ICS 35.020
L 80

中华人民共和国国家标准

GB/T 25063—2010

信息安全技术
服务器安全测评要求

Information security technology—
Testing and evaluation requirement for server security

2010-09-02 发布　　2011-02-01 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

中 华 人 民 共 和 国
国 家 标 准
信息安全技术
服务器安全测评要求
GB/T 25063—2010
*
中国标准出版社出版发行
北京复兴门外三里河北街 16 号
邮政编码:100045
网址 www.spc.net.cn
电话:68523946 68517548
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 2.25 字数 65 千字
2010 年 11 月第一版 2010 年 11 月第一次印刷
*
书号:155066·1-40582

目　　次

前　言

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：浪潮集团有限公司、公安部计算机信息系统安全产品质量监督检验中心。

本标准主要起草人：黄涛、孙大军、刘刚、沈亮、李清玉、颜斌、顾建、顾伟。

引　言

本标准是与GB/T 21028—2007相配套的测评标准，用以指导测评人员从信息安全等级保护的角度对服务器安全进行的测评。

本标准按照GB/T 21028—2007关于服务器5个安全保护等级划分的要求，分别从硬件系统、操作系统、数据库管理系统、应用系统、运行安全、SSOS自身安全保护、SSOS设计和实现和SSOS安全管理等8个方面规定了服务器不同安全等级的测评要求。

关于不同安全等级中逐步增强的服务器安全测评要求，在第4章至第7章的描述中，每一级的新增部分用“**黑体字**”表示。

信息安全技术
服务器安全测评要求

1 范围

本标准规定了服务器安全的测评要求，包括第一级、第二级、第三级和第四级服务器安全测评要求。本标准没有规定第五级服务器安全测评的具体内容要求。

本标准适用于测评机构从信息安全等级保护的角度对服务器安全进行的测评工作。信息系统的主管部门及运营使用单位、服务器软硬生产厂商也可参考使用。

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)或修订版都不适用于本标准，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。凡不注日期的引用文件，其最新版本适用于本标准。

GB/T 5271.8—2001 信息技术 词汇 第8部分：安全(ISO/IEC 2382-8：1998，IDT)

