ICS 35.020
L 80

中华人民共和国国家标准

GB/T 28448—2012

信息安全技术
信息系统安全等级保护测评要求

Information security technology—
Testing and evaluation requirement for classified protection of information system

2012-06-29 发布　　2012-10-01 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
信息系统安全等级保护测评要求
GB/T 28448—2012
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100013)
北京市西城区三里河北街16号(100045)
网址 www.spc.net.cn
总编室:(010)64275323 发行中心:(010)51780235
读者服务部:(010)68523946
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 8.5 字数 257 千字
2012年10月第一版 2012年10月第一次印刷
*
书号:155066·1-45598 定价 100.00 元

目　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由全国信息安全标准化技术委员会提出并归口(SAC/TC 260)。

本标准起草单位:公安部信息安全等级保护评估中心。

本标准主要起草人:朱建平、马力、黄洪、毕马宁、任卫红、谢朝海、李升、袁静、曲洁、刘静、尚旭光、张振峰、李明、陈雪秀。

引　言

依据《中华人民共和国计算机信息系统安全保护条例》(国务院147号令)、《国家信息化领导小组关于加强信息安全保障工作的意见》(中办发[2003]27号)、《关于信息安全等级保护工作的实施意见》(公通字[2004]66号)和《信息安全等级保护管理办法》(公通字[2007]43号)等有关文件要求,制定本标准。

本标准是信息安全等级保护相关系列标准之一。

与本标准相关的系列标准包括:

——GB/T 22239—2008　信息安全技术　信息系统安全等级保护基本要求;

——GB/T 22240—2008　信息安全技术　信息系统安全等级保护定级指南;

——GB/T 28449—2012　信息安全技术　信息系统安全等级保护测评过程指南。

《信息安全技术　信息系统安全等级保护测评过程指南》就有关信息系统安全等级保护测评工作的组织、实施和过程控制方面提供指导。本标准对信息系统进行安全等级保护测试评估的技术活动提出要求,为评价信息系统是否符合GB/T 22239—2008提供了获取证据的途径和方法,用以指导测评人员从信息安全等级保护的角度对信息系统进行测试评估。

本标准中的信息系统指计算机信息系统。

在本标准文本中,黑体字的测评要求表示该要求出现在当前等级而在低于当前等级信息系统的测评要求中没有出现过。

信息安全技术
信息系统安全等级保护测评要求

1 范围

本标准规定了对实现的信息系统是否符合 GB/T 22239—2008 所进行的测试评估活动的要求，包括对第一级信息系统、第二级信息系统、第三级信息系统和第四级信息系统进行测试评估的要求。本标准略去对第五级信息系统进行测评的要求。

本标准适用于信息安全测评服务机构、信息系统的主管部门及运营使用单位对信息系统安全等级保护状况进行的安全测试评估。信息安全监管职能部门依法进行的信息安全等级保护监督检查可以参考使用。

2 规范性引用文件

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

GB/T 5271.8 信息技术 词汇 第 8 部分：安全

GB/T 22239—2008 信息安全技术 信息系统安全等级保护基本要求

3 术语和定义

GB/T 5271.8 和 GB/T 22239—2008 界定的以及下列术语和定义适用于本文件。

3.1

访谈 interview

访谈是指测评人员通过引导信息系统相关人员进行有目的的(有针对性的)交流以帮助测评人员理解、澄清或取得证据的过程。

3.2

检查 examination

检查是指测评人员通过对测评对象(如制度文档、各类设备、安全配置等)进行观察、查验、分析以帮助测评人员理解、澄清或取得证据的过程。

3.3

测试 testing

测试是指测评人员使用预定的方法/工具使测评对象(各类设备或安全配置)产生特定的结果，将运行结果与预期的结果进行比对的过程。

4 概述

4.1 测评框架

信息系统安全等级保护测评(以下简称等级测评)的概念性框架由三部分构成：测评输入、测评过程

和测评输出。测评输入包括 GB/T 22239—2008 第四级目录(即安全控制点的唯一标识符)和采用该安全控制的信息系统的安全保护等级(含业务信息安全保护等级和系统服务保护等级)。过程组件为一组与输入组件中所标识的安全控制相关的特定测评对象和测评方法,输出组件包括一组由测评人员使用的用于确定安全控制有效性的程序化陈述。图 1 给出了框架。

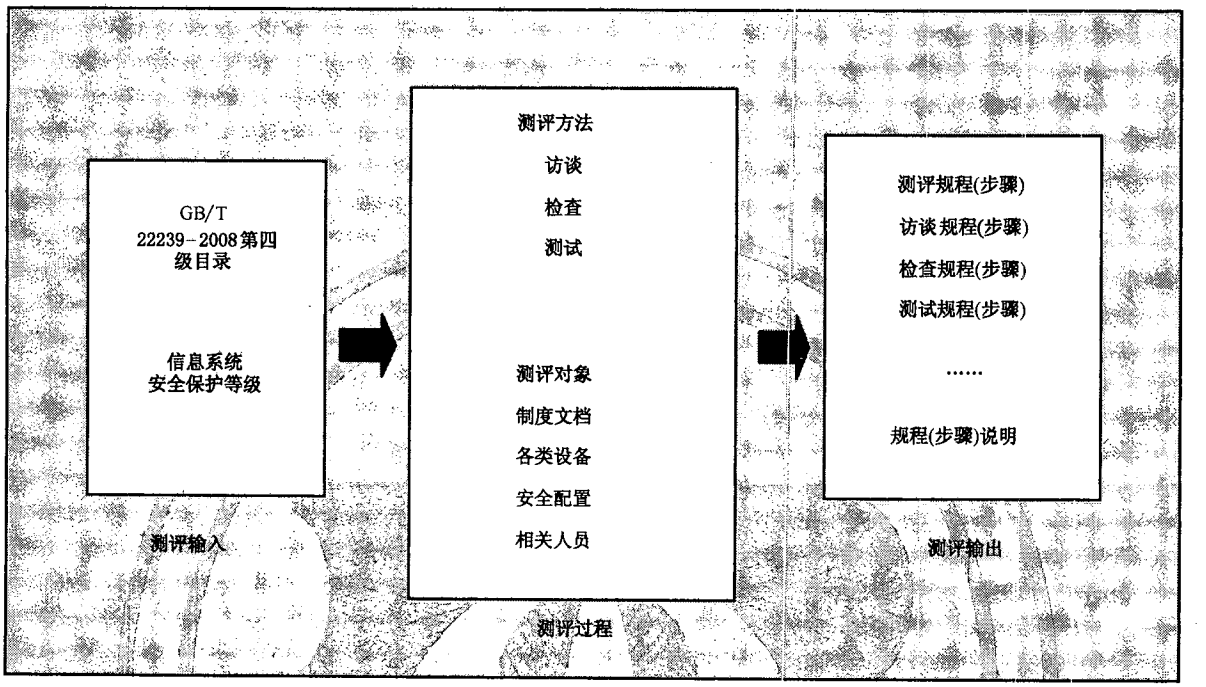

图 1 测评框架

测评对象是指测评实施的对象,即测评过程中涉及到的制度文档、各类设备及其安全配置和相关人员等。

制度文档是指针对信息系统所制定的相关联的文件(如政策、程序、计划、系统安全需求、功能规格及建筑设计)。各类设备是指安装在信息系统之内或边界,能起到特定保护作用的相关部件(如硬件、软件、固件或物理设施)。安全配置是指信息系统所使用的设备为了贯彻安全策略而进行的设置。相关人员或部门,是指应用上述制度、设备及安全配置的人。

对于框架来说,每一个被测安全控制(不同级别)均有一组与之相关的预先定义的测评对象(如制度文档、各类设备及其安全配置和相关人员)。

测评方法:在框架的测评过程组件中,测评方法包括访谈、检查和测试(说明见术语),测评人员通过这些方法试图获取证据。上述三种测评方法(访谈、检查和测评)的测评结果都用以对安全控制的有效性进行评估。

上述的评估方法都由一组相关属性来规范测评方法的测评力度。这些属性是广度(覆盖面)和深度。对于每一种测评方法都标识(定义)了唯一属性,深度特性适用于访谈和检查,而覆盖面特性则适用于全部三种测评方法。具体的描述参见附录 A。

4.2 等级测评内容

等级测评的实施过程由单元测评和整体测评两部分构成。

针对基本要求各安全控制点的测评称为单元测评。单元测评是等级测评工作的基本活动,支持测评结果的可重复性和可再现性。每个单元测评包括测评指标、测评实施和结果判定三部分。其中,测评

指标来源于 GB/T 22239—2008 第四级目录下的各要求项，测评实施描述对测评活动输入、测评对象、测评步骤和方法的要求，结果判定描述测评人员执行测评实施并产生各种测评输出数据后，如何依据这些测评输出数据来判定被测系统是否满足测评指标要求的原则和方法。

单项测评满足概念性框架的三部分内容：测评输入、测评过程和测评输出。

整体测评是在单元测评的基础上，通过进一步分析信息系统安全保护功能的整体相关性，对信息系统实施的综合安全测评。整体测评主要包括安全控制点间、层面间和区域间相互作用的安全测评。整体测评需要与信息系统的实际情况相结合，因此全面地给出整体测评要求的全部输入，测评实施的具体对象、步骤和方法以及明确的结果判定方法是非常困难的，测评人员应根据被测系统的实际情况，结合本标准的要求，实施整体测评。

4.3 测评力度

测评力度是在测评过程中实施测评工作的力度，反映测评的广度和深度，体现为测评工作的实际投入程度。测评广度越大，测评实施的范围越大，测评实施包含的测评对象就越多；测评深度越深，越需要在细节上展开，测评就越严格，因此就越需要更多的投入。投入越多，测评力度就越强，测评就越有保证。测评的广度和深度落实到访谈、检查和测试三种不同的测评方法上，能体现出测评实施过程中访谈、检查和测试的投入程度的不同。

信息安全等级保护要求不同安全保护等级的信息系统应具有不同的安全保护能力，满足相应等级的保护要求。为了检验不同安全保护等级的信息系统是否具有相应等级的安全保护能力，是否满足相应等级的保护要求，需要实施与其安全保护等级相适应的测评，付出相应的工作投入，达到应有的测评力度。第一级到第四级信息系统的测评力度反映在访谈、检查和测试等三种基本测评方法的测评广度和深度上，落实在不同单元测评中具体的测评实施上。不同安全保护等级的信息系统在总体上所对应的测评力度在附录 A 中描述。

4.4 使用方法

本标准第 5 章到第 8 章分别描述了第一级信息系统、第二级信息系统、第三级信息系统和第四级信息系统所有单元测评的内容，在章节上分别对应 GB/T 22239—2008 的第 5 章到第 8 章。在 GB/T 22239—2008 第 5 章到第 8 章中，各章的二级目录都分为安全技术和安全管理两部分，三级目录从安全层面（如物理安全、网络安全、主机安全等）进行划分和描述，四级目录按照安全控制点进行划分和描述（如主机安全层面下分为身份鉴别、访问控制、安全审计等），第五级目录是每一个安全控制点下面包括的具体安全要求项（以下简称“要求项”，这些要求项在本标准中被称为“测评指标”）。本标准中针对每一个安全控制点的测评就构成一个单元测评，单元测评中的每一个具体测评实施要求项（以下简称“测评要求项”）是与安全控制点下面所包括的要求项（测评指标）相对应的。在对每一要求项进行测评时，可能用到访谈、检查和测试三种测试方法，也可能用到其中一种或两种，为了描述简洁，在测评要求项中，没有针对每一个要求项分别进行描述，而是对具有相同测评方法的多个要求项进行了合并描述，但测评实施的内容完全覆盖了 GB/T 22239—2008 中所有要求项的测评要求，使用时，应当从单元测评的测评实施中抽取出对于 GB/T 22239—2008 中每一个要求项的测评要求，并按照这些测评要求开发测评指导书，以规范和指导安全等级测评活动。

测评过程中，测评人员应注意对测评记录和证据的采集、处理、存储和销毁，保护其在测评期间免遭破坏、更改或遗失，并保守秘密。

测评的最终输出是测评报告，测评报告应结合第 11 章的要求给出等级测评结论。

5 第一级信息系统单元测评

5.1 安全技术测评

5.1.1 物理安全

5.1.1.1 物理访问控制

5.1.1.1.1 测评指标

见 GB/T 22239—2008 中 5.1.1.1。

5.1.1.1.2 测评实施

本项要求包括：

a) 应检查机房出入口是否有专人负责控制人员出入；

b) 应检查是否有来访人员进入机房的登记记录。

5.1.1.1.3 结果判定

如果 5.1.1.1.2 中 a)和 b)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

5.1.1.2 防盗窃和防破坏

5.1.1.2.1 测评指标

见 GB/T 22239—2008 中 5.1.1.2。

5.1.1.2.2 测评实施

本项要求包括：

a) 应检查关键设备是否放置在机房内；

b) 应检查关键设备或主要部件是否固定；

c) 应检查关键设备或主要部件上是否设置明显的不易除去的标记。

5.1.1.2.3 结果判定

如果 5.1.1.2.2 中 a)～c)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

5.1.1.3 防雷击

5.1.1.3.1 测评指标

见 GB/T 22239—2008 中 5.1.1.3。

5.1.1.3.2 测评实施

本项要求包括：

a) 应访谈物理安全负责人，询问机房所在建筑物是否设置了避雷装置，是否通过验收或国家有关部门的技术检测；

b) 应检查机房所在建筑物的防雷验收文档是否有设置避雷装置的说明。

5.1.1.3.3 结果判定

如果5.1.1.3.2中a)和b)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

5.1.1.4 防火

5.1.1.4.1 测评指标

见GB/T 22239—2008中5.1.1.4。

5.1.1.4.2 测评实施

应检查机房是否设置了灭火设备，灭火设备是否是经消防检测部门检测合格的产品，其有效期是否合格。

5.1.1.4.3 结果判定

如果5.1.1.4.2为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

5.1.1.5 防水和防潮

5.1.1.5.1 测评指标

见GB/T 22239—2008中5.1.1.5。

5.1.1.5.2 测评实施

本项要求包括：

a) 应检查穿过机房墙壁或楼板的给水排水管道是否采取防渗漏和防结露等保护措施；

b) 应检查机房的窗户、屋顶和墙壁等是否未出现过漏水、渗透和返潮现象，机房的窗户、屋顶和墙壁是否进行过防水防渗处理。

5.1.1.5.3 结果判定

如果5.1.1.5.2中a)和b)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

5.1.1.6 温湿度控制

5.1.1.6.1 测评指标

见GB/T 22239—2008中5.1.1.6。

5.1.1.6.2 测评实施

应检查机房内是否有温湿度控制设施，温湿度控制设施是否正常运行，机房温度、相对湿度是否满足电子信息设备的使用要求。

5.1.1.6.3 结果判定

如果5.1.1.6.2为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合

本单元测评指标要求。

5.1.1.7 电力供应

5.1.1.7.1 测评指标

见 GB/T 22239—2008 中 5.1.1.7。

5.1.1.7.2 测评实施

应检查机房的计算机系统供电线路上是否设置了稳压器和过电压防护设备，这些设备是否正常运行。

5.1.1.7.3 结果判定

如果 5.1.1.7.2 为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

5.1.2 网络安全

5.1.2.1 结构安全

5.1.2.1.1 测评指标

见 GB/T 22239—2008 中 5.1.2.1。

5.1.2.1.2 测评实施

本项要求包括：

a) 应访谈网络管理员，询问关键网络设备的业务处理能力是否满足基本业务需求；

b) 应访谈网络管理员，询问接入网络及核心网络的带宽是否满足基本业务需要；

c) 应检查网络拓扑结构图，查看其与当前运行的实际网络系统是否一致。

5.1.2.1.3 结果判定

本项要求包括：

a) 如果 5.1.2.1.2c)中缺少网络拓扑结构图，则为否定；

b) 如果 5.1.2.1.2 中 a)～c)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

5.1.2.2 访问控制

5.1.2.2.1 测评指标

见 GB/T 22239—2008 中 5.1.2.2。

5.1.2.2.2 测评实施

本项要求包括：

a) 应访谈网络管理员，询问网络访问控制的措施有哪些；询问网络访问控制设备具备哪些访问控制功能；

b) 应检查边界网络设备，查看是否有正确的访问控制列表，以通过源地址、目的地址、源端口、目的端口、协议等进行网络数据流控制，其控制粒度是否至少为用户组。

5.1.2.2.3 结果判定

如果5.1.2.2.2b)为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

5.1.2.3 网络设备防护

5.1.2.3.1 测评指标

见GB/T 22239—2008中5.1.2.3。

5.1.2.3.2 测评实施

本项要求包括：

a) 应检查边界和关键网络设备的设备防护策略，查看是否配置了对登录用户进行身份鉴别的功能；

b) 应检查边界和关键网络设备的设备防护策略，查看是否配置了登录失败处理功能，包括结束会话、限制非法登录次数、登录连接超时自动退出等；

c) 应检查边界和关键网络设备的设备防护策略，查看是否配置了对设备远程管理所产生的鉴别信息进行保护的功能。

5.1.2.3.3 结果判定

如果5.1.2.3.2中a)～c)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

5.1.3 主机安全

5.1.3.1 身份鉴别

5.1.3.1.1 测评指标

见GB/T 22239—2008中5.1.3.1。

5.1.3.1.2 测评实施

应检查关键服务器操作系统和关键数据库管理系统的身份鉴别策略，查看是否提供了身份鉴别措施。

5.1.3.1.3 结果判定

如果5.1.3.1.2为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

5.1.3.2 访问控制

5.1.3.2.1 测评指标

见GB/T 22239—2008中5.1.3.2。

5.1.3.2.2 测评实施

本项要求包括：

a) 应检查关键服务器操作系统的访问控制策略，查看是否对重要文件的访问权限进行了限制，对系统不需要的服务、共享路径等进行了禁用或删除；
b) 应检查关键服务器操作系统和关键数据库管理系统的访问控制策略，查看是否已禁用或者限制匿名/默认账户的访问权限，是否重命名系统默认账户、修改这些账户的默认口令；
c) 应检查关键服务器操作系统和关键数据库管理系统的访问控制策略，是否删除了系统中多余的、过期的以及共享的账户；
d) 应检查关键服务器操作系统和关键数据库管理系统的权限设置情况，查看是否依据安全策略对用户权限进行了限制。

5.1.3.2.3 结果判定

如果5.1.3.2.2中a)～d)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

5.1.3.3 入侵防范

5.1.3.3.1 测评指标

见GB/T 22239—2008中5.1.3.3。

5.1.3.3.2 测评实施

本项要求包括：
a) 应访谈系统管理员，询问关键服务器操作系统和关键数据库管理系统中所安装的系统组件和应用程序是否都是必须的；
b) 应检查关键服务器操作系统和关键数据库管理系统的补丁是否得到了及时更新。

5.1.3.3.3 结果判定

如果5.1.3.3.2中a)和b)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

5.1.3.4 恶意代码防范

5.1.3.4.1 测评指标

见GB/T 22239—2008中5.1.3.4。

5.1.3.4.2 测评实施

应检查关键服务器的恶意代码防范策略，查看是否安装了实时检测与查杀恶意代码的软件产品，并且及时更新了软件版本和恶意代码库。

5.1.3.4.3 结果判定

如果5.1.3.4.2为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

5.1.4 应用安全

5.1.4.1 身份鉴别

5.1.4.1.1 测评指标

见GB/T 22239—2008中5.1.4.1。

5.1.4.1.2 测评实施

本项要求包括：

a) 应检查关键应用系统，查看是否提供身份标识和鉴别功能；

b) 应检查关键应用系统，查看是否提供登录失败处理功能，是否根据安全策略设置了登录失败次数等参数。

5.1.4.1.3 结果判定

如果5.1.4.1.2中a)和b)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

5.1.4.2 访问控制

5.1.4.2.1 测评指标

见GB/T 22239—2008中5.1.4.2。

5.1.4.2.2 测评实施

本项要求包括：

a) 应检查关键应用系统，查看系统是否提供访问控制功能控制用户组或用户对系统功能和用户数据的访问；

b) 应检查关键应用系统，查看是否限制了默认账户的访问权限，是否修改了这些账户的默认口令；

c) 应检查关键应用系统，查看是否删除多余的、过期的账户。

5.1.4.2.3 结果判定

如果5.1.4.2.2中a)～c)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

5.1.4.3 通信完整性

5.1.4.3.1 测评指标

见GB/T 22239—2008中5.1.4.3。

5.1.4.3.2 测评实施

应检查设计、验收文档或源代码，查看是否有关于保护通信完整性的描述。

5.1.4.3.3 结果判定

如果5.1.4.3.2为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

5.1.4.4 软件容错

5.1.4.4.1 测评指标

见GB/T 22239—2008中5.1.4.4。

5.1.4.4.2 测评实施

本项要求包括：

a) 应检查设计或验收文档，查看应用系统有对人机接口输入或通信接口输入的数据进行有效性检验功能的说明；

b) 应测试关键应用系统，查看应用系统是否能明确拒绝不符合格式要求数据。

5.1.4.4.3 结果判定

如果5.1.4.4.2中a)和b)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

5.1.5 数据安全及备份恢复

5.1.5.1 数据完整性

5.1.5.1.1 测评指标

见GB/T 22239—2008中5.1.5.1。

5.1.5.1.2 测评实施

应检查应用系统的设计、验收文档或源代码，查看是否有关于能检测重要业务数据传输过程中完整性受到破坏的描述。

5.1.5.1.3 结果判定

如果5.1.5.1.2为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

5.1.5.2 备份和恢复

5.1.5.2.1 测评指标

见GB/T 22239—2008中5.1.5.2。

5.1.5.2.2 测评实施

应检查是否对关键网络设备、关键主机操作系统、关键数据库管理系统和关键应用系统的重要信息进行了备份，并定期进行恢复测试。

5.1.5.2.3 结果判定

如果5.1.5.2.2为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

5.2 安全管理测评

5.2.1 安全管理制度

5.2.1.1 管理制度

5.2.1.1.1 测评指标

见GB/T 22239—2008中5.2.1.1。

5.2.1.1.2 测评实施

应检查各项安全管理制度，查看是否覆盖物理、网络、主机系统、数据、应用、建设和运维等层面。

5.2.1.1.3 结果判定

如果5.2.1.1.2为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

5.2.1.2 制定和发布

5.2.1.2.1 测评指标

见GB/T 22239—2008中5.2.1.2。

5.2.1.2.2 测评实施

本项要求包括：

a) 应访谈系统安全负责人，询问是否由专人负责制定安全管理制度；

b) 应访谈系统安全负责人，询问安全管理制度是否能够发布到相关人员手中。

5.2.1.2.3 结果判定

如果5.2.1.2.2中a)和b)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

5.2.2 安全管理机构

5.2.2.1 岗位设置

5.2.2.1.1 测评指标

见GB/T 22239—2008中5.2.2.1。

5.2.2.1.2 测评实施

本项要求包括：

a) 应访谈系统安全负责人，询问信息系统是否设置了相关管理岗位，各个岗位的职责分工是否明确；

b) 应检查岗位职责分工文档，查看是否明确了相关岗位的职责。

5.2.2.1.3 结果判定

如果5.2.2.1.2中a)和b)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

5.2.2.2 人员配备

5.2.2.2.1 测评指标

见GB/T 22239—2008中5.2.2.2。

5.2.2.2.2 测评实施

本项要求包括：

a) 应访谈系统安全负责人，询问各个安全管理岗位是否配备了一定数量的人员；

b) 应检查安全管理各岗位人员信息表，查看其是否明确相关岗位的人员信息。

5.2.2.2.3 结果判定

如果5.2.2.2.2中a)和b)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

5.2.2.3 授权和审批

5.2.2.3.1 测评指标

见GB/T 22239—2008中5.2.2.3。

5.2.2.3.2 测评实施

应访谈系统安全负责人，询问是否对信息系统中的关键活动进行审批，审批活动是否得到授权。

5.2.2.3.3 结果判定

如果5.2.2.3.2为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

5.2.2.4 沟通和合作

5.2.2.4.1 测评指标

见GB/T 22239—2008中5.2.2.4。

5.2.2.4.2 测评实施

本项要求包括：

a) 应访谈系统安全负责人，询问是否与公安机关、电信公司和兄弟单位建立联系；

b) 应检查外联单位说明文档，查看外联单位是否包含公安机关、电信公司及兄弟单位，是否说明外联单位的联系人和联系方式等内容。

5.2.2.4.3 结果判定

如果5.2.2.4.2中a)和b)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

5.2.3 人员安全管理

5.2.3.1 人员录用

5.2.3.1.1 测评指标

见GB/T 22239—2008中5.2.3.1。

5.2.3.1.2 测评实施

本项要求包括：

a) 应访谈人事负责人，询问是否由专门的部门或人员负责人员的录用工作；

b) 应访谈人事负责人，询问在人员录用时是否对被录用人的身份和专业资格进行审查；

c) 应检查人员录用管理文档，查看是否说明录用人员应具备的条件（如学历、学位要求，技术人员应具备的专业技术水平，管理人员应具备的安全管理知识等）；

d) 应检查是否具有人员录用时对录用人身份、专业资格等进行审查的相关文档或记录等。

5.2.3.1.3 结果判定

如果5.2.3.1.2中a)～d)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

5.2.3.2 人员离岗

5.2.3.2.1 测评指标

见GB/T 22239—2008中5.2.3.2。

5.2.3.2.2 测评实施

本项要求包括：

a) 应访谈系统安全负责人，询问是否及时终止离岗人员的所有访问权限，取回各种身份证件、钥匙、徽章以及机构提供的软硬件设备等；

b) 应检查是否具有离岗人员交还身份证件、设备等的登记记录。

5.2.3.2.3 结果判定

如果5.2.3.2.2中a)和b)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

5.2.3.3 安全意识教育和培训

5.2.3.3.1 测评指标

见GB/T 22239—2008中5.2.3.3。

5.2.3.3.2 测评实施

应访谈系统安全负责人，询问是否对各个岗位人员进行安全教育和岗位技能培训，告知相关的安全知识、安全责任和惩戒措施。

5.2.3.3.3 结果判定

如果5.2.3.3.2为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

5.2.3.4 外部人员访问管理

5.2.3.4.1 测评指标

见GB/T 22239—2008中5.2.3.4。

5.2.3.4.2 测评实施

本项要求包括：

a) 应访谈系统安全负责人，询问外部人员访问重要区域(如访问机房、重要服务器或设备区等)是否需经有关部门或负责人批准；

b) 应检查外部人员访问管理文档，查看是否具有规范外部人员访问机房等重要区域需经过相关部门或负责人批准的管理要求。

5.2.3.4.3 结果判定

如果5.2.3.4.2中a)和b)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

5.2.4 系统建设管理

5.2.4.1 系统定级

5.2.4.1.1 测评指标

见GB/T 22239—2008中5.2.4.1。

5.2.4.1.2 测评实施

本项要求包括：

a) 应访谈系统建设负责人，询问是否参照定级指南确定信息系统安全保护等级；

b) 应检查系统定级文档，查看文档是否明确信息系统的边界和信息系统的安全保护等级，是否说明定级的方法和理由，是否有相关部门或主管领导的盖章或签名。

5.2.4.1.3 结果判定

如果5.2.4.1.2中a)和b)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

5.2.4.2 安全方案设计

5.2.4.2.1 测评指标

见GB/T 22239—2008中5.2.4.2。

5.2.4.2.2 测评实施

本项要求包括：

a) 应访谈系统建设负责人，询问是否依据风险分析的结果补充和调整过安全措施，具体做过哪些调整；

b) 应检查系统的安全设计方案，查看方案是否描述系统的安全保护等级，是否描述系统的安全保护策略，是否根据系统的安全级别选择了安全措施；

c) 应检查系统的安全设计方案，查看是否详细描述安全措施的实现内容，是否有安全产品的功能、性能和部署等描述，是否有安全建设的费用和计划等。

5.2.4.2.3 结果判定

如5.2.4.2.2中a)～c)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或

部分符合本单元测评指标要求。

5.2.4.3 产品采购和使用

5.2.4.3.1 测评指标

见 GB/T 22239—2008 中 5.2.4.3。

5.2.4.3.2 测评实施

应访谈系统建设负责人，询问系统使用的有关信息安全产品是否符合国家的有关规定，如安全产品获得了销售许可证等。

5.2.4.3.3 结果判定

如果 5.2.4.3.2 为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

5.2.4.4 自行软件开发

5.2.4.4.1 测评指标

见 GB/T 22239—2008 中 5.2.4.4。

5.2.4.4.2 测评实施

本项要求包括：

a) 应访谈系统建设负责人，询问是否进行自主开发软件；
b) 应访谈系统建设负责人，询问自主开发软件是否在独立的环境中完成编码和调试，如相对独立的网络区域，询问软件设计相关文档是否由专人负责保管，负责人是何人；
c) 应检查网络拓扑图和实际开发环境，查看是否实际运行环境和开发环境有效隔离。

5.2.4.4.3 结果判定

如果 5.2.4.4.2 中 a)～c)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

5.2.4.5 外包软件开发

5.2.4.5.1 测评指标

见 GB/T 22239—2008 中 5.2.4.5。

5.2.4.5.2 测评实施

本项要求包括：

a) 应访谈系统建设负责人，询问软件交付前是否依据开发要求的技术指标对软件功能和性能等进行验收测试，软件安装之前是否检测软件中的恶意代码；
b) 应检查是否具有软件开发的相关文档，如需求分析说明书、软件设计说明书等，是否具有软件操作手册或使用指南。

5.2.4.5.3 结果判定

如果 5.2.4.5.2 中 a)和 b)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合

或部分符合本单元测评指标要求。

5.2.4.6 工程实施

5.2.4.6.1 测评指标

见 GB/T 22239—2008 中 5.2.4.6。

5.2.4.6.2 测评实施

应访谈系统建设负责人，询问是否指定专门部门或人员对工程实施过程进行进度和质量控制，由何部门/何人负责。

5.2.4.6.3 结果判定

如果 5.2.4.6.2 为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

5.2.4.7 测试验收

5.2.4.7.1 测评指标

见 GB/T 22239—2008 中 5.2.4.7。

5.2.4.7.2 测评实施

本项要求包括：

a) 应访谈系统建设负责人，询问在信息系统建设完成后是否对其进行安全性测试验收；
b) 应检查是否具有工程测试验收方案，查看其是否明确说明参与测试的部门、人员、测试验收内容、现场操作过程等内容；
c) 应检查是否具有系统测试验收报告。

5.2.4.7.3 结果判定

如果 5.2.4.7.2 中 a)～c)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

5.2.4.8 系统交付

5.2.4.8.1 测评指标

见 GB/T 22239—2008 中 5.2.4.8。

5.2.4.8.2 测评实施

本项要求包括：

a) 应访谈系统建设负责人，询问系统交接工作是否根据交付清单对所交接的设备、文档、软件等进行清点；
b) 应访谈系统建设负责人，询问系统正式运行前是否对运行维护人员进行过培训，针对哪些方面进行过培训；
c) 应检查是否具有系统交付清单，查看交付清单是否说明系统交付的各类设备、软件、文档等；
d) 应检查系统交付提交的文档，查看是否有指导用户进行系统运维的文档等。

