ICS 35.020
L 09

中华人民共和国国家标准

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—
Data base management systems security evaluation criteria

2005-11-11 发布　　2006-05-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　次

前　言

GB 17859—1999《计算机信息系统安全保护等级划分准则》是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工作的正常有序开展，特制定一系列相关的标准。本标准是系列标准之一。

本标准文本中，黑体字表示较低等级中没有出现或增强的评估内容。

本标准的附录A中说明数据库管理系统面临的主要威胁和对策。

本标准的附录A是资料性附录。

本标准由全国信息安全标准化技术委员会提出并归口。

本标准起草单位：北京大学软件工程国家工程中心、东软股份有限公司、公安部公共信息网络安全监察局。

本标准主要起草人：王立福，赵学志，程万军，刘学洋，葛佳。

引　言

数据库管理系统是为数据库的建立、使用和维护而配置的软件。它建立在操作系统的基础上，对数据库进行统一的管理和控制。用户使用的各种数据库命令以及应用程序的执行，都要通过数据库管理系统。数据库管理系统还提供对数据库的维护支持，按照系统管理人员的规定要求，保证数据库的安全性。

数据库管理系统可以帮助不同用户共享一个公共数据集合的软件系统并维护各数据项之间语义上的关联。

数据库管理系统负责在用户应用中存储、格式化、维护和管理用户数据。数据库管理系统通过其内在的功能，以适当的结构来存储数据并通过维护机制来维护这些数据的逻辑关系和完整性，为应用提供一致、完整、安全、可靠的服务。

标准分享网 www.bzfxw.com 免费下载

信息安全技术
数据库管理系统安全评估准则

1 范围

本标准从信息技术方面规定了按照 GB 17859—1999 的五个安全保护等级对数据库管理系统安全保护等级划分所需要的评估内容。

本标准适用于数据库管理系统的安全保护等级的评估，对于数据库管理系统安全功能的研制、开发和测试亦可参照使用。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

GB 17859—1999 计算机信息系统安全保护等级划分准则

GB/T 18336.1—2001 信息技术 安全技术 信息技术安全性评估准则 第1部分：简介和一般模型(idt ISO/IEC 15408-1:1999)

3 术语和定义

GB 17859—1999 和 GB/T 18336.1—2001 确立的术语和定义适用于本标准。

4 安全环境

4.1 物理方面

数据库管理系统所处的物理环境是安全的。对数据库管理系统资源的处理限定在一些可控制的访问设备内，防止未授权的物理访问。所有有关安全策略实施的系统硬件和软件受到保护以免于未授权的物理修改。

4.2 人员方面

有一个或多个能胜任的授权用户来管理数据库管理系统和它所包含信息的安全。管理员应经过一定培训，以便能正确有效地建立和维护安全策略。被授权的管理员能严格遵从系统管理员文档的要求进行操作，不会蓄意破坏数据库管理系统，不会蓄意违反操作规程。授权用户具备必要的授权来访问由数据库管理系统管理的最少量的信息。

4.3 连通性方面

数据库管理系统在系统管理员的配置下正常运行，用户可以通过网络远程访问和使用数据库管理系统。授权用户可以获得他们希望得到的适当服务。

5 评估内容

5.1 用户自主保护级

5.1.1 自主访问控制

数据库管理系统安全功能定义和控制系统中命名用户对命名客体的访问。自主访问控制的实施机制允许用户指定和控制客体的共享，并具备限制访问权限扩散的控制能力。自主访问控制机制根据用

户指定或默认的方式，阻止未授权用户对客体访问。对于每个命名客体，自主访问控制机制提供授权访问和不授权访问的访问控制表。只允许授权用户将访问许可授予未拥有某客体访问权限的用户。

数据库管理系统的安全功能应实施安全机制(如：利用访问控制表)，控制用户对客体的访问。

5.1.2 身份鉴别

5.1.2.1 用户属性定义

数据库管理系统安全功能应给出每个用户与标识相关的安全属性，如：标识符、组等。如果数据库管理系统安全功能维护自己的标识与鉴别数据，那么它应保证每个用户个体在数据库管理系统和其他系统安全功能中的信息相一致。

5.1.2.2 用户标识

数据库管理系统的安全功能应预先设定数据库管理系统代表用户执行的、与安全功能相关的动作，在标识之前，安全功能允许数据库管理系统执行这些预设动作。在其他的安全功能引起的操作动作之前，数据库管理系统的安全功能应成功地标识每个用户。

5.1.2.3 用户鉴别

数据库管理系统的安全功能应预先设定数据库管理系统代表用户执行的、与安全功能相关的动作，在用户被鉴别之前，允许数据库管理系统执行这些预设动作。在其他的安全功能引起的操作动作之前，数据库管理系统的安全功能应成功地鉴别每个用户。

5.1.2.4 鉴别失败处理

数据库管理系统的安全功能应检测到与鉴别事件相关的不成功的鉴别尝试，当不成功鉴别尝试的次数达到或超过了定义的界限时，安全功能应终止会话建立的进程。

5.1.2.5 访问历史

在会话成功建立的基础上，数据库管理系统的安全功能应显示用户上一次成功会话建立的日期、时间、方法、位置等。

5.1.3 数据完整性

数据库管理系统的安全功能允许在规定的客体上执行特定操作的回退。

5.1.4 数据传输

5.1.4.1 内部传输

在数据库管理系统物理分隔的各部分之间传递用户数据时，数据库管理系统的安全功能应执行特定的安全功能策略。

5.1.4.2 数据外部输出

向数据库管理系统安全功能控制范围之外输出用户数据时，数据库管理系统安全功能应在访问控制机制允许的前提下，执行特定的安全功能策略，进行用户数据输出。

5.1.4.3 数据外部输入

当用户数据从数据库管理系统安全功能控制范围之外输入时，数据库管理系统的安全功能应执行特定的安全功能策略。

5.1.5 资源利用

数据库管理系统的安全功能应限制属于同一用户的并发会话的最大数目。

5.1.6 安全功能保护

5.1.6.1 时间戳

数据库管理系统的安全功能应为自身的应用提供可靠的时间戳。

5.1.6.2 安全功能数据传输

在数据库管理系统的分离部分间传输安全功能数据时，数据库管理系统的安全功能应保护安全功能数据不被泄露或修改。当依靠其他系统的安全功能实现安全传输时，应提供其他系统的数据传输保护功能的可信性证据。

标准分享网 www.bzfxw.com 免费下载

5.1.7 安全管理

5.1.7.1 功能管理

数据库管理系统的安全功能应限制管理员对安全功能的启动、关闭和修改的能力。

5.1.7.2 属性管理

数据库管理系统的安全功能应依据访问控制策略，限制授权管理员查询、修改或删除安全属性的能力。

5.1.7.3 安全功能数据管理

数据库管理系统的安全功能应限制管理员查询、修改或删除安全功能数据的能力，仅允许授权管理员管理这些数据。

5.1.8 配置管理

开发者提供的配置管理文档应以版本号做标签，为数据库管理系统提供引用，使一个版本号对应数据库管理系统的唯一版本。

5.1.9 安全功能开发过程

开发者提供的数据库管理系统安全功能的功能规约应描述安全功能及其与外部的接口。

5.1.10 测试

5.1.10.1 功能测试

开发者提供的测试文档应包含测试计划、测试过程描述、预期的测试结果和实际测试结果，其中的测试计划应标识要测试的安全功能、描述要执行的测试目标，测试过程描述应标识要执行的测试、测试概况。

5.1.10.2 覆盖分析

开发者提供的测试覆盖的证据应表明测试文档中所标识的测试和功能规约中所描述的安全功能之间的对应性。

5.1.11 指导性文档

5.1.11.1 管理员指南

开发者提供的管理员指南应描述对于授权安全管理角色可使用的管理功能和接口、安全管理数据库管理系统的方式、受控制的安全参数以及与安全操作有关的用户行为的假设，并描述与为评估而提供的其他所有文件的一致性。

5.1.11.2 用户指南

开发者提供的用户指南，应描述用户可获取的安全功能和接口的用法以及安全操作中用户的职责（包括：用户行为假设）。同时，应描述与为评估而提供的其他所有文件的一致性。

5.1.12 交付和运行

开发者提供的安装过程的文档应说明用于数据库管理系统的安全安装、生成和启动的过程所必需的步骤。并应描述一个启动程序，它包含了用以生成数据库管理系统的选项，从而能决定数据库管理系统是如何以及何时产生的。

5.2 系统审计保护级

5.2.1 自主访问控制

数据库管理系统安全功能定义和控制系统中命名用户对命名客体的访问。自主访问控制的实施机制允许用户指定和控制客体的共享，并具备限制访问权限扩散的控制能力。自主访问控制机制根据用户指定或默认的方式，阻止未授权用户对客体访问。对于每个命名客体，自主访问控制机制提供授权访问和不授权访问的访问控制表。只允许授权用户将访问许可授予未拥有某客体访问权限的用户。

数据库管理系统的安全功能应实施安全机制（如：利用访问控制表），控制用户对客体的访问。

5.2.2 身份鉴别

5.2.2.1 用户属性定义

数据库管理系统安全功能应给出每个用户与标识相关的安全属性，如：标识符、组等。如果数据库管理系统安全功能维护自己的标识与鉴别数据，那么它应保证每个用户个体在数据库管理系统和其他系统安全功能中的信息相一致。

5.2.2.2 用户标识

数据库管理系统的安全功能应预先设定数据库管理系统代表用户执行的、与安全功能相关的动作，在标识之前，安全功能允许数据库管理系统执行这些预设动作。在其他的安全功能引起的操作动作之前，数据库管理系统的安全功能要成功地标识每个用户。