GB 17859—1999 计算机信息系统 安全保护等级划分准则

GB/T 21028—2007 信息安全技术 服务器安全技术要求

3 术语和定义、缩略语

3.1 术语和定义

GB/T 5271.8—2001、GB 17859—1999 和 GB/T 21028—2007 确立的以及下列术语和定义适用于本标准。

3.1.1

检查 examination

测评人员对测评对象采用观察、查验、分析等方法进行静态评估的活动。

3.1.2

测试 testing

测评人员遵循相关的流程，对测评对象采用预定的方法/工具使其产生特定行为的活动。

3.1.3

评价 evaluation

测评人员依据检查和测试获取的信息，对测评对象进行综合分析，确定与技术要求是否一致的活动。

3.2 缩略语

SSOS 服务器安全子系统 security subsystem of server

SSF SSOS 安全功能 SSOS security function

SFP 安全功能策略 security function policy

SSC SSF 控制范围 SSF scope of control

SSP SSOS 安全策略 SSOS security policy

4 第一级安全测评

4.1 硬件系统

4.1.1 设备标签

对第一级设备标签的测评要求包括：

a) 测评者应检查服务器机箱，查看其是否可在显著位置设置标签；

b) 测评者应检查服务器是否设置了设备标签，以及该标签包含的信息；

c) 依据以上检查所获取的信息给出评价意见，确定是否符合 GB/T 21028—2007 中 5.1.1.1.1 规定的要求。

4.1.2 设备可靠运行支持

对第一级设备可靠运行支持的测评要求包括：

a) 测评者应根据服务器硬件配置清单，检查服务器主要部件（CPU、内存等）是否具有数据校验功能；

b) 测评者应检查服务器硬件在启动过程中的自检信息及操作提示是否与使用说明书保持一致；

c) 测评者应对安装于服务器中的至少一款应用软件进行操作，测试其响应情况；

d) 依据以上检查和测试所获取的信息给出评价意见，确定是否符合 GB/T 21028—2007 中 5.1.1.1.2 规定的要求。

4.2 操作系统

4.2.1 身份鉴别

对第一级服务器中操作系统的身份鉴别功能的测评要求包括：

a) 测评者应检查操作系统是否提供了远程管理功能，如提供了远程管理，查看鉴别信息在网络传输过程中的保护措施；

b) 测评者应检查操作系统是否提供了身份鉴别措施（如用户名和口令等）；

c) 依据以上检查所获取的信息给出评价意见，确定是否符合 GB/T 21028—2007 中 5.1.1.2a）规定的要求。

4.2.2 自主访问控制

对第一级服务器中操作系统的自主访问控制功能的测评要求包括：

a) 测评者应检查操作系统的自主访问控制功能，查看其是否能对重要文件的访问权限进行限制，对系统不需要的服务、共享路径等可能被非授权访问的客体进行限制；

b) 测评者应检查操作系统中匿名/默认用户的访问权限是否能被禁用或者限制（如限定在有限的范围内）；

c) 依据以上检查所获取的信息给出评价意见，确定是否符合 GB/T 21028—2007 中 5.1.1.2b）规定的要求。

4.2.3 数据完整性

对第一级服务器中操作系统的数据完整性保护功能的测评要求包括：

a) 测评者应检查操作系统内部在传输用户数据时实现数据完整性保护功能的情况；

b) 测评者应模拟进行大数据量的数据传输或保存时出现异常中断情况，测试操作系统在异常情况下的回退功能以及保护数据完整性的情况；

c) 依据以上检查和测试所获取的信息给出评价意见，确定是否符合 GB/T 21028—2007 中 5.1.1.2c）规定的要求。

4.3 数据库管理系统

4.3.1 身份鉴别

对第一级服务器中数据库管理系统的身份鉴别功能的测评要求包括：

a) 测评者应检查数据库管理系统是否提供了远程管理，如提供了远程管理，查看鉴别信息在网络传输过程中的保护措施；

b) 测评者应检查数据库管理系统是否提供了身份鉴别措施（如用户名或口令等）；

c) 依据以上检查所获取的信息给出评价意见，确定是否符合 GB/T 21028—2007 中 5.1.1.3a）规定的要求。

4.3.2 自主访问控制

对第一级服务器中数据库管理系统的自主访问控制功能的测评要求包括：

a) 测评者应检查数据库管理系统的自主访问控制，查看其是否能明确主体对客体的访问权限（如目录表访问控制/存取控制表访问控制等）；

b) 测评者应检查数据库管理系统中匿名/默认用户的访问权限是否能被禁用或者限制（如限定在有限的范围内）；

c) 依据以上检查所获取的信息给出评价意见，确定是否符合 GB/T 21028—2007 中 5.1.1.3b）规定的要求。

4.3.3 数据完整性

对第一级服务器中数据库管理系统的数据完整性保护功能的测评要求包括：

a) 测评者应检查数据库管理系统内部在传输用户数据时实现数据完整性保护功能的情况；

b) 测评者应模拟数据库管理系统操作时出现递交失败等异常中断情况，测试数据库管理系统在异常情况下的回退功能以及保护数据完整性的情况；

c) 依据以上检查和测试所获取的信息给出评价意见，确定是否符合 GB/T 21028—2007 中 5.1.1.3c）规定的要求。

4.4 应用系统

4.4.1 身份鉴别

对第一级服务器中应用系统的身份鉴别功能的测评要求包括：

a) 测评者应检查应用系统是否提供专用的登录控制模块对登录用户进行身份标识和鉴别，具体采取什么鉴别控制措施；

b) 测评者应检查应用系统是否具有身份标识（如建立账号）和鉴别（如口令等）功能；

c) 测评者应检查应用是否提供了登录失败处理功能（如限制非法登录次数，登录失败次数超过设定值则结束会话等）；

d) 测评者应检查关键应用系统，查看其是否采取措施防止鉴别信息传输过程中被窃听；

e) 依据以上检查所获取的信息给出评价意见，确定是否符合 GB/T 21028—2007 中 5.1.1.4.1 规定的要求。

4.4.2 自主访问控制

对第一级服务器中应用系统的自主访问控制功能的测评要求包括：

a) 测评者应检查应用系统提供的访问控制措施，包括具体措施、访问控制策略等；

b) 测评者应测试系统是否提供访问控制功能控制用户组/用户对系统功能和用户数据的访问；

c) 测评者应检查系统是否有由授权主体设置用户对系统功能操作和对数据访问的权限的功能，是否限制默认用户访问权限；

d) 测评者应通过不同权限的用户登录系统并进行一些操作，检查其权限是否与设定的权限一致；

e) 依据以上检查和测试所获取的信息给出评价意见，确定是否符合 GB/T 21028—2007 中 5.1.1.4.2 规定的要求。

4.4.3 数据完整性

对第一级服务器中应用系统的数据完整性保护功能的测评要求包括：

a) 测评者应检查服务器应用系统用户数据在传输过程中是否具有完整性保证措施；

b) 测评者应检查应用系统设计/验收文档，查看其是否有关于用户数据在传输过程中采用的完整性保证措施的描述；

c) 测评者应检查应用系统是否配备检测/验证重要用户数据在传输过程中完整性受到破坏的功能；

d) 依据以上检查所获取的信息给出评价意见，确定是否符合 GB/T 21028—2007 中 5.1.1.4.3 规定的要求。

4.5 运行安全

4.5.1 恶意代码防护

对第一级服务器中恶意代码防护功能的测评要求包括：

a) 测评者应检查关键服务器，查看是否安装了相应的恶意代码防护软件；

b) 测评者应检查恶意代码软件防护软件的厂家、名称和恶意代码库版本号；

c) 测评者应检查服务器在启动时恶意代码防护软件的运行情况；

d) 依据以上检查所获取的信息给出评价意见，确定是否符合 GB/T 21028—2007 中 5.1.1.5.1 规定的要求。

4.5.2 备份与故障恢复

对第一级服务器中备份与故障恢复功能的测评要求包括：

a) 测评者应检查服务器中的软硬件系统是否具有对重要信息和部件进行备份的功能以及对重要信息和部件进行恢复的功能；

b) 测评者应检查服务器中软硬系统备份和恢复功能的配置是否正确；

c) 依据以上检查所获取的信息给出评价意见，确定是否符合 GB/T 21028—2007 中 5.1.1.5.2 规定的要求。

4.6 SSOS 自身安全保护

对第一级服务器中 SSOS 自身安全保护的测评要求包括：

a) 测评者应检查说明文档，查看 SSF 防物理篡改的描述；

b) 测评者应检查设计文档，查看 SSOS 内 SSF 的安全结构定义形式；

c) 测评者应检查设计文档，查看 SSOS 内 SSF 数据传输时的保护机制的描述；

d) 测评者应检查设计文档，查看在 SSF 发生确定故障的情况下系统采取保护措施的描述；

e) 测评者应检查设计文档，查看会话建立管理机制的描述；

f) 测评者应检查 SSOS 自身安全保护功能的配置是否符合用户操作指南的要求；

g) 依据以上检查所获取的信息给出评价意见，确定是否符合 GB/T 21028—2007 中 5.1.2.1 规定的要求。

4.7 SSOS 设计和实现

对第一级服务器中 SSOS 设计和实现的测评要求包括：

a) 测评者应检查版本号与 SSOS 样本的一致性情况；

b) 测评者应检查分发文档，查看是否包含了 SSOS 的安装、生成和启动过程；

c) 测评者应检查同产品一起交付的操作文档，查看是否包含了维护 SSOS 安全所必须的所有过程；

d) 测评者应检查设计文档，查看 SSF 的设计方法，以及接口、子系统的非形式化描述；

e) 测评者应检查指导性文档是否包括安全管理员指南和用户指南，以及指南内容的完整性情况；

f) 测评者应检查生存周期支持文档，查看开发、操作和维护 SSOS 的描述，以及用于描述产品生存周期进行管理的活动记录；

g) 测评者应检查自测文档的有效性和内容的完整性；

h) 依据以上检查所获取的信息给出评价意见，确定是否符合 GB/T 21028—2007 中 5.1.2.2 规定的要求。

4.8 SSOS 安全管理

对第一级服务器中 SSOS 安全管理的测评要求包括：

a) 测评者应检查开发人员的安全规章制度、开发人员的安全教育培训制度和记录；

b) 测评者应检查开发场所的出入口控制制度和记录，开发环境的防火防盗措施和国家有关部门的许可文件；

c) 测评者应检查开发主机使用管理和记录，设备的购置、修理、处置的制度和记录，上网管理，计算机病毒管理和记录等；

d) 测评者应检查产品代码、文档、样机进行受控管理的制度和记录；

e) 依据以上检查所获取的信息给出评价意见，确定是否符合 GB/T 21028—2007 中 5.1.2.3 规定的要求。

5 第二级安全测评

5.1 硬件系统

5.1.1 设备标签

对第二级设备标签的测评要求包括：

a) 测评者应检查服务器机箱，查看其是否可在显著位置设置标签；

b) 测评者应检查服务器是否设置了设备标签，以及该标签包含的信息；

c) 测评者应检查服务器关键部件（包括硬盘、主板、内存、处理器、网卡等组件、附件）是否设置了标签；

d) 测评者应检查服务器设备标签是否采取有效的保护措施；

e) 依据以上检查所获取的信息给出评价意见，确定是否符合 GB/T 21028—2007 中 5.2.1.1.1 规定的要求。

5.1.2 设备可靠运行支持

对第二级设备可靠运行支持的测评要求包括：

a) 测评者应根据服务器硬件配置清单，检查服务器主要部件（CPU、内存等）是否具有数据校验功能；

b) 测评者应检查关键部件（包括硬盘、主板、内存、处理器、网卡等）与其标签配合的情况，以及机箱面板的保护措施；

c) 测评者应检查服务器硬件在启动过程中的自检信息及操作提示是否与使用说明书保持一致；

d) 测评者应对安装于服务器中的至少一款应用软件进行操作，测试其响应情况；

e) 依据以上检查和测试所获取的信息给出评价意见，确定是否符合 GB/T 21028—2007 中 5.2.1.1.2 规定的要求。

5.1.3 设备电磁防护

对第二级设备电磁防护的测评要求包括：

a) 测评者应检查服务器设备电磁防护指标是否符合国家规定的要求；

b) 依据以上检查所获取的信息给出评价意见，确定是否符合 GB/T 21028—2007 中 5.2.1.1.3 规定的要求。

5.2 操作系统

5.2.1 身份鉴别

对第二级服务器中操作系统的身份鉴别功能的测评要求包括：

a) 测评者应检查操作系统是否提供了远程管理功能，如提供了远程管理，查看鉴别信息在网络传输过程中的保护措施；

b) 测评者应检查操作系统账户列表，查看管理员用户名分配是否能保持唯一性；

c) 测评者应检查操作系统是否提供了身份鉴别措施（如用户名和强化管理的口令等）；

d) 测评者应检查操作系统是否提供鉴别失败处理功能，并能配置非法登录次数的限制值；

e) 测评者应通过错误的用户名和口令试图登录系统，验证鉴别失败处理功能是否有效；

f) 依据以上检查和测试所获取的信息给出评价意见，确定是否符合 GB/T 21028—2007 中 5.2.1.2a）规定的要求。

5.2.2 自主访问控制

对第二级服务器中操作系统的自主访问控制功能的测评要求包括：

a) 测评者应检查操作系统的自主访问控制功能，查看其是否能对重要文件的访问权限进行限制，对系统不需要的服务、共享路径等可能被非授权访问的客体进行限制；

b) 测评者应检查操作系统中匿名/默认用户的访问权限是否能被禁用或者限制（如限定在有限的范围内）；

c) 测评者应检查操作系统的访问控制列表，查看是否能通过访问控制列表获取到用户和权限的对应关系；

d) 测评者应通过审计日志记录，检查日志记录与自主访问控制中的主体相关联的情况；

e) 测评者应依据系统访问控制的安全策略，试图以未授权用户身份/角色访问客体，验证是否不能进行访问。

f) 依据以上检查和测试所获取的信息给出评价意见，确定是否符合 GB/T 21028—2007 中 5.2.1.2b）规定的要求。

5.2.3 安全审计

对第二级服务器中操作系统的安全审计功能的测评要求包括：

a) 测评者应检查安全审计功能的策略，以及审计日志的处理方式；

b) 测评者应通过审计策略和记录，检查审计范围是否能够覆盖系统内重要的安全相关事件，例如，用户标识与鉴别、重要用户行为、系统资源的异常使用、重要系统命令的使用（如删除客体）等；

c) 测评者应检查审计记录信息是否包括事件发生的日期与时间、触发事件的主体与客体、事件的类型、事件成功或失败、身份鉴别事件中请求的来源（如末端标识符）、事件的结果等内容；

d) 测评者应检查审计跟踪设置是否提供定义审计跟踪极限的阈值的功能，当存储空间被耗尽时，能否采取必要的保护措施；

e) 依据以上检查所获取的信息给出评价意见，确定是否符合 GB/T 21028—2007 中 5.2.1.2c）规定的要求。

5.2.4 数据完整性

对第二级服务器中操作系统的数据完整性保护功能的测评要求包括：

a) 测评者应检查操作系统内部在传输鉴别信息和用户数据时实现数据完整性保护功能的情况；

b) 测评者应检查操作系统在存储鉴别信息和重要用户数据时的完整性保护功能；

c) 测评者应模拟进行大数据量的数据传输或保存时出现异常中断情况，测试操作系统在异常情况下的回退功能以及保护数据完整性的情况；

d) 依据以上检查和测试所获取的信息给出评价意见，确定是否符合 GB/T 21028—2007 中

5.2.1.2d)规定的要求。

5.2.5 数据保密性

对第二级服务器中操作系统的数据保密性功能的测评要求包括：

a) 测评者应检查鉴别信息和敏感的用户数据是否采用加密或其他有效措施实现存储保密性；

b) 依据以上检查所获取的信息给出评价意见，确定是否符合 GB/T 21028—2007 中 5.2.1.2e)规定的要求。

5.3 数据库管理系统

5.3.1 身份鉴别

对第二级服务器中数据库管理系统的身份鉴别功能的测评要求包括：

a) 测评者应检查数据库管理系统是否提供了远程管理，如提供了远程管理，查看鉴别信息在网络传输过程中的保护措施；

b) 测评者应检查数据库管理系统账户列表，查看管理员用户名分配是否能保持唯一性；

c) 测评者应检查数据库管理系统是否提供了身份鉴别措施(如用户名或口令等)；

d) 测评者应检查数据库管理系统是否提供鉴别失败处理功能，并能配置非法登录次数的限制值；

e) 测评者应通过错误的用户名和口令试图登录系统，验证鉴别失败处理功能是否有效；

f) 依据以上检查和测试所获取的信息给出评价意见，确定是否符合 GB/T 21028—2007 中 5.2.1.3a)规定的要求。

5.3.2 自主访问控制

对第二级服务器中数据库管理系统的自主访问控制功能的测评要求包括：

a) 测评者应检查数据库管理系统的自主访问控制，查看其是否能明确主体对客体的访问权限(如目录表访问控制/存取控制表访问控制等)；

b) 测评者应检查数据库管理系统中匿名/默认用户的访问权限是否能被禁用或者限制(如限定在有限的范围内)；

c) 测评者应检查数据库管理系统的访问控制列表，查看是否能通过访问控制列表获取到用户和权限的对应关系；

d) 测评者应通过审计日志记录，检查其与自主访问控制中的主体相关联的情况；

e) 测评者应依据系统访问控制的安全策略，试图以未授权用户身份/角色访问客体，验证是否不能进行访问；

f) 依据以上检查和测试所获取的信息给出评价意见，确定是否符合 GB/T 21028—2007 中 5.2.1.3b)规定的要求。

5.3.3 安全审计

对第二级服务器中数据库管理系统的安全审计功能的测评要求包括：

a) 测评者应检查安全审计功能的策略，以及审计日志的处理方式；

b) 测评者应通过审计策略和记录，检查审计范围是否能够覆盖系统内重要的安全相关事件，例如，用户标识与鉴别、重要用户行为、系统资源的异常使用、重要系统命令的使用(如删除客体)等；

c) 测评者应检查审计记录信息是否包括事件发生的日期与时间、触发事件的主体与客体、事件的类型、事件成功或失败、身份鉴别事件中请求的来源(如末端标识符)、事件的结果等内容；

