GA

# 中华人民共和国公共安全行业标准

GA/T 389 — 2002

# 计算机信息系统安全等级保护 数据库管理系统技术要求

Database management system technology requirement in computer information system security protection

2002-07-18 发布　　2002-07-18 实施

中华人民共和国公安部　发布

# 目　　次

# 前　　言

GB17859-1999《计算机信息系统安全保护等级划分准则》作为我国计算机信息系统安全等级管理的重要标准，已于1999年9月13日发布。为促进安全等级管理的工作的正常有序开展，特制定一系列相关的标准，包括：

——计算机信息系统安全等级保护技术要求系列标准；

——计算机信息系统安全等级保护管理要求；

——计算机信息系统安全等级保护工程实施要求；

——计算机信息系统安全等级保护实施管理办法；

——计算机信息系统安全保护等级评测系列标准。

其中，计算机信息系统安全等级保护技术要求系列标准主要包括以下五个标准：

——GA ××1 — ×××× 计算机信息系统安全等级保护通用技术要求；

——GA ××2 — ×××× 计算机信息系统安全等级保护网络系统技术要求；

——GA ××3 — ×××× 计算机信息系统安全等级保护操作系统技术要求；

——GA ××4 — ×××× 计算机信息系统安全等级保护数据库管理系统技术要求；

——GA ××5 — ×××× 计算机信息系统安全等级保护应用系统技术要求。

《计算机信息系统安全等级保护数据库管理技术要求》作为计算机信息系统安全等级保护技术要求系列标准之一，详细说明了计算机信息系统为实现GB17859所提出的安全等级保护要求对数据库管理系统的安全技术要求，以及为确保这些安全技术所实现的安全功能达到其应具有的安全性而采取的保证措施，并将GB17859对计算机信息系统五个安全保护等级每一级的要求，从技术要求方面进行详细描述。

本标准分由公安部公共信息网络安全监察局提出。

本标准起草单位：江南计算技术研究所。

本标准主要起草人：吉增瑞、陆　晔、孙　炜、徐良华、袁志平

# 引　　言

《计算机信息系统安全等级保护数据库管理系统技术要求》是计算机信息系统安全等级保护技术要求系列标准的重要组成部分，用以指导设计者如何设计和实现具有所需要的安全等级的数据库管理系统，主要从对数据库管理系统的安全保护等级进行划分的角度来说明其技术要求，即主要说明为实现《计算机信息系统安全保护等级划分准则》中每一个保护等级的安全要求对数据库管理系统应采取的安全技术措施，以及各安全技术要求在不同安全级中具体实现上的差异。

本标准按照GB17859五个安全等级的划分，对每一个安全等级的安全功能技术要求和安全保证技术要求做了详细描述。本标准参考的主要文件是：

——GB17859-1999 计算机信息系统安全保护等级划分准则；

——ISO/IEC 15408：1999 Information technology—Security techniques— Evaluation Criteria for IT Security ，Version 2.0。

# 计算机信息系统安全等级保护数据库管理系统技术要求

## 1 范围

本标准规定了按照《计算机信息系统安全等级保护划分准则》（以下简称《准则》）对数据库管理系统进行安全保护等级划分所需要的详细技术要求。

本标准适用于按照《准则》的安全等级保护要求所进行的数据库管理系统的设计和实现，按照《准则》安全等级保护要求对数据库管理系统进行的测试、管理也可参照使用。

## 2 规范性引用文件

下列文件中的有关条款通过在本标准有关部分的引用而成为本部分的条款。凡注日期或版次的引用文件，其后的任何修改单（不包括勘误的内容）或修订版本都不适用于本标准，但提倡使用本标准的各方探讨使用其最新版本的可能性。凡不注日期或版次的引用文件，其最新版本适用于本标准。

GB17859-1999 计算机信息系统安全等级划分准则

GA ××1 — ×××× 计算机信息系统安全等级保护通用技术要求

ISO/IEC 9075：1999《数据库语言 SQL》

## 3 定义

GB17859—1999 和 GA ××1 — ××××确立的以及下列术语和定义适用于本标准。

3．1

**实体完整性（body integrity）**

实体完整性规则要求数据库中表示的任一实体是可区分的。对于关系模型，实体完整性表现为关系的主属性（主键、主码）不能是空值（NULL），也不能是重复值，即指基本键的各个分量都不能为空。因为在关系数据库中，基本键唯一地标识各个实体。基本键为空，意味着该实体没有确定的标志，也就不能与其它实体相区别。在基本键为联合键的情况下，如果其值的某个分量为空，就意味着实体的某个属性值未知，也不能与其它实体相区别。

3．2

**参照完整性（reference integrity）**

关系模型中的参照完整性是指，在任一时刻，关系 R1 的某些属性是关于关系 R2 的外键，则该外键的值必须是 R2 中某元组的主键值或为“空值”。空值意味着“不知道”的信息和“无意义”的信息（它不是空字符串或空格字符串，也不是零值或任何其它数值）。关系之间的参照完整性规则是“连接”关系运算正确执行的前提。

3．3

**用户定义完整性（user defined integrity）**

是指根据应用（比如价格的有效范围等）所确定的完整性约束。系统提供定义和检查用户定义完整性规则的机制，其目的是用统一的方式由系统处理，而不是由应用程序完成，这样不仅可以简化应用程序，还提高了完整性保证的可靠性。

## 4 数据库管理系统安全技术要求

### 4.1 身份鉴别

#### 4.1.1 用户标识

应对注册到数据库管理系统中的用户进行唯一性标识。用户标识信息是公开信息，一般以用户名和/或用户 ID 实现。为了管理方便，可将用户分组，也可使用别名。无论用户名、用户 ID、用户组还

是用户别名，都要遵守标识的唯一性原则。

#### 4.1.2 用户鉴别

应对登录到数据库管理系统的用户进行身份真实性鉴别。通过对用户所提供的“鉴别信息”的验证，证明该用户确有所声称的某种身份，这些“鉴别信息”必须是保密的，不易伪造的。

### 4.2 标记与访问控制

#### 4.2.1 标记与安全属性管理

应通过标记为 TCB 安全功能控制范围内的主体与客体设置安全属性。具体要求为：

a) 对于自主访问控制，标记以某种方式表明主体与客体的访问关系；

b) 对于强制访问控制，不同的访问控制模型有不同的标记方法。基于多级安全模型的强制访问控制，标记过程授予主体与客体一定的安全属性，这些安全属性构成采用多级安全模型的强制访问控制机制的属性库——强制访问控制的基础数据。数据库管理系统需要对主、客体独立进行标记。

c) 用户安全属性应在用户建立注册帐户后由系统安全员通过 TCB 所提供的安全员界面进行标记并维护；

d) 客体安全属性应在数据输入到由 TCB 安全功能所控制的范围内时以缺省方式生成或由安全员进行标记并维护；

e) 系统管理员、系统安全员和审计员的安全属性应通过相互标记形成制约关系。

#### 4.2.2 访问控制

应根据数据库特点和要求，实现不同粒度的访问控制。这些特点主要是：

a) 数据以特定结构格式存放，客体的粒度可以是：关系数据库的表、视图、元组（记录）、列（字段）、元素（每个元组的字段）、日志、片段、分区、快照、约束和规则、DBMS 核心代码、用户应用程序、存储过程、触发器、各种访问接口等；

b) 数据库系统有完整定义的访问操作，如表 1 所示；

c) 数据库是数据与逻辑的统一，数据库中不仅存放了数据，还存放了大量的用于管理和使用这些数据的程序，这些程序和数据同样需要进行保护，以防止未授权的使用、篡改、增加或破坏；

d) 数据量大、客体丰富是数据库的又一特点，考虑到性能和代价，应对于不同客体给予不同程度的保护，如对敏感字段加密，对敏感表建立视图等。

e) 数据库系统具有数据生命周期长、用户分散、组成复杂等特点，要求长期的安全保护；

f) 数据库中的三级结构（物理结构、逻辑结构、概念模型结构）和两种数据独立性（物理独立性、逻辑独立性）大大减轻数据库应用程序的维护工作量，但是由于不同的逻辑结构可能对应于相同的物理结构，给访问控制带来新的问题，应对访问规则进行一致性检查；

g) 数据库管理系统的访问控制是在 OS 之上实现的，考虑到效率因素，数据库管理系统的访问控制应在外层实现；

h) 数据库系统中客体具有相互联系的特点，这些“联系”本身也是一种非常有效的信息，防止未授权用户获得或利用这些“联系”，需要进行“推理控制”；

i) 分布式数据库管理系统中，全局应用的访问控制应在全局 DBMS 层实现，局部应用的访问控制应在局部 DBMS 层实现，并根据需要各自选择不同的访问控制策略；

#### 4.2.3 自主访问控制

##### 4.2.3.1 访问操作

应由数据库子语言定义，并与数据一起存放在数据字典中。对任何 SQL 对象进行操作应有明确的权限许可，并且权限随着操作和对象的变化而变化，安全系统应有能力判断这种权限许可。操作与对象紧密相联，即把“操作+对象”作为一个授权。表 1 列出了 GRANT（授权）语句对象类型与相关操作。

表 1 GRANT 语句的对象类型与相关操作

| 对象 | 操作 |
|---|---|
| 基本表 | SELECT 、 INSERT 、 UPDATE 、 DELETE 、 TRIGGER 、 REFERENCES |
| 视图 | SELECT、INSERT、UPDATE、DELETE、REFERENCES |
| 列 | SELECT、INSERT、UPDATE、REFERENCES |
| 域 | USAGE |
| 字符集 | USAGE |
| 排序 | USAGE |
| 转换 | USAGE |
| SQL 调用例程 | EXECUTE |
| UDT | UNDER |

表中，除 USAGE 和 UNDER 外，其余操作均符合 SQL 语句中使用的动词

##### 4.2.3.2 访问规则

应以访问控制表或访问矩阵的形式表示，并通过执行相应的访问控制程序实现。每当执行 SQL 语句、有访问要求出现时，通过调用相应的访问控制程序，实现对访问要求的控制。

##### 4.2.3.3 授权传播限制

应限制具有某一权限的用户将该权限传给其他用户。当一个用户被授予某权限，同时拥有将该权限授予其它用户的权力时，该用户才拥有对该授权的传播权。为了增强数据库系统的安全性，需要对授权传播进行某些限制。

#### 4.2.4 强制访问控制

应采用确定的安全策略模型实现强制访问控制。当前常用的安全策略模型是多级安全模型。该模型将 TCB 安全控制范围内的所有主、客体成分通过标记方式设置安全属性（等级和范畴）。该模型并按由简单保密性原则确定的规则——从下读、向上写，根据访问者主体和被访问者客体的安全属性，实现主、客体之间每次访问的强制性控制。根据数据库管理系统的运行环境的不同，强制访问控制分为：

a) 在单一计算机系统上或网络环境的多机系统上运行的单一数据库管理系统，访问控制所需的安全属性存储在统一的数据库字典中，使用单一的访问规则实现；

b) 在网络环境的多机系统上运行的分布式数据库系统，全局应用的强制访问控制应在全局 DBMS 层实现，局域应用的强制访问控制应在局部 DBMS 层实现。其所采用的访问规则应是一致的。

### 4.3 数据完整性

#### 4.3.1 实体完整性和参照完整性

a) 数据库管理系统应确保数据库中的数据具有实体完整性和参照完整性。关系之间的参照完整性规则是“连接”关系运算正确执行的前提。

b) 用户定义基本表时，应说明主键、外键，被引用表、列和引用行为。当数据录入、更新、删除时，由数据库管理系统应根据说明自动维护实体完整性和参照完整性。

#### 4.3.2 用户定义完整性

a) 数据库管理系统应提供支持用户定义完整性的功能。系统应提供定义和检查用户定义完整性规则的机制，其目的是用统一的方式由系统处理，而不是由应用程序完成，从而不仅可以简化应用程序，还提高了完整性保证的可靠性。

b) 数据库管理系统应支持为约束或断言命名（或提供默认名称），定义检查时间、延迟模式或设置默认检查时间和延迟模式，支持约束和断言的撤消。

#### 4.3.3 数据操作的完整性

数据操作的完整性约束为：

a) 用户定义基本表时应定义主键和外键；

b) 对于候选键，应由用户指明其唯一性；

c) 对于外键，用户应指明被引用关系和引用行为；

d) 应由数据库管理系统检查对主键、外键、候选键数据操作是否符合完整性要求，不允许提交任何违反完整性的事务；

e) 删除或更新某元组时，数据库管理系统应检查该元组是否含有外键，若有，应根据用户预定义的引用行为进行删除。

### 4.4 数据库安全审计

数据库管理系统的安全审计应：

a) 建立独立的安全审计系统；

b) 定义与数据库安全相关的审计事件；

c) 设置专门的安全审计员；

d) 设置专门用于存储数据库系统审计数据的安全审计库；

e) 提供适用于数据库系统的安全审计设置、分析和查阅的工具。

### 4.5 客体重用

数据库系统大量使用的动态资源，多由操作系统分配。实现客体安全重用的操作系统和数据库管理系统应满足以下要求：

a) 数据库管理系统提出资源分配要求，如创建新库，数据库设备初始化等，所得到的资源不应包含该客体以前的任何信息内容；

b) 数据库管理系统提出资源索回要求，应确保这些资源中的全部信息被清除；

c) 数据库管理系统要求创建新的数据库用户进程，应确保分配给每个进程的资源不包含残留信息；

d) 数据库管理系统应确保已经被删除或被释放的信息不再是可用的。

### 4.6 数据库可信恢复

数据库系统中的可信恢复具有特定含义，主要应包括：

a) 确保 TSF 能在确定不减弱保护的情况下启动安全数据库系统的 DBMS；

b) 运行中发生故障或异常情况时，能够在尽量短的时间内恢复到正确、一致、有效的状态，这个状态对于系统运行是正常、安全的状态，并且对于应用来说是一个真实、有意义的状态；

c) 数据库系统可信恢复应由操作系统和数据库系统共同支持；

d) 与可信恢复相关的数据库技术有：事务管理，日志，检查点，备份，分布式数据库特殊处理。

### 4.7 隐蔽信道分析

数据库管理系统的隐蔽信道分析与数据库管理系统的设计密切相关，应在系统开发过程中进行。系统开发者应彻底搜索隐蔽存储信道，并根据实际测量或工程估量确定每一个被标识信道的最大带宽。

隐蔽信道分析是建立在 TCB 的实现、管理员指南、用户指南以及完整定义的外部接口等基础上的。

### 4.8 可信路径

在数据库用户进行注册或进行其它安全性操作时，应提供TCB与用户之间的可信通信路径，实现用户与TSF间的安全数据交换。

### 4.9 推理控制

应采用推理控制的方法防止数据库中的数据信息被非授权地获取。运用推理方法获取权限以外的数据库信息，是一种较为隐蔽的信息攻击方法。在具有较高安全级别要求的数据库系统中，应考虑对这种攻击的防御。

## 5 安全等级划分技术要求

按《准则》对各个级别的不同要求，本部分主要从十个安全要素以及与数据库管理系统安全关系较为密切的推理控制，对安全功能的技术要求和安全保证技术要求作详细描述。

表 1 给出了按《准则》所描述的每一个安全级对安全要素的不同要求。

表 1 每个安全级的安全功能要求

| 安全等级 / 安全要素 | 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 |
|---|---|---|---|---|---|
| 自主访问控制 | + | ++ | ++ | +++ | ++++ |
| 强制访问控制 | | | + | ++ | +++ |
| 标　　记 | | | + | ++ | ++ |
| 身 份 鉴 别 | + | ++ | +++ | +++ | ++++ |
| 客 体 重 用 | | + | + | ++ | ++ |
| 审　　计 | | + | ++ | +++ | ++++ |
| 数据完整性 | + | + | ++ | ++ | +++ |
| 可 信 恢 复 | | | | | + |
| 隐蔽信道分析 | | | | + | ++ |
| 可信路径 | | | | + | ++ |
| 推 理 控 制 | | | | + | + |