5.2.4.8.3 结果判定

如果5.2.4.8.2中a)～d)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

5.2.4.9 安全服务商选择

5.2.4.9.1 测评指标

见GB/T 22239—2008中5.2.4.9。

5.2.4.9.2 测评实施

本项要求包括：

a) 应访谈系统建设负责人，询问信息系统选择的安全服务商有哪些，是否符合国家有关规定；

b) 应检查是否具有与安全服务商签订的安全责任合同书或保密协议等文档，查看其内容是否包含保密范围、安全责任、违约责任、协议的有效期限和责任人的签字等。

5.2.4.9.3 结果判定

如果5.2.4.9.2中a)和b)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

5.2.5 系统运维管理

5.2.5.1 环境管理

5.2.5.1.1 测评指标

见GB/T 22239—2008中5.2.5.1。

5.2.5.1.2 测评实施

本项要求包括：

a) 应访谈系统运维负责人，询问是否有专门的部门或人员对机房供配电、空调、温湿度控制等设施进行定期维护，由何部门/何人负责，维护周期多长；

b) 应访谈系统运维负责人，询问是否有专门的部门或人员对机房的出入、服务器开机/关机等日常工作进行管理，由何部门/何人负责；

c) 应检查是否有机房安全管理制度，查看其内容是否覆盖机房物理访问、物品带进/带出机房和机房环境安全等方面。

5.2.5.1.3 结果判定

如果5.2.5.1.2中a)～c)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

5.2.5.2 资产管理

5.2.5.2.1 测评指标

见GB/T 22239—2008中5.2.5.2。

5.2.5.2.2 测评实施

应检查是否有资产清单，查看其内容是否覆盖资产责任部门、责任人、所处位置和重要程度等方面。

5.2.5.2.3 结果判定

如果5.2.5.2.2为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

5.2.5.3 介质管理

5.2.5.3.1 测评指标

见GB/T 22239—2008中5.2.5.3。

5.2.5.3.2 测评实施

本项要求包括：

a) 应访谈资产管理员，询问介质的存放环境是否采取保护措施防止介质被盗、被毁等；

b) 应访谈资产管理员，询问是否根据介质的目录清单对介质的使用现状进行定期检查；

c) 应检查介质使用管理记录，查看其是否记录介质归档和使用等情况。

5.2.5.3.3 结果判定

如果5.2.5.3.2中a)～c)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

5.2.5.4 设备管理

5.2.5.4.1 测评指标

见GB/T 22239—2008中5.2.5.4。

5.2.5.4.2 测评实施

本项要求包括：

a) 应访谈系统运维负责人，询问是否有专门的部门或人员对各种设备、线路进行定期维护，由何部门/何人负责，维护周期多长；

b) 应检查是否有设备安全管理制度，查看其内容是否对各种软硬件设备的选型、采购、发放和领用等环节进行规定。

5.2.5.4.3 结果判定

如果5.2.5.4.2中a)和b)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

5.2.5.5 网络安全管理

5.2.5.5.1 测评指标

见GB/T 22239—2008中5.2.5.5。

5.2.5.5.2 测评实施

本项要求包括：

a) 应访谈系统运维负责人，询问是否指定专门的部门或人员负责网络管理，维护网络运行日志、监控记录，分析处理报警信息等；

b) 应访谈网络管理员，询问是否定期对网络进行漏洞扫描，扫描周期多长，发现漏洞是否及时修补；

c) 应检查是否有网络漏洞扫描报告，检查扫描时间间隔与扫描周期是否一致。

5.2.5.5.3 结果判定

如果5.2.5.5.2中a)～c)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

5.2.5.6 系统安全管理

5.2.5.6.1 测评指标

见GB/T 22239—2008中5.2.5.6。

5.2.5.6.2 测评实施

本项要求包括：

a) 应访谈系统运维负责人，询问是否指定专门的部门或人员负责系统管理，如根据业务需求和系统安全分析制定系统的访问控制策略，控制分配文件及服务的访问权限；

b) 应访谈系统管理员，询问是否定期对系统进行漏洞扫描，扫描周期多长，发现漏洞是否及时修补，在安装系统补丁前是否对重要文件进行备份；

c) 应检查是否有系统漏洞扫描报告，检查扫描时间间隔与扫描周期是否一致。

5.2.5.6.3 结果判定

如果5.2.5.6.2中a)～c)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

5.2.5.7 恶意代码防范管理

5.2.5.7.1 测评指标

见GB/T 22239—2008中5.2.5.7。

5.2.5.7.2 测评实施

应访谈系统运维负责人，询问是否对员工进行基本恶意代码防范意识的教育，是否告知应及时升级软件版本，使用外来设备、网络上接收文件和外来计算机或存储设备接入网络系统之前应进行病毒检查等。

5.2.5.7.3 结果判定

如果5.2.5.7.2为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

5.2.5.8 备份与恢复管理

5.2.5.8.1 测评指标

见 GB/T 22239—2008 中 5.2.5.8。

5.2.5.8.2 测评实施

本项要求包括：

a) 应访谈系统运维负责人，询问是否识别出需要定期备份的业务信息、系统数据和软件系统，主要有哪些；

b) 应检查备份管理文档，查看其是否明确了备份方式、备份频度、存储介质和保存期等方面内容。

5.2.5.8.3 结果判定

如果 5.2.5.8.2 中 a)和 b)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

5.2.5.9 安全事件处置

5.2.5.9.1 测评指标

见 GB/T 22239—2008 中 5.2.5.9。

5.2.5.9.2 测评实施

本项要求包括：

a) 应访谈系统运维负责人，询问是否告知用户在发现安全弱点和可疑事件时应及时报告；

b) 应检查是否有安全事件报告和处置管理制度，查看其是否明确安全事件的现场处理、事件报告和后期恢复等内容。

5.2.5.9.3 结果判定

如果 5.2.5.9.2 中 a)和 b)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

6 第二级信息系统单元测评

6.1 安全技术测评

6.1.1 物理安全

6.1.1.1 物理位置的选择

6.1.1.1.1 测评指标

见 GB/T 22239—2008 中 6.1.1.1。

6.1.1.1.2 测评实施

本项要求包括：

a) 应访谈物理安全负责人，询问机房和办公场地所在建筑物是否具有防震、防风和防雨等能力；

b) 应检查是否有机房和办公场地所在建筑物抗震设防审批文档；

c) 应检查机房和办公场地所在建筑物是否具有防风和防雨等能力。

6.1.1.1.3 结果判定

如果6.1.1.1.2中a)～c)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

6.1.1.2 物理访问控制

6.1.1.2.1 测评指标

见GB/T 22239—2008中6.1.1.2。

6.1.1.2.2 测评实施

本项要求包括：

a) 应检查机房出入口是否有专人值守负责控制并鉴别进入机房的人员，是否有值守记录；

b) 应检查机房是否不存在专人值守之外的其他开放的出入口；

c) 应检查是否有来访人员进入机房的登记记录；

d) 应检查是否有来访人员进入机房的申请、审批记录，查看申请、审批记录是否包括来访人员的访问范围；

e) 应检查来访人员进入机房时是否有专人陪同。

6.1.1.2.3 结果判定

如果6.1.1.2.2中a)～e)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

6.1.1.3 防盗窃和防破坏

6.1.1.3.1 测评指标

见GB/T 22239—2008中6.1.1.3。

6.1.1.3.2 测评实施

本项要求包括：

a) 应检查重要设备等是否放置在机房内；

b) 应检查重要设备等或设备的主要部件是否固定；

c) 应检查重要设备等或设备的主要部件上是否设置明显的不易除去的标记；

d) 应检查通信线缆铺设是否暗敷或在不易被发现的地方；

e) 应检查主机房是否安装防盗报警设施，防盗报警设施是否正常运行，是否通过了国家相关部门检验，并查看是否有防盗报警设施的运行记录；

f) 应检查介质是否有分类标识，是否分类存放在介质库或档案室内。

6.1.1.3.3 结果判定

如果6.1.1.3.2中a)～f)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

6.1.1.4 防雷击

6.1.1.4.1 测评指标

见 GB/T 22239—2008 中 6.1.1.4。

6.1.1.4.2 测评实施

本项要求包括：

a) 应访谈物理安全负责人，询问机房所在建筑物是否设置了避雷装置，是否通过验收或国家有关部门的技术检测；

b) **应访谈物理安全负责人，询问机房是否设置有交流电源地线；**

c) 应检查机房所在建筑物的防雷验收文档中是否有设置避雷装置的说明；

d) **应检查机房防雷验收文档中是否有设置交流电源地线的说明。**

6.1.1.4.3 结果判定

如果 6.1.1.4.2 中 a)～d)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

6.1.1.5 防火

6.1.1.5.1 测评指标

见 GB/T 22239—2008 中 6.1.1.5。

6.1.1.5.2 测评实施

本项要求包括：

a) 应检查机房是否设置了灭火设备，灭火设备是否是经消防检测部门检测合格的产品，其有效期是否合格；

b) **应检查机房是否部署了火灾自动报警系统，火灾自动报警系统是否是经消防检测部门检测合格的产品，是否处于正常运行状态，是否有火灾自动报警系统的运行记录。**

6.1.1.5.3 结果判定

如果 6.1.1.5.2 中 a)和 b)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

6.1.1.6 防水和防潮

6.1.1.6.1 测评指标

见 GB/T 22239—2008 中 6.1.1.6。

6.1.1.6.2 测评实施

本项要求包括：

a) **应检查机房屋顶或活动地板下是否未安装水管；**

b) 应检查穿过机房墙壁或楼板的给水排水管道是否采取防渗漏和防结露等保护措施；

c) 应检查机房的窗户、屋顶和墙壁等是否未出现过漏水、渗透和返潮现象，机房的窗户、屋顶和墙

壁是否进行过防水防渗处理；

d) 如果机房内安装有空调机和加湿器，应检查是否设置了挡水和排水设施；

e) 如果机房位于湿度较高的地区，应检查机房是否有除湿装置并能够正常运行，是否有防水防潮处理记录。

6.1.1.6.3 结果判定

如果6.1.1.6.2中a)～e)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

6.1.1.7 防静电

6.1.1.7.1 测评指标

见GB/T 22239—2008中6.1.1.7。

6.1.1.7.2 测评实施

应检查重要设备是否有接地构造或其他静电泄放措施。

6.1.1.7.3 结果判定

如果6.1.1.7.2为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

6.1.1.8 温湿度控制

6.1.1.8.1 测评指标

见GB/T 22239—2008中6.1.1.8。

6.1.1.8.2 测评实施

本项要求包括：

a) 应检查机房内是否配备了温湿度自动调节设施，温湿度自动调节设施是否能够正常运行，机房温度、相对湿度是否满足电子信息设备的使用要求；

b) 应检查是否有机房的温湿度记录，是否有温湿度自动调节设施的运行记录。

6.1.1.8.3 结果判定

如果6.1.1.8.2中a)和b)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

6.1.1.9 电力供应

6.1.1.9.1 测评指标

见GB/T 22239—2008中6.1.1.9。

6.1.1.9.2 测评实施

本项要求包括：

a) 应检查机房的计算机系统供电线路上是否设置了稳压器和过电压防护设备，这些设备是否正

常运行。

b) **应检查机房计算机系统是否配备了短期备用电源设备，备用电源设备是否正常运行。**

6.1.1.9.3 结果判定

如果 6.1.1.9.2 中 a)和 b)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

6.1.1.10 电磁防护

6.1.1.10.1 测评指标

见 GB/T 22239—2008 中 6.1.1.10。

6.1.1.10.2 测评实施

应检查机房布线，查看是否做到电源线和通信线缆隔离。

6.1.1.10.3 结果判定

如果 6.1.1.10.2 为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

6.1.2 网络安全

6.1.2.1 结构安全

6.1.2.1.1 测评指标

见 GB/T 22239—2008 中 6.1.2.1。

6.1.2.1.2 测评实施

本项要求包括：

a) **应检查网络设计或验收文档，查看是否有满足关键网络设备业务处理能力需要的设计或描述；**

b) **应检查网络设计或验收文档，查看是否有满足接入网络及核心网络的带宽业务高峰期需要的设计或描述；**

c) 应检查网络拓扑结构图，查看其与当前运行的实际网络系统是否一致；

d) **应检查网络设计或验收文档，查看是否有根据各部门的工作职能、重要性和所涉及信息的重要程度等因素，划分不同的子网或网段，并按照方便管理和控制的原则为各子网和网段分配地址段的设计或描述。**

6.1.2.1.3 结果判定

如果 6.1.2.1.2 中 a)～d)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

6.1.2.2 访问控制

6.1.2.2.1 测评指标

见 GB/T 22239—2008 中 6.1.2.2。

6.1.2.2.2 测评实施

本项要求包括：

a) **应检查边界网络设备的访问控制策略，查看其是否根据会话状态信息对数据流进行控制，控制粒度是否为网段级；**

b) 应检查边界网络设备的访问控制策略，查看是否按用户和系统之间的允许访问规则，允许或拒绝对受控系统进行访问，且控制力度为**单个用户**；

c) **应检查边界网络设备的拨号用户列表，查看其是否对具有拨号访问权限的用户数量进行限制。**

6.1.2.2.3 结果判定

如果 6.1.2.2.2 中 a)～c)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

6.1.2.3 安全审计

6.1.2.3.1 测评指标

见 GB/T 22239—2008 中 6.1.2.3。

6.1.2.3.2 测评实施

本项要求包括：

a) **应检查边界和关键网络设备的安全审计策略，查看其是否包括网络设备运行状况、网络流量、用户行为等；**

b) **应检查边界和关键网络设备的安全审计记录，查看其是否包括：事件的日期和时间、用户、事件类型、事件成功情况及其他与审计相关的信息。**

6.1.2.3.3 结果判定

如果 6.1.2.3.2 中 a)和 b)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

6.1.2.4 边界完整性检查

6.1.2.4.1 测评指标

见 GB/T 22239—2008 中 6.1.2.4。

6.1.2.4.2 测评实施

应检查边界完整性检查设备的非法外联监控策略，查看是否正确设置了对网络内部用户私自连接到外部网络的行为进行有效监控的配置。

6.1.2.4.3 结果判定

如果 6.1.2.4.2 为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合本单元测评指标要求。

6.1.2.5 入侵防范

6.1.2.5.1 测评指标

见 GB/T 22239—2008 中 6.1.2.5。

6.1.2.5.2 测评实施

本项要求包括：

a) 应检查网络入侵防范设备，查看是否能检测以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP 碎片攻击、网络蠕虫攻击等；

b) 应检查网络入侵防范设备的规则库版本，查看其规则库是否及时更新。

6.1.2.5.3 结果判定

如果 6.1.2.5.2 中 a)和 b)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

6.1.2.6 网络设备防护

6.1.2.6.1 测评指标

见 GB/T 22239—2008 中 6.1.2.6。

6.1.2.6.2 测评实施

本项要求包括：

a) 应检查边界和关键网络设备的设备防护策略，查看是否配置了对登录用户进行身份鉴别的功能；

b) 应检查边界和关键网络设备的设备防护策略，查看是否对网络设备的登录地址进行了限制；

c) 应检查边界和关键网络设备的账户列表，查看用户标识是否唯一；

d) 应检查边界和关键网络设备的设备防护策略，查看是否对口令的复杂度和定期修改进行了设置；

e) 应检查边界和关键网络设备的设备防护策略，查看是否配置了登录失败处理功能，包括结束会话、限制非法登录次数、登录连接超时自动退出等；

f) 应检查边界和关键网络设备的设备防护策略，查看是否配置了对设备远程管理所产生的鉴别信息进行保护的功能。

6.1.2.6.3 结果判定

如果 6.1.2.6.2 中 a)～f)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

6.1.3 主机安全

6.1.3.1 身份鉴别

6.1.3.1.1 测评指标

见 GB/T 22239—2008 中 6.1.3.1。

6.1.3.1.2 测评实施

本项要求包括：

a) 应检查重要服务器操作系统和重要数据库管理系统的身份鉴别策略，查看是否提供了身份鉴别措施；

b) 应检查重要服务器操作系统和重要数据库管理系统的身份鉴别策略，查看其身份鉴别信息是否具有不易被冒用的特点，如对用户登录口令的最小长度、复杂度和更换周期进行要求和限制；

c) 应检查重要服务器操作系统和重要数据库管理系统的身份鉴别策略，查看是否配置了登录失败处理功能、设置了非法登录次数的限制值；查看是否设置网络登录连接超时，并自动退出；

d) 应访谈系统管理员和数据库管理员，询问是否对操作系统和数据库管理系统采用了远程管理方式，如果采用远程管理方式，查看是否具有防止鉴别信息在网络传输过程中被窃听的措施；

e) 应检查重要服务器操作系统和重要数据库管理系统账户列表，查看管理员用户名或 UID 分配是否唯一。

6.1.3.1.3 结果判定

如果 6.1.3.1.2 中 a)～e)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

6.1.3.2 访问控制

6.1.3.2.1 测评指标

见 GB/T 22239—2008 中 6.1.3.2。

6.1.3.2.2 测评实施

本项要求包括：

a) 应检查重要服务器操作系统的访问控制策略，查看是否对重要文件的访问权限进行了限制，对系统不需要的服务、共享路径等进行了禁用或删除；

b) 应检查重要数据库管理系统的特权用户和重要操作系统的特权用户，查看不同管理员的系统账户权限是否不同，且不应由同一人担任；

c) 应检查重要服务器操作系统和重要数据库管理系统的访问控制策略，查看是否已禁用或者限制匿名/默认账户的访问权限，是否重命名系统默认账户、修改这些账户的默认口令；

d) 应检查重要服务器操作系统和重要数据库管理系统的访问控制策略，是否删除了系统中多余的、过期的以及共享的账户；

e) 应检查重要服务器操作系统和重要数据库管理系统的权限设置情况，查看是否依据安全策略对用户权限进行了限制。

6.1.3.2.3 结果判定

如果 6.1.3.2.2 中 a)～e)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

6.1.3.3 安全审计

6.1.3.3.1 测评指标

见 GB/T 22239—2008 中 6.1.3.3。

6.1.3.3.2 测评实施

本项要求包括：

a) 应检查重要服务器操作系统和重要数据库管理系统的安全审计策略，查看安全审计配置是否包括系统内重要用户行为、系统资源的异常和重要系统命令的使用等重要的安全相关事件；

b) 应检查重要服务器操作系统和重要数据库管理系统的安全审计策略，查看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、事件的结果等内容；

c) 应检查重要服务器操作系统和重要数据库管理系统的安全审计策略，查看是否通过日志覆盖周期、存储方式、日志文件/空间大小、日志文件操作权限等设置，实现了对审计记录的保护，使其避免受到未预期的删除、修改或覆盖等。

6.1.3.3.3 结果判定

如果6.1.3.3.2中a)～c)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

6.1.3.4 入侵防范

6.1.3.4.1 测评指标

见GB/T 22239—2008中6.1.3.4。

6.1.3.4.2 测评实施

本项要求包括：

a) 应访谈系统管理员，询问重要服务器操作系统和重要数据库管理系统中所安装的系统组件和应用程序是否都是必须的；

b) 应检查是否设置了专门的升级服务器实现对重要服务器操作系统补丁的升级；

c) 应检查重要服务器操作系统和重要数据库管理系统的补丁是否得到了及时更新。

6.1.3.4.3 结果判定

如果6.1.3.4.2中a)～c)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

6.1.3.5 恶意代码防范

6.1.3.5.1 测评指标

见GB/T 22239—2008中6.1.3.5。

6.1.3.5.2 测评实施

本项要求包括：

a) 应检查重要服务器的恶意代码防范策略，查看是否安装了实时检测与查杀恶意代码的软件产品，并且及时更新了软件版本和恶意代码库；

b) 应检查防恶意代码软件是否实现了统一管理。

6.1.3.5.3 结果判定

如果6.1.3.5.2中a)和b)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合

或部分符合本单元测评指标要求。

6.1.3.6 资源控制

6.1.3.6.1 测评指标

见 GB/T 22239—2008 中 6.1.3.6。

6.1.3.6.2 测评实施

本项要求包括：

a) 应检查重要服务器操作系统和重要数据库管理系统的资源控制策略，查看是否设定终端接入方式、网络地址范围等条件限制终端登录；

b) 应检查访问重要服务器的终端是否都设置了操作超时锁定的配置；

c) 应检查重要服务器操作系统和重要数据库管理系统的资源控制策略，查看是否设置了单个用户或应用对系统资源的最大或最小使用限度。

6.1.3.6.3 结果判定

如果 6.1.3.6.2 中 a)～c)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

6.1.4 应用安全

6.1.4.1 身份鉴别

6.1.4.1.1 测评指标

见 GB/T 22239—2008 中 6.1.4.1。

6.1.4.1.2 测评实施

本项要求包括：

a) 应检查关键应用系统，查看是否提供身份标识和鉴别功能；

b) 应检查关键应用系统，查看是否采用了措施保证身份标识具有唯一性，是否对登录用户的口令最小长度、复杂度和更换周期等进行了要求和限制，保证身份鉴别信息不易被冒用；

c) 应检查关键应用系统，查看其提供的登录失败处理功能，是否根据安全策略设置了登录失败次数等参数；

d) 应测试关键应用系统，可通过试图以合法和非法用户分别登录系统，查看是否成功，验证身份标识和鉴别功能是否有效；

e) 应测试关键应用系统，可通过多次输入错误的密码，查看系统的处理方式，验证登录失败处理功能是否有效。

6.1.4.1.3 结果判定

如果 6.1.4.1.2 中 a)～e)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

6.1.4.2 访问控制

6.1.4.2.1 测评指标

见 GB/T 22239—2008 中 6.1.4.2。

6.1.4.2.2 测评实施

本项要求包括：

a) 应检查关键应用系统，查看系统是否提供访问控制功能控制用户对客体的访问；

b) 应检查关键应用系统，查看其访问控制的覆盖范围是否包括与信息安全直接相关的主体、客体及它们之间的操作；访问控制的粒度是否达到主体为用户级，客体为文件、数据库表级；

c) 应检查关键应用系统，查看是否有由授权用户设置其他用户访问系统功能和用户数据的权限的功能，是否限制默认用户的访问权限，是否修改了这些账户的默认口令；

d) 应检查关键应用系统，查看是否删除多余的、过期的账户；

e) 应检查关键应用系统用户角色或权限的分配情况，查看是否授予不同账户为完成各自承担任务所需的最小权限，特权用户的权限是否分离，权限之间是否相互制约；

f) 应测试关键应用系统，可通过以不同权限的用户登录系统，查看其拥有的权限是否与系统赋予的权限一致，验证应用系统访问控制功能是否有效。

6.1.4.2.3 结果判定

如果 6.1.4.2.2 中 a)～f)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

6.1.4.3 安全审计

6.1.4.3.1 测评指标

见 GB/T 22239—2008 中 6.1.4.3。

6.1.4.3.2 测评实施

本项要求包括：

a) 应检查关键应用系统，查看审计范围是否覆盖到每个用户，审计策略是否覆盖系统内重要的安全相关事件，例如，用户标识与鉴别、访问控制的所有操作记录、重要用户行为、系统资源的异常使用、重要系统命令的使用等；

b) 应检查关键应用系统的审计记录，查看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、事件的结果等内容；

c) 应测试重要应用系统，在应用系统上试图产生一些重要的安全相关事件(如用户登录、修改用户权限等)，查看应用系统是否对其进行了审计，验证应用系统安全审计的覆盖情况是否覆盖到每个用户；如果进行了审计则查看审计记录内容是否包含事件的日期、时间、发起者信息、类型、描述和结果等；

d) 应测试重要应用系统，试图非授权删除、修改或覆盖审计记录，验证安全审计的保护情况是否无法非授权删除、修改或覆盖审计记录。

6.1.4.3.3 结果判定

如果 6.1.4.3.2 中 a)～d)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

6.1.4.4 通信完整性

6.1.4.4.1 测评指标

见 GB/T 22239—2008 中 6.1.4.4。

6.1.4.4.2 测评实施

本项要求包括：

a) 应检查设计、验收文档或源代码，查看是否有关于保护通信完整性的描述，如果有则查看是否依据校验码判断对方数据包的有效性；

b) 应测试关键应用系统，可通过获取通信双方的数据包，查看通信报文中是否含有校验码。

6.1.4.4.3 结果判定

如果6.1.4.4.2中a)和b)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

6.1.4.5 通信保密性

6.1.4.5.1 测评指标

见GB/T 22239—2008中6.1.4.5。

6.1.4.5.2 测评实施

本项要求包括：

a) 应检查设计、验收文档或源代码，查看是否有关于保护通信保密性的说明，如果有则查看在通信双方建立连接之前利用密码技术进行会话初始化验证的描述，以及对通信过程中的敏感信息字段进行加密的描述；

b) 应测试关键应用系统，通过查看通信双方数据包的内容，查看系统是否能在通信双方建立连接之前，利用密码技术进行会话初始化验证（如SSL建立加密通道前是否利用密码技术进行了会话初始化验证）；系统在通信过程中，对敏感信息字段是否进行加密。

6.1.4.5.3 结果判定

如果6.1.4.5.2中a)和b)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

6.1.4.6 软件容错

6.1.4.6.1 测评指标

见GB/T 22239—2008中6.1.4.6。

6.1.4.6.2 测评实施

本项要求包括：

a) 应检查设计或验收文档，查看是否有对人机接口输入或通信接口输入的数据进行有效性检验，在故障发生时继续提供一部分功能确保实施必要的措施的描述；

b) 应测试关键应用系统，查看应用系统是否能明确拒绝不符合格式要求数据；

c) 应测试关键应用系统，验证在故障发生时是否继续提供一部分功能，确保能够实施必要的措施。

6.1.4.6.3 结果判定

如果6.1.4.6.2中a)～c)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合

或部分符合本单元测评指标要求。

6.1.4.7 资源控制

6.1.4.7.1 测评指标

见 GB/T 22239—2008 中 6.1.4.7。

6.1.4.7.2 测评实施

本项要求包括：

a) **应检查关键应用系统的配置参数，查看是否提供对最大并发会话连接数进行限制；**

b) **应测试关键应用系统，查看能否对单个账户的多重并发会话进行限制；**

c) **应测试关键应用系统，当通信双方中的一方在一段时间内未作任何响应，查看另一方是否能够自动结束会话。**

6.1.4.7.3 结果判定

如果 6.1.4.7.2 中 a)～c)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

6.1.5 数据安全及备份恢复

6.1.5.1 数据完整性

6.1.5.1.1 测评指标

见 GB/T 22239—2008 中 6.1.5.1。

6.1.5.1.2 测评实施

本项要求包括：

a) **如果关键网络设备、关键主机操作系统和关键数据库管理系统能够进行远程管理，则应查看其能否检测鉴别信息在传输过程中完整性受到了破坏；**

b) 应检查应用系统的设计、验收文档或源代码，查看是否有关于能检测鉴别信息和重要业务数据传输过程中完整性受到破坏的描述。

6.1.5.1.3 结果判定

如果 6.1.5.1.2 中 a)和 b)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

6.1.5.2 数据保密性

6.1.5.2.1 测评指标

见 GB/T 22239—2008 中 6.1.5.2。

6.1.5.2.2 测评实施

应检查关键网络设备、关键主机操作系统、关键数据库管理系统和关键应用系统，查看其鉴别信息是否采用加密或其他有效措施实现了存储保密性。

6.1.5.2.3 结果判定

如果6.1.5.2.2为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

6.1.5.3 备份和恢复

6.1.5.3.1 测评指标

见GB/T 22239—2008中6.1.5.3。

6.1.5.3.2 测评实施

本项要求包括：

a) 应检查是否对关键网络设备、关键主机操作系统、关键数据库管理系统和关键应用系统的重要信息进行了备份，并定期进行恢复测试；

b) **应检查关键网络设备、通信线路和数据处理系统（如包含数据库管理系统在内的数据库服务器）是否提供硬件冗余。**

6.1.5.3.3 结果判定

如果6.1.5.3.2中a)和b)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

6.2 安全管理测评

6.2.1 安全管理制度

6.2.1.1 管理制度

6.2.1.1.1 测评指标

见GB/T 22239—2008中6.2.1.1。

6.2.1.1.2 测评实施

本项要求包括：

a) **应检查信息安全工作的总体方针和安全策略文件，查看文件是否明确机构安全工作的总体目标、范围、原则和安全框架等；**

b) 应检查各项安全管理制度，查看是否覆盖物理、网络、主机系统、数据、应用、建设和运维等层面的管理内容；

c) **应检查是否具有重要管理操作的操作规程（如系统维护手册和用户操作规程等）。**

6.2.1.1.3 结果判定

如果6.2.1.1.2中a)～c)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

6.2.1.2 制定和发布

6.2.1.2.1 测评指标

见GB/T 22239—2008中6.2.1.2。

6.2.1.2.2 测评实施

本项要求包括：

a) 应访谈安全主管，询问是否由专门的部门或人员负责制定安全管理制度；

b) 应访谈安全主管，询问安全管理制度是否能够发布到相关人员手中，是否对制定的安全管理制度进行论证和审定；

c) 应检查管理制度评审记录，查看是否有相关人员的评审意见。

6.2.1.2.3 结果判定

如果6.2.1.2.2中a)～c)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

6.2.1.3 评审和修订

6.2.1.3.1 测评指标

见GB/T 22239—2008中6.2.1.3。

6.2.1.3.2 测评实施

本项要求包括：

a) 应访谈安全主管，询问是否定期对安全管理制度进行评审，发现存在不足或需要改进的是否进行修订；

b) 应检查是否具有安全管理制度评审记录；如果对制度做过修订，检查是否有修订版本的安全管理制度。

6.2.1.3.3 结果判定

如果6.2.1.3.2中a)和b)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

6.2.2 安全管理机构

6.2.2.1 岗位设置

6.2.2.1.1 测评指标

见GB/T 22239—2008中6.2.2.1。

6.2.2.1.2 测评实施

本项要求包括：

a) 应访谈安全主管，询问信息系统是否设置了系统管理员、网络管理员和安全管理员等岗位，各个岗位的职责分工是否明确；是否设立安全管理各个方面的负责人；

b) 应检查岗位职责文档，查看文档是否明确设置安全主管、安全管理各个方面的负责人、系统管理员、网络管理员和安全管理员等各个岗位，各个岗位的职责范围是否清晰、明确。

6.2.2.1.3 结果判定

如果6.2.2.1.2中a)和b)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合

或部分符合本单元测评指标要求。

6.2.2.2 人员配备

6.2.2.2.1 测评指标

见 GB/T 22239—2008 中 6.2.2.2。

6.2.2.2.2 测评实施

本项要求包括：

a) 应访谈安全主管，询问各个安全管理岗位是否配备了一定数量的人员；

b) 应检查安全管理各岗位人员信息表，查看其是否明确系统管理员、网络管理员、安全管理员等重要岗位人员的信息，查看安全管理员是否没有兼任网络管理员、系统管理员、数据库管理员等岗位。

