ICS 35.040
L 80

中华人民共和国国家标准

GB/T 20009—2019
代替 GB/T 20009—2005

信息安全技术
数据库管理系统安全评估准则

Information security technology—
Security evaluation criteria 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

本标准按照GB/T 1.1—2009给出的规则起草。

本标准代替GB/T 20009—2005《信息安全技术　数据库管理系统安全评估准则》。与GB/T 20009—2005相比，除编辑性修改外主要技术变化如下：

——修改了第3章术语和定义及缩略语(见3.1和3.2，2005年版第3章)；

——修改了第4章“安全环境”，标题修改为评估总则，描述了数据库管理系统总体要求、评估要求、评估环境和评估流程(见第4章，2005年版第4章)；

——修改了第5章评估内容，按照GB/T 30270—2013定义了GB/T 20273—2019中的安全功能组件和安全保障组件评估内容(见第5章，2005年版第5章)；

——删除了附录A“数据库管理系统面临的威胁和对策”(见2005年版附录A)；

——按照评估保障级概念列出了EAL2、EAL3和EAL4组件列表及评估准则。

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 20009—2005。

信息安全技术
数据库管理系统安全评估准则

1 范围

本标准依据 GB/T 20273—2019 规定了数据库管理系统安全评估总则、评估内容和评估方法。

本标准适用于数据库管理系统的测试和评估，也可用于指导数据库管理系统的研发。

注：本标准规定的 EAL2 级、EAL3 级、EAL4 级的评估内容和评估方法既适用于基于 GB/T 18336—2015 所有部分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管理系统安全性测评，相关对应关系参见附录 A 中 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(包括所有的修改版)适用于本文件。

GB/T 18336.1～18336.3—2015 信息技术 安全技术 信息技术安全评估准则

GB/T 20273—2019 信息安全技术 数据库管理系统安全技术要求

GB/T 25069—2010 信息安全技术 术语

GB/T 30270—2013 信息技术 安全技术 信息技术安全性评估方法

3 术语和定义、缩略语

3.1 术语和定义

GB/T 25069—2010、GB/T 30270—2013 和 GB/T 20273—2019 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。

CC：通用准则(Common Criteria)

CEM：通用准则评估方法(Common Criteria Evaluation Methodology)

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)

ETR：评估技术报告(Evaluation Technical Report)

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

OR：观察报告(Observation Report)

PP：保护轮廓(Protection Profile)

SFP：安全功能策略(Security Function Policy)

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)

TSC：TSF 控制范围(TSF Scope of Control)
TSF：TOE 安全功能(TOE Security Functionality)
TSFI：TSF 接口(TSF Interface)
TSP：TOE 安全策略(TOE Security Policy)
TSS：TOE 概要规范(TOE Summary Specification)

4 评估总则

4.1 概述

本标准依据 GB/T 30270—2013 给出了 GB/T 20273—2019 定义的数据库管理系统(DBMS)评估对象(TOE)安全功能组件和安全保障组件的评估内容和评估方法。

4.2 评估要求

在对数据库管理系统进行安全评估时，首先依照 GB/T 30270—2013 的安全目标评估方法完成对 DBMS ST 的评估，在此基础上对 DBMS 的安全功能和安全保障进行评估：

a) 安全功能评估目标是保证 GB/T 20273—2019 定义的安全功能组件设计与实现的完整性和正确性，一般通过对 DBMS 发起者提供的评估证据分析和 TOE 安全功能(TSF)独立性测试，确保 DBMS 安全功能满足其安全目标声称的功能要求。独立性测试应依据数据库产品厂商提供的一系列评估证据(如分析、设计与测试文档)和 TOE 安全策略(TSP)，由评估者按照 ST 中的 TSS 对 DBMS 开发者提供的评估对象证据材料进行分析，并按照评估保障级的不同对 DBMS 安全功能组件进行抽样测试，或评估者自己设计相应的测试用例，独立地完成 DBMS 安全功能组件的功能测试，验证 TSF 的实现符合数据库管理系统概要规范。

b) 安全保障评估目标是发现 DBMS 在设计与实现中的缺陷或脆弱性，以便在评估过程中要求开发者纠正评估对象相应的错误，从而减少 DBMS 在发布后运行过程中安全功能失效发生的可能性。因此安全性评估要求测试人员在模拟真实应用环境下，测试 DBMS 是否能抵御各种安全攻击，以确定该评估对象是否存在潜在的安全弱点或安全漏洞。穿透性测试技术是消除 DBMS 在设计或实现中的缺陷或脆弱性的有效方法。测试人员需依照数据库产品的通信协议、结构化查询语言、数据库开发接口、存储过程/函数等安全攻击面评估证据资料，通过模糊测试等穿透性测试技术对安全功能组件实现机制的可信性进行测试以确保安全功能组件的设计、实现和测试不存在未知的弱点/缺陷。

4.3 评估环境

在不同的网络环境和服务器环境支持下，通用数据库产品提供多种安全策略和安全控制机制的解决方案，以满足评估对象消费者的安全要求。数据库管理系统的测试环境分为 3 类：非集群数据库服务测试环境和集群数据库服务测试环境，集群测试环境又细分为共享存储的集群测试环境和非共享存储的集群测试环境。

应根据 GB/T 30270—2013 安全评估基本原则、过程和规程的体系选择某个测试环境，对数据库产品安全功能和安全保障进行评估。数据库管理系统安全组件的每个评估活动都包含两个通用的评估任务：

a) 评估证据输入评估：评估发起者应向安全评估机构提供 DBMS 安全评估所有必需的评估材料：评估发起者应按照 GB/T 30270—2013 准备或开发 TOE 相关的评估证据，评估者应对这些输入要求进行评估。

b) 评估结果输出评估：安全评估机构的输出任务评估的目的是评估输出的观察报告和评估技术

报告应满足评估结果的可重复性和可再现性原则，并应保持各种报告信息类型和数量的一致性。

4.4 评估流程

根据 GB/T 30270—2013 的安全评估过程包括评估准备、评估实施、评估结果等阶段，具体如下：

a) 评估准备阶段：评估发起者应按照 GB/T 30270—2013 给评估者提供安全目标，评估者分析其可行性。评估者可能会需要发起者提供其他评估相关的辅助信息。评估发起者或者 ST 开发者会给评估者提供一部分待评估物。评估者审查安全目标，然后告知发起者对某些内容进行必要的补充完善，以方便未来评估过程的实施。当评估者认为评估发起者对评估所需要的资料都准备齐全了，则评估过程进入下一阶段。

b) 评估实施阶段：评估者生成包括待评估产品列表，评估活动，以及基于 GB/T 30270—2013 评估方法的抽样要求等文档的可行性研究报告。发起者和评估者在评估准备阶段签署一项协议，该协议包含评估的基本框架，同时要考虑到评估体制的局限性以及国家法律和法规的任何要求。协议签订后，评估者即可进入评估实施阶段。在此阶段包含的主要活动内容有：

   1) 评估者检查发起者或者开发者应交付的评估物，然后按照 GB/T 30270—2013 进行必要的评估活动。

   2) 在评估阶段，评估者可能会撰写观察报告。该报告里，评估者会向监管者（评审机构）询问如何满足其监管的要求。

   3) 监管者对评估者的解释请求进行回应，然后允许进行下一步评估。

   4) 监管者同样可能确认和指出一些潜在的缺陷或者威胁，然后要求发起者或者开发者提供额外的信息资料。

c) 评估最终结果阶段：评估者根据文档审核、测试情况、现场检查结果，对 TOE 进行综合评判，并撰写评估技术报告。

5 评估内容

5.1 安全功能评估

5.1.1 概述

在安全功能组件评估内容描述中，方括号【】中的黑体字内容表示已经完成的操作，黑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。

5.1.2 安全审计（FAU 类）

5.1.2.1 审计数据产生（FAU_GEN.1）

审计数据产生组件应按照安全目标设定的数据库标准审计和细粒度审计策略自动产生相应的审计事件记录信息。该组件安全评估内容如下：

a) 应测试评估对象提供的不同级别审计策略能产生下述可审计事件记录：

   1) 数据库审计功能的启动和关闭；

   2) 数据库实例及其组件服务的启动和关闭；

   3) 数据库实例配置参数非缺省值修改事件；

   4) 数据库对象结构修改事件；

   5) GB/T 20273—2019 列出的数据库审计级别【**最小**】的可审计事件；

   6) 其他面向数据库安全审计员的，可绕过访问控制策略的特殊定义【赋值：***ST 作者定义的审***

计事件】的可审计事件；

7） 未指定审计级别【赋值：***数据库对象数据操作级别的细粒度审计的事件***】的所有可审计事件。

b） 应检查审计记录中至少包含如下信息：

1） 事件类型、事件发生日期和时间、主体关联身份/组/角色、涉及的数据库对象、产生审计事件的主机信息、事件操作结果(成功或失败)；

2） 应根据评估对象【赋值：***ST 作者指定的审计事件***】和规定的格式【赋值：***数据类型与格式***】来生成审计数据；

3） 对于每个审计事件类型，基于 GB/T 20273—2019 中包括的安全功能组件的可审计事件定义。

c） 应检查数据库管理系统的审计数据产生策略配置管理 API 或工具，确认审计数据产生机制与功能有效性。

5.1.2.2 用户身份关联(FAU_GEN.2)

用户身份关联组件应将审计事件与主体身份相联系，满足可审计事件追溯到单个数据库用户身份上的要求。该组件安全评估内容如下：

a） 审计记录中应能查看到每个审计事件是否与引发审计事件的用户身份关联信息；

b） 审计记录中应能查看到每个审计事件是否与引发审计事件的【赋值：***ST 作者指定的用户身份鉴别方式***】相关联的数据库会话信息；

c） 应检查提供将审计记录中用户身份与用户所属组/角色身份关联查看辅助视图或管理 API/工具，确认能看到用户身份关联信息。

5.1.2.3 审计查阅(FAU_SAR.1)

审计查阅组件为授权管理员提供获得和解释审计数据的能力。该组件安全评估内容如下：

a） 应测试能否从审计记录中阅读和获取下面所列出的审计信息：

1） 用户身份标识；

2） 审计事件类型；

3） 数据库对象标识；

4） 评估对象指定的【赋值：***ST 作者指定的审计事件***】；

b） 应测试是否以使用户理解的方式提供满足查阅条件的审计记录阅读与管理界面(如图形界面)；

c） 应测试当授权用户是外部 IT 实体时，审计数据应以规范化电子方式无歧义地表示；

d） 应测试是否禁止所有未授权用户对审计数据的访问。

5.1.2.4 限制审计查阅(FAU_SAR.2)

限制审计查阅组件只允许授权管理员查阅部分审计数据。该组件安全评估内容如下：

a） 应测试是否能依据【选择：***主体标识***、***主机标识***、***客体标识***、【***赋值：ST 作者指定审计条件***】】查阅审计信息；

b） 应测试是否能依据【选择：***成功可审计安全事件***、***失败可审计安全事件***、【***赋值：ST 作者指定其他选择条件***】】查阅审计信息；

c） 应测试是否能依据【选择：***数据库系统权限***、***数据库对象权限***、【***赋值：ST 作者指定权限级别***】】查阅审计信息；

d） 应测试管理审计数据授权控制机制和审计数据授权管理员(安全管理员)控制授权管理员访问

审计数据的【赋值：*ST 作者指定角色/系统权限*】；

e) 应测试是否允许安全管理员或授予审计数据查阅权限的授权管理员访问审计数据视图或接口；

f) 应测试是否禁止所有未授权用户对审计数据的访问。

5.1.2.5 可选审计查阅（FAU_SAR.3）

可选审计查阅组件允许授权管理员根据指定的搜索条件来选择要查阅的审计数据。该组件安全评估内容如下：

a) 应测试是否能依据审计数据字段中值的搜索与分类条件对审计记录进行搜索，筛选授权管理员关心的审计数据；

b) 应测试是否能对返回审计数据进行排序和汇总统计；

c) 应测试是否允许授权管理员使用【选择：*SQL 语句*、【*赋值：ST 作者指定方式*】】搜索审计数据和对审计数据排序；

d) 应测试是否提供访问审计数据的应用开发接口能力或审计数据分析辅助工具；

e) 应测试是否禁止所有未授权用户对审计数据的访问。

5.1.2.6 选择性审计（FAU_SEL.1）

选择性审计组件定义了向可审计事件集中加入或从中排除事件的能力。该组件安全评估内容如下：

a) 应测试是否能根据【选择：*客体身份*、*用户身份*、*组身份*、*主体身份*、*主机身份*、【*赋值：ST 作者指定主体属性*】】从审计事件集中选择可审计事件；

b) 应测试是否能根据【选择：*数据库系统权限*、*语句级审计*、*权限级审计*、*模式对象级审计*、*列级数据权限*、*行级数据权限*、【*赋值：ST 作者指定用户操作权限级别*】】从审计事件集中选择可审计事件；

c) 应测试是否能根据【选择：*成功*、*失败*、*二者可审计安全事件选项*、【*赋值：ST 作者指定条件*】】从审计事件集中选择可审计事件；

d) 应测试是否能根据产品审计功能相关的附加属性列表从审计事件集中选择可审计事件。

5.1.2.7 审计数据可用性保证（FAU_STG.2）

审计数据可用性保证组件保证数据库管理系统的审计数据存储出现意外情况时，TSF 还能维护产生的审计数据。该组件安全评估内容如下：

a) 应测试是否能提供数据库系统表或外部文件方式保存审计事件数据，维护审计数据授权控制和审计数据存储管理的能力；

b) 应测试维护控制审计事件数据存储能力参数有效性；

c) 应测试保护所存储的审计记录，只允许安全管理员或授权管理员访问审计记录的访问机制；

d) 应测试 TSF 能【选择：*防止*、*检测*】对审计迹中所存审计记录的未授权修改；

e) 应测试提供的审计数据备份、导出等管理接口/辅助工具，并且只有安全管理员或授权管理员才能操作这些辅助功能；

f) 应测试审计事件具备数据加解密存储保护能力；

g) 应测试在 TSF【选择：*审计存储耗尽*、*失效*、*受攻击*】时，确保【赋值：*保存审计记录的度量*】审计记录将维持有效。

5.1.2.8 防止审计数据丢失（FAU_STG.4）

防止审计数据丢失组件规定了当存储在数据库内部审计迹溢满或存储在数据库外部磁盘中剩余空

间溢满时所采取的动作。该组件安全评估内容如下：

a) 应测试审计数据【选择：*多路复用*、【*赋值：ST 作者指定备份方式*】】功能，并验证审计数据存储位置指定等管理能力；

b) 应测试审计数据归档功能，包括远程归档功能；

c) 应检测审计数据存储可用空间查看视图/工具功能；

d) 应检查是否提供了判断审计记录数据是否已满，并提供忽略可审计事件、阻止可审计事件、覆盖所存储的最早的审计记录或【赋值：*审计存储失效时所采取的其他动作*】等处理机制。

5.1.3 密码支持（FCS 类）

5.1.3.1 密钥生成（FCS_CKM.1）

若密钥由外部环境生成，则检查外部环境提供的密钥生成器是否根据国家标准规定的算法和密钥长度来生成密钥；否则评估对象提供的用户密钥和数据密钥产生。该组件安全评估内容如下：

a) 应测试存储用户密钥装置或密钥管理服务器操作接口，确认数据库密钥存储位置是安全且有据可查的，包括提供与其数据本身具有同类型的密钥备份和恢复机制。

b) 应检测数据库用户密钥和数据密钥与加密的数据库本身分离存放管理接口与管理工具。

c) 应测试是否能根据评估对象【赋值：*ST 作者指定的标准与规范列表*】的特定密钥生成算法【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。

d) 应测试密钥生成提供下列密钥管理功能：

1) 应提供密钥属性配置管理，密钥属性的例子包括用户密钥类型【选择：*公开密钥*、*私有密钥*、*秘密密钥*【*赋值：ST 作者指定密钥类型*】】、有效期和使用用途【选择：*数字签名*、*密钥加密*、*密钥协商*、*数据加密*、【*赋值：ST 作者指定用途*】】；