注： + —— 表示有要求；

++ —— 表示有进一步要求；

+++ —— 表示有更进一步要求；

++++ —— 表示有更高要求。

下面对每一安全级的具体技术要求分别进行描述。其中**“加粗宋体”**表示所描述的内容在该级中第一次出现。

5.1 第一级：用户自主保护级

5.1.1 安全功能

5.1.1.1 自主访问控制

应根据本标准 **4.2.3** 条访问操作、访问规则、和授权传播的描述，按照《通用技术要求》**6.1.3.3** 条自主访问控制所描述的要求设计访问控制功能。本安全级要求：

**a)** 用目录表访问控制、存取控制表访问控制、能力表访问控制等访问控制表访问控制确定主体对客体的访问权限。数据库管理系统中一般不直接采用稀疏的二维存取矩阵，而采用一些比较实用的技术，如：按行存储、按列存储、锁钥法、口令密码法等实现自主访问控制。

**b)** 无论采用何种访问控制策略实现访问控制功能，都应允许命名用户以用户和/或用户组的身份规定并控制对客体的共享，并阻止非授权用户读取信息。

5.1.1.2 身份鉴别

a) 身份鉴别应包括对用户的身份进行标识和鉴别。

b) 用户标识应根据 **4.1.1** 条用户标识的描述，按照《通用技术要求》**6.1.3.1** 条用户标识的要求进行。

c) 用户鉴别应根据 **4.1.2** 条用户鉴别的描述，按照《通用技术要求》**6.1.3.2** 条用户鉴别的要求进行。

d) 进入数据库系统的用户，首先应由支持数据库系统运行的操作系统进行身份鉴别。

e) 应提供用户进入数据库管理系统时的身份鉴别，并按以下要求进行设计：

——凡需进入数据库管理系统的用户，可以选择采用该用户在操作系统中的标识信息，也可以重新进行用户标识。重新进行用户标识应在用户注册（建立账号）时进行。

——当用户登录到数据库管理系统或与数据库服务器进行访问连接时，应进行用户鉴别。

——数据库管理系统用户标识一般使用用户名和用户标识（UID）。为在整个数据库系统范围实现用户的唯一性，应确保数据库管理系统建立的用户在系统中的标识（SID）与在各数据库系统中的标识（用户名或别名，UID 等）之间的一致性。

——分布式数据库系统中，全局应用的用户标识信息和鉴别信息应存放在全局数据字典中，由全局数据库管理安全机制完成全局用户的身份鉴别。局部应用的用户标识信息和鉴别信息应存放于局部数据字典中，由局部数据库安全机制完成局部用户的身份鉴别。

5.1.1.3 数据完整性

**a)** 应根据本标准 **4.3.1** 条实体完整性和参照完整性的描述，按照《通用技术要求》**6.1.3.4** 条数据完整性的要求设计实体完整性和参照完整性；

**b)** 应根据本标准 **4.3.2** 条用户定义完整性的描述，按照《通用技术要求》**6.1.3.4** 条数据完整性的要求设计用户定义完整性；

**c)** 应根据本标准 **4.3.3** 条完整性操作要求的描述，按照《通用技术要求》**6.1.3.4** 条数据完整性的要求设计数据完整性。

5.1.2 TCB 自身安全保护

5.1.2.1 TSF 保护

应按照《通用技术要求》**6.1.4.1** 条 **TSF** 保护的要求，设计和实现数据库管理系统的 **TSF** 保护。本安全级中，数据库管理系统 TSF 保护的具体要求为：

a） 系统在设计时不应留有“后门”，即不应以维护、支持或操作需要为借口，设计有违反或绕过安全规则的任何类型的入口和文档中未说明的任何模式的入口。

b） 安全结构应是一个独立的、严格定义的软件系统子集，并应防止外部干扰和破坏，如修改其代码或数据结构；

c） 数据库管理系统应进行分层设计，并将数据库管理系统进程与和用户进程进行隔离；

d） 应提供设置和升级配置参数的安装机制，在初始化和对与安全有关的数据结构进行保护之前，应对用户和管理员的安全策略属性应进行定义；

e） 应区分普通操作模式和系统维护模式，TCB 的恢复、全系统操作恢复的启动、配置 TCB 内部的数据库和表等动作应在维护模式中执行。

5.1.2.2 资源利用

应按照《通用技术要求》**6.1.4.2** 条资源利用的要求，设计和实现数据库管理系统的资源利用。在本安全级中，资源利用设计的具体要求为：

a） 通过一定措施确保当系统出现某些确定的故障时，TSF 也能维持正常运行；

b） 采取适当的策略，按有限服务优先级提供主体使用 TSC 内某个资源子集的优先级，进行 TCB 资源的管理和分配；

c） 按资源分配中最大限额的要求，进行 TCB 资源的管理和分配，确保用户和主体不会独占某种受控资源。

5.1.2.3 TCB 访问控制

应按照《通用技术要求》**6.1.4.3** 条 **TCB** 访问控制的要求，设计和实现数据库管理系统的 **TCB** 访问控制。本安全级中，数据库管理系统 TCB 访问控制设计的具体要求为：

a） 按可选属性范围限定最小级的要求，选择某种会话安全属性的所有失败的尝试 ，对建立会话的安全属性的范围进行限制；

b） 按多重并发会话限定中基本限定的要求，进行会话管理的设计。TSF 应限制系统的并发会话的最大数量，并应利用缺省值作为会话次数的限定数；

c） 按最小级会话建立机制，对会话建立的管理进行设计。

5.1.3 TCB 设计和实现

5.1.3.1 配置管理

应按照《通用技术要求》**6.1.5.1** 条配置管理的要求，设计和实现数据库管理系统 **TCB** 的配置管理。本安全级的具体要求为：

**a)** 应具有基本的配置管理能力，即要求开发者所使用的版本号与所表示的 TCB 样本完全对应。

5.1.3.2 分发和操作

应按照《通用技术要求》**6.1.5.2** 条分发和操作的要求，设计和实现数据库管理系统的 **TCB** 分发和操作。本安全级的具体要求为：

a） 应以文档形式提供对 TCB 安全地进行分发的过程，以及安装、生成和启动的过程进行说明，并最终生成安全的配置。文档中所描述的内容应包括：

——提供分发的过程；

——安全启动和操作的过程。

**b)** 对系统的未授权修改的风险，应在交付时控制到最低限度。在包装及安全分送和安装过程中，这种控制应采取软件控制的方式，安全性由末端用户确认，所有安全机制都应以功能状态交付。

**c)** 所有软件应提供安全安装默认值，在客户不做选择时，默认值应使安全机制有效地发挥安全功能。

**d)** 随同系统交付的全部默认用户标识码，应在交付时处于非激活状态，并在使用前由管理员激活。

**e)** 用户文档应同交付的软件一起包装，并应有一套规程确保当前送给用户的软件是严格按照最新的版本制作的。

5.1.3.3 开发

应按照《通用技术要求》**6.1.5.3** 条开发的要求，进行数据库管理系统 **TCB** 的开发。本安全级的具体要求为：

a) 按非形式化功能说明、描述性高层设计、TSF 子集实现、TSF 内部结构模块化、描述性低层设计和非形式化对应性说明的要求，进行 TCB 的开发。

b) 系统的设计和开发应保护数据的完整性，例如，检查数据更新的规则，多重输入的正确处理，返回状态的检查，中间结果的检查，合理值输入检查，事务处理更新的正确性检查等。

**c)** 在内部代码检查时，应解决潜在的安全缺陷，关闭或取消所有的后门。

**d)** 所有交付的软件和文档，应进行关于安全缺陷的定期的和书面的检查，并将检查结果告知用户。

**e)** 系统控制数据，如口令、密钥，不应在未受保护的程序或文档中以明文形式存储，应以书面形式提供给用户关于软件所有权法律保护的指南。

5.1.3.4 指导性文档

应按照《通用技术要求》**6.1.5.4** 条指导性文档的要求，编制 **TCB** 的指导性文档。本安全级的具体要求为：

a) 用户文档应提供关于不同用户的可见的安全机制以及如何利用它们的信息，描述没有明示用户的保护结构，并解释它们的用途和提供有关它们使用的指南。文档中不应包括那些如果公开将会危及系统安全的任何信息。

b) 系统管理员文档应提供关于系统的安全开机、操作和重新启动的信息，包括启动系统的过程（如引导系统进入安全方式）、在系统操作失误时恢复安全系统操作的过程、运行软件和数据备份及转储的方法和过程，还应提供一个单独的安装指南，详细说明设置系统的配置和初始化过程。

c) 安全管理员文档应提供有关如何设置、维护和分析系统安全的详细指导，包括当运行一个安全设备时，需要控制的有关功能和特权的警告，以及与安全有关的管理员功能的详细描述，包括增加和删除一个用户、改变主、客体的安全属性等。

**d)** 文档中不应提供任何一旦泄露将会危及系统安全的信息。有关安全的指令和文档应划分等级分别提供给用户、系统管理员和系统安全员。这些文档应为独立的文档，或作为独立的章条插入到管理员指南和用户指南中。文档也可为硬拷贝、电子文档或联机文档。如果是联机文档应控制对其的访问。

5.1.3.5 生命周期支持

应按照《通用技术要求》**6.1.5.5** 条生命周期支持的要求，设计和实现数据库管理系统的 **TCB**。本安全级的具体要求为：

a) 按开发者定义生命周期模型进行 TCB 开发。

b) 文档应详细阐述安全启动和操作的过程，详细说明安全功能在启动、正常操作维护时是否能被撤消或修改，说明在故障或系统出错时如何恢复系统至安全状态。

5.1.3.6 测试

**应按照《通用技术要求》6.1.5.6 条测试的要求，对数据库管理系统的 TCB 进行测试。本安全级的具体要求为：**

**a) 通过一般功能测试和相符性独立测试，确认 TCB 的功能与所要求功能的一致性。**

**b) 所有系统的安全特性，应被全面测试。所有发现的漏洞应被改正、消除或使其无效，并在消除漏洞后重新测试，以证实它们已被消除，且没有引出新的漏洞。**

**c) 应提供测试文档，详细描述测试计划、测试过程、测试结果。**

5.1.4 TCB 安全管理

**应按照《通用技术要求》6.1.6 条 TCB 安全管理所描述的要求，实现 TCB 的安全管理。本安全级的具体要求为：**

**a) 对 TCB 的访问控制、鉴别控制、审计和安全属性管理等相关的功能，以及与一般的安装、配置等有关的功能，制定相应的操作、运行规程和行为规章制度。**

**b) 根据本级中安全功能技术要求所涉及的自主访问控制、身份鉴别、数据完整性、和安全保证技术要求所涉及的配置管理、分发和操作、开发、指导性文档、生命周期支持、测试等所涉及的有关内容设计 TCB 安全管理。**

5.2 第二级：系统审计保护级

5.2.1 安全功能

5.2.1.1 自主访问控制

应根据本标准 4.2.3 条访问操作、访问规则、和授权传播的描述，按照**《通用技术要求》6.2.3.3 条自主访问控制**所描述的要求设计访问控制功能。本安全级要求：

a) 用目录表访问控制、存取控制表访问控制、能力表访问控制等访问控制表访问控制确定主体对客体的访问权限。数据库管理系统中一般不直接采用稀疏的二维存取矩阵，而采用一些比较实用的技术，如：按行存储、按列存储、锁钥法、口令密码法等实现自主访问控制。

b) 无论采用何种访问控制策略实现访问控制功能，都应允许命名用户以用户和/或用户组的身份规定并控制对客体的共享，并阻止非授权用户读取信息。

**c) 自主访问控制应与身份鉴别和审计相结合，通过确认用户身份的真实性和记录用户的各种成功的 或不成功的访问，使用户对自己的行为承担明确的责任。**

5.2.1.2 身份鉴别

a) 身份鉴别应包括用户标识和用户鉴别。

b) 用户标识应根据 4.1.1 条用户标识的描述，按照**《通用技术要求》6.2.3.1 条用户标识**的要求进行。

c) 用户鉴别应根据 4.1.2 条用户鉴别的描述，按照**《通用技术要求》6.2.3.2 条用户鉴别**的要求进行。

d) 进入数据库系统的用户，首先应由支持数据库系统运行的操作系统进行身份鉴别。

e) 应提供用户进入数据库管理系统时的身份鉴别，并按以下要求进行设计：

——凡需进入数据库管理系统的用户，可以选择采用该用户在操作系统中的标识信息，也可以重新进行用户标识。重新进行用户标识应在用户注册（建立账号）时进行。

——当用户登录到数据库管理系统或与数据库服务器进行访问连接时，应进行用户鉴别。

——数据库管理系统用户标识一般使用用户名和用户标识（UID）。为在整个数据库系统范围实现用户的唯一性，应确保数据库管理系统建立的用户在系统中的标识（SID）与在各

数据库系统中的标识（用户名或别名，UID 等）之间的一致性。

——分布式数据库系统中，全局应用的用户标识信息和鉴别信息应存放在全局数据字典中，由全局数据库管理安全机制完成全局用户的身份鉴别。局部应用的用户标识信息和鉴别信息应存放于局部数据字典中，由局部数据库安全机制完成局部用户的身份鉴别。

**——数据库用户的标识和鉴别信息应受到操作系统和数据库系统的双重保护。操作系统应确保任何用户不能通过数据库以外的使用方式获取和破坏数据库用户的标识和鉴别信息。数据库系统应保证用户以安全的方式和途径使用数据库系统的标识和鉴别信息。**

**——数据库用户标识信息应在数据库系统的整个生命期有效，被撤消的用户账号的 UID 不得再次使用。**

5.2.1.3 客体重用

**应根据本标准 4.5 条的要求，按照《通用技术要求》6.2.3.4 条客体重用的要求进行设计。本安全级要求：**

**a) 由数据库管理系统和支持数据库系统的操作系统共同保证信息不因资源的动态分配而遭泄露。如果操作系统支持客体安全重用功能，数据库管理系统仅需保证数据库系统中逻辑上被删除的信息是物理删除的或是不能再用的；如果操作系统不支持客体安全重用功能，数据库管理系统每次进行新资源分配时，应删除其中包含的残留信息。**

5.2.1.4 审计

**应按照本标准 4.4 条的要求和《通用技术要求》6.2.2.3 条安全审计的要求，设计审计功能。本安全级的要求：**

**a) 审计功能的设计应与用户标识与鉴别、自主访问控制、标记与强制访问控制等安全功能的设计紧密结合；**

5.2.1.5 数据完整性

a) 应根据本标准 4.3.1 条实体完整性和参照完整性的描述，按照**《通用技术要求》6.2.3.5 条数据完整性**的要求设计实体完整性和参照完整性；

b) 应根据本标准 4.3.2 条用户定义完整性的描述，按照**《通用技术要求》6.2.3.5 条数据完整性**的要求设计用户定义完整性；

c) 应根据本标准 4.3.3 条完整性操作要求的描述，按照**《通用技术要求》6.2.3.5 条数据完整性**的要求设计数据完整性。

5.2.2 TCB 自身安全保护

5.2.2.1 TSF 保护

应按照**《通用技术要求》6.2.4.1 条 TSF 保护**的要求，设计和实现数据库管理系统的 TSF 保护。本安全级中，数据库管理系统 TSF 保护的具体要求为：

a) 系统在设计时不应留有“后门”，即不应以维护、支持或操作需要为借口，设计有违反或绕过安全规则的任何类型的入口和文档中未说明的任何模式的入口。

b) 安全结构应是一个独立的、严格定义的软件系统子集，并应防止外部干扰和破坏，如修改其代码或数据结构；

c) 数据库管理系统应进行分层设计，并将数据库管理系统进程与和用户进程进行隔离；

d) 应提供设置和升级配置参数的安装机制，在初始化和对与安全有关的数据结构进行保护之前，应对用户和管理员的安全策略属性应进行定义；

e) 应区分普通操作模式和系统维护模式，TCB 的恢复、全系统操作恢复的启动、配置 TCB 内部的

数据库和表等动作应在维护模式中执行。

f) **应防止普通用户从未经允许的系统进入维护模式，并防止普通用户与系统内维护模式交互,从而保证在普通用户访问系统之前，系统能以一个安全的方式进行安装和配置。**

g) **当数据库管理系统安装完成后，在普通用户访问之前，系统应配置好初始用户和管理员职责、审计参数、系统审计跟踪设置以及对客体的合适的访问控制。**

h) **执行系统所提供的实用程序，应限定于对系统的有效使用，只允许系统管理员修改或替换系统提供的实用程序。**

i) **在 TCB 失败或中断后，进程应保证保护文本以最小的损害得到恢复。并按照失败保护中所描述的内容，实现对 TSF 出现失败时的处理。**

j) **系统应能识别由通信渠道接收的信息的来源者，所有待确认的数据应能从进入点被安全地传送到确认系统，如口令不应由公共的或共享的网络以明文发送，可使用数据加密设备或通过加密信道用加密方式传送。**

