ICS 35.040
L80

中华人民共和国国家标准

GB/T XXXX—XXXX

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

200X-XX-XX 发布　　200X-XX-XX 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

（略）

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）、《关于信息系统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 22240-2008 信息安全技术 信息系统安全等级保护定级指南；

——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 AAAA-AAAA 信息安全技术 信息系统安全等级保护实施指南。

一般来说，信息系统需要靠多种安全措施进行综合防范以降低其面临的安全风险。本标准针对信息系统中的单项安全措施和多个安全措施的综合防范，对应地提出单元测评和整体测评的技术要求，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。单元测评对安全技术和安全管理上各个层面的安全控制点提出不同安全保护等级的测评要求。整体测评根据安全控制点间、层面间和区域间相互关联关系以及信息系统整体结构对信息系统整体安全保护能力的影响提出测评要求。

本标准给出了等级测评结论中应包括的主要内容，未规定给出测评结论的具体方法和量化指标。

如果没有特殊指定，本标准中的信息系统主要指计算机信息系统。

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。

信息系统安全等级保护测评要求

1 范围

本标准规定了对信息系统安全等级保护状况进行安全测试评估的要求，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安全测试评估的单元测评要求和信息系统整体测评要求。本标准略去对第五级信息系统进行单元测评的具体内容要求。

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

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

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 所确立的以及下列术语和定义适用于本标准。

3.1 测评力度 testing and evaluation intensity

测评工作实际投入力量的表征，可以由测评广度和深度来描述。

4 总则

4.1 测评原则

a) 客观性和公正性原则

测评工作虽然不能完全摆脱个人主张或判断，但测评人员应当在没有偏见和最小主观判断情形下，按照测评双方相互认可的测评方案，基于明确定义的测评方法和过程，实施测评活动。

b) 经济性和可重用性原则

基于测评成本和工作复杂性考虑，鼓励测评工作重用以前的测评结果，包括商业安全产品测评结果和信息系统先前的安全测评结果。所有重用的结果，都应基于这些结果还能适用于目前的系统，能反映目前系统的安全状态。

c) 可重复性和可再现性原则

无论谁执行测评，依照同样的要求，使用同样的方法，对每个测评实施过程的重复执行都应该得到同样的测评结果。可再现性体现在不同测评者执行相同测评的结果的一致性。可重复性体现在同一测评者重复执行相同测评的结果的一致性。

d) 符合性原则

测评所产生的结果应当是在对测评指标的正确理解下所取得的良好的判断。测评实施过程应当使用正确的方法以确保其满足了测评指标的要求。

4.2 测评内容

信息系统安全等级测评主要包括单元测评和整体测评两部分。

单元测评是等级测评工作的基本活动，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 中的第五级目录中的各要求项（详见 4.5 节说明），测评实施描述测评过程中使用的具体测评方法、涉及的测评对象和具体测评取证过程的要求，结果判定描述测评

人员执行测评实施并产生各种测评数据后，如何依据这些测评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。

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的整体安全性，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以及系统结构的安全测评等。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内容、具体实施过程和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。

测评方法指测评人员在测评实施过程中所使用的方法，主要包括访谈、检查和测试三种测评方法。其中，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、分析或取得证据的过程，检查是指测评人员通过对测评对象（如管理制度、操作记录、安全配置等）进行观察、查验、分析以帮助测评人员理解、分析或取得证据的过程，测试是测评人员使用预定的方法/工具使测评对象产生特定的行为，通过查看和分析结果以帮助测评人员获取证据的过程。

测评对象指测评实施的对象，即测评过程中涉及到的信息系统的相关人员、制度文档、各类设备及其安全配置等。

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 结果重用

在信息系统中，有些安全控制可以不依赖于其所在的地点便可测评，即在其部署到运行环境之前便可以接受安全测评。一些商用安全产品的测评就属于这种安全测评。如果一个信息系统部署和安装在多个地点，且系统具有一组共同的软件、硬件、固件等组成部分，对这些安全控制的测评可以集中在一个集成测试环境中实施，如果没有这种环境，则可以在其中一个预定的运行地点实施，在其他运行地点的安全测评便可重用此测评结果。