5.2.2.3 用户鉴别

数据库管理系统的安全功能应预先设定数据库管理系统代表用户执行的、与安全功能相关的动作，在用户被鉴别之前，允许数据库管理系统执行这些预设动作。在其他的安全功能引起的操作动作之前，数据库管理系统的安全功能应成功地鉴别每个用户。

当进行鉴别时，数据库管理系统的安全功能应仅仅将最少的反馈（如：打入的字符数，鉴别的成功或失败）提供给用户。

5.2.2.4 鉴别失败处理

数据库管理系统的安全功能应能检测到与鉴别事件相关的不成功的鉴别尝试，当不成功鉴别尝试的次数达到或超过了定义的界限时，安全功能应能终止会话建立的进程。

5.2.2.5 访问历史

在会话成功建立的基础上，数据库管理系统的安全功能应显示用户上一次成功会话建立的日期、时间、方法、位置等。

数据库管理系统的安全功能应显示用户上一次不成功的会话尝试的日期、时间、方法、位置等，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。

5.2.3 客体重用

对于数据库管理系统中的所有客体，在指定、分配或再分配给一个主体时，数据库管理系统的安全功能应确保其中没有上一次分配的剩余信息，当依赖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，应提供该客体重用功能的可信性的证据。

5.2.4 审计

5.2.4.1 内容

数据库管理系统的安全功能应能为可审计事件（如：使用客体创建、用户鉴别、客体删除、安全属性变更等）生成一个审计记录，并在每一个审计记录中至少记录以下信息：

——事件发生的日期和时间；

——事件的类型；

——主体身份、客体身份和事件的结果（成功或失败）。

数据库管理系统的安全功能应能维护数据库管理系统的可审计事件，但其中至少包括：

——标识和鉴别机制的使用；

——由用户启动的独立操作（如：创建、删除、更新、检索、插入等）；

——数据库管理员执行的动作；

——访问仲裁机制的使用。

5.2.4.2 查阅

数据库管理系统的安全功能应提供给授权用户从审计记录中读取一定类型的审计信息的能力，其审计记录可被其他系统的安全功能所处理。

5.2.4.3 存储保护

数据库管理系统的安全功能应保护已存储的审计记录，避免未授权的删除，并监测对审计记录的修改，当审计存储已满、失败或受到攻击时，应确保审计记录保持一定的记录数和维持的时间。

标准分享网 www.bzfxw.com 免费下载

5.2.4.4 自动响应

当检测到可能的安全侵害时，数据库管理系统的安全功能应做出响应，如：通知审计管理员，向授权用户提供一组遏制侵害的或采取校正的行动。

5.2.5 数据完整性

5.2.5.1 回退

数据库管理系统的安全功能允许在规定的客体上执行特定操作的回退。

5.2.5.2 完整性监视

对于具有特定用户数据属性的客体，数据库管理系统的安全功能应监视所存储的用户数据是否出现破坏完整性的错误。

5.2.6 数据传输

5.2.6.1 内部传输

在数据库管理系统物理分隔的各部分之间传递用户数据时，数据库管理系统的安全功能应执行特定的安全功能策略。

5.2.6.2 数据外部输出

向数据库管理系统安全功能控制范围之外输出用户数据时，数据库管理系统安全功能应在访问控制机制允许的前提下，执行特定的安全功能策略，进行用户数据输出。

向数据库管理系统安全功能控制范围之外输出与用户数据相关的安全属性时，数据库管理系统安全功能应确保安全属性与输出的用户数据相关。

5.2.6.3 数据外部输入

当用户数据从数据库管理系统安全功能控制范围之外输入时，数据库管理系统的安全功能应执行特定的安全功能策略。

数据库管理系统的安全功能应使用与输入的数据相关的安全属性，确保在安全属性和接受的用户数据之间提供了明确的关联。

5.2.6.4 原发证明

数据库管理系统的安全功能应能对发出的信息产生原发证据。

5.2.6.5 接收证明

数据库管理系统的安全功能应能对接收的信息产生接收证据。

5.2.7 资源利用

5.2.7.1 容错

数据库管理系统的安全功能能检测出已规定的数据库管理系统故障。

5.2.7.2 并发会话

数据库管理系统的安全功能应限制属于同一用户的并发会话的最大数目。

5.2.8 安全功能保护

5.2.8.1 安全功能自检

数据库管理系统的安全功能应在数据库管理系统的特定状态（如：启动时，应授权用户要求）中，检查安全功能的正确执行。

5.2.8.2 时间戳

数据库管理系统的安全功能应为自身的应用提供可靠的时间戳。

5.2.8.3 数据一致性

数据库管理系统的安全功能应确保数据库管理系统各部分间的安全功能数据的一致性。

5.2.8.4 安全功能数据传输

在数据库管理系统的分离部分间传输安全功能数据时，数据库管理系统的安全功能应保护安全功能数据不被泄露或修改。当依靠其他系统的安全功能实现安全传输时，应提供其他系统的数据传输保

护功能的可信性证据。

数据库管理系统的安全功能应分离传送安全功能数据和用户数据。

5.2.8.5 **系统恢复**

当数据库管理系统发生失败或服务中断后，数据库管理系统的安全功能应进入维护方式，将数据库管理系统返回到一个安全状态。

5.2.8.6 **不可旁路**

在数据库管理系统安全功能控制范围内，数据库管理系统的每一项功能执行之前，数据库管理系统的安全功能应确保安全功能被成功地激活。

5.2.9 **安全管理**

5.2.9.1 **功能管理**

数据库管理系统的安全功能应限制管理员对安全功能的启动、关闭和修改的能力。

5.2.9.2 **属性管理**

数据库管理系统的安全功能应依据访问控制策略，限制授权管理员查询、修改或删除安全属性的能力。

数据库管理系统的安全功能应提供安全属性的默认值，仅允许授权管理员为生成的客体或信息规定新的初始值以代替原来的默认值。

5.2.9.3 **安全功能数据管理**

数据库管理系统的安全功能应限制管理员查询、修改或删除安全功能数据的能力，仅允许授权管理员管理这些数据。

数据库管理系统的安全功能应能规定受限的安全功能数据及受限值（如：用户登录次数）。如果安全功能数据超过了指定的限制，应采取必要的动作。

5.2.10 **生存周期支持**

开发者提供的缺陷纠正程序文档，应描述用以接受用户对于安全缺陷报告的程序，以及更正这些缺陷的程序，并说明已采取的纠正措施。

5.2.11 **配置管理**

开发者提供的配置管理文档应以版本号做标签，为数据库管理系统提供引用，使一个版本号对应数据库管理系统的唯一版本。

5.2.12 **安全功能开发过程**

5.2.12.1 **功能规约**

开发者提供的数据库管理系统安全功能的功能规约应描述安全功能及其与外部的接口。

5.2.12.2 **高层设计**

开发者提供的数据库管理系统安全功能的高层设计应按子系统方式描述安全功能及其结构，并标识安全功能子系统的所有接口。

5.2.13 **测试**

5.2.13.1 **功能测试**

开发者提供的测试文档应包含测试计划、测试过程描述、预期的测试结果和实际测试结果，其中的测试计划应标识要测试的安全功能、描述要执行的测试目标，测试过程描述应标识要执行的测试、测试概况。

5.2.13.2 **覆盖分析**

开发者提供的测试覆盖的证据应表明测试文档中所标识的测试和功能规约中所描述的安全功能之间的对应性。

开发者提供的测试覆盖的证据应阐明测试文档所标识的测试和功能规约中所描述的安全功能之间的对应性是完备的。

标准分享网 www.bzfxw.com 免费下载

5.2.14 指导性文档

5.2.14.1 管理员指南

开发者提供的管理员指南应描述对于授权安全管理角色可使用的管理功能和接口、安全管理数据库管理系统的方式、受控制的安全参数以及与安全操作有关的用户行为的假设，并描述与为评估而提供的其他所有文件的一致性。

5.2.14.2 用户指南

开发者提供的用户指南，应描述用户可获取的安全功能和接口的用法以及安全操作中用户的职责（包括：用户行为假设）。同时，应描述与为评估而提供的其他所有文件的一致性。

5.2.15 交付和运行

5.2.15.1 交付

开发者提供的交付文档应向用户说明这一维护安全所必需的交付程序。

5.2.15.2 安装生成

开发者提供的安装过程的文档应说明用于数据库管理系统的安全安装、生成和启动的过程所必需的步骤。并应描述一个启动程序，它包含了用以生成数据库管理系统的选项，从而能决定数据库管理系统是如何以及何时产生的。

5.3 安全标记保护级

5.3.1 自主访问控制

数据库管理系统安全功能定义和控制系统中命名用户对命名客体的访问。自主访问控制的实施机制允许用户指定和控制客体的共享，并具备限制访问权限扩散的控制能力。自主访问控制机制根据用户指定或默认的方式，阻止未授权用户对客体访问。对于每个命名客体，自主访问控制机制提供授权访问和不授权访问的访问控制表。只允许授权用户将访问许可授予未拥有某客体访问权限的用户。

数据库管理系统的安全功能应实施安全机制（如：利用访问控制表），控制用户对客体的访问。

5.3.2 强制访问控制

数据库管理系统安全功能对外部主体能直接或间接访问的所有资源（例如：主体、存储客体、输入输出资源）实施强制访问控制。为这些主体及客体指定敏感标记，这些标记是由等级分类和非等级类别的组合，它们是实施强制访问控制的依据。

数据库管理系统的安全功能应实施安全机制（如：通过主客体的敏感标记），控制用户对相关客体的直接访问。

5.3.3 标记

5.3.3.1 标记定义

数据库管理系统安全功能应给出其控制范围内所有主体及控制的客体的敏感标记。

5.3.3.2 标记管理

数据库管理系统安全功能应执行访问控制策略，仅允许授权管理员管理敏感标记。

5.3.3.3 带标记数据输入

从数据库管理系统安全功能控制范围之外输入带标记的数据时，数据库管理系统安全功能应确保标记和接受的用户数据相关。

5.3.4 身份鉴别

5.3.4.1 用户属性定义

数据库管理系统安全功能应给出每个用户与标识相关的安全属性，如：标识符、组等。如果数据库管理系统安全功能维护自己的标识与鉴别数据，那么它应保证每个用户个体在数据库管理系统和其他系统安全功能中的信息相一致。