5.2.2.2 资源利用

应按照**《通用技术要求》6.2.4.2 条资源利用**的要求，设计和实现数据库管理系统的资源利用。在本安全级中，资源利用设计的具体要求为：

a) 通过一定措施确保当系统出现某些确定的故障时，TSF 也能维持正常运行；

b) 采取适当的策略，按有限服务优先级提供主体使用 TSC 内某个资源子集的优先级，进行 TCB 资源的管理和分配；

c) 按资源分配中最大限额的要求，进行 TCB 资源的管理和分配，确保用户和主体不会独占某种受控资源。

d) **确保在被授权的主体发出请求时，资源能被访问和利用。**

e) **当系统的服务水平降低到预先规定的最小值时，应能检测和发出报告。**

f) **提供管理维护状态中运行的能力，在管理维护状态下各种安全性能全部失效，系统只允许由系统管理员使用。**

5.2.2.3 TCB 访问控制

应按照**《通用技术要求》6.2.4.3 条 TCB 访问控制**的要求，设计和实现数据库管理系统的 TCB 访问控制。本安全级中，数据库管理系统 TCB 访问控制设计的具体要求为：

a) 按可选属性范围限定最小级的要求，选择某种会话安全属性的所有失败的尝试 ，对建立会话的安全属性的范围进行限制；

b) 按多重并发会话限定中基本限定的要求，进行会话管理的设计。**提供适用于 TSF 内所有用户的限制，允许用户会话建立的所有尝试；**

c) **按照 TCB 访问历史所描述的要求，在会话成功建立的基础上，TSF 应显示用户上一次成功/不成功的会话建立的日期，时间，方法，位置，以及从上一次成功的会话建立以来的不成功的尝试的次数。**

d) **按照 TCB 会话建立所描述的要求，TSF 应根据属性允许或拒绝该次会话的建立，这些属性包括：访问地址或端口，用户安全属性（如用户身份、许可证等级、完整性等级、角色中的成员资格），时间范围（如一天中的某些时间、一周的某些天、某些特定日期），或上述属性的组合。**

e) **在会话建立之前，认证机制应对用户身份进行验证；**

f) **成功登录系统后，TCB 应向用户显示的信息包括：**

**——日期、时间、来源和上次成功登录系统的情况；**

**——上次成功访问系统以来身份识别失败的情况；**

**——显示口令到期的天数、成功或不成功的事件次数等。**

5.2.3 TCB 设计和实现

5.2.3.1 配置管理

应按照**《通用技术要求》6.2.5.1 条配置管理**的要求，设计和实现数据库管理系统 TCB 的配置管理。本安全级的具体要求为：

a) 在配置管理能力方面应实现对版本号、**配置项、授权控制**等方面的要求。

b) **配置管理范围方面，应将 TCB 的实现表示、设计文档、测试文档、用户文档、管理员文档以及配置管理文档等置于配置管理之下。**

c) **在系统的整个生存期，即在它的开发、测试和维护期间，应有一个软件配置管理系统处于保持对改变源码和文件的控制状态。只有被授权的代码和代码修改才允许被加进已交付的源码的基本部分。所有改变应被记载和检查，以确保不危及系统的安全。通过技术、物理和保安规章三方面的结合，充分保护生成系统所用到的源码免遭未授权的修改和毁坏。在软件配置管理系统中，应包含以下方面的工具规程：**

**——从源码产生出系统新版本；**

**——鉴定新生成的系统版本；**

**——保护源码免遭未授权修改。**

5.2.3.2 分发和操作

应按照**《通用技术要求》6.2.5.2 条分发和操作**的要求，设计和实现数据库管理系统的 TCB 分发和操作。本安全级的具体要求为：

a) 应以文档形式提供对 TCB 安全地进行分发的过程，以及安装、生成和启动的过程进行说明，并最终生成安全的配置。文档中所描述的内容应包括：

——提供分发的过程；

——安全启动和操作的过程；

**——建立日志的过程。**

b) 对系统的未授权修改的风险，应在交付时控制到最低限度。在包装及安全分送和安装过程中，这种控制应采取软件控制的方式，安全性由末端用户确认，所有安全机制都应以功能状态交付。

c) 所有软件应提供安全安装默认值，在客户不做选择时，默认值应使安全机制有效地发挥安全功能。

d) 随同系统交付的全部默认用户标识码，应在交付时处于非激活状态，并在使用前由管理员激活。

e) 用户文档应同交付的软件一起包装，并应有一套规程确保当前送给用户的软件是严格按照最新的版本制作的。

5.2.3.3 开发

应按照**《通用技术要求》6.2.5.3 条**开发的要求，进行数据库管理系统 TCB 的开发。本安全级的具体要求为：

a) 按非形式化功能说明、**完全定义的外部接口、**描述性高层设计、TSF 子集实现、TSF 内部结构模块化和**复杂性降低**、描述性低层设计非形式化、对应性说明以及**非形式化安全策略模型**的

要求，进行 TCB 的开发。

b) 系统的设计和开发应保护数据的完整性，例如，检查数据更新的规则，多重输入的正确处理，返回状态的检查，中间结果的检查，合理值输入检查，事务处理更新的正确性检查等。

c) 在内部代码检查时，应解决潜在的安全缺陷，关闭或取消所有的后门。

d) 有交付的软件和文档，应进行关于安全缺陷的定期的和书面的检查，并将检查结果告知用户。

e) 系统控制数据，如口令、密钥，不应在未受保护的程序或文档中以明文形式存储，应以书面形式提供给用户关于软件所有权法律保护的指南。

#### 5.2.3.4 指导性文档

应按照**《通用技术要求》6.2.5.4 条指导性文档**的要求，编制 TCB 的指导性文档。本安全级的具体要求为：

a) 用户文档应提供关于不同用户的可见的安全机制以及如何利用它们的信息，描述没有明示用户的保护结构，并解释它们的用途和提供有关它们使用的指南。文档中不应包括那些如果公开将会危及系统安全的任何信息。

b) 系统管理员文档应提供关于系统的安全开机、操作和重新启动的信息，包括启动系统的过程（如引导系统进入安全方式）、在系统操作失误时恢复安全系统操作的过程、运行软件和数据备份及转储的方法和过程，还应提供一个单独的安装指南，详细说明设置系统的配置和初始化过程。

c) 安全管理员文档应提供有关如何设置、维护和分析系统安全的详细指导，包括当运行一个安全设备时，需要控制的有关功能和特权的警告，以及与安全有关的管理员功能的详细描述，包括增加和删除一个用户、改变主、客体的安全属性等。

d) 文档中不应提供任何一旦泄露将会危及系统安全的信息。有关安全的指令和文档应划分等级分别提供给用户、系统管理员和系统安全员。这些文档应为独立的文档，或作为独立的章节插入到管理员指南和用户指南中。文档也可为硬拷贝、电子文档或联机文档。如果是联机文档应控制对其的访问。

**e) 应提供关于所有审计工具的文档，包括为检查和保持审计文件所推荐的过程、针对每种审计事件的详细审计记录文件、为周期性备份和删除审计记录所推荐的过程等。**

**f) 应提供如何进行系统自我评估的章节（带有网络管理、口令要求、拨号访问控制、意外事故计划的安全报告）和为灾害恢复计划所做的建议，以及描述普通侵入技术和其它威胁，并查出和阻止它们的方法。**

#### 5.2.3.5 生命周期支持

应按照**《通用技术要求》6.2.5.5 条生命周期支持**的要求，设计和实现数据库管理系统的 TCB。本安全级的具体要求为：

a) 按开发者定义生命周期模型进行 TCB 开发，并提供**开发过程中的安全措施说明。**

b) 文档应详细阐述安全启动和操作的过程，详细说明安全功能在启动、正常操作维护时是否能被撤消或修改，说明在故障或系统出错时如何恢复系统至安全状态。

**c) 如果系统含有加强安全性的硬件，那么管理员、终端用户或自动的诊断测试，应能在各自的操作环境中运行它并详细说明操作过程。**

#### 5.2.3.6 测试

应按照**《通用技术要求》6.2.5.6 条测试**的要求，对数据库管理系统的 TCB 进行测试。本安全级的具体要求为：

a) 通过一般功能测试和相符性独立测试、**测试的范围分析、高层设计的测试**，确认 TCB 的功能与所要求功能的一致性。

b) 所有系统的安全特性，应被全面测试。**包括查找漏洞，如允许违反系统访问控制要求、允许违反资源访问控制要求、允许拒绝服务、允许多审计或验证数据进行未授权访问等。**所有发现的漏洞应被改正、消除或使其无效，并在消除漏洞后重新测试，以证实它们已被消除，且没有引出新的漏洞。

c) 应提供测试文档，详细描述测试计划、测试过程、测试结果。

5.2.3.7 脆弱性评定

**应按照《通用技术要求》6.2.5.7 条脆弱性评定所描述的要求对所开发的 TCB 进行脆弱性评定。本安全级的具体要求为：**

**a) 从指南检查、TCB 安全功能强度评估和开发者脆弱性分析等方面进行脆弱性评定。**

5.2.4 TCB 安全管理

应按照**《通用技术要求》6.2.6 条 TCB 安全管理**所描述的要求，实现 TCB 的安全管理。本安全级的具体要求为：

a) 对相应的 TCB 的访问控制、鉴别控制、审计和安全属性管理等相关的功能，以及与一般的安装、配置**和维护**有关的功能，制定相应的操作、运行规程和行为规章制度。

b) 根据本级中安全功能技术要求所涉及的自主访问控制、身份鉴别、**客体重用、审计、**数据完整性、和安全保证技术要求所涉及的配置管理、分发和操作、开发、指导性文档、生命周期支持、测试、**脆弱性评定**等所涉及的有关内容设计 TCB 安全管理。

5.3 第三级：安全标记保护级

5.3.1 安全功能

5.3.1.1 自主访问控制

应根据本标准 4.2.3 条访问操作、访问规则、和授权传播的描述，按照**《通用技术要求》6.3.3.3 条自主访问控制**所描述的要求设计访问控制功能。本安全级要求：

a) 用目录表访问控制、存取控制表访问控制、能力表访问控制等访问控制表访问控制确定主体对客体的访问权限。数据库管理系统中一般不直接采用稀疏的二维存取矩阵，而采用一些比较实用的技术，如：按行存储、按列存储、锁钥法、口令密码法等实现自主访问控制。

b) 无论采用何种访问控制策略实现访问控制功能，都应允许命名用户以用户和/或用户组的身份规定并控制对客体的共享，并阻止非授权用户读取信息。

c) 自主访问控制应与身份鉴别和审计相结合，通过确认用户身份的真实性和记录用户的各种成功的或不成功的访问，使用户对自己的行为承担明确的责任。

**d) 应限制授权传播，要求对不可传播的授权进行明确定义提供支持，由系统自动检查并限制这些授权的传播。**

5.3.1.2 强制访问控制

**应根据本标准 4.2.4 条的描述，按照《通用技术要求》6.3.3.5 条强制访问控制的要求，设计访问控制功能。本安全级应：**

**a) 将强制访问控制扩展到计算机信息系统的所有主体与客体，并且，强制访问控制的粒度达到更细的粒度，即客体的最大控制单位应是记录、字段或元素等。**

**b) 应将系统的常规管理、与安全有关的管理以及审计管理，分别由系统管理员、系统安全员和系统审计远来承担，按最小授权原则分别授予它们各自为完成自己所承担任务所需的最小权**

**限，并在三者之间形成相互制约的关系。**

5.3.1.3 标记

**应根据本标准 4.2.1 条标记与安全属性管理和《通用技术要求》6.3.3.4 条标记的要求进行标记功能的设计。本安全级要求：**

**a) 数据库用户的安全属性，应在用户建立注册账号后由系统安全员通过 TCB 所提供的安全员界面操作进行标记，而客体的安全属性则在数据输入到由 TCB 安全功能所控制的范围内时以缺省方式生成或由安全员通过操作界面进行标记；**

5.3.1.4 身份鉴别

应包括用户标识和用户鉴别。

a) 用户标识应根据 4.1.1 条用户标识的描述，按照**《通用技术要求》6.3.3.1 条用户标识**的要求进行。

b) 用户鉴别应根据 4.1.2 条用户鉴别的描述，按照**《通用技术要求》6.3.3.2 条用户鉴别**的要求进行。

c) 进入数据库系统的用户，首先应由支持数据库系统运行的操作系统进行身份鉴别。

d) 应提供用户进入数据库管理系统时的身份鉴别，并按以下要求进行设计：

——凡需进入数据库管理系统的用户，可以选择采用该用户在操作系统中的标识信息，也可以重新进行用户标识。重新进行用户标识应在用户注册（建立账号）时进行。

——当用户登录到数据库管理系统或与数据库服务器进行访问连接时，应进行用户鉴别。

——数据库管理系统用户标识一般使用用户名和用户标识（UID）。为在整个数据库系统范围实现用户的唯一性，应确保数据库管理系统建立的用户在系统中的标识（SID）与在各数据库系统中的标识（用户名或别名，UID 等）之间的一致性。

——分布式数据库系统中，全局应用的用户标识信息和鉴别信息应存放在全局数据字典中，由全局数据库管理安全机制完成全局用户的身份鉴别。局部应用的用户标识信息和鉴别信息应存放于局部数据字典中，由局部数据库安全机制完成局部用户的身份鉴别。

——数据库用户的标识和鉴别信息应受到操作系统和数据库系统的双重保护。操作系统应确保任何用户不能通过数据库以外的使用方式获取和破坏数据库用户的标识和鉴别信息。数据库系统应保证用户以安全的方式和途径使用数据库系统的标识和鉴别信息。

——数据库用户标识信息应在数据库系统的整个生命期有效，被撤消的用户账号的 UID 不得再次使用。

**——身份鉴别应采用高强度的安全机制，如 IC 卡信息、人体生物特征信息（指纹、视网膜）等特殊信息进行身份鉴别，或者采用更加完善的 CA 认证系统等。**

**——IC 卡信息身份鉴别应采用密码技术，以防伪造、复制，应定义鉴别尝试允许次数、尝试时间，定义鉴别失败后同一场地再次鉴别的时间间隔，定义鉴别失败处理的条件和动作，如审计、跟踪、警报、封锁账户（永久或有条件地恢复）、封锁场地（永久或有条件地恢复）等。**

5.3.1.5 客体重用

应根据本标准 4.5 条的要求，按照**《通用技术要求》6.3.3.6 条客体重用**的要求进行设计。本安全级要求：

a) 由数据库管理系统和支持数据库系统的操作系统共同保证信息不因资源的动态分配而遭泄露。如果操作系统支持客体安全重用功能，数据库管理系统仅需保证数据库系统中逻辑上被