6.2.2.2.3 结果判定

如果 6.2.2.2.2 中 a)和 b)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

6.2.2.3 授权和审批

6.2.2.3.1 测评指标

见 GB/T 22239—2008 中 6.2.2.3。

6.2.2.3.2 测评实施

本项要求包括：

a) 应访谈安全主管，询问其是否对信息系统中的关键活动进行审批，审批活动是否得到授权；

b) 应检查审批管理制度文档，查看文档是否明确系统投入运行、网络系统接入和重要资源的访问等关键活动的审批部门、批准人和审批程序；

c) 应检查经审批的文档，查看审批程序与文件要求是否一致，是否有批准人的签字和审批部门的盖章。

6.2.2.3.3 结果判定

如果 6.2.2.3.2 中 a)～c)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

6.2.2.4 沟通和合作

6.2.2.4.1 测评指标

见 GB/T 22239—2008 中 6.2.2.4。

6.2.2.4.2 测评实施

本项要求包括：

a) 应访谈安全主管，询问是否与公安机关、电信公司和兄弟单位建立联系，信息安全职能部门内部之间、各类管理人员之间以及与组织机构内其他部门之间是否建立交流和沟通机制；

b) 应检查部门间和部门内部沟通和合作的相关文档，查看是否包括工作内容、参加人员等的描述；

c) 应检查外联单位说明文档，查看外联单位是否包含公安机关、电信公司及兄弟单位等，是否说明外联单位的联系人和联系方式等内容。

6.2.2.4.3 结果判定

如果6.2.2.4.2中a)～c)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

6.2.2.5 审核和检查

6.2.2.5.1 测评指标

见GB/T 22239—2008中6.2.2.5。

6.2.2.5.2 测评实施

本项要求包括：

a) 应访谈安全管理员，询问是否定期检查系统日常运行、系统漏洞和数据备份等情况；

b) 应检查安全管理员定期实施安全检查的记录，查看检查内容是否包括系统日常运行、系统漏洞和数据备份等情况。

6.2.2.5.3 结果判定

如果6.2.2.5.2中a)和b)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

6.2.3 人员安全管理

6.2.3.1 人员录用

6.2.3.1.1 测评指标

见GB/T 22239—2008中6.2.3.1。

6.2.3.1.2 测评实施

本项要求包括：

a) 应访谈人事负责人，询问是否由专门的部门或人员负责人员的录用工作；

b) 应访谈人事负责人，询问在人员录用时是否对被录用人的身份、背景和专业资格进行审查，对技术人员的技术技能进行考核；

c) 应访谈人事负责人，询问录用后是否与从事关键岗位的人员签署保密协议；

d) 应检查人员录用管理文档，查看是否说明录用人员应具备的条件(如学历、学位要求，技术人员应具备的专业技术水平，管理人员应具备的安全管理知识等)；

e) 应检查是否具有人员录用时对录用人身份、背景和专业资格等进行审查的相关文档或记录，查看是否记录审查内容和审查结果等；

f) 应检查人员录用时的技能考核文档或记录，查看是否记录考核内容和考核结果等；

g) 应检查保密协议，查看是否有保密范围、保密责任、违约责任、协议的有效期限和责任人签字等内容。

6.2.3.1.3 结果判定

如果6.2.3.1.2中a)～g)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

6.2.3.2 人员离岗

6.2.3.2.1 测评指标

见GB/T 22239—2008中6.2.3.2。

6.2.3.2.2 测评实施

本项要求包括：

a) 应访谈安全主管，询问是否及时终止离岗人员的所有访问权限，是否取回各种身份证件、钥匙、徽章以及机构提供的软硬件设备等；

b) **应访谈人事负责人，询问人员离岗是否遵循严格的调离手续；**

c) 应检查是否具有离岗人员交还身份证件、设备等的登记记录；

d) **应检查是否具有按照离岗程序办理调离手续的记录。**

6.2.3.2.3 结果判定

如果6.2.3.2.2中a)～d)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

6.2.3.3 人员考核

6.2.3.3.1 测评指标

见GB/T 22239—2008中6.2.3.3。

6.2.3.3.2 测评实施

本项要求包括：

a) **应访谈安全主管，询问是否定期对各个岗位人员进行安全技能及安全知识的考核；**

b) **应检查考核记录，查看考核人员是否包括各个岗位的人员，考核内容是否包含安全知识、安全技能等。**

6.2.3.3.3 结果判定

如果6.2.3.3.2中a)和b)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

6.2.3.4 安全意识教育和培训

6.2.3.4.1 测评指标

见GB/T 22239—2008中6.2.3.4。

6.2.3.4.2 测评实施

本项要求包括：

a) 应访谈安全主管，询问是否制定培训计划并按计划对各个岗位人员进行安全教育和培训；是否对违反安全策略和规定的人员进行惩戒；

b) 应检查安全教育和培训计划文档，查看计划是否明确了培训方式、培训对象、培训内容、培训时间和地点等，培训内容是否包含信息安全基础知识、岗位操作规程等；

c) 应检查安全教育和培训记录，查看记录是否有培训人员、培训内容、培训结果等的描述。

6.2.3.4.3 结果判定

如果6.2.3.4.2中a)～c)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

6.2.3.5 外部人员访问管理

6.2.3.5.1 测评指标

见GB/T 22239—2008中6.2.3.5。

6.2.3.5.2 测评实施

本项要求包括：

a) 应访谈安全主管，询问外部人员访问重要区域(如访问机房、重要服务器或设备区等)是否需经有关部门或负责人批准，是否由专人全程陪同或监督，是否进行记录并备案管理；

b) 应检查外部人员访问管理文档，查看是否具有规范外部人员访问机房等重要区域需经过相关部门或负责人批准的管理要求；

c) 应检查外部人员访问重要区域的登记记录，查看是否记录了外部人员访问重要区域的进入时间、离开时间、访问区域及陪同人等信息。

6.2.3.5.3 结果判定

如果6.2.3.5.2中a)～c)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

6.2.4 系统建设管理

6.2.4.1 系统定级

6.2.4.1.1 测评指标

见GB/T 22239—2008中6.2.4.1。

6.2.4.1.2 测评实施

本项要求包括：

a) 应访谈系统建设负责人，询问是否参照定级指南确定信息系统安全保护等级；

b) 应检查系统定级文档，查看文档是否明确信息系统的边界和信息系统的安全保护等级，是否说明定级的方法和理由，是否有相关部门或主管领导的盖章或签名。

6.2.4.1.3 结果判定

如果6.2.4.1.2中a)和b)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

6.2.4.2 安全方案设计

6.2.4.2.1 测评指标

见 GB/T 22239—2008 中 6.2.4.2。

6.2.4.2.2 测评实施

本项要求包括：

a) 应访谈系统建设负责人，询问是否依据风险分析的结果补充和调整过安全措施，具体做过哪些调整；

b) **应访谈系统建设负责人，询问安全设计方案是否经过论证和审定，是否经过审批；**

c) 应检查系统的安全设计方案，查看方案是否描述系统的安全保护等级，是否描述系统的安全保护策略，是否根据系统的安全级别选择了安全措施；

d) 应检查系统的安全设计方案，查看是否详细描述安全措施的实现内容，是否有安全产品的功能、性能和部署等描述，是否有安全建设的费用和计划等；

e) **应检查安全设计方案专家论证评审记录或文档，查看是否有相关部门和有关安全技术专家对安全设计方案的评审意见。**

6.2.4.2.3 结果判定

如果 6.2.4.2.2 中 a)～e)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

6.2.4.3 产品采购和使用

6.2.4.3.1 测评指标

见 GB/T 22239—2008 中 6.2.4.3。

6.2.4.3.2 测评实施

本项要求包括：

a) **应访谈系统建设负责人，询问是否有专门的部门负责产品的采购，由何部门负责；**

b) **应访谈系统建设负责人，询问系统是否采用了密码产品，密码产品的采购和使用是否符合国家密码主管部门的要求；**

c) 应访谈系统建设负责人，询问系统使用的有关信息安全产品是否符合国家的有关规定，如安全产品获得了销售许可证等；

d) **应抽样检查安全产品和密码产品的相关凭证，如销售许可等，查看是否使用了符合国家有关规定产品。**

6.2.4.3.3 结果判定

如果 6.2.4.3.2 中 a)～d)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

6.2.4.4 自行软件开发

6.2.4.4.1 测评指标

见 GB/T 22239—2008 中 6.2.4.4。

6.2.4.4.2 测评实施

本项要求包括：

a) 应访谈系统建设负责人，询问是否进行自主开发软件；

b) 应访谈系统建设负责人，询问自主开发软件是否在独立的环境中完成编码和调试，如相对独立的网络区域，询问软件设计相关文档是否由专人负责保管，负责人是何人；

c) **应检查是否有软件开发方面的管理制度，查看文件是否明确软件设计、开发、测试、验收过程的控制方法和人员行为准则，是否明确哪些开发活动应经过授权、审批等；**

d) **应检查是否具有软件使用指南或操作手册等；**

e) 应检查网络拓扑图和实际开发环境，查看是否实际运行环境和开发环境有效隔离。

6.2.4.4.3 结果判定

如果6.2.4.4.2中a)～e)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

6.2.4.5 外包软件开发

6.2.4.5.1 测评指标

见GB/T 22239—2008中6.2.4.5。

6.2.4.5.2 测评实施

本项要求包括：

a) 应访谈系统建设负责人，询问软件交付前是否依据开发要求的技术指标对软件功能和性能等进行验收测试，软件安装之前是否检测软件中的恶意代码；

b) **应访谈系统建设负责人，是否要求开发单位提供源代码，是否根据源代码对软件中可能存在的后门进行审查；**

c) 应检查是否具有软件开发的相关文档，如需求分析说明书、软件设计说明书等，是否具有软件操作手册或使用指南；

d) **应检查部分软件源代码，查看是否具有源代码。**

6.2.4.5.3 结果判定

如果6.2.4.5.2中a)～d)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

6.2.4.6 工程实施

6.2.4.6.1 测评指标

见GB/T 22239—2008中6.2.4.6。

6.2.4.6.2 测评实施

本项要求包括：

a) 应访谈系统建设负责人，询问是否指定专门部门或人员对工程实施过程进行进度和质量控制，由何部门/何人负责；

b) **应检查工程实施方案，查看其是否包括工程时间限制、进度控制和质量控制等方面内容。**

6.2.4.6.3 结果判定

如果6.2.4.6.2中a)和b)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

6.2.4.7 测试验收

6.2.4.7.1 测评指标

见GB/T 22239—2008中6.2.4.7。

6.2.4.7.2 测评实施

本项要求包括：

a) 应访谈系统建设负责人，询问在信息系统建设完成后是否对其进行安全性测试验收；

b) 应检查是否具有工程测试验收方案，查看其是否明确说明参与测试的部门、人员、测试验收内容、现场操作过程等内容；

c) 应检查是否具有系统测试验收报告，**是否有相关部门和人员对系统测试验收报告进行审定的意见。**

6.2.4.7.3 结果判定

如果6.2.4.7.2中a)～c)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

6.2.4.8 系统交付

6.2.4.8.1 测评指标

见GB/T 22239—2008中6.2.4.8。

6.2.4.8.2 测评实施

本项要求包括：

a) 应访谈系统建设负责人，询问系统交接工作是否根据交付清单对所交接的设备、文档、软件等进行清点；

b) 应访谈系统建设负责人，询问系统正式运行前是否对运行维护人员进行过培训，针对哪些方面进行过培训；

c) 应检查是否具有系统交付清单，查看交付清单是否说明系统交付的各类设备、软件、文档等；

d) 应检查系统交付提交的文档，查看是否有指导用户进行系统运维的文档等；

e) **应检查是否有系统交付技术培训记录，查看是否包括培训内容、培训时间和参与人员等。**

6.2.4.8.3 结果判定

如果6.2.4.8.2中a)～e)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

6.2.4.9 安全服务商选择

6.2.4.9.1 测评指标

见GB/T 22239—2008中6.2.4.9。

6.2.4.9.2 测评实施

本项要求包括：

a) 应访谈系统建设负责人，询问信息系统选择的安全服务商有哪些，是否符合国家有关规定；

b) 应检查是否具有与安全服务商签订的安全责任合同书或保密协议等文档，查看其内容是否包含保密范围、安全责任、违约责任、协议的有效期限和责任人的签字等；

c) **应检查是否具有与安全服务商签订的服务合同或安全责任合同书，查看是否明确了后期的技术支持和服务承诺等内容。**

6.2.4.9.3 结果判定

如果6.2.4.9.2中a)～c)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

6.2.5 系统运维管理

6.2.5.1 环境管理

6.2.5.1.1 测评指标

见GB/T 22239—2008中6.2.5.1。

6.2.5.1.2 测评实施

本项要求包括：

a) 应访谈系统运维负责人，询问是否有专门的部门或人员对机房供配电、空调、温湿度控制等设施进行定期维护，由何部门/何人负责，维护周期多长；

b) 应访谈系统运维负责人，询问是否有专门的部门或人员对机房的出入、服务器开机/关机等日常工作进行管理，由何部门/何人负责；

c) **应访谈系统运维负责人，询问为保证办公环境的保密性采取了哪些控制措施，在哪个区域接待来访人员，工作人员调离时是否收回办公室钥匙等；**

d) 应检查是否有机房安全管理制度，查看其内容是否覆盖机房物理访问、物品带进/带出机房和机房环境安全等方面；

e) **应检查是否具有空调、温湿度控制等机房设施的维护保养记录，表明定期对这些设施进行了维护保养。**

6.2.5.1.3 结果判定

如果6.2.5.1.2中a)～e)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

6.2.5.2 资产管理

6.2.5.2.1 测评指标

见GB/T 22239—2008中6.2.5.2。

6.2.5.2.2 测评实施

本项要求包括：

a) **应访谈系统运维负责人，询问是否有资产管理的责任人员或部门，由何部门/何人负责；**
b) 应检查是否有资产清单，查看其内容是否覆盖资产责任部门、责任人、所处位置和重要程度等方面；
c) **应检查是否有资产安全管理方面的制度，查看是否明确信息资产管理的责任部门、责任人，查看其内容是否覆盖资产使用、借用、维护等方面。**

6.2.5.2.3 结果判定

如果6.2.5.2.2中a)～c)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

6.2.5.3 介质管理

6.2.5.3.1 测评指标

见GB/T 22239—2008中6.2.5.3。

6.2.5.3.2 测评实施

本项要求包括：

a) 应访谈资产管理员，询问介质的存放环境是否采取保护措施防止介质被盗、被毁等；
b) 应访谈资产管理员，询问是否根据介质的目录清单对介质的使用现状进行定期检查；
c) **应访谈资产管理员，询问是否将介质保管在一个特定环境里，有专人负责，并根据重要性对介质进行分类和标识；**
d) **应访谈资产管理员，询问对送出维修或销毁的介质在送出之前是否对介质内存储数据进行净化处理；**
e) 应检查介质使用管理记录，查看其是否记录介质归档和使用等情况；
f) **应检查介质存储环境，查看是否对其进行了分类，并具有不同标识。**

6.2.5.3.3 结果判定

如果6.2.5.3.2中a)～f)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

6.2.5.4 设备管理

6.2.5.4.1 测评指标

见GB/T 22239—2008中6.2.5.4。

6.2.5.4.2 测评实施

本项要求包括：

a) 应访谈系统运维负责人，询问是否有专门的部门或人员对各种设备、线路进行定期维护，由何部门/何人负责，维护周期多长；
b) 应检查是否有设备安全管理制度，查看其内容是否对各种软硬件设备的选型、采购、发放和领用等环节进行规定；
c) **应检查设备安全管理制度中是否有对终端计算机、便携机和网络设备等使用方式、操作原则、注意事项等方面的规定，是否有信息处理设备必须经过审批才能带离机房或办公地点的要求。**

6.2.5.4.3 结果判定

如果6.2.5.4.2中a)～c)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

6.2.5.5 网络安全管理

6.2.5.5.1 测评指标

见GB/T 22239—2008中6.2.5.5。

6.2.5.5.2 测评实施

本项要求包括：

a) 应访谈系统运维负责人，询问是否指定专门的部门或人员负责网络管理，维护网络运行日志、监控记录，分析处理报警信息等；

b) 应访谈网络管理员，询问是否定期对网络进行漏洞扫描，扫描周期多长，发现漏洞是否及时修补；

c) **应访谈网络管理员，询问是否根据厂家提供的软件升级版本对网络设备进行过升级，目前的版本号为多少，升级前是否对重要文件进行备份，采取什么方式备份；**

d) **应访谈网络管理员，网络的外联种类有哪些，是否都得到授权与批准，由何部门或何人批准，申请和批准的过程；**

e) **应检查是否有网络安全管理制度，查看其是否覆盖网络安全配置、安全策略、升级与打补丁、授权访问、日志保存时间、口令更新周期等方面内容；**

f) 应检查是否有网络漏洞扫描报告，检查扫描时间间隔与扫描周期是否一致；

g) **应检查是否具有网络设备配置文件的备份文件；**

h) **应检查是否具有内部网络外联的授权批准书。**

6.2.5.5.3 结果判定

如果6.2.5.5.2中a)～h)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

6.2.5.6 系统安全管理

6.2.5.6.1 测评指标

见GB/T 22239—2008中6.2.5.6。

6.2.5.6.2 测评实施

本项要求包括：

a) 应访谈系统运维负责人，询问是否指定专门的部门或人员负责系统管理，如根据业务需求和系统安全分析制定系统的访问控制策略，控制分配文件及服务的访问权限；

b) **应访谈系统管理员，询问系统日常管理的主要内容，是否有操作规程指导日常管理工作，包括重要的日常操作、参数的设置和修改等；**

c) 应访谈系统管理员，询问是否定期对系统进行漏洞扫描，扫描周期多长，发现漏洞是否及时修补，在安装系统补丁前是否对重要文件进行备份，**是否先在测试环境中测试通过再安装；**

d) **应检查是否有系统安全管理制度，查看其内容是否覆盖系统安全策略、安全配置、日志管理和**

日常操作流程等方面；

e) 应检查是否有系统漏洞扫描报告，检查扫描时间间隔与扫描周期是否一致；

f) 应检查是否有详细日常运行维护操作日志。

6.2.5.6.3 结果判定

如果6.2.5.6.2中a)～f)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

6.2.5.7 恶意代码防范管理

6.2.5.7.1 测评指标

见GB/T 22239—2008中6.2.5.7。

6.2.5.7.2 测评实施

本项要求包括：

a) 应访谈系统运维负责人，询问是否对员工进行基本恶意代码防范意识的教育，是否告知应及时升级软件版本，使用外来设备、网络上接收文件和外来计算机或存储设备接入网络系统之前进行病毒检查等；

b) 应访谈系统运维负责人，询问是否指定专人对恶意代码进行检测，发现病毒后是否及时处理；

c) 应检查是否有恶意代码防范方面的管理制度，查看其内容是否覆盖防恶意代码软件的授权使用、恶意代码库升级、定期汇报等方面。

6.2.5.7.3 结果判定

如果6.2.5.7.2中a)～c)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

6.2.5.8 密码管理

6.2.5.8.1 测评指标

见GB/T 22239—2008中6.2.5.8。

6.2.5.8.2 测评实施

应访谈系统运维负责人，询问系统中是否使用密码技术和产品，密码技术和产品的使用是否遵照国家密码管理规定。

6.2.5.8.3 结果判定

如果6.2.5.8.2为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

6.2.5.9 变更管理

6.2.5.9.1 测评指标

见GB/T 22239—2008中6.2.5.9。

6.2.5.9.2 测评实施

本项要求包括：

a) 应访谈系统运维负责人，询问是否针对系统的重大变更制定变更方案指导系统变更工作的开展；

b) 应访谈系统运维负责人，询问重要系统变更前是否得到有关领导的批准，由何人批准，对发生的变更情况是否通知了所有相关人员，以何种方式通知；

c) 应检查系统变更方案，查看其是否覆盖变更类型、变更原因、变更过程、变更前评估等方面内容；

d) 应检查重要系统的变更申请书，查看其是否有主管领导的批准签字。

6.2.5.9.3 结果判定

如果6.2.5.9.2中a)～d)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

6.2.5.10 备份与恢复管理

6.2.5.10.1 测评指标

见GB/T 22239—2008中6.2.5.10。

6.2.5.10.2 测评实施

本项要求包括：

a) 应访谈系统运维负责人，询问是否识别出需要定期备份的业务信息、系统数据和软件系统，主要有哪些；

b) 应检查备份管理文档，查看其是否明确了备份方式、备份频度、存储介质和保存期等方面内容；

c) 应检查数据备份和恢复策略文档，查看其内容是否覆盖备份数据的存放场所、文件命名规则、介质替换频率、数据离站传输方法等方面。

6.2.5.10.3 结果判定

如果6.2.5.10.2中a)～c)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

6.2.5.11 安全事件处置

6.2.5.11.1 测评指标

见GB/T 22239—2008中6.2.5.11。

6.2.5.11.2 测评实施

本项要求包括：

a) 应访谈系统运维负责人，询问是否告知用户在发现安全弱点和可疑事件时应及时报告；

b) 应检查是否有安全事件报告和处置管理制度，查看其是否明确安全事件的级别，明确不同级别安全事件的报告和处置方式等内容；

c) 应检查安全事件处理记录，查看其是否记录引发安全事件的原因，是否记录事件处理过程，是否与管理规定的处理要求一致等。

6.2.5.11.3 结果判定

如果6.2.5.11.2中a)～c)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

6.2.5.12 应急预案管理

6.2.5.12.1 测评指标

见GB/T 22239—2008中6.2.5.12。

6.2.5.12.2 测评实施

本项要求包括：

a) **应访谈系统运维负责人，询问是否制定不同事件的应急预案，是否对系统相关人员进行应急预案培训，多长时间举办一次；**

b) **应检查应急预案框架，查看其内容是否覆盖启动应急预案的条件、应急处理流程、系统恢复流程、事后教育和培训等方面；**

c) **应检查是否具有根据应急预案框架制定的不同事件的应急预案。**

6.2.5.12.3 结果判定

如果6.2.5.12.2中a)～d)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

7 第三级信息系统单元测评

7.1 安全技术测评

7.1.1 物理安全

7.1.1.1 物理位置的选择

7.1.1.1.1 测评指标

见GB/T 22239—2008中7.1.1.1。

7.1.1.1.2 测评实施

本项要求包括：

a) 应访谈物理安全负责人，询问机房和办公场地所在建筑物是否具有防震、防风和防雨等能力；

b) 应检查是否有机房和办公场地所在建筑物抗震设防审批文档；

c) 应检查机房和办公场地所在建筑物是否具有防风和防雨等能力；

d) **应检查机房场地是否不在用水区域的垂直下方；**

e) **如果机房场地位于建筑物的高层或地下室或用水设备的隔壁，应检查机房是否采取了防水和防潮措施。**

7.1.1.1.3 结果判定

如果7.1.1.1.2中a)～e)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

7.1.1.2 物理访问控制

7.1.1.2.1 测评指标

见 GB/T 22239—2008 中 7.1.1.2。

7.1.1.2.2 测评实施

本项要求包括：

a) 应检查机房出入口是否有专人值守负责控制并鉴别进入机房的人员，是否有值守记录；

b) 应检查机房是否不存在专人值守之外的其他开放出入口；

c) 应检查是否有来访人员进入机房的登记记录；

d) 应检查是否有来访人员进入机房的申请、审批记录，查看申请、审批记录是否包括来访人员的访问范围；

e) **应检查来访人员进入机房时是否对其行为进行限制和监控；**

f) **应检查机房是否合理划分区域，是否在机房重要区域前设置交付或安装等过渡区域；是否在不同机房间和同一机房不同区域间设置了有效的物理隔离装置；**

g) **应检查重要区域是否配置了电子门禁系统，查看电子门禁系统是否有验收文档或产品安全认证资质；**

h) **应检查部署在机房重要区域的电子门禁系统是否正常工作（不考虑断电后的工作情况）；检查电子门禁系统记录，查看是否能够鉴别和记录进入人员的身份；检查是否有电子门禁系统运行、定期检查和维护记录。**

7.1.1.2.3 结果判定

如果 7.1.1.2.2 中 a)～h)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

7.1.1.3 防盗窃和防破坏

7.1.1.3.1 测评指标

见 GB/T 22239—2008 中 7.1.1.3。

7.1.1.3.2 测评实施

本项要求包括：

a) 应检查**主要设备**等是否放置在机房内；

b) 应检查**主要设备**等或设备的主要部件是否固定；

c) 应检查**主要设备**等或设备的主要部件上是否设置明显的不易除去的标记；

d) 应检查通信线缆铺设是否暗敷或在不易被发现的地方；

e) 应检查**机房**是否安装防盗报警设施，防盗报警设施是否正常运行，并查看是否有防盗报警设施的运行记录、**定期检查和维护记录**；

f) 应检查介质是否有分类标识，是否分类存放在介质库或档案室内；

g) **应检查机房是否安装摄像、传感等监控报警系统，监控报警系统是否正常运行，并查看是否有监控报警系统的监控记录、定期检查和维护记录；**

h) **应检查是否有机房防盗报警设施和监控报警设施的安全资质材料、安装测试和验收报告。**

7.1.1.3.3 结果判定

如果 7.1.1.3.2 中 a)～h)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

7.1.1.4 防雷击

7.1.1.4.1 测评指标

见 GB/T 22239—2008 中 7.1.1.4。

7.1.1.4.2 测评实施

本项要求包括：

a) 应访谈物理安全负责人，询问机房所在建筑物是否设置了避雷装置，是否通过验收或国家有关部门的技术检测；

b) 应访谈物理安全负责人，询问机房是否设置有交流电源地线；

c) 应检查机房所在建筑物的防雷验收文档中是否有设置避雷装置的说明；

d) 应检查机房防雷验收文档中是否有设置交流电源地线的说明；

e) **应检查机房是否安装防止感应雷的防雷装置，防雷装置是否通过了具有防雷检测资质的检测部门的测试。**

7.1.1.4.3 结果判定

如果 7.1.1.4.2 中 a)～e)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

7.1.1.5 防火

7.1.1.5.1 测评指标

见 GB/T 22239—2008 中 7.1.1.5。

7.1.1.5.2 测评实施

本项要求包括：

a) 应检查机房是否设置了**自动检测火情、自动报警、自动灭火的自动消防系统，自动消防系统是否是经消防检测部门检测合格的产品**，其有效期是否合格；应检查**自动消防系统**是否处于正常运行状态，查看是否有运行记录、定期检查和维护记录；

b) **应检查机房设计或验收文档，查看是否说明机房及相关的工作房间和辅助房采用具有耐火等级的建筑材料；**

c) **应检查机房重要区域与其他区域之间是否采取隔离防火措施。**

7.1.1.5.3 结果判定

如果 7.1.1.5.2 中 a)～c)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

7.1.1.6 防水和防潮

7.1.1.6.1 测评指标

见 GB/T 22239—2008 中 7.1.1.6。

7.1.1.6.2 测评实施

本项要求包括：

a) 应检查机房屋顶或活动地板下是否未安装水管；

b) 应检查穿过机房墙壁或楼板的给水排水管道是否采取防渗漏和防结露等防水保护措施；

c) 应检查机房的窗户、屋顶和墙壁等是否未出现过漏水、渗透和返潮现象，机房的窗户、屋顶和墙壁是否进行过防水防渗处理；

d) 如果机房内安装有空调机和加湿器，应检查是否设置了挡水和排水设施；

e) 如果机房位于湿度较高的地区，应检查机房是否有除湿装置并能够正常运行，是否有防水防潮处理记录**和除湿装置运行记录、定期检查和维护记录**；

f) **应检查是否设置对水敏感的检测仪表或元件，对机房进行防水检测和报警，查看该仪表或元件是否正常运行，是否有运行记录、定期检查和维护记录。**

7.1.1.6.3 结果判定

如果 7.1.1.6.2 中 a)～f)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

7.1.1.7 防静电

7.1.1.7.1 测评指标

见 GB/T 22239—2008 中 7.1.1.7。

7.1.1.7.2 测评实施

本项要求包括：

a) 应检查**主要设备**是否有安全接地构造或其他静电泄放措施；

b) **应检查机房是否采用了防静电地板或敷设防静电地面。**

7.1.1.7.3 结果判定

如果 7.1.1.7.2 中 a)和 b)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

7.1.1.8 温湿度控制

7.1.1.8.1 测评指标

见 GB/T 22239—2008 中 7.1.1.8。

7.1.1.8.2 测评实施

本项要求包括：

a) 应检查机房内是否配备了温湿度自动调节设施，温湿度自动调节设施是否能够正常运行，机房

温度、相对湿度是否满足电子信息设备的使用要求；

b) 应检查是否有机房的温湿度记录，是否有温湿度自动调节设施的运行记录、**定期检查和维护记录**。

7.1.1.8.3 结果判定

如果 7.1.1.8.2 中 a)和 b)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

7.1.1.9 电力供应

7.1.1.9.1 测评指标

见 GB/T 22239—2008 中 7.1.1.9。

7.1.1.9.2 测评实施

本项要求包括：

a) **应访谈物理安全负责人，询问是否采用冗余或并行的电力电缆线路为计算机系统供电**；

b) 应检查机房的计算机系统供电线路上是否设置了稳压器和过电压防护设备，这些设备是否正常运行，**查看供电电压是否正常**；

c) 应检查机房计算机系统是否配备了短期备用电源设备，短期备用电源设备是否正常运行；

d) **应检查是否为机房计算机系统建立了备用供电系统，备用供电系统的基本容量是否能够满足主要设备的正常运行**；

e) 应检查是否有稳压器、过电压防护设备、短期备用电源设备以及**备用供电系统**等设备的检查和维护记录，**备用供电系统运行记录、定期检查和维护记录**。

7.1.1.9.3 结果判定

如果 7.1.1.9.2 中 a)～e)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

7.1.1.10 电磁防护

7.1.1.10.1 测评指标

见 GB/T 22239—2008 中 7.1.1.10。

7.1.1.10.2 测评实施

本项要求包括：

a) **应检查机房设备外壳是否有安全接地**；

b) 应检查机房布线，查看是否做到电源线和通信线缆隔离；

c) **应检查磁介质和处理秘密级信息的设备是否存放在具有电磁屏蔽功能的容器中**。

7.1.1.10.3 结果判定

如果 7.1.1.10.2 中 a)～c)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

7.1.2 网络安全

7.1.2.1 结构安全

7.1.2.1.1 测评指标

见 GB/T 22239—2008 中 7.1.2.1。

7.1.2.1.2 测评实施

本项要求包括：

a) 应检查网络设计或验收文档，查看是否有满足主要网络设备业务处理能力需要的设计或描述；

b) 应检查网络设计或验收文档，查看是否有满足接入网络及核心网络的带宽业务高峰期的需要以及不存在带宽瓶颈等方面的设计或描述；

c) 应检查边界和主要网络设备的路由控制策略，查看是否建立安全的访问路径；

d) 应检查网络拓扑结构图，查看其与当前运行的实际网络系统是否一致；

e) 应检查网络设计或验收文档，查看是否有根据各部门的工作职能、重要性和所涉及信息的重要程度等因素，划分不同的子网或网段，并按照方便管理和控制的原则为各子网和网段分配地址段的设计或描述；

f) 应检查边界和主要网络设备，查看重要网段是否采取了技术隔离手段与其他网段隔离；

g) 应检查边界和主要网络设备，查看是否配置对带宽进行控制的策略，这些策略是否能够保证在网络发生拥堵的时候优先保护重要业务。

7.1.2.1.3 结果判定

如果 7.1.2.1.2 中 a)～g)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

7.1.2.2 访问控制

7.1.2.2.1 测评指标

见 GB/T 22239—2008 中 7.1.2.2。

7.1.2.2.2 测评实施

本项要求包括：

a) 应检查边界网络设备的访问控制策略，查看其是否根据会话状态信息对数据流进行控制，控制粒度是否为端口级；

b) 应检查边界网络设备的访问控制策略，查看其是否对进出网络的信息内容进行过滤，实现对应用层 HTTP、FTP、TELNET、SMTP、POP3 等协议命令级的控制；

c) 应检查边界网络设备，查看是否有会话处于非活跃的时间或会话结束后自动终止网络连接的配置，查看是否设置网络最大流量数及网络连接数；

d) 应检查边界和主要网络设备地址绑定配置，查看重要网段是否采取了地址绑定的措施；

e) 应测试边界网络设备，可通过试图访问未授权的资源，验证访问控制措施对未授权的访问行为的控制是否有效，控制粒度是否为单个用户；

f) 应检查边界网络设备的拨号用户列表，查看其是否对具有拨号访问权限的用户数量进行限制；

g) 应对网络访问控制措施进行渗透测试，可通过采用多种渗透测试技术，验证网络访问控制措施

不存在明显弱点。

7.1.2.2.3 结果判定

如果7.1.2.2.2中a)～g)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

7.1.2.3 安全审计

7.1.2.3.1 测评指标

见GB/T 22239—2008中7.1.2.3。

7.1.2.3.2 测评实施

本项要求包括：

a) 应检查边界和主要网络设备的安全审计策略，查看是否包含网络系统中的网络设备运行状况、网络流量、用户行为等；

b) 应检查边界和主要网络设备的安全审计记录，查看是否包括：事件的日期和时间、用户、事件类型、事件成功情况，及其他与审计相关的信息；

c) 应检查边界和主要网络设备，查看是否为授权用户浏览和分析审计数据提供专门的审计工具，并能根据需要生成审计报表；

d) 应测试边界和主要网络设备，可通过以某个非审计用户登录系统，试图删除、修改或覆盖审计记录，验证安全审计的保护情况与要求是否一致。

7.1.2.3.3 结果判定

如果7.1.2.3.2中a)～d)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

7.1.2.4 边界完整性检查

7.1.2.4.1 测评指标

见GB/T 22239—2008中7.1.2.4。

7.1.2.4.2 测评实施

本项要求包括：

a) 应检查边界完整性检查设备的非法外联和非授权接入策略，查看是否设置了对非法连接到内网和非法连接到外网的行为进行监控并有效的阻断的配置；

b) 应测试边界完整性检查设备，测试是否能够确定出非法外联设备的位置，并对其进行有效阻断；

c) 应测试边界完整性检查设备，测试是否能够对非授权设备私自接入内部网络的行为进行检查，并准确定出位置，对其进行有效阻断。

7.1.2.4.3 结果判定

如果7.1.2.4.2中a)～c)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

7.1.2.5 入侵防范

7.1.2.5.1 测评指标

见 GB/T 22239—2008 中 7.1.2.5。

7.1.2.5.2 测评实施

本项要求包括：

a) 应检查网络入侵防范设备，查看是否能检测以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP 碎片攻击、网络蠕虫攻击等；

b) **应检查网络入侵防范设备的入侵时间记录，查看记录中是否包括入侵的源 IP、攻击的类型、攻击的目的、攻击的时间等；**

c) 应检查网络入侵防范设备的规则库版本，查看其规则库是否及时更新；

d) 应测试网络入侵防范设备，验证其检测策略是否有效；

e) **应测试网络入侵防范设备，验证其报警策略是否有效。**

7.1.2.5.3 结果判定

如果 7.1.2.5.2 中 a)～e)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

7.1.2.6 恶意代码防范

7.1.2.6.1 测评指标

见 GB/T 22239—2008 中 7.1.2.6。

7.1.2.6.2 测评实施

本项要求包括：

a) **应检查在网络边界及核心业务网段处是否有相应的防恶意代码措施；**

b) **应检查防恶意代码产品，查看其运行是否正常，恶意代码库是否及时更新。**

7.1.2.6.3 结果判定

如果 7.1.2.6.2 中 a)和 b)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

7.1.2.7 网络设备防护

7.1.2.7.1 测评指标

见 GB/T 22239—2008 中 7.1.2.7。

7.1.2.7.2 测评实施

本项要求包括：

a) 应检查边界和**主要**网络设备的设备防护策略，查看是否配置了对登录用户进行身份鉴别的功能；

b) 应检查边界和**主要**网络设备的设备防护策略，查看是否对网络设备的登录地址进行了限制；

c) 应检查边界和主要网络设备的账户列表，查看用户标识是否唯一；
d) **应检查边界和主要网络设备，查看是否对同一用户选择两种或两种以上组合的鉴别技术来进行身份鉴别；**
e) 应检查边界和主要网络设备的设备防护策略，查看口令设置是否有复杂度和定期修改要求；
f) 应检查边界和主要网络设备的设备防护策略，查看是否配置了鉴别失败处理功能，包括结束会话、限制非法登录次数、登录连接超时自动退出等；
g) 应检查边界和主要网络设备的设备防护策略，查看是否配置了对设备远程管理所产生的鉴别信息进行保护的功能；
h) **应检查边界和主要网络设备的管理设置，查看是否实现设备特权用户的权限分离；**
i) **应对边界和主要网络设备进行渗透测试，通过使用各种渗透测试技术对网络设备进行渗透测试，验证网络设备防护能力是否符合要求。**

