RSA.2.1 TSF 应对数据库服务器的以下资源:【选择:*物理 I/O、逻辑 I/O、持久存储空间、临时存储空间、一个特定事务持续使用时间或未使用时间、【赋值:ST 定义指定的资源列表】*】分配最高配额,以便【选择:*单个用户、预定义用户、主体*】能在【选择:*一段指定的时间间隔内*】使用。

FRU_RSA.2.2 TSF 应确保数据库服务器的以下资源:【选择:*物理 I/O、逻辑 I/O、持久存储空间、临时存储空间、一个特定事务持续使用时间或未使用时间、【赋值:ST 定义指定的资源列表】*】*的最低供应量*,以便【选择:*单个用户、预定义的用户组、主体*】能【选择:*同时、规定的时间间隔内*】使用。

7.2.9 TOE 访问(FTA 类)

7.2.9.1 可选属性范围限定(FTA_LSA.1)

FTA_LSA.1.1 TSF 应基于【赋值:*属性*】,限制下列会话安全属性的范围:【赋值:*会话安全属性*】。

7.2.9.2 多重并发会话的基本限定(FTA_MCS.1)

FTA_MCS.1.1 TSF 应限制属于同一用户的并发会话的最大数目。

FTA_MCS.1.2 TSF 应缺省地限定每个用户【赋值:*缺省数*】次会话。

7.2.9.3 TSF 原发会话终止(FTA_SSL.3)

FTA_SSL.3.1 TSF 应在达到【赋值:*用户不活动的时间间隔*】之后终止一个交互式会话。

7.2.9.4 TOE 访问历史(FTA_TAH.1)

FTA_TAH.1.1 在会话成功建立的基础上,TSF 应向用户显示上一次成功建立的会话的【赋值:*日期、时间、访问应用程序、IP 地址和访问方法*】。

FTA_TAH.1.2 在会话成功建立的基础上,TSF 应显示上一次会话建立的未成功尝试的【赋值:*日期、时间、访问应用程序、IP 地址和访问方法*】和从上一次成功的会话建立以来的不成功尝试次数。

FTA_TAH.1.3 如果没有向用户提供审阅访问历史信息的机会,TSF 就不能从用户接口擦除该信息。

7.2.9.5 TOE 会话建立(FTA_TSE.1)

FTA_TSE.1.1TSF 应能基于【选择:*用户身份、用户组或角色、主机标识、客户端 IP、时间、【赋值:ST 作者指定属性】*】拒绝数据库会话的建立。

7.2.10 可信路径/信道(FTP 类)

TSF 间可信信道(FTP_ITC.1)

FTP_ITC.1.1TSF 应在它自己和另一个可信 IT 产品之间提供一条通信信道,此信道在逻辑上与其他通信信道截然不同,并对其端点进行了有保障的标识,且能保护信道中数据免遭修改或泄露。

FTP_ITC.1.2 TSF 应允许【选择:*TSF、另一个可信 IT 产品*】经由可信信道发起通信。

FTP_ITC.1.3 对于数据库客户端认证、外部用户身份鉴别、分布式数据部署处理节点间数据通信等采用加密传输的通信信道,TSF 应经由可信信道发起通信。

7.3 安全保障要求

7.3.1 概述

表 9 列出了 DBMS 评估保障级(EAL)2、3 和 4 的 TOE 安全保障组件。

表 9　安全保障组件

保障类	保障组件	评估保障级		
		EAL2	EAL3	EAL4
开发	ADV_ARC.1 安全架构描述	√	√	√
	ADV_FSP.2 安全执行功能规范	√	—	—
	ADV_FSP.3 带完整摘要的功能规范	—	√	—
	ADV_FSP.4 完备的功能规范	—	—	√
	ADV_IMP.1 TSF 实现表示	—	—	√
	ADV_TDS.1 基础设计	√	—	—
	ADV_TDS.2 结构化设计	—	√	—
	ADV_TDS.3 基础模块设计	—	—	√
指导性文档	AGD_OPE.1 操作用户指南	√	√	√
	AGD_PRE.1 准备程序	√	√	√
生命周期支持	ALC_CMC.2 CM 系统的使用	√	—	—
	ALC_CMC.3 授权控制	—	√	—
	ALC_CMC.4 生产支持和接受程序及其自动化	—	—	√
	ALC_CMS.2 部分 TOE CM 覆盖	√	—	—
	ALC_CMS.3 实现表示 CM 覆盖	—	√	—
	ALC_CMS.4 问题跟踪 CM 覆盖	—	—	√
	ALC_DEL.1 交付程序	√	√	√
	ALC_DVS.1 安全措施标识	—	√	√
	ALC_LCD.1 开发者定义的生命周期模型	—	√	√
	ALC_TAT.1 明确定义的开发工具	—	—	√
安全目标	ASE_CCL.1 符合性声明	√	√	√
	ASE_ECD.1 扩展组件定义	√	√	√
	ASE_INT.1 ST 引言	√	√	√
	ASE_OBJ.2 安全目的	√	√	√
	ASE_REQ.2 推导出的安全要求	√	√	√
	ASE_SPD.1 安全问题定义	√	√	√
	ASE_TSS.1 TOE 概要规范	√	√	√
测试	ATE_COV.1 覆盖证据	√	—	—
	ATE_COV.2 覆盖分析	—	√	√
	ATE_DPT.1 测试:基本设计	—	√	—
	ATE_DPT.2 测试:安全执行模块	—	—	√
	ATE_FUN.1 功能测试	√	√	√
	ATE_IND.2 独立测试—抽样	√	√	√

表 9（续）

保障类	保障组件	评估保障级		
		EAL2	EAL3	EAL4
脆弱性分析	AVA_VAN.2 脆弱性分析	√	√	—
	AVA_VAN.3 关注点脆弱性分析	—	—	√
注：√ 代表在该评估保障级下包括的安全保障组件。 — 代表在该评估保障级下未包括的安全保障组件。				

7.3.2 开发（ADV 类）

7.3.2.1 安全架构描述（ADV_ARC.1）

开发者行为元素：

ADV_ARC.1.1D 开发者应设计并实现 TOE，确保 TSF 的安全特性不可旁路。

ADV_ARC.1.2D 开发者应设计并实现 TSF，以防止不可信主体的破坏。

ADV_ARC.1.3D 开发者应提供 TSF 安全架构的描述。

内容和形式元素：

ADV_ARC.1.1C 安全架构的描述应与在 TOE 设计文档中对 SFR-执行的抽象描述的级别一致。

ADV_ARC.1.2C 安全架构的描述应描述与安全功能要求一致的 TSF 安全域。

ADV_ARC.1.3C 安全架构的描述应描述 TSF 初始化过程为何是安全的。

ADV_ARC.1.4C 安全架构的描述应论证 TSF 可防止被破坏。

ADV_ARC.1.5C 安全架构的描述应论证 TSF 可防止 SFR-执行的功能被旁路。

评估者行为元素：

ADV_ARC.1.1E 评估者应确认提供的信息符合证据的内容和形式要求。

7.3.2.2 安全执行功能规范（ADV_FSP.2）

开发者行为元素：

ADV_FSP.2.1D 开发者应提供一个功能规范。

ADV_FSP.2.2D 开发者应提供功能规范到安全功能要求的追溯。

内容和形式元素：

ADV_FSP.2.1C 功能规范应完整地描述 TSF。

ADV_FSP.2.2C 功能规范应描述所有的 TSFI 的目的和使用方法。

ADV_FSP.2.3C 功能规范应识别和描述每个 TSFI 相关的所有参数。

ADV_FSP.2.4C 对于每个 SFR-执行 TSFI，功能规范应描述 TSFI 相关的 SFR-执行行为。

ADV_FSP.2.5C 对于 SFR-执行 TSFI，功能规范应描述由 SFR-执行行为相关处理而引起的直接错误消息。

ADV_FSP.2.6C 功能规范应论证安全功能要求到 TSFI 的追溯。

评估者行为元素：

ADV_FSP.2.1E 评估者应确认所提供的信息满足证据的内容和形式的所有要求。

ADV_FSP.2.2E 评估者应确定功能规范是安全功能要求的一个准确且完备的实例化。

7.3.2.3 带完整摘要的功能规范(ADV_FSP.3)

开发者行为元素:

ADV_FSP.3.1D 开发者应提供一个功能规范。

ADV_FSP.3.2D 开发者应提供功能规范到安全功能要求的追溯。

内容和形式元素:

ADV_FSP.3.1C 功能规范应完全描述 TSF。

ADV_FSP.3.2C 功能规范应描述所有的 TSFI 的目的和使用方法。

ADV_FSP.3.3C 功能规范应识别和描述每个 TSFI 相关的所有参数。

ADV_FSP.3.4C 对于每个 SFR-执行 TSFI,功能规范应描述 TSFI 相关的 SFR-执行行为。

ADV_FSP.3.5C 对于每个 SFR-执行 TSFI,功能规范应描述与 TSFI 的调用相关的安全实施行为和异常而引起的直接错误消息。

ADV_FSP.3.6C 功能规范需总结与每个 TSFI 相关的 SFR-支撑和 SFR-无关的行为。

ADV_FSP.3.7C 功能规范应论证安全功能要求到 TSFI 的追溯。

评估者行为元素:

ADV_FSP.3.1E 评估者应确认所提供的信息满足证据的内容和形式的所有要求。

ADV_FSP.3.2E 评估者应确定功能规范是安全功能要求的一个准确且完备的实例化。

7.3.2.4 完备的功能规范(ADV_FSP.4)

开发者行为元素:

ADV_FSP.4.1D 开发者应提供一个功能规范。

ADV_FSP.4.2D 开发者应提供功能规范到安全功能要求的追溯。

内容和形式元素:

ADV_FSP.4.1C 功能规范应完全描述 TSF。

ADV_FSP.4.2C 功能规范应描述所有的 TSFI 的目的和使用方法。

ADV_FSP.4.3C 功能规范应识别和描述每个 TSFI 相关的所有参数。

ADV_FSP.4.4C 对于每个 SFR-执行 TSFI,功能规范应描述 TSFI 相关的所有行为。

ADV_FSP.4.5C 功能规范应描述可能由每个 TSFI 的调用而引起的所有直接错误消息。

ADV_FSP.4.6C 功能规范应证实安全功能要求到 TSFI 的追溯。

评估者行为元素:

ADV_FSP.4.1E 评估者应确认所提供的信息满足证据的内容和形式的所有要求。

ADV_FSP.4.2E 评估者应确定功能规范是安全功能要求的一个准确且完备的实例化。

7.3.2.5 TSF 实现表示(ADV_IMP.1)

开发者行为元素:

ADV_IMP.1.1D 开发者应为全部 TSF 提供实现表示。

ADV_IMP.1.2D 开发者应提供 TOE 设计描述与实现表示示例之间的映射。

内容和形式元素:

ADV_IMP.1.1C 实现表示应按详细级别定义 TSF,且详细程度达到无需进一步设计就能生成 TSF 的程度。

ADV_IMP.1.2C 实现表示应以开发人员使用的形式提供。

ADV_IMP.1.3C TOE 设计描述与实现表示示例之间的映射应能证明他们的一致性。

评估者行为元素:

ADV_IMP.1.1E 对于选取的实现表示示例，评估者应确认提供的信息满足证据的内容和形式的所有要求。

7.3.2.6 基础设计（ADV_TDS.1）

开发者行为元素：

ADV_TDS.1.1D 开发者应提供 TOE 的设计。

ADV_TDS.1.2D 开发者应提供从功能规范的 TSFI 到 TOE 设计中获取到的最低层分解的映射。

内容和形式元素：

ADV_TDS.1.1C 设计应根据子系统描述 TOE 的结构。

ADV_TDS.1.2C 设计应标识 TSF 的所有子系统。

ADV_TDS.1.3C 设计应对每一个 SFR-支撑或 SFR-无关的 TSF 子系统的行为进行足够详细的描述，以确定它不是 SFR-执行。

ADV_TDS.1.4C 设计应概括 SFR-执行子系统的 SFR-执行行为。

ADV_TDS.1.5C 设计应描述 TSF 的 SFR-执行子系统间的相互作用和 TSF 的 SFR-执行子系统与其他 TSF 子系统间的相互作用。

ADV_TDS.1.6C 映射关系应证实 TOE 设计中描述的所有行为能够映射到调用它的 TSFI。

评估者行为元素：

ADV_TDS.1.1E 评估者应确认提供的信息满足证据的内容与形式的所有要求。

ADV_TDS.1.2E 评估者应确定设计是所有安全功能要求的正确且完备的实例。

7.3.2.7 结构化设计（ADV_TDS.2）

开发者行为元素：

ADV_TDS.2.1D 开发者应提供 TOE 的设计。

ADV_TDS.2.2D 开发者应提供从功能规范的 TSFI 到 TOE 设计中获取到的最低层分解的映射。

内容和形式元素：

ADV_TDS.2.1C 设计应根据子系统描述 TOE 的结构。

ADV_TDS.2.2C TSF 内部描述应证明指定的整个 TSF 结构合理。

ADV_TDS.2.3C 设计应对每一个 TSF 的 SFR-无关子系统的行为进行足够详细的描述，以确定它是 SFR-无关。

ADV_TDS.2.4C 设计应描述 SFR-执行子系统的 SFR-执行行为。

ADV_TDS.2.5C 设计应概括 SFR-执行子系统的 SFR-支撑和 SFR-无关行为。

ADV_TDS.2.6C 设计应概括 SFR-支撑子系统的行为。

ADV_TDS.2.7C 设计应描述 TSF 所有子系统间的相互作用。

ADV_TDS.2.8C 映射关系应证实 TOE 设计中描述的所有行为能够映射到调用它的 TSFI。

评估者行为元素：

ADV_TDS.2.1E 评估者应确认提供的信息满足证据的内容与形式的所有要求。

ADV_TDS.2.2E 评估者应确定设计是所有安全功能要求的正确且完全的实例。

7.3.2.8 基础模块设计（ADV_TDS.3）

开发者行为元素：

ADV_TDS.3.1D 开发者应提供 TOE 的设计。

ADV_TDS.3.2D 开发者应提供从功能规范的 TSFI 到 TOE 设计中获取到的最低层分解的映射。

内容和形式元素：

ADV_TDS.3.1C 设计应根据子系统描述 TOE 的结构。

ADV_TDS.3.2C 设计应根据模块描述 TSF。

ADV_TDS.3.3C 设计应标识 TSF 的所有子系统。

ADV_TDS.3.4C 设计应描述每一个 TSF 子系统。

ADV_TDS.3.5C 设计应描述 TSF 所有子系统间的相互作用。

ADV_TDS.3.6C 设计应提供 TSF 子系统到 TSF 模块间的映射关系。

ADV_TDS.3.7C 设计应描述每一个 SFR-执行模块，包括它的目的及与其他模块间的相互作用。

ADV_TDS.3.8C 设计应描述每一个 SFR-执行模块，包括它的安全功能要求相关接口、其他接口的返回值、与其他模块间的相互作用及调用的接口。

ADV_TDS.3.9C 设计应描述每一个 SFR-支撑或 SFR-无关模块，包括它的的目的及与其他模块间的相互作用。

ADV_TDS.3.10C 映射关系应论证 TOE 设计中描述的所有行为能够映射到调用它的 TSFI。

评估者行为元素：

ADV_TDS.3.1E 评估者应确认提供的信息满足证据的内容与形式的所有要求。

ADV_TDS.3.2E 评估者应确定设计是所有安全功能要求的正确且完全的实例。

7.3.3 指导性文档(AGD 类)

7.3.3.1 操作用户指南(AGD_OPE.1)

开发者行为元素：

AGD_OPE.1.1D 开发者应提供操作用户指南。

内容和形式元素：

AGD_OPE.1.1C 操作用户指南应对每一种用户角色在安全处理环境中应被控制的用户可访问的功能和特权进行描述，包含适当的警示信息。

AGD_OPE.1.2C 操作用户指南应对每一种用户角色怎样以安全的方式使用 TOE 提供的可用接口进行描述。

AGD_OPE.1.3C 操作用户指南应对每一种用户角色可用的功能和接口、尤其是受用户控制的所有安全参数进行描述，适当时应指明安全值。

AGD_OPE.1.4C 操作用户指南应对每一种用户角色与需要执行的用户可访问功能有关的每一种安全相关事件明确说明，包括改变 TSF 所控制实体的安全特性。

AGD_OPE.1.5C 操作用户指南应标识 TOE 运行的所有可能状态(包括操作导致的失败或者操作性错误)，他们与维持安全运行之间的因果关系。

AGD_OPE.1.6C 操作用户指南应对每一种用户角色为了充分实现 ST 中描述的运行环境安全目的所应执行的安全策略进行描述。

AGD_OPE.1.7C 操作用户指南应是明确和合理的。

评估者行为元素：

AGD_OPE.1.1E 评估者应确认所提供的信息满足证据的内容和形式的所有要求。

7.3.3.2 准备程序(AGD_PRE.1)

开发者行为元素：

AGD_PRE.1.1D 开发者应提供 TOE，包括它的准备程序。

内容和形式元素：

AGD_PRE.1.1C 准备程序应描述与开发者交付程序相一致的安全接收所交付 TOE 必需的所有

步骤。

AGD_PRE.1.2C 准备程序应描述安全安装 TOE 以及安全准备与 ST 中描述的运行环境安全目的一致的运行环境必需的所有步骤。

评估者行为元素：

AGD_PRE.1.1E 评估者应确认所提供的信息满足证据的内容和形式的所有要求。

AGD_PRE.1.2E 评估者应运用准备程序确认 TOE 运行能被安全的准备。

7.3.4 生命周期支持(ALC 类)

7.3.4.1 CM 系统的使用(ALC_CMC.2)

开发者行为元素：

ALC_CMC.2.1D 开发者应提供 TOE 及其参照号。

ALC_CMC.2.2D 开发者应提供 CM 文档。

ALC_CMC.2.3D 开发者应使用 CM 系统。

内容和形式元素：

ALC_CMC.2.1C 应给 TOE 标记唯一参照号。

ALC_CMC.2.2C CM 文档应描述用于唯一标识配置项的方法。

ALC_CMC.2.3C CM 系统应唯一标识所有配置项。

评估者行为元素：

ALC_CMC.2.1E 评估者应确认所提供的信息满足证据的内容和形式的所有要求。

7.3.4.2 授权控制(ALC_CMC.3)

开发者行为元素：

ALC_CMC.3.1D 开发者应提供 TOE 及其参照号。

ALC_CMC.3.2D 开发者应提供 CM 文档。

ALC_CMC.3.3D 开发者应使用 CM 系统。

内容和形式元素：

ALC_CMC.3.1C 应给 TOE 标记唯一参照号。

ALC_CMC.3.2C CM 文档应描述用于唯一标识配置项的方法。

ALC_CMC.3.3C CM 系统应唯一标识所有配置项。

ALC_CMC.3.4C CM 系统应提供措施使得只能对配置项进行授权变更。

ALC_CMC.3.5C CM 文档应包括一个 CM 计划。

ALC_CMC.3.6C CM 计划应描述 CM 系统是如何应用于 TOE 的开发过程。

ALC_CMC.3.7C 证据应证实所有配置项都正在 CM 系统下进行维护。

ALC_CMC.3.8C 证据应证实 CM 系统的运行与 CM 计划是一致的。

评估者行为元素：

ALC_CMC.3.1E 评估者应确认所提供的信息满足证据的内容和形式的所有要求。

7.3.4.3 生产支持和接受程序及其自动化(ALC_CMC.4)

开发者行为元素：

ALC_CMC.4.1D 开发者应提供 TOE 及其参照号。

ALC_CMC.4.2D 开发者应提供 CM 文档。

ALC_CMC.4.3D 开发者应使用 CM 系统。

内容和形式元素：

ALC_CMC.4.1C 应给 TOE 标记唯一参照号。

ALC_CMC.4.2C CM 文档应描述用于唯一标识配置项的方法。

ALC_CMC.4.3C CM 系统应唯一标识所有配置项。

ALC_CMC.4.4C CM 系统应提供自动化的措施使得只能对配置项进行授权变更。

ALC_CMC.4.5C CM 系统应以自动化的方式支持 TOE 的生产。

ALC_CMC.4.6C CM 文档应包括 CM 计划。

ALC_CMC.4.7C CM 计划应描述 CM 系统是如何应用于 TOE 的开发的。

ALC_CMC.4.8C CM 计划应描述用来接受修改过的或新创建的作为 TOE 组成部分的配置项的程序。

ALC_CMC.4.9C 证据应论证所有配置项都正在 CM 系统下进行维护。

ALC_CMC.4.10C 证据应论证 CM 系统的运行与 CM 计划是一致的。

评估者行为元素：

ALC_CMC.4.1E 评估者应确认所提供的信息满足证据的内容和形式的所有要求。

7.3.4.4 部分 TOE CM 覆盖(ALC_CMS.2)

开发者行为元素：

ALC_CMS.2.1D 开发者应提供 TOE 配置项列表。

内容和形式元素：

ALC_CMS.2.1C 配置项列表应包括：TOE 本身、安全保障要求的评估证据和 TOE 的组成部分。

ALC_CMS.2.2C 配置项列表应唯一标识配置项。

ALC_CMS.2.3C 对于每一个 TSF 相关的配置项，配置项列表应简要说明该配置项的开发者。

评估者行为元素：

ALC_CMS.2.1E 评估者应确认所提供的信息满足证据的内容和形式的所有要求。

7.3.4.5 实现表示 CM 覆盖(ALC_CMS.3)

开发者行为元素：

ALC_CMS.3.1D 开发者应提供 TOE 配置项列表。

内容和形式元素：

ALC_CMS.3.1C 配置项列表应包括：TOE 本身、安全保障要求的评估证据、TOE 的组成部分和实现表示。

ALC_CMS.3.2C 配置项列表应唯一标识配置项。

ALC_CMS.3.3C 对于每一个 TSF 相关的配置项，配置项列表应简要说明该配置项的开发者。

评估者行为元素：

ALC_CMS.3.1E 评估者应确认所提供的信息满足证据的内容和形式的所有要求。

7.3.4.6 问题跟踪 CM 覆盖(ALC_CMS.4)

开发者行为元素：

ALC_CMS.4.1D 开发者应提供 TOE 配置项列表。

内容和形式元素：

ALC_CMS.4.1C 配置项列表应包括：TOE 本身、安全保障要求的评估证据、TOE 的组成部分、实现表示和安全缺陷报告及其解决状态。

ALC_CMS.4.2C 配置项列表应唯一标识配置项。

ALC_CMS.4.3C 对于每一个 TSF 相关的配置项，配置项列表应简要说明该配置项的开发者。

评估者行为元素：

ALC_CMS.4.1E 评估者应确认所提供的信息满足证据的内容和形式的所有要求。

7.3.4.7 交付程序(ALC_DEL.1)

开发者行为元素：

ALC_DEL.1.1D 开发者应将把 TOE 或其部分交付给消费者的程序文档化。

ALC_DEL.1.2D 开发者应使用交付程序。

内容和形式元素：

ALC_DEL.1.1C 交付文档应描述，在向消费者分发 TOE 版本时，用以维护安全性所必需的所有程序。

评估者行为元素：

ALC_DEL.1.1E 评估者应确认所提供的信息满足证据的内容和形式的所有要求。

7.3.4.8 安全措施标识(ALC_DVS.1)

开发者行为元素：

ALC_DVS.1.1D 开发者应提供开发安全文档。

内容和形式元素：

ALC_DVS.1.1C 开发安全文档应描述在 TOE 的开发环境中，保护 TOE 设计和实现的保密性和完整性所必需的所有物理的、程序的、人员的及其他方面的安全措施。

评估者行为元素：

ALC_DVS.1.1E 评估者应确认所提供的信息满足证据的内容和形式的所有要求。

ALC_DVS.1.2E 评估者应确认安全措施正在被使用。

7.3.4.9 开发者定义的生命周期模型(ALC_LCD.1)