2) 应提供密钥的存储及其使用接口，允许评估对象与外界连接的数据库应用程序接口与加密设备进行交互。

e) 应检查密码生成算法的赋值是否符合国家主管部门认可的相关标准及参数。

5.1.3.2 密钥销毁（FCS_CKM.4）

密钥销毁组件提供符合国家规定的密码管理算法的密钥销毁功能。该组件安全评估内容如下：

a) 应测试是否能根据评估对象【赋值：*ST 作者指定的密码管理算法*】的密钥销毁方法【赋值：*ST 作者指定的密钥销毁方法*】来销毁密钥；

b) 应检测数据库用户密钥、数据密钥等数据库密钥存放管理接口与管理工具；

c) 应检查密码销毁方法是否符合国家主管部门认可的相关标准。

5.1.3.3 密码运算（FCS_COP.1）

密码运算组件提供根据一个特定的算法和一个规定长度的密钥来进行密码运算功能。该组件安全评估内容如下：

a) 应测试是否能根据评估对象【赋值：*ST 作者指定的标准与规范列表*】在评估对象上使用特定的密码算法【赋值：*密码算法*】和密钥长度【赋值：*密钥长度*】执行【赋值：*密码运算列表*】，以验证数据库管理系统密码运算的有效性。

b) 应测试评估对象【赋值：*ST 作者指定的加密算法*】提供数据库透明加密功能。

c) 应测试是否能依据评估对象使用密码安全服务的用户应用、不同密码算法或密钥长度的使用策略及其机制、所运算数据的类型或敏感度密码服务等数据库管理系统安全服务测试密码运算的可用性。

d) 应验证密码运算事件是否被审计：
   1) 密码运算的类型可以包括数字签名的产生或验证、用于完整性校验的密码校验和的产生、安全散列的计算、数据加密或解密、密钥加密或解密、密钥协商和随机数生成；
   2) 主体属性包括同主体有关的主体角色和用户；
   3) 客体属性包括密钥的指定用户、用户角色、使用密钥的密码运算、密钥标识和密钥有效期。
e) 应检查评估对象的密码算法的具体赋值是否符合国家主管部门认可的相关标准及参数。

5.1.4 用户数据保护(FDP 类)

5.1.4.1 子集访问控制(FDP_ACC.1)

子集访问控制组件涵盖授权用户与数据库模式对象和数据库非模式对象之间的授权策略定义。该组件安全评估内容如下：

a) 应测试依据授权用户/授权管理员在数据库对象【选择：*表对象、索引对象、视图对象、约束、同义词、存储过程/函数、数据库文件、表空间/文件组、参数文件、【赋值：ST 作者指定的数据库对象】】*上授予的【选择：*查询、插入、更新、删除、【赋值：ST 作者指定的客体操作列表】】*执行相关的【选择：*GRANT、REVOKE 或【赋值：ST 作者指定的授权接口】】*授权管理。
b) 应测试依据级联授权方法管理【选择：*自主访问控制策略、基于角色控制策略、基于用户组控制策略、【赋值：ST 作者定义的基于属性的访问控制策略】】*限制授权用户/授权管理员访问权限扩散的控制能力。
c) 应测试依据评估对象的【选择：*自主访问控制策略、基于角色控制策略、基于用户组控制策略、【赋值：ST 作者定义的基于属性的访问控制策略】】*在【选择：*数据库级、实例级、【赋值：ST 作者定义的级别】】*执行【选择：*创建、修改、删除、【赋值：ST 作者指定的客体操作列表】】*执行相关的【赋值：*GRANT、REVOKE 或【赋值：ST 作者指定的授权接口】】*成功的执行授权管理。
d) 应测试依据【选择：*默认方式、【赋值：ST 作者指定方式】】*，阻止未授权用户/未授权管理员对数据库对象【选择：*表对象、索引对象、视图对象、约束、同义词、存储过程/函数、数据库文件、表空间、参数文件、【赋值：ST 作者指定的数据库对象】】*的访问操作。
e) 应测试是否能通过【选择：*安全元数据视图，应用程序接口、【赋值：ST 作者指定的方式】】*浏览成功授权的所有数据库级和实例级授权管理员定义的授权管理数据或评估对象安全配置参数。
f) 应测试基于安全目标中的附加规则【选择：*【赋值：安全属性，明确授权用户/授权管理员访问客体的规则】，“无附加规则”】*，分析评估对象的测试文档，采用抽样方式或独立性设计方法验证数据库客体对象访问控制机制的正确性。
g) 应测试基于安全目标中的【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”】*，分析评估对象的测试文档，采用抽样方式或独立性设计方法验证 TSF 拒绝主体访问数据库管理系统控制的客体对象的访问控制机制的正确性。

5.1.4.2 基于安全属性的访问控制(FDP_ACF.1)

基于安全属性的访问控制组件允许评估对象依据授权用户和访问对象的安全属性/属性组允许或拒绝某个鉴别用户对指定数据库对象的访问。该组件安全评估内容如下：

a) 应测试基于【选择：*自主访问控制策略、基于角色控制策略、基于用户组控制策略、【赋值：ST 作者定义的基于属性的访问控制策略】】*对数据库对象的相关操作执行访问控制，具体应包括：
   1) 与一个授权用户/授权管理员相关的授权用户身份和/或角色/组成员关系；
   2) 数据库对象(模式对象和非模式对象)可实施的访问操作和/或角色/组权限；

3） 对数据库对象执行【选择：*自主访问控制策略*、*基于角色控制策略*、*基于用户组控制策略*、【*赋值：ST 作者定义的基于属性的访问控制策略*】】，阻止未授权用户/管理员对数据库对象访问（模式对象和非模式对象）。

b） 应执行【赋值：*在授权用户/授权管理员和数据库对象之间，通过对数据库对象采取受控操作来管理访问的规则*】，以决定 DBMS 授权用户/授权管理员与数据库对象之间的操作是否被允许。这些规则包括：

1） 如果授权用户是访问数据库对象的所有者，则允许用户的访问请求；

2） 如果访问控制策略机制允许授权用户对数据库对象的访问，则允许用户的访问请求；

3） 如果授权用户作为一个用户组或角色（直接角色或间接角色）的成员执行请求的访问模式，则允许用户的访问请求；

4） 如果 PUBLIC 能访问受控的数据库对象，则允许用户的访问请求；

5） 否则拒绝用户的访问请求。

c） 应测试 DBMS 是否能通过【选择：*安全元数据视图，应用程序接口*、【*赋值：ST 作者指定的安全元数据访问方法*】】浏览成功授权的所有数据库对象操作列表和授权用户定义的【选择：*自主访问控制策略*、*基于角色控制策略*、*基于用户组控制策略*、【*赋值：ST 作者定义的基于属性的访问控制策略*】】安全元数据。

5.1.4.3 子集信息流控制（FDP_IFC.1）

子集信息流控制组件要求每个确定的基于标签访问控制（LBAC）安全策略适用于数据库管理系统内某些数据库对象上允许执行的访问请求。该组件安全评估内容如下：

a） 应测试基于授权用户/授权管理员和数据库对象安全属性【选择：*用户安全标签*、*关系的行或列安全性标签*、【*赋值：ST 作者指定数据库对象安全属性元素*】】强制应用【**LBAC 安全策略**】，通过标签中【选择：*安全分级*、*安全范围*、*安全分组值*、【*赋值：ST 作者指定的标签元素*】】的访问规则处理得到的输出来确定用户安全分类与数据标签分级判断是否通过，从而控制授权用户对标签受控的数据库对象的访问。

b） 应测试子集信息流控制是否配合评估对象提供的【选择：*自主访问控制策略*、*基于角色控制策略*、*基于用户组控制策略*、【*赋值：ST 作者定义的基于属性的访问控制策略*】】粗粒度访问控制，只有授权用户/授权管理员在获得访问某数据库模式权限后才应用【**LBAC 安全策略保护的数据库表中数据读、写操作**】访问控制引擎控制授权用户/授权管理员是否能够访问那些被标识由他们访问数据对象。

c） 应测试基于安全目标中的附加规则【选择：【*赋值：基于安全属性，明确拒绝信息流的规则*】，*“无附加规则”*】，分析评估对象的测试文档，采用抽样方式或独立性设计方法验证子集信息流控制机制对数据库客体对象访问控制的正确性。

d） 应测试基于安全目标中的【选择：【*赋值：基于安全属性，明确拒绝信息流的规则*】，*“无附加的显式拒绝规则”*】，分析评估对象的测试文档，采用抽样方式或独立性设计方法验证子集信息流控制机制拒绝授权用户访问受控数据库对象的正确性。

5.1.4.4 分级安全属性（FDP_IFF.2）

分级安全属性组件通过用户安全标签和数据分级安全属性构成的数据库分级安全属性网格，以供基于标签的访问控制数据安全策略使用。该组件安全评估内容如下：

a） 应测试是否能具有【选择：*安全分级*、*安全范围*、*安全分组*、【*赋值：ST 作者指定数据库对象安全属性元素*】】及基于这些元素的标签定义，包括标签与被保护数据库对象和授权用户/授权管理员的绑定关系定义接口或辅助工具。

b) 应测试是否能通过授权用户/授权管理员绑定标签和数据库对象(数据库数据表的行、列或属性值)绑定标签之间的信息流交换,如果满足以下基于安全属性之间的序关系的规则:【

1) **为了读取 LBAC 保护的数据库数据表的行、列或属性值:**

- **用户安全性标签的安全分级应大于或等于数据库数据表的行、列和属性值安全性标签的安全分级;**
- **用户安全性标签的安全范围应包含数据库数据表的行、列和属性值安全性标签的安全范围;**
- **用户安全性标签的安全分组应至少包含数据库数据表的行、列和属性值安全性标签的安全分组中的一个元素(或者这样一个元素的祖先)。**

2) **为了写 LBAC 保护的数据库数据表行、列或属性值:**

- **用户安全性标签的安全分级应小于或等于数据库数据表的行、列和属性值安全性标签的安全分级;**
- **用户安全性标签的安全范围应包含数据库数据表的行、列和属性值安全性标签的安全范围;**
- **用户安全性标签的安全分组应至少包含数据库数据表的行、列和属性值安全性标签的安全分组中的一个元素(或者这样一个元素的祖先)。**

3) **每一种情况中,在数据库对象操作的基于安全属性的访问控制策略的规则都应被满足】。**

c) 应测试只有授权管理员【选择:***安全管理员,【赋值:ST 规定的管理角色】能够改变用户的安全性标签,具有适当权限的授权用户/授权管理员***】能改变受 LBAC 保护的数据表的行、列和属性值的安全性标签属性。

d) 应测试拥有特权的安全管理员(豁免的用户)能够忽略对【选择:***读元组、读元组集合、读树、写元组、写元组集合、写树的检查、【赋值:ST 作者指定数据库对象标签类型】***】,明确地给数据库对象授权一个信息流。

e) 应测试基于规则【赋值:***基于安全属性,明确拒绝信息流的规则***】明确的拒绝一个数据库对象的信息流。

f) 应测试对任意两个信息流控制安全属性强制下列关系:

1) 存在一个有序函数,对于给定的两个有效的安全属性,函数能够判定它们是否相等,是否其中一个大于另一个,还是两者不可比较;

2) 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等于这两个安全属性;

3) 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。

5.1.4.5 带有安全属性的用户数据输出(FDP_ETC.2)

带有安全属性的用户数据输出组件要求 TSF 利用一个功能执行合适的 SFP,该功能准确无误地将 TOE 安全属性与所输出的用户数据相关联。该组件安全评估内容如下:

a) 应测试基于授权用户/授权管理员和数据库对象安全属性【选择:***用户安全标签、关系的行或列安全性标签、【赋值:ST 作者指定数据库对象安全属性元素】***】强制应用**【LBAC 安全策略】**,通过标签中【选择:***安全分级、安全范围、安全分组值、【赋值:ST 作者指定的标签元素】***】的访问规则处理得到的输出来确定用户安全分类与数据标签分级判断是否通过,从而控制授权用户对带有安全属性的用户数据的访问;

b) 应测试输出用户数据时评估对象提供相应的【选择：*自主访问控制策略*、*基于角色控制策略*、*基于用户组控制策略*、【*赋值：ST 作者定义的基于属性的访问控制策略*】】粗粒度访问控制，只有授权用户/授权管理员在获得访问某数据库模式权限后才应用【**LBAC 安全策略保护的数据库表中数据读、写操作**】访问控制引擎控制授权用户/授权管理员是否能够访问那些被标识由他们访问的用户数据；

c) 应测试基于安全目标中的附加规则【选择：【*赋值：基于安全属性，明确拒绝信息流的规则*】，“*无附加规则*”】，分析评估对象的测试文档，采用抽样方式或独立性设计方法验证带有安全属性的用户数据输出机制是否将安全属性与所输出的用户数据相关联；

d) 应测试输出用户数据时可依据用户数据的安全属性【选择：*用户安全标签*、*关系的行或列安全性标签*、【*赋值：ST 作者指定数据库对象安全属性元素*】】组织输出的数据；

e) 应测试用户数据安全属性的脱敏或匿名机制，确认评估对象具有对输出带有安全属性的用户数据安全保护能力；

f) 应测试带有安全属性的输出用户数据的属性一致性检测方法和技术。

5.1.4.6 不带安全属性的用户数据输入（FDP_ITC.1）

不带安全属性的用户数据输入组件要求安全属性正确表示用户数据，且与客体分离。该组件安全评估内容如下：

a) 应测试在【选择：*用户安全标签*、*关系的行或列安全性标签*、【*赋值：ST 作者指定数据库对象安全属性元素*】】控制下从 TOE 之外输入用户数据时，TSF 执行某个【赋值：*访问控制 SFP 和/或信息流控制 SFP*】；

b) 应测试从 TOE 外部输入带有安全属性的用户数据时，TSF 能忽略任何与用户数据相关的安全属性；

c) 应测试在【选择：*用户安全标签*、*关系的行或列安全性标签*、【*赋值：ST 作者指定数据库对象安全属性元素*】】控制下从 TOE 之外输入用户数据时，TSF 应执行下面的规则：【选择：*自主访问控制策略*、*基于角色控制策略*、*基于用户组控制策略*、【*赋值：ST 作者定义的输入控制规则*】】。

5.1.4.7 基本内部传送保护（FDP_ITT.1）

基本内部传送保护组件要求用户数据在 TOE 的各部分间传输时受保护。该组件安全评估内容如下：

a) 应检测数据库服务器数据字典共享缓冲和用户数据共享缓存隔离策略和机制，确保两个共享缓存间数据字典传输时受保护；

b) 应测试确认用户数据在数据库服务器的数据共享缓存和事务空间之间传输（逻辑 I/O）时受保护；

c) 应测试确认用户数据在数据库服务器的数据共享缓存和磁盘存储之间传输（物理 I/O）时受保护；

d) 应测试确认用户数据在分布式环境下不同数据库服务器数据共享缓存间传输（远程逻辑 I/O）时受保护；

e) 应测试确认远程用户数据输入/输出时的传输安全。

5.1.4.8 子集残余信息保护（FDP_RIP.1）

子集残余信息保护组件确保数据库对象数据在缓存、磁盘等共享存储资源分配或释放时，相关客体资源的任何残余信息内容都是不可再利用的。该组件安全评估内容如下：

a) 应测试确认数据库服务器共享内存、磁盘存储空间等服务器资源的任何先前的信息内容，在资

源被分配给其他授权用户/授权管理员使用之后是不再可用的；

b) 应测试确认授权用户/授权管理员执行清除数据(DELETE)、删除客体(DROP)或清空数据(TRANCATE)等数据库事务操作后，未授权用户/未授权管理员不能恢复相关数据；

c) 应测试确认授权管理员通过评估对象清除表空间、数据文件等逻辑存储和物理存储对象后，未授权用户/未授权管理员不能恢复相关数据存储对象；

d) 应测试当依赖评估对象其他系统的安全功能来完成数据库管理系统客体重用功能时，评估对象提供该客体重用功能的可信性的证据。

5.1.4.9 基本回退(FDP_ROL.1)