删除的信息是物理删除的或是不能再用的；如果操作系统不支持客体安全重用功能，数据库管理系统每次进行新资源分配时，应删除其中包含的残留信息。

5.3.1.6 审计

应按照本标准 4.4 条的要求和**《通用技术要求》6.3.2.4 条安全审计**的要求，设计审计功能。本安全级的要求：

a) 审计功能的设计应与用户标识与鉴别、自主访问控制、标记与**强制访问控制**等安全功能的设计紧密结合；

b) **对与标识及强制访问控制等安全机制有关的内容，如安全属性的操作等进行审计；**

**c) 对网络环境下运行的数据库管理系统，应建立分布式的审计系统，并以审计中心进行管理和控制。**

5.3.1.7 数据完整性

a) 应根据本标准 4.3.1 条实体完整性和参照完整性的描述，按照**《通用技术要求》6.3.3.7 条数据完整性**的要求设计实体完整性和参照完整性；

b) 应根据本标准 4.3.2 条用户定义完整性的描述，按照**《通用技术要求》6.3.3.7 条数据完整性**的要求设计用户定义完整性；

c) 应根据本标准 4.3.3 条完整性操作要求的描述，按照**《通用技术要求》6.3.3.7 条数据完整性**的要求设计数据完整性。

5.3.2 TCB 自身安全保护

5.3.2.1 TSF 保护

应按照**《通用技术要求》6.3.4.1 条 TSF 保护**的要求，设计和实现数据库管理系统的 TSF 保护。本安全级中，数据库管理系统 TSF 保护的具体要求为：

a) 系统在设计时不应留有“后门”，即不应以维护、支持或操作需要为借口，设计有违反或绕过安全规则的任何类型的入口和文档中未说明的任何模式的入口。

b) 安全结构应是一个独立的、严格定义的软件系统子集，并应防止外部干扰和破坏，如修改其代码或数据结构；

c) 数据库管理系统应进行分层设计，并将数据库管理系统进程与和用户进程进行隔离；

d) 应提供设置和升级配置参数的安装机制，在初始化和对与安全有关的数据结构进行保护之前，应对用户和管理员的安全策略属性应进行定义；

e) 应区分普通操作模式和系统维护模式，TCB 的恢复、全系统操作恢复的启动、配置 TCB 内部的数据库和表等动作应在维护模式中执行。

f) 应防止普通用户从未经允许的系统进入维护模式，并防止普通用户与系统内维护模式交互,从而保证在普通用户访问系统之前，系统能以一个安全的方式进行安装和配置。

g) 当数据库管理系统安装完成后，在普通用户访问之前，系统应配置好初始用户和管理员职责、审计参数、系统审计跟踪设置以及对客体的合适的访问控制。

h) 执行系统所提供的实用程序，应限定于对系统的有效使用，只允许系统管理员修改或替换系统提供的实用程序。

i) 在 TCB 失败或中断后，进程应保证保护文本以最小的损害得到恢复。并按照失败保护中所描述的内容，实现对 TSF 出现失败时的处理。**系统因故障或其它原因中断后，应有一种机制恢复系统。系统应提供在管理维护状态中运行的能力，管理维护状态只能被系统管理员使用，且各种安全功能全部失效。**

j) 系统应能识别由通信渠道接收的信息的来源者，所有待确认的数据应能从进入点被安全地传送到确认系统，如口令不应由公共的或共享的网络以明文发送，可使用数据加密设备或通过加密信道用加密方式传送。

**k) 系统应为系统管理员提供一种机制，来产生安全参数值的详细报告。**

5.3.2.2 资源利用

应按照**《通用技术要求》6.3.4.2 条资源利用**的要求，设计和实现数据库管理系统的资源利用。在本安全级中，资源利用设计的具体要求为：

a) 通过一定措施确保当系统出现某些确定的故障时，TSF 也能维持正常运行；

b) 采取适当的策略，按有限服务优先级提供主体使用 TSC 内某个资源子集的优先级，进行 TCB 资源的管理和分配；

c) 按资源分配中最大限额的要求，进行 TCB 资源的管理和分配，确保用户和主体不会独占某种受控资源。

d) 确保在被授权的主体发出请求时，资源能被访问和利用。

e) 当系统的服务水平降低到预先规定的最小值时，应能检测和发出报告。

f) 提供管理维护状态中运行的能力，在管理维护状态下各种安全性能全部失效，系统只允许由系统管理员使用。

**g) 系统应提供软件及数据备份和复原的过程，在系统中应加入再启动的同步点，以便于系统的复原。**

**h) 数据库管理系统应能提供命名的或用户可访问的系统资源的修改历史记录。**

**i) 系统应提供能用于定期确认系统正确操作的机制和过程，包括对可能在全系统内传播的错误状态的检测以及超过规定门限的通讯差错的检测等。**

5.3.2.3 TCB 访问控制

应按照**《通用技术要求》6.3.4.3 条 TCB 访问控制**的要求，设计和实现数据库管理系统的 TCB 访问控制。本安全级中，数据库管理系统 TCB 访问控制设计的具体要求为：

a) 按可选属性范围限定最小级的要求，选择某种会话安全属性的所有失败的尝试 ，对建立会话的安全属性的范围进行限制；

b) 按多重并发会话限定中基本限定的要求，进行会话管理的设计。提供适用于 TSF 内所有用户的限制, 允许用户会话建立的所有尝试；

c) 按照 TCB 访问历史所描述的要求，在会话成功建立的基础上，TSF 应显示用户上一次成功/不成功的会话建立的日期，时间，方法，位置，以及从上一次成功的会话建立以来的不成功的尝试的次数。

d) 按照 TCB 会话建立所描述的要求，TSF 应根据属性允许或拒绝该次会话的建立，这些属性包括：访问地址或端口，用户安全属性（如用户身份、许可证等级、完整性等级、角色中的成员资格），时间范围（如一天中的某些时间、一周的某些天、某些特定日期），或上述属性的组合。

e) 在会话建立之前，认证机制应对用户身份进行验证；

a) 成功登录系统后，TCB 应向用户显示的信息包括：

——日期、时间、来源和上次成功登录系统的情况；

——上次成功访问系统以来身份识别失败的情况；

——显示口令到期的天数、成功或不成功的事件次数等。

b) **在规定的未使用时限后，系统应根据提供所提供的期限默认值断开会话或重新认证用户。**

c) **系统应提供锁定用户键盘的机制，键盘开锁过程应要求验证用户。**

d) **当用户不正确的登录次数达到系统规定的次数时，系统应退出登录过程并终止与用户的交互。系统应提供门限默认值。当门限值被超过时，系统应立即通知系统管理员，同时系统可以指定一段停顿时间，在这段时间之后，才允许重新开始登录程序。系统应具有在连续的侵入尝试下，增加时间间隔的能力，从而延长系统被攻破的时间。**

e) **系统应保证即使输入的用户标识是无效的，也应进行完整的用户验证过程，出错的反馈信息不应暴露哪一部分的验证信息是错误的。**

f) **系统应提供一种机制，能按钟点、周日、年月日等条件规定哪些用户能进入系统，哪些用户不能进入系统。**

g) **系统应提供一种机制，能按照进入方式或地点拒绝或接受用户。**

h) **系统应提供一种机制，能限制用户在指定的网络地址或端口访问系统。例如，限制系统管理员只能通过系统控制台访问系统。**

i) **系统应提供一种机制，限制指定的用户或用户组只能进行不修改的访问。**

5.3.3 TCB 设计和实现

5.3.3.1 配置管理

应按照**《通用技术要求》6.3.5.1 条配置管理**的要求，设计和实现数据库管理系统 TCB 的配置管理。本安全级的具体要求为：

a) **在配置管理自动化方面要求部分的配置管理自动化。**

b) 在配置管理能力方面应实现对版本号、配置项、授权控制等方面的要求。

c) 配置管理范围方面，应将 TCB 的实现表示、设计文档、测试文档、用户文档、管理员文档以及配置管理文档等置于配置管理之下，**要求实现对配置管理范围内的问题，特别是安全缺陷问题进行跟踪。**

d) 在系统的整个生存期，即在它的开发、测试和维护期间，应有一个软件配置管理系统处于保持对改变源码和文件的控制状态。只有被授权的代码和代码修改才允许被加进已交付的源码的基本部分。所有改变应被记载和检查，以确保不危及系统的安全。通过技术、物理和保安规章三方面的结合，充分保护生成系统所用到的源码免遭未授权的修改和毁坏。在软件配置管理系统中，应包含以下方面的工具规程：

——从源码产生出系统新版本；

——鉴定新生成的系统版本；

——保护源码免遭未授权修改。

5.3.3.2 分发和操作

应按照**《通用技术要求》6.3.5.2 条分发和操作**的要求，设计和实现数据库管理系统的 TCB 分发和操作。本安全级的具体要求为：

a) 应以文档形式提供对 TCB 安全地进行分发的过程，以及安装、生成和启动的过程进行说明，并最终生成安全的配置。文档中所描述的内容应包括：

——提供分发的过程；

——安全启动和操作的过程；

**——建立日志的过程；**

**——修改检测的内容；**

**——对任何安全加强功能在启动、正常操作维护时能被撤消或修改的阐述；**

**——在故障或硬件、软件出错后恢复系统至安全状态的规程；**

**——对含有加强安全性的硬件部件，应说明用户或自动的诊断测试的操作环境和使用方法；**

**——所有诊断测试过程中，为加强安全性的硬件部件所提供例证的结果；**

**——在启动和操作时产生审计踪迹输出的例证。**

b) 对系统的未授权修改的风险，应在交付时控制到最低限度。在包装及安全分送和安装过程中，这种控制应采取软件控制的方式，安全性由末端用户确认，所有安全机制都应以功能状态交付。

c) 所有软件应提供安全安装默认值，在客户不做选择时，默认值应使安全机制有效地发挥安全功能。

d) 随同系统交付的全部默认用户标识码，应在交付时处于非激活状态，并在使用前由管理员激活。

e) 用户文档应同交付的软件一起包装，并应有一套规程确保当前送给用户的软件是严格按照最新的版本制作的。

**f) 以安全方式开发并交付系统后，仍应提供对产品的长期维护和评估的支持，包括产品中的安全漏洞和现场问题的解决。**

**g) 应以书面形式向用户通告新的全问题。**

**h) 可能受到威胁的所有的安全问题，均应描述其特点，并被作为主要的问题对待，直到它被解决或在用户同意下降级使用。**

**i) 为了支持已交付的软件的每个版本，对所有已有的安全漏洞都应有文档说明，并提交用户。**

**j) 安全漏洞应及时修改。安全功能的增加和改进应独立于系统版本的升级。**

**k) 没有用户授权，不应在正进行生产性运行的系统上实施新特性和简易原型的开发、测试和安装。**

**l) 新版本不应违反最初的安全策略和设想，应避免在维护、增加或功能升级中引入安全漏洞。所有功能的改变和安全结构设置的缺省默认值都应在文档中被记录。在新版本交付用户使用时，用户应能得到相应的文档。**

5.3.3.3 开发

应按照**《通用技术要求》6.3.5.3 条**开发的要求，进行数据库管理系统 TCB 的开发。本安全级的具体要求为：

a) 按非形式化功能说明、完全定义的外部接口、**安全加强的高层设计、TSF 完全实现、**TSF 内部结构模块化和复杂性降低、描述性低层设计非形式化、对应性说明以及非形式化安全策略模型的要求，进行 TCB 的开发。

b) 系统的设计和开发应保护数据的完整性，例如，检查数据更新的规则，多重输入的正确处理，返回状态的检查，中间结果的检查，合理值输入检查，事务处理更新的正确性检查等。

c) 在内部代码检查时，应解决潜在的安全缺陷，关闭或取消所有的后门。

d) 有交付的软件和文档，应进行关于安全缺陷的定期的和书面的检查，并将检查结果告知用户。

e) 系统控制数据，如口令、密钥，不应在未受保护的程序或文档中以明文形式存储，应以书面形式提供给用户关于软件所有权法律保护的指南。

**f) 在数据库管理系统开发的敏感阶段，应保持一个安全环境，该安全环境要求：**

**——描述数据库管理系统开发所使用的计算机系统的安全使用和维护情况的安全策略和措施**

**应有书面记载，并可供检查；**

**——系统开发过程中使用的所有计算机系统应接受定期的和有书面记载的内部安全审计，描述审计过程的文件和真实的审计报告应可供检查；**

**——除授权的分发机构外，不应在开发环境外部复制或分发内部文档；**

**——开发环境的计算机系统使用的所有软件应当合法地从确定的渠道获得；**

**——开发者个人独自开发的软件，应在被开发管理者审核后才能用于开发的系统。**

5.3.3.4 指导性文档

应按照**《通用技术要求》6.3.5.4 条指导性文档**的要求，编制 TCB 的指导性文档。本安全级的具体要求为：

a) **应为最终用户提供简单概要、分章节或手册形式的文档，保证用户拥有进行安全操作所需要的所有信息。与安全有关的信息应包含在一个特别的手册中或许多标准的文本集中，提供用户查阅所有的安全功能。这些信息可随系统发送，也可明确指出它包含在哪个文本当中。**

b) **通过提供指导性文档，应把如何安全使用和维护数据库管理系统的信息交付给系统的用户、系统管理员和系统安全员。对文档的总体要求是：**

**——应对所有的安全访问和相关过程、特权、功能等适当的管理加以阐述；**

**——应阐述安全管理和安全服务的交互，并提供新的 TCB 安全生成的指导；**

**——应详细给出每种审计事件的审计记录的结构，以便考察和维护审计文件和进程；**

**——应提供一个准则集，用于保证附加的说明的一致性不受破坏。**

c) 用户文档应提供关于不同用户的可见的安全机制以及如何利用它们的信息，描述没有明示用户的保护结构，并解释它们的用途和提供有关它们使用的指南。文档中不应包括那些如果公开将会危及系统安全的任何信息。

d) 系统管理员文档应提供关于系统的安全开机、操作和重新启动的信息，包括启动系统的过程（如引导系统进入安全方式）、在系统操作失误时恢复安全系统操作的过程、运行软件和数据备份及转储的方法和过程，还应提供一个单独的安装指南，详细说明设置系统的配置和初始化过程。

e) 安全管理员文档应提供有关如何设置、维护和分析系统安全的详细指导，包括当运行一个安全设备时，需要控制的有关功能和特权的警告，以及与安全有关的管理员功能的详细描述，包括增加和删除一个用户、改变主、客体的安全属性等。**安全管理员文档应提供安全管理员了解如何用安全的方式管理系统，除了给出一般的安全忠告，还要明确：**

**——在系统用安全的方法设置时，围绕用户、用户账号、用户组成员关系、主体和客体的属性等，应如何安装或终止安装；**

**——在系统的生命周期内如何用安全的方法维护系统，包括为了防止系统被破坏而进行的每天、每周、每月的安全常规备份等；**

**——如何用安全的方法重建部分 TCB（如内核）的方法（如果允许在系统上重建 TCB）；**

**——说明审计跟踪机制，使授权用户可以有效地使用审计跟踪来执行本地的安全策略；**

**——必要时，如何调整系统的安全默认配置。**

f) 文档中不应提供任何一旦泄露将会危及系统安全的信息。有关安全的指令和文档应划分等级分别提供给用户、系统管理员和系统安全员。这些文档应为独立的文档，或作为独立的章节插入到管理员指南和用户指南中。文档也可为硬拷贝、电子文档或联机文档。如果是联机文档应控制对其的访问。

g) 应提供关于所有审计工具的文档，包括为检查和保持审计文件所推荐的过程、针对每种审计事件的详细审计记录文件、为周期性备份和删除审计记录所推荐的过程等。

h) 应提供如何进行系统自我评估的章节（带有网络管理、口令要求、拨号访问控制、意外事故计划的安全报告）和为灾害恢复计划所做的建议，以及描述普通侵入技术和其它威胁，并查出和阻止它们的方法。