5.3.4.2 用户标识

数据库管理系统的安全功能应预先设定数据库管理系统代表用户执行的、与安全功能相关的动作，

在标识之前，安全功能允许数据库管理系统执行这些预设动作。在其他的安全功能引起的操作动作之前，数据库管理系统的安全功能要成功地标识每个用户。

5.3.4.3 用户鉴别

数据库管理系统的安全功能应预先设定数据库管理系统代表用户执行的、与安全功能相关的动作，在用户被鉴别之前，允许数据库管理系统执行这些预设动作。在其他的安全功能引起的操作动作之前，数据库管理系统的安全功能应成功地鉴别每个用户。

当进行鉴别时，数据库管理系统的安全功能应仅仅将最少的反馈（如：打入的字符数，鉴别的成功或失败）提供给用户。

数据库管理系统的安全功能应提供多鉴别机制以支持用户鉴别。

5.3.4.4 鉴别失败处理

数据库管理系统的安全功能应能检测到与鉴别事件相关的不成功的鉴别尝试，当不成功鉴别尝试的次数达到或超过了定义的界限时，安全功能应能终止会话建立的进程。

在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。

5.3.4.5 访问历史

在会话成功建立的基础上，数据库管理系统的安全功能应显示用户上一次成功会话建立的日期、时间、方法、位置等。

数据库管理系统的安全功能应显示用户上一次不成功的会话尝试的日期、时间、方法、位置等，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。

5.3.4.6 不可观察性

数据库管理系统的安全功能应提供给一个或多个授权用户观察资源和服务用情况的能力。

5.3.5 客体重用

对于数据库管理系统中的所有客体，在指定、分配或再分配给一个主体时，数据库管理系统的安全功能应确保其中没有上一次分配的剩余信息。当依赖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，应提供该客体重用功能的可信性的证据。

5.3.6 审计

5.3.6.1 内容

数据库管理系统的安全功能应能为可审计事件（如：使用客体创建、用户鉴别、客体删除、安全属性变更等）生成一个审计记录，并在每一个审计记录中至少记录以下信息：

——事件发生的日期和时间；

——事件的类型；

——主体身份、客体身份和事件的结果（成功或失败）。

数据库管理系统的安全功能应能维护数据库管理系统的可审计事件，但其中至少包括：

——标识和鉴别机制的使用；

——由用户启动的独立操作（如：创建、删除、更新、检索、插入等）；

——数据库管理员执行的动作；

——访问仲裁机制的使用。

5.3.6.2 查阅

数据库管理系统的安全功能应提供给授权用户从审计记录中读取一定类型的审计信息的能力，其审计记录可被其他系统的安全功能所处理。

数据库管理系统的安全功能应提供对审计数据进行基于一定准则的选择查阅的能力，并能对结果进行搜索、分类或排序。

5.3.6.3 存储保护

标准分享网 www.bzfxw.com 免费下载

数据库管理系统的安全功能应保护已存储的审计记录，避免未授权的删除，并监测对审计记录的修改，当审计存储已满、失败或受到攻击时，应确保审计记录保持一定的记录数和维持的时间。

当审计记录超过预定的限制值时，数据库管理系统的安全功能应采取相应的行动，如：向审计管理员发出警告。

5.3.6.4 分析

数据库管理系统的安全功能应用一定的规则去监控审计事件，并指出潜在的侵害。对不能由数据库管理系统安全功能独立分辨的审计事件，数据库管理系统审计机制应提供可被授权主体调用的审计记录接口。

5.3.6.5 自动响应

当检测到可能的安全侵害时，数据库管理系统的安全功能应做出响应，如：通知审计管理员，向授权用户提供一组遏制侵害的或采取校正的行动。

5.3.7 数据完整性

5.3.7.1 数据鉴别

数据库管理系统的安全功能能为客体产生信息真实性的证据（如：单向函数、数字签名）。

5.3.7.2 回退

数据库管理系统的安全功能允许在规定的客体上执行特定操作的回退。

数据库管理系统的安全功能能规定回退可以实施的严格条件（如：角色要求等）。

5.3.7.3 完整性监视

对于具有特定用户数据属性的客体，数据库管理系统的安全功能应监视所存储的用户数据是否出现破坏完整性的错误。

数据库管理系统的安全功能当检测到破坏完整性的错误时应采取行动（如：提示管理员）。

5.3.8 数据传输

5.3.8.1 内部传输

在数据库管理系统物理分隔的各部分之间传递用户数据时，数据库管理系统的安全功能应执行特定的安全功能策略。

数据库管理系统的安全功能应监视是否有完整性错误出现。

5.3.8.2 数据外部输出

向数据库管理系统安全功能控制范围之外输出用户数据时，数据库管理系统安全功能应在访问控制机制允许的前提下，执行特定的安全功能策略，进行用户数据输出。

向数据库管理系统安全功能控制范围之外输出与用户数据相关的安全属性时，数据库管理系统安全功能应确保安全属性与输出的用户数据相关。

5.3.8.3 数据外部输入

当用户数据从数据库管理系统安全功能控制范围之外输入时，数据库管理系统的安全功能应执行特定的安全功能策略。

数据库管理系统的安全功能应使用与输入的数据相关的安全属性，确保在安全属性和接受的用户数据之间提供了明确的关联。

5.3.8.4 原发证明

数据库管理系统的安全功能应能对发出的信息产生原发证据。

数据库管理系统的安全功能应能将信息原发者的相关属性与证据适用的信息内容相关联。

5.3.8.5 接收证明

数据库管理系统的安全功能应能对接收的信息产生接收证据。

数据库管理系统的安全功能应能将信息接收者的相关属性与接收证据的相关内容相关联。

5.3.9 密码支持

5.3.9.1 密钥管理

数据库管理系统的安全功能能根据符合国家规定的方法来管理密钥，包括产生、分发、访问及销毁密钥。

5.3.9.2 密码运算

数据库管理系统的安全功能能根据国家规定的特定的密码算法和密钥长度来执行密码运算。

5.3.10 资源利用

5.3.10.1 容错

数据库管理系统的安全功能能检测出已规定的数据库管理系统故障。

5.3.10.2 并发会话

数据库管理系统的安全功能应限制属于同一用户的并发会话的最大数目。

5.3.11 安全功能保护

5.3.11.1 安全功能自检

数据库管理系统的安全功能应在数据库管理系统的特定状态(如：启动时，应授权用户要求)中，检查安全功能的正确执行。

数据库管理系统的安全功能应为授权用户提供验证安全功能数据完整性的能力。

5.3.11.2 时间戳

数据库管理系统的安全功能应为自身的应用提供可靠的时间戳。

5.3.11.3 域分离

数据库管理系统的安全功能应分离在数据库管理系统安全功能控制范围内各主体的安全域。

5.3.11.4 数据一致性

数据库管理系统的安全功能应确保数据库管理系统各部分间的安全功能数据的一致性。

5.3.11.5 安全功能数据传输

在数据库管理系统的分离部分间传输安全功能数据时，数据库管理系统的安全功能应保护安全功能数据不被泄露或修改。当依靠其他系统的安全功能实现安全传输时，应提供其他系统的数据传输保护功能的可信性证据。