d) 测评者应检查审计跟踪设置是否提供定义审计跟踪极限的阈值的功能，当存储空间被耗尽时，能否采取必要的保护措施；

e) 依据以上检查所获取的信息给出评价意见，确定是否符合 GB/T 21028—2007 中 5.2.1.3c)规定的要求。

5.3.4 数据完整性

对第二级服务器中数据库管理系统的数据完整性保护功能的测评要求包括：

a) 测评者应检查数据库管理系统内部在传输鉴别信息和用户数据时实现数据完整性保护功能的情况；

b) 测评者应检查数据库管理系统在存储鉴别信息和重要用户数据时的完整性保护功能；

c) 测评者应模拟数据库管理系统操作时出现递交失败等异常中断情况，测试数据库管理系统在异常情况下的回退功能以及保护数据完整性的情况；

d) 依据以上检查和测试所获取的信息给出评价意见，确定是否符合 GB/T 21028—2007 中 5.2.1.3d)规定的要求。

5.3.5 数据保密性

对第二级服务器中数据库管理系统的数据保密性功能的测评要求包括：

a) 测评者应检查鉴别信息和敏感的用户数据是否采用加密或其他有效措施实现存储保密性；

b) 依据以上检查所获取的信息给出评价意见，确定是否符合 GB/T 21028—2007 中 5.2.1.3e)规定的要求。

5.4 应用系统

5.4.1 身份鉴别

对第二级服务器中应用系统的身份鉴别功能的测评要求包括：

a) 测评者应检查应用系统是否提供专用的登录控制模块对登录用户进行身份标识和鉴别，具体采取什么鉴别控制措施；

b) 测评者应检查应用系统是否能保证用户标识的唯一性(如 UID、用户名或其他信息在系统中是唯一的，用该标识能唯一识别该用户)；

c) 测评者应检查应用系统是否具有身份标识(如建立账号)和鉴别(如口令等)功能；

d) 测评者应检查应用是否提供了登录失败处理功能(如限制非法登录次数，登录失败次数超过设定值则结束会话等)；

e) 测评者应检查关键应用系统，查看其是否采取措施防止鉴别信息传输过程中被窃听；

f) 测评者应通过已注册用户身份登录系统，查看登录是否成功，验证其身份标识和鉴别功能是否有效；

g) 测评者应通过错误的用户名和口令试图登录系统，验证鉴别失败处理功能是否有效；

h) 依据以上检查和测试所获取的信息给出评价意见，确定是否符合 GB/T 21028—2007 中 5.2.1.4.1规定的要求。

5.4.2 自主访问控制

对第二级服务器中应用系统的自主访问控制功能的测评要求包括：

a) 测评者应检查应用系统提供的访问控制措施，包括具体措施、访问控制策略等；

b) 测评者应检查系统是否提供访问控制功能控制用户组/用户对系统功能和用户数据的访问；

c) 测评者应检查系统是否有由授权主体设置用户对系统功能操作和对数据访问的权限的功能，是否限制默认用户访问权限；

d) 测评者应通过不同权限的用户登录系统并进行一些操作，检查其权限是否与设定的权限一致；

e) 测评者应检查应用系统的访问控制列表，查看是否能通过访问控制列表获取到用户和权限的对应关系；

f) 测评者应通过审计日志记录，检查日志记录与自主访问控制中的主体相关联的情况；

g) 依据以上检查所获取的信息给出评价意见，确定是否符合 GB/T 21028—2007 中 5.2.1.4.2 规定的要求。

5.4.3 安全审计

对第二级服务器中应用系统的安全审计功能的测评要求包括：

a) 测评者应检查安全审计功能的策略，以及审计日志的处理方式；

b) 测评者应通过审计策略和记录，检查审计范围是否能够覆盖系统内重要的安全相关事件，例如，用户标识与鉴别、重要用户行为、系统资源的异常使用、重要系统命令的使用（如删除客体）等；

c) 测评者应检查审计记录信息是否包括事件发生的日期与时间、触发事件的主体与客体、事件的类型、事件成功或失败、身份鉴别事件中请求的来源（如末端标识符）、事件的结果等内容；

d) 测评者应检查审计跟踪设置是否提供定义审计跟踪极限的阈值的功能，当存储空间被耗尽时，能否采取必要的保护措施；

e) 测评者应以某个用户试图产生一些重要的安全相关事件（如鉴别失败等），测试安全审计的覆盖情况和记录情况与要求是否一致；

f) 测评者应以某个系统用户试图删除、修改或覆盖审计记录，测试安全审计的保护情况与要求是否一致；

g) 依据以上检查和测试所获取的信息给出评价意见，确定是否符合 GB/T 21028—2007 中 5.2.1.4.3规定的要求。

5.4.4 数据完整性

对第二级服务器中应用系统的数据完整性保护功能的测评要求包括：

a) 测评者应检查服务器应用系统用户数据在传输过程中是否具有完整性保证措施；

b) 测评者应检查应用系统设计/验收文档，查看其是否有关于用户数据在传输过程中采用的完整性保证措施的描述；

c) 测评者应检查应用系统是否配备检测/验证重要用户数据在传输过程中完整性受到破坏的功能；

d) 依据以上检查所获取的信息给出评价意见，确定是否符合 GB/T 21028—2007 中 5.2.1.4.4 规定的要求。

5.4.5 数据保密性

对第二级服务器中应用系统的数据保密性功能的测评要求包括：

a) 测评者应检查鉴别信息和敏感的用户数据是否采用加密或其他有效措施实现存储保密性；

b) 测评者应检查应用系统设计/验收文档，查看其是否有关于其鉴别信息、敏感的用户数据采用加密或其他有效措施实现存储保密性的描述；

c) 依据以上检查所获取的信息给出评价意见，确定是否符合 GB/T 21028—2007 中 5.2.1.4.5 规定的要求。

5.5 运行安全

5.5.1 恶意代码防护

对第二级服务器中恶意代码防护功能的测评要求包括：

a) 测评者应检查关键服务器，查看是否安装了相应的恶意代码防护软件；

b) 测评者应检查恶意代码软件防护软件的厂家、名称和恶意代码库版本号；

c) 测评者应检查服务器在启动时恶意代码防护软件的运行情况；

d) 测评者应检查恶意代码防护软件的事件日志，查看安全策略执行的有效性；

e) 测评者应检查恶意代码防护软件是否由统一的管理平台进行集中管理；

f) 依据以上检查所获取的信息给出评价意见，确定是否符合 GB/T 21028—2007 中 5.2.1.5.1 规定的要求。

5.5.2 备份与故障恢复

对**第二级**服务器中备份与故障恢复功能的测评要求包括：

a) 测评者应检查服务器中的软硬件系统是否具有对重要信息和部件进行备份的功能以及对重要信息和部件进行恢复的功能；

b) 测评者应检查服务器中软硬系统备份和恢复功能的配置是否正确；

c) 测评者应检查服务器中关键部件是否采取了冗余措施；

d) 依据以上检查所获取的信息给出评价意见，确定是否符合 **GB/T** 21028—2007 **中** 5.2.1.5.2 规定的要求。

5.6 SSOS 自身安全保护

对**第二级**服务器中 SSOS 自身安全保护的测评要求包括：

a) 测评者应检查说明文档，查看 SSF 防物理篡改的描述；

b) 测评者应检查设计文档，查看 SSOS 内 SSF 的安全结构定义形式；

c) 测评者应检查设计文档，查看 SSOS 内 SSF 数据传输时的保护机制**和数据恢复**的描述；

d) 测评者应检查设计文档，查看在 SSF 发生确定故障的情况下系统采取保护措施的描述；

e) 测评者应检查设计文档，查看会话建立管理机制的描述**和审计记录**；

f) 测评者应检查 SSOS 自身安全保护功能的配置是否符合用户操作指南的要求；

g) 依据以上检查所获取的信息给出评价意见，确定是否符合 **GB/T** 21028—2007 **中** 5.2.2.1 规定的要求。

5.7 SSOS 设计和实现

对**第二级**服务器中 SSOS 设计和实现的测评要求包括：

a) 测评者应检查版本号与 SSOS 样本的一致性情况，**以及在产品开发、测试和维护期间的日志记录**；

b) 测评者应检查分发文档，查看是否包含了 SSOS 的安装、生成和启动过程；

c) 测评者应检查同产品一起交付的操作文档，查看是否包含了维护 SSOS 安全所必须的所有过程；

d) 测评者应检查设计文档，查看 SSF 的设计方法，以及接口、子系统的非形式化描述；

e) 测评者应检查指导性文档是否包括安全管理员指南和用户指南，以及指南内容的完整性情况；

f) 测评者应检查生存周期支持文档，查看开发、操作和维护 SSOS 的描述，以及用于描述产品生存周期进行管理的活动记录；

g) 测评者应检查自测文档的有效性和内容的完整性；

h) 依据以上检查所获取的信息给出评价意见，确定是否符合 **GB/T** 21028—2007 **中** 5.2.2.2 规定的要求。

5.8 SSOS 安全管理

对**第二级**服务器中 SSOS 安全管理的测评要求包括：

a) 测评者应检查开发人员的安全规章制度、开发人员的安全教育培训制度和记录；

b) 测评者应检查开发场所的出入口控制制度和记录，开发环境的防火防盗措施和国家有关部门的许可文件；

c) 测评者应检查开发主机使用管理和记录，设备的购置、修理、处置的制度和记录，上网管理，计算机病毒管理和记录等；

d) 测评者应检查产品代码、文档、样机进行受控管理的制度和记录；

e) 依据以上检查所获取的信息给出评价意见，确定是否符合 **GB/T** 21028—2007 **中** 5.2.2.3 规定的要求。

6 第三级安全测评

6.1 硬件系统

6.1.1 设备标签

对**第三级**设备标签的测评要求包括：

a) 测评者应检查服务器机箱，查看其是否可在显著位置设置标签；

b) 测评者应检查服务器是否设置了设备标签，以及该标签包含的信息；

c) 测评者应检查服务器关键部件（包括硬盘、主板、内存、处理器、网卡等组件、附件）是否设置了标签；

d) 测评者应检查服务器设备标签是否采取有效的保护措施；

e) 依据以上检查所获取的信息给出评价意见，确定是否符合 **GB/T** 21028—2007 中 5.3.1.1.1 规定的要求。

6.1.2 设备可靠运行支持

对**第三级**设备可靠运行支持的测评要求包括：

a) 测评者应根据服务器硬件配置清单，检查服务器主要部件（CPU、内存等）是否具有数据校验功能；

b) 测评者应检查关键部件（包括硬盘、主板、内存、处理器、网卡等）与其标签配合的情况，以及机箱面板的保护措施；

c) 测评者应检查硬盘、风扇和电源的热插拔功能，内存的容错功能，以及电源、硬盘的冗余措施；

d) 测评者应检查服务器硬件在启动过程中的自检信息及操作提示是否与使用说明书保持一致；

e) 测评者应对安装于服务器中的至少一款应用软件进行操作，测试其响应情况；

f) 依据以上检查和测试所获取的信息给出评价意见，确定是否符合 **GB/T** 21028—2007 中 5.3.1.1.2 规定的要求。

6.1.3 设备工作状态监控

对第三级设备工作状态监控的测评要求包括：

a) 测评者应检查服务器中电源、风扇、机箱、磁盘控制等关键部件是否具备可管理接口；

b) 测评者应检查是否通过可管理接口实现了对关键部件的监控功能，并对其进行操作，验证其功能的有效性；

c) 测评者应模拟上述部件发生故障，测试其报警功能；

d) 依据以上检查和测试所获取的信息给出评价意见，确定是否符合 GB/T 21028—2007 中 5.3.1.1.3 规定的要求。

6.1.4 设备电磁防护

对**第三级**设备电磁防护的测评要求包括：

a) 测评者应检查服务器设备电磁防护指标是否符合国家规定的要求；

b) 依据以上检查所获取的信息给出评价意见，确定是否符合 **GB/T** 21028—2007 中 5.3.1.1.4 规定的要求。

6.2 操作系统

6.2.1 身份鉴别

对**第三级**服务器中操作系统的身份鉴别功能的测评要求包括：

a) 测评者应检查操作系统是否提供了远程管理功能，如提供了远程管理，查看鉴别信息在网络传输过程中的保护措施；

b) 测评者应检查操作系统账户列表，查看管理员用户名分配是否能保持唯一性；

c) 测评者应检查操作系统是否提供了身份鉴别措施（如用户名和强化管理的口令等）；

d) **测评者应检查是否提供两个及两个以上身份鉴别技术的组合来进行身份鉴别(如采用用户名/口令、挑战应答、动态口令、物理设备、生物识别技术和数字证书方式的身份鉴别技术中的任意两个组合);**

e) 测评者应检查操作系统是否提供鉴别失败处理功能,并能配置非法登录次数的限制值;

f) 测评者应通过错误的用户名和口令试图登录系统,验证鉴别失败处理功能是否有效;

g) **测评者应通过渗透性测试对操作系统进行用户口令强度进行测试,查看能否破解用户口令,破解口令后能否登录进入系统;**

h) **测评者应通过性渗透测试来检查是否存在绕过认证方式进行系统登录的方法,例如,认证程序存在的安全漏洞,社会工程或其他手段等;**

i) 依据以上检查和测试所获取的信息给出评价意见,确定是否符合 **GB/T** 21028—2007 中 5.3.1.2**a**)规定的要求。

6.2.2 自主访问控制

对**第三级**服务器中操作系统的自主访问控制功能的测评要求包括:

a) 测评者应检查操作系统的自主访问控制功能,查看其是否能对重要文件的访问权限进行限制,对系统不需要的服务、共享路径等可能被非授权访问的客体进行限制;

b) 测评者应检查操作系统中匿名/默认用户的访问权限是否能被禁用或者限制(如限定在有限的范围内);

c) 测评者应检查操作系统的访问控制列表,查看是否能通过访问控制列表获取到用户和权限的对应关系;

d) 测评者应通过审计日志记录,检查日志记录与自主访问控制中的主体相关联的情况;

e) 测评者应依据系统访问控制的安全策略,试图以未授权用户身份/角色访问客体,验证是否不能进行访问;

f) **测评者应检查系统是否提供了特权用户权限分享的机制,如可分为系统管理员、安全管理员、安全审计员等;**

g) 依据以上检查和测试所获取的信息给出评价意见,确定是否符合 **GB/T** 21028—2007 中 5.3.1.2**b**)规定的要求。

6.2.3 标记

对第三级服务器中操作系统的标记功能的测评要求包括:

a) **测评者应检查操作系统是否提供对重要文件和用户设置标记的功能;**

b) **依据以上检查所获取的信息给出评价意见,确定是否符合 GB/T** 21028—2007 **中** 5.3.1.2**c**)**规定的要求。**

6.2.4 强制访问控制

对第三级服务器中操作系统的强制访问控制功能的测评要求包括:

a) **测评者应检查强制访问控制模型是否采用"向下读,向上写"模型,如果操作系统采用其他的强制访问控制模型,则操作系统文档是否对这种模型进行详细分析,并有权威机构对这种强制访问控制模型的合理性和完善性进行检测证明;**

b) **测评者应检查强制访问控制是否与用户身份鉴别、标识等安全功能密切配合,并且控制粒度达到主体为用户级,客体为文件;**

c) **测评者应依据系统文档描述测试强制访问控制模型,以授权用户和非授权用户身份访问客体,验证是否只有授权用户可以访问客体;**

d) **测评者应通过渗透测试检查是否可通过非法操作来终止强制访问模块,非法修改强制访问相关规则;**

e) **依据以上检查和测试所获取的信息给出评价意见,确定是否符合 GB/T** 21028—2007 **中**

5.3.1.2d)规定的要求。

6.2.5 数据流控制

对第三级服务器中操作系统的数据流控制功能的测评要求包括：

a) 测评者应检查数据在不同等级系统间的流动时是否提供了控制措施；

b) 依据以上检查所获取的信息给出评价意见，确定是否符合 GB/T 21028—2007 中5.3.1.2e)规定的要求。

6.2.6 安全审计

对第三级服务器中操作系统的安全审计功能的测评要求包括：

a) 测评者应检查安全审计功能的策略，以及审计日志的处理方式；

b) 测评者应通过审计策略和记录，检查审计范围是否能够覆盖系统内重要的安全相关事件，例如，用户标识与鉴别、重要用户行为、系统资源的异常使用、重要系统命令的使用(如删除客体)等；

c) 测评者应检查审计记录信息是否包括事件发生的日期与时间、触发事件的主体与客体、事件的类型、事件成功或失败、身份鉴别事件中请求的来源(如末端标识符)、事件的结果等内容；

d) 测评者应检查是否提供了浏览和分析审计数据提供专门的审计工具(如对审计记录进行分类、排序、查询、统计、分析和组合查询等)，并能根据需要生成审计报表；

e) 测评者应通过非法终止审计功能或修改其配置，验证审计功能是否受到保护；

f) 测评者应以某个系统用户试图删除、修改或覆盖审计记录，测试安全审计的保护情况与要求是否一致；

g) 测评者应检查审计跟踪设置是否提供定义审计跟踪极限的阈值的功能，当存储空间被耗尽时，能否采取必要的保护措施；

h) 依据以上检查和测试所获取的信息给出评价意见，确定是否符合 GB/T 21028—2007 中5.3.1.2f)规定的要求。

6.2.7 数据完整性

对第三级服务器中操作系统的数据完整性保护功能的测评要求包括：

a) 测评者应检查操作系统内部在传输鉴别信息和用户数据时实现数据完整性保护功能的情况；

b) 测评者应检查操作系统在存储鉴别信息和重要用户数据时的完整性保护功能；

c) 测评者应模拟进行大数据量的数据传输或保存时出现异常中断情况，测试操作系统在异常情况下的回退功能以及保护数据完整性的情况；

d) 依据以上检查和测试所获取的信息给出评价意见，确定是否符合 GB/T 21028—2007 中5.3.1.2g)规定的要求。

6.2.8 数据保密性

对第三级服务器中操作系统的数据保密性功能的测评要求包括：

a) 测评者应检查鉴别信息和敏感的用户数据是否采用加密或其他有效措施实现存储保密性；

b) 测评者应检查系统管理数据、鉴别信息是否采用了加密或其他有效措施实现传输保密性；

c) 依据以上检查所获取的信息给出评价意见，确定是否符合 GB/T 21028—2007 中 5.3.1.2h)规定的要求。

6.3 数据库管理系统

6.3.1 身份鉴别

对第三级服务器中数据库管理系统的身份鉴别功能的测评要求包括：

a) 测评者应检查数据库管理系统是否提供了远程管理，如提供了远程管理，查看鉴别信息在网络传输过程中的保护措施；

b) 测评者应检查数据库管理系统账户列表，查看管理员用户名分配是否能保持唯一性；

c) 测评者应检查数据库管理系统是否提供了身份鉴别措施(如用户名或口令等);

d) 测评者应检查是否提供两个及两个以上身份鉴别技术的组合来进行身份鉴别(如采用用户名/口令、挑战应答、动态口令、物理设备、生物识别技术和数字证书方式的身份鉴别技术中的任意两个组合);

e) 测评者应检查数据库管理系统是否提供鉴别失败处理功能,并能配置非法登录次数的限制值;

f) 测评者应通过错误的用户名和口令试图登录系统,验证鉴别失败处理功能是否有效;

g) 测评者应通过渗透性测试对数据库管理系统进行用户口令强度进行测试,查看能否破解用户口令,破解口令后能否登录进入系统;

h) 测评者应通过性渗透测试来检查是否存在绕过认证方式进行系统登录的方法,例如,认证程序存在的安全漏洞,社会工程或其他手段等;

i) 依据以上检查和测试所获取的信息给出评价意见,确定是否符合 **GB/T** 21028—2007 中 5.3.1.3**a**)规定的要求。

6.3.2 自主访问控制

对**第三级**服务器中数据库管理系统的自主访问控制功能的测评要求包括:

a) 测评者应检查数据库管理系统的自主访问控制,查看其是否能明确主体对客体的访问权限(如目录表访问控制/存取控制表访问控制等);

b) 测评者应检查数据库管理系统中匿名/默认用户的访问权限是否能被禁用或者限制(如限定在有限的范围内);

c) 测评者应检查数据库管理系统的访问控制列表,查看是否能通过访问控制列表获取到用户和权限的对应关系;

d) 测评者应通过审计日志记录,检查其与自主访问控制中的主体相关联的情况;

e) 测评者应依据系统访问控制的安全策略,试图以未授权用户身份/角色访问客体,验证是否不能进行访问;

f) 检查系统是否提供了特权用户权限分享的机制,如可分为系统管理员、安全管理员、安全审计员等;

g) 依据以上检查和测试所获取的信息给出评价意见,确定是否符合 **GB/T** 21028—2007 中 5.3.1.3**b**)规定的要求。

6.3.3 标记

对第三级服务器中数据库管理系统的标记功能的测评要求包括:

a) 测评者应检查数据库管理系统是否提供对重要数据表和用户设置标记的功能;

b) 依据以上检查所获取的信息给出评价意见,确定是否符合 GB/T 21028—2007 **中** 5.3.1.3**c**)**规定的要求。**

6.3.4 强制访问控制

对第三级服务器中数据库管理系统的强制访问控制功能的测评要求包括:

a) 测评者应检查强制访问控制模型是否采用"向下读,向上写"模型,如果数据库管理系统采用其他的强制访问控制模型,则操作系统文档是否对这种模型进行详细分析,并有权威机构对这种强制访问控制模型的合理性和完善性进行检测证明;

b) 测评者应检查强制访问控制是否与用户身份鉴别、标识等安全功能密切配合,并且控制粒度达到主体为用户级,客体为数据表;

c) 测评者应依据系统文档描述测试强制访问控制模型,以授权用户和非授权用户身份访问客体,验证是否只有授权用户可以访问客体;

d) 测评者应通过渗透测试检查是否可通过非法操作来终止强制访问模块,非法修改强制访问相关规则;

e) 依据以上检查和测试所获取的信息给出评价意见，确定是否符合 GB/T 21028—2007 中 5.3.1.3d)规定的要求。

6.3.5 数据流控制

对第三级服务器中数据库管理系统的数据流控制功能的测评要求包括：

a) 测评者应检查数据在不同等级系统间的流动时是否提供了控制措施；

b) 依据以上检查所获取的信息给出评价意见，确定是否符合 GB/T 21028—2007 中 5.3.1.3e)规定的要求。

6.3.6 安全审计

对第三级服务器中数据库管理系统的安全审计功能的测评要求包括：

a) 测评者应检查安全审计功能的策略，以及审计日志的处理方式；

b) 测评者应通过审计策略和记录，检查审计范围是否能够覆盖系统内重要的安全相关事件，例如，用户标识与鉴别、重要用户行为、系统资源的异常使用、重要系统命令的使用(如删除客体)等；

c) 测评者应检查审计记录信息是否包括事件发生的日期与时间、触发事件的主体与客体、事件的类型、事件成功或失败、身份鉴别事件中请求的来源(如末端标识符)、事件的结果等内容；

d) 测评者应检查是否提供了浏览和分析审计数据提供专门的审计工具(如对审计记录进行分类、排序、查询、统计、分析和组合查询等)，并能根据需要生成审计报表；

e) 测评者应通过非法终止审计功能或修改其配置，验证审计功能是否受到保护；

f) 测评者应以某个系统用户试图删除、修改或覆盖审计记录，测试安全审计的保护情况与要求是否一致；

g) 测评者应检查审计跟踪设置是否提供定义审计跟踪极限的阈值的功能，当存储空间被耗尽时，能否采取必要的保护措施；

h) 依据以上检查和测试所获取的信息给出评价意见，确定是否符合 GB/T 21028—2007 中 5.3.1.3f)规定的要求。

6.3.7 数据完整性

对第三级服务器中数据库管理系统的数据完整性保护功能的测评要求包括：

a) 测评者应检查数据库管理系统内部在传输鉴别信息和用户数据时实现数据完整性保护功能的情况；

b) 测评者应检查数据库管理系统在存储鉴别信息和重要用户数据时的完整性保护功能；

c) 测评者应模拟数据库管理系统操作时出现递交失败等异常中断情况，测试数据库管理系统在异常情况下的回退功能以及保护数据完整性的情况；

d) 依据以上检查和测试所获取的信息给出评价意见，确定是否符合 GB/T 21028—2007 中 5.3.1.3g)规定的要求。

6.3.8 数据保密性

对第三级服务器中数据库管理系统的数据保密性功能的测评要求包括：

a) 测评者应检查鉴别信息和敏感的用户数据是否采用加密或其他有效措施实现存储保密性；

b) 测评者应检查系统管理数据、鉴别信息是否采用了加密或其他有效措施实现传输保密性；

c) 依据以上检查所获取的信息给出评价意见，确定是否符合 GB/T 21028—2007 中 5.3.1.3h)规定的要求。

6.4 应用系统

6.4.1 身份鉴别

对第三级服务器中应用系统的身份鉴别功能的测评要求包括：

a) 测评者应检查应用系统是否提供专用的登录控制模块对登录用户进行身份标识和鉴别，具体

采取什么鉴别控制措施；

b) 测评者应检查应用系统是否能保证用户标识的唯一性(如 UID、用户名或其他信息在系统中是唯一的,用该标识能唯一识别该用户)；

c) 测评者应检查应用系统是否具有身份标识(如建立账号)和鉴别(如口令等)功能；

d) 测评者应检查是否提供两个及两个以上身份鉴别技术的组合来进行身份鉴别(如采用用户名/口令、挑战应答、动态口令、物理设备、生物识别技术和数字证书方式的身份鉴别技术中的任意两个组合)；