7.1.2.7.3 结果判定

如果7.1.2.7.2中a)～i)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

7.1.3 主机安全

7.1.3.1 身份鉴别

7.1.3.1.1 测评指标

见GB/T 22239—2008中7.1.3.1。

7.1.3.1.2 测评实施

本项要求包括：

a) 应检查主要服务器操作系统和主要数据库管理系统的身份鉴别策略，查看是否提供了身份鉴别措施；
b) 应检查主要服务器操作系统和主要数据库管理系统的身份鉴别策略，查看其身份鉴别信息是否具有不易被冒用的特点，如对用户登录口令的最小长度、复杂度和更换周期进行要求和限制；
c) 应检查主要服务器操作系统和主要数据库管理系统的身份鉴别策略，查看是否配置了登录失败处理功能、设置了非法登录次数的限制值；查看是否设置网络登录连接超时，并自动退出；
d) 如果操作系统或数据库采用远程管理方式，查看是否具有防止鉴别信息在网络传输过程中被窃听的措施；
e) 应检查主要服务器操作系统和主要数据库管理系统账户列表，查看管理员用户名或UID分配是否唯一；
f) **应检查主要服务器操作系统和主要数据库管理系统的身份鉴别策略，查看是否采用两种或两种以上身份鉴别技术的组合来进行身份鉴别；**
g) **应渗透测试主要服务器操作系统，可通过使用口令破解工具等，对服务器操作系统进行用户口令强度检测，查看是否能够破解用户口令，破解口令后是否能够登录进入系统；**
h) **应渗透测试主要服务器操作系统，测试是否存在绕过认证方式进行系统登录的方法。**

7.1.3.1.3 结果判定

如果7.1.3.1.2中a)～f)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合

或部分符合本单元测评指标要求。

7.1.3.2 访问控制

7.1.3.2.1 测评指标

见 GB/T 22239—2008 中 7.1.3.2。

7.1.3.2.2 测评实施

本项要求包括：

a) 应检查主要服务器操作系统的安全策略，查看是否对重要文件的访问权限进行了限制，对系统不需要的服务、共享路径等进行了禁用或删除；

b) **应检查主要服务器操作系统和主要数据库管理系统的访问控制策略，查看特权用户的权限是否进行分离，如可分为系统管理员、安全管理员、安全审计员等；查看是否采用最小授权原则；**

c) 应检查操作系统的特权用户和数据库管理系统的特权用户，查看不同管理员的系统账户权限是否不同，且不应由同一人担任；

d) 应检查主要服务器操作系统和主要数据库管理系统的访问控制策略，查看是否已禁用或者限制匿名/默认账户的访问权限，是否重命名系统默认账户、修改这些账户的默认口令；

e) 应检查主要服务器操作系统和主要数据库管理系统的访问控制策略，是否删除了系统中多余的、过期的以及共享的账户；

f) 应检查主要服务器操作系统和主要数据库管理系统的权限设置情况，查看是否依据安全策略对用户权限进行了限制；

g) **应检查主要服务器操作系统和主要数据库管理系统的访问控制策略，查看是否对重要信息资源设置敏感标记；是否依据安全策略严格控制用户对有敏感标记重要信息资源的操作。**

7.1.3.2.3 结果判定

如果 7.1.3.2.2 中 a)～g)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

7.1.3.3 安全审计

7.1.3.3.1 测评指标

见 GB/T 22239—2008 中 7.1.3.3。

7.1.3.3.2 测评实施

本项要求包括：

a) 应检查主要服务器操作系统、重要终端操作系统和主要数据库管理系统的安全审计策略，查看安全审计配置是否包括系统内重要用户行为、系统资源的异常和重要系统命令的使用等重要的安全相关事件；

b) 应检查主要服务器操作系统、重要终端操作系统和主要数据库管理系统的安全审计策略，查看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、事件的结果等内容；

c) 应检查主要服务器操作系统、重要终端操作系统和主要数据库管理系统的安全审计策略，查看是否通过日志覆盖周期、存储方式、日志文件/空间大小、日志文件操作权限等设置，实现了对审计记录的保护，使其避免受到未预期的删除、修改或覆盖等；

d) 应检查主要服务器操作系统、重要终端操作系统和主要数据库管理系统的安全审计策略，查看是否为授权用户提供浏览和分析审计记录的功能，是否可以根据需要自动生成不同格式的审计报表；

e) 应测试主要服务器操作系统、重要终端操作系统和主要数据库管理系统，可通过非审计员的其他账户试图中断审计进程，验证审计进程是否受到保护。

7.1.3.3.3 结果判定

如果7.1.3.3.2中a)～e)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

7.1.3.4 剩余信息保护

7.1.3.4.1 测评指标

见GB/T 22239—2008中7.1.3.4。

7.1.3.4.2 测评实施

应检查主要操作系统和主要数据库管理系统技术开发手册或产品检测报告，查看是否明确用户的鉴别信息存储空间被释放或再分配给其他用户前的处理方法和过程；是否明确文件、目录和数据库记录等资源所在的存储空间被释放或重新分配给其他用户前的处理方法和过程。

7.1.3.4.3 结果判定

如果7.1.3.4.2为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

7.1.3.5 入侵防范

7.1.3.5.1 测评指标

见GB/T 22239—2008中7.1.3.5。

7.1.3.5.2 测评实施

本项要求包括：

a) 应检查入侵防范系统的入侵防范策略，查看是否能够记录对主要服务器攻击的源IP、攻击类型、攻击目标、攻击时间等，在发生严重入侵事件时是否提供报警（如声音、短信和EMAIL等）；

b) 应检查主要服务器是否提供对重要程序的完整性进行检测，并在检测到完整性受到破坏后具有恢复的措施的功能；

c) 应检查主要服务器操作系统中所安装的系统组件和应用程序是否都是必须的；

d) 应检查是否设置了专门的升级服务器实现对主要服务器操作系统补丁的升级，主要服务器操作系统是否具有操作系统补丁更新策略；

e) 应检查主要服务器操作系统和主要数据库管理系统的补丁是否得到了及时更新；

f) 应渗透测试主要服务器操作系统和主要数据库管理系统，查看入侵防范系统是否及时正确记录了本次攻击行为，并自动报警。

7.1.3.5.3 结果判定

如果7.1.3.5.2中a)～e)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合

或部分符合本单元测评指标要求。

7.1.3.6 恶意代码防范

7.1.3.6.1 测评指标

见 GB/T 22239—2008 中 7.1.3.6。

7.1.3.6.2 测评实施

本项要求包括：

a) 应检查主要服务器的恶意代码防范策略，查看是否安装了实时检测与查杀恶意代码的软件产品，并且及时更新了软件版本和恶意代码库；

b) **应检查主机防恶意代码软件或硬件，查看其厂家名称、产品版本号和恶意代码库名称等，查看其是否与网络防恶意代码软件有不同的恶意代码库；**

c) 应检查主机防恶意代码软件是否实现了统一管理。

7.1.3.6.3 结果判定

如果 7.1.3.6.2 中 a)～c)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

7.1.3.7 资源控制

7.1.3.7.1 测评指标

见 GB/T 22239—2008 中 7.1.3.7。

7.1.3.7.2 测评实施

本项要求包括：

a) 应检查主要服务器操作系统和主要数据库管理系统的资源控制策略，查看是否设定了终端接入方式、网络地址范围等条件限制终端登录；

b) 应检查访问主要服务器的终端是否都设置了操作超时锁定的配置；

c) **应检查主要服务器操作系统的资源控制策略，查看是否对 CPU、硬盘、内存和网络等资源的使用情况进行监控；**

d) 应检查主要服务器操作系统和主要数据库管理系统的资源控制策略，查看是否设置了单个用户或应用对系统资源的最大或最小使用限度；

e) **应检查主要服务器操作系统和主要数据库管理系统的资源控制策略，查看是否在服务水平降低到预先规定的阈值时，能检测和报警。**

7.1.3.7.3 结果判定

如果 7.1.3.7.2 中 a)～e)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

7.1.4 应用安全

7.1.4.1 身份鉴别

7.1.4.1.1 测评指标

见 GB/T 22239—2008 中 7.1.4.1。

7.1.4.1.2 测评实施

本项要求包括：

a) 应检查主要应用系统，查看是否提供身份标识和鉴别功能；

b) **应检查主要应用系统，查看是否采用了两种或两种以上组合的身份鉴别技术来进行身份鉴别；**

c) 应检查主要应用系统，查看是否采用了措施保证身份标识具有唯一性，是否对登录用户的口令最小长度、复杂度和更换周期等进行了要求和限制，保证身份鉴别信息不易被冒用；

d) 应检查主要应用系统，查看是否提供登录失败处理功能，是否根据安全策略设置了登录失败次数等参数；

e) 应测试主要应用系统，可通过试图以合法和非法用户分别登录系统，验证身份标识和鉴别功能是否有效；

f) 应测试主要应用系统，可通过多次输入错误的密码，验证登录失败处理功能是否有效；

g) **应渗透测试主要应用系统，如多次猜测用户口令，验证应用系统身份标识和鉴别功能是否不存在明显的弱点。**

7.1.4.1.3 结果判定

如果 7.1.4.1.2 中 a)～f)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

7.1.4.2 访问控制

7.1.4.2.1 测评指标

见 GB/T 22239—2008 中 7.1.4.2。

7.1.4.2.2 测评实施

本项要求包括：

a) 应检查主要应用系统，查看是否依据安全策略控制用户对文件、数据库表等客体的访问；

b) 应检查主要应用系统，查看其访问控制的覆盖范围是否包括与信息安全直接相关的主体、客体及它们之间的操作；

c) 应检查主要应用系统，查看是否有由授权用户设置其他用户访问系统功能和用户数据权限的功能，是否限制了默认用户的访问权限，是否修改了这些账户的默认口令；

d) 应检查主要应用系统的用户角色或权限的分配情况，查看是否仅授予不同账户为完成各自承担任务所需的最小权限，特权用户的权限是否分离，权限之间是否相互制约，如系统管理员不能进行审计操作、审计员不能进行系统管理操作等；

e) 应检查关键应用系统，查看是否删除多余的、过期的账户；

f) **应检查主要应用系统，查看是否能对重要信息资源设置敏感标记，这些敏感标记是否以默认方式生成或由安全员建立、维护和管理；**

g) **应检查主要应用系统，查看是否依据安全策略严格控制用户对有敏感标记重要信息资源的操作；**

h) 应测试主要应用系统，可通过以不同权限的用户登录系统，查看其拥有的权限是否与系统赋予的权限一致，验证应用系统访问控制功能是否有效；

i) 应测试主要应用系统，可通过以默认用户登录系统，并进行一些合法和非法操作，验证系统是否严格限制了默认账户的访问权限；

j) 应渗透测试主要应用系统，进行试图绕过访问控制的操作，验证应用系统的访问控制功能是否不存在明显的弱点。

7.1.4.2.3 结果判定

如果7.1.4.2.2中a)～i)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

7.1.4.3 安全审计

7.1.4.3.1 测评指标

见GB/T 22239—2008中7.1.4.3。

7.1.4.3.2 测评实施

本项要求包括：

a) 应检查主要应用系统，查看审计范围是否覆盖到每个用户，审计策略是否覆盖系统内重要的安全相关事件，例如，用户标识与鉴别、访问控制的所有操作记录、重要用户行为、系统资源的异常使用、重要系统命令的使用等；

b) 应检查主要应用系统的审计记录，查看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、事件的结果等内容；

c) 应检查主要应用系统，查看是否为授权用户浏览和分析审计数据提供专门的审计分析功能，并能根据需要生成审计报表；

d) 应测试主要应用系统，在应用系统上试图产生一些重要的安全相关事件(如进行用户登录、修改用户权限等操作)，查看应用系统是否对其进行了审计，验证应用系统安全审计的覆盖情况是否覆盖到每个用户；如果进行了审计则查看审计记录内容是否包含事件的日期、时间、发起者信息、类型、描述和结果等；

e) 应测试主要应用系统，试图非授权终止审计进程或审计功能，删除、修改或覆盖审计记录，查看安全审计进程和记录的保护情况。

7.1.4.3.3 结果判定

如果7.1.4.3.2中a)～e)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

7.1.4.4 剩余信息保护

7.1.4.4.1 测评指标

见GB/T 22239—2008中7.1.4.4。

7.1.4.4.2 测评实施

本项要求包括：

a) 应检查设计、验收文档或源代码，查看其是否有关于系统在释放或再分配鉴别信息所在存储空间给其他用户前如何将其进行完全清除(无论这些信息是存放在硬盘上还是在内存中)的描述；

b) 应检查设计、验收文档或源代码，查看其是否有关于释放或重新分配系统内文件、目录和数据库记录等资源所在存储空间给其他用户前进行完全清除的描述；

c) 应测试主要应用系统，用某用户登录系统并进行操作后，在该用户退出后用另一用户登录，试图操作（读取、修改或删除等）其他用户产生的文件、目录和数据库记录等资源，查看操作是否成功，验证系统提供的剩余信息保护功能是否正确（确保系统内的文件、目录和数据库记录等资源所在的存储空间，被释放或重新分配给其他用户前得到完全清除）。

7.1.4.4.3 结果判定

如果7.1.4.4.2中a)～c)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

7.1.4.5 通信完整性

7.1.4.5.1 测评指标

见GB/T 22239—2008中7.1.4.5。

7.1.4.5.2 测评实施

本项要求包括：

a) 应检查设计、验收文档或源代码，查看其是否有关于保护通信完整性的说明，如果有则查看是否有根据校验码判断对方数据有效性，以及散列（Hash）密码计算报文校验码的描述；

b) 应测试主要应用系统，可通过获取通信双方的数据包，查看通信报文中是否含有校验码。

7.1.4.5.3 结果判定

如果7.1.4.5.2中a)和b)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

7.1.4.6 通信保密性

7.1.4.6.1 测评指标

见GB/T 22239—2008中7.1.4.6。

7.1.4.6.2 测评实施

本项要求包括：

a) 应检查设计、验收文档或源代码，查看其是否有关于保护通信保密性的说明，如果有则查看是否有在通信双方建立连接之前利用密码技术进行会话初始化验证的描述，以及对整个报文或会话过程是否进行加密的描述；

b) 应测试主要应用系统，通过获取通信双方数据包并查看数据包的内容，查看系统是否能在通信双方建立连接之前，利用密码技术进行会话初始化验证（如SSL建立加密通道前是否利用密码技术进行了会话初始化验证）；并查看系统在通信过程中，对整个报文或会话过程是否进行加密。

7.1.4.6.3 结果判定

如果7.1.4.6.2中a)和b)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

7.1.4.7 抗抵赖

7.1.4.7.1 测评指标

见 GB/T 22239—2008 中 7.1.4.7。

7.1.4.7.2 测评实施

本项要求包括：

a) 如果业务应用有明确的抗抵赖需求，则应检查应用系统，查看系统是否提供在请求的情况下为数据原发者和接收者提供数据原发证据的功能；是否提供在请求的情况下为数据原发者和接收者提供数据接收证据的功能；

b) 如果业务应用有明确的抗抵赖需求，则应测试应用系统，通过模拟通信过程进行通信，查看系统是否提供在请求的情况下为数据原发者和接收者提供数据原发证据的功能；是否提供在请求的情况下为数据原发者和接收者提供数据接收证据的功能。

7.1.4.7.3 结果判定

如果 7.1.4.7.2 中 a)和 b)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

7.1.4.8 软件容错

7.1.4.8.1 测评指标

见 GB/T 22239—2008 中 7.1.4.8。

7.1.4.8.2 测评实施

本项要求包括：

a) 应检查设计或验收文档，查看是否有对人机接口输入或通信接口输入的数据进行有效性检验，在故障发生时自动保护当前所有状态保证系统能够进行恢复的描述；

b) 应测试主要应用系统，查看应用系统是否能明确拒绝不符合格式要求数据；

c) 应测试主要应用系统，验证是否提供自动保护功能，当故障发生时自动保护当前所有状态，保证系统能够进行恢复。

7.1.4.8.3 结果判定

如果 7.1.4.8.2 中 a)～c)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

7.1.4.9 资源控制

7.1.4.9.1 测评指标

见 GB/T 22239—2008 中 7.1.4.9。

7.1.4.9.2 测评实施

本项要求包括：

a) 应检查主要应用系统的配置参数，查看是否提供对最大并发会话连接数进行限制；

b) 应检查主要应用系统，查看是否对一个访问账户或一个请求进程占用的资源分配最大限额和最小限额；

c) 应检查主要应用系统，查看是否有服务水平最小值的设定，当系统的服务水平降低到预先设定的最小值时，系统报警；

d) 应检查主要应用系统，查看是否能根据安全策略设定主体的服务优先级，根据优先级分配系统资源；

e) 应测试主要应用系统，当应用系统的通信双方中的一方在一段时间内未作任何响应，查看另一方是否能够自动结束会话；

f) 应测试主要应用系统，可通过对系统进行超过规定的单个账户的多重并发会话数进行连接，验证系统是否能够正确地限制单个账户的多重并发会话数；

g) 应测试主要应用系统，可试图使服务水平降低到预先规定的最小值，验证系统是否能够正确检测并报警。

7.1.4.9.3 结果判定

如果7.1.4.9.2中a)～g)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

7.1.5 数据安全及备份恢复

7.1.5.1 数据完整性

7.1.5.1.1 测评指标

见GB/T 22239—2008中7.1.5.1。

7.1.5.1.2 测评实施

本项要求包括：

a) 如果主要网络设备、主要主机操作系统和主要数据库管理系统能够进行远程管理，则应查看其能否检测系统管理数据(如配置文件)、鉴别信息在传输过程中完整性受到了破坏，并在检测到完整性错误时采取必要的恢复措施；

b) 应检查应用系统的设计、验收文档或源代码，查看是否有关于能检测系统管理数据、鉴别信息和重要业务数据传输过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施的描述；

c) 应检查主要网络设备、主要操作系统和主要数据库管理系统，查看是否配备检测系统管理数据(如配置文件)和鉴别信息在存储过程中完整性受到破坏的功能，并在检测到完整性错误时是否能采取必要的恢复措施；

d) 应检查主要应用系统，查看是否配备检测系统管理数据、鉴别信息和业务数据在存储过程中完整性受到破坏的功能，并在检测到完整性错误时是否能采取必要的恢复措施。

7.1.5.1.3 结果判定

如果7.1.5.1.2中a)～d)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

7.1.5.2 数据保密性

7.1.5.2.1 测评指标

见 GB/T 22239—2008 中 7.1.5.2。

7.1.5.2.2 测评实施

本项要求包括：

a) 应检查主要网络设备、主要操作系统和主要数据库管理系统，查看其管理数据和鉴别信息是否采用加密或其他有效措施实现了传输和存储保密性；

b) 应检查主要应用系统，查看其管理数据、鉴别信息和重要业务数据是否采用加密或其他有效措施实现传输和存储保密性；

c) 应测试主要网络设备、主要操作系统、主要数据库管理系统和主要应用系统，可通过用嗅探工具获取通信数据包，查看是否为密文。

7.1.5.2.3 结果判定

如果 7.1.5.2.2 中 a)～c)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

7.1.5.3 备份和恢复

7.1.5.3.1 测评指标

见 GB/T 22239—2008 中 7.1.5.3。

7.1.5.3.2 测评实施

本项要求包括：

a) 应检查是否对主要网络设备、主要主机操作系统、主要数据库管理系统和主要应用系统的重要信息进行了备份，备份方式(如是否为完全数据备份)、频率和介质存放方式是否达到相关标准的要求，是否定期对备份数据进行恢复测试；

b) 应检查主要网络设备、主要主机操作系统、主要数据库管理系统和主要应用系统是否对重要信息进行了异地数据备份；

c) 应检查网络拓扑结构是否不存在关键节点的单点故障；

d) 应检查主要网络设备、通信线路和数据处理系统(如包含数据库管理系统在内的数据库服务器)是否提供硬件冗余。

7.1.5.3.3 结果判定

如果 7.1.5.3.2 中 a)～d)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

7.2 安全管理测评

7.2.1 安全管理制度

7.2.1.1 管理制度

7.2.1.1.1 测评指标

见 GB/T 22239—2008 中 7.2.1.1。

7.2.1.1.2 测评实施

本项要求包括：

a) **应访谈安全主管，询问机构是否形成全面的信息安全管理制度体系，制度体系是否由总体方针、安全策略、管理制度、操作规程等构成；**

b) 应检查信息安全工作的总体方针和安全策略文件，查看文件是否明确机构安全工作的总体目标、范围、原则和安全框架等；

c) 应检查各项安全管理制度，查看是否覆盖物理、网络、主机系统、数据、应用、建设和运维等层面的管理内容；

d) 应检查是否具有日常管理操作的操作规程（如系统维护手册和用户操作规程等）。

7.2.1.1.3 结果判定

如果7.2.1.1.2中a)～d)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

7.2.1.2 制定和发布

7.2.1.2.1 测评指标

见GB/T 22239—2008中7.2.1.2。

7.2.1.2.2 测评实施

本项要求包括：

a) 应访谈安全主管，询问是否由专门的部门或人员负责制定安全管理制度；

b) 应访谈安全主管，询问安全管理制度是否能够发布到相关人员手中，是否对制定的安全管理制度进行论证和审定，**是否按照统一的格式标准或要求制定；**

c) **应检查制度制定和发布要求管理文档，查看文档是否说明安全管理制度的制定和发布程序、格式要求及版本编号等相关内容；**

d) 应检查管理制度评审记录，查看是否有相关人员的评审意见；

e) **应检查各项安全管理制度文档，查看文档是否是正式发布的文档，是否注明适用和发布范围，是否具有版本标识，是否具有管理层的签字或单位盖章；查看各项制度文档格式是否统一；**

f) **应检查安全管理制度的收发登记记录，查看是否通过正式、有效的方式收发（如正式发文、领导签署和单位盖章等），是否注明发布范围。**

7.2.1.2.3 结果判定

如果7.2.1.2.2中a)～f)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

7.2.1.3 评审和修订

7.2.1.3.1 测评指标

见GB/T 22239—2008中7.2.1.3。

7.2.1.3.2 测评实施

本项要求包括：

a) **应访谈安全主管，询问是否由信息安全领导小组负责定期对安全管理制度体系的合理性和适用性进行审定，是否定期或不定期对安全管理制度进行检查、审定；**
b) **应检查是否具有安全管理制度体系的评审记录，是否记录了相关人员的评审意见；**
c) 应检查是否具有安全管理制度的检查或评审记录，如果对制度做过修订，检查是否有修订版本的安全管理制度。

7.2.1.3.3 结果判定

如果7.2.1.3.2中a)～c)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

7.2.2 安全管理机构

7.2.2.1 岗位设置

7.2.2.1.1 测评指标

见GB/T 22239—2008中7.2.2.1。

7.2.2.1.2 测评实施

本项要求包括：

a) **应访谈安全主管，询问是否设立指导和管理信息安全工作的委员会或领导小组，其最高领导是否由单位主管领导委任或授权的人员担任；**
b) **应访谈安全主管，询问是否设立专职的安全管理机构(即信息安全管理工作的职能部门)，是否明确各部门的职责分工；**
c) 应访谈安全主管，询问信息系统是否设置了系统管理员、网络管理员和安全管理员等岗位，各个岗位的职责分工是否明确；是否设立安全管理各个方面的负责人；
d) **应检查部门、岗位职责文件，查看文件是否明确安全管理机构的职责，是否明确机构内各部门的职责和分工，部门职责是否涵盖物理、网络和系统安全等各个方面；**查看文件是否明确设置安全主管、安全管理各个方面的负责人、系统管理员、网络管理员、安全管理员等各个岗位职责；**查看文件是否明确各个岗位人员应具有的技能要求；**
e) **应检查是否具有信息安全管理委员会或领导小组成立的正式文件；**
f) **应检查信息安全管理委员会或领导小组职责文件，查看是否明确管理委员会或领导小组职责和其最高领导岗位的职责。**

7.2.2.1.3 结果判定

如果7.2.2.1.2中a)～f)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

7.2.2.2 人员配备

7.2.2.2.1 测评指标

见GB/T 22239—2008中7.2.2.2。

7.2.2.2.2 测评实施

本项要求包括：

a) 应访谈安全主管，询问各个安全管理岗位是否配备了一定数量的人员，对关键事务岗位是否配备多人；

b) 应检查人员配备要求管理文档，查看是否明确应配备系统管理员、网络管理员、安全管理员等重要岗位人员并明确应配备专职的安全管理员；查看是否明确关键事务的管理人员应配备2人或2人以上共同管理；

c) 应检查安全管理各岗位人员信息表，查看其是否明确系统管理员、网络管理员、安全管理员等重要岗位人员的信息，安全管理员是否是专职人员。

7.2.2.2.3 结果判定

如果7.2.2.2.2中a)～c)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

7.2.2.3 授权和审批

7.2.2.3.1 测评指标

见GB/T 22239—2008中7.2.2.3。

7.2.2.3.2 测评实施

本项要求包括：

a) 应访谈安全主管，询问其是否规定对信息系统中的重要活动进行审批，审批活动是否得到授权；是否定期审查、更新需审批项目；

b) 应检查审批管理制度文档，查看文档是否明确审批事项、需逐级审批的事项、审批部门、批准人等；是否明确系统变更、重要操作、物理访问和系统接入等事项的审批流程；是否明确需定期审查、更新审批的项目、审批部门、批准人和审查周期等；

c) 应检查经逐级审批的文档，查看是否具有各级批准人的签字和审批部门的盖章；

d) 应检查关键活动的审批过程记录，查看记录的审批程序与文件要求是否一致。

7.2.2.3.3 结果判定

如果7.2.2.3.2中a)～d)均为肯定，则该测评指标符合要求，否则，信息系统不符合或部分符合本单元测评指标要求。

7.2.2.4 沟通和合作

7.2.2.4.1 测评指标

见GB/T 22239—2008中7.2.2.4。

7.2.2.4.2 测评实施

本项要求包括：

a) 应访谈安全主管，询问是否与外单位(公安机关、电信公司、兄弟单位、供应商、业界专家、专业的安全公司、安全组织等)建立沟通、合作机制；是否与组织机构内其他部门之间及内部各部门管理人员之间建立沟通、合作机制；

b) 应访谈安全主管，询问是否召开过部门间协调会议，组织其他部门人员共同协助处理信息系统安全有关问题，安全管理机构内部是否召开过安全工作会议以部署安全工作的实施；信息安全领导小组或者管理委员会是否定期召开例会；

c) 应访谈安全主管，询问是否聘请信息安全专家作为常年的安全顾问，指导信息安全建设，参与安全规划和安全评审等；

d) 应检查组织内部机构之间以及信息安全职能部门内部的安全工作会议文件或会议记录，查看是否有会议内容、会议时间、参加人员和会议结果等的描述；

e) 应检查信息安全领导小组或者管理委员会定期例会会议文件或会议记录，查看是否有会议内容、会议时间、参加人员、会议结果等的描述；

f) 应检查外联单位联系列表，查看外联单位是否包含公安机关、电信公司、兄弟单位、供应商、业界专家、专业的安全公司和安全组织等，是否说明外联单位的名称、合作内容、联系人和联系方式等内容；

g) 应检查是否具有安全顾问名单或者聘请安全顾问的证明文件，查看是否有安全顾问指导信息安全建设、参与安全规划和安全评审的相关文档或记录。

7.2.2.4.3 结果判定

如果7.2.2.4.2中a)～g)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

7.2.2.5 审核和检查

7.2.2.5.1 测评指标

见GB/T 22239—2008中7.2.2.5。

7.2.2.5.2 测评实施

本项要求包括：

a) 应访谈安全主管，询问是否组织人员定期对信息系统安全技术措施和安全管理制度落实情况进行全面安全检查；

b) 应访谈安全管理员，询问是否定期检查系统日常运行、系统漏洞和数据备份等情况；

c) 应检查安全检查管理制度文档，查看文档是否规定定期进行全面安全检查，是否规定检查内容、检查程序和检查周期等，检查内容是否包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等；

d) 应检查全面安全检查报告，查看报告中是否有检查内容、检查人员、检查数据汇总表、检查结果等的描述，检查内容是否包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等；

e) 应检查安全管理员定期实施安全检查的报告，查看检查内容是否包括系统日常运行、系统漏洞和数据备份等情况；

f) 应检查是否具有执行安全检查时的安全检查表、安全检查记录和结果通告记录。

7.2.2.5.3 结果判定

如果7.2.2.5.2中a)～f)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

7.2.3 人员安全管理

7.2.3.1 人员录用

7.2.3.1.1 测评指标

见GB/T 22239—2008中7.2.3.1。

7.2.3.1.2 测评实施

本项要求包括：

a) 应访谈人事负责人，询问是否由专门的部门或人员负责人员的录用工作；

b) 应访谈人事负责人，询问在人员录用时是否对被录用人的身份、背景、专业资格和资质进行审查，对技术人员的技术技能进行考核；

c) 应访谈人事负责人，询问是否与被录用人员签署保密协议；

d) **应访谈人事负责人，询问对从事关键岗位的人员是否从内部人员中选拔，是否要求其签署岗位安全协议；**

e) 应检查人员录用管理文档，查看是否说明录用人员应具备的条件（如学历、学位要求，技术人员应具备的专业技术水平，管理人员应具备的安全管理知识等）；

f) 应检查是否具有人员录用时对录用人身份、背景、专业资格和资质等进行审查的相关文档或记录，查看是否记录审查内容和审查结果等；

g) 应检查人员录用时的技能考核文档或记录，查看是否记录考核内容和考核结果等；

h) 应检查保密协议，查看是否有保密范围、保密责任、违约责任、协议的有效期限和责任人的签字等内容；

i) **应检查岗位安全协议，查看是否有岗位安全责任定义、协议的有效期限和责任人签字等内容。**

7.2.3.1.3 结果判定

如果7.2.3.1.2中a)～i)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

7.2.3.2 人员离岗

7.2.3.2.1 测评指标

见GB/T 22239—2008中7.2.3.2。

7.2.3.2.2 测评实施

本项要求包括：

a) 应访谈安全主管，询问是否及时终止离岗人员的所有访问权限，是否取回各种身份证件、钥匙、徽章以及机构提供的软硬件设备等；

b) 应访谈人事负责人，询问人员离岗是否遵循严格的调离手续，**是否要求人员调离时须承诺相关保密义务后方可离开；**

c) **应检查人员离岗的管理文档，查看是否规定了人员调离手续和离岗要求等；**

d) 应检查是否具有离岗人员交还身份证件、设备等的登记记录；

e) 应检查是否具有按照离岗程序办理调离手续的记录；

f) **应检查保密承诺文档，查看是否有调离人员的签字。**

7.2.3.2.3 结果判定

如果7.2.3.2.2中a)～f)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

7.2.3.3 人员考核

7.2.3.3.1 测评指标

见 GB/T 22239—2008 中 7.2.3.3。

7.2.3.3.2 测评实施

本项要求包括：

a) 应访谈安全主管，询问是否定期对各个岗位人员进行安全技能及安全知识的考核，是否对关键岗位人员定期进行安全审查和技能考核；

b) 应检查考核记录，查看考核人员是否包括各个岗位的人员，**考核内容是否包含安全知识、安全技能等**；

c) **应检查是否具有对关键岗位人员的安全审查记录。**

7.2.3.3.3 结果判定

如果 7.2.3.3.2 中 a)～c)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

7.2.3.4 安全意识教育和培训

7.2.3.4.1 测评指标

见 GB/T 22239—2008 中 7.2.3.4。

7.2.3.4.2 测评实施

本项要求包括：

a) 应访谈安全主管，询问是否制定培训计划并按计划对各个岗位人员进行安全教育和培训；是否对违反安全策略和规定的人员进行惩戒；

b) **应检查安全责任和惩戒措施管理文档，查看是否包含具体的安全责任和惩戒措施；**

c) **应检查信息安全教育及技能培训和考核管理制度文档，查看是否明确培训周期、培训方式、培训内容和考核方式等相关内容；**

d) 应检查安全教育和培训计划文档，**查看是否具有不同岗位的培训计划**；查看计划是否明确了培训方式、培训对象、培训内容、培训时间和地点等，培训内容是否包含信息安全基础知识、岗位操作规程等；