5.3.3.5 生命周期支持

应按照**《通用技术要求》6.3.5.5 条生命周期支持**的要求，设计和实现数据库管理系统的 TCB。本安全级的具体要求为：

a) **按标准的生命周期模型进行开发，提供安全措施说明，并明确定义开发工具。**

b) 文档应详细阐述安全启动和操作的过程，详细说明安全功能在启动、正常操作维护时是否能被撤消或修改，说明在故障或系统出错时如何恢复系统至安全状态。

c) 如果系统含有加强安全性的硬件，那么管理员、终端用户或自动的诊断测试，应能在各自的操作环境中运行它并详细说明操作过程。

5.3.3.6 测试

应按照**《通用技术要求》6.3.5.6 条测试**的要求，对数据库管理系统的 TCB 进行测试。本安全级的具体要求为：

a) 应通过一般功能测试和**抽样性独立测试**，测试的范围分析，高层设计测试、**低层设计测试，顺序的功能测试等**，确认 TCB 的功能与所要求的功能相一致。

b) 所有系统的安全特性，应被全面测试。包括查找漏洞，如允许违反系统访问控制要求、允许违反资源访问控制要求、允许拒绝服务、允许多审计或验证数据进行未授权访问等。所有发现的漏洞应被改正、消除或使其无效，并在消除漏洞后重新测试，以证实它们已被消除，且没有引出新的漏洞。

c) 应提供测试文档，详细描述测试计划、测试过程、测试结果。

5.3.3.7 脆弱性评定

应按照《通用技术要求》6**.3.5.7 条脆弱性评定**所描述的要求对所开发的 TCB 进行脆弱性评定。本安全级的具体要求为：

a) 从指南检查、**分析确认**，TCB 安全功能强度评估，开发者脆弱性分析、**独立脆弱性分析**等方面进行脆弱性评定。

5.3.4 TCB 安全管理

应按照**《通用技术要求》6.3.6 条 TCB 安全管理**所描述的要求，实现 TCB 的安全管理。本安全级的具体要求为：

a) 对相应的 TCB 的访问控制、鉴别控制、审计和安全属性管理等相关的功能，以及与一般的安装、配置和维护有关的功能，制定相应的操作、运行规程和行为规章制度。

b) 根据本级中安全功能技术要求所涉及的自主访问控制、**标记、强制访问控制**、身份鉴别、客体重用、审计、数据完整性、和安全保证技术要求所涉及的配置管理、分发和操作、开发、指导性文档、生命周期支持、测试、脆弱性评定等所涉及的有关内容设计 TCB 安全管理。

**c) 将系统管理员、安全员和审计员等重要安全角色分别设置专人担任，并按“最小授权原则”分别授予他们各自为完成自身任务所需的最小权限，并形成相互制约的关系。**

## 5.4 第四级：结构化保护级

### 5.4.1 安全功能

#### 5.4.1.1 自主访问控制

应根据本标准 4.2.3 条访问操作、访问规则、和授权传播的描述，按照**《通用技术要求》6.4.3.3 条自主访问控制**所描述的要求设计访问控制功能。本安全级要求：

**a) 将自主访问控制扩展到计算机信息系统的所有主体与客体，并且，要求自主访问控制的粒度达到更细的粒度。即，自主访问控制中的客体的最大控制单位应是记录、字段、元素等。**

b) 用目录表访问控制、存取控制表访问控制、能力表访问控制等访问控制表访问控制确定主体对客体的访问权限。数据库管理系统中一般不直接采用稀疏的二维存取矩阵，而采用一些比较实用的技术，如：按行存储、按列存储、锁钥法、口令密码法等实现自主访问控制。

c) 无论采用何种访问控制策略实现访问控制功能，都应允许命名用户以用户和/或用户组的身份规定并控制对客体的共享，并阻止非授权用户读取信息。

d) 自主访问控制应与身份鉴别和审计相结合，通过确认用户身份的真实性和记录用户的各种成功的或不成功的访问，使用户对自己的行为承担明确的责任。

e) 应限制授权传播，要求对不可传播的授权进行明确定义提供支持，由系统自动检查并限制这些授权的传播。

#### 5.4.1.2 强制访问控制

应根据本标准 4.2.4 条的描述，按照**《通用技术要求》6.4.3.5 条强制访问控制**的要求，设计访问控制功能。本安全级应：

**a) 将强制访问控制扩展到计算机信息系统的所有主体与客体，并且，强制访问控制的粒度达到更细的粒度，即客体的最大控制单位应是记录、字段或元素等。**

b) 应将系统的常规管理、与安全有关的管理以及审计管理，分别由系统管理员、系统安全员和系统审计员来承担，按最小授权原则分别授予它们各自为完成自己所承担任务所需的最小权限，并在三者之间形成相互制约的关系。

#### 5.4.1.3 标记

应根据本标准 4.2.1 条标记与安全属性管理和**《通用技术要求》6.4.3.4 条标记**的要求进行标记功能的设计。本安全级要求：

a) 数据库用户的安全属性，应在用户建立注册账号后由系统安全员通过 TCB 所提供的安全员界面操作进行标记，而客体的安全属性则在数据输入到由 TCB 安全功能所控制的范围内时以缺省方式生成或由安全员通过操作界面进行标记；

**b) 将标记扩展到信息系统中的所有主体与客体，对于从 TCB 控制外导入到数据库系统中的未标记信息进行默认标记或由安全管理员进行标记。对于输出到 TCB 控制范围以外的数据，如打印输出的数据时，应明显的表示出该数据的安全标记。**

#### 5.4.1.4 身份鉴别

应包括用户标识和用户鉴别。

a) 用户标识应根据 4.1.1 条用户标识的描述，按照**《通用技术要求》6.4.3.1 条用户标识**的要求进行。

b) 用户鉴别应根据 4.1.2 条用户鉴别的描述，按照**《通用技术要求》6.4.3.2 条用户鉴别**的要求进行。

c) 进入数据库系统的用户，首先应由支持数据库系统运行的操作系统进行身份鉴别。

d) 应提供用户进入数据库管理系统时的身份鉴别，并按以下要求进行设计：

——凡需进入数据库管理系统的用户，可以选择采用该用户在操作系统中的标识信息，也可以重新进行用户标识。重新进行用户标识应在用户注册（建立账号）时进行。

——当用户登录到数据库管理系统或与数据库服务器进行访问连接时，应进行用户鉴别。

——数据库管理系统用户标识一般使用用户名和用户标识（UID）。为在整个数据库系统范围实现用户的唯一性，应确保数据库管理系统建立的用户在系统中的标识（SID）与在各数据库系统中的标识（用户名或别名，UID 等）之间的一致性。

——分布式数据库系统中，全局应用的用户标识信息和鉴别信息应存放在全局数据字典中，由全局数据库管理安全机制完成全局用户的身份鉴别。局部应用的用户标识信息和鉴别信息应存放于局部数据字典中，由局部数据库安全机制完成局部用户的身份鉴别。

——数据库用户的标识和鉴别信息应受到操作系统和数据库系统的双重保护。操作系统应确保任何用户不能通过数据库以外的使用方式获取和破坏数据库用户的标识和鉴别信息。数据库系统应保证用户以安全的方式和途径使用数据库系统的标识和鉴别信息。

——数据库用户标识信息应在数据库系统的整个生命期有效，被撤消的用户账号的 UID 不得再次使用。

——身份鉴别应采用高强度的安全机制，如 IC 卡信息、人体生物特征信息（指纹、视网膜）等特殊信息进行身份鉴别，或者采用更加完善的 CA 认证系统等。

——IC 卡信息身份鉴别应采用密码技术，以防伪造、复制，应定义鉴别尝试允许次数、尝试时间，定义鉴别失败后同一场地再次鉴别的时间间隔，定义鉴别失败处理的条件和动作，如审计、跟踪、警报、封锁账户（永久或有条件地恢复）、封锁场地（永久或有条件地恢复）等。

#### 5.4.1.5 客体重用

应根据本标准 4.5 条的要求，按照**《通用技术要求》6.4.3.6 条客体重用**的要求进行设计。本安全级要求：

a) 由数据库管理系统和支持数据库系统的操作系统共同保证信息不因资源的动态分配而遭泄露。如果操作系统支持客体安全重用功能，数据库管理系统仅需保证数据库系统中逻辑上被删除的信息是物理删除的或是不能再用的；如果操作系统不支持客体安全重用功能，数据库管理系统每次进行新资源分配时，应删除其中包含的残留信息。

**b) 在释放存储重要信息的资源时，应采用特殊的方法对其残留的信息进行彻底清除。**

#### 5.4.1.6 审计

应按照本标准 5.4 条的要求和**《通用技术要求》6.4.2.4 条安全审计**的要求，设计审计功能。本安全级的要求：

a) 审计功能的设计应与用户标识与鉴别、自主访问控制、标记与强制访问控制等安全功能的设计紧密结合；

b) 对与标识及强制访问控制等安全机制有关的内容，如安全属性的操作等进行审计；

c) 对网络环境下运行的数据库管理系统，应建立分布式的审计系统，并以审计中心进行管理和控制。

#### 5.4.1.7 数据完整性

a) 应根据本标准 4.3.1 条实体完整性和参照完整性的描述，按照**《通用技术要求》6.4.3.7 条数据完整性**的要求设计实体完整性和参照完整性；

b) 应根据本标准 4.3.2 条用户定义完整性的描述，按照**《通用技术要求》6.4.3.7 条数据完整性**的要求设计用户定义完整性；

c) 应根据本标准 4.3.3 条完整性操作要求的描述，按照**《通用技术要求》6.4.3.7 条数据完整性**的要求设计数据完整性。

5.4.1.9 隐蔽信道分析

**应根据本标准 4.7.1 条一般性隐蔽信道分析的描述和《通用技术要求》6.4.3.8 条隐蔽信道分析的要求进行隐蔽信道分析。**

5.4.1.10 可信路径

**在对用户进行初始登录和鉴别时或在用户与 TCB 间进行数据传送时，应根据 4.8 条可信路径的描述的和《通用技术要求》6.4.3.9 条可信路径的要求进行可信路径的设计。**

5.4.1.11 推理控制

**应根据附录 A.8 所描述的推理方法、用于推理的信息以及防止推理的方法中对数据重新分级或对约束重新分级的方法实现推理控制。**

5.4.2 TCB 自身安全保护

5.4.2.1 TSF 保护

应按照**《通用技术要求》6.4.4.1 条 TSF 保护**的要求，设计和实现数据库管理系统的 TSF 保护。本安全级中，数据库管理系统 TSF 保护的具体要求为：

a) 系统在设计时不应留有“后门”，即不应以维护、支持或操作需要为借口，设计有违反或绕过安全规则的任何类型的入口和文档中未说明的任何模式的入口。

b) 安全结构应是一个独立的、严格定义的软件系统子集，并应防止外部干扰和破坏，如修改其代码或数据结构；

c) 数据库管理系统应进行分层设计，并将数据库管理系统进程与和用户进程进行隔离；

d) 应提供设置和升级配置参数的安装机制，在初始化和对与安全有关的数据结构进行保护之前，应对用户和管理员的安全策略属性应进行定义；

e) 应区分普通操作模式和系统维护模式，TCB 的恢复、全系统操作恢复的启动、配置 TCB 内部的数据库和表等动作应在维护模式中执行。

f) 应防止普通用户从未经允许的系统进入维护模式，并防止普通用户与系统内维护模式交互,从而保证在普通用户访问系统之前，系统能以一个安全的方式进行安装和配置。

g) 当数据库管理系统安装完成后，在普通用户访问之前，系统应配置好初始用户和管理员职责、审计参数、系统审计跟踪设置以及对客体的合适的访问控制。

h) 执行系统所提供的实用程序，应限定于对系统的有效使用，只允许系统管理员修改或替换系统提供的实用程序。

i) 在 TCB 失败或中断后，进程应保证保护文本以最小的损害得到恢复。并按照失败保护中所描述的内容，实现对 TSF 出现失败时的处理。系统因故障或其它原因中断后，应有一种机制恢复系统。系统应提供在管理维护状态中运行的能力，管理维护状态只能被系统管理员使用，且各种安全功能全部失效。

j) 系统应能识别由通信渠道接收的信息的来源者，所有待确认的数据应能从进入点被安全地传送到确认系统，如口令不应由公共的或共享的网络以明文发送，可使用数据加密设备或通过加密信道用加密方式传送。

k) 系统应为系统管理员提供一种机制，来产生安全参数值的详细报告。

5.4.2.2 资源利用

应按照**《通用技术要求》6.4.4.2 条资源利用**的要求，设计和实现数据库管理系统的资源利用。在本安全级中，资源利用设计的具体要求为：

a) 通过一定措施确保当系统出现某些确定的故障时，TSF 也能维持正常运行；
b) 采取适当的策略，按有限服务优先级提供主体使用 TSC 内某个资源子集的优先级，进行 TCB 资源的管理和分配；
c) 按资源分配中最大限额的要求，进行 TCB 资源的管理和分配，确保用户和主体不会独占某种受控资源。
d) 确保在被授权的主体发出请求时，资源能被访问和利用。
e) 当系统的服务水平降低到预先规定的最小值时，应能检测和发出报告。
f) 提供管理维护状态中运行的能力，在管理维护状态下各种安全性能全部失效，系统只允许由系统管理员使用。
g) 系统应提供软件及数据备份和复原的过程，在系统中应加入再启动的同步点，以便于系统的复原。
h) 数据库管理系统应能提供命名的或用户可访问的系统资源的修改历史记录。
i) 系统应提供能用于定期确认系统正确操作的机制和过程，包括对可能在全系统内传播的错误状态的检测以及超过规定门限的通讯差错的检测等。

5.4.2.3 TCB 访问

应按照**《通用技术要求》6.4.4.3 条 TCB 访问控制**的要求，设计和实现数据库管理系统的 TCB 访问控制。本安全级中，数据库管理系统 TCB 访问控制设计的具体要求为：

a) 按可选属性范围限定最小级的要求，选择某种会话安全属性的所有失败的尝试 ，对建立会话的安全属性的范围进行限制；
b) 按多重并发会话限定中基本限定的要求，进行会话管理的设计。提供适用于 TSF 内所有用户的限制, 允许用户会话建立的所有尝试；
c) 按照 TCB 访问历史所描述的要求，在会话成功建立的基础上，TSF 应显示用户上一次成功/不成功的会话建立的日期，时间，方法，位置，以及从上一次成功的会话建立以来的不成功的尝试的次数。
d) 按照 TCB 会话建立所描述的要求，TSF 应根据属性允许或拒绝该次会话的建立，这些属性包括：访问地址或端口，用户安全属性（如用户身份、许可证等级、完整性等级），时间范围（如一天中的某些时间、一周的某些天、某些特定日期），或上述属性的组合。
e) 在会话建立之前，认证机制应对用户身份进行验证；
f) 成功登录系统后，TCB 应向用户显示的信息包括：
——日期、时间、来源和上次成功登录系统的情况；
——上次成功访问系统以来身份识别失败的情况；
——显示口令到期的天数、成功或不成功的事件次数等。
g) 在规定的未使用时限后，系统应根据提供所提供的期限默认值断开会话或重新认证用户。
h) 系统应提供锁定用户键盘的机制，键盘开锁过程应要求验证用户。
i) 当用户不正确的登录次数达到系统规定的次数时，系统应退出登录过程并终止与用户的交互。系统应提供门限默认值。当门限值被超过时，系统应立即通知系统管理员，同时系统可以指定一段停顿时间，在这段时间之后，才允许重新开始登录程序。系统应具有在连续的侵入尝

试下，增加时间间隔的能力，从而延长系统被攻破的时间。

j) 系统应保证即使输入的用户标识是无效的，也应进行完整的用户验证过程，出错的反馈信息不应暴露哪一部分的验证信息是错误的。

k) 系统应提供一种机制，能按钟点、周日、年月日等条件规定哪些用户能进入系统，哪些用户不能进入系统。

l) 系统应提供一种机制，能按照进入方式或地点拒绝或接受用户。

m) 系统应提供一种机制，能限制用户在指定的网络地址或端口访问系统。例如，限制系统管理员只能通过系统控制台访问系统。

n) 系统应提供一种机制，限制指定的用户或用户组只能进行不修改的访问。

### 5.4.3 TCB 设计和实现

#### 5.4.3.1 配置管理

应按照**《通用技术要求》6.4.5.1 条配置管理**的要求，设计和实现数据库管理系统 TCB 的配置管理。本安全级的具体要求为：

a) 在配置管理自动化方面要求部分的配置管理自动化。

b) 在配置管理能力方面应实现对版本号、配置项、授权控制、**生成支持和验收过程及进一步的支持**等方面的要求。

d) 配置管理范围方面，应将 TCB 的实现表示、设计文档、测试文档、用户文档、管理员文档以及配置管理文档等置于配置管理之下，要求实现对配置管理范围内的问题，特别是安全缺陷问题进行跟踪，**还应包括开发工具配置管理。**

e) 在系统的整个生存期，即在它的开发、测试和维护期间，应有一个软件配置管理系统处于保持对改变源码和文件的控制状态。只有被授权的代码和代码修改才允许被加进已交付的源码的基本部分。所有改变应被记载和检查，以确保不危及系统的安全。通过技术、物理和保安规章三方面的结合，充分保护生成系统所用到的源码免遭未授权的修改和毁坏。在软件配置管理系统中，应包含以下方面的工具规程：