基本回退组件确保评估对象在既定的限制条件下回退或撤销有限个数据库操作，这是保证数据库完整性的基本机制。该组件安全评估内容如下：

a) 应测试评估对象的检查点保存(SAVEPOINT)机制，确认是否允许对复杂事务回退到指定事务保存点(即回滚部分 SQL 语句操作)；

b) 应测试评估对象的事务回退(ROLLBACK)机制，确认是否允许未提交数据库事务全体 SQL 语句的回滚操作；

c) 应测试 TOE 数据库服务器宕机等数据库实例，重启 DBMS 时的数据库故障恢复功能；

d) 应测试 TOE 数据库存储磁盘介质故障后的数据库恢复管理功能，包括【选择：***基于时间点***、【***赋值：ST 作者指定恢复方式***】】的数据库快速恢复功能；

e) 对于分布式部署环境下的数据库管理系统，应测试评估对象的两阶段提交机制，保证多副本数据的一致性和事务的原子性。

5.1.4.10 存储数据完整性监视和行动(FDP_SDI.2)

存储数据完整性监视和行动组件要求 TSF 监视存储在由 TSF 控制的载体内的用户数据是否存在已被识别的完整性错误，如检测到某个错误时应允许采取相应动作的能力。该组件安全评估内容如下：

a) 应测试评估对象的 TSF 在事务处理过程中基于【选择：***唯一***、***非空***、【***赋值：ST 作者指定的数据完整性约束条件***】】，对涉及的用户数据监视事务操作前后是否存在【赋值：***完整性错误***】，并在检测到错误时自动的启动事务回滚等机制，确保共享缓存中数据完整性；

b) 应测试评估对象的 TSF 在确保事务提交时，事务相关的日志是否通过日志写机制：【赋值：***ST 作者指定的日志先写机制***】将日志缓存数据存储到磁盘，并在提交事务的日志刷新到磁盘出现故障时自动的启动事务回滚等机制，确保用户数据完整性；

c) 应测试评估对象的 TSF 是否基于数据库对象依赖关系【选择：***索引数据***、***视图定义***、***存储过程***、【***赋值：ST 作者指定的定义的依赖关系***】】，对所有监控数据库对象(如表数据)，监视存储在由 TSF 控制的载体内的对象数据(如索引数据和用户数据)间是否存在【赋值：***完整性错误***】，并给出对象间存储数据(如表数据和索引数据)完整性检测方法和处理技术；

d) 应测试评估对象的 TSF 是否提供多副本存储数据完整性检测机制，并在检测到错误时自动的启动数据复制机制，确保副本数据的一致性；

e) 应测试评估对象的 TSF 是否提供归档日志数据存储完整性和一致性检测机制，并在检测到错误时指示用户采取必要的管控措施或机制，确保归档数据的完整性和可用性；

f) 应测试评估对象的 TSF 是否提供备份数据完整性检测机制，并在检测到错误时指示用户采取必要的管控措施或机制，确保备份数据的完整性和可用性；

g) 应测试评估对象的 TSF 是否在运行过程中确保联机数据文件的数据完整性，并在检测到错误时指示用户采取必要的管控措施或机制，确保存储数据的完整性和可用性。

5.1.5 标识和鉴别(FIA 类)

5.1.5.1 鉴别失败处理(FIA_AFL.1)

鉴别失败处理组件为不成功的用户鉴别尝试(包括尝试次数和时间的阈值)定义一个值,并明确规定达到该值时所应采取的动作。该组件安全评估内容如下:

a) 应测试【选择:*基于口令*、*基于令牌*、*基于生物特征*、【*赋值:ST 作者指定方式*】】的用户鉴别失败处理机制,即当检测到【赋值:*登录 DBMS 用户*】不满足授权管理员定义的鉴别策略【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:ST 作者指定的可接受值范围*】】时,TSF 应通过合适的方式告知【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信息;

b) 应测试 TSF 是否在不成功鉴别尝试的指定次数已达到或超出【赋值:*ST 作者指定可接受值范围*】,TSF 应阻止用户登录,直到授权安全管理员采取行动或直到授权安全管理员配置的时间【赋值:*ST 作者指定可接受值范围*】已经到达;

c) 应测试在数据库会话建立的进程终止后,数据库管理系统的安全功能能使得用户账户无效,或是进行尝试的登录点无效。

5.1.5.2 用户属性定义(FIA_ATD.1)

用户属性定义组件提供一组除用户标识外的安全属性,以用来执行评估对象受信任上下文相关的安全策略(TSP)。该组件安全评估内容如下:

a) 应测试确认 TSF 为每个授权数据库用户会话维护一个上下文对象,提供下列安全属性:

1) 用户标识/组成员及验证数据;
2) 用户安全相关的授权角色;
3) 用户口令与资源限制脚本标准;
4) 数据库对象访问权限;
5) 数据库管理权限;
6) 【赋值:*任何 ST 作者附加的管理员安全属性*】。

b) 应测试管理控制存储过程和用户定义函数的执行上下文切换的能力,确认提供通信协议信任属性、网络地址信任属性、网络加密信任属性、身份验证信任属性等受信任连接管理功能。

5.1.5.3 秘密的验证(FIA_SOS.1)

秘密验证组件对用户所提供的秘密(口令、密钥等)进行既定的质量度量以及生成满足既定度量的秘密。该组件安全评估内容如下:

a) 应测试确认 TSF 是否验证秘密满足【赋值:*一个既定的质量度量*】的秘密策略定义及秘密验证机制能力。例如:

1) 口令将被限制在最小和最大数量的字符长度之间;
2) 口令将包含一个大写和小写字符的组合;
3) 口令至少包含一个数字字符;
4) 口令至少包含一个特殊字符;
5) 口令不能是用户标识或用户名称;
6) 口令具有效期天数;
7) 以前使用的口令可能无法再度使用的最少天数等。

b) 应测试确认 TSF 能够为【赋值:*TSF 功能列表*】使用 TSF 产生的秘密。

c) 对于 TSF 外部机制产生的秘密，应测试确认 TSF 保证秘密满足 TSF 定义的安全策略（例如，一定长度、密文保存等）。

5.1.5.4 鉴别的时机（FIA_UAU.1）

鉴别的时机组件允许用户在其身份被鉴别前执行某些动作。该组件安全评估内容如下：

应测试确认 TSF 是否允许在用户被鉴别之前，代表用户的【赋值：*数据库管理系统安全功能促成的行动列表*】被执行。例如：

a) 获取当前数据库管理系统版本信息；
b) 建立数据库会话（连接信息）；
c) 获得用户登录帮助信息；
d) 如果不成功，返回错误信息。

5.1.5.5 多重鉴别机制（FIA_UAU.5）

多重鉴别机制组件提供多种用户鉴别机制，为特定的事件鉴别用户的身份。该组件安全评估内容如下：

a) 应测试 TSF 的【选择：*数据库鉴别*、*操作系统鉴别*、*第三方鉴别*【*赋值：ST 作者指定鉴别机制*】】等鉴别方式，以支持特定系统权限的数据库用户身份鉴别；
b) 应测试确认 TSF 是否允许数据库用户为不同的【选择：*数据库鉴别*、*操作系统鉴别*、*第三方鉴别*【*赋值：ST 作者指定鉴别机制*】】鉴别机制，配置相应的安全选件，提供多重鉴别机制管理接口与管理视图；
c) 应测试确认 TSF 是否依据选择【赋值：*多重鉴别机制的工作规则*】为授权管理员和授权用户鉴别任何用户所声称的身份；
d) 应测试确认 TSF 是否保证非数据库鉴别机制用户秘密的安全通信，以保证 TOE 通过鉴别服务器（IT 环境提供）对客户进行远程鉴别（操作系统鉴别、第三方鉴别）。

5.1.5.6 受保护的鉴别反馈（FIA_UAU.7）

受保护的鉴别反馈组要求数据库管理系统在鉴别时仅将最少信息反馈提供给用户。该组件安全评估内容如下：

a) 应测试当输入用户鉴别特征信息（如：打入的字符或字数）时，评估对象的反馈是否隐藏了相关信息；
b) 应测试当用户输入正确的鉴别特征信息时，鉴别成功评估对象的反馈信息是否泄露部分信息；
c) 应测试当用户输入正确的鉴别特征信息时，鉴别失败评估对象的反馈信息是否泄露部分信息。

5.1.5.7 标识的时机（FIA_UID.1）

标识的时机组件要求在 TSF 允许其执行任何动作之前，数据库用户识别他们自己。该组件安全评估内容如下：

a) 应测试确认 TSF 是否在允许任何其他代表用户的数据库管理系统安全功能促成的行动执行前，数据库管理系统安全功能应要求该用户已被成功标识；
b) 应测试确认 TSF 是否在允许任何数据库用户的数据库请求行动执行前，用户应能成功连接数据库，数据库鉴别组件应提供连接标识、连接状态、连接用户相关信息的数据字典视图与图形化查看工具；
c) 应测试确认已被成功鉴别用户信息保存在数据库会话信息中，数据库会话管理应提供包括会话标识、进程/线程标识、用户标识、最近的用户请求命令、缺省模式、客户应用程序、登录时间、

会话状态的数据字典视图与图形化查看工具。

5.1.5.8 用户-主体绑定(FIA_USB.1)

用户-主体绑定组件建立和维护用户安全属性与代表用户活动的主体间关联关系。该组件安全评估内容如下:

a) 应测试确认 TSF 将下列用户安全属性与代表用户活动的主体相关联:
   1) 用户标识;
   2) 口令管理信息;
   3) 用户权限;
   4) 用户角色;
   5) 绑定标签等。
b) 应测试确认 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:
   1) 在 TSF 鉴别用户身份成功,主体与数据库建立连接后,用户安全属性将保存到数据库会话中,通过主体会话可以获取用户标识等安全属性;
   2) 如果在用户属性定义中已经直接定义或通过角色等定义了数据库会话中用户的数据库对象和系统对象的权限信息,则一旦用户的数据库会话建立,相关的系统和数据库对象授权将生效;
   3) 用户可通过角色状态控制数据库会话中用户权限的可用性。
c) 应测试确认 TSF 在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:
   1) 如果授权用户会话当前的系统与对象权限被 TSF 直接或间接修改,用户会话中的权限应立即生效;
   2) 在用户连接数据过程中,用户能通过会话控制用户角色的启用与禁用;
   3) 如果用户操纵其他用户的视图、存储过程/函数,则一旦其他用户修改了这些数据库对象授权后,用户在下次使用这些数据库视图对象或存储过程/函数对象时生效;
   4) 用户在修改自己的口令策略时应符合授权管理员制定的安全策略。

5.1.6 安全管理(FMT 类)

5.1.6.1 安全功能行为的管理(FMT_MOF.1)

安全功能行为的管理组件允许授权用户/角色管理 TSF 中使用规则或具有指定可管理条件的功能的行为。该组件安全评估内容如下:

a) 应测试 TSF 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:
   1) 管理【赋值:*数据库管理系统实例安全功能组件配置参数*】;
   2) 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*】;
   3) 在安全告警事件中配置要【赋值:*执行行为*】的管理;
   4) 在鉴别失败事件中要【赋值:*采取行为*】的管理;
   5) 在用户成功被鉴别之前所能【赋值:*采取行为*】的管理;
   6) 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;
   7) 对重放攻击中所采取【赋值:*行为*】的管理;
   8) 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；

9) ST 中附加【赋值：***安全功能列表***】的管理。

b) 应测试确认 TSF 以视图的方式提供安全功能管理元数据管理辅助工具或查看视图。

c) 应测试 TSF 在 DBMS 的特定状态(如：安装或启动)中，检查安全功能的正确执行。

d) 应测试确认 TSF 为授权用户提供验证安全功能数据完整性的能力。

e) 应测试确认 TSF 为授权用户提供验证安全功能可执行码完整性的能力。

5.1.6.2 安全属性的管理[FMT_MSA_EXT.1(1)]

安全属性管理功能组件允许安全管理员查看和修改 TSF 安全属性。该组件安全评估内容如下：

a) 应测试 TSF 强制实施【赋值：***自主访问控制策略***、***基于角色控制策略***、***基于用户组控制策略***】，以仅限于【选择：***授权管理员或授权用户***】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***】】。

b) 应测试 TSF 强制实施【赋值：***基于标签的强制访问控制安全策略(LBAC SFP)***】，以仅限于【赋值：***LBAC 授权的用户***】能够【【***赋值：安全属性***】以【***赋值：安全标签***】】。

c) 应测试访问控制属性和用户角色赋予可以由具有适当权限的用户授予和撤销，授权管理员在指派给他们的数据库上总是可以通过属性配置修改用户的访问权限，安全管理员总是可以授予和撤销数据库用户的角色。

d) LBAC 策略允许用户将标签赋给部分受控主体和受控客体对象。

5.1.6.3 安全属性的管理[FMT_MSA_EXT.1(2)]

安全属性管理功能组件允许安全管理员查看和修改 TSF 安全属性。该组件安全评估内容如下：

a) 应测试 TSF 强制实施【赋值：***自主访问控制策略***、***基于角色控制策略***、***基于用户组控制策略***】，以仅限于【选择：***授权管理员或授权用户***】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***】】。

b) 应测试 TSF 强制实施【赋值：***基于标签的强制访问控制安全策略(LBAC SFP)***】，以仅限于【赋值：***LBAC 授权的用户***】能够【【***赋值：安全属性***】以【***赋值：安全标签***】】。

c) 应测试访问控制属性和用户角色赋予可以由具有适当权限的管理员授予和撤销，授权管理员在指派给他们的数据库上总是可以通过属性配置修改用户的访问权限，安全管理员总是可以授予和撤销数据库用户的角色。

d) LBAC 策略允许用户将标签赋给所有受控主体和受控客体对象，只对 EAL4 级评估对象有效。

5.1.6.4 静态属性初始化(FMT_MSA_EXT.3)

静态属性初始化功能组件确保数据库安全配置参数及安全属性的默认值实际上设成了适当的允许或限制。该组件安全评估内容如下：

a) 应测试 TSF 与底层的操作系统的权限设置相一致的特权用户、特权用户组、作业管理权限及例级和数据库级的各种系统特权权限及其权限管理机制和方法，例如，数据库实例各种进程/线程运行权限的设置，与主机安全属性相关的设置(在 Windows 平台是注册表，在 unix/linux 平台是/etc/下的相关文件)等；

b) 应测试确认 TSF 是否依照【赋值：***自主访问控制策略***、***基于角色控制策略***、***基于用户组控制策略***】，为用于执行安全功能策略的数据库对象的安全属性提供【赋值：***受限的***】默认值；

c) 应测试确认静态属性初始化适用的数据库对象(如数据库或数据库表)，确认当较低级别的对象(例如，行，单元)创建时，默认情况下这些对象可能继承顶层对象的权限。

5.1.6.5 TSF 数据的管理(FMT_MTD.1)

TSF 数据的管理组件允许授权管理员(角色)控制评估对象安全功能管理数据的管理。这里的 TSF 数据包括数据库管理系统配置参数、数据库实例和数据库配置参数、数据库审计策略与数据、数据库事务特性及各种约束条件。该组件安全评估内容如下:

a) 应测试确认 TSF 是否仅限于具有【选择:*系统管理员*、*安全管理员*、【*赋值:授权管理员*】】角色的授权管理员能够【赋值:*替换缺省,修改,删除,【赋值:其他操作】*】 TOE 的【赋值:*用户标识和安全角色*】;

b) 应测试确认 TSF 是否仅限于具有【选择:*系统管理员*、*安全管理员*、【*赋值:授权管理员*】】角色的授权管理员能够【赋值:*替换缺省,修改,删除,【赋值:其他操作】*】TOE 的【赋值:*认证数据*】;

c) 应测试确认 TSF 是否仅限于具有【选择:*系统管理员*、*安全管理员*、【*赋值:授权管理员*】】角色的授权管理员能够【赋值:*包括或排除可审计事件*】;

d) 应测试确认 TSF 是否仅限于具有【选择:*系统管理员*、*安全管理员*、【*赋值:授权管理员*】】角色的授权管理员能够【**删除和【查看】**】TOE 的【赋值:*审计事件集*】;

e) 应测试确认 TSF 是否根据【赋值:*数据库对象列表*】仅限于【选择:*系统管理员*、*安全管理员*、【*赋值:授权管理员*】】能够在数据库对象及数据上执行操作【选择:*改变默认值*、*查询*、*修改*、*删除*、*清除*、【*赋值:其他操作*】】。