e) 应检查安全教育和培训记录，查看记录是否有培训人员、培训内容、培训结果等的描述。

7.2.3.4.3 结果判定

如果 7.2.3.4.2 中 a)～e)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

7.2.3.5 外部人员访问管理

7.2.3.5.1 测评指标

见 GB/T 22239—2008 中 7.2.3.5。

7.2.3.5.2 测评实施

本项要求包括：

a) 应访谈安全主管，询问外部人员访问重要区域（如访问机房、重要服务器或设备区等）是否需经有关部门或负责人书面批准，是否由专人全程陪同或监督，是否进行记录并备案管理；

b) **应检查外部人员访问管理文档，查看是否明确允许外部人员访问的范围（区域、系统、设备、信息等内容），外部人员进入的条件（对哪些重要区域的访问须提出书面申请批准后方可进入），外部人员进入的访问控制措施（由专人全程陪同或监督等）等；**

c) **应检查外部人员访问重要区域的书面申请文档，查看是否具有批准人允许访问的批准签字等；**

d) 应检查外部人员访问重要区域的登记记录，查看是否记录了外部人员访问重要区域的进入时间、离开时间、访问区域及陪同人等。

7.2.3.5.3 结果判定

如果 7.2.3.5.2 中 a)～d)均为肯定，则该测评指标符合要求，否则，信息系统不符合或部分符合本单元测评指标要求。

7.2.4 系统建设管理

7.2.4.1 系统定级

7.2.4.1.1 测评指标

见 GB/T 22239—2008 中 7.2.4.1。

7.2.4.1.2 测评实施

本项要求包括：

a) 应访谈系统建设负责人，询问是否参照定级指南确定信息系统安全保护等级，**是否组织相关部门和有关安全技术专家对定级结果进行论证和审定；**

b) 应检查系统定级文档，查看文档是否明确信息系统的边界和信息系统的安全保护等级，是否说明定级的方法和理由，是否有相关部门或主管领导的盖章或签名；

c) **应检查定级结果的论证评审会议文档，查看是否有相关部门和有关安全技术专家对定级结果的论证意见。**

7.2.4.1.3 结果判定

如果 7.2.4.1.2 中 a)～c)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

7.2.4.2 安全方案设计

7.2.4.2.1 测评指标

见 GB/T 22239—2008 中 7.2.4.2。

7.2.4.2.2 测评实施

本项要求包括：

a) **应访谈系统建设负责人，询问是否授权专门的部门对信息系统的安全建设进行总体规划，由何**

部门负责；

b) 应访谈系统建设负责人，询问是否根据信息系统的等级划分情况统一考虑总体安全策略、安全技术框架、安全管理策略、总体建设规划和详细设计方案等；

c) 应访谈系统建设负责人，询问是否对安全建设的配套文件进行论证和审定，是否根据等级测评、安全评估的结果定期调整和修订安全建设的配套文件；

d) 应检查是否有系统安全建设的工作计划，查看文件是否明确了系统的近期安全建设计划和远期安全建设计划；

e) 应检查是否有系统总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等配套文件，查看各个文件是否有机构管理层的批准；

f) 应检查配套文件的论证评审记录或文档，查看是否有相关部门和有关安全技术专家对总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件的论证意见；

g) 应检查是否具有总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件的维护记录或修订版本。

7.2.4.2.3 结果判定

如果7.2.4.2.2中a)～g)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

7.2.4.3 产品采购和使用

7.2.4.3.1 测评指标

见GB/T 22239—2008中7.2.4.3。

7.2.4.3.2 测评实施

本项要求包括：

a) 应访谈系统建设负责人，询问是否有专门的部门负责产品的采购，由何部门负责；

b) 应访谈系统建设负责人，询问系统是否采用了密码产品，密码产品的采购和使用是否符合国家密码主管部门的要求；

c) 应访谈系统建设负责人，询问系统使用的有关信息安全产品是否符合国家的有关规定，如安全产品获得了销售许可证等；

d) 应访谈系统建设负责人，询问采购产品前是否预先对产品进行选型测试确定产品的候选范围，是否有产品采购清单指导产品采购，是否定期审定和更新候选产品采购清单，审定周期多长；

e) 应抽样检查安全产品和密码产品的相关凭证，如销售许可等，查看是否使用了符合国家有关规定产品；

f) 应检查是否具有产品选型测试结果文档、候选产品采购清单及审定或更新的记录。

7.2.4.3.3 结果判定

如果7.2.4.3.2中a)～f)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

7.2.4.4 自行软件开发

7.2.4.4.1 测评指标

见GB/T 22239—2008中7.2.4.4。

7.2.4.4.2 测评实施

本项要求包括：

a) 应访谈系统建设负责人，询问是否进行自主开发软件，是否对**程序资源库的修改、更新、发布进行授权和批准，授权部门是何部门，批准人是何人，是否要求开发人员不能做测试人员（即二者分离）**，自主开发软件是否在独立的模拟环境中完成编码和调试，如相对独立的网络区域；

b) 应访谈系统建设负责人，询问软件设计相关文档是否由专人负责保管，负责人是何人，**如何控制使用，测试数据和测试结果是否受到控制**；

c) **应访谈软件开发人员，询问其是否了解软件开发管理制度，是否了解代码编写安全规范，是否按照代码编写安全规范进行软件开发**；

d) 应检查软件开发管理制度，查看文件是否明确软件设计、开发、测试、验收过程的控制方法和人员行为准则，是否明确哪些开发活动应经过授权、审批；

e) **应检查代码编写安全规范，查看规范中是否明确代码编写规则，应抽样部分源代码，检查是否按照代码编写安全规范开发**；

f) **应检查对程序资源库的修改、更新、发布进行授权和审批的文档或记录，查看是否有批准人的签字**；

g) **应检查是否具有软件开发相关文档（源代码、测试数据、测试结果等）的使用控制记录**；

h) 应检查是否具有软件使用指南或操作手册等；

i) 应检查网络拓扑图和实际开发环境，查看是否实际运行环境和开发环境有效隔离。

7.2.4.4.3 结果判定

如果 7.2.4.4.2 中 a)～i)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

7.2.4.5 外包软件开发

7.2.4.5.1 测评指标

见 GB/T 22239—2008 中 7.2.4.5。

7.2.4.5.2 测评实施

本项要求包括：

a) 应访谈系统建设负责人，询问软件交付前是否依据开发要求的技术指标对软件功能和性能等进行验收测试，软件安装之前是否检测软件中的恶意代码；

b) 应访谈系统建设负责人，是否要求开发单位提供源代码，是否根据源代码对软件中可能存在的后门进行审查；

c) 应检查是否具有软件开发的相关文档，如需求分析说明书、软件设计说明书等，是否具有软件操作手册或使用指南；

d) 应检查部分软件源代码，查看是否具有源代码，**应检查软件源代码审查记录，查看是否包括对可能存在后门的审查结果**。

7.2.4.5.3 结果判定

如果 7.2.4.5.2 中 a)～d)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

7.2.4.6 工程实施

7.2.4.6.1 测评指标

见 GB/T 22239—2008 中 7.2.4.6。

7.2.4.6.2 测评实施

本项要求包括：

a) 应访谈系统建设负责人，询问是否指定专门部门或人员对工程实施过程进行进度和质量控制，由何部门/何人负责；

b) **应访谈系统建设负责人，询问是否要求工程实施单位提供其能够实施安全工程的资质证明和能力保证；**

c) **应检查系统建设方面的管理制度，查看其是否包括工程实施过程的控制方法、实施参与人员的行为准则等方面内容；**

d) 应检查工程实施方案，查看其是否包括工程时间限制、进度控制和质量控制等方面内容，**是否按照工程实施方面的管理制度进行各类控制、产生阶段性文档等。**

7.2.4.6.3 结果判定

如果 7.2.4.6.2 中 a)～d)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

7.2.4.7 测试验收

7.2.4.7.1 测评指标

见 GB/T 22239—2008 中 7.2.4.7。

7.2.4.7.2 测评实施

本项要求包括：

a) **应访谈系统建设负责人，询问是否有专门的部门负责测试验收工作，由何部门负责；是否委托第三方测试机构对信息系统进行独立的安全性测试；**

b) **应访谈系统建设负责人，询问是否根据设计方案或合同要求组织相关部门和人员制定工程测试验收方案，并对系统测试验收报告进行审定；**

c) **应检查系统建设方面的管理制度，查看其是否包括对系统测试验收的控制方法和人员行为准则规定；**

d) 应检查是否具有工程测试验收方案，查看其是否明确说明参与测试的部门、人员、测试验收内容、现场操作过程等内容，**过程控制是否符合管理规定的要求；**

e) 应检查是否具有系统测试验收报告，是否有相关部门和人员对系统测试验收报告进行审定的意见，**是否有第三方测试机构的签字或盖章。**

7.2.4.7.3 结果判定

如果 7.2.4.7.2 中 a)～e)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

7.2.4.8 系统交付

7.2.4.8.1 测评指标

见 GB/T 22239—2008 中 7.2.4.8。

7.2.4.8.2 测评实施

本项要求包括：

a) 应访谈系统建设负责人，询问是否有专门的部门负责系统交接工作，系统交接工作是否根据交付清单对所交接的设备、文档、软件等进行清点；

b) 应访谈系统建设负责人，询问系统正式运行前是否对运行维护人员进行过培训，针对哪些方面进行过培训；

c) 应检查系统建设方面的管理制度，查看其是否包括系统交付的控制方法和人员行为准则的规定；

d) 应检查是否具有系统交付清单，查看交付清单是否说明系统交付的各类设备、软件、文档等；

e) 应检查系统交付提交的文档，查看是否有指导用户进行系统运维的文档等，提交的文档是否符合管理规定的要求；

f) 应检查是否有系统交付技术培训记录，查看是否包括培训内容、培训时间和参与人员等。

7.2.4.8.3 结果判定

如果 7.2.4.8.2 中 a)～f)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

7.2.4.9 系统备案

7.2.4.9.1 测评指标

见 GB/T 22239—2008 中 7.2.4.9。

7.2.4.9.2 测评实施

本项要求包括：

a) 应访谈系统建设负责人，询问是否有专门的部门或人员负责管理系统定级的相关文档，由何部门/何人负责；询问对系统定级相关备案文档使用的控制方式；

b) 应检查是否具有将系统等级及相关材料报主管部门备案的记录或备案文档；

c) 应检查是否具有将系统等级及相关备案材料报相应公安机关备案的记录或证明。

7.2.4.9.3 结果判定

如果 7.2.4.9.2 中 a)～c)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

7.2.4.10 安全服务商选择

7.2.4.10.1 测评指标

见 GB/T 22239—2008 中 7.2.4.11。

7.2.4.10.2 测评实施

本项要求包括：

a) 应访谈系统建设负责人，询问信息系统选择的安全服务商有哪些，是否符合国家有关规定；

b) 应检查是否具有与安全服务商签订的安全责任合同书或保密协议等文档，查看其内容是否包含保密范围、安全责任、违约责任、协议的有效期限和责任人的签字等；

c) 应检查是否具有与安全服务商签订的服务合同或安全责任合同书，查看是否明确了后期的技术支持和服务承诺等内容。

7.2.4.10.3 结果判定

如果7.2.4.10.2中a)～c)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

7.2.5 系统运维管理

7.2.5.1 环境管理

7.2.5.1.1 测评指标

见GB/T 22239—2008中7.2.5.1。

7.2.5.1.2 测评实施

本项要求包括：

a) 应访谈系统运维负责人，询问是否有专门的部门或人员对机房供配电、空调、温湿度控制等设施进行定期维护，由何部门/何人负责，维护周期多长；

b) 应访谈系统运维负责人，询问是否有专门的部门或人员对机房的出入、服务器开机/关机等日常工作进行管理，由何部门/何人负责；

c) 应访谈系统运维负责人，询问为保证办公环境的保密性采取了哪些控制措施，在哪个区域接待来访人员，工作人员调离时是否收回办公室钥匙等；

d) 应检查是否有机房安全管理制度，查看其内容是否覆盖机房物理访问、物品带进/带出机房和机房环境安全等方面；

e) 应检查是否具有空调、温湿度控制等机房设施的维护保养记录，表明定期对这些设施进行了维护保养；

f) **应检查办公环境，查看其是否包括工作人员离开座位时退出登陆状态、桌面没有敏感信息文件等。**

7.2.5.1.3 结果判定

如果7.2.5.1.2中a)～f)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

7.2.5.2 资产管理

7.2.5.2.1 测评指标

见GB/T 22239—2008中7.2.5.2。

7.2.5.2.2 测评实施

本项要求包括：

a) 应访谈系统运维负责人，询问是否有资产管理的责任人员或部门，由何部门/何人负责；

b) 应检查是否有资产清单，查看其内容是否覆盖资产责任部门、责任人、所处位置和重要程度等方面；

c) 应检查是否有资产安全管理方面的制度，查看是否明确信息资产管理的责任部门、责任人，查看其内容是否覆盖资产使用、借用、维护等方面；

d) **应检查是否有资产安全管理方面的制度，查看是否明确了依据资产的重要程度对资产进行分类和标识管理的方法，是否明确了信息分类标识的原则和方法，是否说明了不同类别的资产采取的不同管理措施。**

7.2.5.2.3 结果判定

如果 7.2.5.2.2 中 a)～d)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

7.2.5.3 介质管理

7.2.5.3.1 测评指标

见 GB/T 22239—2008 中 7.2.5.3。

7.2.5.3.2 测评实施

本项要求包括：

a) 应访谈资产管理员，询问介质的存放环境是否采取保护措施防止介质被盗、被毁等；

b) 应访谈资产管理员，询问是否根据介质的目录清单对介质的使用现状进行定期检查；

c) 应访谈资产管理员，询问是否将介质保管在一个特定环境里，有专人负责，并根据重要性对介质进行分类和标识；

d) **应访谈资产管理员，询问是否对某些重要介质实行异地存储，异地存储环境是否与本地环境相同；**

e) **应访谈资产管理员，询问是否定期对存储介质的完整性（数据是否损坏或丢失）和可用性（介质是否受到物理破坏）进行检查，是否对重要数据进行加密存储；**

f) 应访谈资产管理员，询问对送出维修或销毁的介质在送出之前是否对介质内存储数据进行净化处理，**对介质带出工作环境和重要介质中的数据和软件是否进行保密性处理；对保密性较高的介质销毁前是否有领导批准；**

g) **应访谈资产管理员，询问对介质的物理传输过程是否要求选择可靠传输人员、严格介质的打包、选择安全的物理传输途径、双方在场交付等环节的控制；**

h) **应检查是否有介质安全管理制度，查看是否对介质的存放环境、使用、维护和销毁等方面作出规定；**

i) 应检查介质使用管理记录，查看其是否记录介质归档和使用等情况；

j) 应检查介质存储环境，查看是否对其进行了分类，并具有不同标识；

k) **应抽样检查重要介质，查看是否可以使用，查看需要加密存储的数据是否加密。**

7.2.5.3.3 结果判定

如果 7.2.5.3.2 中 a)～k)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合

或部分符合本单元测评指标要求。

7.2.5.4 设备管理

7.2.5.4.1 测评指标

见 GB/T 22239—2008 中 7.2.5.4。

7.2.5.4.2 测评实施

本项要求包括：

a) 应访谈系统运维负责人，询问是否有专门的部门或人员对各种设备、线路进行定期维护，由何部门/何人负责，维护周期多长；

b) 应检查是否有设备安全管理制度，查看其内容是否对各种软硬件设备的选型、采购、发放和领用等环节进行规定；

c) 应检查设备安全管理制度中是否有对终端计算机、便携机和网络设备等使用方式、操作原则、注意事项等方面的规定，是否有信息处理设备必须经过审批才能带离机房或办公地点的要求；

d) **应检查设备安全管理制度中是否有对涉外维修和服务的审批、维修过程的监督控制管理等要求；**

e) **应检查是否有关键设备的操作规程。**

7.2.5.4.3 结果判定

如果 7.2.5.4.2 中 a)～e)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

7.2.5.5 监控管理和安全管理中心

7.2.5.5.1 测评指标

见 GB/T 22239—2008 中 7.2.5.5。

7.2.5.5.2 测评实施

本项要求包括：

a) **应访谈系统运维负责人，询问是否对通信线路、主机、网络设备和应用软件的运行状况，对设备状态、恶意代码、网络流量、补丁升级、安全审计等安全相关事项进行集中管理，是否形成监测记录文档，是否组织人员对监测记录进行整理并保管；**

b) **应访谈系统运维负责人，询问其是否组织人员定期对监测记录进行分析、评审，是否发现可疑行为并对其采取必要的措施，是否形成分析报告；**

c) **应检查是否具有安全集中管理的相关工具，可以实施对设备状态、恶意代码、补丁升级、安全审计等安全相关事项的集中监控和管理；**

d) **应检查监测记录，查看是否记录监控对象、监控内容、监控的异常现象处理等方面，查看是否对异常现象及处理措施形成分析报告。**

7.2.5.5.3 结果判定

如果 7.2.5.5.2 中 a)～d)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

7.2.5.6 网络安全管理

7.2.5.6.1 测评指标

见 GB/T 22239—2008 中 7.2.5.6。

7.2.5.6.2 测评实施

本项要求包括：

a) 应访谈系统运维负责人，询问是否指定专门的部门或人员负责网络管理，维护网络运行日志、监控记录，分析处理报警信息等；

b) 应访谈网络管理员，询问是否定期对网络进行漏洞扫描，扫描周期多长，发现漏洞是否及时修补；

c) 应访谈网络管理员，询问是否根据厂家提供的软件升级版本对网络设备进行过升级，目前的版本号为多少，升级前是否对重要文件进行备份，采取什么方式备份；

d) 应访谈网络管理员，网络的外联种类有哪些，是否都得到授权与批准，由何部门或何人批准，申请和批准的过程；

e) 应检查是否有网络安全管理制度，查看其是否覆盖网络安全配置、安全策略、升级与打补丁、授权访问、日志保存时间、口令更新周期等方面内容；

f) **应检查是否有网络安全管理制度，查看其是否明确了允许或者拒绝便携式和移动式设备网络接入的规定；**

g) 应检查是否有网络漏洞扫描报告，检查扫描时间间隔与扫描周期是否一致，**检查网络设备是否实现了最小服务配置；**

h) 应检查是否具有网络设备配置文件的备份文件，**是否离线备份；**

i) 应检查是否具有内部网络外联的授权批准书，**检查是否有网络违规行为（如拨号上网等）的检查手段和工具。**

7.2.5.6.3 结果判定

如果 7.2.5.6.2 中 a)～i)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

7.2.5.7 系统安全管理

7.2.5.7.1 测评指标

见 GB/T 22239—2008 中 7.2.5.7。

7.2.5.7.2 测评实施

本项要求包括：

a) 应访谈系统运维负责人，询问是否指定专门的部门或人员负责系统管理，如根据业务需求和系统安全分析制定系统的访问控制策略，控制分配文件及服务的访问权限；

b) 应访谈系统运维负责人，询问是否**对系统管理员用户进行分类，明确各个角色的权限、责任和风险，权限设定是否遵循最小授权原则；**

c) 应访谈系统管理员，询问系统日常管理的主要内容，是否有操作规程指导日常管理工作，包括重要的日常操作、参数的设置和修改等；

d) 应访谈系统管理员，询问是否定期对系统进行漏洞扫描，扫描周期多长，发现漏洞是否及时修补，在安装系统补丁前是否对重要文件进行备份，是否先在测试环境中测试通过再安装；

e) 应检查是否有系统安全管理制度，查看其内容是否覆盖系统安全策略、安全配置、日志管理和日常操作流程等方面；

f) 应检查是否有系统漏洞扫描报告，检查扫描时间间隔与扫描周期是否一致，**检查系统服务是否实现了最小服务配置**；

g) 应检查是否有详细日常运行维护操作日志。

7.2.5.7.3 结果判定

如果7.2.5.7.2中a)～g)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

7.2.5.8 恶意代码防范管理

7.2.5.8.1 测评指标

见GB/T 22239—2008中7.2.5.8。

7.2.5.8.2 测评实施

本项要求包括：

a) 应访谈系统运维负责人，询问是否对员工进行基本恶意代码防范意识的教育，是否告知应及时升级软件版本，使用外来设备、网络上接收文件和外来计算机或存储设备接入网络系统之前进行病毒检查等；

b) 应访谈系统运维负责人，询问是否指定专人对恶意代码进行检测，发现病毒后是否及时处理；

c) **应访谈安全管理员，询问是否定期检查恶意代码库的升级情况，对截获的危险病毒或恶意代码是否及时进行分析处理，并形成书面的报表和总结汇报**；

d) 应检查是否有恶意代码防范方面的管理制度，查看其内容是否覆盖防恶意代码软件的授权使用、恶意代码库升级、定期汇报等方面；

e) **应检查是否具有恶意代码检测记录、恶意代码库升级记录和分析报告，查看升级记录是否记录升级时间、升级版本等内容；查看分析报告是否描述恶意代码的特征、修补措施等内容。**

7.2.5.8.3 结果判定

如果7.2.5.8.2中a)～e)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

7.2.5.9 密码管理

7.2.5.9.1 测评指标

见GB/T 22239—2008中7.2.5.9。

7.2.5.9.2 测评实施

本项要求包括：

a) **应访谈系统运维负责人，询问系统中是否使用密码技术和产品，密码技术和产品的使用是否遵照国家密码管理规定**；

b) **应检查是否具有密码使用方面的管理制度。**

7.2.5.9.3 结果判定

如果7.2.5.9.2中a)和b)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

7.2.5.10 变更管理

7.2.5.10.1 测评指标

见GB/T 22239—2008中7.2.5.10。

7.2.5.10.2 测评实施

本项要求包括：

a) 应访谈系统运维负责人，询问是否针对系统的重大变更制定变更方案指导系统变更工作的开展；

b) 应访谈系统运维负责人，**询问变更方案是否经过评审**，重要系统变更前是否得到有关领导的批准，由何人批准，对发生的变更情况是否通知了所有相关人员，以何种方式通知；

c) **应检查是否有变更管理制度，查看其是否覆盖变更前审批、变更过程记录、变更后通报等方面内容，是否包括变更申报、审批程序，是否规定需要申报的变更类型、申报流程、审批部门、批准人等方面内容；**

d) 应检查系统变更方案，查看其是否覆盖变更类型、变更原因、变更过程、变更前评估、**变更失败恢复程序**等方面内容，查看其是否有主管领导的批准签字。

7.2.5.10.3 结果判定

如果7.2.5.10.2中a)～d)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

7.2.5.11 备份与恢复管理

7.2.5.11.1 测评指标

见GB/T 22239—2008中7.2.5.11。

7.2.5.11.2 测评实施

本项要求包括：

a) 应访谈系统运维负责人，询问是否识别出需要定期备份的业务信息、系统数据和软件系统，主要有哪些；

b) **应检查是否有备份与恢复方面的管理制度**，查看其是否明确了备份方式、备份频度、存储介质和保存期等方面内容，是否明确了数据的存放场所、文件命名规则、介质替换频率、数据离站传输方法等方面内容；

c) **应访谈系统管理员、数据库管理员和网络管理员，询问是否定期执行恢复程序，周期多长，系统是否按照恢复程序完成恢复，如有问题，是否针对问题改进恢复程序或调整其他因素；**

d) **应检查备份和恢复记录，查看其是否包含备份内容、备份操作、备份介质存放等内容，记录内容与备份和恢复策略是否一致。**

7.2.5.11.3 结果判定

如果7.2.5.11.2中a)～d)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符

合或部分符合本单元测评指标要求。

7.2.5.12 安全事件处置

7.2.5.12.1 测评指标

见 GB/T 22239—2008 中 7.2.5.12。

7.2.5.12.2 测评实施

本项要求包括：

a) 应访谈系统运维负责人，询问是否告知用户在发现安全弱点和可疑事件时应及时报告；

b) 应检查是否有安全事件报告和处置管理制度，查看其是否明确安全事件的级别，明确不同级别安全事件的报告和处置方式等内容；

c) 应检查是否有安全事件报告和处置管理制度，查看其是否细化了不同安全事件的处理和报告程序，是否明确具体报告方式、报告内容、报告人等方面内容，造成系统中断和造成信息泄密的重大安全事件是否采用了不同于其他的处理程序和报告程序；

d) 应检查安全事件处理记录，查看其是否记录引发安全事件的原因，是否记录事件处理过程，是否与管理规定的处理要求一致等。

7.2.5.12.3 结果判定

如果 7.2.5.12.2 中 a)～d)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

7.2.5.13 应急预案管理

7.2.5.13.1 测评指标

见 GB/T 22239—2008 中 7.2.5.13。

7.2.5.13.2 测评实施

本项要求包括：

a) **应访谈系统运维负责人，询问是否具有应急预案小组，**询问是否制定不同事件的应急预案，**应急预案执行所需资金是否做过预算并能够落实；**

b) 应访谈系统运维负责人，是否对系统相关人员进行应急预案培训，多长时间举办一次，**是否定期对应急预案进行演练，演练周期多长，是否对应急预案定期进行审查；**

c) **应检查是否具有定期审查应急预案的管理规定，查看是否明确应急预案中需要定期审查和根据实际情况更新的内容；**

d) 应检查应急预案框架，查看其内容是否覆盖启动应急预案的条件、应急处理流程、系统恢复流程、事后教育和培训等方面；

e) 应检查是否具有根据应急预案框架制定的不同事件的应急预案，**是否具有应急预案培训记录、演练记录和审查记录。**

7.2.5.13.3 结果判定

如果 7.2.5.13.2 中 a)～e)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

8 第四级信息系统单元测评

8.1 安全技术测评

8.1.1 物理安全

8.1.1.1 物理位置的选择

8.1.1.1.1 测评指标

见 GB/T 22239—2008 中 8.1.1.1。

8.1.1.1.2 测评实施

本项要求包括：

a) 应访谈物理安全负责人，询问机房和办公场地所在建筑物是否具有防震、防风和防雨等能力；
b) 应检查是否有机房和办公场地所在建筑物抗震设防审批文档；
c) 应检查机房和办公场地所在建筑物是否具有防风和防雨等能力；
d) 应检查机房场地是否不在用水区域的垂直下方；
e) 如果机房场地位于建筑物的高层或地下室或用水设备的隔壁，应检查机房是否采取了防水和防潮措施。

8.1.1.1.3 结果判定

如果 8.1.1.1.2 中 a)～e)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

8.1.1.2 物理访问控制

8.1.1.2.1 测评指标

见 GB/T 22239—2008 中 8.1.1.2。

8.1.1.2.2 测评实施

本项要求包括：

a) 应检查机房和**重要区域是否配置了电子门禁系统，每道**电子门禁系统是否都有验收文档或产品安全认证资质；
b) 应检查机房出入口是否有专人值守负责控制、鉴别进入机房的人员，是否有值守记录和**电子门禁记录**；
c) 应检查机房是否不存在专人值守和**电子门禁系统控制**之外的其他开放出入口；
d) 应检查是否有来访人员进入机房的登记记录；
e) 应检查是否有来访人员进入机房的申请、审批记录，查看申请、审批记录是否包括来访人员的访问范围；
f) 应检查来访人员进入机房时是否对其行为进行限制和监控；
g) 应检查机房是否合理划分区域，是否在机房重要区域前设置交付或安装等过渡区域；是否在不同机房间和同一机房不同区域间设置了有效的物理隔离装置；
h) 应检查**每道电子门禁系统**是否都能正常工作(不考虑断电后的工作情况)；检查**每道电子门禁系统**记录，查看是否能够鉴别和记录进入人员的身份；检查是否有**每道电子门禁系统**运行、定

期检查和维护记录。

8.1.1.2.3 结果判定

本项要求包括：

如果 8.1.1.2.2 中 a)～h)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

8.1.1.3 防盗窃和防破坏

8.1.1.3.1 测评指标

见 GB/T 22239—2008 中 8.1.1.3。

8.1.1.3.2 测评实施

本项要求包括：

a) 应检查**设备**是否放置在机房内；
b) 应检查**设备**或设备的主要部件是否固定；
c) 应检查**设备**等或设备的主要部件上是否设置明显的不易除去的标记；
d) 应检查通信线缆铺设是否暗敷或在不易被发现的地方；
e) 应检查机房是否安装防盗报警设施，防盗报警设施是否正常运行，并查看是否有防盗报警设施的运行记录、定期检查和维护记录；
f) 应检查介质是否有分类标识，是否分类存放在介质库或档案室内；
g) 应检查机房是否安装摄像、传感等监控报警系统，监控报警系统是否正常运行，并查看是否有监控报警系统的监控记录、定期检查和维护记录；
h) 应检查是否有机房防盗报警设施和监控报警设施的安全资质材料、安装测试和验收报告。

8.1.1.3.3 结果判定

如果 8.1.1.3.2 中 a)～h)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

8.1.1.4 防雷击

8.1.1.4.1 测评指标

见 GB/T 22239—2008 中 8.1.1.4。

8.1.1.4.2 测评实施

本项要求包括：

a) 应访谈物理安全负责人，询问机房所在建筑物是否设置了避雷装置，是否通过验收或国家有关部门的技术检测；
b) 应访谈物理安全负责人，询问机房是否设置有交流电源地线；
c) 应检查机房所在建筑物的防雷验收文档中是否有设置避雷装置的说明，**是否符合机房设计相关国家标准的要求**；
d) 应检查机房防雷验收文档中是否有设置交流电源地线的说明，**是否符合机房设计相关国家标准的要求**；
e) 应检查机房是否安装防止感应雷的防雷装置，防雷装置是否通过了具有检测资质的防雷检测