开发者行为元素：

ALC_LCD.1.1D 开发者应建立一个生命周期模型，用于 TOE 的开发和维护。

ALC_LCD.1.2D 开发者应提供生命周期定义文档。

内容和形式元素：

ALC_LCD.1.1C 生命周期定义文档应描述用于开发和维护 TOE 的模型。

ALC_LCD.1.2C 生命周期模型应为 TOE 的开发和维护提供必要的控制。

评估者行为元素：

ALC_LCD.1.1E 评估者应确认所提供的信息满足证据的内容和形式的所有要求。

7.3.4.10 明确定义的开发工具(ALC_TAT.1)

开发者行为元素：

ALC_TAT.1.1D 开发者应标识用于开发 TOE 的每个工具。

ALC_TAT.1.2D 开发者应在文档中描述每个开发工具所选取的实现依赖选项。

内容和形式元素：

ALC_TAT.1.1C 用于实现的每个开发工具都应是明确定义的。

ALC_TAT.1.2C 每个开发工具的文档应无歧义地定义所有语句和实现用到的所有协定与命令的含义。

ALC_TAT.1.3C 每个开发工具的文档应无歧义地定义所有实现依赖选项的含义。

评估者行为元素：

ALC_TAT.1.1E 评估者应确认所提供的信息满足证据的内容和形式的所有要求。

7.3.5 安全目标评估(ASE 类)

7.3.5.1 符合性声明(ASE_CCL.1)

开发者行为元素：

ASE_CCL.1.1D 开发者应提供符合性声明。

ASE_CCL.1.2D 开发者应提供符合性声明的基本原理。

内容和形式元素：

ASE_CCL.1.1C ST 应声明其与 GB/T 18336.1—2015、GB/T 18336.2—2015、GB/T 18336.3—2015 的符合性，标识出 ST 和 TOE 的符合性遵从的 GB/T 18336.1—2015、GB/T 18336.2—2015、GB/T 18336.3—2015 的版本。

ASE_CCL.1.2C 符合性声明应描述 ST 与 GB/T 18336.2—2015 的符合性，无论是与 GB/T 18336.2—2015 相符或还是对 GB/T 18336.2—2015 的扩展。

ASE_CCL.1.3C 符合性声明应描述 ST 与 GB/T 18336.3—2015 的符合性，无论是与 GB/T 18336.3—2015 相符还是对 GB/T 18336.3—2015 的扩展。

ASE_CCL.1.4C 符合性声明应与扩展组件定义是相符的。

ASE_CCL.1.5C 符合性声明应标识 ST 声明遵从的所有 PP 和安全要求包。

ASE_CCL.1.6C 符合性声明应描述 ST 和包的符合性，无论是与包的相符或是与扩展包相符。

ASE_CCL.1.7C 符合性声明的基本原理应证实 TOE 类型与符合性声明所遵从的 PP 中的 TOE 类型是相符的。

ASE_CCL.1.8C 符合性声明的基本原理应证实安全问题定义的陈述与符合性声明所遵从的 PP 中的安全问题定义陈述是相符的。

ASE_CCL.1.9C 符合性声明的基本原理应证实安全目的陈述与符合性声明所遵从的 PP 中的安全目的陈述是相符的。

ASE_CCL.1.10C 符合性声明的基本原理应证实安全要求的陈述与符合性声明所遵从的 PP 中的安全要求的陈述是相符的。

评估者行为元素：

ASE_CCL.1.1E 评估者应确认所提供的信息满足证据的内容和形式的所有要求。

7.3.5.2 扩展组件定义(ASE_ECD.1)

开发者行为元素：

ASE_ECD.1.1D 开发者应提供安全要求的陈述。

ASE_ECD.1.2D 开发者应提供扩展组件的定义。

内容和形式元素：

ASE_ECD.1.1C 安全要求陈述应标识所有扩展的安全要求。

ASE_ECD.1.2C 扩展组件定义应为每一个扩展的安全要求定义一个扩展的组件。

ASE_ECD.1.3C 扩展组件定义应描述每个扩展的组件与已有组件、族和类的关联性。

ASE_ECD.1.4C 扩展组件定义应使用已有的组件、族、类和方法学作为陈述的模型。

ASE_ECD.1.5C 扩展组件应由可测量的和客观的元素组成，以便于证实这些元素之间的符合性或不符合性。

评估者行为元素：

ASE_ECD.1.1E 评估者应确认所提供的信息满足证据的内容和形式的所有要求。

ASE_ECD.1.2E 评估者应确认扩展组件不能利用已经存在的组件明确的表达。

7.3.5.3 ST 引言(ASE_INT.1)

开发者行为元素：

ASE_INT.1.1D 开发者应提供 ST 引言。

内容和形式元素：

ASE_INT.1.1C ST 引言应包含 ST 参照号，TOE 参照号，TOE 概述和 TOE 描述。

ASE_INT.1.2C ST 参照号应唯一标识 ST。

ASE_INT.1.3C TOE 参照号应标识 TOE。

ASE_INT.1.4C TOE 概述应概括 TOE 的用法及其主要安全特性。

ASE_INT.1.5C TOE 概述应标识 TOE 类型。

ASE_INT.1.6C TOE 概述应标识任何 TOE 要求的非 TOE 范围内的硬件/软件/固件。

ASE_INT.1.7C TOE 描述应描述 TOE 的物理范围。

ASE_INT.1.8C TOE 描述应描述 TOE 的逻辑范围。

评估者行为元素：

ASE_INT.1.1E 评估者应确认所提供的信息满足证据的内容和形式的所有要求。

ASE_INT.1.2E 评估者应确认 TOE 参考、TOE 概述和 TOE 描述是相互一致的。

7.3.5.4 安全目的(ASE_OBJ.2)

开发者行为元素：

ASE_OBJ.2.1D 开发者应提供安全目的的陈述。

ASE_OBJ.2.2D 开发者应提供安全目的的基本原理。

内容和形式元素：

ASE_OBJ.2.1C 安全目的的陈述应描述 TOE 的安全目的和运行环境安全目的。

ASE_OBJ.2.2C 安全目的基本原理应追溯到 TOE 的每一个安全目的，以便于能追溯到安全目的所对抗的威胁及安全目的实施的组织安全策略。

ASE_OBJ.2.3C 安全目的基本原理应追溯到运行环境的每一个安全目的，以便于能追溯到安全目的所对抗的威胁、安全目的实施的组织安全策略和安全目的支持的假设。

ASE_OBJ.2.4C 安全目的基本原理应证实安全目的能抵抗所有威胁。

ASE_OBJ.2.5C 安全目的基本原理应证实安全目的执行所有组织安全策略。

ASE_OBJ.2.6C 安全目的基本原理应证实运行环境安全目的支持所有的假设。

评估者行为元素：

ASE_OBJ.2.1E 评估者应确认所提供的信息满足证据的内容和形式的所有要求。

7.3.5.5 推导出的安全要求(ASE_REQ.2)

开发者行为元素：

ASE_REQ.2.1D 开发者应提供安全要求的陈述。

ASE_REQ.2.2D 开发者应提供安全要求的基本原理。

内容和形式元素：

ASE_REQ.2.1C 安全要求的陈述应描述安全功能要求和安全保障要求。

ASE_REQ.2.2C 应对安全功能要求和安全保障要求中使用的所有主体、客体、操作、安全属性、外部实体及其他术语进行定义。

ASE_REQ.2.3C 安全要求的陈述应对安全要求的所有操作进行标识。

ASE_REQ.2.4C 所有操作应被正确地执行。

ASE_REQ.2.5C 应满足安全要求间的依赖关系，或者安全要求基本原理应论证不需要满足某个依赖关系。

ASE_REQ.2.6C 安全要求基本原理应描述每一个安全功能要求可追溯至对应的 TOE 安全目的。

ASE_REQ.2.7C 安全要求基本原理应证实安全功能要求可满足所有的 TOE 安全目的。

ASE_REQ.2.8C 安全要求基本原理应说明选择安全保障要求的理由。

ASE_REQ.2.9C 安全要求的陈述应是内在一致的。

评估者行为元素：

ASE_REQ.2.1E 评估者应确认所提供的信息满足证据的内容和形式的所有要求。

7.3.5.6 安全问题定义(ASE_SPD.1)

开发者行为元素：

ASE_SPD.1.1D 开发者应提供安全问题定义。

内容和形式元素：

ASE_SPD.1.1C 安全问题定义应描述威胁。

ASE_SPD.1.2C 所有的按摩器威胁都应根据威胁主体、资产和敌对行为进行描述。

ASE_SPD.1.3C 安全问题定义应描述组织安全策略。

ASE_SPD.1.4C 安全问题定义应描述 TOE 运行环境的相关假设。

评估者行为元素：

ASE_SPD.1.1E 评估者应确认所提供的信息满足证据的内容和形式的所有要求。

7.3.5.7 TOE 概要规范(ASE_TSS.1)

开发者行为元素：

ASE_TSS.1.1D 开发者应提供 TOE 概要规范。

内容和形式元素：

ASE_TSS.1.1C TOE 概要规范应描述 TOE 是如何满足每一项安全功能要求的。

评估者行为元素：

ASE_TSS.1.1E 评估者应确认所提供的信息满足证据的内容和形式的所有要求。

ASE_TSS.1.2E 评估者应确认 TOE 概要规范与 TOE 概述、TOE 描述是一致的。

7.3.6 测试(ATE 类)

7.3.6.1 覆盖证据(ATE_COV.1)

开发者行为元素：

ATE_COV.1.1D 开发者应提供测试覆盖的证据。

内容和形式元素：

ATE_COV.1.1C 测试覆盖的证据应表明测试文档中的测试与功能规范中的 TSF 接口之间的对应性。

评估者行为元素：

ATE_COV.1.1E 评估者应确认所提供的信息满足证据的所有内容和形式要求。

7.3.6.2 覆盖分析(ATE_COV.2)