e) 测评者应检查应用是否提供了登录失败处理功能(如限制非法登录次数,登录失败次数超过设定值则结束会话等)；

f) 测评者应检查关键应用系统,查看其是否采取措施防止鉴别信息传输过程中被窃听；

g) 测评者应通过已注册用户身份登录系统,查看登录是否成功,验证其身份标识和鉴别功能是否有效；

h) 测评者应通过错误的用户名和口令试图登录系统,验证鉴别失败处理功能是否有效；

i) 依据以上检查和测试所获取的信息给出评价意见,确定是否符合 GB/T 21028—2007 中 5.3.1.4.1规定的要求。

6.4.2 自主访问控制

对第三级服务器中应用系统的自主访问控制功能的测评要求包括：

a) 测评者应检查应用系统提供的访问控制措施,包括具体措施、访问控制策略等；

b) 测评者应测试系统是否提供访问控制功能控制用户组/用户对系统功能和用户数据的访问；

c) 测评者应检查系统是否有由授权主体设置用户对系统功能操作和对数据访问的权限的功能,是否限制默认用户访问权限；

d) 测评者应通过不同权限的用户登录系统并进行一些操作,检查其权限是否与设定的权限一致；

e) 测评者应检查应用系统的访问控制列表,查看是否能通过访问控制列表获取到用户和权限的对应关系；

f) 测评者应通过审计日志记录,检查日志记录与自主访问控制中的主体相关联的情况；

g) 测评者应检查应用系统是否提供了特权用户的权限分离功能(如系统管理员只能对系统进行维护,安全管理员只能进行策略配置和安全设置,安全审计员只能维护审计信息等)；

h) 依据以上检查和测试所获取的信息给出评价意见,确定是否符合 GB/T 21028—2007 中 5.3.1.4.2规定的要求。

6.4.3 标记

对第三级服务器中应用系统的标记功能的测评要求包括：

a) 测评者应检查应用系统是否提供对重要数据和用户设置标记的功能；

b) 依据以上检查所获取的信息给出评价意见,确定是否符合 GB/T 21028—2007 中 5.3.1.4.3 规定的要求。

6.4.4 强制访问控制

对第三级服务器中应用系统的强制访问控制功能的测评要求包括：

a) 测评者应检查应用系统是否提供了强制访问控制功能,以及该功能模型的合理性和完善性；

b) 测评者应检查强制访问控制是否与用户身份鉴别、标识等安全功能密切配合；

c) 测评者应依据系统文档描述测试强制访问控制模型,以授权用户和非授权用户身份访问客体,验证是否只有授权用户可以访问客体；

d) 测评者应通过渗透测试检查是否可通过非法操作来终止强制访问模块,非法修改强制访问相关规则；

e) 依据以上检查和测试所获取的信息给出评价意见,确定是否符合 GB/T 21028—2007 中

5.3.1.4.4规定的要求。

6.4.5 数据流控制

对第三级服务器中应用系统的数据流控制功能的测评要求包括：

a) 测评者应检查数据在不同等级应用系统间的流动时是否提供了控制措施；

b) 依据以上检查所获取的信息给出评价意见，确定是否符合GB/T 21028—2007中5.3.1.4.5规定的要求。

6.4.6 安全审计

对第三级服务器中应用系统的安全审计功能的测评要求包括：

a) 测评者应检查安全审计功能的策略，以及审计日志的处理方式；

b) 测评者应通过审计策略和记录，检查审计范围是否能够覆盖系统内重要的安全相关事件，例如，用户标识与鉴别、重要用户行为、系统资源的异常使用、重要系统命令的使用(如删除客体)等；

c) 测评者应检查审计记录信息是否包括事件发生的日期与时间、触发事件的主体与客体、事件的类型、事件成功或失败、身份鉴别事件中请求的来源(如末端标识符)、事件的结果等内容；