——从源码产生出系统新版本；

——鉴定新生成的系统版本；

——保护源码免遭未授权修改。

#### 5.4.3.2 分发和操作

应按照**《通用技术要求》6.4.5.2 条分发和操作**的要求，设计和实现数据库管理系统的 TCB 分发和操作。本安全级的具体要求为：

a) 应以文档形式提供对 TCB 安全地进行分发的过程，以及安装、生成和启动的过程进行说明，并最终生成安全的配置。文档中所描述的内容应包括：

——提供分发的过程；

——安全启动和操作的过程；

——建立日志的过程；

——修改检测的内容；

——对任何安全加强功能在启动、正常操作维护时能被撤消或修改的阐述；

——在故障或硬件、软件出错后恢复系统至安全状态的规程；

——对含有加强安全性的硬件部件，应说明用户或自动的诊断测试的操作环境和使用方法；

——所有诊断测试过程中，为加强安全性的硬件部件所提供例证的结果；

——在启动和操作时产生审计踪迹输出的例证。

b) 对系统的未授权修改的风险，应在交付时控制到最低限度。在包装及安全分送和安装过程中，这种控制应采取软件控制的方式，安全性由末端用户确认，所有安全机制都应以功能状态交付。

c) 所有软件应提供安全安装默认值，在客户不做选择时，默认值应使安全机制有效地发挥安全功能。

d) 随同系统交付的全部默认用户标识码，应在交付时处于非激活状态，并在使用前由管理员激活。

e) 用户文档应同交付的软件一起包装，并应有一套规程确保当前送给用户的软件是严格按照最新的版本制作的。

f) 以安全方式开发并交付系统后，仍应提供对产品的长期维护和评估的支持，包括产品中的安全漏洞和现场问题的解决。

g) 应以书面形式向用户通告新的全问题。

h) 可能受到威胁的所有的安全问题，均应描述其特点，并被作为主要的问题对待，直到它被解决或在用户同意下降级使用。

i) 为了支持已交付的软件的每个版本，对所有已有的安全漏洞都应有文档说明，并提交用户。

j) 安全漏洞应及时修改。安全功能的增加和改进应独立于系统版本的升级。

k) 没有用户授权，不应在正进行生产性运行的系统上实施新特性和简易原型的开发、测试和安装。

l) 新版本不应违反最初的安全策略和设想，应避免在维护、增加或功能升级中引入安全漏洞。所有功能的改变和安全结构设置的缺省默认值都应在文档中被记录。在新版本交付用户使用时，用户应能得到相应的文档。

#### 5.4.3.3 开发

应按照**《通用技术要求》6.4.5.3 条**开发的要求，进行数据库管理系统 TCB 的开发。本安全级的具体要求为：

a) 按**半形式化功能说明，半形式化高层设计、半形式化高层解释，TSF 的结构化实现，TSF 内部结构复杂性最小化，半形式化低层设计，半形式化一致性说明，以及半形式化的 TCB 安全策略模型**的要求，进行 TCB 的开发。

b) 系统的设计和开发应保护数据的完整性，例如，检查数据更新的规则，多重输入的正确处理，返回状态的检查，中间结果的检查，合理值输入检查，事务处理更新的正确性检查等。

c) 在内部代码检查时，应解决潜在的安全缺陷，关闭或取消所有的后门。

d) 有交付的软件和文档，应进行关于安全缺陷的定期的和书面的检查，并将检查结果告知用户。

e) 系统控制数据，如口令、密钥，不应在未受保护的程序或文档中以明文形式存储，应以书面形式提供给用户关于软件所有权法律保护的指南。

f) 在数据库管理系统开发的敏感阶段，应保持一个安全环境，该安全环境要求：

——描述数据库管理系统开发所使用的计算机系统的安全使用和维护情况的安全策略和措施应有书面记载，并可供检查；

——系统开发过程中使用的所有计算机系统应接受定期的和有书面记载的内部安全审计，描述审计过程的文件和真实的审计报告应可供检查；

——除授权的分发机构外，不应在开发环境外部复制或分发内部文档；

——开发环境的计算机系统使用的所有软件应当合法地从确定的渠道获得；

——开发者个人独自开发的软件，应在被开发管理者审核后才能用于开发的系统。

5.4.3.4 指导性文档

应按照**《通用技术要求》6.4.5.4 条指导性文档**的要求，编制 TCB 的指导性文档。本安全级的具体要求为：

a) 应为最终用户提供简单概要、分章节或手册形式的文档，保证用户拥有进行安全操作所需要的所有信息。与安全有关的信息应包含在一个特别的手册中或许多标准的文本集中，提供用户查阅所有的安全功能。这些信息可随系统发送，也可明确指出它包含在哪个文本当中。

b) 通过提供指导性文档，应把如何安全使用和维护数据库管理系统的信息交付给系统的用户、系统管理员和系统安全员。对文档的总体要求是：

——应对所有的安全访问和相关过程、特权、功能等适当的管理加以阐述；

——应阐述安全管理和安全服务的交互，并提供新的 TCB 安全生成的指导；

——应详细给出每种审计事件的审计记录的结构，以便考察和维护审计文件和进程；

——应提供一个准则集，用于保证附加的说明的一致性不受破坏。

c) 用户文档应提供关于不同用户的可见的安全机制以及如何利用它们的信息，描述没有明示用户的保护结构，并解释它们的用途和提供有关它们使用的指南。文档中不应包括那些如果公开将会危及系统安全的任何信息。

d) 系统管理员文档应提供关于系统的安全开机、操作和重新启动的信息，包括启动系统的过程（如引导系统进入安全方式）、在系统操作失误时恢复安全系统操作的过程、运行软件和数据备份及转储的方法和过程，还应提供一个单独的安装指南，详细说明设置系统的配置和初始化过程。

e) 安全管理员文档应提供有关如何设置、维护和分析系统安全的详细指导，包括当运行一个安全设备时，需要控制的有关功能和特权的警告，以及与安全有关的管理员功能的详细描述，包括增加和删除一个用户、改变主、客体的安全属性等。安全管理员文档应提供安全管理员了解如何用安全的方式管理系统，除了给出一般的安全忠告，还要明确：

——在系统用安全的方法设置时，围绕用户、用户账号、用户组成员关系、主体和客体的属性等，应如何安装或终止安装；

——在系统的生命周期内如何用安全的方法维护系统，包括为了防止系统被破坏而进行的每天、每周、每月的安全常规备份等；

——如何用安全的方法重建部分 TCB（如内核）的方法（如果允许在系统上重建 TCB）；

——说明审计跟踪机制，使授权用户可以有效地使用审计跟踪来执行本地的安全策略；

——必要时，如何调整系统的安全默认配置。

f) 文档中不应提供任何一旦泄露将会危及系统安全的信息。有关安全的指令和文档应划分等级分别提供给用户、系统管理员和系统安全员。这些文档应为独立的文档，或作为独立的章节插入到管理员指南和用户指南中。文档也可为硬拷贝、电子文档或联机文档。如果是联机文档应控制对其的访问。

g) 应提供关于所有审计工具的文档，包括为检查和保持审计文件所推荐的过程、针对每种审计事件的详细审计记录文件、为周期性备份和删除审计记录所推荐的过程等。

h) 应提供如何进行系统自我评估的章节（带有网络管理、口令要求、拨号访问控制、意外事故计划的安全报告）和为灾害恢复计划所做的建议，以及描述普通侵入技术和其它威胁，并查

出和阻止它们的方法。

5.4.3.5 生命周期支持

应按照**《通用技术要求》6.4.5.5 条生命周期支持**的要求，设计和实现数据库管理系统的 TCB。本安全级的具体要求为：

c) 按标准的生命周期模型进行开发，**提供充分的安全措施，应用部分的工具和技术应遵照实现标准。**

d) 文档应详细阐述安全启动和操作的过程，详细说明安全功能在启动、正常操作维护时是否能被撤消或修改，说明在故障或系统出错时如何恢复系统至安全状态。

d) 如果系统含有加强安全性的硬件，那么管理员、终端用户或自动的诊断测试，应能在各自的操作环境中运行它并详细说明操作过程。

5.4.3.6 测试

应按照**《通用技术要求》6.4.5.6 条测试**的要求，对数据库管理系统的 TCB 进行测试。本安全级的具体要求为：

a) 应通过一般功能测试和抽样性独立测试，**严格的测试范围分析**，高层设计测试、低层设计测试、实**现表示测试**，顺序的功能测试等，确认 TCB 的功能与所要求的功能相一致。

b) 所有系统的安全特性，应被全面测试。包括查找漏洞，如允许违反系统访问控制要求、允许违反资源访问控制要求、允许拒绝服务、允许多审计或验证数据进行未授权访问等。所有发现的漏洞应被改正、消除或使其无效，并在消除漏洞后重新测试，以证实它们已被消除，且没有引出新的漏洞。

c) 应提供测试文档，详细描述测试计划、测试过程、测试结果。

5.4.3.7 脆弱性评定

应按照《通用技术要求》6**.4.5.7 条脆弱性评定**所描述的要求对所开发的 TCB 进行脆弱性评定。本安全级的具体要求为：

a) 从**一般性的和/或系统化的隐蔽信道分析**，指南检查、分析确认、**对安全状态的检查和分析**，TCB 安全功能强度评估，开发者脆弱性分析、独立脆弱性分析、**中级抵抗力分析**等方面进行脆弱性评定。

5.4.4 TCB 安全管理要求

应按照**《通用技术要求》6.4.6 条 TCB 安全管理**所描述的要求，实现 TCB 的安全管理。本安全级的具体要求为：

a) 对相应的 TCB 的访问控制、鉴别控制、审计和安全属性管理等相关的功能，以及与一般的安装、配置和维护有关的功能，制定相应的操作、运行规程和行为规章制度。

b) 根据本级中安全功能技术要求所涉及的自主访问控制、标记、强制访问控制、身份鉴别、客体重用、审计、数据完整性、**隐蔽信道分析、可信路径**和安全保证技术要求所涉及的配置管理、分发和操作、开发、指导性文档、生命周期支持、测试、脆弱性评定等所涉及的有关内容设计 TCB 安全管理。

c) 将系统管理员、安全员和审计员等重要安全角色分别设置专人担任，并按“最小授权原则”分别授予他们各自为完成自身任务所需的最小权限，并形成相互制约的关系。

## 5.5 第五级：访问验证保护级

### 5.5.1 安全功能

#### 5.5.1.1 自主访问控制

应根据本标准 4.2.3 条访问操作、访问规则、和授权传播的描述，按照**《通用技术要求》6.5.3.3 条自主访问控制**所描述的要求设计访问控制功能。本安全级要求：

a) 将自主访问控制扩展到计算机信息系统的所有主体与客体，并且，要求自主访问控制的粒度达到更细的粒度。即，自主访问控制中的客体的最大控制单位应是记录、字段、元素等。

b) 用目录表访问控制、存取控制表访问控制、能力表访问控制等访问控制表访问控制确定主体对客体的访问权限。数据库管理系统中一般不直接采用稀疏的二维存取矩阵，而采用一些比较实用的技术，如：按行存储、按列存储、锁钥法、口令密码法等实现自主访问控制。

c) 无论采用何种访问控制策略实现访问控制功能，都应允许命名用户以用户和/或用户组的身份规定并控制对客体的共享，并阻止非授权用户读取信息。

d) 自主访问控制应与身份鉴别和审计相结合，通过确认用户身份的真实性和记录用户的各种成功的或不成功的访问，使用户对自己的行为承担明确的责任。

e) 应限制授权传播，要求对不可传播的授权进行明确定义提供支持，由系统自动检查并限制这些授权的传播。

#### 5.5.1.2 强制访问控制

应根据本标准 4.2.4 条的描述，按照**《通用技术要求》6.5.3.5 条强制访问控制**的要求，设计访问控制功能。本安全级应：

a) 将强制访问控制扩展到计算机信息系统的所有主体与客体，并且，强制访问控制的粒度达到更细的粒度，即客体的最大控制单位应是记录、字段或元素等。

b) 将系统的常规管理、与安全有关的管理以及审计管理，分别由系统管理员、系统安全员和系统审计远来承担，按最小授权原则分别授予它们各自为完成自己所承担任务所需的最小权限，并在三者之间形成相互制约的关系。

#### 5.5.1.3 标记

应根据本标准 4.2.1 条标记与安全属性管理和**《通用技术要求》6.5.3.4 条标记**的要求进行标记功能的设计。本安全级要求：

a) 数据库用户的安全属性，应在用户建立注册账号后由系统安全员通过 TCB 所提供的安全员界面操作进行标记，而客体的安全属性则在数据输入到由 TCB 安全功能所控制的范围内时以缺省方式生成或由安全员通过操作界面进行标记；

b) 将标记扩展到信息系统中的所有主体与客体，对于从 TCB 控制外导入到数据库系统中的未标记信息进行默认标记或由安全管理员进行标记。对于输出到 TCB 控制范围以外的数据，如打印输出的数据时，应明显的表示出该数据的安全标记。

#### 5.5.1.4 身份鉴别

a) 身份鉴别应包括用户标识和用户鉴别。

b) 用户标识应根据 4.1.1 条用户标识的描述，按照**《通用技术要求》6.5.3.1 条用户标识**的要求进行。

c) 用户鉴别应根据 4.1.2 条用户鉴别的描述，按照**《通用技术要求》6.5.3.2 条用户鉴别**的要求进行。

d) 进入数据库系统的用户，首先应由支持数据库系统运行的操作系统进行身份鉴别。

e) 应提供用户进入数据库管理系统时的身份鉴别，并按以下要求进行设计：

——凡需进入数据库管理系统的用户，可以选择采用该用户在操作系统中的标识信息，也可以重新进行用户标识。重新进行用户标识应在用户注册（建立账号）时进行。

——当用户登录到数据库管理系统或与数据库服务器进行访问连接时，应进行用户鉴别。

——数据库管理系统用户标识一般使用用户名和用户标识（UID）。为在整个数据库系统范围实现用户的唯一性，应确保数据库管理系统建立的用户在系统中的标识（SID）与在各数据库系统中的标识（用户名或别名，UID 等）之间的一致性。

——分布式数据库系统中，全局应用的用户标识信息和鉴别信息应存放在全局数据字典中，由全局数据库管理安全机制完成全局用户的身份鉴别。局部应用的用户标识信息和鉴别信息应存放于局部数据字典中，由局部数据库安全机制完成局部用户的身份鉴别。

——数据库用户的标识和鉴别信息应受到操作系统和数据库系统的双重保护。操作系统应确保任何用户不能通过数据库以外的使用方式获取和破坏数据库用户的标识和鉴别信息。数据库系统应保证用户以安全的方式和途径使用数据库系统的标识和鉴别信息。

——数据库用户标识信息应在数据库系统的整个生命期有效，被撤消的用户账号的 UID 不得再次使用。

——身份鉴别应采用高强度的安全机制，如 IC 卡信息、人体生物特征信息（指纹、视网膜）等特殊信息进行身份鉴别，或者采用更加完善的 CA 认证系统等。

——IC 卡信息身份鉴别应采用密码技术，以防伪造、复制，应定义鉴别尝试允许次数、尝试时间，定义鉴别失败后同一场地再次鉴别的时间间隔，定义鉴别失败处理的条件和动作，如审计、跟踪、警报、封锁账户（永久或有条件地恢复）、封锁场地（永久或有条件地恢复）等。