开发者行为元素：

ATE_COV.2.1D 开发者应提供对测试覆盖的分析。

内容和形式元素：

ATE_COV.2.1C 测试覆盖分析应论证测试文档中的测试与功能规范中 TSF 接口之间的对应性。

ATE_COV2.2C 测试覆盖分析应论证已经对功能规范中的所有 TSF 接口都进行了测试。

评估者行为元素：

ATE_COV.2.1E 评估者应确认所提供的信息满足证据内容和形式的所有要求。

7.3.6.3 测试：基本设计（ATE_DPT.1）

开发者行为元素：

ATE_DPT.1.1D 开发者应提供测试深度分析。

内容和形式元素：

ATE_DPT.1.1C 测试深度分析应证实测试文档中的测试与 TOE 设计中 TSF 子系统之间的对应性。

ATE_DPT.1.2C 测试深度分析应证实 TOE 设计中的所有 TSF 子系统都已经进行过测试。

评估者行为元素：

ATE_DPT1.1E 评估者应确认所提供的信息满足证据内容和形式的所有要求。

7.3.6.4 测试：安全执行模块（ATE_DPT.2）

开发者行为元素：

ATE_DPT.2.1D 开发者应提供测试深度分析。

内容和形式元素：

ATE_DPT.2.1C 深度测试分析应论证测试文档中的测试与 TOE 设计中的 TSF 子系统、SFR-执行模块之间的一致性。

ATE_DPT.2.2C 测试深度分析应论证 TOE 设计中的所有 TSF 子系统都已经进行过测试。

ATE_DPT.2.3C 测试深度分析应论证 TOE 设计中的 SFR-执行模块都已经进行过测试。

评估者行为元素：

ATE_DPT.2.1E 评估者应确认所提供的信息满足证据内容和形式的所有要求。

7.3.6.5 功能测试（ATE_FUN.1）

开发者行为元素：

ATE_FUN.1.1D 开发者应测试 TSF，并文档化测试结果。

ATE_FUN.1.2D 开发者应提供测试文档。

内容和形式元素：

ATE_FUN.1.1C 测试文档应包括测试计划、预期的测试结果和实际的测试结果。

ATE_FUN.1.2C 测试计划应标识要执行的测试并描述执行每个测试的方案，这些方案应包括对于其他测试结果的任何顺序依赖性。

ATE_FUN.1.3C 预期的测试结果应指出测试成功执行后的预期输出。

ATE_FUN.1.4C 实际的测试结果应和预期的测试结果一致。

评估者行为元素：

ATE_FUN.1.1E 评估者应确认所提供的信息满足证据内容和形式的所有要求。

7.3.6.6 独立测试—抽样（ATE_IND.2）

开发者行为元素：

ATE_IND.2.1D 开发者应提供用于测试的 TOE。

内容和形式元素：

ATE_IND.2.1C TOE 应适合测试。

ATE_IND.2.2C 开发者应提供一组与开发者 TSF 功能测试中同等的一系列资源。

评估者行为元素：

ATE_IND.2.1E 评估者应确认所提供的信息满足证据的内容和形式的所有要求。

ATE_IND.2.2E 评估者应执行测试文档中的测试样本，以验证开发者的测试结果。

ATE_IND.2.3E 评估者应测试 TSF 的一个子集以确认 TSF 按照规定运行。

7.3.7 脆弱性评定（AVA 类）

7.3.7.1 脆弱性分析（AVA_VAN.2）

开发者行为元素：

AVA_VAN.2.1D 开发者应提供用于测试的 TOE。

内容和形式元素：

AVA_VAN.2.1C TOE 应适合测试。

评估者行为元素：

AVA_VAN.2.1E 评估者应确认所提供的信息满足证据的内容和形式的所有要求。

AVA_VAN.2.2E 评估者应执行公共领域的调查以标识 TOE 的潜在脆弱性。

AVA_VAN.2.3E 评估者应执行独立的 TOE 脆弱性分析去标识 TOE 潜在的脆弱性，在分析过程中使用指导性文档、功能规范、TOE 设计和安全结构描述。

AVA_VAN.2.4E 评估者应基于已标识的潜在脆弱性实施渗透性测试，确定 TOE 能抵抗具有基本攻击潜力的攻击者的攻击。

7.3.7.2 关注点脆弱性分析（AVA_VAN.3）

开发者行为元素：

AVA_VAN.3.1D 开发者应提供用于测试的 TOE。

内容和形式元素：

AVA_VAN.3.1C TOE 应适合测试。

评估者行为元素：

AVA_VAN.3.1E 评估者应确认所提供的信息满足证据的内容和形式的所有要求。

AVA_VAN.3.2E 评估者应执行公共领域的调查以标识 TOE 的潜在脆弱性。

AVA_VAN.3.3E 评估者应针对 TOE 执行一个独立的脆弱性分析去标识 TOE 中潜在的脆弱性，在分析过程中使用指导性文档、功能规范、TOE 设计、安全结构描述和实现表示。

AVA_VAN.3.4E 评估者应基于已标识的潜在脆弱性实施渗透性测试，确定 TOE 能抵抗具有增强型基本攻击潜力的攻击者的攻击。

8 基本原理

8.1 安全目的基本原理

8.1.1 概述

每一种威胁、组织安全策略和假设都至少有一个或一个以上的安全目的与其对应，以保证安全问题的解决方案是完备的。当然不存在任何一个安全目的没有与其对应的威胁、组织安全策略和假设，这证

明了每个安全目的都是必要的;没有多余的安全目的不对应威胁、组织安全策略和假设,这说明安全目的是充分的。

8.1.2 威胁对应安全目的

表 10 说明了 TOE 安全目的能应对所有可能的威胁。

表 10 威胁与 TOE 安全目的的对应关系

威胁	TOE 安全目的																	
	O.ACCESS_HISTORY	O.ACCESS.LBAC	O.ADMIN_GUIDANCE	O.ADMIN_ROLE	O.AUDIT_GENERATION	O.AUDIT_PROTECTION	O.AVAIL	O.CONFIG	O.CRYPTOGRAGHY	O.DOCUMENTED_DESIGN	O.FUNCTIONAL_TEST	O.INTERNAL_TOE_DOMAINS	O.MANAGE	O.RESIDUAL_INFORMATION	O.RESOURCE_SHARING	O.TOE_ACCESS	O.TRUSTED_PATH	O.VULNERABILITY_ANALYSIS
管理员误操作 T.MISOPERATION_ADMIN	—	—	√	√	—	—	—	—	—	—	—	—	√	—	—	—	—	—
审计机制失效 T.AUDIT_FAILURE	—	—	—	—	√	√	—	—	—	—	—	—	—	√	—	—	—	—
密码攻击 T.CRYPTO_COMPROMISE	—	—	—	—	—	—	—	—	√	√	—	—	—	√	—	—	—	—
数据传输窃听 T.EAVESDROP	—	—	—	—	—	—	—	—	√	—	—	—	—	—	—	—	√	—
设计缺陷 T.FLAWED_DESIGN	—	—	—	—	—	—	—	√	—	√	—	—	—	—	—	—	—	√
实现缺陷 T.FLAWED_IMPLEMENTATION	—	—	—	—	—	—	—	√	—	√	√	—	—	—	—	—	—	√
标签数据失控 T.LBAC	—	√	—	√	—	—	—	—	—	—	—	—	—	—	—	—	—	—
假冒授权用户 T.MASQUERADE	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	√	—	—
测试缺陷 T.POOR_TEST	—	—	—	—	—	—	—	—	—	√	√	—	—	—	—	—	—	√
残余信息利用 T.RESIDUAL_DATA	—	—	—	—	—	—	—	—	—	—	—	—	—	√	—	—	—	—
安全功能失效 T.TSF_COMPROMISE	—	—	—	—	—	—	—	—	—	—	—	√	√	√	—	—	√	—
非授权访问 T.UNAUTHORIZED_ACCESS	√	—	—	—	—	—	—	—	—	—	—	—	√	—	—	√	—	—
服务失效 T.UNAVAILABILITY	—	—	—	—	—	—	√	—	—	—	—	—	—	—	√	—	—	—
未标识动作 T.UNIDENTIFIED_ACTIONS	—	—	—	—	√	√	—	—	—	—	—	—	—	—	—	—	—	—
管理员误操作 T.MISOPERATION_ADMIN	—	—	√	√	—	—	—	—	—	—	—	—	√	—	—	—	—	—
审计机制失效 T.AUDIT_FAILURE	—	—	—	—	√	√	—	—	—	—	—	—	—	√	—	—	—	—
密码攻击 T.CRYPTO_COMPROMISE	—	—	—	—	—	—	—	—	√	√	—	—	—	√	—	—	—	—
数据传输窃听 T.EAVESDROP	—	—	—	—	—	—	—	—	√	—	—	—	—	—	—	—	√	—
设计缺陷 T.FLAWED_DESIGN	—	—	—	—	—	—	—	√	—	√	—	—	—	—	—	—	—	√
实现缺陷 T.FLAWED_IMPLEMENTATION	—	—	—	—	—	—	—	√	—	√	√	—	—	—	—	—	—	√
标签数据失控 T.LBAC	—	√		√	—	—	—	—	—	—	—	—	—	—	—	—	—	—

表 10（续）

威胁	TOE 安全目的																
	O.ACCESS_HISTORY	O.ACCESS.LBAC	O.ADMIN_GUIDANCE	O.ADMIN_ROLE	O.AUDIT_GENERATION	O.AUDIT_PROTECTION	O.AVAIL	O.CONFIG	O.CRYPTOGRAGHY	O.DOCUMENTED_DESIGN	O.FUNCTIONAL_TEST	O.INTERNAL_TOE_DOMAINS	O.MANAGE	O.RESIDUAL_INFORMATION	O.RESOURCE_SHARING	O.TOE_ACCESS	O.TRUSTED_PATH	O.VULNERABILITY_ANALYSIS
假冒授权用户 T.MASQUERADE	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	√	—	—
测试缺陷 T.POOR_TEST	—	—	—	—	—	—	—	—	—	√	√	—	—	—	—	—	—	√
残余信息利用 T.RESIDUAL_DATA	—	—	—	—	—	—	—	—	—	—	—	—	—	√	—	—	—	—
安全功能失效 T.TSF_COMPROMISE	—	—	—	—	—	—	—	—	—	—	—	√	√	√	—	—	√	—
非授权访问 T.UNAUTHORIZED_ACCESS	√	—	—	—	—	—	—	—	—	—	—	—	√	—	—	√	—	—
服务失效 T.UNAVAILABILITY	—	—	—	—	—	—	√	—	—	—	—	—	—	—	√	—	—	—
未标识动作 T.UNIDENTIFIED_ACTIONS	—	—	—	—	√	√	—	—	—	—	—	—	—	—	—	—	—	—

注：√ 代表有对应关系。
— 代表无对应关系。

表 11 说明了 DBMS 运行环境安全目的能应对所有可能的威胁。

表 11 威胁与环境安全目的的对应关系

威胁	环境安全目的											
	OE.AUDIT_PROTECTION	OE.AUDIT_REVIEW	OE.CONFIG	OE.DOMAIN_SEPARATION	OE.NO_GENERAL_PURPOSE	OE.NO_HARM	OE.SELF_PROTECTION	OE.SECURE_COMMS	OE.TIME_STAMPS	OE.TOE_ACCESS	OE.TOE_NO_BYPASS	OE.TRUST_IT
管理员误操作 T.MISOPERATION_ADMIN	—	—	—	—	√	√	—	—	—	—	—	—
审计机制失效 T.AUDIT_FAILURE	√	—	—	—	—	—	√	—	—	—	—	—
密码攻击 T.CRYPTO_COMPROMISE	—	—	—	—	—	—	√	—	—	—	—	—
数据传输窃听 T.EAVESDROP	—	—	—	—	—	—	—	√	—	—	—	√

表 11（续）

威胁	环境安全目的											
	OE.AUDIT_PROTECTION	OE.AUDIT_REVIEW	OE.CONFIG	OE.DOMAIN_SEPARATION	OE.NO_GENERAL_PURPOSE	OE.NO_HARM	OE.SELF_PROTECTION	OE.SECURE_COMMS	OE.TIME_STAMPS	OE.TOE_ACCESS	OE.TOE_NO_BYPASS	OE.TRUST_IT
假冒授权用户 T.MASQUERADE	—	—	—	—	—	—	—	—	—	√	√	—
安全功能失效 T.TSF_COMPROMISE	—	—	√	√	—	—	√	—	—	—	—	—
非授权访问 T.UNAUTHORIZED_ACCESS	—	—	—	—	—	—	√	—	—	√	—	—
未标识动作 T.UNIDENTIFIED_ACTIONS	√	√	—	—	—	—	—	—	—	—	—	—

注：√ 代表有对应关系。
— 代表无对应关系。

下面论述每一种威胁对应的安全目的及其原理。

T.MISOPERATION_ADMIN

O.ADMIN_GUIDANCE 确保授权管理员拥有可指导他们以安全方式管理 TOE 的指南文档；O.ADMIN_ROLE 指 TSF 提供职责分离、角色约束等数据库管理角色功能，通过使用最小特权原则可减轻授权管理员失误的影响；O.MANAGE 提供给安全管理员查看授权管理功能和安全功能配置参数的能力，以便对授权管理员可能错误地安装或配置数据库实例组件，或是恶意破坏用户或 DBMS 的安全等行为，进行判断其安全配置与安全策略的一致性，从而消除人为使用和配置安全功能的威胁；OE.NO_GENERAL_PURPOSE 确保在数据库服务器上不会因为未授权软件的安装或 DBMS 相关服务配置端口的引入而产生意外的错误；OE.NO_HARM 通过保证授权管理员是不敌对的、训练有素的（能够合理地管理 DBMS），从而缓解管理员的威胁。

T.AUDIT_FAILURE

O.AUDIT_GENERATION 确保能依据审计策略创建与用户关联的安全相关事件的记录能力。O.AUDIT_PROTECTION 或 OE.AUDIT_PROTECTION 提供保护存储在数据库内或 IT 环境中审计记录的能力；O.RESIDUAL_INFORMATION 防止未经授权的用户读取服务器共享缓存残留的审计记录或跟踪审计，从而保证清除 TSF 中的任何残余审计记录不再需要时不可访问来缓解该威胁；OE.SELF_PROTECTION 通过确保 TSF 及运行环境保护自身免于用户的攻击，有助于对抗恶意用户或进程可能执行的访问、修改或删除审计记录操作，从而导致审计记录丢失或被篡改，也有可能阻止未来审计记录被篡改，从而导致产生掩盖用户的威胁；OE.TIME_STAMPS 保证数据库外部的 IT 环境提供可靠的时间戳。