5.1.6.6 撤销(FMT_REV.1)

撤销组件负责处理数据库各种实体安全属性的撤销。该组件安全评估内容如下:

a) 应测试确认 TSF 是否仅限于【赋值:*已标识的授权角色*】能够撤销 TSC 内与【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:其他安全属性*】】;

b) 应测试执行规则【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:撤销规则的详细说明*】】等数据库对象属性管理能力。

5.1.6.7 管理功能规范(FMT_SMF.1)

管理功能规范组件提供系统接口以便于授权管理员定义控制被测数据库管理系统安全相关操作的参数。该组件安全评估内容如下:

a) 应测试确认 TSF 是否能执行【赋值:*DBMS 提供的安全管理功能列表*】安全管理功能。例如下列管理功能:

1) 添加和删除数据库用户;
2) 改变授权用户的数据库管理系统账户状态;
3) 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;
4) 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;
5) 配置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);
6) 管理连接数据库用户会话的属性;
7) 使能和禁用数据库加密功能;
8) 使能和禁用数据库用户角色状态;
9) 管理数据库加密密钥;
10) 创建和销毁加密密钥;
11) 启动和停止审计;

12） 定义审计策略，选择性审计；
13） 创建、删除和查阅审计记录数据；
14） 定义当审计文件填满时采取的行动；
15） 创建和删除基于标签的访问控制(LBAC)策略和标签；
16） 授权和撤销 LBAC 安全标签与授权用户/授权管理员与数据库对象的绑定；
17） 创建、删除、授权和撤销数据库角色；
18） 授权、撤销数据库管理员访问属性；
19） 管理数据库用户口令策略；
20） 管理数据库用户对系统资源使用的最大限额等。

b） 应测试确认 TSF 是否能以视图方式展示【赋值：***DBMS 提供的安全管理功能列表***】安全元数据或提供【赋值：***DBMS 提供的安全管理功能列表***】管理图形化工具。

5.1.6.8 安全角色(FMT_SMR.1)

安全角色组件要求数据库管理系统的安全功能应能支持维护授权角色。该组件安全评估内容如下：

a） 应测试确认 TSF 是否提供或安全管理定义的【赋值：***已标识的授权角色***】角色创建功能；
b） 应测试确认 TSF 是否提供或安全管理定义的【赋值：***已标识的授权角色***】角色授权管理功能；
c） 应测试确认 TSF 是否提供角色权限管理功能；
d） 应测试确认 TSF 是否提供角色启用、禁用功能；
e） 应测试确认 TSF 是否提供角色口令管理功能。

5.1.6.9 安全角色限制(FMT_SMR.2)

安全角色限制组件控制数据库用户的不同角色，包括控制角色之间关系的规则。该组件安全评估内容如下：

a） 应测试确认 TSF 是否维护系统提供或安全管理定义的【赋值：***已标识的授权角色***】角色；例如下列角色：
1） 安全管理员；
2） 审计管理员；
3） 数据库管理员；
4） 系统管理员；
5） 由授权的安全管理员定义的安全角色。

b） 应测试确认 TSF 是否能够把鉴别用户和数据库角色关联起来，通过数据库会话管理角色关联的用户系统权限和数据库权限。

c） 应测试确认 TSF 是否确保条件【赋值：***不同角色的条件***】得到满足，例如：
1） 所有角色应能本地管理评估对象；
2） 所有角色应能远程管理评估对象；
3） 所有角色是不同的，每个角色所执行的操作不能重叠，但下列情况除外：【赋值：***ST 作者许重叠的安全功能***】。

5.1.7 TSF 保护(FPT 类)

5.1.7.1 失效即保持安全状态(FPT_FLS.1)

失效即保持安全状态组件要求 TSF 失效时保持一种安全状态。该组件安全评估内容如下：

a) 应测试确认 TSF 是否保证网络通信出现暂时性故障，用户数据库会话处于安全状态；
b) 应测试确认 TSF 是否在数据约束条件不满足时能回退前面的操作；
c) 应测试确认 TSF 在处理用户请求的前台服务器进程故障时能保证事务的原子性和数据完整性；
d) 应测试确认 TSF 在日志写进程出席故障或日志文件存储空间出现故障时能阻止用户的请求，并提醒用户；
e) 应测试确认 TSF 在归档进程出席故障或归档日志存储空间出现故障时能提醒用户；
f) 应测试确认 TSF 在实时采集数据库缓存、CPU 计算能力等系统资源状态信息，并通过视图、图形界面或应用编程接口方式提供给用户；
g) 应测试确认 TSF 是否具备数据库、表空间、数据文件读写状态控制能力。

5.1.7.2 TSF 数据传送的分离(FPT_ITT.2)

TSF 数据传送的分离组件要求评估对象不同部分间传送时，TSF 应将用户数据从 TSF 数据中分离出来。该组件安全评估内容如下：

a) 应测试数据库事务空间、共享数据空间、磁盘空间等不同数据操作空间之间数据传输机制；
b) 应测试检查不同用户安全域数据的分离策略和实施机制；
c) 应测试确认数据库分布式部署环境下不同节点的认证机制；
d) 应测试确认数据库分布式部署时的安全功能数据在不同节点传送时不被【选择：***泄漏***、***篡改***、***丢失***】。

当数据在数据库管理系统不同部分间传送时，TSF 应将用户数据从 TSF 数据中分离出来。

5.1.7.3 无过度损失的自动恢复(FPT_RCV.3)

无过度损失的自动恢复组件是确保数据库运行出现故障后成功完成恢复数据库，使数据库回退到一个安全状态。该组件安全评估内容如下：

a) 应测试确认 TSF 在【赋值：***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***】】，数据库自动执行恢复时，TSF 能进入一种维护模式，该模式提供将 TOE 返回到一个安全状态的能力；
b) 应测试确认 TSF【赋值：***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***】】时，TSF 能通过自动化过程使数据库服务器返回到一个安全状态；
c) 应测试确认 TSF 提供从失效或服务中断状态数据库恢复的功能，检查在 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；
d) 应测试确认 TSF 提供【赋值：***ST 作者定义的数据库提交事务能被恢复机制***】的能力。

5.1.7.4 内部 TSF 的一致性(FPT_TRC.1)

内部 TSF 的一致性组件确保评估对象安全功能数据在多点复制时的一致性。该组件安全评估内容如下：

a) 应测试确认 TSF 在分布式部署时能保证 TSF 数据在不同节点间复制时是前后一致的；
b) 应测试确认 TSF 在含有所复制的 TSF 数据的 TOE 部分断开连接时，数据库管理系统安全功能在处理任何对【赋值：***依赖于 TSF 数据赋值一致性的安全功能列表***】的请求前，应确保重建连接后所复制 TSF 数据的一致性。

5.1.7.5 TSF 控制切换/故障转移(FPT_OVR_EXT.1)

TSF 控制切换/故障转移组件提供从一个数据库服务器 TSF 组件到另外一个数据库服务器 TSF

组件的 TSF 切换和故障转移能力。该组件安全评估内容如下：

a) 应测试确认 TSF 能依据用户指定的切换指令，保证在不丢失主/备用节点运行事务数据基础上提供主/备用节点 TSF 控制切换能力；

b) 应测试确认 TSF 能依据用户强制切换指令，保证在不丢失主/备用节点已提交事务数据基础上提供主/备用节点切换能力；

c) 应测试确认 TSF 确保故障切换/转移是针对多主副本节点数据一致性，确保 TSF 切换过程中数据不丢失。

5.1.8 资源利用(FRU 类)

5.1.8.1 降级容错(FRU_FLT.1)

降级容错组件要求如果发生了确定的失效，TOE 能继续正确发挥既定能力。该组件安全评估内容如下：

a) 应测试 DBMS 是否提供验证有关客户端、服务器、网络架构硬件的数据库通信协议及其配置的故障检测能力。

b) 应测试 DBMS 是否提供网络传输异常中断容错解决方案。

c) 应测试 DBMS 是否提供数据库实例启动/关闭时错误检测和处理能力。

d) 应测试 DBMS 是否提供数据库打开/关闭时错误检测和处理能力。

e) 应测试 DBMS 是否提供以下 3 种加载异常数据时的错误检测和处理能力：

1) 加载 DBMS 不支持的格式数据或较低版本的数据文件；

2) 加载一组超大的数据表数据；

3) 加载数据过程中，强制中断。

f) 应测试 DBMS 是否提供集中式事务恢复或分布式事务恢复处理能力。

g) 应测试 DBMS 是否提供支持事务死锁检测和避免。

h) 应测试 DBMS 是否提供数据库节点故障后的恢复能力。

i) 应测试 DBMS 是否提供故障时快速地切换到备用服务器的能力。

j) 应测试 DBMS 重要操作的提示与及时警告能力。

k) 应测试 DBMS 多实例快速切换时是否提供在集群环境下实现多机共享数据库并发事务处理、是否提供自动的实现事务并行处理及均分负载、是否实现数据库在故障时的容错和无断点恢复等容错能力。

l) 应测试 DBMS 是否提供控制数据多路复用、在线日志多路复用和归档日志多路复用能力。

m) 应测试数据库备份执行功能出现异常时，DBMS 其他功能是否不出现服务停止的异常。

n) 应测试备份过程中磁盘空间不足或备份用磁盘出现故障时，DBMS 其他功能是否不出现服务停止的异常。

5.1.8.2 最低和最高配额(FRU_RSA.2)

最低和最高配额组件提供数据库服务器资源配额机制，确保用户能使用或不会独占数据库服务器受控资源。该组件安全评估内容如下：

a) 应测试 TSF 是否提供了对授权用户的【选择：*数据库查询和事务物理和逻辑 I/O 大小，永久数据库空间，临时数据库空间，一个特定作业持续使用时间或未使用时间，【赋值：ST 作者指定资源】】*资源分配最高配额，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；

b) 应测试 TSF 是否提供了对授权用户的【选择：*数据库查询和事务物理和逻辑 I/O 大小，永久数*

据库空间，临时数据库空间，一个特定作业持续使用时间或未使用时间，【赋值：ST 作者指定资源】】资源分配最高配额，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；

c) 应测试 TSF 是否提供了主体使用数据库服务器资源的视图、工具或 API。

5.1.9 TOE 访问(FTA 类)

5.1.9.1 可选属性范围限定(FTA_LSA.1)

可选属性范围限定组件规定数据库会话建立时限制会话安全属性范围的要求。该组件安全评估内容如下：

a) 应测试 DBMS 是否提供数据字典视图或图形化管理工具来查看下列用户会话信息：
   1) 会话编号；
   2) 进程编号；
   3) 用户标识；
   4) 用户姓名；
   5) 最近的用户请求命令、会话状态(在用、非活动、断开等)；
   6) 连接服务器方式(共享/非共享)；
   7) 缺省模式；
   8) 客户应用程序；
   9) 客户终端机器信息；
   10) 客户操作系统信息；
   11) 对应 SQL 语句/存储过程信息；
   12) 等待此会话的锁信息；
   13) 登录时间；
   14) 等待时间统计信息；
   15) 使用时间统计信息；
   16) 会话状态(等待、执行等)；
   17) 会话跟踪信息；
   18) 会话服务信息。

b) 应测试 DBMS 是否提供数据字典视图或图形化管理工具来查看数据库会话的连接信息：
   1) 连接名称；
   2) 连接用户信息；
   3) 状态信息；
   4) 使用协议；
   5) 连接类型(同构/异构)；
   6) 当前事务信息。

c) 应测试确认 TSF 是否依据基于【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*】。

d) 应测试确认 TSF 具备管理员对会话安全属性范围的管理能力。

5.1.9.2 多重并发会话的基本限定(FTA_MCS.1)

多重并发会话限定组件控制同一授权用户访问数据库的并发会话数，即规定基于用户安全属性限定并发会话的数量。该组件安全评估内容如下：

a) 应检查限制属于同一授权用户的并发会话的最大数目控制参数有效性；
b) 应能查看同一授权用户的当前并发会话信息；
c) 应能查看同一授权用户的每一个会话的客户端应用的【选择：*操作系统用户标识、客户端执行机器标识、客户端应用程序标识、【赋值：ST 作者指定属性】】*信息；
d) 应检查每个授权用户缺省地限定【赋值：*缺省数*】次会话的有效性。

5.1.9.3 TSF 原发会话终止(FTA_SSL.3)

TSF 原发会话终止组件要求 TSF 提供原发和用户原发的交互式会话的锁定、解锁和终止能力。该组件安全评估内容如下：

a) 应测试 TSF 在规定的时间内用户一直不活动，系统就发起对一个交互式会话的锁定能力；
b) 应测试 TSF 提供用户锁定和解锁其拥有的交互式会话的能力；
c) 应测试 TSF 提供用户在一段指定时间不活动后终止该会话的能力；
d) 应测试 TSF 为用户提供自己终止交互会话的能力。

5.1.9.4 TOE 访问历史(FTA_TAH.1)

TOE 访问历史组件为授权用户显示访问该用户账号的成功和不成功尝试历史的一些信息，并保存和检索这些相关信息。该组件安全评估内容如下：

a) 应测试在 TOE 会话成功建立的基础上，TSF 向用户显示上一次成功建立的会话的【赋值：*日期、时间、访问方法和位置*】；
b) 应测试在 TOE 会话成功建立的基础上，TSF 显示上一次会话建立的未成功尝试的【赋值：*日期、时间、访问方法和位置*】和从上一次成功的会话建立以来的不成功尝试次数；
c) 应测试如果评估对象没有向授权用户提供审阅访问历史信息的机会，TSF 就不能从 TOE 访问历史中或使用用户接口擦除该用户的 TOE 访问信息；
d) 应检查给授权管理员提供访问 TOE 访问历史数据接口或视图，确认能看到 TOE 访问历史。

5.1.9.5 TOE 会话建立(FTA_TSE.1)

TOE 会话建立组件提供了拒绝用户基于属性对 TOE 进行访问的要求。该组件安全评估内容如下：

a) 应测试确认能基于【赋值：*用户身份和/或组身份，主机标识、客户端网络地址标识、时间、【赋值：ST 作者指定属性】】*接受或拒绝数据库会话的建立；
b) 应测试确认提供了 TOE 会话客户端应用的【选择：*操作系统用户标识、客户端执行机器标识、客户端应用程序标识、【赋值：ST 作者指定属性】】*连接信息管理视图或应用开发接口；
c) 应测试属于同一授权用户/授权管理员的并发会话的接受或拒绝数据库会话建立的最大数目；
d) 应检查【选择：*正执行 SQL 语句、等待操作、被标注为删、【赋值：ST 作者指定状态】】*会话状态查看功能；
e) 应测试 TOE 会话【赋值：*用户身份和/或组身份，主机标识、客户端网络地址标识、时间、【赋值：ST 作者指定属性】】*会话属性查看功能；
f) 应测试 TOE 会话终止管理功能。