#### 5.5.1.5 客体重用

应根据本标准 4.5 条的要求，按照**《通用技术要求》6.5.3.6 条客体重用**的要求进行设计。本安全级要求：

a) 由数据库管理系统和支持数据库系统的操作系统共同保证信息不因资源的动态分配而遭泄露。如果操作系统支持客体安全重用功能，数据库管理系统仅需保证数据库系统中逻辑上被删除的信息是物理删除的或是不能再用的；如果操作系统不支持客体安全重用功能，数据库管理系统每次进行新资源分配时，应删除其中包含的残留信息。

b) 在释放存储重要信息的资源时，应采用特殊的方法对其残留的信息进行彻底清除，。

#### 5.5.1.6 审计

应按照本标准 4.4 条的要求和**《通用技术要求》6.5.2.4 条安全审计**的要求，设计审计功能。本安全级的要求：

a) 审计功能的设计应与用户标识与鉴别、自主访问控制、标记与强制访问控制等安全功能的设计紧密结合；

b) 对与标识及强制访问控制等安全机制有关的内容，如安全属性的操作等进行审计；

c) 对网络环境下运行的数据库管理系统，应建立分布式的审计系统，并以审计中心进行管理和控制。

#### 5.5.1.7 数据完整性

a) 应根据本标准 4.3.1 条实体完整性和参照完整性的描述，按照**《通用技术要求》6.5.3.7 条数据完整性**的要求设计实体完整性和参照完整性；

b) 应根据本标准 4.3.2 条用户定义完整性的描述，按照**《通用技术要求》6.5.3.7 条数据完整性**的要求设计用户定义完整性；

c) 应根据本标准 4.3.3 条完整性操作要求的描述，按照**《通用技术要求》6.5.3.7 条数据完整性**的要求设计数据完整性。

5.5.1.8 可信恢复

**应根据 4.6 条数据库可信恢复的描述和《通用技术要求》6.5.2.6 条备份与故障恢复中所描述的要求进行设计。**

5.5.1.9 隐蔽信道分析

系统开发者应根据实际测量和工程估算，分析系统中存在的隐蔽信道，并采取相应措施进行防范。本级要求按照本标准 5.7.1 条一般性隐蔽信道分析和**《通用技术要求》6.5.3.8 条隐蔽信道分析**的要求进行隐蔽信道分析。

5.5.1.10 可信路径

在对用户进行初始登录和鉴别时或在用户与 TCB 间进行数据传送时，应根据 4.8 条可信路径的描述的和**《通用技术要求》6.5.3.9 条可信路径**的要求进行可信路径的设计。

5.5.1.11 推理控制

应根据附录 A.8 所描述的推理方法、用于推理的信息以及防止推理的方法中对数据重新分级或对约束重新分级的方法实现推理控制。

5.5.2 TCB 自身安全保护

5.5.2.1 TSF 保护

应按照**《通用技术要求》6.5.4.1 条 TSF 保护**的要求，设计和实现数据库管理系统的 TSF 保护。本安全级中，数据库管理系统 TSF 保护的具体要求为：

a) 系统在设计时不应留有“后门”，即不应以维护、支持或操作需要为借口，设计有违反或绕过安全规则的任何类型的入口和文档中未说明的任何模式的入口。

b) 安全结构应是一个独立的、严格定义的软件系统子集，并应防止外部干扰和破坏，如修改其代码或数据结构；

c) 数据库管理系统应进行分层设计，并将数据库管理系统进程与和用户进程进行隔离；

d) 应提供设置和升级配置参数的安装机制，在初始化和对与安全有关的数据结构进行保护之前，应对用户和管理员的安全策略属性应进行定义；

e) 应区分普通操作模式和系统维护模式，TCB 的恢复、全系统操作恢复的启动、配置 TCB 内部的数据库和表等动作应在维护模式中执行。

f) 应防止普通用户从未经允许的系统进入维护模式，并防止普通用户与系统内维护模式交互,从而保证在普通用户访问系统之前，系统能以一个安全的方式进行安装和配置。

g) 当数据库管理系统安装完成后，在普通用户访问之前，系统应配置好初始用户和管理员职责、审计参数、系统审计跟踪设置以及对客体的合适的访问控制。

h) 执行系统所提供的实用程序，应限定于对系统的有效使用，只允许系统管理员修改或替换系统提供的实用程序。

i) 在 TCB 失败或中断后，进程应保证保护文本以最小的损害得到恢复。并按照失败保护中所描述的内容，实现对 TSF 出现失败时的处理。系统因故障或其它原因中断后，应有一种机制恢复系统。系统应提供在管理维护状态中运行的能力，管理维护状态只能被系统管理员使用，且各种安全功能全部失效。

j) 系统应能识别由通信渠道接收的信息的来源者，所有待确认的数据应能从进入点被安全地传送到确认系统，如口令不应由公共的或共享的网络以明文发送，可使用数据加密设备或通过加密信道用加密方式传送。

k) 系统应为系统管理员提供一种机制，来产生安全参数值的详细报告。

#### 5.5.2.2 资源利用

应按照**《通用技术要求》6.5.4.2 条资源利用**的要求，设计和实现数据库管理系统的资源利用。在本安全级中，资源利用设计的具体要求为：

a) 通过一定措施确保当系统出现某些确定的故障时，TSF 也能维持正常运行；

b) 采取适当的策略，按有限服务优先级提供主体使用 TSC 内某个资源子集的优先级，进行 TCB 资源的管理和分配；

c) 按资源分配中最大限额的要求，进行 TCB 资源的管理和分配，确保用户和主体不会独占某种受控资源。

d) 确保在被授权的主体发出请求时，资源能被访问和利用。

e) 当系统的服务水平降低到预先规定的最小值时，应能检测和发出报告。

f) 提供管理维护状态中运行的能力，在管理维护状态下各种安全性能全部失效，系统只允许由系统管理员使用。

g) 系统应提供软件及数据备份和复原的过程，在系统中应加入再启动的同步点，以便于系统的复原。

h) 数据库管理系统应能提供命名的或用户可访问的系统资源的修改历史记录。

i) 系统应提供能用于定期确认系统正确操作的机制和过程，包括对可能在全系统内传播的错误状态的检测以及超过规定门限的通讯差错的检测等。

#### 5.5.2.3 TCB 访问

应按照**《通用技术要求》6.5.4.3 条 TCB 访问控制**的要求，设计和实现数据库管理系统的 TCB 访问控制。本安全级中，数据库管理系统 TCB 访问控制设计的具体要求为：

a) 按可选属性范围限定最小级的要求，选择某种会话安全属性的所有失败的尝试 ，对建立会话的安全属性的范围进行限制；

b) 按多重并发会话限定中基本限定的要求，进行会话管理的设计。提供适用于 TSF 内所有用户的限制, 允许用户会话建立的所有尝试；

c) 按照 TCB 访问历史所描述的要求，在会话成功建立的基础上，TSF 应显示用户上一次成功/不成功的会话建立的日期，时间，方法，位置，以及从上一次成功的会话建立以来的不成功的尝试的次数。

d) 按照 TCB 会话建立所描述的要求，TSF 应根据属性允许或拒绝该次会话的建立，这些属性包括：访问地址或端口，用户安全属性（如用户身份、许可证等级、完整性等级），时间范围（如一天中的某些时间、一周的某些天、某些特定日期），或上述属性的组合。

e) 在会话建立之前，认证机制应对用户身份进行验证；

f) 成功登录系统后，TCB 应向用户显示的信息包括：

——日期、时间、来源和上次成功登录系统的情况；

——上次成功访问系统以来身份识别失败的情况；

——显示口令到期的天数、成功或不成功的事件次数等。

g) 在规定的未使用时限后，系统应根据提供所提供的期限默认值断开会话或重新认证用户。

h) 系统应提供锁定用户键盘的机制，键盘开锁过程应要求验证用户。

i) 当用户不正确的登录次数达到系统规定的次数时，系统应退出登录过程并终止与用户的交互。系统应提供门限默认值。当门限值被超过时，系统应立即通知系统管理员，同时系统可以指定一段停顿时间，在这段时间之后，才允许重新开始登录程序。系统应具有在连续的侵入尝试下，增加时间间隔的能力，从而延长系统被攻破的时间。

j) 系统应保证即使输入的用户标识是无效的，也应进行完整的用户验证过程，出错的反馈信息不应暴露哪一部分的验证信息是错误的。

k) 系统应提供一种机制，能按钟点、周日、年月日等条件规定哪些用户能进入系统，哪些用户不能进入系统。

l) 系统应提供一种机制，能按照进入方式或地点拒绝或接受用户。

m) 系统应提供一种机制，能限制用户在指定的网络地址或端口访问系统。例如，限制系统管理员只能通过系统控制台访问系统。

n) 系统应提供一种机制，限制指定的用户或用户组只能进行不修改的访问。

#### 5.5.3 TCB 设计和实现

##### 5.5.3.1 配置管理

应按照**《通用技术要求》6.5.5.1 条配置管理**的要求，设计和实现数据库管理系统 TCB 的配置管理。本安全级的具体要求为：

**a) 在配置管理自动化方面要求完全的配置管理自动化。**

b) 在配置管理能力方面应实现对版本号、配置项、授权控制、生成支持和验收过程及进一步的支持等方面的要求。

c) 配置管理范围方面，应将 TCB 的实现表示、设计文档、测试文档、用户文档、管理员文档以及配置管理文档等置于配置管理之下，要求实现对配置管理范围内的问题，特别是安全缺陷问题进行跟踪，还应包括开发工具配置管理。

d) 在系统的整个生存期，即在它的开发、测试和维护期间，应有一个软件配置管理系统处于保持对改变源码和文件的控制状态。只有被授权的代码和代码修改才允许被加进已交付的源码的基本部分。所有改变应被记载和检查，以确保不危及系统的安全。通过技术、物理和保安规章三方面的结合，充分保护生成系统所用到的源码免遭未授权的修改和毁坏。在软件配置管理系统中，应包含以下方面的工具规程：

——从源码产生出系统新版本；

——鉴定新生成的系统版本；

——保护源码免遭未授权修改。

##### 5.5.3.2 分发和操作

应按照**《通用技术要求》6.5.5.2 条分发和操作**的要求，设计和实现数据库管理系统的 TCB 分发和操作。本安全级的具体要求为：

a) 应以文档形式提供对 TCB 安全地进行分发的过程，以及安装、生成和启动的过程进行说明，并最终生成安全的配置。文档中所描述的内容应包括：

——提供分发的过程；

——安全启动和操作的过程；

——建立日志的过程；

——修改检测的内容；

——对任何安全加强功能在启动、正常操作维护时能被撤消或修改的阐述；

——在故障或硬件、软件出错后恢复系统至安全状态的规程；

——对含有加强安全性的硬件部件，应说明用户或自动的诊断测试的操作环境和使用方法；

——所有诊断测试过程中，为加强安全性的硬件部件所提供例证的结果；

——在启动和操作时产生审计踪迹输出的例证。

b) 对系统的未授权修改的风险，应在交付时控制到最低限度。在包装及安全分送和安装过程中，这种控制应采取软件控制的方式，安全性由末端用户确认，所有安全机制都应以功能状态交付。

c) 所有软件应提供安全安装默认值，在客户不做选择时，默认值应使安全机制有效地发挥安全功能。

d) 随同系统交付的全部默认用户标识码，应在交付时处于非激活状态，并在使用前由管理员激活。

e) 用户文档应同交付的软件一起包装，并应有一套规程确保当前送给用户的软件是严格按照最新的版本制作的。

f) 以安全方式开发并交付系统后，仍应提供对产品的长期维护和评估的支持，包括产品中的安全漏洞和现场问题的解决。

g) 应以书面形式向用户通告新的全问题。

h) 可能受到威胁的所有的安全问题，均应描述其特点，并被作为主要的问题对待，直到它被解决或在用户同意下降级使用。

i) 为了支持已交付的软件的每个版本，对所有已有的安全漏洞都应有文档说明，并提交用户。

j) 安全漏洞应及时修改。安全功能的增加和改进应独立于系统版本的升级。

k) 没有用户授权，不应在正进行生产性运行的系统上实施新特性和简易原型的开发、测试和安装。

l) 新版本不应违反最初的安全策略和设想，应避免在维护、增加或功能升级中引入安全漏洞。所有功能的改变和安全结构设置的缺省默认值都应在文档中被记录。在新版本交付用户使用时，用户应能得到相应的文档。

#### 5.5.3.3 开发

应按照**《通用技术要求》6.4.5.3 条**开发的要求，进行数据库管理系统 TCB 的开发。本安全级的具体要求为：

a) 按**形式化功能说明，形式化高层设计，**TSF 的结构化实现，TSF 内部结构复杂性最小化，**形式化低层设计，形式化一致性说明，以及形式化的 TCB 安全策略模型**的要求，进行 TCB 的开发。

b) 系统的设计和开发应保护数据的完整性，例如，检查数据更新的规则，多重输入的正确处理，返回状态的检查，中间结果的检查，合理值输入检查，事务处理更新的正确性检查等。

c) 在内部代码检查时，应解决潜在的安全缺陷，关闭或取消所有的后门。

d) 有交付的软件和文档，应进行关于安全缺陷的定期的和书面的检查，并将检查结果告知用户。

e) 系统控制数据，如口令、密钥，不应在未受保护的程序或文档中以明文形式存储，应以书面形式提供给用户关于软件所有权法律保护的指南。

f) 在数据库管理系统开发的敏感阶段，应保持一个安全环境，该安全环境要求：

——描述数据库管理系统开发所使用的计算机系统的安全使用和维护情况的安全策略和措施应有书面记载，并可供检查；

——系统开发过程中使用的所有计算机系统应接受定期的和有书面记载的内部安全审计，描述审计过程的文件和真实的审计报告应可供检查；

——除授权的分发机构外，不应在开发环境外部复制或分发内部文档；

——开发环境的计算机系统使用的所有软件应当合法地从确定的渠道获得；

——开发者个人独自开发的软件，应在被开发管理者审核后才能用于开发的系统。

5.5.3.4 指导性文档

应按照**《通用技术要求》6.5.5.4 条指导性文档**的要求，编制 TCB 的指导性文档。本安全级的具体要求为：

a) 应为最终用户提供简单概要、分章节或手册形式的文档，保证用户拥有进行安全操作所需要的所有信息。与安全有关的信息应包含在一个特别的手册中或许多标准的文本集中，提供用户查阅所有的安全功能。这些信息可随系统发送，也可明确指出它包含在哪个文本当中。

b) 通过提供指导性文档，应把如何安全使用和维护数据库管理系统的信息交付给系统的用户、系统管理员和系统安全员。对文档的总体要求是：

——应对所有的安全访问和相关过程、特权、功能等适当的管理加以阐述；

——应阐述安全管理和安全服务的交互，并提供新的 TCB 安全生成的指导；

——应详细给出每种审计事件的审计记录的结构，以便考察和维护审计文件和进程；

——应提供一个准则集，用于保证附加的说明的一致性不受破坏。

c) 用户文档应提供关于不同用户的可见的安全机制以及如何利用它们的信息，描述没有明示用户的保护结构，并解释它们的用途和提供有关它们使用的指南。文档中不应包括那些如果公开将会危及系统安全的任何信息。

d) 系统管理员文档应提供关于系统的安全开机、操作和重新启动的信息，包括启动系统的过程（如引导系统进入安全方式）、在系统操作失误时恢复安全系统操作的过程、运行软件和数据备份及转储的方法和过程，还应提供一个单独的安装指南，详细说明设置系统的配置和初始化过程。

e) 安全管理员文档应提供有关如何设置、维护和分析系统安全的详细指导，包括当运行一个安全设备时，需要控制的有关功能和特权的警告，以及与安全有关的管理员功能的详细描述，包括增加和删除一个用户、改变主、客体的安全属性等。安全管理员文档应提供安全管理员了解如何用安全的方式管理系统，除了给出一般的安全忠告，还要明确：

——在系统用安全的方法设置时，围绕用户、用户账号、用户组成员关系、主体和客体的属性等，应如何安装或终止安装；

——在系统的生命周期内如何用安全的方法维护系统，包括为了防止系统被破坏而进行的每天、每周、每月的安全常规备份等；

——如何用安全的方法重建部分 TCB（如内核）的方法（如果允许在系统上重建 TCB）；

——说明审计跟踪机制，使授权用户可以有效地使用审计跟踪来执行本地的安全策略；

——必要时，如何调整系统的安全默认配置。

f) 文档中不应提供任何一旦泄露将会危及系统安全的信息。有关安全的指令和文档应划分等级分别提供给用户、系统管理员和系统安全员。这些文档应为独立的文档，或作为独立的章节插入到管理员指南和用户指南中。文档也可为硬拷贝、电子文档或联机文档。如果是联机文档应控制对其的访问。

g) 应提供关于所有审计工具的文档，包括为检查和保持审计文件所推荐的过程、针对每种审计

事件的详细审计记录文件、为周期性备份和删除审计记录所推荐的过程等。

h) 应提供如何进行系统自我评估的章节（带有网络管理、口令要求、拨号访问控制、意外事故计划的安全报告）和为灾害恢复计划所做的建议，以及描述普通侵入技术和其它威胁，并查出和阻止它们的方法。