数据库管理系统的安全功能应分离传送安全功能数据和用户数据。

数据库管理系统的安全功能应能检测安全功能数据被修改、替换、重排、删除等完整性错误。

5.3.11.6 系统恢复

当数据库管理系统发生失败或服务中断后，数据库管理系统的安全功能应进入维护方式，将数据库管理系统返回到一个安全状态。

5.3.11.7 不可旁路

在数据库管理系统安全功能控制范围内，数据库管理系统的每一项功能执行之前，数据库管理系统的安全功能应确保安全功能被成功地激活。

5.3.11.8 物理保护

数据库管理系统的安全功能应对可能损害其安全的物理篡改提供明确的检测，并能判断出特定的物理篡改。

5.3.12 安全管理

5.3.12.1 功能管理

数据库管理系统的安全功能应限制管理员对安全功能的启动、关闭和修改的能力。

5.3.12.2 属性管理

数据库管理系统的安全功能应依据访问控制策略，限制授权管理员查询、修改或删除安全属性的能力。

数据库管理系统的安全功能应提供安全属性的默认值，仅允许授权管理员为生成的客体或信息规

标准分享网 www.bzfxw.com 免费下载

定新的初始值以代替原来的默认值。

数据库管理系统的安全功能应确保安全属性只接受安全的值。

5.3.12.3 **安全功能数据管理**

数据库管理系统的安全功能应限制管理员查询、修改或删除安全功能数据的能力，仅允许授权管理员管理这些数据。

数据库管理系统的安全功能应能规定受限的安全功能数据及受限值（如：用户登录次数）。如果安全功能数据超过了指定的限制，应采取必要的动作。

5.3.12.4 **安全管理角色**

数据库管理系统的安全功能应能支持维护授权角色。

5.3.13 **生存周期支持**

5.3.13.1 **开发安全**

开发者提供的开发安全文件应描述在数据库管理系统开发环境中在物理上、程序上、人员上以及其他方面的安全措施。

5.3.13.2 **缺陷纠正**

开发者提供的缺陷纠正程序文档，应描述用以接受用户对于安全缺陷报告的程序，以及更正这些缺陷的程序，并说明已采取的纠正措施。

5.3.13.3 **工具和技术**

开发者提供的开发工具文档应标识在开发数据库管理系统中使用的工具和参照的标准，并描述有关实现的开发工具的选项。

5.3.14 **配置管理**

5.3.14.1 **能力**

开发者提供的配置管理文档应以版本号做标签，为数据库管理系统提供引用，使一个版本号对应数据库管理系统的唯一版本。

开发者提供的配置管理文档应包括配置清单、配置管理计划和接受计划，其中配置清单应描述对配置项进行唯一标识的方法，并清楚地标识出组成安全功能的配置项。

5.3.14.2 **范围**

开发者提供的配置管理文档应描述配置管理系统是如何跟踪配置项的，并说明至少能跟踪：数据库管理系统实现表示，设计文档，测试文档，用户文档，管理员文档和配置管理文档。

5.3.15 **安全功能开发过程**

5.3.15.1 **安全策略模型**

开发者提供的安全策略模型应描述所有可以模型化的安全策略的规则和特性。

5.3.15.2 **功能规约**

开发者提供的数据库管理系统安全功能的功能规约应描述安全功能及其与外部的接口。

开发者提供的数据库管理系统安全功能的功能规约应完备地表示安全功能。

5.3.15.3 **高层设计**

开发者提供的数据库管理系统安全功能的高层设计应按子系统方式描述安全功能及其结构，并标识安全功能子系统的所有接口。

开发者提供的数据库管理系统安全功能的高层设计应将有关安全功能策略实施的子系统与其他子系统分离。

5.3.15.4 **低层设计**

开发者提供的数据库管理系统安全功能的低层设计应以模块术语描述安全功能，并描述每一个模块的目的、接口。

5.3.15.5 **实现**

开发者提供的数据库管理系统安全功能的实现表示(如:源代码)文档应是内在一致的,并且无歧义地定义了详细的数据库管理系统安全功能。

5.3.15.6 **表示对应性**

对于所提供的安全策略表示的每个相邻对,开发者应提供相邻两阶段开发文档之间的对应性分析,并阐明上一阶段的安全策略表示在下一阶段文档中得到正确而完备地细化。

5.3.16 **测试**

5.3.16.1 **功能测试**

开发者提供的测试文档应包含测试计划、测试过程描述、预期的测试结果和实际测试结果,其中的测试计划应标识要测试的安全功能、描述要执行的测试目标,测试过程描述应标识要执行的测试、测试概况。

5.3.16.2 **覆盖分析**

开发者提供的测试覆盖的证据应表明测试文档中所标识的测试和功能规约中所描述的安全功能之间的对应性。

开发者提供的测试覆盖的证据应阐明测试文档所标识的测试和功能规约中所描述的安全功能之间的对应性是完备的。

5.3.16.3 **深度**

开发者提供的测试深度分析文档应说明测试文档中所标识的测试足以说明该安全功能动作和高层设计是一致的。

5.3.17 **指导性文档**

5.3.17.1 **管理员指南**

开发者提供的管理员指南应描述对于授权安全管理角色可使用的管理功能和接口、安全管理数据库管理系统的方式、受控制的安全参数以及与安全操作有关的用户行为的假设,并描述与为评估而提供的其他所有文件的一致性。

5.3.17.2 **用户指南**

开发者提供的用户指南,应描述用户可获取的安全功能和接口的用法以及安全操作中用户的职责(包括:用户行为假设)。同时,应描述与为评估而提供的其他所有文件的一致性。

5.3.18 **脆弱性**

开发者提供的脆弱性分析文档应标识脆弱性的分布,并说明在所期望的环境中这些脆弱性不会被利用。

5.3.19 **交付和运行**

5.3.19.1 **交付**

开发者提供的交付文档应向用户说明这一维护安全所必需的交付程序。

5.3.19.2 **安装生成**

开发者提供的安装过程的文档应说明用于数据库管理系统的安全安装、生成和启动的过程所必需的步骤。并应描述一个启动程序,它包含了用以生成数据库管理系统的选项,从而能决定数据库管理系统是如何以及何时产生的。

5.4 **结构化保护级**

5.4.1 **自主访问控制**

数据库管理系统安全功能定义和控制系统中命名用户对命名客体的访问。自主访问控制的实施机制允许用户指定和控制客体的共享,并具备限制访问权限扩散的控制能力。自主访问控制机制根据用户指定或默认的方式,阻止未授权用户对客体访问。对于每个命名客体,自主访问控制机制提供授权访问和不授权访问的访问控制表。只允许授权用户将访问许可授予未拥有某客体访问权限的用户。

数据库管理系统的安全功能应实施安全机制(如:利用访问控制表),控制用户对客体的访问。

标准分享网 www.bzfxw.com 免费下载

5.4.2 强制访问控制

数据库管理系统安全功能对外部主体能直接或间接访问的所有资源(例如:主体、存储客体、输入输出资源)实施强制访问控制。为这些主体及客体指定敏感标记,这些标记是由等级分类和非等级类别的组合,它们是实施强制访问控制的依据。

数据库管理系统的安全功能应实施安全机制(如:通过主客体的敏感标记),控制用户对相关客体的直接访问。

数据库管理系统的安全功能应实施安全机制,控制所有主客体之间的访问。

5.4.3 标记

5.4.3.1 标记定义

数据库管理系统安全功能应给出其控制范围内所有主体和客体的敏感标记。

5.4.3.2 标记管理

数据库管理系统安全功能应执行访问控制策略,仅允许授权管理员管理敏感标记。

5.4.3.3 带标记数据输入

从数据库管理系统安全功能控制范围之外输入带标记的数据时,数据库管理系统安全功能应确保标记和接受的用户数据相关。

5.4.4 身份鉴别

5.4.4.1 用户属性定义

数据库管理系统安全功能应给出每个用户与标识相关的安全属性,如:标识符、组等。如果数据库管理系统安全功能维护自己的标识与鉴别数据,那么它应保证每个用户个体在数据库管理系统和其他系统安全功能中的信息相一致。

5.4.4.2 用户标识

数据库管理系统的安全功能应预先设定数据库管理系统代表用户执行的、与安全功能相关的动作,在标识之前,安全功能允许数据库管理系统执行这些预设动作。在其他的安全功能引起的操作动作之前,数据库管理系统的安全功能要成功地标识每个用户。

5.4.4.3 用户鉴别

数据库管理系统的安全功能应预先设定数据库管理系统代表用户执行的、与安全功能相关的动作,在用户被鉴别之前,允许数据库管理系统执行这些预设动作。在其他的安全功能引起的操作动作之前,数据库管理系统的安全功能应成功地鉴别每个用户。

当进行鉴别时,数据库管理系统的安全功能应仅仅将最少的反馈(如:打入的字符数,鉴别的成功或失败)提供给用户。

数据库管理系统的安全功能应提供多鉴别机制以支持用户鉴别。

5.4.4.4 鉴别失败处理

数据库管理系统的安全功能应能检测到与鉴别事件相关的不成功的鉴别尝试,当不成功鉴别尝试的次数达到或超过了定义的界限时,安全功能应能终止会话建立的进程。

在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。

5.4.4.5 访问历史

在会话成功建立的基础上,数据库管理系统的安全功能应显示用户上一次成功会话建立的日期、时间、方法、位置等。

数据库管理系统的安全功能应显示用户上一次不成功的会话尝试的日期、时间、方法、位置等,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。

5.4.4.6 不可观察性

数据库管理系统的安全功能应提供给一个或多个授权用户观察资源和服务用情况的能力。

对于由数据库管理系统的安全功能规定的受保护用户进行的操作，安全功能应确保未授权用户不能观察到。

5.4.5 客体重用

对于数据库管理系统中的所有客体，在指定、分配或再分配给一个主体时，数据库管理系统的安全功能应确保其中没有上一次分配的剩余信息，当依赖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，应提供该客体重用功能的可信性的证据。

5.4.6 审计

5.4.6.1 内容

数据库管理系统的安全功能应能为可审计事件(如：使用客体创建、用户鉴别、客体删除、安全属性变更等)生成一个审计记录，并在每一个审计记录中至少记录以下信息：

——事件发生的日期和时间；

——事件的类型；

——主体身份、客体身份和事件的结果(成功或失败)。

数据库管理系统的安全功能应能维护数据库管理系统的可审计事件，但其中至少包括：

——标识和鉴别机制的使用；

——由用户启动的独立操作(如：创建、删除、更新、检索、插入等)；

——数据库管理员执行的动作；

——访问仲裁机制的使用。

5.4.6.2 查阅

数据库管理系统的安全功能应提供给授权用户从审计记录中读取一定类型的审计信息的能力，其审计记录可被其他系统的安全功能所处理。

数据库管理系统的安全功能应提供对审计数据进行基于一定准则的选择查阅的能力，并能对结果进行搜索、分类或排序。

5.4.6.3 存储保护

数据库管理系统的安全功能应保护已存储的审计记录，避免未授权的删除，并监测对审计记录的修改，当审计存储已满、失败或受到攻击时，应确保审计记录保持一定的记录数和维持的时间。

当审计记录超过预定的限制值时，数据库管理系统的安全功能应采取相应的行动，如：向审计管理员发出警告。

如果审计记录已满，数据库管理系统的安全功能应阻止除具有特殊权限的授权用户外产生的所有可审计事件，并且在审计存储失败时采取相应的行动(如：通知审计管理员)。

5.4.6.4 分析

数据库管理系统的安全功能应用一定的规则去监控审计事件，并指出潜在的侵害。对不能由数据库管理系统安全功能独立分辨的审计事件，数据库管理系统审计机制应提供可被授权主体调用的审计记录接口。

数据库管理系统的安全功能应维护系统的使用轮廓(是一个表征用户或主体活动特征的结构，它表现了用户或主体怎样用不同的方法与安全功能交互)，对于那些其行动已记录在轮廓中的用户，应维护其相对应的置疑等级，当用户的置疑等级超过限制条件时，应能指出对安全策略可能发生的侵害。