5.1.10 可信路径/信道(FTP 类)

TSF 间可信信道(FTP_ITC.1)：

TSF 间可信信道组件确保分布式数据处理在 TSF 和其他可信 IT 产品之间建立一个可信信道，并能保护通信数据免遭修改和泄露。该组件安全评估内容如下：

a) 对于分布式部署环境下的 TOE，应检查在不同节点间是否提供了一条缓存与控制通信信道，确认此信道在逻辑上与客户端与数据库服务器之间通信信道不同，其端点具有保证标识，并且能保护信道中数据免遭修改或泄露；
b) 应检查是否允许【选择：*TSF*、*基于外部认证的鉴别服务器*、【*赋值：ST 作者指定的另一个可信 IT 产品*】】经由可信信道发起通信；
c) 应检查【赋值：*需要可信信道的功能列表*】，测试确认 TSF 经由可信信道发起通信。

5.2 安全保障评估

5.2.1 开发（ADV 类）

5.2.1.1 安全架构描述（ADV_ARC.1）

安全架构描述组件评估是确定数据库的 TSF 结构是否使 TSF 不能被篡改或绕过，且提供安全域的 TSF 是否分离了这些域。安全评估活动的证据包括：安全目标、数据库安全功能规范、TOE 设计文档、安全架构描述、TOE 实现技术资料、操作性用户指南等。该组件安全评估内容如下：

a) 评估者应检查安全架构的描述，以确定证据提供的信息的详细水平与在细节与功能规范和 TOE 设计文件中包含的 SFR 强制实施抽象的描述相称；
b) 评价者应检查安全架构的描述，以确定它描述了 TSF 维护的安全域；
c) 评估者应检查安全架构描述以确定初始化过程保持了安全性；
d) 评估者应检查安全架构描述，以确定它包含的信息足以证明 TSF 能够保护自身不受非受信活动实体的篡改；
e) 评估者应检查安全架构描述，以确定该描述的分析充分说明了 SFR 强制实施机制是如何不能被绕过的；
f) 评估者也应确保安全架构描述是全面的，表现为每个接口都结合声明的 SFR 的全集进行了分析。

5.2.1.2 安全执行功能规范（ADV_FSP.2）

安全执行功能规范组件评估是确认开发者是否对 TOE 安全功能接口的目的、使用方法机器参数作了充分描述。另外每个安全功能接口的行为、结果、出错信息描述应足够充分，以便评估人员能确认 TSFI 是安全相关的。安全执行功能规范组件评估证据包括：安全目标、功能规范、TOE 设计。如果 TOE 的 ST 有评估证据的话，那么所使用的评估证据应包括：安全架构描述和用户操作指南。该组件安全评估内容如下：

a) 评估者应检查功能规范，标识出 TSF 对应的 TSFI，以确定该规范完整地描述了 TSF 的接口；
b) 评估者应检查功能规范，以确认是否描述了每个 TSFI 目的，以使得评估者能够理解这些接口；
c) 评估者应检查功能规范，以确定该规范完整地描述了每个 TSFI 的使用方法；
d) 评估者应检查 TSFI 的表示，以确定该表示完整地指出了与各 TSFI 相关的所有参数；
e) 评估者应检查 TSFI 的表示，以确定该表示完整和准确地描述了各 TSFI 相关的所有参数；
f) 评估者应检查 TSFI 的表示所有相关行动，以确定外部 TOE 安全功能接口进行详细的描述，以使得评估者能够确定接口是否是与安全相关的；
g) 评估者应检查 TSFI 的表示，以确定其充分并正确地描述了各外部接口的相关参数、异常和出错信息的 TOE 行为；
h) 评估者应检查功能规范，以确定 SFR 能够追溯到对应的 TSFI；
i) 评估者应检查功能规范，以确定它是 TOE 安全功能要求的一个准确且完备的实例化。

5.2.1.3 带完整摘要的功能规范(ADV_FSP.3)

带完整摘要功能规范组件评估是确认开发者是否对 TOE 安全功能接口的目的、使用方法机器参数作了充分描述。另外每个安全功能接口的行为、结果、出错信息描述应足够充分,以便评估人员能比较不同 TSFI 之间安全相关强度。带完整摘要功能规范组件评估证据包括:安全目标、功能规范和 TOE 设计。如果 TOE 的 ST 有评估证据的话,那么所使用的评估证据应包括:安全架构描述、实现表示、TSF 内部描述和用户操作指南。该组件安全评估内容如下:

a) 评估者应检查功能规范,标识出 TSF 对应的接口(TSFI),以确定该规范完整地描述了 TSF 的接口;
b) 评估者应检查功能规范,以确认是否描述了每个 TSFI 目的,以使得评估者能够理解这些接口;
c) 评估者应检查功能规范,以该规范完整地描述了每个 TSFI 的使用方法;
d) 评估者应检查 TSFI 的表示,以确定该表示完整地指出了与各 TSFI 相关的所有参数;
e) 评估者应检查 TSFI 的表示,以确定该表示完整和准确地描述了各 TSFI 相关的所有参数;
f) 评估者应检查 TSFI 的表示所有相关行动,以确定外部 TOE 安全功能接口进行详细的描述,以使得评估者能够确定接口是否是与安全相关的;
g) 评估者应检查 TSFI 的表示,以确定其充分并正确地描述了各外部接口的相关参数、异常和出错信息的 TOE 行为;
h) 评估者应检查 TSFI 的表示,以确定每个 TSFI 是否概述了 SFR 支持和 SFR 不相关的行为;
i) 评估者应检查功能规范,以确定 SFR 能够追溯到对应的 TSFI;
j) 评估者应检查功能规范,以确定它是 TOE 安全功能要求的一个准确且完备的实例化。

5.2.1.4 完备的功能规范(ADV_FSP.4)

完备的功能规范组件评估时确定开发者是否完全描述了所有 TSFI,描述的方式是否可使评估者能够肯定 TSFI 完整精确地描述了执行 ST 的安全功能需求。接口的完整度是基于实现介绍判断的。完备的功能规范组件评估证据包括:安全目标、功能规范、TOE 设计和实现表示。如果 TOE 的 ST 有评估证据的话,那么所使用的评估证据应包括:安全体系结构描述、TSF 内部描述、安全策略模型。该组件安全评估内容如下:

a) 评估者应检查功能规范,标识出 TSF 对应的 TSFI,以确定该规范完整地描述了 TSF 的接口;
b) 评估者应检查功能规范,以确定接口描述的结构化/半结构化、上下一致,并使用常用术语;
c) 评估者应检查功能规范,以确定它说明了各 TSFI 接口所提供的功能的总述;
d) 评估这应检查功能规范,以确定规范给出了各 TSFI 的使用方法;
e) 评估者应检查功能规范,以确定 TSFI 的完整性;
f) 评估者应检查 TSFI 的表示,以确定该表示完整地指出了与各 TSFI 相关的所有参数;
g) 评估者应检查 TSFI 的表示,以确定该表示完整和准确地描述了各 TSFI 相关的所有参数;
h) 评估者应检查 TSFI 的表示,以确定该表示完整地、准确地描述了与各 TSFI 相关的所有行动;
i) 评估者应检查 TSFI 的表示,以确定该表示完整地、准确地描述了调用各 TSFI 产生的所有错误信息;
j) 评估者应检查 TSFI 的表示,以确定该表示完整和准确地描述了调用各 TSFI 产生的所有错误信息;
k) 评估者应检查功能规范,以确定规范完整地、准确地描述了调用一个 TSFI 不会产生的所有错误信息;
l) 评估者应检查功能规范,以确定对于每一个包含在 TSF 实现内但不是从 TSFI 调用中产生的

错误，该规范都给出了原因；

m） 评估者应检查功能规范，以确定 SFR 能够追溯到对应的 TSFI；

n） 评估者应检查功能规范，以确定它是 TOE 安全功能要求的一个准确且完备的实例化。

5.2.1.5 TSF 实现表示（ADV_IMP.1）

TSF 实现表示组件评估是确定开发者编写的实现介绍适合于给其他分析活动使用；其适用性由它与该组件需求的一致性决定。TSF 实现表示组件评估证据包括：实现表示、与 ALC-TAT 相关的开发工具文档和 TOE 设计描述。该组件安全评估内容如下：

a） 评估者应检查实现表示，以确定其无歧义地定义了 TSF，且详细程度达到了不需要进一步的设计就能生成 TSF 的程度；

b） 评估者应检查开发者提供的实现表示，以确定它是以开发人员使用的形式提供的；

c） 评估者应检查 TOE 设计描述与实现表示示例之间的映射应能证明它们的一致性的。

5.2.1.6 基础设计（ADV_TDS.1）

基础设计组件评估是确定 TOE 的设计是否提供了一个足以确定 TSF 边界的描述，以供评估者确定 TOE 完整、准确地执行了 SFR。基础设计组件评估证据包括：安全目标、功能规范、安全架构和 TOE 设计。该组件安全评估内容如下：

a） 评估者应检查 TOE 设计，以确定它以子系统方式描述了整个 TOE 结构；

b） 评估者应检查 TOE 设计，以确定整个 TSF 所有子系统都进行了标识；

c） 评估者应检查 TOE 设计，以确定 TSF 的 SFR-支撑或 SFR-无关子系统行为被足够描述清楚，以保证评估人员能区分 SFR-支撑或 SFR-无关子系统；

d） 评估者应检查 TOE 设计，以确定它完整、准确和详细地描述了 TSF 的 SFR-执行子系统的 SFR-执行行为；

e） 评估者应检查 TOE 设计，以确定它描述了 TSF 各子系统之间的相互作用；

f） 评估者应检查 TOE 设计，以确定 TOE 设计中描述的所有行为能够映射到调用它的 TSFI；

g） 评估者应检查 TOE 设计，以确定设计是所有安全功能要求的正确且完备的实例。

5.2.1.7 结构化设计（ADV_TDS.2）

结构化设计组件评估是确定高层设计是否按照子系统提供了 TSF 的描述，提供了这些子系统接口的描述，并是功能规范的一个正确实现。结构化设计组件评估证据包括：安全目标、功能规范、安全架构描述和 TOE 设计描述。该组件安全评估内容如下：

a） 评估者应检查 TOE 设计，以确定它以子系统方式描述了整个 TOE 设计；

b） 评估者应检查 TOE 设计，以确定整个 TSF 所有子系统都进行了标识；

c） 评估者应检查 TOE 设计，以确定 TSF 的 SFR-无关子系统的行为描述足够让评估者确认 SFR-无关的子系统；

d） 评估者应检查 TOE 设计，以确定它完整、准确和详细地描述了 TSF 的 SFR-执行子系统的 SFR-执行行为；

e） 评估者应检查 TOE 设计，以确定它完整和准确地提供了 SRF-执行子系统的 SFR-支撑和 SFR-无关的行为描述；

f） 评估者应检查 TOE 设计，以确定它完整和准确地提供了 SFR-支撑子系统的行为描述；

g） 评估者应检查 TOE 设计，以确定它描述了 TSF 各子系统之间的相互作用；

h） 评估者应检查 TOE 设计，以确定 TOE 设计中描述的所有行为能够映射到调用它的 TSFI；

i） 评估者应检查 TOE 设计，以确定设计是所有安全功能要求的正确且完备的实例。

5.2.1.8 基础模块设计(ADV_TDS.3)

基础模块设计评估是确定 TOE 设计是否提供了一个足以确定 TSF 边界的描述,且以模块方式描述了 TOE 内部描述。它提供了 SFR-执行模块和 SFR-支撑模块的详细描述,以供评估者确定 TOE 完整、准确地执行了 SFR。基础模块设计组件评估证据包括:安全目标、功能规范、安全架构描述和 TOE 设计描述。该组件安全评估内容如下:

a) 评估者应检查 TOE 设计,以确定它以子系统方式描述了整个 TOE 设计;
b) 评估者应检查 TOE 设计,以确定完整的 TSF 是以模块方式描述的;
c) 评估者应检查 TOE 设计,以确定整个 TSF 所有子系统都进行了标识;
d) 评估者应检查 TOE 设计,以确定 TSF 的每个子系统描述了它在安全目标中 SRF 强制实施的角色;
e) 评估者应检查 TOE 设计,以确定 TSF 中每个 SFR-无关子系统描述的足够让评估者确认它是 SFR-无关子系统;
f) 评估者应检查 TOE 设计,以确定 TSF 各子系统之间的相互作用已经描述;
g) 评估者应检查 TOE 设计,以确定提供了 TSF 子系统到 TSF 模块间的映射关系;
h) 评估者应检查 TOE 设计,以确定每一个 SFR-执行模块,包括它的目的及与其他模块间的相互作用;
i) 评估者应检查 TOE 设计,以确定每一个 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;
j) 评估者应检查 TOE 设计,以确定描述每一个 SFR-支撑或 SFR-无关模块,包括它的目的及与其他模块间的相互作用;
k) 评估者应检查 TOE 设计,以确定映射关系应论证 TOE 设计中描述的所有行为能够映射到调用它的 TSFI。

5.2.2 指导性文档(AGD 类)

5.2.2.1 操作用户指南(AGD_OPE.1)

操作用户指南组件是判断用户手册是否描述了每个用户角色的安全功能和 TSF 接口,是否说明了 TOE 的安全使用方法,是否所有操作模式的安全步骤,是否有简易的 TOE 不安全状态的预防和探测,以及是否有歧义或其他不合理内容。操作用户指南组件评估依据包括安全目标、功能规范、TOE 设计和用户操作指南。该组件安全评估内容如下:

a) 评估者应检查用户操作手册,以判断它是否描述了,每个用户角色的可用的功能,在安全处理环境控制下的权限,包括适当的警告;
b) 评估者应检查用户操作手册,以判断它是否描述了每个用户角色相应的 TOE 提供接口的安全用法;
c) 评估者应检查用户操作手册,以判断它是否描述每个用户角色可用的功能和接口,特别是用户可以控制的安全参数,指出安全参数合适的数值;
d) 评估者应检查用户操作手册,以判断它是否描述了每个用户角色每种需要演示的功能的安全相关事件,包括在 TSF 控制下的实体的属性变更和运行失败和错误之后的操作;
e) 评估者应检查用户操作手册和其他评估证据,以判断手册是否指出所有可能的 TOE 操作的模式(包括,可选的,运行失败和错误之后的操作),它们对维护安全操作的影响和后果;
f) 评估者应检查用户操作手册,以判断它是否对每个用户角色描述了,应当运用的安全措施,以满足 ST 描述的安全操作环境的安全目标;

g) 评估者应检查用户操作手册，以判断它是否清晰；
h) 评估者应检查用户操作手册，以判断它是否合理。

5.2.2.2 准备程序(AGD_PRE.1)

准备程序组件判断 TOE 的安全准备步骤是否被记录并得到安全的配置。准备程序组件评估依据包括安全目标、TOE 及其准备步骤和开发者提供服务的步骤。该组件安全评估内容如下：

a) 评估者应检查接受步骤，以判断是否描述了所有安全接受 TOE 交付的必要步骤，以及和开发商交付步骤的配合；
b) 评估者应检查所提供的安装步骤，以判断是否描述了，TOE 安全安装的所有必要步骤；为了达到依据 ST 描述了操作环境的安全目标，所需进行的安全准备步骤；
c) 评估者应运行所有必要的 TOE 准备步骤，以判断只有用给定的准备步骤，TOE 和它的操作环境可以被安全的准备。

5.2.3 生命周期支持(ALC 类)