d) 测评者应检查审计跟踪设置是否提供定义审计跟踪极限的阈值的功能，当存储空间被耗尽时，能否采取必要的保护措施；

e) 测评者应检查应用系统是否提供了浏览和分析审计数据提供专门的审计工具(如对审计记录进行分类、排序、查询、统计、分析和组合查询等)，并能根据需要生成审计报表；

f) 测评者应通过非法终止审计功能或修改其配置，验证审计功能是否受到保护；

g) 测评者应以某个系统用户试图删除、修改或覆盖审计记录，测试安全审计的保护情况与要求是否一致；

h) 测评者应以某个用户试图产生一些重要的安全相关事件(如鉴别失败等)，测试安全审计的覆盖情况和记录情况与要求是否一致；

i) 测评者应以某个系统用户试图删除、修改或覆盖审计记录，测试安全审计的保护情况与要求是否一致；

j) 依据以上检查和测试所获取的信息给出评价意见，确定是否符合GB/T 21028—2007中5.3.1.4.6规定的要求。

6.4.7 数据完整性

对第三级服务器中应用系统的数据完整性保护功能的测评要求包括：

a) 测评者应检查服务器应用系统用户数据在传输过程中是否具有完整性保证措施；

b) 测评者应检查应用系统设计/验收文档，查看其是否有关于用户数据在传输过程中采用的完整性保证措施的描述；

c) 测评者应检查应用系统是否配备检测/验证重要用户数据在传输过程中完整性受到破坏的功能；

d) 依据以上检查所获取的信息给出评价意见，确定是否符合GB/T 21028—2007中5.3.1.4.7规定的要求。

6.4.8 数据保密性

对第三级服务器中应用系统的数据保密性功能的测评要求包括：

a) 测评者应检查鉴别信息和敏感的用户数据是否采用加密或其他有效措施实现存储保密性；

b) 测评者应检查应用系统设计/验收文档，查看其是否有关于其鉴别信息、敏感的用户数据采用加密或其他有效措施实现存储保密性的描述；

c) 依据以上检查所获取的信息给出评价意见，确定是否符合GB/T 21028—2007中5.3.1.4.8规定的要求。

6.5 运行安全

6.5.1 安全监控

对第三级服务器中安全监控功能的测评要求包括：

a) 测评者应检查服务器配套管理软件是否提供了对服务器中关键软件运行状态的监控功能；

b) 测评者应检查服务器主机和网络安全监控功能的实现和管理方式；

c) 测评者应检查服务器网络安全监控组件中有关统一管理接口的说明，并验证管理接口的有效性；

d) 测评者应模拟安全事件产生，验证主机和网络安全监控策略是有否有效；

e) 测评者应检查审计记录和报警事件，验证系统审计功能和报警功能是否有效；

f) 测评者应测试网络应用行为分类监控的功能，以及根据策略进行报警和阻断的功能；

g) 依据以上检查和测试所获取的信息给出评价意见，确定是否符合 GB/T 21028—2007 中 5.3.1.5.1规定的要求。

6.5.2 恶意代码防护

对第三级服务器中恶意代码防护功能的测评要求包括：

a) 测评者应检查关键服务器是否制定了恶意代码防护策略，并安装了相应的恶意代码防护软件；

b) 测评者应检查恶意代码软件防护软件的厂家、名称和恶意代码库版本号；

c) 测评者应检查服务器在启动时恶意代码防护软件的运行情况；

d) 测评者应检查恶意代码防护软件的事件日志，查看安全策略执行的有效性；

e) 测评者应检查恶意代码防护软件是否由统一的管理平台进行集中管理；

f) 依据以上检查所获取的信息给出评价意见，确定是否符合 GB/T 21028—2007 中 5.3.1.5.2 规定的要求。

6.5.3 备份与故障恢复

对第三级服务器中备份与故障恢复功能的测评要求包括：

a) 测评者应检查服务器中的软硬件系统是否具有对重要信息和部件进行备份的功能以及对重要信息和部件进行恢复的功能；

b) 测评者应检查服务器局部数据备份、完全数据备份的周期和策略；

c) 测评者应检查服务器中软硬系统备份和恢复功能的配置是否正确；

d) 测评者应检查设计/验收文档，查看其是否有本地和异地数据备份和恢复功能及策略的描述；

e) 测评者应检查服务器中关键部件是否采取了冗余措施；

f) 依据以上检查所获取的信息给出评价意见，确定是否符合 GB/T 21028—2007 中 5.3.1.5.3 规定的要求。

6.5.4 可信时间戳

对第三级服务器中可信时间戳功能的测评要求包括：

a) 测评者应检查服务器是否提供时间同步功能；

b) 测评者应核对时间，检查其可靠性情况，以及时间格式；

c) 依据以上检查所获取的信息给出评价意见，确定是否符合 GB/T 21028—2007 中 5.3.1.5.4 规定的要求。

6.6 SSOS 自身安全保护

对第三级服务器中 SSOS 自身安全保护的测评要求包括：

a) 测评者应检查说明文档，查看 SSF 防物理篡改的描述；

b) 测评者应检查设计文档，查看 SSOS 内 SSF 的安全结构定义形式；

c) 测评者应检查设计文档，查看 SSOS 内 SSF 数据传输时的保护、数据恢复、数据分离传输和数据完整性保护机制的描述；

d) 测评者应检查设计文档，查看在 SSF 发生确定故障的情况下系统采取保护措施的描述；

e) 测评者应检查设计文档，查看会话建立管理机制的描述和审计记录；

f) 测评者应检查 SSOS 自身安全保护功能的配置是否符合用户操作指南的要求；

g) 测评者应检查用户访问系统资源进行修改的历史记录；

h) 依据以上检查所获取的信息给出评价意见，确定是否符合 **GB/T** 21028—2007 **中** 5.3.2.1 规定的要求。

6.7 SSOS 设计和实现

对**第三级**服务器中 SSOS 设计和实现的测评要求包括：

a) 测评者应检查版本号、**配置项**、**授权管理**与 SSOS 样本的一致性情况，以及在产品开发、测试和维护期间的日志记录；

b) 测评者应检查对配置管理范围内的问题，特别是安全缺陷问题的跟踪记录；

c) 测评者应检查分发文档，查看是否包含了 SSOS 的安装、生成和启动过程；

d) 测评者应检查同产品一起交付的操作文档，查看是否包含了维护 SSOS 安全所必须的所有过程；

e) 测评者应检查设计文档，查看 SSF 的设计方法，以及接口、子系统的非形式化描述；

f) 测评者应检查指导性文档是否包括安全管理员指南和用户指南，以及指南内容的完整性情况；

g) 测评者应检查生存周期支持文档，查看开发、操作和维护 SSOS 的描述，以及用于描述产品生存周期进行管理的活动记录；

h) 测评者应检查自测文档的有效性和内容的完整性；

i) 测评者应检查对 SSOS 安全功能强度评价，如对安全机制的安全行为的合格性或统计结果，以及在独立脆弱性分析中所做的渗透测试的记录；

j) 依据以上检查所获取的信息给出评价意见，确定是否符合 **GB/T** 21028—2007 **中** 5.3.2.2 规定的要求。

6.8 SSOS 安全管理

对**第三级**服务器中 SSOS 安全管理的测评要求包括：

a) 测评者应检查开发人员的安全规章制度、开发人员的安全教育培训制度和记录；

b) 测评者应检查开发场所的出入口控制制度和记录，开发环境的防火防盗措施和国家有关部门的许可文件；

c) 测评者应检查开发主机使用管理和记录，设备的购置、修理、处置的制度和记录，上网管理，计算机病毒管理和记录等；

d) 测评者应检查产品代码、文档、样机进行受控管理的制度和记录；

e) 依据以上检查所获取的信息给出评价意见，确定是否符合 **GB/T** 21028—2007 **中** 5.3.2.3 规定的要求。

7 第四级安全测评

7.1 硬件系统

7.1.1 设备标签

对**第四级**设备标签的测评要求包括：

a) 测评者应检查服务器机箱，查看其是否可在显著位置设置标签；

b) 测评者应检查服务器是否设置了设备标签，以及该标签包含的信息；

c) 测评者应检查服务器关键部件(包括硬盘、主板、内存、处理器、网卡等组件、附件)是否设置了标签；

d) 测评者应检查服务器设备**标签类型**以及标签是否采取有效的保护措施；

e) 依据以上检查所获取的信息给出评价意见，确定是否符合 GB/T 21028—2007 中 5.4.1.1.1 规定的要求。

7.1.2 设备可靠运行支持

对**第四级**设备可靠运行支持的测评要求包括：

a) 测评者应根据服务器硬件配置清单，检查服务器主要部件(CPU、内存等)是否具有数据校验功能；

b) 测评者应检查关键部件(包括硬盘、主板、内存、处理器、网卡等)与其标签配合的情况，以及机箱面板的保护措施；

c) 测评者应检查硬盘、风扇、电源、**PCI 适配器、网卡和内存**的热插拔功能，内存的容错功能，以及电源、硬盘的冗余措施；

d) 测评者应检查服务器硬件在启动过程中的自检信息及操作提示是否与使用说明书保持一致；

e) 测评者应对安装于服务器中的至少一款应用软件进行操作，测试其响应情况；

f) 依据以上检查和测试所获取的信息给出评价意见，确定是否符合 GB/T 21028—2007 中 5.4.1.1.2 规定的要求。

7.1.3 设备工作状态监控

对**第四级**设备工作状态监控的测评要求包括：

a) 测评者应检查服务器中电源、风扇、机箱、磁盘控制等关键部件是否具备可管理接口；

b) 测评者应检查是否通过可管理接口实现了对关键部件的监控功能，并对其进行操作，验证其功能的有效性；

c) 测评者应模拟上述部件发生故障，测试其报警**和状态恢复**功能；

d) 依据以上检查和测试所获取的信息给出评价意见，确定是否符合 GB/T 21028—2007 中 5.4.1.1.3 规定的要求。

7.1.4 设备电磁防护

对**第四级**设备电磁防护的测评要求包括：

a) 测评者应检查服务器设备电磁防护指标是否符合国家规定的要求；

b) 依据以上检查所获取的信息给出评价意见，确定是否符合 GB/T 21028—2007 中 5.4.1.1.4 规定的要求。

7.2 操作系统

7.2.1 身份鉴别

对**第四级**服务器中操作系统的身份鉴别功能的测评要求包括：

a) 测评者应检查操作系统是否提供了远程管理功能，如提供了远程管理，查看鉴别信息在网络传输过程中的保护措施；

b) 测评者应检查操作系统账户列表，查看管理员用户名分配是否能保持唯一性；

c) 测评者应检查操作系统是否提供了身份鉴别措施(如用户名和强化管理的口令等)；

d) 测评者应检查是否提供两个及两个以上身份鉴别技术的组合来进行身份鉴别(如采用用户名/口令、挑战应答、动态口令、物理设备、生物识别技术和数字证书方式的身份鉴别技术中的任意两个组合)；

e) 测评者应检查操作系统是否提供鉴别失败处理功能，并能配置非法登录次数的限制值；

f) 测评者应通过错误的用户名和口令试图登录系统，验证鉴别失败处理功能是否有效；

g) 测评者应测试系统在通过正常登录是否有登录警示信息；

h) 测评者应通过渗透性测试对操作系统进行用户口令强度进行测试，查看能否破解用户口令，破解口令后能否登录进入系统；

i) 测评者应通过性渗透测试来检查是否存在绕过认证方式进行系统登录的方法，例如，认证程序

存在的安全漏洞，社会工程或其他手段等；

j) 依据以上检查和测试所获取的信息给出评价意见，确定是否符合 GB/T 21028—2007 中5.4.1.2a)规定的要求。

7.2.2 自主访问控制

对第四级服务器中操作系统的自主访问控制功能的测评要求包括：

a) 测评者应检查操作系统的自主访问控制功能，查看其是否能对重要文件的访问权限进行限制，对系统不需要的服务、共享路径等可能被非授权访问的客体进行限制；

b) 测评者应检查操作系统中匿名/默认用户的访问权限是否能被禁用或者限制(如限定在有限的范围内)；

c) 测评者应检查操作系统的访问控制列表，查看是否能通过访问控制列表获取到用户和权限的对应关系；

d) 测评者应通过审计日志记录，检查日志记录与自主访问控制中的主体相关联的情况；

e) 测评者应依据系统访问控制的安全策略，试图以未授权用户身份/角色访问客体，验证是否不能进行访问；

f) 测评者应检查系统是否提供了特权用户权限分享的机制，如可分为系统管理员、安全管理员、安全审计员等；

g) 依据以上检查和测试所获取的信息给出评价意见，确定是否符合 GB/T 21028—2007 中5.4.1.2b)规定的要求。

7.2.3 标记

对第四级服务器中操作系统的标记功能的测评要求包括：

a) 测评者应检查操作系统是否提供对所有文件和用户设置标记的功能；

b) 依据以上检查所获取的信息给出评价意见，确定是否符合 GB/T 21028—2007 中 5.4.1.2c)规定的要求。

7.2.4 强制访问控制

对第四级服务器中操作系统的强制访问控制功能的测评要求包括：

a) 测评者应检查强制访问控制模型是否采用“向下读，向上写”模型，如果操作系统采用其他的强制访问控制模型，则操作系统文档是否对这种模型进行详细分析，并有权威机构对这种强制访问控制模型的合理性和完善性进行检测证明；

b) 测评者应检查强制访问控制是否与用户身份鉴别、标识等安全功能密切配合，并且控制粒度达到主体为用户级，客体为文件；

c) 测评者应检查系统中所有主客体是否都能包含在强制访问控制范围内；

d) 测评者应依据系统文档描述测试强制访问控制模型，以授权用户和非授权用户身份访问客体，验证是否只有授权用户可以访问客体；

e) 测评者应通过渗透测试检查是否可通过非法操作来终止强制访问模块，非法修改强制访问相关规则；

f) 依据以上检查和测试所获取的信息给出评价意见，确定是否符合 GB/T 21028—2007 中5.4.1.2d)规定的要求。

7.2.5 数据流控制

对第四级服务器中操作系统的数据流控制功能的测评要求包括：

a) 测评者应检查数据在不同等级系统间的流动时是否提供了控制措施；

b) 依据以上检查所获取的信息给出评价意见，确定是否符合 GB/T 21028—2007 中5.4.1.2e)规定的要求。

7.2.6 安全审计

对**第四级**服务器中操作系统的安全审计功能的测评要求包括：

a) 测评者应检查安全审计功能的策略，以及审计日志的处理方式；

b) 测评者应通过审计策略和记录，检查审计范围是否能够覆盖系统内重要的安全相关事件，例如，用户标识与鉴别、重要用户行为、系统资源的异常使用、重要系统命令的使用（如删除客体）等；

c) 测评者应检查审计记录信息是否包括事件发生的日期与时间、触发事件的主体与客体、事件的类型、事件成功或失败、身份鉴别事件中请求的来源（如末端标识符）、事件的结果等内容；

d) 测评者应检查是否提供了浏览和分析审计数据提供专门的审计工具（如对审计记录进行分类、排序、查询、统计、分析和组合查询等），并能根据需要生成审计报表；

e) 测评者应通过非法终止审计功能或修改其配置，验证审计功能是否受到保护；

f) 测评者应以某个系统用户试图删除、修改或覆盖审计记录，测试安全审计的保护情况与要求是否一致；

g) 测评者应检查审计跟踪设置是否提供定义审计跟踪极限的阈值的功能，当存储空间被耗尽时，能否采取必要的保护措施；

h) 测评者应检查系统是否提供集中审计系统连接的接口，并能根据集中审计系统的要求发送审计数据；

i) 依据以上检查和测试所获取的信息给出评价意见，确定是否符合 **GB/T** 21028—2007 中 5.4.1.2**f**）规定的要求。

7.2.7 数据完整性

对**第四级**服务器中操作系统的数据完整性保护功能的测评要求包括：

a) 测评者应检查操作系统内部在传输鉴别信息和用户数据时实现数据完整性保护功能的情况；

b) 测评者应检查操作系统在存储鉴别信息和重要用户数据时的完整性保护功能；

c) 测评者应模拟进行大数据量的数据传输或保存时出现异常中断情况，测试操作系统在异常情况下的回退功能以及保护数据完整性的情况；

d) 依据以上检查和测试所获取的信息给出评价意见，确定是否符合 **GB/T** 21028—2007 中 5.4.1.2**g**）规定的要求。

7.2.8 数据保密性

对**第四级**服务器中操作系统的数据保密性功能的测评要求包括：

a) 测评者应检查鉴别信息和敏感的用户数据是否采用加密或其他有效措施实现存储保密性；

b) 测评者应检查系统管理数据、鉴别信息是否采用了加密或其他有效措施实现传输保密性；

c) 依据以上检查所获取的信息给出评价意见，确定是否符合 **GB/T** 21028—2007 中5.4.1.2**h**）规定的要求。

7.2.9 可信路径

对第四级服务器中操作系统的可信路径功能的测评要求包括：

a) 测评者应检查操作系统文档，查看系统提供了哪些可信路径功能；

b) 测评者应测试可信路径功能是否有效；

c) 依据以上检查和测试所获取的信息给出评价意见，确定是否符合 GB/T 21028—2007 中 5.4.1.2**i**）规定的要求。

7.3 数据库管理系统

7.3.1 身份鉴别

对**第四级**服务器中数据库管理系统的身份鉴别功能的测评要求包括：

a) 测评者应检查数据库管理系统是否提供了远程管理，如提供了远程管理，查看鉴别信息在网络

传输过程中的保护措施；

b) 测评者应检查数据库管理系统账户列表，查看管理员用户名分配是否能保持唯一性；

c) 测评者应检查数据库管理系统是否提供了身份鉴别措施（如用户名或口令等）；

d) 测评者应检查是否提供两个及两个以上身份鉴别技术的组合来进行身份鉴别（如采用用户名/口令、挑战应答、动态口令、物理设备、生物识别技术和数字证书方式的身份鉴别技术中的任意两个组合）；