5.4.6.5 自动响应

当检测到可能的安全侵害时，数据库管理系统的安全功能应做出响应，如：通知审计管理员，向授权用户提供一组遏制侵害的或采取校正的行动。

5.4.7 数据完整性

5.4.7.1 数据鉴别

数据库管理系统的安全功能能为客体产生信息真实性的证据(如：单向函数、数字签名)。

标准分享网 www.bzfxw.com 免费下载

数据库管理系统的安全功能能提供支持，用以验证信息的真实性证据和产生证据的用户身份。

5.4.7.2 回退

数据库管理系统的安全功能允许在规定的客体上执行特定操作的回退。

数据库管理系统的安全功能能规定回退可以实施的严格条件(如：角色要求等)。

5.4.7.3 完整性监视

对于具有特定用户数据属性的客体，数据库管理系统的安全功能应监视所存储的用户数据是否出现破坏完整性的错误。

数据库管理系统的安全功能当检测到破坏完整性的错误时应采取行动(如：提示管理员)。

5.4.8 数据传输

5.4.8.1 内部传输

在数据库管理系统物理分隔的各部分之间传递用户数据时，数据库管理系统的安全功能应执行特定的安全功能策略。

数据库管理系统的安全功能应监视是否有完整性错误出现。

数据库管理系统的安全功能应能支持规定对完整性错误将采取的动作。

5.4.8.2 数据外部输出

向数据库管理系统安全功能控制范围之外输出用户数据时，数据库管理系统安全功能应在访问控制机制允许的前提下，执行特定的安全功能策略，进行用户数据输出。

向数据库管理系统安全功能控制范围之外输出与用户数据相关的安全属性时，数据库管理系统安全功能应确保安全属性与输出的用户数据相关。

对于某些特定的安全属性，数据库管理系统的安全功能应保证无论何时都不会被输出。

5.4.8.3 数据外部输入

当用户数据从数据库管理系统安全功能控制范围之外输入时，数据库管理系统的安全功能应执行特定的安全功能策略。

数据库管理系统的安全功能应使用与输入的数据相关的安全属性，确保在安全属性和接受的用户数据之间提供了明确的关联。

对于输入的用户数据，数据库管理系统的安全功能应确保对其安全属性的解析与用户数据源的解析是一致的。

5.4.8.4 可信路径

数据库管理系安全功能应在它和用户之间提供一条可信的通信路径，此路径在逻辑上明显不同于其他路径，并能保护通信数据免遭修改和泄露。

5.4.8.5 原发证明

数据库管理系统的安全功能应能对发出的信息产生原发证据。

数据库管理系统的安全功能应能将信息原发者的相关属性与证据适用的信息内容相关联。

数据库管理系统的安全功能应能验证信息原发证据的真实性。

5.4.8.6 接收证明

数据库管理系统的安全功能应能对接收的信息产生接收证据。

数据库管理系统的安全功能应能将信息接收者的相关属性与接收证据的相关内容相关联。

数据库管理系统的安全功能应能验证信息接收证据的真实性。

5.4.9 密码支持

5.4.9.1 密钥管理

数据库管理系统的安全功能能根据符合国家规定的方法来管理密钥，包括产生、分发、访问及销毁密钥。

5.4.9.2 密码运算

数据库管理系统的安全功能能根据国家规定的特定的密码算法和密钥长度来执行密码运算。

5.4.10 资源利用

5.4.10.1 容错

数据库管理系统的安全功能能检测出已规定的数据库管理系统故障。

当规定的故障发生时，数据库管理系统的安全功能应确保数据库管理系统其余部分的能力均能实现。

5.4.10.2 并发会话

数据库管理系统的安全功能应限制属于同一用户的并发会话的最大数目。

5.4.11 安全功能保护

5.4.11.1 安全功能自检

数据库管理系统的安全功能应在数据库管理系统的特定状态(如：启动时，应授权用户要求)中，检查安全功能的正确执行。

数据库管理系统的安全功能应为授权用户提供验证安全功能数据完整性的能力。

数据库管理系统的安全功能应为授权用户提供验证安全功能可执行码完整性的能力。

5.4.11.2 时间戳

数据库管理系统的安全功能应为自身的应用提供可靠的时间戳。

5.4.11.3 域分离

数据库管理系统的安全功能应分离在数据库管理系统安全功能控制范围内各主体的安全域。

数据库管理系统的安全功能应为自身执行时维护一个安全域，防止不可信主体进行干扰和篡改。

5.4.11.4 数据一致性

数据库管理系统的安全功能应确保数据库管理系统各部分间的安全功能数据的一致性。

当包含复本的安全功能数据的数据库管理系统组成部分被断开，而又重建连接后，对于任何依赖于安全功能数据复本的安全功能请求，数据库管理系统的安全功能应确保复制的安全功能数据的一致性。

5.4.11.5 安全功能数据传输

在数据库管理系统的分离部分间传输安全功能数据时，数据库管理系统的安全功能应保护安全功能数据不被泄露或修改。当依靠其他系统的安全功能实现安全传输时，应提供其他系统的数据传输保护功能的可信性证据。

数据库管理系统的安全功能应分离传送安全功能数据和用户数据。

数据库管理系统的安全功能应能检测安全功能数据被修改、替换、重排、删除等完整性错误。

数据库管理系统的安全功能应规定对完整性错误将采取的动作。

5.4.11.6 系统恢复

当数据库管理系统发生失败或服务中断后，数据库管理系统的安全功能应进入维护方式，将数据库管理系统返回到一个安全状态。

数据库管理系统的安全功能应具备从失败或服务中断状态恢复到最近的安全状态的能力。

5.4.11.7 不可旁路

在数据库管理系统安全功能控制范围内，数据库管理系统的每一项功能执行之前，数据库管理系统的安全功能应确保安全功能被成功地激活。

5.4.11.8 物理保护

数据库管理系统的安全功能应对可能损害其安全的物理篡改提供明确的检测，并能判断出特定的物理篡改。

数据库管理系统的安全功能应监视需主动检测的安全功能设备及要素，当其发生物理篡改时，应采取行动，如：通知指定的管理员。

5.4.12 安全管理

标准分享网 www.bzfxw.com 免费下载

5.4.12.1 功能管理

数据库管理系统的安全功能应限制管理员对安全功能的启动、关闭和修改的能力。

5.4.12.2 属性管理

数据库管理系统的安全功能应依据访问控制策略，限制授权管理员查询、修改或删除安全属性的能力。

数据库管理系统的安全功能应提供安全属性的默认值，仅允许授权管理员为生成的客体或信息规定新的初始值以代替原来的默认值。

数据库管理系统的安全功能应确保安全属性只接受安全的值。

5.4.12.3 安全功能数据管理

数据库管理系统的安全功能应限制管理员查询、修改或删除安全功能数据的能力，仅允许授权管理员管理这些数据。

数据库管理系统的安全功能应能规定受限的安全功能数据及受限值(如：用户登录次数)。如果安全功能数据超过了指定的限制，应采取必要的动作。

数据库管理系统的安全功能应确保安全功能数据只接受安全的值。

5.4.12.4 时限授权

对于支持有效期的各种安全属性，数据库管理系统的安全功能应限制授权管理员规定有效期的能力。

5.4.12.5 安全管理角色

数据库管理系统的安全功能应支持维护授权角色。

数据库管理系统的安全功能应将角色与用户关联起来，并确保一个用户不同角色应满足的条件。(如：一个帐号同时不能具有多于一个的角色)