5.2.3.1 CM 系统的使用(ALC_CMC.2)

CM 系统的使用组件判断开发者是否已经清晰地定义了 TOE 及其相关的配置项，对这些配置项的修改是否恰当地由工具自动控制，以使得 CM 系统更少地受到人为错误或疏忽的影响。CM 系统的使用组件评估的依据包括安全目标、适合测试的 TOE 和配置管理文档。该组件安全评估内容包括：

a) 评估者应核查所提交评估的 TOE 是否标记了参照号；
b) 评估者应核查所使用的 TOE 参照号的一致性；
c) 评估者应核查所使用 CM 文档应有用于描述唯一标识配置项的方法；
d) 评估者应核查 CM 系统所有配置项以在 CM 文档中各配置项的一致性。

5.2.3.2 授权控制(ALC_CMC.3)

授权控制组件判断开发者使用 CM 唯一标识了所有的系统配置项，且每个配置项的修改都被 CM 系统控制。授权控制组件评估的依据包括安全目标、适合测试的 TOE 和配置管理文档。该组件安全评估内容如下：

a) 评估者应核查所提交评估的 TOE 是否标记了参照号；
b) 评估者应核查所使用的 TOE 参照号的一致性；
c) 评估者应核查所使用 CM 文档应有用于描述唯一标识配置项的方法；
d) 评估者应核查 CM 系统所有配置项标识与 CM 文档中各配置项方法相一致；
e) 评估者应核查在 CM 计划中描述的 CM 访问控制措施使得只能对配置项进行授权变更；
f) 评估者应核查在 CM 文档应包括一个 CM 计划；
g) 评估者应核查 CM 计划应描述 CM 系统是如何应用于 TOE 的开发过程；
h) 评估者应核查证据应证实所有配置项都正在 CM 系统下进行维护；
i) 评估者应核查证据应证实 CM 系统的运行与 CM 计划是一致的。

5.2.3.3 生产支持和接受程序及其自动化(ALC_CMC.4)

生产支持和接受程序及其自动化组件判断开发者是否已经清晰地定义了 TOE 及其相关的配置项，对这些配置项的修改是否恰当地由工具自动控制，以使得 CM 系统更少地受到人为错误或疏忽的影响。生产支持和接受程序及其自动化组件的依据包括安全目标、适合测试的 TOE 和配置管理文档。该组件安全评估内容如下：

a) 评估者应核查所提交评估的 TOE 是否标记了参照号；
b) 评估者应核查所使用的 TOE 参照号的一致性；
c) 评估者应核查所使用 CM 文档应有用于描述唯一标识配置项的方法；
d) 评估者应核查 CM 系统所有配置项标识与 CM 文档中各配置项方法相一致；
e) 评估者应核查在 CM 计划中描述的 CM 访问控制措施使得只能对配置项进行授权变更；
f) 评估者应核查在 CM 计划中提供了自动化的措施使得只能对配置项进行授权变更；
g) 评估者应核查 TOE 生产系统支持程序以确定 CM 系统应以自动化的方式支持 TOE 的生产；
h) 评估者应核查在 CM 文档应包括一个 CM 计划；
i) 评估者应核查 CM 计划确认是否描述了 CM 系统是如何应用于 TOE 的开发过程；
j) 评估者应核查 CM 计划确认是否描述了 TOE 配置项修改和增减的程序规范；
k) 评估者应核查证据应证实所有配置项都正在 CM 系统下进行维护；
l) 评估者应核查 CM 文档以确认它包含了 CM 计划规定的 CM 配置记录内容；
m) 评估者应核查证据应证实 CM 系统的运行与 CM 计划是一致的。

5.2.3.4 部分 TOE CM 覆盖(ALC_CMS.2)

部分 TOE CM 覆盖组件判断 TOE 中的配置列表是否包括了 TOE 所有组成，包括相关的评估证据。这些配置项应与 ALC_CMC 受控程序相一致。部分 TOE CM 覆盖组件的安全评估依据包括安全目标和配置列表。该组件安全评估内容如下：

a) 评估者应核查配置列表以确认包括：TOE 本身、安全保障要求的评估证据和 TOE 的组成部分；
b) 评估者应核查配置列表以确认能唯一标识使用配置项；
c) 评估者应核查配置列表以确认对于每一个 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。

5.2.3.5 实现表示 CM 覆盖(ALC_CMS.3)

实现表示 CM 覆盖组件判断 TOE 中的配置列表是否包括了 TOE 所有组成，TOE 实现表示和相关的评估证据。这些配置项应与 ALC_CMC 受控程序相一致。实现表示 CM 覆盖组件的安全评估依据包括安全目标和配置列表。该组件安全评估内容如下：

a) 评估者应核查配置列表以确认包括：TOE 本身、TOE 实现表示、安全保障要求的评估证据和 TOE 的组成部分；
b) 评估者应核查配置列表以确认能唯一标识使用配置项；
c) 评估者应核查配置列表以确认对于每一个 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。

5.2.3.6 问题跟踪 CM 覆盖(ALC_CMS.4)

问题跟踪 CM 覆盖组件判断 TOE 中的配置列表是否包括了 TOE 所有组成，TOE 实现表示、安全弱点和相关的评估证据。这些配置项应与 ALC_CMC 受控程序相一致。问题跟踪 CM 覆盖组件的安全评估依据包括安全目标和配置列表。该组件安全评估内容如下：

a) 评估者应核查配置列表以确认包括：TOE 本身、TOE 实现表示、安全保障要求的评估证据、安全缺陷报告及其解决状态和 TOE 的组成部分；
b) 评估者应核查配置列表以确认能唯一标识使用配置项；
c) 评估者应核查配置列表以确认对于每一个 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。

5.2.3.7 交付程序(ALC_DEL.1)

交付程序组件评估目的是确定交付文档是否描述了在将 TOE 分发到用户现场时,用于保持其安全性的所有程序。交付程序组件安全评估证据包括安全目标和交付文档。该组件安全评估内容如下:

a) 评估者需要检查交付文档,以确定它描述了在将 TOE 版本及其部件发布给消费者时,所有维护安全性所需的过程;

b) 评估者应检查交付过程的各个方面,以确定其使用了交付程序。

5.2.3.8 安全措施标识(ALC_DVS.1)

安全措施标识组件评估目的是确定开发者在开发环境中的安全性操作足以提供 TOE 设计和实现的保密性和完整性。安全措施标识评估依据安全目标和安全开发。该组件安全评估内容如下:

a) 评估者应检查开发安全性文档,以确定它细化了在开发环境中用到的所有安全性度量,确认 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;

b) 评估者应检查开发的保密性和完整性策略,以确定使用的安全性措施是足够的;

c) 评估者需要检查开发安全性文档及相关的安全评估证据,以确定各种安全措施都已经被应用。

5.2.3.9 开发者定义的生命周期模型(ALC_LCD.1)

开发者定义的生命周期模型组件评估目标是确定开发者是否使用了文档化且可度量的 TOE 生命周期模型。开发者定义的生命周期模型组件安全评估依据包括安全目标和生命周期定义文档。该组件安全评估内容如下:

a) 评估者应检查所使用的生命周期模型的文档化描述,以确定它覆盖了开发和维护的过程,包括其计算参数的细节和/或用于度量 TOE 开发的指标;

b) 评估者应检查生命周期模型,以确定由生命周期模型描述的程序、工具和技术的使用将对 TOE 的开发和维护作出必要的积极贡献;

c) 评估者应检查生命周期输出文档,以确定它提供了使用可度量的生命周期模型的 TOE 开发的度量结果。

5.2.3.10 明确定义的开发工具(ALC_TAT.1)

明确定义的开发工具组件安全评估目的是确定开发者和他的分包商是否使用了良好定义的、产出一致的和预期的结果的开发工具[比如编程语言或者计算机辅助设计系统(CAD)],并确定是否应用了实现标准。明确定义的开发工具评估依据包括开发者标识的用于开发 TOE 的每个工具和每个开发工具所选取的实现依赖选项。该组件安全评估内容如下:

a) 评估者应核查用于实现的每个开发工具都应是明确定义的;

b) 评估者应核查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;

c) 评估者应核查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。

5.2.4 安全目标评估(ASE 类)

5.2.4.1 符合性声明(ASE_CCL.1)

符合性声明组件安全评估目的是确认安全目标与安全要求(保护轮廓)的一致性。符合性声明组件安全评估依据包括开发者提供的符合性声明和符合性声明的基本原理。该组件安全评估内容如下:

a) 评估者应核查安全目标的符合性声明，确认标识出 ST 和 TOE 声明符合性遵从的 GB/T 18336的版本；
b) 评估者应核查安全目标的符合性声明，确认描述了 ST 和 GB/T 18336.2—2015 的符合性，无论是与 GB/T 18336.2—2015 相符或是与 GB/T 18336.2—2015 的扩展部分相符；
c) 评估者应核查安全目标的符合性声明，确认描述了 ST 和 GB/T 18336.3—2015 的符合性，无论是与 GB/T 18336.3—2015 相符或是与 GB/T 18336.3—2015 的扩展部分相符；
d) 评估者应核查 GB/T 18336.2—2015 的符合性声明，确认功能扩展组件定义是相一致的；
e) 评估者应核查 GB/T 18336.3—2015 的符合性声明，确认保障扩展组件定义是相一致的；
f) 评估者应核查符合性声明应标识 ST 声明遵从的所有 PP 和安全要求包；
g) 评估者应核查符合性声明，对 ST 中每一个可标识，描述了符合性声明，无论是与包的相符或是与扩展包相符；
h) 评估者应核查符合性声明的基本原理，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；
i) 评估者应核查符合性声明的基本原理，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；
j) 评估者应核查符合性声明的基本原理，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；
k) 评估者应核查符合性声明的基本原理，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。

5.2.4.2 扩展组件定义（ASE_ECD.1）

对扩展组件定义的评估需要确定这些组件是明确的、没有歧义的并且是必要的。该组件安全评估内容如下：

a) 评估者应核查安全目标中所有不是标识为扩展安全要求的安全要求来自于 GB/T 18336.2—2015 或 GB/T 18336.3—2015；
b) 评估者应核查安全目标中扩展组件定义，确定每一个扩展的安全要求都定义一个扩展的组件；
c) 评估者需要核查扩展组件定义，确定每个扩展的组件使用了 GB/T 18336—2015 提供的组件、族和类定义格式，及与 GB/T 18336—2015 已有的组件、族和类关联性；
d) 评估者应核查扩展组件定义，确定每个扩展组件定义标识了这个组件所有可能的依赖关系；
e) 评估者应核查扩展组件定义，确定功能扩展组件的描述使用了 GB/T 18336.2—2015 组件作为其陈述的模型；
f) 评估者应核查扩展组件定义，确定功能扩展组件族的描述使用了 GB/T 18336.2—2015 族作为其陈述的模型；
g) 评估者应核查扩展组件定义，确定扩展组件类的描述使用了 GB/T 18336.2—2015 类作为其陈述的模型；
h) 评估者应核查扩展组件定义，确定保障扩展组件的描述使用了 GB/T 18336.3—2015 组件作为其陈述的模型；
i) 评估者应核查扩展组件定义，确定提供了每个保障扩展组件的评估方法；
j) 评估者应核查扩展组件定义，确定保障扩展组件族的描述使用了已有的保障族作为其陈述的模型；
k) 评估者应核查扩展组件定义，确定保障扩展组件类的描述使用了已有的保障类作为其陈述的模型；
l) 评估者应核查扩展组件定义，确保扩展组件是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；

m) 评估者应核查扩展组件定义，以确认扩展组件不能利用已经存在的组件明确的表达。

5.2.4.3 ST 引言(ASE_INT.1)

对 ST 引言的评估需要证实 ST 和 TOE 被正确标识，TOE 的三层抽象方式描述正确，并且这三方面的描述相互一致。该组件安全评估内容如下：

a) 评估者应核查开发者提供的 ST 引言，确认它包含 ST 参照号、TOE 参照号、TOE 概述和 TOE 描述；

b) 评估者应核查 ST 参照号，确认它能唯一标识 ST；

c) 评估者应核查 TOE 参照号，确认能唯一标识 TOE；

d) 评估者应核查 TOE 参照号，确认它不会误导消费者辨识 TOE；

e) 评估者应核查 TOE 概述，确认它正确的概括 TOE 的用法及其主要安全特性；

f) 评估者应核查 TOE 概述，确认它正确标识了 TOE 类型；

g) 评估者应核查 TOE 概述，确认它不会误导消费者辨识 TOE 类型；

h) 评估者应核查 TOE 概述，确认它标识了任何 TOE 要求的非 TOE 范围内的硬件/软件/固件；

i) 评估者应核查 TOE 描述，确认它正确的描述 TOE 的物理范围；

j) 评估者应核查 TOE 描述，确认它正确的描述 TOE 的逻辑范围；

k) 评估者应核查 TOE 参照号，TOE 概述和 TOE 描述，确认它们之间的相互一致性。

5.2.4.4 安全目的(ASE_OBJ.2)

安全目的评估是确定安全目的描述是否完备和一致，并确定安全目的是否能对抗已标识的威胁，实现已标识的组织安全策略并遵循规定的假设。该组件安全评估内容如下：

a) 评估者应核查开发者提供的安全目的的陈述，确认它描述 TOE 的安全目的和运行环境安全目的；

b) 评估者应核查安全目的基本原理，确认 TOE 的每一个安全目的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；

c) 评估者应核查安全目的基本原理，确认 TOE 运行环境的每一个安全目的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；

d) 评估者应核查安全目的基本原理，能证实安全目的能抵抗所有威胁；

e) 评估者应核查安全目的基本原理，能证实安全目的执行所有组织安全策略；

f) 评估者应核查安全目的基本原理，能证实运行环境安全目的支持所有的假设。

5.2.4.5 推导出的安全要求(ASE_REQ.2)

推导出的安全要求组件评估目的是确定 TOE 安全要求(包括 TOE 安全功能要求和 TOE 安全保证要求)和 IT 环境安全要求是否完备和一致，并为 TOE 的开发提供充分的基础，将达到其安全目的。该组件安全评估内容如下：

a) 评估者应核查安全要求的陈述是否描述了 TOE 安全功能要求；

b) 评估者应核查安全要求的陈述是否描述了 TOE 保障安全要求；

c) 评估者应核查安全目标，确认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了定义；

d) 评估者应核查安全要求的陈述，确认对安全要求的所有操作进行了标识；

e) 评估者应核查安全要求的陈述，确认所有赋值操作都应被正确地执行；

f) 评估者应核查安全要求的陈述，确认所有迭代操作都应被正确地执行；

g) 评估者应核查安全要求的陈述，确认所有选择操作都应被正确地执行；
h) 评估者应核查安全要求的陈述，确认所有细化操作都应被正确地执行；
i) 评估者应核查安全要求的陈述，确认安全要求间的依赖关系应满足，或者安全要求基本原理应证明不需要满足某个依赖关系；
j) 评估者应核查安全要求的基本原理，确认每一个安全功能要求可追溯至对应的 TOE 安全目的；
k) 评估者应核查安全要求的基本原理，证明安全功能要求可满足所有的 TOE 安全目的；
l) 评估者应核查安全要求的基本原理，确认有安全保障要求的选择理由。

5.2.4.6 安全问题定义(ASE_SPD.1)

安全问题定义评估是确定 ST 中 TOE 安全问题的陈述是否为有关 TOE 及其预期应用环境的安全问题提供了一个清晰、一致的定义。该组件安全评估内容如下：

a) 评估者应核查安全问题定义描述了威胁；
b) 评估者应核查安全问题定义，确认对所有的威胁都根据威胁主体、资产和敌对行为进行了描述；
c) 评估者应核查安全问题定义描述了组织安全策略；
d) 评估者应核查安全问题定义描述了 TOE 运行环境的相关假设。