e) 测评者应测试系统在通过正常登录是否有登录警示信息；

f) 测评者应检查数据库管理系统是否提供鉴别失败处理功能，并能配置非法登录次数的限制值；

g) 测评者应通过错误的用户名和口令试图登录系统，验证鉴别失败处理功能是否有效；

h) 测评者应通过渗透性测试对数据库管理系统进行用户口令强度进行测试，查看能否破解用户口令，破解口令后能否登录进入系统；

i) 测评者应通过性渗透测试来检查是否存在绕过认证方式进行系统登录的方法，例如，认证程序存在的安全漏洞，社会工程或其他手段等；

j) 依据以上检查和测试所获取的信息给出评价意见，确定是否符合 **GB/T 21028—2007 中 5.4.1.3a)**规定的要求。

7.3.2 自主访问控制

对**第四级**服务器中数据库管理系统的自主访问控制功能的测评要求包括：

a) 测评者应检查数据库管理系统的自主访问控制，查看其是否能明确主体对客体的访问权限（如目录表访问控制/存取控制表访问控制等）；

b) 测评者应检查数据库管理系统中匿名/默认用户的访问权限是否能被禁用或者限制（如限定在有限的范围内）；

c) 测评者应检查数据库管理系统的访问控制列表，查看是否能通过访问控制列表获取到用户和权限的对应关系；

d) 测评者应通过审计日志记录，检查其与自主访问控制中的主体相关联的情况；

e) 测评者应依据系统访问控制的安全策略，试图以未授权用户身份/角色访问客体，验证是否不能进行访问；

f) 检查系统是否提供了特权用户权限分享的机制，如可分为系统管理员、安全管理员、安全审计员等；

g) 依据以上检查和测试所获取的信息给出评价意见，确定是否符合 **GB/T 21028—2007 中 5.4.1.3b)**规定的要求。

7.3.3 标记

对**第四级**服务器中数据库管理系统的标记功能的测评要求包括：

a) 测评者应检查数据库管理系统是否提供对所有数据表和用户设置标记的功能；

b) 依据以上检查所获取的信息给出评价意见，确定是否符合 **GB/T 21028—2007 中5.4.1.3c)**规定的要求。

7.3.4 强制访问控制

对**第四级**服务器中数据库管理系统的强制访问控制功能的测评要求包括：

a) 测评者应检查强制访问控制模型是否采用“向下读，向上写”模型，如果数据库管理系统采用其他的强制访问控制模型，则操作系统文档是否对这种模型进行详细分析，并有权威机构对这种强制访问控制模型的合理性和完善性进行检测证明；

b) 测评者应检查强制访问控制是否与用户身份鉴别、标识等安全功能密切配合，并且控制粒度达到主体为用户级，客体为数据表；

c) 测评者应检查系统中所有主客体是否都能包含在强制访问控制范围内；

d) 测评者应依据系统文档描述测试强制访问控制模型，以授权用户和非授权用户身份访问客体，验证是否只有授权用户可以访问客体；

e) 测评者应通过渗透测试检查是否可通过非法操作来终止强制访问模块，非法修改强制访问相关规则；

f) 依据以上检查和测试所获取的信息给出评价意见，确定是否符合 GB/T 21028—2007 中5.4.1.3**d**)规定的要求。

7.3.5 数据流控制

对**第四级**服务器中数据库管理系统的数据流控制功能的测评要求包括：

a) 测评者应检查数据在不同等级系统间的流动时是否提供了控制措施；

b) 依据以上检查所获取的信息给出评价意见，确定是否符合 GB/T 21028—2007 中5.4.1.3**e**)规定的要求。

7.3.6 安全审计

对**第四级**服务器中数据库管理系统的安全审计功能的测评要求包括：

a) 测评者应检查安全审计功能的策略，以及审计日志的处理方式；

b) 测评者应通过审计策略和记录，检查审计范围是否能够覆盖系统内重要的安全相关事件，例如，用户标识与鉴别、重要用户行为、系统资源的异常使用、重要系统命令的使用(如删除客体)等；

c) 测评者应检查审计记录信息是否包括事件发生的日期与时间、触发事件的主体与客体、事件的类型、事件成功或失败、身份鉴别事件中请求的来源(如末端标识符)、事件的结果等内容；

d) 测评者应检查是否提供了浏览和分析审计数据提供专门的审计工具(如对审计记录进行分类、排序、查询、统计、分析和组合查询等)，并能根据需要生成审计报表；

e) 测评者应通过非法终止审计功能或修改其配置，验证审计功能是否受到保护；

f) 测评者应以某个系统用户试图删除、修改或覆盖审计记录，测试安全审计的保护情况与要求是否一致；

g) 测评者应检查审计跟踪设置是否提供定义审计跟踪极限的阈值的功能，当存储空间被耗尽时，能否采取必要的保护措施；

h) 测评者应检查系统是否提供集中审计系统连接的接口，并能根据集中审计系统的要求发送审计数据；

i) 依据以上检查和测试所获取的信息给出评价意见，确定是否符合 GB/T 21028—2007 中5.4.1.3**f**)规定的要求。

7.3.7 数据完整性

对**第四级**服务器中数据库管理系统的数据完整性保护功能的测评要求包括：

a) 测评者应检查数据库管理系统内部在传输鉴别信息和用户数据时实现数据完整性保护功能的情况；

b) 测评者应检查数据库管理系统在存储鉴别信息和重要用户数据时的完整性保护功能；

c) 测评者应模拟数据库管理系统操作时出现递交失败等异常中断情况，测试数据库管理系统在异常情况下的回退功能以及保护数据完整性的情况；

d) 依据以上检查和测试所获取的信息给出评价意见，确定是否符合 GB/T 21028—2007 中5.4.1.3**g**)规定的要求。

7.3.8 数据保密性

对**第四级**服务器中数据库管理系统的数据保密性功能的测评要求包括：

a) 测评者应检查鉴别信息和敏感的用户数据是否采用加密或其他有效措施实现存储保密性；

b) 测评者应检查系统管理数据、鉴别信息是否采用了加密或其他有效措施实现传输保密性；

c) 依据以上检查所获取的信息给出评价意见，确定是否符合 **GB/T** 21028—2007 中 5.4.1.3**h**)规定的要求。

7.3.9 可信路径

对第四级服务器中数据库管理系统的可信路径功能的测评要求包括：

a) **测评者应检查数据库管理系统文档，查看系统提供了哪些可信路径功能；**

b) **测评者应测试可信路径功能是否有效；**

c) **依据以上检查和测试所获取的信息给出评价意见，确定是否符合 GB/T** 21028—2007 **中** 5.4.1.3**i**)**规定的要求。**

7.3.10 推理控制

对第四级服务器中数据库管理系统的推理控制功能的测评要求包括：

a) **测评者应检查数据库管理系统文档，查看系统提供了哪些推理控制功能；**

b) **测评者应检查推理攻击分析和测试报告；**

c) **依据以上检查所获取的信息给出评价意见，确定是否符合 GB/T** 21028—2007 **中**5.4.1.3**j**)**规定的要求。**

7.4 应用系统

7.4.1 身份鉴别

对**第四级**服务器中应用系统的身份鉴别功能的测评要求包括：

a) 测评者应检查应用系统是否提供专用的登录控制模块对登录用户进行身份标识和鉴别，具体采取什么鉴别控制措施；

b) 测评者应检查应用系统是否能保证用户标识的唯一性(如 UID、用户名或其他信息在系统中是唯一的，用该标识能唯一识别该用户)；

c) 测评者应检查应用系统是否具有身份标识(如建立账号)和鉴别(如口令等)功能；

d) 测评者应检查是否提供两个及两个以上身份鉴别技术的组合来进行身份鉴别(如采用用户名/口令、挑战应答、动态口令、物理设备、生物识别技术和数字证书方式的身份鉴别技术中的任意两个组合)；

e) **测评者应测试系统在通过正常登录是否有登录警示信息；**

f) 测评者应检查应用是否提供了登录失败处理功能(如限制非法登录次数，登录失败次数超过设定值则结束会话等)；

g) 测评者应检查关键应用系统，查看其是否采取措施防止鉴别信息传输过程中被窃听；

h) 测评者应通过已注册用户身份登录系统，查看登录是否成功，验证其身份标识和鉴别功能是否有效；

i) 测评者应通过错误的用户名和口令试图登录系统，验证鉴别失败处理功能是否有效；

j) 依据以上检查和测试所获取的信息给出评价意见，确定是否符合 **GB/T** 21028—2007 **中** 5.4.1.4.1规定的要求。

7.4.2 自主访问控制

对**第四级**服务器中应用系统的自主访问控制功能的测评要求包括：

a) 测评者应检查应用系统提供的访问控制措施，包括具体措施、访问控制策略等；

b) 测评者应测试系统是否提供访问控制功能控制用户组/用户对系统功能和用户数据的访问；

c) 测评者应检查系统是否有由授权主体设置用户对系统功能操作和对数据访问的权限的功能，是否限制默认用户访问权限；

d) 测评者应通过不同权限的用户登录系统并进行一些操作，检查其权限是否与设定的权限一致；

e) 测评者应检查应用系统的访问控制列表，查看是否能通过访问控制列表获取到用户和权限的对应关系；

f) 测评者应通过审计日志记录，检查日志记录与自主访问控制中的主体相关联的情况；

g) 测评者应检查应用系统是否提供了特权用户的权限分离功能（如系统管理员只能对系统进行维护，安全管理员只能进行策略配置和安全设置，安全审计员只能维护审计信息等）；

h) 依据以上检查和测试所获取的信息给出评价意见，确定是否符合 GB/T 21028—2007 中 5.4.1.4.2规定的要求。

7.4.3 标记

对**第四级**服务器中应用系统的标记功能的测评要求包括：

a) 测评者应检查应用系统是否提供对重要数据和用户设置标记的功能；

b) 依据以上检查所获取的信息给出评价意见，确定是否符合 GB/T 21028—2007 中 5.4.1.4.3 规定的要求。

7.4.4 强制访问控制

对**第四级**服务器中应用系统的强制访问控制功能的测评要求包括：

a) 测评者应检查应用系统是否提供了强制访问控制功能，以及该功能模型的合理性和完善性；

b) 测评者应检查强制访问控制是否与用户身份鉴别、标识等安全功能密切配合；

c) 测评者应依据系统文档描述测试强制访问控制模型，以授权用户和非授权用户身份访问客体，验证是否只有授权用户可以访问客体；

d) 测评者应通过渗透测试检查是否可通过非法操作来终止强制访问模块，非法修改强制访问相关规则；

e) 依据以上检查和测试所获取的信息给出评价意见，确定是否符合 GB/T 21028—2007 中 5.4.1.4.4规定的要求。

7.4.5 数据流控制

对**第四级**服务器中应用系统的数据流控制功能的测评要求包括：

a) 测评者应检查数据在不同等级应用系统间的流动时是否提供了控制措施；

b) 依据以上检查所获取的信息给出评价意见，确定是否符合 GB/T 21028—2007 中 5.4.1.4.5 规定的要求。

7.4.6 安全审计

对**第四级**服务器中应用系统的安全审计功能的测评要求包括：

a) 测评者应检查安全审计功能的策略，以及审计日志的处理方式；

b) 测评者应通过审计策略和记录，检查审计范围是否能够覆盖系统内重要的安全相关事件，例如，用户标识与鉴别、重要用户行为、系统资源的异常使用、重要系统命令的使用（如删除客体）等；