在信息系统所有安全控制中，有一些安全控制与它所处于的运行环境紧密相关（如与人员或物理有关的某些安全控制），对其测评必须在分发到相应运行环境中才能进行。如果多个信息系统处在地域临近的封闭场地内，系统所属的机构在同一个领导层管理之下，对这些安全控制在多个信息系统中进行重复测评，可能是对有效资源的一种浪费。因此，可以在一个选定的信息系统中进行测评，其他相关信息系统可以直接重用这些测评结果。

4.5 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，在章节上分别对应国标 GB/T 22239-2008 的第 5 章到第 8 章。在国标 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 5.1.1.1。

5.1.1.1.2 测评实施

本项要求包括：

a) 应访谈物理安全负责人，了解部署了哪些控制人员进出机房的保护措施；

b) 应检查是否有专人负责机房的出入控制且有进入机房人员的登记记录。

5.1.1.1.3 结果判定

如果5.1.1.1.2 b）为肯定，则信息系统符合本单元测评指标要求，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 5.1.1.2。

5.1.1.2.2 测评实施

本项要求包括：

a) 应访谈物理安全负责人，了解采取了哪些防止设备、介质等丢失的保护措施；

b) 应检查关键设备是否放置在机房内或其它不易被盗窃和被破坏的可控范围内；

c) 应检查关键设备或设备的主要部件的固定情况，查看其是否不易被移动或被搬走，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 b）和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 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，询问机房建筑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） 应检查机房建筑是否有避雷装置。

5.1.1.3.3 结果判定

如果5.1.1.3.2 b）为肯定，则信息系统符合本单元测评指标要求，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 5.1.1.4。

5.1.1.4.2 测评实施

本项要求包括：

a） 应访谈物理安全负责人，询问机房是否设置了灭火设备，是否制定了有关机房消防的管理制度和消防预案，是否进行了消防培训；

b） 应检查机房是否设置了灭火设备，灭火设备摆放位置是否合理，其有效期是否合格。

5.1.1.4.3 结果判定

如果5.1.1.4.2 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。

5.1.1.5 防水和防潮

5.1.1.5.1 测评指标

见GB/T 22239-2008 5.1.1.5。

5.1.1.5.2 测评实施

本项要求包括：

a） 应访谈物理安全负责人，询问机房是否部署了防水防潮措施，是否没有出现过漏水和返潮事件；如果机房内有上/下水管安装，则查看是否采取必要的保护措施；

b） 应检查穿过主机房墙壁或楼板的管道是否采取必要的防渗防漏等防水保护措施；

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，机房及其环境是否不存在明显的漏水和返潮的威胁；如果出现漏水、渗透和返潮现象是否能够及时修复解决。

5.1.1.5.3 结果判定

如果5.1.1.5.2 b）和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。

5.1.1.6 温湿度控制

5.1.1.6.1 测评指标

见GB/T 22239-2008 5.1.1.6。

5.1.1.6.2 测评实施

本项要求包括：

a） 应访谈物理安全负责人，询问机房是否配备了空调等温湿度控制设施，保证温湿度能够满足计算机设备运行的要求，是否在机房管理制度中规定了温湿度控制的要求；

b） 应检查空调设备是否能够正常运行，检查机房温湿度是否满足计算站场地的技术条件要求。

5.1.1.6.3 结果判定

如果5.1.1.6.2 b）为肯定，则信息系统符合本单元测评指标要求，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 5.1.1.7。

5.1.1.7.2 测评实施

本项要求包括：

a) 应访谈物理安全负责人，询问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；
b) 应检查机房，查看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 b）为肯定，则信息系统符合本单元测评指标要求，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 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5.1.2.1.2 c）中缺少网络拓扑结构图，则为否定；
b) 如果5.1.2.1.2 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 5.1.2.2。

5.1.2.2.2 测评实施

本项要求包括：

a) 应访谈安全管理员，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5.1.2.2.2 b）为肯定，则信息系统符合本单元测评指标要求，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 5.1.2.3。

5.1.2.3.2 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防护措施有哪些；询问关键网络设备的登录和验证方式做过何种配置；询问远程管理的设备是否采取措施防止鉴别信息泄漏；
b) 应检查边界和关键网络设备，查看是否配置了对登录用户进行身份鉴别的功能；
c) 应检查边界和关键网络设备，查看是否配置了鉴别失败处理功能；
d) 应检查边界和关键网络设备，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 b）-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 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 5.1.3.1。