5.4.13 生存周期支持

5.4.13.1 开发安全

开发者提供的开发安全文件应描述在数据库管理系统开发环境中在物理上、程序上、人员上以及其他方面的安全措施。

5.4.13.2 缺陷纠正

开发者提供的缺陷纠正程序文档，应描述用以接受用户对于安全缺陷报告的程序，以及更正这些缺陷的程序，并说明已采取的纠正措施。

开发者提供的缺陷纠正程序文档，应描述用以跟踪所有数据库管理系统版本里安全缺陷的程序，标识对安全缺陷所采取的纠正措施。

5.4.13.3 生存周期模型

开发者提供的生存周期定义文档应描述所建立的用于开发和维护数据库管理系统的生存周期模型。

5.4.13.4 工具和技术

开发者提供的开发工具文档应标识在开发数据库管理系统中使用的工具和参照的标准，并描述有关实现的开发工具的选项。

开发者提供的开发工具文档应明确定义所有基于实现的选项的含义。

5.4.14 配置管理

5.4.14.1 自动化

开发者提供的配置管理文档应描述在配置管理系统中使用的自动生成工具。

5.4.14.2 能力

开发者提供的配置管理文档应以版本号做标签，为数据库管理系统提供引用，使一个版本号对应数据库管理系统的唯一版本。

开发者提供的配置管理文档应包括配置清单、配置管理计划和接受计划，其中配置清单应描述对配置项进行唯一标识的方法，并清楚地标识出组成安全功能的配置项。

开发者提供的配置管理文档应在配置管理计划中描述配置管理系统是如何使用的，并阐明实施中的配置管理与配置管理计划的一致性。

5.4.14.3 范围

开发者提供的配置管理文档应描述配置管理系统是如何跟踪配置项的，并说明至少能跟踪：数据库管理系统实现表示、设计文档、测试文档、用户文档、管理员文档和配置管理文档。

开发者提供的配置管理文档应说明配置管理系统能跟踪安全缺陷。

5.4.15 安全功能开发过程

5.4.15.1 安全策略模型

开发者提供的安全策略模型应描述所有可以模型化的安全策略的规则和特性。

开发者提供形式化的安全策略模型，并阐明或适当时严格证明功能规约和安全策略模型之间的对应性，并说明功能规约中的安全功能对于安全策略模型来说，是一致的而且是完备的。

5.4.15.2 功能规约

开发者提供的数据库管理系统安全功能的功能规约应描述安全功能及其与外部的接口。

开发者提供的数据库管理系统安全功能的功能规约应完备地表示安全功能。

开发者应提供半形式化的数据库管理系统安全功能的功能规约。使用半形式化风格来描述安全功能与其外部接口，可以由非形式化的、解释性的文字来支持。

5.4.15.3 高层设计

开发者提供的数据库管理系统安全功能的高层设计应按子系统方式描述安全功能及其结构，并标识安全功能子系统的所有接口。

开发者提供的数据库管理系统安全功能的高层设计应将有关安全功能策略实施的子系统与其他子系统分离。

开发者提供的数据库管理系统安全功能的高层设计应是半形式化的。

5.4.15.4 低层设计

开发者提供的数据库管理系统安全功能的低层设计应以模块术语描述安全功能，并描述每一个模块的目的、接口。

开发者提供的数据库管理系统安全功能的低层设计应是半形式化的，并详细描述数据库管理系统安全功能模块所有接口的目的与方法。

5.4.15.5 实现

开发者提供的数据库管理系统安全功能的实现表示（如：源代码）文档应是内在一致的，并且无歧义地定义了详细的数据库管理系统安全功能。

开发者提供的数据库管理系统安全功能的实现表示文档应描述实现的各部分之间的关系。

5.4.15.6 表示对应性

对于所提供的安全策略表示的每个相邻对，开发者应提供相邻两阶段开发文档之间的对应性分析，并阐明上一阶段的安全策略表示在下一阶段文档中得到正确而完备地细化。

当安全策略表示的相邻对是半形式化或形式化的时候，对应性阐明也应是半形式化或形式化的。

5.4.16 测试

5.4.16.1 功能测试

开发者提供的测试文档应包含测试计划、测试过程描述、预期的测试结果和实际测试结果，其中的测试计划应标识要测试的安全功能、描述要执行的测试目标，测试过程描述应标识要执行的测试、测试概况。

开发者提供的测试文档应包含对顺序依赖性的分析。

标准分享网 www.bzfxw.com 免费下载

5.4.16.2 覆盖分析

开发者提供的测试覆盖的证据应表明测试文档中所标识的测试和功能规约中所描述的安全功能之间的对应性。

开发者提供的测试覆盖的证据应阐明测试文档所标识的测试和功能规约中所描述的安全功能之间的对应性是完备的。

5.4.16.3 深度

开发者提供的测试深度分析文档应说明测试文档中所标识的测试足以说明该安全功能动作和高层设计是一致的。

5.4.17 指导性文档

5.4.17.1 管理员指南

开发者提供的管理员指南应描述对于授权安全管理角色可使用的管理功能和接口、安全管理数据库管理系统的方式、受控制的安全参数以及与安全操作有关的用户行为的假设，并描述与为评估而提供的其他所有文件的一致性。

5.4.17.2 用户指南

开发者提供的用户指南，应描述用户可获取的安全功能和接口的用法以及安全操作中用户的职责(包括：用户行为假设)。同时，应描述与为评估而提供的其他所有文件的一致性。

5.4.18 脆弱性

5.4.18.1 隐蔽信道分析

开发者提供的隐蔽信道分析的文档应标识出隐蔽信道并且估计它们的容量。

5.4.18.2 安全功能强度

开发者提供的安全功能强度的分析文档应对每个具有安全功能强度声明的安全机制，进行安全功能强度的分析。

5.4.18.3 脆弱性分析

开发者提供的脆弱性分析文档应标识脆弱性的分布，并说明在所期望的环境中这些脆弱性不会被利用。

开发者提供的脆弱性分析文档应能说明对脆弱性的搜索是系统化的。

5.4.19 交付和运行

5.4.19.1 交付

开发者提供的交付文档应向用户说明这一维护安全所必需的交付程序。

开发者提供的交付文档应描述如何用各种方法和技术措施来检测修改，或检测描述开发者的主拷贝和用户方收到的版本之间的差异。

5.4.19.2 安装生成

开发者提供的安装过程的文档应说明用于数据库管理系统的安全安装、生成和启动的过程所必需的步骤。并应描述一个启动程序，它包含了用以生成数据库管理系统的选项，从而能决定数据库管理系统是如何以及何时产生的。

5.5 访问验证保护级

5.5.1 自主访问控制

数据库管理系统安全功能定义和控制系统中命名用户对命名客体的访问。自主访问控制的实施机制允许用户指定和控制客体的共享，并具备限制访问权限扩散的控制能力。自主访问控制机制根据用户指定或默认的方式，阻止未授权用户对客体访问。对于每个命名客体，自主访问控制机制提供授权访问和不授权访问的访问控制表。只允许授权用户将访问许可授予未拥有某客体访问权限的用户。

数据库管理系统的安全功能应实施安全机制(如：利用访问控制表)，控制用户对客体的访问。

数据库管理系统的安全功能能为特定的客体规定用户访问模式。

5.5.2 强制访问控制

数据库管理系统安全功能对外部主体能直接或间接访问的所有资源(例如:主体、存储客体、输入输出资源)实施强制访问控制。为这些主体及客体指定敏感标记,这些标记是由等级分类和非等级类别的组合,它们是实施强制访问控制的依据。

数据库管理系统的安全功能应实施安全机制(如:通过主客体的敏感标记),控制用户对相关客体的直接访问。

数据库管理系统的安全功能应实施安全机制,控制所有主客体之间的访问。

5.5.3 标记

5.5.3.1 标记定义

数据库管理系统安全功能应给出其控制范围内所有主体和客体的敏感标记。

5.5.3.2 标记管理

数据库管理系统安全功能应执行访问控制策略,仅允许授权管理员管理敏感标记。

5.5.3.3 带标记数据输入

从数据库管理系统安全功能控制范围之外输入带标记的数据时,数据库管理系统安全功能应确保标记和接受的用户数据相关。

5.5.4 身份鉴别

5.5.4.1 用户属性定义

数据库管理系统安全功能应给出每个用户与标识相关的安全属性,如:标识符、组等。如果数据库管理系统安全功能维护自己的标识与鉴别数据,那么它应保证每个用户个体在数据库管理系统和其他系统安全功能中的信息相一致。

5.5.4.2 用户标识

数据库管理系统的安全功能应预先设定数据库管理系统代表用户执行的、与安全功能相关的动作,在标识之前,安全功能允许数据库管理系统执行这些预设动作。在其他的安全功能引起的操作动作之前,数据库管理系统的安全功能要成功地标识每个用户。

5.5.4.3 用户鉴别

数据库管理系统的安全功能应预先设定数据库管理系统代表用户执行的、与安全功能相关的动作,在用户被鉴别之前,允许数据库管理系统执行这些预设动作。在其他的安全功能引起的操作动作之前,数据库管理系统的安全功能应成功地鉴别每个用户。

当进行鉴别时,数据库管理系统的安全功能应仅仅将最少的反馈(如:打入的字符数,鉴别的成功或失败)提供给用户。

数据库管理系统的安全功能应提供多鉴别机制以支持用户鉴别。

数据库管理系统的安全功能应规定重鉴别条件,在对应的条件下,对用户进行重新鉴别。

5.5.4.4 鉴别失败处理

数据库管理系统的安全功能应能检测到与鉴别事件相关的不成功的鉴别尝试,当不成功鉴别尝试的次数达到或超过了定义的界限时,安全功能应能终止会话建立的进程。

在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。

5.5.4.5 访问历史

在会话成功建立的基础上,数据库管理系统的安全功能应显示用户上一次成功会话建立的日期、时间、方法、位置等。

数据库管理系统的安全功能应显示用户上一次不成功的会话尝试的日期、时间、方法、位置等,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。

5.5.4.6 不可观察性

标准分享网 www.bzfxw.com 免费下载

数据库管理系统的安全功能应提供给一个或多个授权用户观察资源和服务用情况的能力。

对于由数据库管理系统的安全功能规定的受保护用户进行的操作，安全功能应确保未授权用户不能观察到。

5.5.5 **客体重用**

对于数据库管理系统中的所有客体，在指定、分配或再分配给一个主体时，数据库管理系统的安全功应确保其中没有上一次分配的剩余信息，当依赖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，应提供该客体重用功能的可信性的证据。

5.5.6 **审计**

5.5.6.1 **内容**

数据库管理系统的安全功能应能为可审计事件(如：使用客体创建、用户鉴别、客体删除、安全属性变更等)生成一个审计记录，并在每一个审计记录中至少记录以下信息：

——事件发生的日期和时间；

——事件的类型；

——主体身份、客体身份和事件的结果(成功或失败)。

数据库管理系统的安全功能应能维护数据库管理系统的可审计事件，但其中至少包括：

——标识和鉴别机制的使用；

——由用户启动的独立操作(如：创建、删除、更新、检索、插入等)；

——数据库管理员执行的动作；

——访问仲裁机制的使用。

5.5.6.2 **查阅**

数据库管理系统的安全功能应提供给授权用户从审计记录中读取一定类型的审计信息的能力，其审计记录可被其他系统的安全功能所处理。

数据库管理系统的安全功能应提供对审计数据进行基于一定准则的选择查阅的能力，并能对结果进行搜索、分类或排序。

5.5.6.3 **存储保护**

数据库管理系统的安全功能应保护已存储的审计记录，避免未授权的删除，并监测对审计记录的修改，当审计存储已满、失败或受到攻击时，应确保审计记录保持一定的记录数和维持的时间。

当审计记录超过预定的限制值时，数据库管理系统的安全功能应采取相应的行动，如：向审计管理员发出警告。

如果审计记录已满，数据库管理系统的安全功能应阻止除具有特殊权限的授权用户外产生的所有可审计事件，并且在审计存储失败时采取相应的行动(如：通知审计管理员)。

5.5.6.4 **分析**

数据库管理系统的安全功能应用一定的规则去监控审计事件，并指出潜在的侵害。对不能由数据库管理系统安全功能独立分辨的审计事件，数据库管理系统审计机制应提供可被授权主体调用的审计记录接口。