T.CRYPTO_COMPROMISE

O.CRYPTOGRAGHY 保证数据库存储加密和通信加密功能的可靠性。O.DOCUMENTED_DESIGN 要求数据库密码相关的运算和密钥生成功能进行说明；O.RESIDUAL_INFORMATION 通过保证清除 TSF 中的任何残余数据和在加密密钥不再需要时不可访问来缓解该威胁；OE.SELF_PRO-

TECTION 通过确保 TSF 及运行环境保护自身免于用户的攻击，从而有助于对抗密码相关的威胁。

T.EAVESDROP

O.CRYPTOGRAGHY 加密可以消除数据库与外部实体通信、存储数据读写等数据传输过程中的窃听威胁；O.TRUSTED_PATH 和 OE.TRUST_IT 支撑 DBMS 运行所需的操作系统、外部认证实体等数据库安全性有关的 IT 环境应与 TOE 安全策略和他们之间的关系保持一致，以避免外部实体的不可信导致 DBMS 的安全功能失效；OE.SECURE_COMMS 通过安全的通信线路保护用户和 TSF 数据免于被修改和浏览，从而消除此威胁。

T.FLAWED_DESIGN

O.CONFIG 要求在开发过程中对 DBMS 组件配置及其开发证据进行分析、跟踪和控制，以对抗 TOE 设计任务被重新分配并及时纠正设计中的错误；O.DOCUMENTED_DESIGN 要求 TOE 按照软件工程原理进行开发，所有 DBMS 设计、设计原则和设计技术等得到充分、准确地记录，保证在 TOE 审查评估中能有详细的设计文档；O.VULNERABILITY_ANALYSIS 确保 DBMS 设计进行了针对设计缺陷的独立脆弱性分析，以证明 TOE 的设计和实施中不包含任何明显的缺陷。

T.FLAWED_IMPLEMENTATION

O.CONFIG 要求在整个 TOE 开发过程中对 DBMS 组件配置及其开发证据进行分析、跟踪和控制，以对抗 TOE 实现任务被重新分配并及时纠正实现中的错误　O.DOCUMENTED_DESIGN 确保形式化的 TOE 实现文档满足安全功能设计要求。O.FUNCTIONAL_TEST 增加了通过测试从而发现已经存在于实现中的错误的可能。O.VULNERABILITY_ANALYSIS 确保对实现进行了适当的独立渗透性测试和脆弱性分析，从而证明 TOE 的设计与实现不允许攻击者进行潜在的安全攻击。

T.LBAC

O.ACCESS.LBAC 要求通过 TOE 的标签策略控制数据库对象的访问，它能减轻 T.LBAC 的威胁；O.ADMIN_ROLE 要求 TOE 提供安全管理员角色功能，确保标签策略定义的完整性和一致性。另外 O.ACCESS.LBAC 将支持组织安全策略 P.LBAC。

T.MASQUERADE

O.TOE_ACCESS 确保只有认证用户才能访问 TOE，并保证对 TOE 内部的数据字典数据、用户数据和安全功能组件实施了访问控制措施；OE.TOE_ACCESS 在允许访问 TOE 或通过 TOE 转发的服务前要通过 IT 环境进行身份鉴别；OE.TOE_NO_BYPASS 确保用户访问 TOE 或通过 TOE 转发的某种服务之前 TSF 及其环境应调用所有已配置实施的功能（身份鉴别、访问控制规则等）。

T.POOR_TEST

O.DOCUMENTED_DESIGN 确保规范化的安全功能测试用例集满足 TOE 安全功能设计要求。O.FUNCTIONAL_TEST 确保充分的功能测试被执行，从而证明 TSF 满足安全设计要求，以及 TSF 运行与记录一致要求。O.VULNERABILITY_ANALYSIS 要求进行合适的渗透性测试和独立脆弱性分析来缓解此威胁。

T.RESIDUAL_DATA

O.RESIDUAL_INFORMATION 通过确保当数据库服务器资源（缓存、磁盘）被用户或进程释放并配置给其他用户或进程时，TSF 数据和用户数据不再持久存在。

T.TSF_COMPROMISE

O.INTERNAL_TOE_DOMAINS 确保 TOE 为授权用户数据建立单独的用户安全域，保证多用户并发访问数据的隔离性和一致性；O.MANAGE 提供了限制授权管理员使用 TSF 功能和 TSF 数据（查看、修改或删除）或执行代码的能力；O.RESIDUAL_INFORMATION 确保服务器共享资源中删除的 TSF 数据不能重新被配置给其他用户；O.TRUSTED_PATH 确保 TSF 和不同授权主体（远程管理员、依赖方和可信 IT 实体）间存在可信通信路径来解决此威胁；OE.CONFIG 要求 TOE 及其运行支撑环境提供管理与配置 DBMS 运行安全所需的功能和设施，并防止这些功能和设施被未授权使用；

OE.SELF_PROTECTION 确保 TOE 足以保护自身免受外部来源的威胁，所有 TSP 功能可以被调用，保证 TOE IT 环境提供与 TOE 相似的安全保护。OE.DOMAIN_SEPARATION 保证数据库服务器及其网络应用环境将为 TOE 运行提供独立安全域。

T.UNAUTHORIZED_ACCESS

O.ACCESS_HISTORY 确保 TOE 能够存储和检索上一次成功登录时，用户不知情情况下的登录尝试和执行的操作信息；O.TOE_ACESS 确保 TOE 在允许访问 TOE 服务前要进行身份鉴别，要求控制登录用户可以访问的 TOE、TOE 安全功能和 TS 数据，阻止授权用户不适当地更改 TOE 配置数据及其安全威胁；O.MANAGE 与 OE.CONFIG 要求 TOE 及其环境仅限于确保管理员修改与 TOE 相关联的安全属性；OE.TOE_ACCESS 在允许访问 TOE 或通过 TOE 转发的服务前要通过 IT 环境进行身份鉴别；OE.SELF_PROTECTION 确保 TOE 足以保护自身免受外部来源的威胁，所有 TSP 功能可以被调用，保证 TOE IT 环境提供与 TOE 相似的安全保护。

T.UNAVAILABILITY

O.RESOURCE_SHARING 要求 TOE 提供关于数据库服务器 CPU 时间、共享内存、可获得的网络连接数、服务器存储空间的共享控制，来消除恶意进程或用户可能通过使用资源耗尽所拒绝的服务攻击来阻止他人获得数据库服务器资源的行为，或者由于 TOE 的主数据库服务器故障而导致数据库对用户不可用，或 TOE 可能由于合法用户任务请求过多导致的服务过载；O.AVAIL 确保数据库服务器磁盘介质故障的情况下，通过数据库恢复的方法，保障数据库服务可用性；或在主数据库服务器对用户不可用时，由 TOE 提供控制切换和故障转移功能，提高数据库的可用性。

T.UNIDENTIFIED_ACTIONS

O.AUDIT_GENERATION 或 O.AUDIT_GENERATION 保证与配置审计策略相关的操作审计数据的生成，消除 TOE 中存在的授权管理员不能标识并且可能发生的非授权操作的威胁，提供采取必要行动以应对这些潜在未被授权访问操作的安全问责管理的措施。

8.1.3 组织安全策略对应安全目的

表 12 说明了 TOE 及其运行环境安全目的能应对所有可能的组织安全策略。

表 12 组织安全策略与安全目的的对应关系

组织安全策略	安全目的											
	O. ACCESS. LBAC	O. ADMIN_ROLE	O. AUDIT_GENERATION	O. AUDIT_PROTECTON	O. CRYPTOGRAPHY	O. FUNCTIONAL_TEST	O. AVAIL	O. RESIDUAL_INFORMATION	O. TOE_ACCESS	O. TRUSTED_PATH	O. VULNERABILITY_ANALYSIS	OE. TIME_STAMPS
责任与义务 P.ACCOUNTABILITY	—	√	√	—	—	—	—	—	√	—	—	√
密码策略 P.CRYPTOGRAPHY	—	—	—	—	√	—	—	√	—	—	—	—
标签策略 P.LABEL	√	√	—	—	—	—	—	—	—	—	—	—
角色分离策略 P.ROLES	—	√	—	—	—	—	—	—	—	√	—	—

表 12（续）

组织安全策略	安全目的											
	O.ACCESS.LBAC	O.ADMIN_ROLE	O.AUDIT_GENERATION	O.AUDIT_PROTECTON	O.CRYPTOGRAPHY	O.FUNCTIONAL_TEST	O.AVAIL	O.RESIDUAL_INFORMATION	O.TOE_ACCESS	O.TRUSTED_PATH	O.VULNERABILITY_ANALYSIS	OE.TIME_STAMPS
系统完整性策略 P.SYSTEM_INTEGRITY	—	—	—	—	—	√	√	—	—	—	—	—
脆弱性分析与测试策略 P.VULNERABILITY_ANALYSIS_TEST	—	—	—	—	—	—	—	—	—	—	√	—
责任与义务 P.ACCOUNTABILITY	—	√	√	—	—	—	—	—	√	—	—	√
密码策略 P.CRYPTOGRAPHY	—	—	—	—	√	—	—	√	—	—	—	—
标签策略 P.LABEL	√	√	—	—	—	—	—	—	—	—	—	—
角色分离策略 P.ROLES	—	√	—	—	—	—	—	—	—	√	—	—
系统完整性策略 P.SYSTEM_INTEGRITY	—	—	—	—	—	√	√	—	—	—	—	—
脆弱性分析与测试策略 P.VULNERABILITY_ANALYSIS_TEST	—	—	—	—	—	—	—	—	—	—	√	—

注：√ 代表有对应关系。
— 代表无对应关系。

下面论述每一种组织安全策略对应的 TOE 安全目的及其原理。

P.ACCOUNTABILITY

O.ADMIN_ROLE 提供安全管理员管理 DBMS 安全性所必需的功能和设施，防止这些管理功能和管理设施被未授权用户使用；O.AUDIT_GENERATION 提供审计机制记录特定用户的操作，供管理员根据用户 ID 等属性追踪触发安全事件的能力。O.AUDIT_PROTECTON 保护审计事件，从而确保 DBMS 能够在威胁状态发生改变时捕捉安全相关的事件；O.TOE_ACCESS 要求 TOE 在允许任何授权用户访问或任何代表用户的程序访问之前，标识和授权所有授权用户；OE.TIME_STAMPS 保证数据库外部的 IT 环境提供可靠的时间戳。

P.CRYPTOGRAPHY

O.CRYPTOGRAGHY 保证 TOE 使用的密码算法应符合国家、行业或组织要求的密码管理相关标准或规范，并且 TOE 应提供密码功能以维护 DBMS 资产的保密性和完整性；O.RESIDUAL_INFORMATION 通过确保当数据库服务器共享资源被用户或进程释放后并配置给其他用户或进程时，TSF 数据和用户相关密钥数据不再持久存在。

P.LABEL

O.ACCESS.LBAC 要求 TOE 提供基于标签的访问控制机制，组织提供基于安全标签的数据分级、

用户分类与分组的读/写权限安全策略 O.ADMIN_ROLE 要求组织安全管理员按照 TOE 的标签访问控制策略定义标签，并确保标签策略定义的完整性和一致性。

P.ROLES

O.ADMIN_ROLE 保证 TOE 应提供与不同数据库管理操作相适应的授权管理员角色，以提供职责分离、角色约束等角色管理功能；O.TRUSTED_PATH 要求所有可信用户的各远程管理会话都经由安全信道授权和引导，所有可信 IT 实体通过受保护信道连接，从而避免泄露和欺骗问题。

P.SYSTEM_INTEGRITY

O.FUNCTIONAL_TEST 要求 TSF 运行一套安全功能测试用例集以证明 TSF（硬件和软件）和 TSF 加密组件在 DBMS 初始启动后正确运行，管理员还可以通过 O.FUNCTIONAL_TEST 验证 TSF 数据和存储代码的完整性，也可以利用 DBMS 提供的加密机制验证 TSF 加密数据和存储代码；O.AVAIL 应提供能够定期验证其备份与恢复数据的安全策略及其运行支撑环境正确的操作，并在管理员的帮助下，它应能够恢复到任何被检测到错误前的一致性状态。