#### 5.5.3.5 生命周期支持

应按照**《通用技术要求》6.4.5.5 条生命周期支持**的要求，设计和实现数据库管理系统的 TCB。本安全级的具体要求为：

a) 应按**可测量的生命周期模型**进行开发，提供充分的安全措施，**所有部分的工具和技术应遵照实现标准。**

b) 文档应详细阐述安全启动和操作的过程，详细说明安全功能在启动、正常操作维护时是否能被撤消或修改，说明在故障或系统出错时如何恢复系统至安全状态。

c) 如果系统含有加强安全性的硬件，那么管理员、终端用户或自动的诊断测试，应能在各自的操作环境中运行它并详细说明操作过程。

#### 5.5.3.6 测试

应按照**《通用技术要求》6.5.5.6 条测试**的要求，对数据库管理系统的 TCB 进行测试。本安全级的具体要求为：

a) 应通过一般功能测试和**完全性独立测试**，严格的测试范围分析，高层设计测试、低层设计测试、实现表示测试，顺序的功能测试等，确认 TCB 的功能与所要求的功能相一致。

b) 所有系统的安全特性，应被全面测试。包括查找漏洞，如允许违反系统访问控制要求、允许违反资源访问控制要求、允许拒绝服务、允许多审计或验证数据进行未授权访问等。所有发现的漏洞应被改正、消除或使其无效，并在消除漏洞后重新测试，以证实它们已被消除，且没有引出新的漏洞。

c) 应提供测试文档，详细描述测试计划、测试过程、测试结果。

#### 5.5.3.7 脆弱性评定

应按照《通用技术要求》6**.5.5.7 条脆弱性评定**所描述的要求对所开发的 TCB 进行脆弱性评定。本安全级的具体要求为：

a) 从**彻底的隐蔽信道分析**，指南检查、分析确认、对安全状态的检查和分析，TCB 安全功能强度评估，开发者脆弱性分析、独立脆弱性分析、**高级抵抗力分析**等方面进行脆弱性评定。

### 5.5.4 TCB 安全管理

应按照**《通用技术要求》6.5.6 条 TCB 安全管理**所描述的要求，实现 TCB 的安全管理。本安全级的具体要求为：

a) 对相应的 TCB 的访问控制、鉴别控制、审计和安全属性管理等相关的功能，以及与一般的安装、配置和维护有关的功能，制定相应的操作、运行规程和行为规章制度。

b) 根据本级中安全功能技术要求所涉及的自主访问控制、标记、强制访问控制、身份鉴别、客体重用、审计、数据完整性、隐蔽信道分析、可信路径、**可信恢复**和安全保证技术要求所涉及的配置管理、分发和操作、开发、指导性文档、生命周期支持、测试、脆弱性评定等所涉及的有关内容设计 TCB 安全管理。

c) 将系统管理员、安全员和审计员等重要安全角色分别设置专人担任，并按“最小授权原则”分别授予他们各自为完成自身任务所需的最小权限，并形成相互制约的关系。

# 附 录 A

（说明性附录）

## 标准概念说明

### A.1 组成与相互关系

一个安全的数据库管理系统，无论其安全等级达到《准则》所规定的哪一个级，都应从安全功能和安全保证两方面考虑其安全性。安全功能主要说明数据库管理系统所实现的安全策略和安全机制符合《准则》中哪一级的要求，安全保证则是通过一定的方法保证数据库管理系统所提供的安全功能确实达到了确定的功能要求。本标准描述数据库管理系统的每一安全级所应达到的安全功能要求和安全保证要求。

图 A-1 给出本标准的主要组成成分与相互关系。

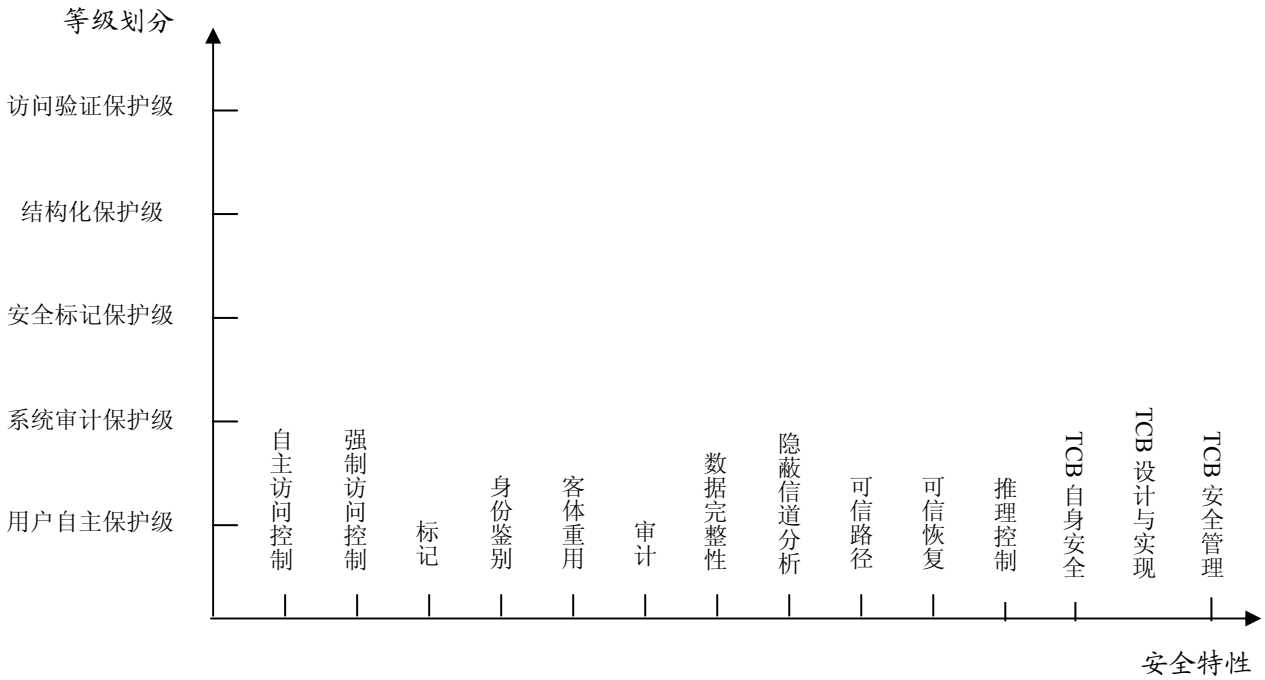


图 A-1 《数据库管理系统技术要求》的组成与相互关系

### A.2 数据库管理系统安全的特殊要求

数据库管理系统（DBMS）是指对对以库结构形式存储在计算机系统中的数据进行管理的人机系统。安全的数据库管理系统需要有相应的安全硬件、安全操作系统来支持，并在硬件、软件和人员管理方面有自身的特殊要求。

硬件方面，由于数据库存放大量数据，DBMS 自身体积大，因此对硬件资源提出了较高要求，主要是：

——应有足够大的内存用来运行操作系统、DBMS 核心模块和应用程序及作为数据缓冲区；

——应有大容量的直接存取存储设备和用作数据备份的存储介质（如磁带等）；

——应有较高的数据传输能力，应尽量降低因安全策略（如加密传输、事务管理）的实施带来的

附加开销，保证系统的可用性；

——实现某些安全功能（如数据加密/解密）可能需要附加硬件，及对附加硬件的管理。

软件方面，包括 DBMS、支持 DBMS 运行的操作系统及其接口的安全与数据库管理系统的安全密切相关，应为数据库管理系统提供安全的支持。

人员管理方面，数据库管理系统应有专门的安全管理机构和人员设置，包括：数据库系统管理员、数据库系统安全员、数据库系统审计员。

### A.3 数据库管理系统的用户管理

数据库管理系统的用户管理具有以下特点：

——拥有大量用户，且用户具有不同身份，享有不同权限；

——需要对特权用户，如数据库管理系统管理员、安全管理员、审计员进行严格管理；

——一个数据库系统可以包含多个数据库，一个用户可以同时使用多个数据库。同一用户可以通过“假名”对应于多个数据库用户名。

### A.4 数据库管理系统的安全性

数据库管理系统的安全性主要体现在：

——保密性：保护存储在数据库中的数据不被泄露和未授权的获取；

——完整性：保护存储在数据库中的数据不被破坏和删除；

——一致性：确保存储在数据库中的数据满足实体完整性、参照完整性和用户定义完整性要求；

——可用性：确保存储在数据库中的数据不因人为的和自然的原因对授权用户不可用。

### A.5 数据库管理系统安全等级的划分

这里所讨论的数据库管理系统，主要是指多用户系统。对于单处理机环境的数据库管理系统，安全等级的划分相对简单，而对于多处理机环境的数据库管理系统，由于其组成成分具有相对的独立性，并且这些数据库管理系统运行于网络环境，因而在考虑对其进行安全等级划分时，应首先考虑各组成成分的安全等级划分，并充分考虑网络传输中的安全因素，然后，综合考虑整个数据库管理系统的安全等级。其基本原则是：以各组成成分的安全等级应不低于整体系统的安全等级。数据库管理系统一般是在操作系统的支持下运行的。支持数据库管理系统运行的操作系统的安全等级也应不低于数据库管理系统的安全等级。

### A.6 关于数据库管理系统中的主体与客体

在一个数据库管理系统中，每一个实体成分都必须或者是主体，或者是客体，或者既是主体又是客体。

系统中最基本的主体应该是用户（包括一般用户和系统管理员、系统安全员、系统审计员等特殊用户）。每个进入系统的用户必须是唯一标识的，并经过鉴别确定为真实的。系统中的所有事件要求，几乎全是由用户激发的。进程是系统中最活跃的实体，用户的所有事件要求都要通过 DBMS 进程的运行来处理。进程作为用户的客体，同时又是其访问对象的主体。

在数据库系统中，客体可以是按照一定格式存储在一定记录介质上的数据信息（通常以数据库的库结构格式存储数据），也可以是数据库系统中的进程，而最终的客体是一定记录介质上的数据信息。从用户到进程，再到数据信息，构成一个服务链。服务者是要求者的客体，要求者是服务者的主体。按照不同安全等级的不同要求，数据库客体的粒度可以是整个库，也可以是表、视图、存储过程等，还可以是表中的一个记录、字段或元素等等。

### A.7 关于数据库管理系统中的TCB、TSF和TSP

在一个通用数据管理库系统中，TCB 是所有安全保护装置的组合体。一个 TCB 可以包含多个安全

功能模块（TSF）,每一个 TSF 实现一个安全功能策略（TSP），这些 TSP 共同构成一个安全域，以防止不可信主体的干扰和篡改。实现 TSF 有两种方法，一种是设置前端过滤器，另一种是设置访问监督器。两者都是在一定硬件和操作系统基础上，通过软件实现确定的安全策略和提供所要求的附加服务。比如，作为前端过滤器的 TSF，能防止非法进入系统，作为访问监督器的 TSF，能防止越权访问。

对于网络环境下的多处理机环境的数据库系统，一个 TSF 可能跨网络实现。这些 TSF 协同工作，构成一个物理上分散、逻辑上统一的分布式安全系统。其所提供的安全策略和附加服务则为各个 TSF 的总和。

### A.8 关于推理控制

推理是自然界和人类社会中普遍存在的现象。由于关系数据库中元组、属性、元素之间的相互关联性，推理问题成为数据库安全的重要内容。运用推理方法获取权限以外的数据库信息，是一种较为隐蔽的信息攻击方法。在具有较高安全级别要求的数据库系统中，应考虑对这种攻击的防御。

数据库安全中推理的特定含义为：用户根据较低安全级别的、可见的数据推出同级或较高安全级别的不可见信息。由于人类用以进行推理的信息千差万别，用推理获取新信息的方式也极为不同，所以要防止未授权的推理是非常复杂的，也不可能给出通用的解决方案。这里，仅对推理方法、用于推理的信息和防止推理的方法做简单描述。

a） 推理方法

推理方法的多种多样是造成推理问题复杂的首要因素。可用的推理方法有：

——演绎推理；

——归纳推理；

——类似推理，例如，“X 象 Y”；当给定 Y 的性质时，就推理出了 X 的性质；

——经验推理；

——语义联系推理，从实体自身的知识推理出实体间的联系；

——存在性推理，从某些信息可推理出实体的存在，例如，由信息“U 属于人事部”，可推理出“有一个称为 U 的实体”；

——统计推理，对一群实体进行不同的统计性研究（均值、中值、总和、计数等等）可以得到关于个体的信息。

b） 用于推理的信息

推理信息的广泛性是造成推理问题复杂的另一因素。可用于推理的信息类型有：

——模式元数据，包括关系名和属性名；

——其它元数据，例如，值约束、由触发器/过程实现的其它约束；

——关系中的数据，即数据的值；

——统计数据；

——派生数据；

——数据的存在性；

——数据的改变或消失（如安全级别上升）；

——未存于数据库中，但在应用域已知的数据语义；

——未存于数据库中，关于应用域（进程和数据）的专门信息；

——普通知识和普通常识。

c） 防止推理的方法

如果要防止所有的未授权泄露，应遵循多级数据库的基本安全原则：一个数据项的安全类级

别应支配所有施加影响于该数据项的安全类级别。即：给定数据项 X、Y，若 X 影响 Y，则 X 的安全类级别应受 Y 的安全类级别支配。

虽然有许多这样的推理问题可以通过仔细地考虑数据项的安全类级别的设置而防止，但是，预测或检测所有的推理问题是很难的。比较可行的办法是：

——对数据重新分级；

——对约束重新分级。

### A.9 关于密码技术和数据库加密

密码技术已成为当今计算机信息系统安全保护的关键技术，在较高安全等级保护中所采用的安全策略，必须以密码技术作为构成信息安全保护的重要机制，或将密码技术与系统安全技术相结合，组成统一的安全机制。数据库管理系统中密码技术的主要应用领域包括关键信息的存储加密保护和传输加密保护，以及以 PKI 为基础的 CA 认证系统实现对用户身份和设备的真实性的认证。各个安全等级密码技术的具体配置由国家密码主管部门决定。

### A.10 关于安全数据库管理系统的开发方法

开发一个安全的数据库管理系统可以有两种途径。一种是从头设计；另一种是对原有系统进行加固。

从头设计是指开发一个完整的新系统。这时，需要将数据库管理系统的功能与所需要的安全功能一起考虑，在实现数据库管理系统功能的同时构建安全的数据库管理系统。用这种途径所实现的系统核心部分往往就是一个按安全功能要求实现的 TCB，当然应包括所需要的数据库管理系统功能。随着数据库管理系统功能的扩展，TCB 的安全功能的控制范围随之扩展，直到数据库管理系统功能全部实现。

对原有数据库管理系统进行加固，是当前常见的增强通用数据库管理系统安全性的方法。这种方法往往只能采用增加外部安全控制模块来实现前端过虑器或访问监督器，其所能实现的安全功能会受到某些限制。比如，要用加固的方法实现一个结构化的 TCB 设计是十分困难的。因此，采用对已有系统进行加固的方法，目前所能达到的安全等级保护一般最高为第三级。

# 参　考　文　献

1. ISO/IEC 15408-1：1999 Information technology—Security techniques—Evaluation Criteria for IT Security Part1:Introduction and general model Part 1:Introduction and general model，Version 2.0

2. ISO/IEC 15408-2：1999 Information technology—Security techniques—Evaluation Criteria for IT Security Part2:Security functional requirements Part2:Security functional requirements，Version 2.0

3. ISO/IEC 15408-3：1999 Information technology—Security techniques—Evaluation Criteria for IT Security Part3:Security assurance requirements Part3:Security assurance requirements，Version 2.0

4. SQL-3 参考大全，Peter Gulutzan、Trudy Pelzer 著，齐舒创作室译，毅鸣校，机械工业出版社，2000.1