部门的测试。

8.1.1.4.3 结果判定

如果8.1.1.4.2中a)～e)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

8.1.1.5 防火

8.1.1.5.1 测评指标

见GB/T 22239—2008中8.1.1.5。

8.1.1.5.2 测评实施

本项要求包括：

a) 应检查机房是否设置了自动检测火情、自动报警、自动灭火的自动消防系统，自动消防系统是否是经消防检测部门检测合格的产品，其有效期是否合格；应检查自动消防系统是否处于正常运行状态，查看是否有运行记录、定期检查和维护记录；

b) 应检查机房设计或验收文档，查看是否说明机房及相关的工作房间和辅助房采用具有耐火等级的建筑材料；

c) 应检查机房重要区域与其他区域之间是否采取隔离防火措施。

8.1.1.5.3 结果判定

如果8.1.1.5.2中a)～c)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

8.1.1.6 防水和防潮

8.1.1.6.1 测评指标

见GB/T 22239—2008中8.1.1.6。

8.1.1.6.2 测评实施

本项要求包括：

a) 应检查机房屋顶或活动地板下是否未安装水管；

b) 应检查穿过机房墙壁或楼板的给水排水管道是否采取防渗漏和防结露等防水保护措施；

c) 应检查机房的窗户、屋顶和墙壁等是否未出现过漏水、渗透和返潮现象，机房的窗户、屋顶和墙壁是否进行过防水防渗处理；

d) 如果机房内安装有空调机和加湿器，应检查是否设置了挡水和排水设施；

e) 如果机房位于湿度较高的地区，应检查机房是否有除湿装置并能够正常运行，是否有防水防潮处理记录和除湿装置运行记录、定期检查和维护记录；

f) 应检查是否设置对水敏感的检测仪表或元件，对机房进行防水检测和报警，查看该仪表或元件是否正常运行，是否有运行记录、定期检查和维护记录。

8.1.1.6.3 结果判定

如果8.1.1.6.2中a)～f)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

8.1.1.7 防静电

8.1.1.7.1 测评指标

见 GB/T 22239—2008 中 8.1.1.7。

8.1.1.7.2 测评实施

本项要求包括：

a) 应检查机房内**所有设备可导电金属外壳、各类金属管道、金属线槽等是否有安全接地或其他静电泄放措施**；

b) 应检查机房是否采用了防静电地板或敷设防静电地面；

c) **应检查机房是否采用了防静电工作台、静电消除剂或静电消除器等防静电措施；应查看是否有使用静电消除剂或静电消除器等的除湿操作记录。**

8.1.1.7.3 结果判定

如果 8.1.1.7.2 中 a)～c)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

8.1.1.8 温湿度控制

8.1.1.8.1 测评指标

见 GB/T 22239—2008 中 8.1.1.8。

8.1.1.8.2 测评实施

本项要求包括：

a) 应检查机房内是否配备了温湿度自动调节设施，温湿度自动调节设施是否能够正常运行，机房温度、相对湿度是否满足电子信息设备的使用要求；

b) 应检查是否有机房的温湿度记录，是否有温湿度自动调节设施的运行记录、定期检查和维护记录。

8.1.1.8.3 结果判定

如果 8.1.1.8.2 中 a)和 b)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

8.1.1.9 电力供应

8.1.1.9.1 测评指标

见 GB/T 22239—2008 中 8.1.1.9。

8.1.1.9.2 测评实施

本项要求包括：

a) 应访谈物理安全负责人，询问是否采用冗余或并行的电力电缆线路为计算机系统供电；

b) 应检查机房的计算机系统供电线路上是否设置了稳压器和过电压防护设备，这些设备是否正常运行，查看供电电压是否正常；

c) 应检查机房计算机系统是否配备了短期备用电源设备，短期备用电源设备是否正常运行；
d) 应检查是否为机房计算机系统建立了备用供电系统，备用供电系统的基本容量是否能够满足主要设备的正常运行；
e) 应检查是否有稳压器、过电压防护设备、短期备用电源设备以及备用供电系统等设备的检查和维护记录，备用供电系统运行记录、定期检查和维护记录。

8.1.1.9.3 结果判定

如果8.1.1.9.2中a)～e)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

8.1.1.10 电磁防护

8.1.1.10.1 测评指标

见GB/T 22239—2008中8.1.1.10。

8.1.1.10.2 测评实施

本项要求包括：

a) **应检查是否有针对机房关键区域的电子屏蔽或屏蔽机房设计或验收文档；**
b) 应检查机房设备外壳是否有安全接地；
c) 应检查机房布线，查看是否做到电源线和通信线缆隔离；
d) **应检查磁介质和处理秘密级信息的设备是否为低辐射设备，磁介质和处理秘密级信息的设备所在区域是否实施了电磁屏蔽；**
e) **对采用了电子屏蔽的机房，应检查在机房有设备运行时是否开启了电子屏蔽装置；检查进入机房的电源线和非光纤通信线是否经过滤波器，光纤通信线是否经过波导管，机房门是否及时关闭；**
f) **对屏蔽机房，应检查是否有定期测试电磁泄漏的报告，且报告中明确指出屏蔽机房电磁屏蔽功能完好。**

8.1.1.10.3 结果判定

如果8.1.1.10.2中a)～f)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

8.1.2 网络安全

8.1.2.1 结构安全

8.1.2.1.1 测评指标

见GB/T 22239—2008中8.1.2.1。

8.1.2.1.2 测评实施

本项要求包括：

a) 应检查网络设计或验收文档，查看是否有满足网络设备业务处理能力需要的设计或描述；
b) 应检查网络设计或验收文档，查看是否有满足接入网络及核心网络的带宽业务高峰期的需要以及不存在带宽瓶颈等方面的设计或描述；

c) 应检查边界和网络设备的路由控制策略，查看是否建立安全的访问路径；
d) 应检查网络拓扑结构图，查看其与当前运行的实际网络系统是否一致；
e) 应检查网络设计或验收文档，查看是否有根据各部门的工作职能、重要性和所涉及信息的重要程度等因素，划分不同的子网或网段，并按照方便管理和控制的原则为各子网和网段分配地址段的设计或描述；
f) 应检查边界和网络设备，查看重要网段是否采取了技术隔离手段与其他网段隔离；
g) 应检查边界和网络设备，查看是否有对带宽进行控制的策略，这些策略是否能够保证在网络发生拥堵的时候优先保护重要业务。

8.1.2.1.3 结果判定

如果8.1.2.1.2中a)～g)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

8.1.2.2 访问控制

8.1.2.2.1 测评指标

见GB/T 22239—2008中8.1.2.2。

8.1.2.2.2 测评实施

本项要求包括：

a) 应检查在网络边界是否部署网络访问控制设备，是否启用访问控制策略，同时访谈安全管理员，询问访问控制策略的设计原则是什么；**询问访问控制策略是否做过调整，以及调整后和调整前的情况如何**；询问是否禁止远程拨号访问网络；
b) **应检查边界网络设备，查看是否采取协议转换或其他相应的控制措施来实现禁止数据带通用协议通过；**
c) **应检查边界网络设备，查看是否能有根据数据的敏感标记允许或拒绝数据通过的功能；**
d) **应检查边界网络设备，查看是否禁用远程拨号访问功能；**
e) **应测试边界网络设备，可通过发送带通用协议的数据，测试访问控制措施是否有效阻断这种连接。**

8.1.2.2.3 结果判定

如果8.1.2.2.2中a)～e)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

8.1.2.3 安全审计

8.1.2.3.1 测评指标

见GB/T 22239—2008中8.1.2.3。

8.1.2.3.2 测评实施

本项要求包括：

a) 应检查边界和网络设备的安全审计策略，查看是否对网络设备运行状况、网络流量、用户行为等进行全面的监测、记录；
b) 应检查边界和网络设备的安全审计记录，查看是否包括：事件的日期和时间、用户、事件类型、

事件成功情况及其他与审计相关的信息；

c) 应检查边界和网络设备，查看其是否为授权用户浏览和分析审计数据提供专门的审计工具，并能根据需要生成审计报表；

d) 应测试边界和主要网络设备，可通过以某个非审计用户登录系统，试图删除、修改或覆盖审计记录，验证安全审计的保护情况与要求是否一致；

e) 应检查边界和网络设备是否定义了审计跟踪极限的阈值，当存储空间被耗尽时，是否能够采取必要的保护措施，例如，报警并导出、丢弃未记录的审计信息、暂停审计或覆盖以前的审计记录等；

f) 应检查是否进行了集中审计，查看时钟是否与时钟服务器保持同步。

8.1.2.3.3 结果判定

如果 8.1.2.3.2 中 a)～f)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

8.1.2.4 边界完整性检查

8.1.2.4.1 测评指标

见 GB/T 22239—2008 中 8.1.2.4。

8.1.2.4.2 测评实施

本项要求包括：

a) 应检查边界完整性检查设备的非法外联和非授权接入策略，查看是否设置了对非法连接到内网和非法连接到外网的行为进行监控并有效的阻断的配置；

b) 应测试边界完整性检查设备，测试是否能够确定出非法外联设备的位置，并对其进行有效阻断；

c) 应测试边界完整性检查设备，测试是否能够对非授权设备私自接入内部网络的行为进行检查，并准确定出位置，对其进行有效阻断。

8.1.2.4.3 结果判定

如果 8.1.2.4.2 中 a)～c)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

8.1.2.5 入侵防范

8.1.2.5.1 测评指标

见 GB/T 22239—2008 中 8.1.2.5。

8.1.2.5.2 测评实施

本项要求包括：

a) 应检查网络入侵防范设备，查看是否能检测以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP 碎片攻击、网络蠕虫攻击等；

b) 应检查网络入侵防范设备的入侵事件记录，查看记录中是否包括入侵的源 IP、攻击的类型、攻击的目的、攻击的时间等；查看是否设置了安全警告方式；查看是否设置了在发生严重入侵事件时自动采取相应动作的配置；

c) 应检查网络入侵防范设备的规则库，查看其规则库是否及时更新；
d) 应测试网络入侵防范设备，验证其检测策略是否有效；
e) 应测试网络入侵防范设备，验证其报警与自动采取动作等策略是否有效。

8.1.2.5.3 结果判定

如果 8.1.2.5.2 中 a)～e)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

8.1.2.6 恶意代码防范

8.1.2.6.1 测评指标

见 GB/T 22239—2008 中 8.1.2.6。

8.1.2.6.2 测评实施

本项要求包括：
a) 应检查在网络边界及核心业务网段处是否有相应的防恶意代码措施；
b) 应检查防恶意代码产品，查看其运行是否正常，恶意代码库是否及时更新。

8.1.2.6.3 结果判定

如果 8.1.2.6.2 中 a)和 b)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

8.1.2.7 网络设备防护

8.1.2.7.1 测评指标

见 GB/T 22239—2008 中 8.1.2.7。

8.1.2.7.2 测评实施

本项要求包括：
a) 应检查边界和主要网络设备的设备防护策略，查看是否配置了对登录用户进行身份鉴别的功能；
b) 应检查边界和主要网络设备的设备防护策略，查看是否对网络设备的登录地址进行了限制；
c) 应检查边界和主要网络设备的账户列表，查看用户标识是否唯一；
d) 应检查是否对同一用户选择两种或两种以上组合的鉴别技术来进行身份鉴别且其中一种是不可伪造的；
e) 应检查边界和主要网络设备的设备防护策略，查看口令设置是否有复杂度和定期修改要求；
f) 应检查边界和主要网络设备的设备防护策略，查看是否配置了鉴别失败处理功能，包括结束会话、限制非法登录次数、登录连接超时自动退出等措施；
g) 应检查边界和网络设备的设备防护策略，查看是否配置了对设备远程管理所产生的鉴别信息进行保护的功能；
h) 应检查边界和网络设备的管理配置，查看是否实现设备特权用户的权限分离；
i) 应对边界和网络设备进行渗透测试，通过使用各种渗透测试技术对网络设备进行渗透测试，验证网络设备防护能力是否符合要求。

8.1.2.7.3 结果判定

如果 8.1.2.7.2 中 a)～i)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

8.1.3 主机安全

8.1.3.1 身份鉴别

8.1.3.1.1 测评指标

见 GB/T 22239—2008 中 8.1.3.1。

8.1.3.1.2 测评实施

本项要求包括：

a) 应检查服务器操作系统和数据库管理系统的身份鉴别策略，查看是否提供了身份鉴别措施；

b) 应检查服务器操作系统和数据库管理系统的身份鉴别策略，查看是否提供了身份鉴别措施，身份鉴别信息是否具有不易被冒用的特点，如对用户登录口令的最小长度、复杂度和更换周期进行了要求和限制；

c) 应检查服务器操作系统和数据库管理系统的身份鉴别策略，查看是否配置了鉴别失败处理功能，并设置了非法登录次数的限制值；查看是否设置网络登录连接超时，并自动退出；

d) **应测试服务器操作系统和数据库管理系统，通过正常登录，查看是否有登录警示信息，并且在警示信息中是否有未授权访问可能导致的后果的描述；**

e) 如果操作系统或数据库采用远程管理方式，查看是否具有防止鉴别信息在网络传输过程中被窃听的措施；

f) 应检查服务器操作系统和数据库管理系统账户列表，查看管理员用户名分配是否唯一；

g) 应检查服务器操作系统和数据库管理系统的身份鉴别策略，查看身份鉴别是否采用两个以上身份鉴别技术的组合来进行身份鉴别，**并且有一种是不可伪造的；**

h) 应渗透测试服务器操作系统和数据库管理系统，可通过使用口令破解工具等，对服务器操作系统进行用户口令强度检测，查看是否能够破解用户口令，破解口令后是否能够登录进入系统；

i) 应渗透测试服务器操作系统和数据库管理系统，测试是否存在绕过认证方式进行系统登录的方法。

8.1.3.1.3 结果判定

如果 8.1.3.1.2 中 a)～g)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

8.1.3.2 安全标记

8.1.3.2.1 测评指标

见 GB/T 22239—2008 中 8.1.3.2。

8.1.3.2.2 测评实施

本项要求包括：

a) **应检查服务器操作系统和数据库管理系统，查看是否能对所有主体和客体设置敏感标记，这些**

敏感标记是否构成多级安全模型的属性库，主体和客体的敏感标记是否以默认方式生成或由安全员建立、维护和管理；

b) **应测试服务器操作系统和数据库管理系统，对主体和客体设置敏感标记，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，而非授权用户不能访问客体。**

8.1.3.2.3 结果判定

如果8.1.3.2.2中a)和b)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

8.1.3.3 访问控制

8.1.3.3.1 测评指标

见GB/T 22239—2008中8.1.3.3。

8.1.3.3.2 测评实施

本项要求包括：

a) 应检查服务器操作系统的访问控制策略，查看是否对重要文件的访问权限进行了限制，对系统不需要的服务、共享路径等进行了禁用或删除；

b) 应检查服务器操作系统和数据库管理系统的访问控制策略，查看特权用户的权限是否进行分离，如可分为系统管理员、安全管理员、安全审计员等；查看是否采用最小授权原则；

c) 应检查数据库管理系统的特权用户和服务器的操作系统的特权用户，查看不同管理员的系统账户权限是否不同，且不应由同一人担任；

d) 应检查服务器操作系统和数据库管理系统的访问控制策略，查看是否已禁用或者限制匿名/默认账户的访问权限，是否重命名系统默认账户、修改这些账户的默认口令；

e) 应检查服务器操作系统和数据库管理系统的访问控制策略，是否删除了系统中多余的、过期的以及共享的账户；

f) 应检查服务器操作系统和数据库管理系统的权限设置情况，查看是否依据安全策略对用户权限进行了限制；

g) **应检查服务器操作系统和数据库管理系统的访问控制策略，查看是否依据安全策略和所有主体和客体设置的敏感标记控制主体对客体的访问；操作系统的访问控制粒度是否达到主体为用户级或进程级，客体为文件级，数据库管理系统访问控制粒度是否达到主体为用户级或进程级，客体为文件、数据库表、记录和字段级。**

8.1.3.3.3 结果判定

如果8.1.3.3.2中a)～g)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

8.1.3.4 可信路径

8.1.3.4.1 测评指标

见GB/T 22239—2008中8.1.3.4。

8.1.3.4.2 测评实施

本项要求包括：

a) 应检查服务器操作系统文档，查看系统提供了哪些可信路径功能；
b) 应检查服务器操作系统，查看文档声称的可信路径功能是否有效；
c) 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；
d) 应检查数据库管理系统，查看文档声称的可信路径功能是否有效。

8.1.3.4.3 结果判定

如果8.1.3.4.2中a)～d)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

8.1.3.5 安全审计

8.1.3.5.1 测评指标

见GB/T 22239—2008中8.1.3.5。

8.1.3.5.2 测评实施

本项要求包括：

a) 应检查服务器操作系统、重要终端操作系统和数据库管理系统的安全审计策略，查看安全审计配置是否包括系统内重要用户行为、系统资源的异常和重要系统命令的使用等重要的安全相关事件；
b) 应检查服务器操作系统、重要终端操作系统和数据库管理系统的安全审计策略，查看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、事件的结果等内容；
c) 应检查服务器操作系统、重要终端操作系统和数据库管理系统的安全审计策略，查看是否通过日志覆盖周期、存储方式、日志文件/空间大小、日志文件操作权限等设置，实现了对审计记录的保护，使其避免受到未预期的删除、修改或覆盖等；
d) 应检查服务器操作系统、重要终端操作系统和数据库管理系统的安全审计策略，查看是否为授权用户提供浏览和分析审计记录的功能，是否可以根据需要自动生成不同格式的审计报表；
e) **应检查服务器操作系统、重要终端操作系统和数据库管理系统的安全审计策略，查看是否实现了集中审计功能，通过集中审计平台将服务器操作系统、重要终端操作系统和数据库管理系统的审计记录进行集中存储、管理、查看和统计分析；**
f) 应测试服务器操作系统、重要终端操作系统和数据库管理系统，可通过非审计员的其他账户试图中断审计进程，验证审计进程是否受到保护。

8.1.3.5.3 结果判定

如果8.1.3.5.2中a)～f)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

8.1.3.6 剩余信息保护

8.1.3.6.1 测评指标

见GB/T 22239—2008中8.1.3.6。

8.1.3.6.2 测评实施

应检查操作系统和数据库管理系统技术开发手册或产品检测报告，查看是否明确用户的鉴别信息

存储空间被释放或再分配给其他用户前的处理方法和过程；是否明确文件、目录和数据库记录等资源所在的存储空间被释放或重新分配给其他用户前的处理方法和过程。

8.1.3.6.3 结果判定

如果 8.1.3.6.2 为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

8.1.3.7 入侵防范

8.1.3.7.1 测评指标

见 GB/T 22239—2008 中 8.1.3.7。

8.1.3.7.2 测评实施

本项要求包括：

a) 应检查入侵防范系统的入侵防范策略，查看是否能够记录对服务器攻击的源 IP、攻击类型、攻击目标、攻击时间等，在发生严重入侵事件时是否提供报警(如声音、短信和 EMAIL 等)；

b) 应检查服务器是否提供对重要程序的完整性进行检测，并在检测到完整性受到破坏后具有恢复的措施的功能；

c) 应检查服务器操作系统中所安装的系统组件和应用程序是否都是必须的；

d) 应检查是否设置了专门的升级服务器实现对服务器操作系统补丁的升级，是否具有操作系统补丁更新策略；

e) 应检查服务器操作系统和数据库管理系统的补丁是否得到了及时更新；

f) 应渗透测试服务器操作系统和数据库管理系统，查看入侵防范系统是否及时正确记录了本次攻击行为，并自动报警。

8.1.3.7.3 结果判定

如果 8.1.3.7.2 中 a)～f)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

8.1.3.8 恶意代码防范

8.1.3.8.1 测评指标

见 GB/T 22239—2008 中 8.1.3.8。

8.1.3.8.2 测评实施

本项要求包括：

a) 应检查服务器的恶意代码防范策略，查看是否安装了实时检测与查杀恶意代码的软件产品，并且及时更新了软件版本和恶意代码库；

b) 应检查主机防恶意代码软件或硬件，查看其厂家名称、产品版本号和恶意代码库名称等，查看其是否与网络防恶意代码软件有不同的恶意代码库；

c) 应检查主机防恶意代码软件是否实现了统一管理。

8.1.3.8.3 结果判定

如果 8.1.3.8.2 中 a)～c)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合

或部分符合本单元测评指标要求。

8.1.3.9 资源控制

8.1.3.9.1 测评指标

见 GB/T 22239—2008 中 8.1.3.9。

8.1.3.9.2 测评实施

本项要求包括：

a) 应检查服务器操作系统和数据库管理系统的资源访问策略，查看是否设定了终端接入方式、网络地址范围等条件限制终端登录；
b) 应检查访问服务器的终端是否都设置了操作超时锁定的配置。
c) 应检查服务器操作系统的资源访问策略，查看是否对 CPU、硬盘、内存和网络等资源的使用情况进行监控；
d) 应检查服务器操作系统和数据库管理系统的资源访问策略，查看是否设置了单个用户或应用对系统资源的最大或最小使用限度；
e) 应检查服务器操作系统和数据库管理系统的资源访问策略，查看是否在服务水平降低到预先规定的阈值时，能检测和报警。

8.1.3.9.3 结果判定

如果 8.1.3.9.2 中 a)～e)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

8.1.4 应用安全

8.1.4.1 身份鉴别

8.1.4.1.1 测评指标

见 GB/T 22239—2008 中 8.1.4.1。

8.1.4.1.2 测评实施

本项要求包括：

a) 应检查应用系统，查看是否提供身份标识和鉴别功能；
b) 应检查应用系统，查看是否采用了两种或两种以上组合的身份鉴别技术来进行身份鉴别，**并且至少有一种是不可伪造的**；
c) 应检查应用系统，查看是否采用了措施保证身份标识具有唯一性，是否对登录用户的口令最小长度、复杂度和更换周期等进行了要求和限制，保证身份鉴别信息不易被冒用；
d) 应检查应用系统，查看是否提供登录失败处理功能，是否根据安全策略设置了登录失败次数等参数；
e) 应测试应用系统，可通过试图以合法和非法用户分别登录系统，验证身份标识和鉴别功能是否有效；
f) 应测试应用系统，可通过多次输入错误的密码，验证登录失败处理功能是否有效；
g) 应渗透测试应用系统，如多次猜测用户口令，验证应用系统身份标识和鉴别功能是否不存在明显的弱点。

8.1.4.1.3 结果判定

如果 8.1.4.1.2 中 a)～f)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

8.1.4.2 安全标记

8.1.4.2.1 测评指标

见 GB/T 22239—2008 中 8.1.4.2。

8.1.4.2.2 测评实施

本项要求包括：

a) **应检查设计、验收文档或源代码，查看文档中是否有应用系统采用敏感标记的说明；**

b) **应检查应用系统，查看是否能对所有主体和客体设置敏感标记，这些敏感标记是否构成多级安全模型的属性库，主体和客体的敏感标记是否以默认方式生成或由安全员建立、维护和管理；**

c) **应测试应用系统，对主体和客体设置敏感标记，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，而非授权用户不能访问客体。**

8.1.4.2.3 结果判定

如果 8.1.4.2.2 中 a)～c)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

8.1.4.3 访问控制

8.1.4.3.1 测评指标

见 GB/T 22239—2008 中 8.1.4.3。

8.1.4.3.2 测评实施

本项要求包括：

a) 应检查应用系统，查看是否依据安全策略控制用户对文件、数据库表等客体的访问；

b) 应检查应用系统，查看其访问控制的覆盖范围是否包括与信息安全直接相关的主体、客体及它们之间的操作；

c) 应检查应用系统，查看其是否有由授权用户设置其他用户访问系统功能和用户数据的权限的功能；

d) **应检查应用系统的用户列表，查看其是否不存在默认账户，如果有是否禁止了默认账户的访问；**

e) 应检查应用系统的用户角色或权限的分配情况，查看是否仅授予不同账户为完成各自承担任务所需的最小权限，特权用户的权限是否分离，权限之间是否相互制约，如系统管理员不能进行审计操作、审计员不能进行系统管理操作等；

f) **应检查应用系统，查看其是否具有通过比较安全标签来确定是授予还是拒绝主体对客体的访问的功能；**

g) 应测试应用系统，可通过以不同权限的用户登录系统，查看其拥有的权限是否与系统赋予的权限一致，验证应用系统访问控制功能是否有效；

h) 应测试应用系统，可通过以默认用户登录系统并进行一些操作，查看系统是否禁止了默认账户

的访问；

i) 应渗透测试应用系统，进行试图绕过访问控制的操作，验证应用系统的访问控制功能是否不存在明显的弱点。

8.1.4.3.3 结果判定

如果8.1.4.3.2中a)～h)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

8.1.4.4 可信路径

8.1.4.4.1 测评指标

见GB/T 22239—2008中8.1.4.4。

8.1.4.4.2 测评实施

本项要求包括：

a) **应检查设计或验收文档，查看文档中是否有在系统对用户进行身份鉴别和用户对系统进行访问时系统与用户之间能够建立一条安全的信息传输路径的描述；**

b) **应检查应用系统，可通过查看系统对用户进行身份鉴别和用户对系统进行访问的路径，分析在系统对用户进行身份鉴别和用户对系统进行访问时系统能否在系统与用户之间建立一条安全的信息传输路径。**

8.1.4.4.3 结果判定

如果8.1.4.4.2中a)和b)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

8.1.4.5 安全审计

8.1.4.5.1 测评指标

见GB/T 22239—2008中8.1.4.5。

8.1.4.5.2 测评实施

本项要求包括：

a) 应检查关键应用系统，查看审计范围是否覆盖到每个用户，审计策略是否覆盖系统内重要的安全相关事件，例如，用户标识与鉴别、访问控制的所有操作记录、重要用户行为、系统资源的异常使用、重要系统命令的使用等；

b) 应检查应用系统的审计记录，查看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、事件的结果等内容；

c) 应检查应用系统，查看是否为授权用户浏览和分析审计数据提供专门的审计分析功能，并能根据需要生成审计报表；

d) **应检查应用系统，查看是否有集中审计接口，并根据信息系统的统一安全策略实现集中审计；**

e) 应测试主要应用系统，在应用系统上试图产生一些重要的安全相关事件(如用户登录、修改用户权限等)，查看应用系统是否对其进行了审计，验证应用系统安全审计的覆盖情况是否覆盖到每个用户；如果进行了审计则查看审计记录内容是否包含事件的日期、时间、发起者信息、类型、描述和结果等；

f) 应测试应用系统，试图非授权终止审计进程或审计功能，非授权删除、修改或覆盖审计记录，查看安全审计进程和记录的保护情况。

8.1.4.5.3 结果判定

如果8.1.4.5.2中a)～f)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

8.1.4.6 剩余信息保护

8.1.4.6.1 测评指标

见GB/T 22239—2008中8.1.4.6。

8.1.4.6.2 测评实施

本项要求包括：

a) 应检查设计、验收文档或源代码，查看其是否有关于系统在释放或再分配鉴别信息所在存储空间给其他用户前如何将其进行完全清除（无论这些信息是存放在硬盘上还是在内存中）的描述；

b) 应检查设计、验收文档或源代码，查看其是否有关于释放或重新分配系统内文件、目录和数据库记录等资源所在存储空间给其他用户前进行完全清除的描述；

c) 应测试主要应用系统，用某用户登录系统并进行操作后，在该用户退出后用另一用户登录，试图操作（读取、修改或删除等）其他用户产生的文件、目录和数据库记录等资源，查看操作是否不成功，验证系统提供的剩余信息保护功能是否正确（确保系统内的文件、目录和数据库记录等资源所在的存储空间，被释放或重新分配给其他用户前得到完全清除）。

8.1.4.6.3 结果判定

如果8.1.4.6.2中a)～c)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

8.1.4.7 通信完整性

8.1.4.7.1 测评指标

见GB/T 22239—2008中8.1.4.7。

8.1.4.7.2 测评实施

本项要求包括：

a) 应检查设计、验收文档或源代码，查看是否有关于保护通信完整性的说明，如果有则查看是否有根据校验码判断对方数据有效性，以及散列（Hash）密码计算报文校验码的描述；

b) 应测试应用系统，可通过获取通信双方的数据包，查看通信报文是否含有的校验码。

8.1.4.7.3 结果判定

如果8.1.4.7.2中a)和b)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

8.1.4.8 通信保密性

8.1.4.8.1 测评指标

见 GB/T 22239—2008 中 8.1.4.8。

8.1.4.8.2 测评实施

本项要求包括：

a) **应检查应用系统，查看其是否基于硬件化的设备，产生密钥，进行加解密运算；**

b) **应检查相关证明材料（证书），查看主要应用系统采用的密码算法是否符合国家有关部门的要求；**

c) 应测试应用系统，通过获取通信双方数据包并查看数据包的内容，查看系统是否能在通信双方建立连接之前，利用密码技术进行会话初始化验证；在通信过程中，是否对整个报文或会话过程进行加密。

8.1.4.8.3 结果判定

本项要求包括：

a) 如果 8.1.4.8.2 b)缺少相关文档材料，则为否定；

b) 如果 8.1.4.8.2 中 a)～c)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

8.1.4.9 抗抵赖

8.1.4.9.1 测评指标

见 GB/T 22239—2008 中 8.1.4.9。

8.1.4.9.2 测评实施

本项要求包括：

a) 如果业务应用有明确的抗抵赖需求，则应检查应用系统是否提供在请求的情况下为数据原发者和接收者提供数据原发证据的功能；是否提供在请求的情况下为数据原发者和接收者提供数据接收证据的功能；

b) 如果业务应用有明确的抗抵赖需求，则应测试应用系统，通过双方进行通信，查看系统是否提供在请求的情况下为数据原发者和接收者提供数据原发证据的功能；系统是否提供在请求的情况下为数据原发者和接收者提供数据接收证据的功能。

8.1.4.9.3 结果判定

如果 8.1.4.9.2 中 a)和 b)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

8.1.4.10 软件容错

8.1.4.10.1 测评指标

见 GB/T 22239—2008 中 8.1.4.10。

8.1.4.10.2 测评实施

本项要求包括：

a) 应检查设计或验收文档，查看应用系统有对人机接口输入或通信接口输入的数据进行有效性检验功能的说明；

b) 应测试应用系统，查看应用系统是否能明确拒绝不符合格式要求数据；

c) 应测试应用系统，验证是否提供自动保护功能，当故障发生时自动保护当前所有状态，保证系统能够进行恢复；

d) **应测试应用系统，验证是否具有自动恢复能力，当故障发生时，是否能立即启动新的进程，恢复原来的工作状态。**

8.1.4.10.3 结果判定

如果8.1.4.10.2中a)～d)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

8.1.4.11 资源控制

8.1.4.11.1 测评指标

见GB/T 22239—2008中8.1.4.11。

8.1.4.11.2 测评实施

本项要求包括：

a) 应检查应用系统的配置参数，查看是否提供对最大并发会话连接数进行限制；

b) 应检查应用系统，查看是否对一个访问账户或一个请求进程占用的资源分配最大限额和最小限额；

c) 应检查应用系统，查看是否有服务水平最小值的设定，当系统的服务水平降低到预先设定的最小值时，系统报警，**并合理自动调整资源分配**；

d) 应检查应用系统，查看是否能根据安全策略设定主体的服务优先级，根据优先级分配系统资源；

e) 应测试应用系统，当应用系统的通信双方中的一方在一段时间内未作任何响应，查看另一方是否能够自动结束会话；

f) 应测试应用系统，可通过对系统进行超过规定的单个账户的多重并发会话数进行连接，验证系统是否能够正确地限制单个账户的多重并发会话数；

g) 应测试应用系统，可试图使服务水平降低到预先规定的最小值，验证系统是否能够正确检测并报警。

8.1.4.11.3 结果判定

如果8.1.4.11.2中a)～g)肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

8.1.5 数据安全及备份恢复

8.1.5.1 数据完整性

8.1.5.1.1 测评指标

见GB/T 22239—2008中8.1.5.1。

8.1.5.1.2 测评实施

本项要求包括：

a) 如果网络设备、主机操作系统和数据库管理系统能够进行远程管理，则应查看其能否检测系统管理数据（如配置文件）、鉴别信息在传输过程中完整性受到了破坏，并在检测到完整性错误时采取必要的恢复措施；

b) 应检查应用系统的设计、验收文档或源代码，查看是否有关于能检测系统管理数据、鉴别信息和重要业务数据传输过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施的描述；

c) 应检查网络设备、操作系统和数据库管理系统，查看是否配备检测系统管理数据（如配置文件）和鉴别信息在存储过程中完整性受到破坏的功能，并在检测到完整性错误时是否能采取必要的恢复措施；

d) 应检查应用系统，查看是否配备检测系统管理数据、鉴别信息和业务数据在存储过程中完整性受到破坏的功能，并在检测到完整性错误时是否能采取必要的恢复措施；

e) **应检查网络设备、操作系统、数据库管理系统和应用系统中是否为重要通信提供专用通信协议或安全通信协议服务，避免来自基于通用通信协议的攻击破坏数据完整性。**