P.VULNERABILITY_ANALYSIS_TEST

O.VULNERABILITY_ANALYSIS 进行了合适的渗透性测试独立脆弱性分析，以证明 DBMS 的设计和实现不允许拥有中等攻击潜力的攻击者通过违反 DBMS 安全策略来实现该组织策略。

8.1.4 假设对应安全目的

表 13 说明了 TOE 及其运行安全目的能够应对的假设。

表 13 假设与安全目的的对应关系

假设	安全目的									
	O.ADMIN_ROLE	OE.AUDIT_PROTECTION	OE.AUDIT_REVIEW	OE.DIR_CONTROL	OE.DOMAIN_SEPARATION	OE.NO_HARM	OE.NO_GENERAL_PURPOSE	OE.PHYSICAL	OE.SECURE_COMMS	OE.TOE_NO_BYPASS
目录服务器保护 A.DIR_PROTECTION	—	—	—	√	—	—	—	—	√	—
安全域分离 A.DOMAIN_SEPARATION	—	—	—	—	√	—	—	—	—	√
角色分工管理 A.MANAGER	√	—	—	—	—	—	—	—	—	—
多层应用问责 A.MIDTIER	—	√	√	√	—	√	—	—	—	—
人员假设 A.NO_HARM	—	—	—	—	—	√	—	—	—	—
服务器专用 A.NO_GENERAL_PURPOSE	—	—	—	—	—	—	√	—	—	—
物理安全 A.PHYSICAL	—	—	—	—	—	—	—	√	—	—
通信安全 A.SECURE_COMMS	—	—	—	—	—	—	—	—	√	—

注：√ 代表有对应关系。
— 代表无对应关系。

下面论述每一种假设对应的安全目的及其原理。

A.DIR_PROTECTION

OE.DIR_CONTROL 提供企业级别用户身份鉴别管理与配置指南。OE.SECURE_COMMS 将保证在目录服务器和 TOE 之间的用户标识和鉴别信息的安全通信。

注：目录服务器不是 TOE 的组成部分，因此 ST 作者需明确目录控制目的(OE.DIR_CONTROL)。

A.DOMAIN_SEPARATION

OE.DOMAIN_SEPARATION 提供一个可分离的安全执行域，不同节点间应以一种安全方式进行通信。OE.TOE_NO_BYPASS 通过确保配置数据库客户端、应用服务器等远程或本地应用程序使得信息只能通过 TOE 在客户端与数据库服务器或多数据库服务器主机(分布式数据库)之间进行流动来缓解安全威胁。

A.MANAGER

O.ADMIN_ROLE 确保在 TOE 中将有一个或多个指定能力的管理 TOE 和 TSF 的不同管理员，他们之间依据最小特权、职责分离、深度防御等安全原则进行了角色分工。

A.MIDTIER

OE.DIR_CONTROL 确保在分布式多层次环境中的任意中间层次都应将原始的客户标识(ID)发送给 TOE，以阻止非法用户访问 LDAP 服务器保存的 TSF 数据。OE.NO_HARM 确保数据库管理员是可信的，训练有素的，并且遵循组织安全策略和相关的目录服务器使用指南管理数据库。OE.AUDIT_PROTECTION 和 OE.AUDIT_REVIEW 确保多层应用运行的日志被 IT 环境安全保护，不可被篡改，但可被授权管理员查询与浏览。

A.NO_HARM

OE.NO_HARM 保证使用评估对象的组织应确保其数据库管理员是可信的，训练有素且遵循组织安全策略和相关的数据库管理员指南。

A.NO_GENERAL_PURPOSE

OE.NO_GENERAL_PURPOSE DBMS 服务器除了提供 DBMS 运行、管理和支持的必要服务外，不存在与 DBMS 运行无关的计算或存储功能。

A.PHYSICAL

OE.PHYSICAL 保证 IT 环境应提供与 TOE 和 TOE 所包含数据的价值相一致的物理安全。

A.SECURE_COMMS

OE.SECURE_COMMS 保证 TOE 与用户和应用终端之间的通信信道是安全可靠的(如满足私密性和完整性)，其典型的实现方式是通过共享密钥、公/私钥对，或者利用存储的其他密钥来产生会话密钥。

8.2 安全要求基本原理

8.2.1 概述

本条说明安全功能与保证组件要求的充分必要性和基本原理，即每个安全目的都至少有一个安全要求(包括功能要求和保障要求)组件与其对应，每个安全要求都至少解决了一个安全目的。因此本标准规定的 TOE 安全要求对 TOE 安全目的而言是充分和必要的。

8.2.2 安全功能组件

表 14 说明了 TOE 的每个安全功能组件要求都至少解决了一个 TOE 安全目的。

表 14　安全功能组件与 TOE 安全目的的对应关系

安全功能组件	安全目的											
	O.ACCESS_HISTORY	O.ACCESS.LBAC	O.ADMIN_ROLE	O.AUDIT_GENERATION	O.AUDIT_PROTECTION	O.AVAIL	O.CRYPTOGRAGHY	O.MANAGE	O.RESIDUAL_INFORMATION	O.RESOURCE_SHARING	O.TOE_ACCESS	O.TRUSTED_PATH
FAU_GEN.1 审计数据产生	—	—	—	√	—	—	—	—	—	—	—	—
FAU_GEN.2 用户身份关联	—	—	—	√	—	—	—	—	—	—	—	—
FAU_SAR.1 审计查阅	—	—	—	—	√	—	—	—	—	—	—	—
FAU_SAR.2 限制审计查阅	—	—	—	—	√	—	—	—	—	—	—	—
FAU_SAR.3 可选审计查阅	—	—	—	—	√	—	—	—	—	—	—	—
FAU_SEL.1 选择性审计	—	—	—	√	√	—	—	—	—	—	—	—
FAU_STG.2 审计数据可用性保证	—	—	—	—	√	—	—	—	—	—	—	—
FAU_STG.4 防止审计数据丢失	—	—	—	—	√	—	—	—	—	—	—	—
FCS_CKM.1 密钥生成	—	—	—	—	—	—	√	—	√	—	—	—
FCS_CKM.4 密钥销毁	—	—	—	—	—	—	√	—	√	—	—	—
FCS_COP.1 密码运算	—	—	—	—	—	—	√	—	—	—	—	—
FDP_ACC.1 子集访问控制	—	—	—	—	—	—	—	—	—	—	√	—
FDP_ACF.1 基于安全属性的访问控制	—	—	—	—	—	—	—	—	—	—	√	—
FDP_IFC.1 子集信息流控制	—	√	—	—	—	—	—	—	—	—	—	—
FDP_IFF.2 分级安全属性	—	√	—	—	—	—	—	—	—	—	—	—
FDP_ETC.2 带有安全属性用户数据输出	—	√	—	—	—	—	—	—	—	—	√	—
FDP_ITC.1 不带安全属性用户数据输入	—	—	—	—	—	—	—	—	—	—	√	—
FDP_ITT.1 基本内部传送保护	—	—	—	—	—	√	—	—	—	√	√	—
FDP_RIP.1 子集残余信息保护	—	—	—	—	—	—	—	—	√	—	—	—
FDP_ROL.1 基本回退	—	—	—	—	—	√	—	—	—	—	—	—
FDP_SDI.2 存储数据完整性监视和行动	—	—	—	—	√	—	—	—	—	—	√	—
FIA_AFL.1 鉴别失败处理	—	—	—	√	—	—	—	—	—	—	√	—
FIA_ATD.1 用户属性定义	—	—	—	—	—	—	—	—	—	—	√	—
FIA_SOS.1 秘密的验证	—	—	—	—	—	—	—	—	—	—	√	—
FIA_UAU.1 鉴别的时机	—	—	—	—	—	—	—	—	—	—	√	—
FIA_UAU.5 多重鉴别机制	—	—	—	—	—	—	—	—	—	—	√	—

表 14（续）

安全功能组件	安全目的											
	O.ACCESS_HISTORY	O.ACCESS.LBAC	O.ADMIN_ROLE	O.AUDIT_GENERATION	O.AUDIT_PROTECTION	O.AVAIL	O.CRYPTOGRAGHY	O.MANAGE	O.RESIDUAL_INFORMATION	O.RESOURCE_SHARING	O.TOE_ACCESS	O.TRUSTED_PATH
FIA_UAU.7 受保护的鉴别反馈	—	—	—	—	—	—	—	—	—	—	√	—
FIA_UID.1 标识的时机	—	—	—	—	—	—	—	—	—	—	√	—
FIA_USB.1 用户-主体绑定	—	—	—	√	—	—	—	—	—	—	√	—
FMT_MOF.1 安全功能行为的管理	—	√	—	—	—	—	—	√	—	√	—	—
FMT_MSA_EXT.1 安全属性的管理	—	√	—	—	—	—	—	√	—	—	—	—
FMT_MSA_EXT.3 静态属性初始化	—	√	—	—	—	—	—	√	—	—	—	—
FMT_REV.1 撤消	—	—	—	—	—	—	—	√	—	—	—	—
FMT_MTD.1TSF 数据的管理	—	—	—	—	—	—	—	√	—	—	—	—
FMT_SMF.1 管理功能规范	—	√	—	—	—	—	—	√	—	—	—	—
FMT_SMR.1 安全角色	—	—	√	—	—	—	—	√	—	—	—	—
FMT_SMR.2 安全角色限制	—	—	√	—	—	—	—	√	—	—	—	—
FPT_FLS.1 失效即保持安全状态	—	—	—	—	—	√	—	—	—	—	—	—
FPT_ITT.2TSF 数据传输的分离	—	√	—	—	—	—	—	—	—	—	—	—
FPT_RCV.3 无过度损失的自动恢复	—	—	—	—	—	√	—	—	—	—	—	—
FPT_TRC.1 内部 TSF 的一致性	—	—	—	—	—	—	—	—	—	—	√	—
FPT_OVR_EXT.1TSF 故障切换/转移	—	—	—	—	—	√	—	—	—	—	—	—
FRU_FLT.1 降级容错	—	—	—	—	—	√	—	—	—	—	—	—
FRU_PRS.1 有限服务优先级	—	—	—	—	—	—	—	—	—	√	—	—
FRU_RSA.2 最低最高配额	—	—	—	—	—	—	—	—	—	√	—	—
FTA_LSA.1 可选属性范围限定	—	—	—	—	—	—	—	—	—	—	√	—
FTA_MCS.1 多重并发会话的基本限定	—	—	—	—	—	—	—	—	—	—	√	—
FTA_SSL.3TSF 原发会话终止	—	—	—	—	—	—	—	—	—	—	√	—
FTA_TAH.1TOE 访问历史	√	—	—	—	—	—	—	—	—	—	—	—
FTA_TSE.1TOE 会话建立	—	—	—	—	—	—	—	—	—	—	√	—
FTP_ITC.1 可信信道	—	—	—	√	—	—	√	—	—	—	—	√

注：√ 代表有对应关系。
— 代表无对应关系。

下面论述每一种 TOE 安全目的对应的 DBMS 安全功能组件及其原理。

O.ACCESS_HISTORY

FTA_TAH.1 要求 TOE 能够存储和检索以前未经授权的登录尝试，包括每次用户登录到 TOE 的用户名、密码、服务等帐户信息。

O.ACCESS_LBAC

FDP_IFC.1 定义了数据库对象信息控制政策，要求绑定标签的数据库对象有确定的信息流控制 SFP；FDP_IFF.2 要求 SFR 中有信息流控制数据库对象和授权主体使用数据库标签元素（分级安全属性）定义了信息控制策略规则；FMT_MOF.1 和 FMT_SMF.1 确保基于标签的访问控制机制（信息流控制政策）的数据库对象的 TSF 数据免受未经授权的修改；FMT_MSA_EXT.1、FMT_SMF.1、FMT_MSA_EXT.3 提供标签控制的安全属性管理，这些标签组成的数据将用于控制对数据库对象的访问控制。FDP_ETC.2 要求带标签的数据导出时要求 TSF 利用一个功能执行合适的 SFP，该功能准确无误地将安全属性与从 TOE 外所输出的用户数据相关联。