数据库管理系统的安全功能应维护系统的使用轮廓(是一个表征用户或主体活动特征的结构，它表现了用户或主体怎样用不同的方法与安全功能交互)，对于那些其行动已记录在轮廓中的用户，应维护其相对应的置疑等级，当用户的置疑等级超过限制条件时，应能指出对安全策略可能发生的侵害。

数据库管理系统的安全功能能维护有侵害性的系统事件序列的内部表示，当一个系统事件或事件序列被发现并与内部表示匹配时，安全功能应能指出攻击即将到来。

5.5.6.5 **自动响应**

当检测到可能的安全侵害时，数据库管理系统的安全功能应做出响应，如：通知审计管理员，向授权用户提供一组遏制侵害的或采取校正的行动。

5.5.7 数据完整性

5.5.7.1 数据鉴别

数据库管理系统的安全功能能为客体产生信息真实性的证据(如:单向函数、数字签名)。

数据库管理系统的安全功能能提供支持,用以验证信息的真实性证据和产生证据的用户身份。

5.5.7.2 回退

数据库管理系统的安全功能允许在规定的客体上执行特定操作的回退。

数据库管理系统的安全功能能规定回退可以实施的严格条件(如:角色要求等)。

5.5.7.3 完整性监视

对于具有特定用户数据属性的客体,数据库管理系统的安全功能应监视所存储的用户数据是否出现破坏完整性的错误。

数据库管理系统的安全功能当检测到破坏完整性的错误时应采取行动(如:提示管理员)。

5.5.8 数据传输

5.5.8.1 内部传输

在数据库管理系统物理分隔的各部分之间传递用户数据时,数据库管理系统的安全功能应执行特定的安全功能策略。

数据库管理系统的安全功能应监视是否有完整性错误出现。

数据库管理系统的安全功能应能支持规定对完整性错误将采取的动作。

5.5.8.2 数据外部输出

向数据库管理系统安全功能控制范围之外输出用户数据时,数据库管理系统安全功能应在访问控制机制允许的前提下,执行特定的安全功能策略,进行用户数据输出。

向数据库管理系统安全功能控制范围之外输出与用户数据相关的安全属性时,数据库管理系统安全功能应确保安全属性与输出的用户数据相关。

对于某些特定的安全属性,数据库管理系统的安全功能应保证无论何时都不会被输出。

5.5.8.3 数据外部输入

当用户数据从数据库管理系统安全功能控制范围之外输入时,数据库管理系统的安全功能应执行特定的安全功能策略。

数据库管理系统的安全功能应使用与输入的数据相关的安全属性,确保在安全属性和接受的用户数据之间提供了明确的关联。

对于输入的用户数据,数据库管理系统的安全功能应确保对其安全属性的解析与用户数据源的解析是一致的。

5.5.8.4 可信路径

数据库管理系统安全功能应在它和用户之间提供一条可信的通信路径,此路径在逻辑上明显不同于其他路径,并能保护通信数据免遭修改和泄露。

5.5.8.5 原发证明

数据库管理系统的安全功能应能对发出的信息产生原发证据。

数据库管理系统的安全功能应能将信息原发者的相关属性与证据适用的信息内容相关联。

数据库管理系统的安全功能应能验证信息原发证据的真实性。

5.5.8.6 接收证明

数据库管理系统的安全功能应能对接收的信息产生接收证据。

数据库管理系统的安全功能应能将信息接收者的相关属性与接收证据的相关内容相关联。

数据库管理系统的安全功能应能验证信息接收证据的真实性。

5.5.9 密码支持

5.5.9.1 密钥管理

标准分享网 www.bzfxw.com 免费下载

数据库管理系统的安全功能能根据符合国家规定的方法来管理密钥，包括产生、分发、访问及销毁密钥。

5.5.9.2 **密码运算**

数据库管理系统的安全功能能根据国家规定的特定的密码算法和密钥长度来执行密码运算。

5.5.10 **资源利用**

5.5.10.1 **容错**

数据库管理系统的安全功能能检测出已规定的数据库管理系统故障。

当规定的故障发生时，数据库管理系统的安全功能应确保数据库管理系统其余部分的能力均能实现。

5.5.10.2 **并发会话**

数据库管理系统的安全功能应限制属于同一用户的并发会话的最大数目。

5.5.11 **安全功能保护**

5.5.11.1 **安全功能自检**

数据库管理系统的安全功能应在数据库管理系统的特定状态(如：启动时，应授权用户要求)中，检查安全功能的正确执行。

数据库管理系统的安全功能应为授权用户提供验证安全功能数据完整性的能力。

数据库管理系统的安全功能应为授权用户提供验证安全功能可执行码完整性的能力。

5.5.11.2 **时间戳**

数据库管理系统的安全功能应为自身的应用提供可靠的时间戳。

5.5.11.3 **域分离**

数据库管理系统的安全功能应分离在数据库管理系统安全功能控制范围内各主体的安全域。

数据库管理系统的安全功能应为自身执行时维护一个安全域，防止不可信主体进行干扰和篡改。

数据库管理系统的安全功能应为安全功能中与访问控制有关的部分，维护一个自身执行时的安全域，防止被安全功能的其余部分和不可信主体的干扰和篡改。

5.5.11.4 **数据一致性**

数据库管理系统的安全功能应确保数据库管理系统各部分间的安全功能数据的一致性。

当包含复本的安全功能数据的数据库管理系统组成部分被断开，而又重建连接后，对于任何依赖于安全功能数据复本的安全功能请求，数据库管理系统的安全功能应确保复制的安全功能数据的一致性。

当安全功能与其他可信 IT 产品共享安全功能数据时，数据库管理系统的安全功能应具备对共享的安全功能数据的一致性解析能力。

5.5.11.5 **安全功能数据传输**

在数据库管理系统的分离部分间传输安全功能数据时，数据库管理系统的安全功能应保护安全功能数据不被泄露或修改。当依靠其他系统的安全功能实现安全传输时，应提供其他系统的数据传输保护功能的可信性证据。