5.2.4.7 TOE 概要规范(ASE_TSS.1)

TOE 概要规范评估是确定 TOE 概要规范是否为安全功能和安全保障措施提供了清晰的、一致的高层定义，且满足指定的 TOE 安全要求。该组件安全评估内容如下：

a) 评估者应核查 TOE 概要规范，是否描述了 TOE 是如何满足每一项安全功能要求的；
b) 评估者应核查 TOE 概要规范，确认 TOE 概要规范与 TOE 概述、TOE 描述是一致的。

5.2.5 测试(ATE 类)

5.2.5.1 覆盖证据(ATE_COV.1)

覆盖证据组件评估目的是确定开发人员是否已经测试了所有的 TSFI(评估对象安全功能接口)，并且开发人员的测试覆盖凭证可以证明测试文档定义的测试与功能规范描述的 TSFI 相对应。覆盖证据组件评估目的依据是开发者提供的测试覆盖的分析。覆盖证据组件评估内容包括：评估者应检查测试覆盖分析，以确定测试文档中的测试项与功能规范中的接口准确对应。

5.2.5.2 覆盖分析(ATE_COV.2)

覆盖分析组件评估目的是确定开发人员是否已经测试了所有的 TSFI(评估对象安全功能接口)，并且开发人员的测试覆盖凭证可以证明测试文档定义的测试与功能规范描述的 TSFI 相对应。覆盖分析组件评估目的依据是开发者提供的测试覆盖的分析。该组件安全评估内容如下：

a) 评估者应检查测试覆盖分析，以确定测试文档中的测试项与功能规范中的接口准确对应；
b) 评估者应检查测试计划，以确定对于每一个接口的测试方法与该接口期望的行为相对应；
c) 评估者应检查测试程序，以确定测试条件、测试步骤和与其测试结果可以充分测试每一个接口；
d) 评估者应检查测试覆盖分析，以确定功能规范中的接口与测试文档中的测试项的对应性是完备的。

5.2.5.3 测试：基本设计（ATE_DPT.1）

测试：基本设计安全评估目的是确定开发人员是否已经对照 TOE 设计和安全结构描述，测试了所有的 TSF 子系统和模块。安全评估活动的证据包括：安全目标、功能规范、TOE 设计、安全架构描述、测试文档和测试深度分析。该组件安全评估内容如下：

a） 评估者应检查测试深度分析，以确定测试文档中包括 TSF 子系统行为及其交互行为的描述；
b） 评估者应检查测试计划、测试条件、测试步骤和期望结果以确定对于行为描述的测试方法与 TOE 设计中描述的子系统行为相对应；
c） 评估者应检查测试计划、测试条件、测试步骤和期望结果以确定对于行为描述的测试方法与 TOE 设计中描述的子系统交互行为相对应；
d） 评估者应检查测试程序，证实 TOE 设计中的所有 TSF 子系统都已经进行过测试。

5.2.5.4 测试：安全执行模块（ATE_DPT.2）

测试：安全执行模块组件确定开发人员是否已经对照 TOE 设计和安全结构描述，测试了所有的 TSF 子系统和模块。安全评估活动的证据包括：安全目标、功能规范、TOE 设计、安全架构描述、测试文档和测试深度分析。该组件安全评估内容如下：

a） 评估者应检查测试深度分析，以确定测试文档中包括 TSF 子系统行为及其交互行为的描述；
b） 评估者应检查测试计划、测试条件、测试步骤和期望结果以确定对于行为描述的测试方法与 TOE 设计中描述的子系统行为相对应；
c） 评估者应检查测试计划、测试条件、测试步骤和期望结果以确定对于行为描述的测试方法与 TOE 设计中描述的子系统交互行为相对应；
d） 评估者应检查测试深度分析以确定测试文档中包括 TSF 模块接口；
e） 评估者应检查测试计划、测试条件、测试步骤和期望结果以确定对于每一个 TSF 模块接口的测试方法与该接口期望的行为相对应；
f） 评估者应检查测试程序以确定 TSF 子系统行为及交互行为的所有描述都被测试；
g） 评估者应检查测试程序以确定所有 TSF 模块的所有安全功能都被测试。

5.2.5.5 功能测试（ATE_FUN.1）

功能测试是确定开发人员是否在测试文档中正确描述了测试项。安全评估活动的证据包括：安全目标、功能规范和测试文档。该组件安全评估内容如下：

a） 评估者应检查测试文档是否包括测试计划、预期测试结果和实际测试结果；
b） 评估者应检查测试计划以确定它描述了每个测试执行的场景；
c） 评估者应检查测试计划，以确定 TOE 测试配置是否与在 ST 中列出的评估配置一致；
d） 评估者应检查测试计划以确定对于任何顺序的依赖性测试计划提供足够的规程；
e） 评估者应检查测试文档以确定其包括所有期望的测试结果；
f） 评估者应检查测试文档中的实际测试结果与预期测试结果相一致；
g） 评估者应报告评估者的测试工作，概要性的阐述测试方法、配置、深度和结果。

5.2.5.6 独立测试—抽样（ATE_IND.2）

独立测试—抽样组件通过对 TSF 的一个子集进行独立测试，确定 TOE 是否按规定运转，并通过执行开发者测试的一个例子，以获得对开发者测试结果的信任。安全评估活动的证据包括：安全目标、功能说明书、TOE 设计、用户指南、管理员指南、配置管理文档、测试文档和适合测试的 TOE。该组件安全评估内容如下：

a) 评估者应检查 TOE,以确定测试配置与 ST 规定的评估配置是一致的。
b) 评估者应检查 TOE,以确定它已被正确安装并处于某个已知状态。
c) 评估者应检查开发者提供的资源集,以确认它们与开发者做 TSF 功能测试时使用的资源集等同。
d) 评估者应根据开发者测试计划和程序设计一个测试子集。
e) 评估者应核查所有的实际测试结果,是否与预期测试结果一致。
f) 评估者选择一个适合于 TOE 的测试子集和测试策略。
g) 评估者应为测试子集编制测试文档,以便有足够的细节使得测试是可再现的。
h) 评估者使用所开发的测试文档作为对 TOE 进行测试的基础,对 TOE 实施测试。
i) 评估者应记录包含在测试子集中的如下测试信息:
   1) 待测试的安全功能行为的标识;
   2) 连接和设置执行测试所需要的所有测试设备的规程;
   3) 建立测试所需的先决条件的规程;
   4) 激发安全功能的规程;
   5) 观察安全功能行为的规程;
   6) 所有预期结果的描述,以及对观察到的行为进行的必要分析,该分析是为了与预期结果进行比较;
   7) 结束测试和为 TOE 建立必要的测试后状态的规程;
   8) 实际测试结果。
j) 评估者应核查所有的实际测试结果,是否与预期测试结果一致。
k) 评估者应在 ETR 中报告评估者的测试工作,概要性的阐述测试方法、配置、深度和结果。

5.2.6 脆弱性评定(AVA 类)

5.2.6.1 脆弱性分析(AVA_VAN.2)

脆弱性分析组件确保数据库管理系统在其运行环境下是否存在会被具有中等攻击潜力的攻击者利用的脆弱性。安全评估活动的证据包括:安全目标、功能说明书、TOE 设计、安全架构描述、TOE 实现表示、指导文档、适合测试的 TOE、支持潜在脆弱性识别的公开信息、基本设计测试的结果和当前关于公共域潜在脆弱性和攻击的信息。该组件安全评估内容如下:

a) 评估者应检查 TOE 以确定测试配置和 ST 所说明的测试配置一致。
b) 评估者应检查 TOE 以确定它被正确安装并且处于一个已知状态。
c) 评估者应检查公共可资源,以识别 TOE 中可能的潜在漏洞。
d) 评估者应对 ST、指导文档、功能说明、TOE 设计、安全结构描述和实现表示进行系统的分析以识别 TOE 中可能的潜在漏洞。
e) 评估者应在 ETR 中记录待测试的并且可应用于 TOE 运行环境的识别出的潜在漏洞。
f) 评估者应在独立搜索潜在脆弱性的基础上,进行穿透性测试。
g) 评估者应为基于潜在脆弱性列表的穿透性测试撰写足够详细的穿透性测试文档,以提供测试的可重复性;测试文档包括:
   1) 用于测试的 TOE 安全漏洞标识;
   2) 驱动穿透性测试需要的所有测试装置的连接和设置指令;
   3) 建立所有穿透性测试准备条件的指令;
   4) 仿真 TSF 的指令;
   5) 观察 TSF 行为的指令;

6） 所有预期结果的描述和针对期望结果对观察行为进行比较分析指令；
7） 总结 TOE 测试和测试后对 TOE 后期状态维护指令。

h） 评估者应对 TOE 进行穿透性测试。
i） 评估者应记录穿透性测试的真实结果。
j） 评估者应在 ETR 中报告评估者对穿透性测试的努力，主要包括测试方法、测试配置、测试深度和测试结果。
k） 评估者应检查所有穿透性测试的结果以确定 TOE 在它的运行环境下能抵御具有基本攻击潜力的攻击者的攻击。
l） 评估者应在 ETR 中报告所有可利用的脆弱性和剩余脆弱性，详细包括：
1） 它的来源（例如，在 CEM 评估活动中发现的、评估人员知道的或在公共资源中阅读到的）；
2） 安全功能要求没有满足；
3） 具体描述；
4） 在运行环境中是否可以利用（即可利用还是残留）；
5） 时间长短、专业化水平和 TOE 知识水平，以及对标识漏洞进行攻击需要的攻击及可能性等，包括相应的利用价值。

5.2.6.2 关注点脆弱性分析（AVA_VAN.3）

关注点脆弱性分析组件确保数据库管理系统在其运行环境下是否存在会被具有中等攻击潜力的攻击者利用的脆弱性。安全评估活动的证据包括：安全目标、功能说明书、TOE 设计、安全架构描述、TOE 实现表示、指导文档、适合测试的 TOE、支持潜在脆弱性识别的公开信息、基本设计测试的结果和当前关于公共域潜在脆弱性和攻击的信息。该组件安全评估内容如下：

a） 评估者应检查 TOE 以确定测试配置和 ST 所说明的测试配置一致。
b） 评估者应检查 TOE 以确定它被正确安装并且处于一个已知状态。
c） 评估者应检查公共可资源，以识别 TOE 中可能的潜在漏洞。
d） 评估者应对 ST、指导文档、功能说明、TOE 设计、安全结构描述和实现表示进行系统的分析以识别 TOE 中可能的潜在漏洞。
e） 评估者应在 ETR 中记录待测试的并且可应用于 TOE 运行环境的识别出的潜在漏洞。
f） 评估者应在独立搜索潜在脆弱性的基础上，进行穿透性测试。
g） 评估者应为基于潜在脆弱性列表的穿透性测试撰写足够详细的穿透性测试文档，以提供测试的可重复性；测试文档包括：
1） 用于测试的 TOE 安全漏洞标识；
2） 驱动穿透性测试需要的所有测试装置的连接和设置指令；
3） 建立所有穿透性测试准备条件的指令；
4） 仿真 TSF 的指令；
5） 观察 TSF 行为的指令；
6） 所有预期结果的描述和针对期望结果对观察行为进行比较分析指令；
7） 总结 TOE 测试和测试后对 TOE 后期状态维护指令。

h） 评估者应对 TOE 进行穿透性测试。
i） 评估者应记录穿透性测试的真实结果。
j） 评估者应在 ETR 中报告评估者对穿透性测试的努力，主要包括测试方法、测试配置、测试深度和测试结果。
k） 评估者应检查所有穿透性测试的结果以确定 TOE 在它的运行环境下能抵御抵抗具有增强型

基本攻击潜力的攻击者的攻击。

l) 评估者应在 ETR 中报告所有可利用的脆弱性和剩余脆弱性，详细内容包括：
   1) 它的来源（例如，在 CEM 评估活动中发现的、评估人员知道的或在公共资源中阅读到的）；
   2) 安全功能要求没有满足；
   3) 具体描述；
   4) 在运行环境中是否可以利用（即可利用还是残留）；
   5) 时间长短、专业化水平和 TOE 知识水平，以及对标识漏洞进行攻击需要的攻击及可能性等，包括相应的利用价值。

5.3 评估方法

5.3.1 评估原则

依照 GB/T 30270—2013，评估者对安全目标进行评估后，对 GB/T 20273—2019 规定的安全要求给予裁决。依据 GB/T 30270—2013，给予裁决的最小结构是 GB/T 20273—2019 规定的安全功能组件和安全保障组件的评估者行为元素。作为执行相应评估方法行为及其组成工作单元的结果，GB/T 20273—2019的每一个要求均被赋予一个裁决。如安全目标未声明 GB/T 20273—2019 符合性要求，则安全评估人员对未包含在本标准中的安全组件，按照 GB/T 30270—2013 独立选择相应的组件进行评估。

5.3.2 评估方法

安全功能组件和安全保障组件采用的评估方法包括但不限于：

a) 检查（examine）：评估者通过采用专业技能分析形成一个裁决。使用此动词的语句表明哪些是需要分析的以及什么样的属性需要分析。
b) 核查（check）：评估者不必采用专门技能仅通过简单比较形成一个裁决。评估者作出一个快速决定，但可能只需要一个快速分析或完全不用分析。
c) 独立测试（independent testing）：评估者依据评估对象的功能组件，采用抽样测试，或评估者自己设计测试用例的测试，完成数据库安全功能组件的功能测试。
d) 穿透性测试（penetration testing）：评估者采用专门技能，以未经授权的动作绕过某一系统的安全机制的方式，检查数据库管理系统的安全功能，以发现安全问题的手段，也称渗透性测试或逆向测试。
e) 确认（confirm）：已对某事项进行了详细的审核以作出独立的决定；所需要的严格程度依赖于事项的本质特征。这个术语仅用于评估者行为。
f) 确定（determine）：通过独立分析来肯定一个特定的结论，该分析以达成一个特定的结论为目的。
g) 确保（ensure）：保证在行为及其结果之间存在牢固的因果关系。
h) 证实（demonstrate）：得出一个由分析获得的结论，它不如“证明”那样严格。
i) 论证（justification）：分析以得出一个结论。“论证”比“证实”更严格。从需要非常仔细、全面地解释逻辑论证的每一步来说，这个术语要求十分严格。
j) 证明（prove）：通过数学意义上的形式化分析来说明对应关系。
k) 验证（verity）：通过严格细致地审查，独立地确定充分性。

5.3.3 评估内容

依照 GB/T 30270—2013，评估者对 GB/T 20273—2019（表 1 所示）设计相应的功能测试用例的安

全功能要求进行测试评估。

表 1　不同评估保障级安全功能评估内容

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	√	√	√
	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		√	√
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	√	√	√

表 1（续）

功能类	功能组件	评估保障级		
		EAL2	EAL3	EAL4
安全管理	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_MTD.1 TSF 数据的管理	√	√	√
	FMT_REV.1 撤销	√	√	√
	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 最低和最高配额	√	√	√
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选择的安全功能组件				

依照 GB/T 20273—2019，评估人员依据 GB/T 30270—2013 对表 2 所示的各级别保障要求进行评估。

表 2　不同评估保障级安全保障评估内容

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			√
安全目标评估	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 2（续）

保障类	保障组件	评估保障级		
		EAL2	EAL3	EAL4
脆弱性评定	AVA_VAN.2 脆弱性分析	√	√	
	AVA_VAN.3 关注点脆弱性分析			√
注：√代表在该保障级别下选择的安全保障组件。				