8.1.5.1.3 结果判定

如果8.1.5.1.2中a)～e)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

8.1.5.2 数据保密性

8.1.5.2.1 测评指标

见GB/T 22239—2008中8.1.5.2。

8.1.5.2.2 测评实施

本项要求包括：

a) 应检查网络设备、操作系统和数据库管理系统，查看其管理数据和鉴别信息是否采用加密或其他有效措施实现了传输和存储保密性；

b) 应检查应用系统，查看其管理数据、鉴别信息和重要业务数据是否采用加密或其他有效措施实现传输和存储保密性；

c) **应检查网络设备、操作系统、数据库管理系统和应用系统中是否为重要通信提供专用通信协议或安全通信协议服务，避免来自基于通用通信协议的攻击破坏数据保密性；**

d) 应测试操作系统、网络设备操作系统、数据库管理系统和应用系统，可通过用嗅探工具获取系统传输数据包，查看是否为密文。

8.1.5.2.3 结果判定

如果8.1.5.2.2中a)～d)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

8.1.5.3 备份和恢复

8.1.5.3.1 测评指标

见GB/T 22239—2008中8.1.5.3。

8.1.5.3.2 测评实施

本项要求包括：

a) 应检查是否对网络设备、主机操作系统、数据库管理系统和应用系统的重要信息进行了备份，备份方式(如是否为完全数据备份)、频率和介质存放方式是否达到相关标准的要求，是否定期对备份数据进行恢复测试；

b) **应检查是否建立了异地灾难备份中心，能否对业务应用进行实时无缝切换；**

c) **应检查能否对网络设备、主机操作系统、数据库管理系统和应用系统的重要信息进行实时异地备份，实时将数据备份到灾难备份中心；**

d) 应检查网络设备、主要主机操作系统、主要数据库管理系统和主要应用系统是否对重要信息进行了异地数据备份；

e) 应检查网络拓扑结构是否不存在关键节点的单点故障；

f) 应检查网络设备、通信线路和数据处理系统(如包含数据库管理系统在内的数据库服务器)是否提供硬件冗余；

g) **如果条件允许，应验证能否对业务应用进行实时无缝切换。**

8.1.5.3.3 结果判定

如果8.1.5.3.2中a)～g)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

8.2 安全管理测评

8.2.1 安全管理制度

8.2.1.1 管理制度

8.2.1.1.1 测评指标

见GB/T 22239—2008中8.2.1.1。

8.2.1.1.2 测评实施

本项要求包括：

a) 应访谈安全主管，询问机构是否形成全面的信息安全管理制度体系，制度体系是否由总体方针、安全策略、管理制度、操作规程等构成；

b) 应检查信息安全工作的总体方针和安全策略文件，查看文件是否明确机构安全工作的总体目标、范围、原则和安全框架等；

c) 应检查各项安全管理制度，查看是否覆盖物理、网络、主机系统、数据、应用、建设和运维等层面的管理内容；

d) 应检查是否具有日常管理操作的操作规程(如系统维护手册和用户操作规程等)。

8.2.1.1.3 结果判定

如果8.2.1.1.2中a)～d)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

8.2.1.2 制定和发布

8.2.1.2.1 测评指标

见 GB/T 22239—2008 中 8.2.1.2。

8.2.1.2.2 测评实施

本项要求包括：

a) 应访谈安全主管，询问是否由专门的部门或人员负责制定安全管理制度；

b) 应访谈安全主管，询问安全管理制度是否能够发布到相关人员手中，是否对制定的安全管理制度进行论证和审定，是否按照统一的格式标准或要求制定，**对有密级的管理制度是否采取相应措施有效管理**；

c) 应检查制度制定和发布要求管理文档，查看文档是否说明安全管理制度的制定和发布程序、格式要求、版本编号和**密级标注方法**等相关内容；

d) 应检查管理制度评审记录，查看是否有相关人员的评审意见；

e) 应检查各项安全管理制度文档，查看文档是否是正式发布的文档，是否注明适用和发布范围，是否有版本标识，**是否有密级标注**，是否有管理层的签字或单位盖章；查看各项制度文档格式是否统一；

f) 应检查安全管理制度的收发登记记录，查看是否通过正式、有效的方式收发（如正式发文、领导签署和单位盖章等），是否注明发布范围。

8.2.1.2.3 结果判定

如果 8.2.1.2.2 中 a)～f)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

8.2.1.3 评审和修订

8.2.1.3.1 测评指标

见 GB/T 22239—2008 中 8.2.1.3。

8.2.1.3.2 测评实施

本项要求包括：

a) 应访谈安全主管，询问是否由信息安全领导小组负责定期对安全管理制度体系的合理性和适用性进行审定，**是否有专门部门或人员负责制度的日常维护**；

b) **应访谈安全主管，询问评审和修订有密级的安全管理制度时对参加评审和修订的人员是否考虑到相应保密要求**；

c) **应检查是否具有需要定期修订的安全管理制度列表，查看列表是否注明修订周期**；

d) 应检查是否具有安全管理制度体系的评审记录，**查看记录的日期间隔与评审周期是否一致**，是否记录了相关人员的评审意见；

e) 应检查是否具有安全管理制度的检查或评审记录，**查看记录的日期间隔与评审周期是否一致**；如果对制度做过修订，检查是否有修订版本的安全管理制度。

8.2.1.3.3 结果判定

如果 8.2.1.3.2 中 a)～e)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合

或部分符合本单元测评指标要求。

8.2.2 安全管理机构

8.2.2.1 岗位设置

8.2.2.1.1 测评指标

见 GB/T 22239—2008 中 8.2.2.1。

8.2.2.1.2 测评实施

本项要求包括：

a) 应访谈安全主管，询问是否设立指导和管理信息安全工作的委员会或领导小组，其最高领导是否由单位主管领导委任或授权的人员担任；

b) 应访谈安全主管，询问是否设立专职的安全管理机构(即信息安全管理工作的职能部门)，是否明确各部门的职责分工；

c) 应访谈安全主管，询问信息系统是否设置了系统管理员、网络管理员和安全管理员等岗位，各个岗位的职责分工是否明确；是否设立安全管理各个方面的负责人；

d) **应访谈安全主管、安全管理各个方面的负责人、系统管理员、网络管理员和安全管理员，询问其是否明确其岗位职责；**

e) 应检查部门、岗位职责文件，查看文件是否明确安全管理机构的职责，是否明确机构内各部门的职责和分工，部门职责是否涵盖物理、网络和系统安全等各个方面；查看文件是否明确设置安全主管、安全管理各个方面的负责人、系统管理员、网络管理员、安全管理员等各个岗位职责；查看文件是否明确各个岗位人员应具有的技能要求；

f) 应检查是否具有信息安全管理委员会或领导小组成立的正式文件；

g) 应检查信息安全管理委员会或领导小组职责文件，查看是否明确委员会或领导小组职责和其最高领导岗位的职责。

8.2.2.1.3 结果判定

如果 8.2.2.1.2 中 a)～g)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

8.2.2.2 人员配备

8.2.2.2.1 测评指标

见 GB/T 22239—2008 中 8.2.2.2。

8.2.2.2.2 测评实施

本项要求包括：

a) 应访谈安全主管，询问各个安全管理岗位是否配备了一定数量的人员，对关键事务岗位是否配备多人；

b) 应检查人员配备要求管理文档，查看是否明确应配备系统管理员、网络管理员、安全管理员等重要岗位人员并明确应配备专职的安全管理员；查看是否明确关键事务的管理人员应配备2人或2人以上共同管理；

c) 应检查安全管理各岗位人员信息表，查看其是否明确系统管理员、网络管理员和安全管理员等

重要岗位人员的信息，安全管理员是否是专职人员。

8.2.2.2.3 结果判定

如果8.2.2.2.2中a)～c)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

8.2.2.3 授权和审批

8.2.2.3.1 测评指标

见GB/T 22239—2008中8.2.2.3。

8.2.2.3.2 测评实施

本项要求包括：

a) 应访谈安全主管，询问其是否规定对信息系统中的关键活动进行审批，审批活动是否得到授权；是否定期审查、更新审批项目；

b) 应检查审批管理制度文档，查看文档是否明确审批事项、需逐级审批的事项、审批部门、批准人等，是否明确系统变更、重要操作、物理访问和系统接入等事项的审批流程；是否明确需定期审查、更新审批的项目、审批部门、批准人和审查周期等；

c) 应检查经逐级审批的文档，查看是否具有各级批准人的签字和审批部门的盖章；

d) 应检查关键活动的审批过程记录，查看记录的审批程序与文件要求是否一致。

8.2.2.3.3 结果判定

如果8.2.2.3.2中a)～d)均为肯定，则该测评指标符合要求，否则，信息系统不符合或部分符合本单元测评指标要求。

8.2.2.4 沟通和合作

8.2.2.4.1 测评指标

见GB/T 22239—2008中8.2.2.4。

8.2.2.4.2 测评实施

本项要求包括：

a) 应访谈安全主管，询问是否与外单位(公安机关、电信公司、兄弟单位、供应商、业界专家、专业的安全公司、安全组织等)建立沟通、合作机制；是否与组织机构内其他部门之间及内部各部门管理人员之间建立沟通、合作机制，是否定期或不定期召开协调会议；

b) 应访谈安全主管，询问是否召开过部门间协调会议，组织其他部门人员共同协助处理信息系统安全有关问题，安全管理机构内部是否召开过安全工作会议以部署安全工作的实施；信息安全领导小组或者管理委员会是否定期召开例会；

c) 应访谈安全主管，询问是否聘请信息安全专家作为常年的安全顾问，指导信息安全建设，参与安全规划和安全评审等；

d) 应检查组织内部机构之间以及信息安全职能部门内部的安全工作会议文件或会议记录，查看是否有会议内容、会议时间、参加人员和会议结果等的描述；

e) 应检查信息安全领导小组或者管理委员会定期例会会议文件或会议记录，查看是否有会议内容、会议时间、参加人员、会议结果等的描述；

f) 应检查外联单位联系列表，查看外联单位是否包含公安机关、电信公司、兄弟单位、供应商、业界专家、专业的安全公司和安全组织等，是否说明外联单位的名称、合作内容、联系人和联系方式等内容；

g) 应检查是否具有安全顾问名单或者聘请安全顾问的证明文件，查看是否有安全顾问指导信息安全建设、参与安全规划和安全评审的相关文档或记录。

8.2.2.4.3 结果判定

如果8.2.2.4.2中a)～g)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

8.2.2.5 审核和检查

8.2.2.5.1 测评指标

见GB/T 22239—2008中8.2.2.5。

8.2.2.5.2 测评实施

本项要求包括：

a) 应访谈安全主管，询问是否组织人员定期对信息系统安全技术措施和安全管理制度落实情况进行全面安全检查；

b) 应访谈安全管理员，询问是否定期检查系统日常运行、系统漏洞和数据备份等情况，是否对检查结果进行通报；

c) 应检查安全检查管理制度文档，查看文档是否规定定期进行全面安全检查，是否规定检查内容、检查程序和检查周期等，检查内容是否包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等；

d) 应检查全面安全检查报告，查看**报告日期间隔与检查周期是否一致**，报告中是否有检查内容、检查人员、检查数据汇总表、检查结果等的描述，检查内容是否包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等；

e) 应检查安全管理员定期实施安全检查的报告，查看**报告日期间隔与检查周期是否一致**，检查内容是否包括系统日常运行、系统漏洞和数据备份等情况；

f) 应检查是否具有执行安全检查时的安全检查表、安全检查记录和结果通告记录，查看**安全检查记录中记录的检查程序与制度要求是否一致**。

8.2.2.5.3 结果判定

如果8.2.2.5.2中a)～f)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

8.2.3 人员安全管理

8.2.3.1 人员录用

8.2.3.1.1 测评指标

见GB/T 22239—2008中8.2.3.1。

8.2.3.1.2 测评实施

本项要求包括：

a) 应访谈人事负责人，询问是否由专门的部门或人员负责人员的录用工作；
b) 应访谈人事负责人，询问在人员录用时是否对被录用人的身份、背景、专业资格和资质进行审查，对技术人员的技术技能进行考核；
c) 应访谈人事负责人，询问是否与被录用人员签署保密协议；
d) 应访谈人事负责人，询问对从事关键岗位的人员是否从内部人员中选拔，是否要求其签署岗位安全协议；
e) 应检查人员录用管理文档，查看是否说明录用人员应具备的条件(如学历、学位要求，技术人员应具备的专业技术水平，管理人员应具备的安全管理知识等)；
f) 应检查是否具有人员录用时对录用人身份、背景、专业资格和资质等进行审查的相关文档或记录，查看是否记录审查内容和审查结果等；
g) 应检查人员录用时的技能考核文档或记录，查看是否记录考核内容和考核结果等；
h) 应检查保密协议，查看是否有保密范围、保密责任、违约责任、协议的有效期限和责任人的签字等内容；
i) 应检查岗位安全协议，查看是否有岗位安全责任定义、协议的有效期限和责任人签字等内容。

8.2.3.1.3 结果判定

如果8.2.3.1.2中a)～i)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

8.2.3.2 人员离岗

8.2.3.2.1 测评指标

见GB/T 22239—2008中8.2.3.2。

8.2.3.2.2 测评实施

本项要求包括：

a) 应访谈安全主管，询问对即将离岗人员是否及时终止离岗人员的所有访问权限，是否取回各种身份证件、钥匙、徽章以及机构提供的软硬件设备等；
b) 应访谈人事负责人，询问人员离岗是否遵循严格的调离手续，是否要求人员调离时须承诺相关保密义务后方可离开；
c) 应检查人员离岗的管理制度文档，查看是否说明人员离岗要求、人员调离手续等相关内容；
d) 应检查是否具有离岗人员交还身份证件、设备等的登记记录；
e) 应检查是否具有按照离职程序办理调离手续的记录，查看调离手续与文件规定是否一致；
f) 应检查保密承诺文档，查看是否有调离人员的签字。

8.2.3.2.3 结果判定

如果8.2.3.2.2中a)～f)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

8.2.3.3 人员考核

8.2.3.3.1 测评指标

见GB/T 22239—2008中8.2.3.3。

8.2.3.3.2 测评实施

本项要求包括：

a) 应访谈安全主管，询问是否定期对各个岗位人员进行安全技能及安全知识的考核，是否对关键岗位人员定期进行安全审查和技能考核；

b) **应访谈安全主管，询问是否对安全保密制度执行情况进行检查或考核；**

c) **应检查保密制度文档，查看是否包括保密内容、保密责任和义务等内容；**

d) 应检查考核记录，查看记录的考核人员是否包括各个岗位的人员，考核内容是否包含**保密知识**、安全知识、安全技能等；**查看记录日期与考核周期是否一致；**

e) 应检查是否具有对关键岗位人员的安全审查记录。

8.2.3.3.3 结果判定

如果 8.2.3.3.2 中 a)～e)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

8.2.3.4 安全意识教育和培训

8.2.3.4.1 测评指标

见 GB/T 22239—2008 中 8.2.3.4。

8.2.3.4.2 测评实施

本项要求包括：

a) 应访谈安全主管，询问是否制定培训计划并按计划对各个岗位人员进行安全教育和培训；是否对违反安全策略和规定的人员进行惩戒；

b) **应访谈安全管理员、系统管理员、网络管理员，考查其是否了解其工作相关的信息安全基础知识、安全责任和惩戒措施等；**

c) 应检查安全责任和惩戒措施管理文档，查看是否包含具体的安全责任和惩戒措施；

d) 应检查信息安全教育及技能培训和考核管理文档，查看是否明确培训周期、培训方式、培训内容和考核方式等相关内容；

e) 应检查安全教育和培训计划文档，查看是否具有不同岗位的培训计划；查看计划是否明确了培训方式、培训对象、培训内容、培训时间和地点等，培训内容是否包含信息安全基础知识、岗位操作规程等；

f) 应检查安全教育和培训记录，查看记录是否有培训人员、培训内容、培训结果等的描述；**查看记录与培训计划是否一致。**

8.2.3.4.3 结果判定

如果 8.2.3.4.2 中 a)～f)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

8.2.3.5 外部人员访问管理

8.2.3.5.1 测评指标

见 GB/T 22239—2008 中 8.2.3.5。

8.2.3.5.2 测评实施

本项要求包括：

a) 应访谈安全主管，询问外部人员访问重要区域（如访问机房、重要服务器或设备区等）是否需经有关部门或负责人书面批准，是否由专人全程陪同或监督，是否进行记录并备案管理；

b) 应检查外部人员访问管理文档，查看是否明确允许外部人员访问的范围（区域、系统、设备、信息等内容，**对哪些关键区域不允许外部人员访问**），外部人员进入的条件（对哪些重要区域的访问须提出书面申请批准后方可进入），外部人员进入的访问控制措施（由专人全程陪同或监督等）等；

c) 应检查外部人员访问重要区域的书面申请文档，是否具有批准人允许访问的批准签字等；

d) 应检查外部人员访问重要区域的登记记录，查看是否记录了外部人员访问重要区域的进入时间、离开时间、访问区域及陪同人等信息。

8.2.3.5.3 结果判定

如果8.2.3.5.2中a)～d)均为肯定，则该测评指标符合要求，否则，信息系统不符合或部分符合本单元测评指标要求。

8.2.4 系统建设管理

8.2.4.1 系统定级

8.2.4.1.1 测评指标

见GB/T 22239—2008中8.2.4.1。

8.2.4.1.2 测评实施

本项要求包括：

a) 应访谈系统建设负责人，询问是否参照定级指南确定信息系统安全保护等级，是否组织相关部门和有关安全技术专家对定级结果进行论证和审定；

b) 应检查系统定级文档，查看文档是否明确信息系统的边界和信息系统的安全保护等级，是否说明定级的方法和理由，是否有相关部门或主管领导的盖章或签名；

c) 应检查定级结果的论证评审会议文档，查看是否有相关部门和有关安全技术专家对定级结果的论证意见。

8.2.4.1.3 结果判定

如果8.2.4.1.2中a)～c)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

8.2.4.2 安全方案设计

8.2.4.2.1 测评指标

见GB/T 22239—2008中8.2.4.2。

8.2.4.2.2 测评实施

本项要求包括：

a) 应访谈系统建设负责人，询问是否授权专门的部门对信息系统的安全建设进行总体规划，由何部门负责；
b) 应访谈系统建设负责人，询问是否根据信息系统的等级划分情况统一考虑总体安全策略、安全技术框架、安全管理策略、总体建设规划和详细设计方案等；
c) 应访谈系统建设负责人，询问是否对安全建设的配套文件进行论证和审定，是否根据等级测评、安全评估的结果定期调整和修订安全建设的配套文件；
d) 应检查是否有系统安全建设的工作计划，查看文件是否明确了系统的近期安全建设计划和远期安全建设计划；
e) 应检查是否有系统总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等配套文件，查看各个文件是否有机构管理层的批准；
f) 应检查配套文件的论证评审记录或文档，查看是否有相关部门和有关安全技术专家对总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件的论证意见；
g) 应检查是否具有总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件的维护记录或修订版本。

8.2.4.2.3 结果判定

如果 8.2.4.2.2 中 a)～g)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

8.2.4.3 产品采购和使用

8.2.4.3.1 测评指标

见 GB/T 22239—2008 中 8.2.4.3。

8.2.4.3.2 测评实施

本项要求包括：

a) 应访谈系统建设负责人，询问是否有专门的部门负责产品的采购，由何部门负责；
b) 应访谈系统建设负责人，询问系统是否采用了密码产品，密码产品的采购和使用是否符合国家密码主管部门的要求；
c) 应访谈系统建设负责人，询问系统使用的有关信息安全产品是否符合国家的有关规定，如安全产品获得了销售许可证等。
d) 应访谈系统建设负责人，询问采购产品前是否预先对产品进行选型测试确定产品的候选范围，是否有产品采购清单指导产品采购，是否定期审定和更新候选产品采购清单，审定周期多长；
e) **应访谈系统建设负责人，询问是否对重要部位的产品委托专业测评单位进行专项测试，是否有专项测试报告；**
f) 应抽样检查安全产品和密码产品的相关凭证，如销售许可等，查看是否使用了符合国家有关规定产品；
g) 应检查是否具有产品选型测试结果文档、候选产品采购清单及审定或更新的记录，**是否有重要部位的产品的专项测试报告。**

8.2.4.3.3 结果判定

如果 8.2.4.3.2 中 a)～g)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合

或部分符合本单元测评指标要求。

8.2.4.4 自行软件开发

8.2.4.4.1 测评指标

见 GB/T 22239—2008 中 8.2.4.4。

8.2.4.4.2 测评实施

本项要求包括：

a) 应访谈系统建设负责人，询问是否进行自主开发软件，是否对程序资源库的修改、更新、发布进行授权和批准，授权部门是何部门，批准人是何人，是否要求开发人员不能做测试人员（即二者分离），自主开发软件是否在独立的模拟环境中完成编码和调试，如相对独立的网络区域；

b) 应访谈系统建设负责人，询问软件设计相关文档是否由专人负责保管，负责人是何人，如何控制使用，测试数据和测试结果是否受到控制；

c) **应访谈系统建设负责人，询问开发人员有哪些人，是否是专职人员，询问对开发人员的开发活动采取哪些控制措施，是否有专门的监控、审查措施；**

d) 应访谈软件开发人员，询问其是否了解软件开发管理制度，是否了解代码编写安全规范，是否按照代码编写安全规范进行软件开发；

e) 应检查软件开发管理制度，查看文件是否明确软件设计、开发、测试、验收过程的控制方法和人员行为准则，是否明确哪些开发活动应经过授权、审批；

f) 应检查代码编写安全规范，查看规范中是否明确代码编写规则，应抽样部分源代码，检查是否按照代码编写安全规范开发；

g) 应检查对程序资源库的修改、更新、发布进行授权和审批的文档或记录，查看是否有批准人的签字；

h) 应检查是否具有软件开发相关文档（源代码、测试数据、测试结果等）的使用控制记录；

i) 应检查是否具有软件使用指南或操作手册等；

j) 应检查网络拓扑图和实际开发环境，查看是否实际运行环境和开发环境有效隔离；

k) **应检查是否具有对开发人员的审查记录，查看审查记录是否记录审查结果等。**

8.2.4.4.3 结果判定

如果 8.2.4.4.2 中 a)～k)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

8.2.4.5 外包软件开发

8.2.4.5.1 测评指标

见 GB/T 22239—2008 中 8.2.4.5。

8.2.4.5.2 测评实施

本项要求包括：

a) 应访谈系统建设负责人，询问软件交付前是否依据开发要求的技术指标对软件功能和性能等进行验收测试，软件安装之前是否检测软件中的恶意代码；

b) 应访谈系统建设负责人，是否要求开发单位提供源代码，是否根据源代码对软件中可能存在的后门和隐蔽信道进行审查；

c) 应检查是否具有软件开发的相关文档，如需求分析说明书、软件设计说明书等，是否具有软件操作手册或使用指南；

d) 应检查部分软件源代码，查看是否具有源代码，应检查软件源代码审查记录，查看是否包括对可能存在后门和**隐蔽信道**的审查结果。

8.2.4.5.3 结果判定

如果8.2.4.5.2中a)～d)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

8.2.4.6 工程实施

8.2.4.6.1 测评指标

见GB/T 22239—2008中8.2.4.6。

8.2.4.6.2 测评实施

本项要求包括：

a) 应访谈系统建设负责人，询问是否指定专门部门或人员对工程实施过程进行进度和质量控制，由何部门/何人负责；

b) 应访谈系统建设负责人，询问是否要求工程实施单位提供其能够实施安全工程的资质证明和能力保证；

c) **应访谈系统建设负责人，询问是否由第三方工程监理单位对工程实施过程进行进度和质量控制；**

d) 应检查系统建设方面的管理制度，查看其是否包括工程实施过程的控制方法、实施参与人员的行为准则等方面内容。

e) 应检查工程实施方案，查看其是否包括工程时间限制、进度控制和质量控制等方面内容，是否按照工程实施方面的管理制度进行各类控制、产生阶段性文档等；

f) **应检查是否具有第三方工程监理单位出具的工程监理报告。**

8.2.4.6.3 结果判定

如果8.2.4.6.2中a)～e)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

8.2.4.7 测试验收

8.2.4.7.1 测评指标

见GB/T 22239--2008中8.2.4.7。

8.2.4.7.2 测评实施

本项要求包括：

a) 应访谈系统建设负责人，询问是否有专门的部门负责测试验收工作，由何部门负责；是否委托第三方测试机构对信息系统进行独立的安全性测试；

b) 应访谈系统建设负责人，询问是否根据设计方案或合同要求组织相关部门和人员制定工程测试验收方案，并对系统测试验收报告进行审定；

c) 应检查系统建设方面的管理制度，查看其是否包括对系统测试验收的控制方法和人员行为准

则规定；

d) 应检查是否具有工程测试验收方案，查看其是否明确说明参与测试的部门、人员、测试验收内容、现场操作过程等内容，过程控制是否符合管理规定的要求；

e) 应检查是否具有系统测试验收报告，是否有相关部门和人员对系统测试验收报告进行审定的意见，是否有第三方测试机构的签字或盖章。

8.2.4.7.3 结果判定

如果8.2.4.7.2中a)～e)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

8.2.4.8 系统交付

8.2.4.8.1 测评指标

见GB/T 22239—2008中8.2.4.8。

8.2.4.8.2 测评实施

本项要求包括：

a) 应访谈系统建设负责人，询问是否有专门的部门负责系统交接工作，系统交接工作是否根据交付清单对所交接的设备、文档、软件等进行清点；

b) 应访谈系统建设负责人，询问系统正式运行前是否对运行维护人员进行过培训，针对哪些方面进行过培训；

c) 应检查系统建设方面的管理制度，查看其是否包括系统交付的控制方法和人员行为准则的规定；

d) 应检查是否具有系统交付清单，查看交付清单是否说明系统交付的各类设备、软件、文档等；

e) 应检查系统交付提交的文档，查看是否有指导用户进行系统运维的文档等，提交的文档是否符合管理规定的要求；

f) 应检查是否有系统交付技术培训记录，查看是否包括培训内容、培训时间和参与人员等。

8.2.4.8.3 结果判定

如果8.2.4.8.2中a)～f)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

8.2.4.9 系统备案

8.2.4.9.1 测评指标

见GB/T 22239—2008中8.2.4.9。

8.2.4.9.2 测评实施

本项要求包括：

a) 应访谈系统建设负责人，询问是否有专门的部门或人员负责管理系统定级的相关文档，由何部门/何人负责；询问对系统定级相关备案文档使用的控制方式；

b) 应检查是否具有将系统等级及相关材料报主管部门备案的记录或备案文档；

c) 应检查是否具有将系统等级及相关备案材料报相应公安机关备案的记录或证明。

8.2.4.9.3 结果判定

如果 8.2.4.9.2 中 a)～c)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

8.2.4.10 等级测评

略。

8.2.4.11 安全服务商选择

8.2.4.11.1 测评指标

见 GB/T 22239—2008 中 8.2.4.11。

8.2.4.11.2 测评实施

本项要求包括：

a) 应访谈系统建设负责人，询问信息系统选择的安全服务商有哪些，是否符合国家有关规定；

b) 应检查是否具有与安全服务商签订的安全责任合同书或保密协议等文档，查看其内容是否包含保密范围、安全责任、违约责任、协议的有效期限和责任人的签字等；

c) 应检查是否具有与安全服务商签订的服务合同或安全责任合同书，查看是否明确了后期的技术支持和服务承诺等内容。

8.2.4.11.3 结果判定

如果 8.2.4.11.2 中 a)～c)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

8.2.5 系统运维管理

8.2.5.1 环境管理

8.2.5.1.1 测评指标

见 GB/T 22239—2008 中 8.2.5.1。

8.2.5.1.2 测评实施

本项要求包括：

a) 应访谈系统运维负责人，询问是否有专门的部门或人员对机房供配电、空调、温湿度控制等设施进行定期维护，由何部门/何人负责，维护周期多长；

b) 应访谈系统运维负责人，询问是否有专门的部门或人员对机房的出入、服务器开机/关机等日常工作进行管理，由何部门/何人负责；

c) 应访谈系统运维负责人，询问为保证办公环境的保密性采取了哪些控制措施，在哪个区域接待来访人员，工作人员调离时是否收回办公室钥匙等；

d) 应检查是否有机房安全管理制度，查看其内容是否覆盖机房物理访问、物品带进/带出机房和机房环境安全等方面。

e) 应检查是否具有空调、温湿度控制等机房设施的维护保养记录，表明定期对这些设施进行了维护保养；

f) 应检查办公环境，查看其是否包括工作人员离开座位时退出登陆状态、桌面没有敏感信息文件等；

g) **应检查办公环境是否有与机房相同的物理安全措施，如门禁控制、摄像监控系统等，出入办公环境和机房不同区域是否要经过相应级别的授权。**

8.2.5.1.3 结果判定

如果8.2.5.1.2中a)～g)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

8.2.5.2 资产管理

8.2.5.2.1 测评指标

见GB/T 22239—2008中8.2.5.2。

8.2.5.2.2 测评实施

本项要求包括：

a) 应访谈系统运维负责人，询问是否有资产管理的责任人员或部门，由何部门/何人负责；

b) 应检查是否有资产清单，查看其内容是否覆盖资产责任部门、责任人、所处位置和重要程度等方面；

c) 应检查是否有资产安全管理方面的制度，查看是否明确信息资产管理的责任部门、责任人，查看其内容是否覆盖资产使用、借用、维护等方面；

d) 应检查是否有资产安全管理方面的制度，查看是否明确了依据资产的重要程度对资产进行分类和标识管理的方法，是否明确了信息分类标识的原则和方法，是否说明了不同类别的资产采取的不同管理措施。

8.2.5.2.3 结果判定

如果8.2.5.2.2中a)～d)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

8.2.5.3 介质管理

8.2.5.3.1 测评指标

见GB/T 22239—2008中8.2.5.3。

8.2.5.3.2 测评实施

本项要求包括：

a) 应访谈资产管理员，询问介质的存放环境是否采取保护措施防止介质被盗、被毁等；

b) 应访谈资产管理员，询问是否根据介质的目录清单对介质的使用现状进行定期检查；

c) 应访谈资产管理员，询问是否将介质保管在一个特定环境里，有专人负责，并根据重要性对介质进行分类和标识；

d) 应访谈资产管理员，询问是否对某些重要介质实行异地存储，异地存储环境是否与本地环境相同；

e) 应访谈资产管理员，询问是否定期对存储介质的完整性(数据是否损坏或丢失)和可用性(介质是否受到物理破坏)进行检查，是否对重要数据进行加密存储；

f) 应访谈资产管理员，询问对送出维修或销毁的介质在送出之前是否对介质内存储数据进行净化处理，对介质带出工作环境和重要介质中的数据和软件是否进行保密性处理；对保密性较高的介质销毁前是否有领导批准；

g) 应访谈资产管理员，询问对介质的物理传输过程是否要求选择可靠传输人员、严格介质的打包、选择安全的物理传输途径、双方在场交付等环节的控制；

h) 应检查是否有介质安全管理制度，查看是否对介质的存放环境、使用、维护和销毁等方面作出规定，**是否明确了保密性较高的信息存储介质应获得批准并在双人监控下才能销毁的要求**；

i) 应检查介质使用管理记录，查看其是否记录介质归档和使用等情况；

j) 应检查介质存储环境，查看是否对其进行了分类，并具有不同标识；

k) 应抽样检查重要介质，查看是否可以使用，查看需要加密存储的数据是否加密；

l) **应模拟保密性介质销毁过程，查看其销毁过程是否符合管理规定要求。**

8.2.5.3.3 结果判定

如果8.2.5.3.2中a)～l)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

8.2.5.4 设备管理

8.2.5.4.1 测评指标

见GB/T 22239—2008中8.2.5.4。

8.2.5.4.2 测评实施

本项要求包括：

a) 应访谈系统运维负责人，询问是否有专门的部门或人员对各种设备、线路进行定期维护，由何部门/何人负责，维护周期多长；

b) 应检查是否有设备安全管理制度，查看其内容是否对各种软硬件设备的选型、采购、发放和领用等环节进行规定；

c) 应检查设备安全管理制度中是否有对终端计算机、便携机和网络设备等使用方式、操作原则、注意事项等方面的规定，是否有信息处理设备必须经过审批才能带离机房或办公地点的要求；

d) 应检查设备安全管理制度中是否有对涉外维修和服务的审批、维修过程的监督控制管理等要求；

e) 应检查是否有关键设备的操作规程。

8.2.5.4.3 结果判定

如果8.2.5.4.2中a)～e)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

8.2.5.5 监控管理和安全管理中心

8.2.5.5.1 测评指标

见GB/T 22239—2008中8.2.5.5。

8.2.5.5.2 测评实施

本项要求包括：

a) 应访谈系统运维负责人，询问是否对通信线路、主机、网络设备和应用软件的运行状况，对设备状态、恶意代码、网络流量、补丁升级、安全审计等安全相关事项进行集中管理，是否形成监测记录文档，是否组织人员对监测记录进行整理并保管；
b) 应访谈系统运维负责人，询问其是否组织人员定期对监测记录进行分析、评审，是否发现可疑行为并对其采取必要的措施，是否形成分析报告；
c) 应检查是否具有安全集中管理的相关工具，可以实施对设备状态、恶意代码、补丁升级、安全审计等安全相关事项的集中监控和管理；
d) 应检查监测记录，查看是否记录监控对象、监控内容、监控的异常现象处理等方面，查看是否对异常现象及处理措施形成分析报告。