5.1.3.1.2 测评实施

本项要求包括：

a) 应访谈系统管理员和数据库管理员，询问操作系统和数据库管理系统的身份标识与鉴别机制采取何种措施实现；

b) 应检查关键服务器操作系统和关键数据库管理系统，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 b)为肯定，则信息系统符合本单元测评指标要求，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 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) 应检查关键服务器操作系统和关键数据库管理系统，查看匿名/默认帐户的访问权限是否已被禁用或者限制，是否删除了系统中多余的、过期的以及共享的帐户；

c) 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 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。

5.1.3.3 入侵防范

5.1.3.3.1 测评指标

见GB/T 22239-2008 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，询问操作系统补丁更新的方式和周期；

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 b)肯定，则信息系统符合本单元测评指标要求，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 5.1.3.4。

5.1.3.4.2 测评实施

本项要求包括：

a) 应访谈系统安全管理员，询问主机系统是否采取恶意代码实时检测与查杀措施，恶意代码实时检测与查杀措施的部署覆盖范围如何；

b) 应检查关键服务器，查看是否安装了实时检测与查杀恶意代码的软件产品并进行及时更新。

5.1.3.4.3 结果判定

如果5.1.3.4.2 b）为肯定，则信息系统符合本单元测评指标要求，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 5.1.4.1。

5.1.4.1.2 测评实施

本项要求包括：

a) 应访谈应用系统管理员，询问应用系统是否有专用的登录控制模块对登录的用户进行身份标识和鉴别，具体采取的鉴别措施是什么；

b) 应访谈应用系统管理员，询问应用系统是否具有登录失败处理功能；

c) 应访谈应用系统管理员，询问应用系统是否采取措施防止鉴别信息传输过程中被窃听，具体措施是什么；

d) 应检查关键应用系统，查看其是否提供身份标识和鉴别功能；

e) 应检查关键应用系统，查看其提供的登录失败处理功能，是否根据安全策略配置了相关参数。

5.1.4.1.3 结果判定

如果5.1.4.1.2 d）和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。

5.1.4.2 访问控制

5.1.4.2.1 测评指标

见GB/T 22239-2008 5.1.4.2。

5.1.4.2.2 测评实施

本项要求包括：

a) 应访谈应用系统管理员，询问应用系统是否提供访问控制措施，以及具体措施和访问控制策略有哪些；

b) 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/用户对系统功能和用户数据的访问；

c) 应检查关键应用系统，查看其是否具有由授权用户设置其它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；

d) 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。

5.1.4.2.3 结果判定

如果5.1.4.2.2 b）-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。

5.1.4.3 通信完整性

5.1.4.3.1 测评指标

见GB/T 22239-2008 5.1.4.3。

5.1.4.3.2 测评实施

本项要求包括：

a） 应访谈安全管理员，询问应用系统是否具有在数据传输过程中保护其完整性的措施，具体措施是什么；

b） 应检查设计或验收文档，查看其是否有关于保护通信完整性的说明。

5.1.4.3.3 结果判定

如果5.1.4.3.2 b）为肯定，则信息系统符合本单元测评指标要求，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 5.1.4.4。

5.1.4.4.2 测评实施

本项要求包括：

a） 应访谈应用系统管理员，询问应用系统是否具有保证软件容错能力的措施，具体措施有哪些；

b） 应检查关键应用系统，查看应用系统是否具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的功能；

c） 应测试关键应用系统，可通过对人机接口输入的不同长度或格式的数据，查看系统的反应，验证系统人机接口有效性检验功能是否正确。

5.1.4.4.3 结果判定

如果5.1.4.4.2 b）和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。

5.1.5 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 5.1.5.1。

5.1.5.1.2 测评实施

本项要求包括：

a） 应访谈安全管理员，询问关键应用系统用户数据在传输过程中是否有完整性保证措施，具体措施有哪些；

b） 应检查关键应用系统，查看其是否配备检测重要用户数据在传输过程中完整性受到破坏的功能。

5.1.5.1.3 结果判定

如果 5.1.5.1.2 b）为肯定，则信息系统符合本单元测评指标要求，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 5.1.5.2。