c) 测评者应检查审计记录信息是否包括事件发生的日期与时间、触发事件的主体与客体、事件的类型、事件成功或失败、身份鉴别事件中请求的来源（如末端标识符）、事件的结果等内容；

d) 测评者应检查审计跟踪设置是否提供定义审计跟踪极限的阈值的功能，当存储空间被耗尽时，能否采取必要的保护措施；

e) 测评者应检查应用系统是否提供了浏览和分析审计数据提供专门的审计工具（如对审计记录进行分类、排序、查询、统计、分析和组合查询等），并能根据需要生成审计报表；

f) 测评者应通过非法终止审计功能或修改其配置，验证审计功能是否受到保护；

g) 测评者应以某个系统用户试图删除、修改或覆盖审计记录，测试安全审计的保护情况与要求是否一致；

h) 测评者应以某个用户试图产生一些重要的安全相关事件（如鉴别失败等），测试安全审计的覆盖情况和记录情况与要求是否一致；

i) 测评者应以某个系统用户试图删除、修改或覆盖审计记录，测试安全审计的保护情况与要求是

否一致；

j） 依据以上检查和测试所获取的信息给出评价意见，确定是否符合 **GB/T** 21028—2007 **中** 5.4.1.4.6规定的要求。

7.4.7 数据完整性

对**第四级**服务器中应用系统的数据完整性保护功能的测评要求包括：

a） 测评者应检查服务器应用系统用户数据在传输过程中是否具有完整性保证措施；

b） 测评者应检查应用系统设计/验收文档，查看其是否有关于用户数据在传输过程中采用的完整性保证措施的描述；

c） 测评者应检查应用系统是否配备检测/验证重要用户数据在传输过程中完整性受到破坏的功能；

d） 依据以上检查所获取的信息给出评价意见，确定是否符合 **GB/T** 21028—2007 **中** 5.4.1.4.7 规定的要求。

7.4.8 数据保密性

对**第四级**服务器中应用系统的数据保密性功能的测评要求包括：

a） 测评者应检查鉴别信息和敏感的用户数据是否采用加密或其他有效措施实现存储保密性；

b） 测评者应检查应用系统设计/验收文档，查看其是否有关于其鉴别信息、敏感的用户数据采用加密或其他有效措施实现存储保密性的描述；

c） 依据以上检查所获取的信息给出评价意见，确定是否符合 **GB/T** 21028—2007 **中** 5.4.1.4.8 规定的要求。

7.4.9 可信路径

对第四级服务器中应用系统的可信路径功能的测评要求包括：

a） **测评者应检查应用系统文档，查看系统提供了哪些可信路径功能；**

b） **测评者应测试可信路径功能是否有效；**

c） **依据以上检查和测试所获取的信息给出评价意见，确定是否符合 GB/T** 21028—2007 **中** 5.4.1.4.9规定的要求。

7.5 运行安全

7.5.1 安全监控

对**第四级**服务器中安全监控功能的测评要求包括：

a） 测评者应检查服务器配套管理软件是否提供了对服务器中关键软件运行状态的监控功能；

b） 测评者应检查服务器主机和网络安全监控功能的实现和管理方式；

c） 测评者应检查服务器网络安全监控组件中有关统一管理接口的说明，并验证管理接口的有效性；

d） 测评者应模拟安全事件产生，验证主机和网络安全监控策略是有否有效；

e） 测评者应检查审计记录和报警事件，验证系统审计功能和报警功能是否有效；

f） 测评者应测试网络应用行为分类监控的功能，以及根据策略进行报警和阻断的功能；

g） 依据以上检查和测试所获取的信息给出评价意见，确定是否符合 **GB/T** 21028—2007 **中** 5.4.1.5.1规定的要求。

7.5.2 恶意代码防护

对**第四级**服务器中恶意代码防护功能的测评要求包括：

a） 测评者应检查关键服务器是否制定了恶意代码防护策略，并安装了相应的恶意代码防护软件；

b） 测评者应检查恶意代码软件防护软件的厂家、名称和恶意代码库版本号；

c） 测评者应检查服务器在启动时恶意代码防护软件的运行情况；

d） 测评者应检查恶意代码防护软件的事件日志，查看安全策略执行的有效性；

e) 测评者应检查恶意代码防护软件是否由统一的管理平台进行集中管理；

f) 测评者应检查恶意代码防护软件在出现异常情况时是否能进行自动修复；

g) 依据以上检查所获取的信息给出评价意见，确定是否符合 **GB/T** 21028—2007 **中** 5.4.1.5.2 规定的要求。

7.5.3 备份与故障恢复

对**第四级**服务器中备份与故障恢复功能的测评要求包括：

a) 测评者应检查服务器中的软硬件系统是否具有对重要信息和部件进行备份的功能以及对重要信息和部件进行恢复的功能；

b) 测评者应服务器局部数据备份、完全数据备份的周期和策略；

c) 测评者应检查服务器中软硬系统备份和恢复功能的配置是否正确；

d) 测评者应检查设计/验收文档，查看其是否有本地和异地数据备份和恢复功能及策略的描述；

e) 测评者应检查服务器中关键部件是否采取了冗余措施；

f) 测评者应检查是否为重要服务器系统配备了本地和异地备份功能，配置是否正确；是否有异地灾难备份中心；

g) 测评者应检查应用系统是否配备了异地无缝切换功能，以及测试业务应用系统，验证其异地无缝切换功能是否有效；

h) 依据以上检查所获取的信息给出评价意见，确定是否符合 **GB/T** 21028—2007 **中** 5.4.1.5.3 规定的要求。

7.5.4 可信技术支持

对第四级服务器中可信技术支持功能的测评要求包括：

a) 测评者应检查可信技术支持功能中密码模块是否符合国家相关部门规定；

b) 测评者应检查可信技术支持功能是否采用硬件实现，其硬件模块是否与服务器实现了绑定；

c) 测评者应检查服务器在启动过程中是否通过可信技术支持功能建立了信任链；

d) 测评者应检查用户身份鉴别和存储加密是否建立在可信技术支持之上；

e) 依据以上检查所获取的信息给出评价意见，确定是否符合 GB/T 21028—2007 **中** 5.4.1.5.4 **规定的要求。**

7.5.5 可信时间戳

对**第四级**服务器中可信时间戳功能的测评要求包括：

a) 测评者应检查服务器是否提供时间同步功能；

b) 测评者应核对时间，检查其可靠性情况，以及时间格式；

c) 依据以上检查所获取的信息给出评价意见，确定是否符合 **GB/T** 21028—2007 **中** 5.4.1.5.5 规定的要求。

7.6 SSOS 自身安全保护

对**第四级**服务器中 SSOS 自身安全保护的测评要求包括：

a) 测评者应检查说明文档，查看 SSF 防物理篡改的描述；

b) 测评者应检查设计文档，查看 SSOS 内 SSF 的安全结构定义形式；

c) 测评者应检查设计文档，查看 SSOS 内 SSF 数据传输时的保护、数据恢复、数据分离传输和数据完整性保护机制的描述；

d) 测评者应检查设计文档，查看在 SSF 发生确定故障的情况下系统采取保护措施的描述；

e) 测评者应检查设计文档，查看会话建立管理机制的描述和审计记录；

f) 测评者应检查 SSOS 自身安全保护功能的配置是否符合用户操作指南的要求；

g) 测评者应检查用户访问系统资源进行修改的历史记录；

h) 依据以上检查所获取的信息给出评价意见，确定是否符合 **GB/T** 21028—2007 **中** 5.4.2.1 规

定的要求。

7.7 SSOS 设计和实现

对**第四级**服务器中 SSOS 设计和实现的测评要求包括：

a) 测评者应检查版本号、配置项、授权管理与 SSOS 样本的一致性情况，以及在产品开发、测试和维护期间的日志记录；

b) 测评者应检查对配置管理范围内的问题，特别是安全缺陷问题的跟踪记录；

c) 测评者应检查分发文档，查看是否包含了 SSOS 的安装、生成和启动过程；

d) 测评者应检查同产品一起交付的操作文档，查看是否包含了维护 SSOS 安全所必须的所有过程；

e) 测评者应检查设计文档，查看 SSF 的设计方法，以及接口、子系统的**半形式化**描述；

f) 测评者应检查指导性文档是否包括安全管理员指南和用户指南，以及指南内容的完整性情况；

g) 测评者应检查生存周期支持文档，查看开发、操作和维护 SSOS 的描述，以及用于描述产品生存周期进行管理的活动记录；

h) 测评者应检查自测文档的有效性和内容的完整性；

i) 测评者应检查对 SSOS 安全功能强度评价，如对安全机制的安全行为的合格性或统计结果，以及在独立脆弱性分析中所做的渗透测试的记录；

j) 测评者应检查一般性隐蔽信道的分析材料中对存储信道的搜索和标识的描述；

k) 依据以上检查所获取的信息给出评价意见，确定是否符合 **GB/T** 21028—2007 **中** 5.4.2.2 规定的要求。

7.8 SSOS 安全管理

对**第四级**服务器中 SSOS 安全管理的测评要求包括：

a) 测评者应检查开发人员的安全规章制度、开发人员的安全教育培训制度和记录；

b) 测评者应检查开发场所的出入口控制制度和记录，开发环境的防火防盗措施和国家有关部门的许可文件；

c) 测评者应检查开发主机使用管理和记录，设备的购置、修理、处置的制度和记录，上网管理，计算机病毒管理和记录等；

d) 测评者应检查产品代码、文档、样机进行受控管理的制度和记录；

e) 依据以上检查所获取的信息给出评价意见，确定是否符合 **GB/T** 21028—2007 **中** 5.4.2.3 规定的要求。

8 第五级安全测评

第五级信息系统是涉及国家安全、社会秩序、经济建设和公共利益的重要信息系统，对第五级信息系统中服务器的安全测评由相应部门或机构另行规范。

GB/T 25063—2010

参 考 文 献

[1] GB/T 18336.1—2008 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(ISO/IEC 15408-1:2005,IDT)

[2] GB/T 18336.2—2008 信息技术 安全技术 信息技术安全性评估准则 第2部分:安全功能要求(ISO/IEC 15408-2:2005,IDT)

[3] GB/T 18336.3—2008 信息技术 安全技术 信息技术安全性评估准则 第3部分:安全保证要求(ISO/IEC 15408-3:2005,IDT)

[4] GB/T 20272—2006 信息安全技术 操作系统安全技术要求

[5] GB/T 20273—2006 信息安全技术 数据库管理系统安全技术要求

[6] Trusted Computing Group TPM Main Specification Version 1.2:Part 1 Design Principles,May 2004

GB/T 25063-2010

*

书号:155066·1-40582