5.3.4 评估结果

本标准认可 3 种互相排斥的裁决情形：

a） 通过：评估者完成了 GB/T 30270—2013 “评估者行为元素”，并确定接受评估的 PP、ST 或 TOE 的要求得到满足。通过评估的条件在相关行为的组成工作单元中给定。

b） 待定：评估者未完成与 GB/T 30270—2013“评估者行为元素”相关的一个或多个评估方法行为工作单元。

c） 不通过：评估者完成了 GB/T 30270—2013“评估者行为元素”，并确定接受评估的 PP、ST 或 TOE 未满足要求。

所有的裁决最初都是“待定”，直到被赋予“通过”或“不通过”裁决为止。

当且仅当所有组成部分的裁决都为“通过”，总体裁决才为“通过”。如果某个评估者行为元素的裁决为“不通过”，则相应保证组件、保证类的裁决和总体裁决都为“不通过”。

附 录 A
（资料性附录）
标准修订说明

A.1 GB/T 20009—2005 评估内容与本标准安全功能要求映射表

表 A.1 为 GB/T 20009—2005 评估内容与本标准安全功能要求映射表。修订后标准中 EAL2 级、EAL3 级、EAL4 级的安全要求既适用于基于 GB/T 18336—2015 下的数据库安全性测评，也同样适用于基于 GB 17859—1999 下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 20009—2005 评估内容与本标准安全功能要求映射表

GB/T 20009—2005 评估内容							功能类	GB/T 20009—2019 评估内容	备注
评估内容		用户自主保护级	系统审计保护级	安全标记保护级	结构化保护级	访问验证保护级		安全功能要求	
审计	内容		√	√	√	√	FAU 类：安全审计	FAU_GEN.1	覆盖
			√	√	√	√		FAU_GEN.2	新增
	查阅		√	√	√	√		FAU_SAR.1	覆盖
			√	√	√	√		FAU_SAR.2	新增
				√	√	√		FAU_SAR.3	覆盖
			√	√	√	√		FAU_SEL.1	新增
	存储保护		√	√	√	√		FAU_STG.2	覆盖
			√	√	√			FAU_STG.4	覆盖
	分析								删除
	自动响应								删除
数据传输	原发证明						FCO 类：通信		删除
	接收证明								删除
密码支持	密钥管理			√	√	√	FCS 类：密码支持	FCS_CKM.1	覆盖
				√	√	√		FCS_CKM.4	覆盖
	密码运算			√	√	√		FCS_COP.1	覆盖
自主访问控制		√	√	√	√	√	FDP 类：用户数据保护	FDP_ACC.1	覆盖
		√	√	√	√	√		FDP_ACF.1	覆盖
强制访问控制				√	√	√		FDP_ACC.1	覆盖
				√	√	√		FDP_ACF.1	覆盖
客体重用			√	√	√	√		FDP_RIP.1	覆盖

表 A.1（续）

GB/T 20009—2005 评估内容							功能类	GB/T 20009—2019 评估内容	备注
评估内容		用户自主保护级	系统审计保护级	安全标记保护级	结构化保护级	访问验证保护级		安全功能要求	
数据完整性	回退	√	√	√	√	√	FDP 类：用户数据保护	FDP_ROL.1	覆盖
	完整性监视		√	√	√	√		FDP_SDI.2	覆盖
	数据鉴别								删除
数据传输	内部传输	√	√	√	√	√		FDP_ITT.1	覆盖
	数据外部输出	√	√	√	√	√		FDP_ETC.1	覆盖
	数据外部输入	√	√	√	√	√		FDP_ITC.1	覆盖
				√	√	√		FDP_IFC.1	新增
				√	√	√		FDP_IFF.2	新增
身份鉴别	用户属性定义	√	√	√	√	√	FIA 类：标识和鉴别	FIA_ATD.1	覆盖
	用户标识	√	√	√	√	√		FIA_UID.1	覆盖
	用户鉴别	√	√	√	√	√		FIA_UAU.1	覆盖
				√	√	√		FIA_UAU.5	覆盖
			√	√	√	√		FIA_UAU.7	覆盖
	鉴别失败处理	√	√	√	√	√		FIA_AFL.1	覆盖
				√	√	√		FIA_SOS.1	新增
		√	√	√	√	√		FIA_USB.1	新增
安全管理	功能管理	√	√	√	√	√	FMT 类：安全管理	FMT_MOF.1	覆盖
	属性管理	√	√	√	√	√		FMT_MSA.1	覆盖
			√	√	√	√		FMT_MSA_EXT.3	覆盖
	安全功能数据管理	√	√	√	√	√		FMT_MTD.1	覆盖
	安全管理角色			√	√	√		FMT_SMR.1	覆盖
					√	√		FMT_SMR.2	覆盖
	标记			√	√	√		FMT_MSA_EXT.1(1)/(2)	覆盖
		√	√	√	√	√		FMT_REV.1	新增
		√	√	√	√	√		FMT_SMF.1	新增

表 A.1（续）

GB/T 20009—2005 评估内容							功能类	GB/T 20009—2019 评估内容	备注
评估内容		用户自主保护级	系统审计保护级	安全标记保护级	结构化保护级	访问验证保护级		安全功能要求	
安全功能保护	安全功能自检						FPT 类：TSF 保护		删除
	时间戳								删除
	域分离								删除
	数据一致性		√	√	√	√		FPT_TRC.1	覆盖
	安全功能数据传输	√	√	√	√	√		FPT_ITT.2	覆盖
	系统恢复					√		FPT_FLS.1	覆盖
	可信恢复		√	√	√	√		FPT_RCV.3	覆盖
	不可旁路								删除
	物理保护								删除
				√	√	√		FPT_OVR_EXT.1	新增
资源利用	容错		√	√	√	√	FRU 类：资源利用	FRU_FLT.1	覆盖
		√	√	√	√	√		FRU_PRS.1	新增
			√	√	√	√		FRU_RSA.2	新增
	访问历史	√	√	√	√	√	FTA 类：TOE 访问	FTA_TAH.1	覆盖
	并发会话	√	√	√	√	√		FTA_MCS.1	覆盖
	时限授权				√	√		FTA_LSA.1	覆盖
				√	√	√		FTA_SSL.3	新增
	不可观察性							FTA_TSE.1	覆盖
数据传输	可信路径				√	√	FTP 类：可信路径/信道	FTP_ITC.1	覆盖

注：覆盖：代表 GB/T 20009—2005 安全功能项对应到本标准中的安全功能要求。
新增：代表本标准中新增的安全功能要求。
删除：代表本标准中删除的 GB/T 20009—2005 内容。

A.2 基于 GB/T 20009—2005 的各级别所对应的安全要求

表 A.2 用于参考 GB/T 20009—2005 中各个级别的功能项映射到本标准中的安全功能组件。

表 A.2　GB/T 20009—2005 评估内容与本标准安全功能要求映射表

基于 GB/T 20009—2005 的各级别所对应的安全要求					
安全要求类	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
FAU 类：安全审计		FAU_GEN.1	FAU_GEN.1	FAU_GEN.1	FAU_GEN.1
		FAU_GEN.2	FAU_GEN.2	FAU_GEN.2	FAU_GEN.2
		FAU_SAA..1	***FAU_SAA.1***	***FAU_SAA.1***	***FAU_SAA.1***
		FAU_SAR.1	***FAU_SAA.2***	***FAU_SAA.2***	***FAU_SAA.2***
		FAU_SAR.2	FAU_SAR.1	***FAU_SAA.3***	***FAU_SAA.4***
		FAU_SEL.1	FAU_SAR.2	FAU_SAR.1	FAU_SAR.1
		FAU_STG.1	FAU_SAR.3	FAU_SAR.2	FAU_SAR.2
			FAU_SEL.1	FAU_SAR.3	FAU_SAR.3
			FAU_ARP.1	FAU_SEL.1	FAU_SEL.1
			FAU_STG.2	***FAU_ARP.1***	***FAU_ARP.1***
				FAU_STG.2	FAU_STG.2
				FAU_STG.4	FAU_STG.4
FDP 类：用户数据保护	FDP_ACC.1	FDP_ACC.1	FDP_ACC.1	FDP_ACC.1	FDP_ACC.1
	FDP_ACF.1	FDP_ACF.1	FDP_ACF.1	FDP_ACF.1	FDP_ACF.1
	FDP_ROL.1	FDP_ROL.1	FDP_IFC.1	FDP_ITC.1	FDP_ITC.1
	FDP_SDI.2	FDP_SDI.2	FDP_IFF.2	FDP_ETC.2	FDP_ETC.2
	FDP_UIT.1	***FDP_UIT.1***	FDP_ROL.1	FDP_IFC.1	FDP_IFC.1
		FDP_UCT.1	FDP_SDI.2	FDP_IFF.2	FDP_IFF.2
			FDP_UIT.1	FDP_ROL.1	FDP_ROL.1
			FDP_UCT.1	FDP_SDI.2	FDP_SDI.2
			FDP_ITC.1	***FDP_UIT.1***	***FDP_UIT.1***
				FDP_UCT.1	***FDP_UCT.1***
FMT 类：安全管理	FMT_MSA_EXT.3	FMT_MSA_EXT.3	FMT_MSA_EXT.1(1)	FMT_MSA_EXT.1(2)	FMT_MSA_EXT.1(2)
	FMT_MOF.1	FMT_SMF.1	FMT_MSA_EXT.3	FMT_MSA_EXT.3	FMT_MSA_EXT.3
	FMT_SMF.1	FMT_MOF.1	FMT_MOF.1	FMT_MOF.1	FMT_MOF.1
		FMT_MTD.1	FMT_SMF.1	FMT_SMF.1	FMT_SMF.1
		FMT_MSA.1	FMT_MTD.1	FMT_MTD.1	FMT_MTD.1
			FMT_SMR.1	FMT_SMR.1	FMT_SMR.1
			FMT_MSA.1	FMT_MSA.1	FMT_MSA.1

表 A.2（续）

基于 GB/T 20009—2005 的各级别所对应的安全要求					
安全要求类	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
FIA 类：标识和鉴别	FIA_UID.1	FIA_UID.1	FIA_UID.1	FIA_UID.1	FIA_UID.1
	FIA_UAU.1	FIA_UAU.1	FIA_UAU.1	FIA_UAU.1	FIA_UAU.1
	FIA_UAU.7	FIA_UAU.7	FIA_UAU.7	FIA_UAU.7	FIA_UAU.7
	FIA_AFL.1	FIA_AFL.1	FIA_AFL.1	FIA_AFL.1	FIA_AFL.1
	FIA_USB.1	FIA_USB.1	FIA_USB.1	FIA_USB.1	FIA_USB.1
		FIA_UAU.5	FIA_UAU.5	FIA_UAU.5	FIA_UAU.5
FPT 类：TSF 保护	***FPT_PHP.1***	***FPT_PHP.1***	***FPT_PHP.2***	***FPT_PHP.2***	***FPT_PHP.2***
	FPT_RVM.1	***FPT_RVM.1***	***FPT_RVM.1***	***FPT_PHP.3***	***FPT_PHP.3***
	FPT_SEP.1	***FPT_SEP.1***	***FPT_SEP.1***	***FPT_RVM.1***	***FPT_RVM.1***
	FPT_RCV.1	***FPT_RCV.1***	***FPT_RCV.1***	***FPT_SEP.1***	***FPT_SEP.1***
	FPT_ITT.2	FPT_ITT.2	FPT_ITT.2	FPT_RCV.1	FPT_RCV.2
		FPT_TRC.1	FPT_TRC.1	FPT_ITT.2	FPT_ITT.2
			FPT_ITA.1	FPT_TRC.1	FPT_TRC.1
				FPT_ITA.1	***FPT_ITA.1***
FRU 类：资源利用	FRU_FLT.1	FRU_FLT.1	FRU_FLT.1	FRU_FLT.1	FRU_FLT.1
	FRU_PRS.1	FRU_PRS.1	FRU_PRS.1	FRU_PRS.1	FRU_PRS.1
	FRU_RSA.1	FRU_RSA.2	FRU_RSA.2	FRU_RSA.2	FRU_RSA.2
FTA 类：TOE 访问	FTA_LSA.1	FTA_LSA.1	FTA_LSA.1	FTA_LSA.1	FTA_LSA.1
	FTA_MCS.1	FTA_MCS.1	FTA_MCS.1	FTA_MCS.1	FTA_MCS.1
	FTA_TSE.1	FTA_TAH.1	FTA_TAH.1	FTA_TAH.1	FTA_TAH.1
		FTA_TSE.1	FTA_SSL.3	FTA_SSL.3	FTA_SSL.3
			FTA_TSE.1	FTA_TSE.1	FTA_TSE.1
FTP 类：可信路径/信道				FTP_TRP.1	FTP_TRP.1
ADV 类：开发	ADV_FSP.1	ADV_ARC.1	ADV_ARC.1	ADV_ARC.1	ADV_ARC.1
		ADV_FSP.2	ADV_FSP.3	ADV_FSP.4	ADV_FSP.5
		ADV_TDS.1	ADV_TDS.2	ADV_IMP.1	ADV_IMP.1
				ADV_TDS.3	ADV_INT.2
					ADV_TDS.4
AGD 类：指导性文档	AGD_OPE.1	AGD_OPE.1	AGD_OPE.1	AGD_OPE.1	AGD_OPE.1
	ADV_PRE.1	ADV_PRE.1	ADV_PRE.1	ADV_PRE.1	ADV_PRE.1

表 A.2（续）

基于 GB/T 20009—2005 的各级别所对应的安全要求					
安全要求类	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
ALC 类：生命周期支持	ALC_CMC.1	ALC_CMC.2	ALC_CMC.3	ALC_CMC.4	ALC_CMC.4
	ALC_CMS.1	ALC_CMS.2	ALC_CMS.3	ALC_CMS.4	ALC_CMS.5
		ALC_DEL.1	ALC_DEL.1	ALC_DEL.1	ALC_DEL.1
			ALC_LCD.1	ALC_DVS.1	ALC_DVS.1
				ALC_LCD.1	ALC_LCD.1
				ALC_TAT.1	ALC_TAT.2
ASE 类：安全目标评估	ASE_CCL.1	ASE_CCL.1	ASE_CCL.1	ASE_CCL.1	ASE_CCL.1
	ASE_ECD.1	ASE_ECD.1	ASE_ECD.1	ASE_ECD.1	ASE_ECD.1
	ASE_INT.1	ASE_INT.1	ASE_INT.1	ASE_INT.1	ASE_INT.1
	ASE_OBJ.1	ASE_OBJ.2	ASE_OBJ.2	ASE_OBJ.2	ASE_OBJ.2
	ASE_REQ.1	ASE_REQ.2	ASE_REQ.2	ASE_REQ.2	ASE_REQ.2
	ASE_TSS.1	ASE_SPD.1	ASE_SPD.1	ASE_SPD.1	ASE_SPD.1
		ASE_TSS.1	ASE_TSS.1	ASE_TSS.1	ASE_TSS.1
ATE 类：测试	ATE_IND.1	ATE_COV.1	ATE_COV.2	ATE_COV.2	ATE_COV.2
		ATE_FUN.1	ATE_DPT.1	ATE_DPT.2	ATE_DPT.3
		ATE_IND.2	ATE_FUN.1	ATE_FUN.1	ATE_FUN.1
			ATE_IND.2	ATE_IND.2	ATE_IND.2
AVA 类：脆弱性评定	AVA_VAN.1	AVA_VAN.2	AVA_VAN.2	AVA_VAN.3	AVA_VAN.4
注：表中“***斜体加粗***”代表本标准中已经删除的安全要求。					

中 华 人 民 共 和 国
国 家 标 准
信息安全技术
数据库管理系统安全评估准则
GB/T 20009—2019
*
中 国 标 准 出 版 社 出 版 发 行
北京市朝阳区和平里西街甲 2 号(100029)
北京市西城区三里河北街 16 号(100045)
网址:www.spc.org.cn
服务热线:400-168-0010
2019 年 7 月第一版
*
书号:155066·1-63320

GB/T 20009-2019