O.ADMIN_ROLE

FMT_SMR.1 和 FMT_SMR.2 要求 TOE 应预定义不同角色的授权管理员特权，并提供创建和控制角色及其角色之间关系的规则，支持管理角色分离原则。

O.AUDIT_GENERATION

FAU_GEN.1 定义 TOE 应记录的事件集，确保授权管理员能够控制 TOE 发生的安全相关事件及包含在审计记录中的每个事件信息；FAU_GEN.2 确保审计记录可以关联可审计的事件和授权用户身份或授权用户组标识；FAU_SEL.1 允许授权管理员在审计策略配置时选择哪一些审计事件被记录在历史记录存储中；FIA_USB.1 通过要求绑定与用户相关联的安全属性满足该目的。

O.AUDIT_PROTECTION

FAU_SAR.1 和 FAU_SAR.1 确保 TOE 或 IT 环境保存为负责管理 TOE 的授权管理员提供查阅 TOE 审计记录的设施；FAU_SAR.3 为管理员提供了依据已建立的标准选择性查阅审计数据内容的能力，允许管理员把审计查阅的焦点放在特定时间发生、包含特定操作或由特定主客体对象执行的事件上；FAU_STG.2 和 FAU_STG.4 确保所存储的审计记录避免未授权的删除或修改；FAU_SEL.1 允许授权管理员在审计策略配置时选择哪一些审计事件被记录在历史记录存储中；FDP_SDI.2 确保审计数据存储的完整性，并在检测到某个错误时，TOE 能采取相应动作。

O.AVAIL

FDP_ROL.1 保障 TOE 出现故障时能快速的执行恢复操作，保证数据服务操作的原子性和持久性；FRU_FLT.1 要求如果发生了确定的失效，TOE 能继续正确发挥既定能力；FPT_OVR_EXT.1 指定 TOE 分布式部署时应提供 TSF 故障切换和故障转移功能；FPT_RCV.3 要求 TOE 在发生数据库服务器进程失效、数据库存储介质失效时提供数据库自动恢复机制，从而保障数据库事务特性。

O.CRYPTOGRAPHY

FCS_CKM.1 和 FCS_CKM.4 确保 TOE 能够产生和销毁加解密密钥，且 TOE 生成或销毁密钥时应符合国家、行业或组织要求的密码管理相关标准或规范，并且 TOE 应提供密码功能以维护 DBMS 资产的保密性和完整性。FCS_COP.1 要求使用随机数产生器，且在数据加密和解密时使用国家、行业或组织要求的算法。FPT_ITC.1 要求使用加密机制的 TOE 在与外部 TOE 通信时应使用可信通道。

O.MANAGE

FMT_MTD_.1 确保授权管理员能够管理 TSF 数据；FMT_MSA_EXT.1 为确保授权管理员管理指定的安全属性；FMT_MSA_EXT.3 确保安全属性的默认值设置为适当的允许值或限制范围内；FMT_REV.1 提供在某一时刻将实施的安全属性撤消；FMT_MOF.1 允许授权管理员具备管理服务器资源使用规则或具有指定资源使用条件的功能行为；FMT_SMF.1 通过提供对加密数据、审计记录和密钥数据的管理功能来支持该目的；FMT_SMR.1 规定 TSF 认同的与授权管理员安全相关的一些内置数据库角色/权限；FMT_SMR.2 除了规定角色外，还规定了控制角色之间约束条件的规则。FDP_SDI.2 确保管理员设置的数据库完整性约束条件及 TOE 存储数据的完整性，并在检测到某个错误时，TOE 能采取相应动作。

O.RESIDUAL_INFORMATION

FDP_RIP.1 要求 TSF 确保任何资源的任何残余信息内容在资源分配或释放时，对于所有客体都是不可再利用的。FCS_CKM.1 适用于 TSF 所使用密钥的分发，用于确保重新分配密钥时，旧的密钥内容不再可用。

O.RESOURCE_SHARING

FRU_RSA.2 是用来减轻潜在数据库服务器共享计算资源耗尽尝试；需要消耗的数据库服务器资源应限制在 FMT_MTD_EXT.1 规定的限额范围内；FMT_MOF.1 允许授权管理员具备管理服务器资源使用规则或具有指定资源使用条件的功能行为。

O.TOE_ACCESS

FIA_AFL.1 确保 TOE 可以保护自身及其用户免受对他们鉴别证书的蛮力攻击；FIA_ATD.1 允许授权管理员对每个授权用户的安全属性分别加以维护；FIA_USB.1 要求对用户属性及其映入的主体属性之间的关联关系的管理规则进行规范；FIA_UID.1 和 FIA_SOS.1 通过确保 TOE 在执行任何数据库用户请求前鉴别每一个用户来满足该目的；FIA_UAU.1 和 FIA_UAU.5 通过确保授权管理员和授权用户在访问 TOE 及其服务之前被鉴别来实现该目的；FTA_LSA.1 提供关于 TOE 在建立会话时限制会话安全属性范围的要求；FTA_MCS.1 确保 TOE 可以提供多个并发会话控制；FTA_TSE.1 通过限制用户对逻辑访问 TOE 能力有助于实现这一目标；FTA_SSL.3.1 为 TSF 提供在用户在一段指定时间不活动后终止该会话的要求。FDP_ACC.1 要求访问控制策略(SFP)适用于对数据库对象客体子集可能执行的操作子集；FDP_ACF.1 允许 TSF 基于安全属性和已命名属性组执行访问，TSF 有能力根据安全属性明确地授权或拒绝对某个数据库对象进行访问；FPT_TRC_EXT.1 要求 TSF 确保数据库安全元数据在多处复制时的一致性；FDP_ITC.1 和 FDP_ETC.2 要求 TOE 在导入导出数据时要求 TSF 利用一个功能执行合适的 SFP；FDP_ITT.1 要求数据库在分布式部署时用户数据在 TOE 的各部分间传输时受保护。FPT_ITT.2 要求对在 TOE 的不同部件间传送的 TSF 数据进行分离和保护。

O.TRUSTED_PATH

FTP_ITC.1 为数据库外部用户身份标识或鉴别的 IT 环境所提供的服务建立可信信道。

8.2.3 安全保障组件

表 15 是 TOE 安全保障组件与 TOE 安全目的之间的对应关系。

表 15 安全保障组件与安全目的的对应关系

安全保障组件	TOE 安全目的					
	O.ADMIN_GUIDANCE	O.CONFIG	O.DOCUMENTED_DESIGN	O.FUNCTIONAL_TEST	O.INTERNAL_TOE_DOMAINS	O.VULNERABILITY_ANALYSIS
ADV_ARC.1 安全架构描述	—	—	√	—	√	—
ADV_FSP.2 安全执行功能规范	—	—	√	—	—	—
ADV_FSP.3 带完整摘要的功能规范	—	—	√	—	—	—

表 15（续）

安全保障组件	TOE 安全目的					
	O.ADMIN_GUIDANCE	O.CONFIG	O.DOCUMENTED_DESIGN	O.FUNCTIONAL_TEST	O.INTERNAL_TOE_DOMAINS	O.VULNERABILITY_ANALYSIS
ADV_FSP.4 完备的功能规范	—	—	√	—	—	—
ADV_IMP.1 TSF 实现表示	—	—	—	—	—	—
ADV_TDS.1 基础设计	—	—	√	—	—	—
ADV_TDS.2 结构化设计	—	—	√	—	—	—
ADV_TDS.3 基础模块设计	—	—	√	—	—	—
AGD_OPE.1 操作用户指南	√	—	—	—	—	—
AGD_PRE.1 准备程序	√	—	—	—	—	—
ALC_CMC.2 CM 系统的使用	—	√	—	—	—	—
ALC_CMC.3 授权控制	—	√	—	—	—	—
ALC_CMC.4 生产支持和接受程序及其自动化	—	√	—	—	—	—
ALC_CMS.2 部分 TOE CM 覆盖	—	√	—	—	—	—
ALC_CMS.3 实现表示 CM 覆盖	—	√	—	—	—	—
ALC_CMS.4 问题跟踪 CM 覆盖	—	√	—	—	—	—
ALC_DEL.1 交付程序	√	—	—	—	—	—
ALC_DVS.1 安全措施标识	—	—	√	—	—	—
ALC_LCD.1 开发者定义的生命周期模型	—	—	√	—	—	—
ALC_TAT.1 明确定义的开发工具	—	—	√	—	—	—
ATE_COV.1 覆盖证据	—	—	—	√	—	—
ATE_COV.2 覆盖分析	—	—	—	√	—	—
ATE_DPT.1 测试:基本设计	—	—	—	√	—	—
ATE_DPT.2 测试:安全执行模块	—	—	—	√	—	—
ATE_FUN.1 功能测试	—	—	—	√	—	—
ATE_IND.2 独立测试—抽样	—	—	—	√	—	—
AVA_VAN.2 脆弱性分析	—	—	—	—	—	√
AVA_VAN.3 关注点脆弱性分析	—	—	—	—	—	√

注：√ 代表有对应关系。
— 代表无对应关系。

下面论述每一种 TOE 安全目的对应的 DBMS 安全保障组件及其原理。

O.ADMIN_GUIDANCE

AGD_OPE.1 用户操作指南描述了 DBMS 安全机制提供的安全功能，以及提供 DBMS 安全使用的一些规程和指导，包括警示信息；AGD_PRE.1 准备程序给出了包括调查 DBMS 组件配置或 DBMS 安装环境是否存在不一致，或 DBMS 中存在的不安全安装方式，以避免误导用户相信 DBMS 的安装是合理和安全的；ALC_DEL.1 保证数据库管理员拥有安装、生成、启动 TOE 程序文档的权利，确保管理员在操作过程中遵循了安装和配置指南，告诉他们如何正确地部署 DBMS，并在数据库维护的过程中不受到干扰。

O.CONFIG

ALC_CMC.2，ALC_CMC.3 和 ALC_CMC.4 要求 TOE 提供一种跟踪任何变化的方法和确保所有修改都是经过了授权的，并且确保他们所控制的 TOE 部分的完整性；ALC_CMS.2，ALC_CMS.3 和 ALC_CMS.4 要求有一个现场配置管理(CM)系统，并且包含在 TOE 中的每个配置项是唯一标识，提供一个清晰、明确的 TOE 组成清单，即通过要求开发者拥有描述 TOE 变化和 TOE 评估报告管理方式的配置管理计划来满足该目的。

O.DOCUMENTED_DESIGN

ADV_ARC.1 要求开发者提供对 TSF 安全架构的描述，包括描述支持隐含的声明；ADV_FSP.2 要求开发者提供所有 TSFI 的目的、使用方法、参数和参数描述，包括对于 SFR-执行 TSFI，开发者应描述 SFR-执行行为和直接错误消息；ADV_FSP.3 除了 ADV_FSP.2 要求的信息之外，开发者应提供足够的关于 SFR-支撑和 SFR-无关行为的信息，包括开发者应文档化由调用 SFR-执行的 TSFI 产生的所有直接错误消息；ADV_FSP.4 要求所有 TSFI(无论是 SFR-执行、SFR-支撑还是 SFR-无关)应以同等程度来描述，包括所有的直接错误消息；ADV_TDS.1、ADV_TDS.2 和 ADV_TDS.3 提供了与 TSF 描述的上下文，以及对 TSF 的详尽描述；ALC_DVS.1 要求开发安全文档应描述在 TOE 的开发环境中，保护 TOE 设计和实现的保密性和完整性所必需的所有物理的、程序的、人员的及其他方面的安全措施；ALC_LCD.1 要求生命周定义文档应描述用于开发和维护 TOE 的生命周期模型，为 TOE 的开发和维护提供必要的控制；ALC_TAT.1 要求开发者应标识用于开发 TOE 的每个工具，应无歧义地定义所有语句和实现用到的所有协定与命令的含义。

O.FUNCTIONAL_TEST

ATE_COV.1 和 ATE_COV.2 要求开发者提供测试覆盖范围分析以表明开发者的测试套件测试 TSFI 的范围。该组件也要求独立地确认测试套件的范围，这有助于确保通过测试验证 TSFI 的安全相关功能；ATE_FUN.1 要求开发者提供必要的测试文档以允许独立地分析开发者安全功能测试的覆盖范围。另外，开发者应提供测试套件的可执行代码和源代码，以便评估者可以使用这些代码从而独立地验证提供商的测试结果和支持测试覆盖范围分析；ATE_IND.2 要求通过规定独立方运行测试套件的子集，独立地确认开发者的测试结果。该组件也要求第三方执行附加的功能测试，以解决开发者测试套件中没有证明的功能行为。一旦成功地完成这些要求，就可以证明 TOE 遵循了规定的安全功能要求；ATE_DPT.1 和 ATE_DPT.2 要求开发人员提供一个测试覆盖率分析，演示了覆盖测试套件的深度。