8.2.5.5.3 结果判定

如果 8.2.5.5.2 中 a)～d)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

8.2.5.6 网络安全管理

8.2.5.6.1 测评指标

见 GB/T 22239—2008 中 8.2.5.6。

8.2.5.6.2 测评实施

本项要求包括：

a) 应访谈系统运维负责人，询问是否指定专门的部门或人员负责网络管理，维护网络运行日志、监控记录，分析处理报警信息等；
b) 应访谈网络管理员，询问是否定期对网络进行漏洞扫描，扫描周期多长，发现漏洞是否及时修补；
c) 应访谈网络管理员，询问是否根据厂家提供的软件升级版本对网络设备进行过升级，目前的版本号为多少，升级前是否对重要文件进行备份，采取什么方式备份；
d) 应访谈网络管理员，网络的外联种类有哪些，是否都得到授权与批准，由何部门或何人批准，申请和批准的过程；
e) 应检查是否有网络安全管理制度，查看其是否覆盖网络安全配置、安全策略、升级与打补丁、授权访问、日志保存时间、口令更新周期等方面内容；
f) 应检查是否有网络安全管理制度，查看其是否明确了**禁止便携式和移动式设备网络接入的规定，是否明确了网络账户权限审批、权限分配、账户注销等方面的规定**；
g) 应检查是否有网络漏洞扫描报告，检查扫描时间间隔与扫描周期是否一致，检查网络设备是否实现了最小服务配置；
h) 应检查是否具有网络设备配置文件的备份文件，是否离线备份；
i) 应检查是否具有内部网络外联的授权批准书，检查是否有网络违规行为(如拨号上网等)的检查手段和工具。

8.2.5.6.3 结果判定

如果 8.2.5.6.2 中 a)～i)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

8.2.5.7 系统安全管理

8.2.5.7.1 测评指标

见 GB/T 22239—2008 中 8.2.5.7。

8.2.5.7.2 测评实施

本项要求包括：

a) 应访谈系统运维负责人，询问是否指定专门的部门或人员负责系统管理，如根据业务需求和系统安全分析制定系统的访问控制策略，控制分配文件及服务的访问权限；

b) 应访谈系统运维负责人，询问是否对系统管理员用户进行分类，明确各个角色的权限、责任和风险，权限设定是否遵循最小授权原则；

c) 应访谈系统管理员，询问系统日常管理的主要内容，是否有操作规程指导日常管理工作，包括重要的日常操作、参数的设置和修改等；

d) 应访谈系统管理员，询问是否定期对系统进行漏洞扫描，扫描周期多长，发现漏洞是否及时修补，在安装系统补丁前是否对重要文件进行备份，是否先在测试环境中测试通过再安装；

e) 应检查是否有系统安全管理制度，查看其内容是否覆盖系统安全策略、安全配置、日志管理和日常操作流程等方面，**是否明确了系统账户权限审批、权限分配、账户注销等方面的规定**；

f) 应检查是否有系统漏洞扫描报告，检查扫描时间间隔与扫描周期是否一致，检查系统服务是否实现了最小服务配置；

g) 应检查是否有详细日常运行维护操作日志，是否详细记录系统资源使用情况，如处理速度、存储容量等。

8.2.5.7.3 结果判定

如果 8.2.5.7.2 中 a)～g)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

8.2.5.8 恶意代码防范管理

8.2.5.8.1 测评指标

见 GB/T 22239—2008 中 8.2.5.8。

8.2.5.8.2 测评实施

本项要求包括：

a) 应访谈系统运维负责人，询问是否对员工进行基本恶意代码防范意识的教育，是否告知应及时升级软件版本，使用外来设备、网络上接收文件和外来计算机或存储设备接入网络系统之前进行病毒检查等；

b) 应访谈系统运维负责人，询问是否指定专人对恶意代码进行检测，发现病毒后是否及时处理；

c) 应访谈安全管理员，询问是否定期检查恶意代码库的升级情况，对截获的危险病毒或恶意代码是否及时进行分析处理，并形成书面的报表和总结汇报；

d) 应检查是否有恶意代码防范方面的管理制度，查看其内容是否覆盖防恶意代码软件的授权使用、恶意代码库升级、定期汇报等方面；

e) 应检查是否具有恶意代码检测记录、恶意代码库升级记录和分析报告，查看升级记录是否记录升级时间、升级版本等内容；查看分析报告是否描述恶意代码的特征、修补措施等内容。

8.2.5.8.3 结果判定

如果8.2.5.8.2中a)～e)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

8.2.5.9 密码管理

8.2.5.9.1 测评指标

见GB/T 22239—2008中8.2.5.9。

8.2.5.9.2 测评实施

本项要求包括：

a) 应访谈系统运维负责人，询问系统中是否使用密码技术和产品，密码技术和产品的使用是否遵照国家密码管理规定；

b) 应检查是否具有密码使用方面的管理制度。

8.2.5.9.3 结果判定

如果8.2.5.9.2中a)和b)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

8.2.5.10 变更管理

8.2.5.10.1 测评指标

见GB/T 22239—2008中8.2.5.10。

8.2.5.10.2 测评实施

本项要求包括：

a) 应访谈系统运维负责人，询问是否针对系统的重大变更制定变更方案指导系统变更工作的开展；

b) 应访谈系统运维负责人，询问变更方案是否经过评审，重要系统变更前是否得到有关领导的批准，由何人批准，对发生的变更情况是否通知了所有相关人员，以何种方式通知；

c) 应检查是否有变更管理制度，查看其是否覆盖变更前审批、变更过程记录、变更后通报等方面内容，是否包括变更申报、审批程序，是否规定需要申报的变更类型、申报流程、审批部门、批准人等方面内容；

d) 应检查系统变更方案，查看其是否覆盖变更类型、变更原因、变更过程、变更前评估、变更失败恢复程序等方面内容，查看其是否有主管领导的批准签字。

8.2.5.10.3 结果判定

如果8.2.5.10.2中a)～d)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

8.2.5.11 备份与恢复管理

8.2.5.11.1 测评指标

见GB/T 22239—2008中8.2.5.11。

8.2.5.11.2 测评实施

本项要求包括：

a) 应访谈系统运维负责人，询问是否识别出需要定期备份的业务信息、系统数据和软件系统，主要有哪些；

b) **应访谈系统运维负责人，询问是否根据信息系统的备份技术要求制定相应的灾难恢复计划，是否对灾难恢复计划进行测试并根据测试结果进行修订，目前的灾难恢复计划文档为第几版；**

c) 应检查是否有备份与恢复方面的管理制度，查看其是否明确了备份方式、备份频度、存储介质和保存期等方面内容，是否明确了数据的存放场所、文件命名规则、介质替换频率、数据离站传输方法等方面内容，**是否明确了保密数据的备份和恢复过程**；

d) 应访谈系统管理员、数据库管理员和网络管理员，询问是否定期执行恢复程序，周期多长，系统是否按照恢复程序完成恢复，如有问题，是否针对问题改进恢复程序或调整其他因素；

e) 应检查备份和恢复记录，查看其是否包含备份内容、备份操作、备份介质存放等内容，记录内容与备份和恢复策略是否一致，**检查是否具有保密数据的备份过程记录**；

f) **应检查对灾难恢复计划的测试文档或记录，查看测试内容是否包括运行系统恢复、人员协调、备用系统性能测试、通信连接等方面，如果做过修订，查看是否有修订后的版本。**

8.2.5.11.3 结果判定

如果8.2.5.11.2中a)～f)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

8.2.5.12 安全事件处置

8.2.5.12.1 测评指标

见GB/T 22239—2008中8.2.5.12。

8.2.5.12.2 测评实施

本项要求包括：

a) 应访谈系统运维负责人，询问是否告知用户在发现安全弱点和可疑事件时应及时报告；

b) 应检查是否有安全事件报告和处置管理制度，查看其是否明确安全事件的级别，明确不同级别安全事件的报告和处置方式等内容；

c) 应检查是否有安全事件报告和处置管理制度，查看其是否细化了不同安全事件的处理和报告程序，是否明确具体报告方式、报告内容、报告人等方面内容，造成系统中断和造成信息泄密的重大安全事件是否采用了不同于其他的处理程序和报告程序；

d) 应检查安全事件处理记录，查看其是否记录引发安全事件的原因，是否记录事件处理过程，是否与管理规定的处理要求一致等。

8.2.5.12.3 结果判定

如果8.2.5.12.2中a)～d)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

8.2.5.13 应急预案管理

8.2.5.13.1 测评指标

见GB/T 22239—2008中8.2.5.13。

8.2.5.13.2 测评实施

本项要求包括：

a) 应访谈系统运维负责人，询问是否具有应急预案小组，询问是否制定不同事件的应急预案，应急预案执行所需资金是否做过预算并能够落实；

b) 应访谈系统运维负责人，是否对系统相关人员进行应急预案培训，多长时间举办一次，是否定期对应急预案进行演练，演练周期多长，是否对应急预案定期进行审查；

c) 应检查是否具有定期审查应急预案的管理规定，查看是否明确应急预案中需要定期审查和根据实际情况更新的内容；

d) 应检查应急预案框架，查看其内容是否覆盖启动应急预案的条件、应急处理流程、系统恢复流程、事后教育和培训等方面；

e) 应检查是否具有根据应急预案框架制定的不同事件的应急预案，是否具有应急预案培训记录、演练记录和审查记录，**是否有对应急预案定期修订的纪录**。

8.2.5.13.3 结果判定

如果8.2.5.13.2中a)～e)均为肯定，则信息系统符合本单元测评指标要求，否则，信息系统不符合或部分符合本单元测评指标要求。

9 第五级信息系统单元测评

略。

10 信息系统整体测评

10.1 概述

GB/T 22239—2008中的要求项，是为了对抗相应等级的威胁或具备相应等级的恢复能力而设计的，但由于安全措施的实现方式多种多样，安全技术也在不断发展，信息系统的运行使用单位所采用的安全措施和技术并不一定和GB/T 22239—2008的要求项完全一致。因此，需要从信息系统整体上是否能够对抗相应等级威胁的角度，对单元测评中的不符合项和部分符合项进行综合分析，分析这些不符合项或部分符合项是否会影响到信息系统整体安全保护能力的缺失。信息系统的整体测评，就是在单元测评的基础上，评价信息系统的整体安全保护能力有没有缺失，是否能够对抗相应等级的安全威胁。

信息系统整体测评应从安全控制点间、层面间和区域间等方面进行安全分析和测评，并最后从系统结构安全方面进行综合分析，对系统结构进行安全测评。关于整体测评的进一步说明可参见附录B。

安全控制点间安全测评是指对同一区域同一层面内的两个或者两个以上不同安全控制点间的关联进行测评分析，其目的是确定这些关联对信息系统整体安全保护能力的影响。

层面间安全测评是指对同一区域内的两个或者两个以上不同层面安全控制点间的关联进行测评分析，其目的是确定这些关联对信息系统整体安全保护能力的影响。

区域间安全测评是指对两个或者两个以上不同物理或逻辑区域间安全控制点间的关联进行测评分析，其目的是确定这些关联对信息系统整体安全保护能力的影响。

10.2 安全控制点间测评

在单元测评完成后，如果信息系统的某个安全控制点中的要求项存在不符合或部分符合，应进行安全控制点间测评，应分析在同一功能区域同一层面内，是否存在其他安全控制点对该安全控制点具有补

充作用(如物理访问控制和防盗窃、安全审计和抗抵赖等)。同时,分析是否存在其他的安全措施或技术与该要求项具有相似的安全功能。

根据测评分析结果,综合判断该安全控制点所对应的系统安全保护能力是否缺失,如果经过综合分析单元测评中的不符合项或部分符合项不造成系统整体安全保护能力的缺失,则该安全控制点对应的单元测评结论应调整为符合。

10.3 层面间测评

在单元测评完成后,如果信息系统的某个安全控制点中的要求项存在不符合或部分符合,应进行层面间安全测评,重点分析其他层面上功能相同或相似的安全控制点是否对该安全控制点存在补充作用(如应用层加密与网络层加密、主机层与应用层上的身份鉴别等),以及技术与管理上各层面的关联关系(如主机安全与系统运维管理、应用安全与系统运维管理等)。

根据测评分析结果,综合判断该安全控制点所对应的系统安全保护能力是否缺失,如果经过综合分析单元测评中的不符合项或部分符合项不造成系统整体安全保护能力的缺失,则该安全控制点对应的单元测评结论应调整为符合。

10.4 区域间测评

在单元测评完成后,如果信息系统的某个安全控制点中的要求项存在不符合或部分符合,应进行区域间安全测评,重点分析系统中访问控制路径(如不同功能区域间的数据流流向和控制方式),是否存在区域间安全功能的相互补充。

根据测评分析结果,综合判断该安全控制点所对应的系统安全保护能力是否缺失,如果经过综合分析单元测评中的不符合项或部分符合项不造成系统整体安全保护能力的缺失,则该安全控制点对应的单元测评结论应调整为符合。

11 等级测评结论

11.1 各层面的测评结论

等级测评报告可以给出信息系统在安全技术和安全管理各个层面的测评结论。

汇总单元测评结果,可以给出安全技术和安全管理上各个层面的等级测评结论。在安全技术五个层面的等级测评结论中,通常物理安全测评结论应重点给出信息系统在防范各种自然灾害和人为物理破坏方面安全控制措施的落实情况;网络安全测评结论应重点给出信息系统在网络结构安全、网络访问控制和入侵检测、防范等方面安全控制措施的落实情况;主机安全测评结论应重点给出身份鉴别、访问控制、安全审计和恶意代码防范等方面安全控制措施的落实情况;应用安全测评结论应重点给出身份鉴别、访问控制、安全审计和通信保密等方面的安全控制措施的落实情况;数据安全及备份恢复测评结论应重点给出数据保密性、数据完整性和备份恢复功能安全控制措施的落实情况等。在安全管理五个方面的等级测评结论中,通常安全管理制度应重点给出管理制度体系的完备性和制修订的及时性等方面的测评结论;安全管理机构应重点给出机构、岗位设置和人员配备等方面的测评结论;人员安全管理应重点给出人员录用、离岗和培训等方面的测评结论;系统建设管理可重点给出安全方案设计、产品采购、系统的测试验收和交付等方面的测评结论;系统运维管理可重点给出系统监控管理、网络和系统安全管理、恶意代码防范管理、密码管理以及应急预案管理等方面的测评结论。

不同等级信息系统在不同层面上会有不同的关注点,应反映到相应层面的等级测评结论中。

11.2 风险分析和评价

等级测评报告中应对整体测评之后单元测评结果中的不符合项或部分符合项进行风险分析和

评价。

采用风险分析的方法对单元测评结果中存在的不符合项或部分符合项，分析所产生的安全问题被威胁利用的可能性，判断其被威胁利用后对业务信息安全和系统服务安全造成影响的程度，综合评价这些不符合项或部分符合项对信息系统造成的安全风险。

11.3 测评结论

等级测评报告应给出信息系统安全等级保护测评结论，确认信息系统达到相应等级保护要求的程度。

应结合各层面的测评结论和对单元测评结果的风险分析给出等级测评结论：

a) 如果单元测评结果中没有不符合项或部分符合项，则测评结论为“符合”；

b) 如果单元测评结果存在不符合项或部分符合项，但所产生的安全问题不会导致信息系统存在高等级安全风险，则测评结论为“基本符合”；

c) 如果单元测评结果存在不符合项或部分符合项，且所产生的安全问题导致信息系统存在高等级安全风险，则测评结论为“不符合”。

附 录 A
（资料性附录）
测 评 力 度

A.1 概述

本标准在第5章到第8章描述了第一级到第四级信息系统的单元测评的具体测评实施过程要求。为了便于理解、对比不同测评方法的测评力度以及不同级别信息系统单元测评的测评力度增强情况，分别编制表A.1测评方法的测评力度描述和表A.2不同安全保护等级信息系统的测评力度要求表。

A.2 测评方法的测评力度描述

测评方法是测评人员依据测评内容选取的、实施特定测评操作的具体方法。本标准涉及访谈、检查和测试等三种基本测评方法。访谈、检查和测试等三种基本测评方法的测评力度可以通过其测评的深度和广度来描述，如表A.1所示。

表A.1 测评方法的测评力度

测评方法	深度	广度
访谈	访谈的深度体现在访谈过程的严格和详细程度，可以分为四种：简要的、充分的、较全面的和全面的。简要访谈只包含通用和高级的问题；充分访谈包含通用和高级的问题以及一些较为详细的问题；较全面访谈包含通用和高级的问题以及一些有难度和探索性的问题；全面访谈包含通用和高级的问题以及较多有难度和探索性的问题	访谈的广度体现在访谈人员的构成和数量上。访谈覆盖不同类型的人员和同一类人的数量多少，体现出访谈的广度不同
检查	检查的深度体现在检查过程的严格和详细程度，可以分为四种：简要的、充分的、较全面的和全面的。简要检查主要是对功能级上的文档、机制和活动，使用简要的评审、观察或检查以及检查列表和其他相似手段的简短测评；充分检查有详细的分析、观察和研究，除了功能级上的文档、机制和活动外，还适当需要一些总体/概要设计信息；较全面检查有详细、彻底分析、观察和研究，除了功能级上的文档、机制和活动外，还需要总体/概要和一些详细设计以及实现上的相关信息；全面检查有详细、彻底分析、观察和研究，除了功能级上的文档、机制和活动外，还需要总体/概要和详细设计以及实现上的相关信息	检查的广度体现在检查对象的种类（文档、机制等）和数量上。检查覆盖不同类型的对象和同一类对象的数量多少，体现出对象的广度不同
测试	测试的深度体现在执行的测试类型上：功能/性能测试和渗透测试。功能/性能测试只涉及机制的功能规范、高级设计和操作规程；渗透测试涉及机制的所有可用文档，并试图智取进入信息系统	测试的广度体现在被测试的机制种类和数量上。测试覆盖不同类型的机制以及同一类型机制的数量多少，体现出对象的广度不同

A.3 信息系统测评力度

为了进一步理解不同等级信息系统在测评力度上的不同，表 A.2 在表 A.1 的基础上，从测评对象数量和种类以及测评深度等方面详细分析了不同测评方法的测评力度在不同安全保护等级信息系统安全测评中的具体体现。

表 A.2 不同安全保护等级信息系统的测评力度要求

测评力度		信息系统安全保护等级			
		第一级	第二级	第三级	第四级
访谈	广度	测评对象在种类和数量上抽样，种类和数量都较少	测评对象在种类和数量上抽样，种类和数量都较多	测评对象在数量上抽样，在种类上基本覆盖	测评对象在数量上抽样，在种类上全部覆盖
	深度	简要	充分	较全面	全面
检查	广度	测评对象在种类和数量上抽样，种类和数量都较少	测评对象在种类和数量上抽样，种类和数量都较多	测评对象在数量上抽样，在种类上基本覆盖	测评对象在数量上抽样，在种类上全部覆盖
	深度	简要	充分	较全面	全面
测试	广度	测评对象在种类和数量、范围上抽样，种类和数量都较少，范围小	测评对象在种类和数量、范围上抽样，种类和数量都较多，范围大	测评对象在数量和范围上抽样，在种类上基本覆盖	测评对象在数量、范围上抽样，在种类上基本覆盖
	深度	功能测试/性能测试	功能测试/性能测试	功能测试/性能测试，渗透测试	功能测试/性能测试，渗透测试

从表 A.2 可以看到，对不同等级的信息系统进行等级测评时，选择的测评对象的种类和数量是不同的，随着信息系统安全保护等级的增高，抽查的测评对象的种类和数量也随之增加。

对不同安全保护等级信息系统进行等级测评时，实际抽查测评对象的种类和数量，应当达到表 A.2 的要求，以满足相应等级的测评力度要求。在具体测评对象选择工作过程中，可参照遵循以下原则：

a) 完整性原则，选择的设备、措施等应能满足相应等级的测评力度要求；
b) 重要性原则，应抽查重要的服务器、数据库和网络设备等；
c) 安全性原则，应抽查对外暴露的网络边界；
d) 共享性原则，应抽查共享设备和数据交换平台/设备；
e) 代表性原则，抽查应尽量覆盖系统各种设备类型、操作系统类型、数据库系统类型和应用系统的类型。

附 录 B
（资料性附录）
关于整体测评的进一步说明

B.1 概述

信息系统的安全功能综合集成到信息系统不同层面后，会在层面内、层面间和区域间产生连接、交互、依赖、协调、协同等相互关联关系，共同作用于信息系统，使信息系统的整体安全功能与信息系统的结构以及安全控制点间、层面间和区域间的相互关联关系密切相关。整体测评就是通过分析安全控制点间，以及层面间和区域间的安全控制点间可能产生的功能增强、补充等关联作用，找出其他安全控制点对单项测评结果为不符合或部分符合的安全控制点进行补充或增强。

信息系统在安全控制点部署、层面整合和区域互连等系统集成后呈现出的安全集成特性，在单元测评中是没有体现的。因此，在单元测评的基础上，有必要对集成系统和运行环境进行整体测评分析和判断，以确定安全控制部署、层面整合、区域互连乃至整体系统结构等是否会增强或者削弱信息系统的整体安全保护能力；缺失或者低等级的安全控制是否会影响到系统的整体安全功能，在高等级的信息系统中使用低等级的安全控制是否能够达到相应等级的安全要求等。

在测评内容方面，在单元测评的基础上，信息系统整体安全性测评应重点测评分析不同安全控制的部署、层面的整合和区域的互连后其安全功能的相互作用和对信息系统整体安全功能的影响，具体应包括安全控制点间安全测评、层面间安全测评、区域间安全测评和系统结构安全测评等。

B.2 区域和层面

B.2.1 区域

根据在信息系统保护中所提供的安全功能，可以把信息系统划分为一个或者多个不同的区域。每个区域内的安全功能即可以为本区域提供服务，也可以为其他区域提供服务，使信息系统在整体安全性上表现出分区域的集成特性。

例如，可以把信息系统分为内部计算环境、区域边界和外部通信网络三大类。内部计算环境一般位于信息系统运营使用单位的物理控制范围内的局域网内，是信息系统进行信息存储和处理的主体。区域边界通常是处在内部计算环境和外部通信网络之间。外部通信网络区通常是信息系统提供通信的公共网络（如 Internet、PSTN、ISDN、公共无线网络等）或专用网络（如 DDN 等）。而基于统一的安全策略对计算环境、区域边界和通信网络的安全机制实施统一管理的设备可以在内部计算环境内，也可以独立构成一个功能区，即安全管理区。

不同区域之间可能需要进行信息交换，特别是有业务交互、数据通信的两个区域。为了进行信息交换，保证信息交换的安全，区域之间会产生连接、交互、依赖、协调、协同等相互关联关系，使得区域之间安全功能发生相互作用，进而相互影响。

不同区域之间相互作用会影响到区域的安全功能，可能使一个区域的安全功能得到增强、补充或依赖。发生增强作用说明两个区域发生关联关系后，一个区域已有的安全功能得到进一步增强，发挥更好的安全保护功能，具有更好的安全保护能力。发生补充作用说明两个区域发生关联关系后，一个区域原本没有的一部分安全功能，通过另一个区域的相互作用，得到补充，使其具备这些安全功能。出现依赖说明一个区域的安全功能依赖于另一个区域配合，才能发挥应有的作用。

B.2.2 层面

安全控制措施需要作用在信息系统的不同层面上，这些层面主要包括物理安全、网络安全、主机系统安全、应用安全和数据安全等技术上的五个层面以及安全管理机构、安全管理制度、人员安全管理、系统建设管理和系统运维管理等管理上的五个方面。

a) 物理安全。

物理安全是支持信息系统运行的设施环境以及构成信息系统的计算机、设备和介质等物理层面的安全。一般来说，物理层面构成组件位于被测单位（被测系统的运营使用单位）的物理控制范围内，主要分布在机房、介质存放地和终端运行场地等空间范围内。两个或者多个物理空间相连相通区域的物理安全控制措施，因为有空间上的连接连通，可能会发生关联关系，使其安全功能相互作用。

b) 网络安全。

网络层面构成组件负责支撑信息系统进行网络互联，为信息系统各个构成组件进行通信提供安全传输服务，一般包括计算机、网络设备（包括网络安全设备）、连接线路以及它们构成的网络拓扑等。两个不同区域面临不同的威胁，通过网络互联互通后，这些安全威胁可能会从一个区域影响到另一个区域，而安全功能的作用，也可以通过网络的互联互通，从一个区域影响到另一个区域。

c) 主机系统安全。

主机系统层面构成的组件主要有服务器、终端/工作站等所有计算机设备上的操作系统、数据库管理系统及其相关环境等，它们直接为信息系统对信息进行采集、加工、存储、传输、检索等处理提供环境，包括为信息系统用户提供人机交互的环境。

分布在同一服务器和终端/工作站等主机系统上的身份鉴别、访问控制、安全审计、系统资源控制等安全功能，需要相互协作，共同发挥作用，才能保证系统的安全。同时，为了进一步加强操作系统环境的安全，还可以在服务器和终端/工作站上安装主机入侵防范和主机恶意代码防范软件等。这使得操作系统的安全环境变得更为复杂，因此，有必要分析这些安全控制的引入对其他安全控制的影响。

d) 应用安全。

从功能上看，大多数应用系统主要是完成三种任务：获取用户输入，将输入存储为数据，按预定的操作规则处理这些数据。在应用系统中，用户一般需要和系统中的数据进行交互。因此，可以根据用户与数据之间所具有的层次把信息系统划分为三种：单层应用体系结构、两层应用体系结构和多层（三层以上）应用体系结构。

在单层应用体系结构中，用户界面、商业规则和数据管理等都在单一的应用层内实现。对数据本身来说，它可以是物理上位于一个远端位置，但是存取数据的逻辑却是应用系统的一部分。在这样的体系结构中，数据处理主要不是通过数据库，而是文件来存取数据，应用程序提供身份鉴别、访问控制及安全审计等安全功能。

在两层应用体系结构模型中，商业规则和用户界面仍然结合在一起构成应用系统的客户端。但是数据的存取和管理独立出来由单独的通常是运行在不同的系统上的程序来完成，这样的数据存取和管理程序通常是数据库管理系统，如 MS SQL Server、Sybase 和 Oracle 等。安全功能由客户端程序和数据库共同提供。

在多层应用体系结构模型中，商业规则被进一步从客户端独立出来，运行在一个介于用户界面和数据存储的单独的系统之上。客户端程序提供应用系统的用户界面，用户输入数据，查看反馈回来的请求结果，商业中间层由封装了商业逻辑的组件构成，这些商业逻辑组件模拟日常的商业任务，数据库管理系统离前端应用较远，中间有业务逻辑的隔离。三个部分均可以提供安全功能服务。

e) 数据安全。

数据安全构成组件主要为信息系统安全功能数据和用户数据提供安全保护。这些数据可能处于传输和处理过程中，也可能处于存储状态。对于传输和处理过程中的数据，一般有机密性和完整性的安全

要求，而对于存储中的数据，还需要有备份恢复的安全要求。

安全功能数据主要用于控制和管理信息系统的安全配置设置，使信息系统的安全功能能得到正确有效的执行。传输中的安全功能数据最常见的是用户鉴别信息，一般来说，它需要通过网络从客户端传输到服务器来进行鉴别。存储中的安全功能数据常见的有 ACL 列表、安全检测策略、审计配置等信息。用户数据主要是用于完成应用系统的使命，由应用系统按照应用目标和规则对其进行采集、加工、存储、传输、检索等处理的数据信息。

f） 安全管理机构。

安全管理机构包括安全管理的岗位设置、人员配备、授权和审批、沟通和合作等方面内容，严格的安全管理应该由相对独立的职能部门和岗位来完成。安全管理机构从组织上保证了信息系统的安全。

g） 安全管理制度。

在被测系统中，安全管理制度一般是文档化的，被正式制定、评审、发布和修订，内容包括策略、制度、规程、表格和记录等，构成一个塔字结构的文档体系，如图 B.1 所示。

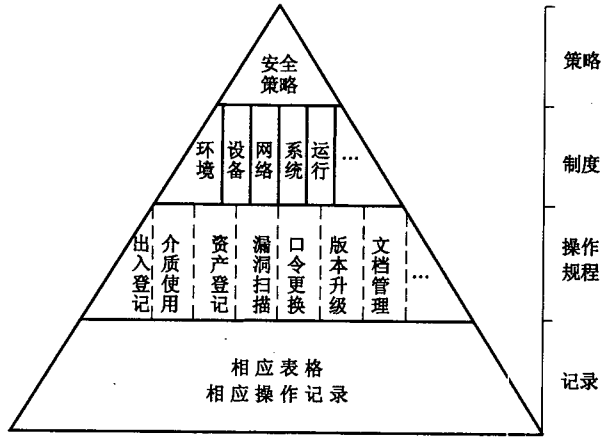

图 B.1 文档结构图

安全管理制度规范了各种安全管理制度的制修订和发布行为。安全管理制度直接关系到各种安全控制技术的正确部署、安全配置和合理使用。因此，安全管理制度的制修订和发布行为也将间接影响到信息系统的整体安全。

h） 人员安全管理。

人员安全管理包括信息系统用户、安全管理人员和第三方人员的管理，覆盖人员录用、人员离岗、人员考核、安全意识教育和培训、第三方人员管理等方面内容。工作人员直接运行、管理和维护信息系统的各种设备、设施和相关技术手段，与他们直接发生关联关系。因此，他们的知识结构和工作能力直接影响到信息系统其他层面的安全。

i） 系统建设管理。

系统建设管理包括系统定级、安全方案设计、产品采购、自行软件开发、外包软件开发、工程实施、测试验收、系统交付、安全测评、系统备案等信息系统安全等级建设的各个方面。信息系统的安全是一个过程，是一项工程，它不但涉及到当前的运行状态，而且还关系到信息系统安全建设的各个阶段。只有在信息系统安全建设的各个阶段确保安全，才能使得运行中的信息系统有安全保证。

j） 系统运维管理。

系统运维管理包括运行环境管理、资产管理、介质管理、设备管理、监控管理和安全管理中心、恶意代码防范管理、网络安全管理、系统安全管理、密码管理、变更管理、备份与恢复管理、安全事件处置和应急预案管理等方面内容。系统运维各个方面都直接关系到相关安全控制技术的正确、安全配置和合理使用。对信息系统运维各个方面提出具体的安全要求，可以为工作人员进行正确管理和运行提供工作

准绳，直接影响到整个信息系统的安全。

B.3 信息系统整体测评实例

B.3.1 安全控制点间安全测评实例

实例：物理访问控制与防盗窃防破坏间的测评分析。

某信息中心机房没有安装防盗报警设备，不符合物理安全-防盗窃和防破坏控制点的二级要求，但该机房只有一个出入口，并安排了专人24小时值守中心机房的出入口（物理访问控制符合要求）。通过专人值守可以发现并阻止设备被盗窃，有助于补充防盗窃防破坏安全控制点的安全保护缺失，但不能使该控制点完全符合要求。

B.3.2 层面间安全测评实例

实例：物理安全与主机系统安全的测评分析。

某单位屏蔽机房允许进入该机房的人员极为有限，所有外来人员进入机房必须由内部人员陪同，且行动授限，使得机房内的AIX主机在物理访问方面较为安全可控。尽管AIX主机上的本地登录用户的身份鉴别强度低于相应安全等级的要求，但考虑物理安全的加强（严格限制进入的人员）可以增强主机系统身份鉴别较弱的安全功能不足，使主机系统在总体的安全功能上不会受到影响，仍能基本满足相应等级的安全要求。

B.3.3 区域间安全测评实例

实例：计算环境与安全管理区的测评分析。

某定级信息系统的计算环境中包括三种业务，分别由三个独立的应用程序进行业务数据处理，三个应用程序都不提供身份鉴别功能，而由安全管理区的统一认证服务器提供统一的用户登录和身份认证。安全管理区提供的身份认证功能可以替代三个应用程序应用层面身份鉴别控制点的功能缺失。

参 考 文 献

[1] GB/T 20269—2006 信息安全技术 信息系统安全管理要求
[2] GB/T 20270—2006 信息安全技术 网络基础安全技术要求
[3] GB/T 20271—2006 信息安全技术 信息系统通用安全技术要求
[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] GB/T 20282—2006 信息安全技术 信息系统安全工程管理要求
[7] GB/T 18336—2008(所有部分) 信息安全技术 信息技术安全性评估准则
[8] ISO/IEC 27001:2005 Information technology—Security techniques—Information security management systems—Requirements
[9] ISO/IEC 17799: 2005 Information technology—Security techniques—Code of practice forinformation security management

GB/T 28448-2012

*
书号:155066·1-45598
定价: 100.00 元