数据库管理系统的安全功能应分离传送安全功能数据和用户数据。

数据库管理系统的安全功能应能检测安全功能数据被修改、替换、重排、删除等完整性错误。

数据库管理系统的安全功能应规定对完整性错误将采取的动作。

5.5.11.6 **系统恢复**

当数据库管理系统发生失败或服务中断后，数据库管理系统的安全功能应进入维护方式，将数据库管理系统返回到一个安全状态。

数据库管理系统的安全功能应具备从失败或服务中断状态恢复到最近的安全状态的能力。

5.5.11.7 **可信恢复**

数据库管理系统的安全功能应确保或者安全功能操作被成功完成，或者在失败时将安全功能恢复

到前后一致的状态。

5.5.11.8 **不可旁路**

在数据库管理系统安全功能控制范围内，数据库管理系统的每一项功能执行之前，数据库管理系统的安全功能应确保安全功能被成功地激活。

5.5.11.9 **物理保护**

数据库管理系统的安全功能应对可能损害其安全的物理篡改提供明确的检测，并能判断出特定的物理篡改。

数据库管理系统的安全功能应监视需主动检测的安全功能设备及要素，当其发生物理篡改时，应采取行动，如：通知指定的管理员。

5.5.12 **安全管理**

5.5.12.1 **功能管理**

数据库管理系统的安全功能应限制管理员对安全功能的启动、关闭和修改的能力。

5.5.12.2 **属性管理**

数据库管理系统的安全功能应依据访问控制策略，限制授权管理员查询、修改或删除安全属性的能力。

数据库管理系统的安全功能应提供安全属性的默认值，仅允许授权管理员为生成的客体或信息规定新的初始值以代替原来的默认值。

数据库管理系统的安全功能应确保安全属性只接受安全的值。

5.5.12.3 **安全功能数据管理**

数据库管理系统的安全功能应限制管理员查询、修改或删除安全功能数据的能力，仅允许授权管理员管理这些数据。

数据库管理系统的安全功能应能规定受限的安全功能数据及受限值（如：用户登录次数）。如果安全功能数据超过了指定的限制，应采取必要的动作。

数据库管理系统的安全功能应确保安全功能数据只接受安全的值。

5.5.12.4 **时限授权**

对于支持有效期的各种安全属性，数据库管理系统的安全功能应限制授权管理员规定有效期的能力。

数据库管理系统的安全功能应支持授权管理员对有效期后所采取的活动作出规定。

5.5.12.5 **安全管理角色**

数据库管理系统的安全功能应能支持维护授权角色。

数据库管理系统的安全功能应将角色与用户关联起来，并确保一个用户不同角色应满足的条件。（如：一个帐号同时不能具有多于一个的角色）

5.5.13 **生存周期支持**

5.5.13.1 **开发安全**

开发者提供的开发安全文件应描述在数据库管理系统开发环境中在物理上、程序上、人员上以及其他方面的安全措施。

开发者提供的开发安全文件应提供证据，证明安全措施对维护数据库管理系统的机密性和完整性提供了必要的保护级别。

5.5.13.2 **缺陷纠正**

开发者提供的缺陷纠正程序文档，应描述用以接受用户对于安全缺陷报告的程序，以及更正这些缺陷的程序，并说明已采取的纠正措施。

开发者提供的缺陷纠正程序文档，应描述用以跟踪所有数据库管理系统版本里安全缺陷的程序，标识对安全缺陷所采取的纠正措施。

5.5.13.3 **生存周期模型**

标准分享网 www.bzfxw.com 免费下载

开发者提供的生存周期定义文档应描述所建立的用于开发和维护数据库管理系统的生存周期模型。

开发者提供的生存周期定义文档应说明选择该模型的原因。

5.5.13.4 **工具和技术**

开发者提供的开发工具文档应标识在开发数据库管理系统中使用的工具和参照的标准，并描述有关实现的开发工具的选项。

开发者提供的开发工具文档应明确定义所有基于实现的选项的含义。

5.5.14 **配置管理**

5.5.14.1 **自动化**

开发者提供的配置管理文档应描述在配置管理系统中使用的自动生成工具。

开发者提供的配置管理文档应说明该生成工具能自动地确定数据库管理系统与以前版本之间的变化，以及因给定的配置项的修改而受到影响的其他所有配置项。

5.5.14.2 **能力**

开发者提供的配置管理文档应以版本号做标签，为数据库管理系统提供引用，使一个版本号对应数据库管理系统的唯一版本。

开发者提供的配置管理文档应包括配置清单、配置管理计划和接受计划，其中配置清单应描述对配置项进行唯一标识的方法，并清楚地标识出组成安全功能的配置项。

开发者提供的配置管理文档应在配置管理计划中描述配置管理系统是如何使用的，并阐明实施中的配置管理与配置管理计划的一致性。

开发者提供的配置管理文档应在计划中描述对修改过的或新建的配置项进行的接受程序，并提供保证对配置项只进行授权修改的方法。

5.5.14.3 **范围**

开发者提供的配置管理文档应描述配置管理系统是如何跟踪配置项的，并说明至少能跟踪：数据库管理系统实现表示、设计文档、测试文档、用户文档、管理员文档和配置管理文档。

开发者提供的配置管理文档应说明配置管理系统能跟踪安全缺陷。

5.5.15 **安全功能开发过程**

5.5.15.1 **安全策略模型**

开发者提供的安全策略模型应描述所有可以模型化的安全策略的规则和特性。

开发者提供形式化的安全策略模型，并阐明或适当时严格证明功能规约和安全策略模型之间的对应性，并说明功能规约中的安全功能对于安全策略模型来说，是一致的而且是完备的。

当功能规约是半形式或形式化时，与功能规约之间的对应性的阐明也应是半形式或形式化的。

5.5.15.2 **功能规约**

开发者提供的数据库管理系统安全功能的功能规约应描述安全功能及其与外部的接口。

开发者提供的数据库管理系统安全功能的功能规约应完备地表示安全功能。

开发者应提供**形式化的**数据库管理系统安全功能的功能规约。使用半形式化风格来描述安全功能与其外部接口，可以由非形式化的、解释性的文字来支持。

5.5.15.3 **高层设计**

开发者提供的数据库管理系统安全功能的高层设计应按子系统方式描述安全功能及其结构，并标识安全功能子系统的所有接口。

开发者提供的数据库管理系统安全功能的高层设计应将有关安全功能策略实施的子系统与其他子系统分离。

开发者提供的数据库管理系统安全功能的高层设计应是**形式化**的。

5.5.15.4 **低层设计**

开发者提供的数据库管理系统安全功能的低层设计应以模块术语描述安全功能，并描述每一个模块的目的、接口。

开发者提供的数据库管理系统安全功能的低层设计应是半形式化的，并详细描述数据库管理系统安全功能模块所有接口的目的与方法。

5.5.15.5 **实现**

开发者提供的数据库管理系统安全功能的实现表示(如：源代码)文档应是内在一致的，并且无歧义地定义了详细的数据库管理系统安全功能。

开发者提供的数据库管理系统安全功能的实现表示文档应描述实现的各部分之间的关系。

开发者提供的数据库管理系统安全功能的实现表示文档应是构造较小的且易于理解的。

5.5.15.6 **表示对应性**

对于所提供的安全策略表示的每个相邻对，开发者应提供相邻两阶段开发文档之间的对应性分析，并阐明上一阶段的安全策略表示在下一阶段文档中得到正确而完备地细化。

当安全策略表示的相邻对是半形式化或形式化的时候，对应性阐明也应是半形式化或形式化的。

5.5.16 **测试**

5.5.16.1 **功能测试**

开发者提供的测试文档应包含测试计划、测试过程描述、预期的测试结果和实际测试结果，其中的测试计划应标识要测试的安全功能、描述要执行的测试目标，测试过程描述应标识要执行的测试、测试概况。

开发者提供的测试文档应包含对顺序依赖性的分析。

5.5.16.2 **覆盖分析**

开发者提供的测试覆盖的证据应表明测试文档中所标识的测试和功能规约中所描述的安全功能之间的对应性。

开发者提供的测试覆盖的证据应阐明测试文档所标识的测试和功能规约中所描述的安全功能之间的对应性是完备的。

开发者提供的测试覆盖的证据应严格地阐明功能规约所标识的安全功能的所有外部接口均已经被完全测试。

5.5.16.3 **深度**

开发者提供的测试深度分析文档应说明测试文档中所标识的测试足以说明该安全功能动作和高层设计是一致的。

开发者提供的测试深度分析文档应说明测试文档中所标识的测试足以阐明该安全功能动作与高层设计和低层设计是一致的。

5.5.17 **指导性文档**

5.5.17.1 **管理员指南**

开发者提供的管理员指南应描述对于授权安全管理角色可使用的管理功能和接口、安全管理数据库管理系统的方式、受控制的安全参数以及与安全操作有关的用户行为的假设，并描述与为评估而提供的其他所有文件的一致性。

5.5.17.2 **用户指南**

开发者提供的用户指南，应描述用户可获取的安全功能和接口的用法以及安全操作中用户的职责(包括：用户行为假设)。同时，应描述与为评估而提供的其他所有文件的一致性。

5.5.18 **脆弱性**

5.5.18.1 **隐蔽信道分析**

开发者提供的隐蔽信道分析的文档应标识出隐蔽信道并且估计它们的容量。

开发者提供的隐蔽信道分析的文档应阐明对于隐蔽信道的分析是系统化的、彻底的。

5.5.18.2 **安全功能强度**

开发者提供的安全功能强度的分析文档应对每个具有安全功能强度声明的安全机制，进行安全功能强度的分析。

5.5.18.3 **脆弱性分析**

开发者提供的脆弱性分析文档应标识脆弱性的分布，并说明在所期望的环境中这些脆弱性不会被利用。

开发者提供的脆弱性分析文档应能说明对脆弱性的搜索是系统化的。

5.5.19 **交付和运行**

5.5.19.1 **交付**

开发者提供的交付文档应向用户说明这一维护安全所必需的交付程序。

开发者提供的交付文档应描述如何用各种方法和技术措施来检测修改，或检测描述开发者的主拷贝和用户方收到的版本之间的差异。

5.5.19.2 **安装生成**

开发者提供的安装过程的文档应说明用于数据库管理系统的安全安装、生成和启动的过程所必需的步骤。并应描述一个启动程序，它包含了用以生成数据库管理系统的选项，从而能决定数据库管理系统是如何以及何时产生的。

附 录 A
（资料性附录）
数据库管理系统面临的威胁和对策

A.1 数据库管理系统可能面对的主要威胁

数据库管理系统保护的资源包括数据库管理系统存储、处理或传送的信息。数据库管理系统阻止对信息的未授权访问，未授权访问包括：泄漏、修改和破坏。对数据库管理系统可能构成威胁的用户分为两类：数据库管理系统的未授权用户和授权用户。即使在非敌对环境中工作的，有着良好管理秩序的组织中，数据库管理系统的授权用户也可能由于疏忽或其他偶然因素对系统的安全构成威胁。所以数据库管理系统应防止这类威胁。

下面列出了数据库管理系统可能会遇到的安全威胁：

——未授权的用户可能尝试避开数据库管理系统的安全措施，存取数据库管理系统中的数据信息；

——未授权的用户可能猜测鉴别信息，从而利用此信息发起对数据库管理系统的攻击；

——未授权的用户可能使用未经许可的服务，获得数据库中数据的拷贝，导致数据库系统存储的数据被非法利用；

——系统用户可能越权查阅和修改其不应访问的受保护信息；

——用户信息流被转发到系统安全策略所不允许的用户；

——未授权用户窃取合法用户的帐号和密码或者授权用户冒充其他用户向数据库管理系统请求访问并访问数据；

——系统审计员没有及时审阅审计信息，致使攻击者未能被发现；

——安全管理员对系统安全参数的设置不正确，导致安全机制失效；

——授权用户将自身的访问特权不适当地授予其他用户，导致系统安全策略受到威胁，使用户数据不适当地泄漏；

——未授权或授权用户向数据库管理系统请求大量服务，以此大量耗费数据库管理系统的系统资源，使其不能正常工作；

——未授权或授权用户可能通过使用耗费尽审计数据的存储容量方式，导致审计数据的丢失或无法继续记录审计数据；

——由于系统软件或者硬件的故障，导致数据丢失，系统停止服务。

A.2 数据库管理系统可采用的降低威胁的方法

数据库管理系统可以采用以下方法以抵御威胁：

——数据库管理系统中，主体对客体的访问受系统安全功能的限制和裁定，特定客体的访问权限由主、客体安全属性、用户身份和环境等条件所决定，这些条件在对应的安全策略中规定。

——数据库管理系统要对系统用户进行标识和鉴别，并通过系统审计来记录用户的操作和所造成的影响，使用监督和事后评判等机制，保证用户的责任可追溯、行为得到控制。

——在物理上分离的部件之间传递信息流应遵从数据库管理系统中所确定的信息流策略；

——数据库管理系统所保护的资源仅限于需要了解该资源的授权用户知晓并进行访问和修改；

标准分享网 www.bzfxw.com 免费下载

——数据库管理系统应维护主体及客体的敏感标记(安全级别),以此做为实施访问控制的基础;

——在数据库管理系统的空闲存储客体空间中,对客体初始指定、分配或再分配前,需要撤销客体所含信息的所有授权;

——当主体获得对一个已被释放的客体的访问权时,当前主体不能获得原主体活动所产生的任何信息。