INTERNAL_TOE_DOMAINS

ADV_ARC.1 提供由 TSF 维护的数据库用户安全域与数据库实例组件、服务器资源及用户数据管理特殊功能相一致的安全体系结构的描述；FDP_ITT.1 要求在 TOE 的不同安全域间传输时受保护。

O.VULNERABILITY_ANALYSIS

AVA_VAN.2 和 AVA_VAN.3 保证 TOE 应适合测试，评估者应确认所提供的信息满足证据的内容和形式的所有要求，评估者应执行公共领域的调查以标识 TOE 的潜在脆弱性，评估者应针对 TOE 执行独立的脆弱性分析去标识 TOE 潜在的脆弱性，在分析过程中使用指导性文档、功能规范、TOE 设计、安全结构描述和实现表示，评估者应基于已标识的潜在脆弱性实施渗透性测试，确定 TOE 能抵抗

具有基本攻击潜力至增强型基本攻击潜力的攻击者的攻击。

8.3 组件依赖关系

PP/ST 作者在选取 GB/T 18336 安全功能组件和安全保障组件时，应满足所选组件之间的相互依赖关系，表 16 列出了本标准所选安全功能组件的依赖关系，表 17 列出了所选安全保障组件的依赖关系。

表 16 安全功能组件依赖关系

序号	安全功能要求	依赖关系
1	FAU_GEN.1	FPT_STM.1
2	FAU_GEN.2	FAU_GEN.1，FIA_UID.1
3	FAU_SAR.1	FAU_GEN.1
4	FAU_SAR.2	FAU_SAR.1
5	FAU_SAR.3	FAU_SAR.1
6	FAU_SEL.1	FAU_GEN.1，FMT_MTD.1
7	FAU_STG.2	FAU_GEN.1
8	FAU_STG.4	FAU_STG.1
9	FCS_CKM.1	FCS_COP.1，FCS_CKM.4
10	FCS_CKM.4	FCS_CKM.1
11	FCS_COP.1	FCS_CKM.1，FCS_CKM.4
12	FDP_ACC.1	FDP_ACF.1
13	FDP_ACF.1	FDP_ACC.1，FMT_MSA.3
14	FDP_ETC.2	FDP_ACC.1 或 FDP_IFC.1
15	FDP_IFC.1	FDP_IFF.1
16	FDP_IFF.2	FDP_IFC.1，FMT_MSA.3
17	FDP_ITC.1	FDP_ACC.1 或 FDP_IFC.1，FMT_MSA.3
18	FDP_ITT.1	FDP_ACC.1 或 FDP_IFC.1
19	FDP_RIP.1	无
20	FDP_ROL.1	FDP_ACC.1 或 FMT_IFC.1
21	FDP_SDI.2	无
22	FIA_UID.1	无
23	FIA_AFL.1	FIA_UAU.1
24	FIA_UAU.1	FIA_UID.1
25	FIA_UAU.5	无
26	FIA_UAU.7	FIA_UAU.1
27	FIA_ATD.1	无
28	FIA_SOS.1	无
29	FIA_USB.1	FIA_ATD.1

表 16（续）

序号	安全功能要求	依赖关系
30	FMT_MOF.1	FMT_SMR.1，FMT_SMF.1
31	FMT_MSA.1	FDP_ACC.1 或 FDP_IFC.1，FMT_SMR.1，FMT_SMF.1
32	FMT_MSA.3	FMT_MSA.1，FMT_SMR.1
33	FMT_MTD.1	FMT_SMR.1，FMT_SMF.1
34	FMT_SMR.1	FIA_UID.1
35	FMT_SMR.2	FIA_UID.1
36	FMT_REV.1	FMT_SMR.1
37	FMT_SMF.1	无
38	FPT_FLS.1	无
39	FPT_TRC.1	FPT_ITT.2
40	FPT_ITI.2	无
41	FPT_RCV.3	AGD_OPE.1
42	FRU_FLT.1	FPT_FLS.1
43	FRU_RSA.2	无
44	FTA_TSE.1	无
45	FTA_SSL.3	无
46	FTA_LSA.1	无
47	FTA_TAH.1	无
48	FTA_MCS.1	FIA_UID.1
49	FTP_ITC.1	无

表 17　安全保障组件依赖关系

序号	安全保障要求	依赖关系
1	ADV_ARC.1	ADV_FSP.1，ADV_TDS.1
2	ADV_FSP.2	ADV_TDS.1
3	ADV_FSP.3	ADV_TDS.1
4	ADV_FSP.4	ADV_TDS.1
5	ADV_TDS.1	ADV_FSP.2
6	ADV_TDS.2	ADV_FSP.3
7	ADV_TDS.3	ADV_FSP.4
8	ADV_IMP.1	ADV_TDS.3，ALC_TAT.1
9	AGD_OPE.1	ADV_FSP.1
10	AGD_PRE.1	无

表 17（续）

序号	安全保障要求	依赖关系
11	ALC_CMC.2	ALC_CMS.1
12	ALC_CMC.3	ALC_CMS.1，ALC_DVS.1，ALC_LCD.1
13	ALC_CMC.4	ALC_CMS.1，ALC_DVS.1，ALC_LCD.1
14	ALC_CMS.2	无
15	ALC_CMS.3	无
16	ALC_CMS.4	无
17	ALC_DEL.1	无
18	ALC_DVS.1	无
19	ALC_LCD.1	无
20	ALC_TAT.1	ADV_IMP.1
21	ASE_CCL.1	ASE_INT.1，ASE_ECD.1，ASE_REQ.1
22	ASE_ECD.1	无
23	ASE_INT.1	无
24	ASE_OBJ.2	ASE_SPD.1
25	ASE_REQ.2	ASE_OBJ.2，ASE_ECD.1
26	ASE_SPD.1	无
27	ASE_TSS.1	ASE_INT.1，ASE_REQ.1，ADV_FSP.1
28	ATE_COV.1	ADV_FSP.2，ATE_FUN.1
29	ATE_COV.2	ADV_FSP.2，ATE_FUN.1
30	ATE_DPT.1	ADV_ARC.1，ADV_TDS.2，ATE_FUN.1
31	ATE_DPT.2	ADV_ARC.1，ADV_TDS.3，ATE_FUN.1
32	ATE_FUN.1	ATE_COV.1
33	ATE_IND.2	ADV_FSP.2，AGD_OPE.1，AGD_PRE.1 ATE_COV.1，ATE_FUN.1
34	AVA_VAN.2	ADV_ARC.1，ADV_FSP.2，ADV_TDS.1 AGD_OPE.1，AGD_PRE.1
35	AVA_VAN.3	ADV_ARC.1，ADV_FSP.4，ADV_TDS.3，ADV_IMP.1 AGD_OPE.1，AGD_PRE.1，ATE_DPT.1

附 录 A
（资料性附录）
关于标准修订和使用说明

表 A.1 为 GB/T 20273—2006 评估内容与本标准安全功能要求映射表，本标准中 EAL2、EAL3、EAL4 级的安全要求既适用于基于 GB/T 18336.1—2015、GB/T 18336.2—2015、GB/T 18336.3—2015 的数据库安全性测评，同样适用于基于 GB 17859—1999 的数据库标准第二级系统审计保护级、第三级安全标记保护级、第四级结构化保护级的安全性测评。

表 A.1 GB/T 20273—2006 评估内容与本标准安全功能要求映射表

GB/T 20273—2006 评估内容							GB/T 20273—2019 评估内容	备注
评估内容		第一级：用户自主保护级	第二级：系统审计保护级	第三级：安全标记保护级	第四级：结构化保护级	第五级：访问验证保护级	安全功能要求	
安全功能	身份鉴别						FIA_UID.1	√
							FIA_UAU.1	√
							FIA_UAU.7	√
							FIA_AFL.1	√
							FIA_USB.1	√
							FIA_UAU.5	√
	自主访问控制						FDP_ACC.1	√
							FDP_ACF.1	√
	标记						FMT_MSA_EXT.1(1)	√
							FMT_MSA_EXT.1(2)	√
							FDP_ITC.1	√
							FDP_ETC.2	√
	强制访问控制						FDP_ACC.1	√
							FDP_ACF.1	√
	数据流控制						FDP_IFC.1	√
							FDP_IFF.2	√
	安全审计						FAU_GEN.1	√
							FAU_GEN.2	√
							FAU_SAA.1	—
							FAU_SAR.1	√
							FAU_SAR.2	√
							FAU_SEL.1	√
							FAU_STG.1	—
							FAU_ARP.1	—

表 A.1（续）

GB/T 20273—2006 评估内容							GB/T 20273—2019 评估内容	备注
评估内容		第一级：用户自主保护级	第二级：系统审计保护级	第三级：安全标记保护级	第四级：结构化保护级	第五级：访问验证保护级	安全功能要求	
安全功能	安全审计						FAU_SAA.2	—
							FAU_SAR.3	√
							FAU_STG.2	√
							FAU_STG.4	√
							FAU_SAA.3	—
							FAU_SAA.4	—
	用户数据完整性						FDP_ROL.1	√
							FDP_SDI.2	√
							FDP_UIT.1	—
	用户数据保密性						FDP_UCT.1	—
	可信路径						FTP_ITC.1	√
	推理控制						对该部分内容的评估直接依据 GB/T 18336.3—2015 各级别的脆弱性评定要求进行评估	
SSODB 自身安全保护	SSF 物理安全保护						FPT_PHP.1	—
							FPT_PHP.2	—
							FPT_PHP.3	—
	SSF 运行安全保护						FPT_RVM.1	—
							FPT_SEP.1	—
							FMT_MSA_EXT.3	√
							FPT_RCV.1	—
							FPT_RCV.2	—
	SSF 数据安全保护						FPT_ITT.2	√
							FPT_TRC.1	√
							FPT_ITA.1	—
	资源利用						FRU_FLT.1	√
							FRU_PRS.1	—
							FRU_RSA.1	—
							FRU_RSA.2	√

表 A.1（续）

GB/T 20273—2006 评估内容							GB/T 20273—2019 评估内容	备注
评估内容		第一级：用户自主保护级	第二级：系统审计保护级	第三级：安全标记保护级	第四级：结构化保护级	第五级：访问验证保护级	安全功能要求	
SSODB自身安全保护	SSODB访问控制						FTA_LSA.1	√
							FTA_MCS.1	√
							FTA_TAH.1	√
							FTA_SSL.3	√
							FTA_TSE.1	√
SSODB设计和实现	配置管理						对该部分内容的评估直接依据 GB/T 18336.3—2015 各级别的保障要求进行评估	
	分发和操作							
	开发							
	文档要求							
	生命周期支持							
	测试							
	脆弱性评定							
SSODB安全管理							FMT_MOF.1	√
							FMT_SMF.1	√
							FMT_MSA.1	√
							FMT_MTD.1	√
							FMT_SMR.2	√
							FDP_ITT.1	+
							FDP_RIP.1	+
							FIA_ATD.1	+
							FIA_SOS.1	+
							FMT_REV.1	+
							FPT_FLS.1	+
							FPT_RCV.3	+
							FPT_OVR_EXT.1	+
							FCS_CKM.1	+
							FCS_CKM.4	+
							FCS_COP.1	+

注：√ 代表原标准安全功能项对应到本标准中的安全功能要求；
+ 代表本标准中新增的安全功能要求；
— 代表本标准中删除的原标准内容；
灰色部分代表原标准中安全功能所覆盖的范围。

参 考 文 献

[1] GB 17859—1999 计算机信息系统 安全保护等级划分准则

[2] U.S.Government Protection Profile for Database Management System, Version 1.3, National Security Agency (NSA), Dec 24, 2010.

[3] Consistency Instruction Manual, For development of US Government Protection Profiles (PP), Release 3.0, Feb 1, 2005.