5.1.5.2.2 测评实施

本项要求包括：

a） 应访谈网络管理员，询问是否对网络设备中的配置文件进行备份，备份策略是什么；当其受到破坏时，恢复策略是什么；

b） 应访谈系统管理员，询问是否对操作系统中的重要信息进行备份，备份策略是什么；当其受到破坏时，恢复策略是什么；

c） 应访谈数据库管理员，询问是否对数据库管理系统中的关键数据进行备份，备份策略是什么；当其受到破坏时，恢复策略是什么；

d) 应访谈安全管理员，询问是否对应用系统中的应用程序进行备份，备份策略是什么；当其受到破坏时，恢复策略是什么；

e) 应检查关键主机操作系统、关键网络设备、关键数据库管理系统和关键应用系统，查看其是否提供备份和恢复功能，备份和恢复功能的配置是否正确，并且查看实际备份结果是否与备份策略一致。

5.1.5.2.3 结果判定

如果 5.1.5.2.2 e）为肯定，则信息系统符合本单元测评指标要求，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 5.2.1.1。

5.2.1.1.2 测评实施

本项要求包括：

a) 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、建设和管理等层面。

5.2.1.1.3 结果判定

如果5.2.1.1.2 a）为肯定，则信息系统符合本单元测评指标要求，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 5.2.1.2。

5.2.1.2.2 测评实施

本项要求包括：

a) 应访谈安全主管，询问是否有专人负责制定安全管理制度；

b) 应访谈安全管理制度制、修订人员，询问安全管理制度的发布方式，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 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 5.2.2.1。

5.2.2.1.2 测评实施

本项要求包括：

a) 应访谈安全主管，询问信息系统设置了哪些工作岗位，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，查看其定义的岗位职责中是否包括系统管理员、网络管理员、安全管理员等重要岗位的职责。

5.2.2.1.3 结果判定

如果5.2.2.1.2 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 5.2.2.2。

5.2.2.2.2 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的人员配备情况；

b) 应检查安全管理各岗位人员信息表，查看其是否明确机房管理员、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。

5.2.2.2.3 结果判定

如果5.2.2.2.2 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 5.2.2.3。

5.2.2.3.2 测评实施

本项要求包括：

a) 应访谈安全主管，询问其是否需要对信息系统中的关键活动进行审批，审批部门是何部门，批准人是何人，他们的审批活动是否得到授权；

b) 应访谈安全主管，询问其对关键活动的审批范围。

5.2.2.3.3 结果判定

如果5.2.2.3.2 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。

5.2.2.4 沟通和合作

5.2.2.4.1 测评指标

见 GB/T 22239-2008 5.2.2.4。

5.2.2.4.2 测评实施

本项要求包括：

a) 应访谈安全主管，询问是否经常与公安机关、电信公司和兄弟单位联系，联系和合作方式有哪些；

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 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 5.2.3.1。

5.2.3.1.2 测评实施

本项要求包括：

a) 应访谈安全主管，询问是否有专门的部门或人员负责人员的录用工作，由何部门/何人负责；

b) 应访谈人事管理相关人员，询问在人员录用时对人员条件有哪些要求，是否对被录用人的身份和专业资格进行审查；

c) 应检查人员录用要求管理文档，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，查看是否记录审查内容和审查结果等。

5.2.3.1.3 结果判定

如果5.2.3.1.2 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 5.2.3.2。

5.2.3.2.2 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，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) 应检查是否具有对离岗人员的安全处理记录（如交还身份证件、设备等的登记记录）。

5.2.3.2.3 结果判定

如果5.2.3.2.2 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 5.2.3.3。

5.2.3.3.2 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，具体的培训方式有哪些；

b) 应访谈安全管理员，考查其对工作相关的信息安全基础知识、安全责任和惩戒措施等的理解程度。

5.2.3.3.3 结果判定

如果5.2.3.3.2 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。

5.2.3.4 外部人员访问管理

5.2.3.4.1 测评指标

见 GB/T 22239-2008 5.2.3.4。

5.2.3.4.2 测评实施

本项要求包括：

a) 应访谈安全管理员，询问对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）采取了哪些安全措施，是否经有关部门或负责人批准才能访问；

b) 应检查外部人员访问管理文档，查看是否有对外部人员访问机房等重要区域应经过相关部门或负责人批准的内容。

5.2.3.4.3 结果判定

如果5.2.3.4.2 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 5.2.4.1。

5.2.4.1.2 测评实施

本项要求包括：

a) 应访谈安全主管，询问确定信息系统安全保护等级的方法是否参照定级指南的指导，定级过程是否有书面描述；定级结果是否获得了相关部门的批准；

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，查看定级结果是否有相关部门的批准盖章。

5.2.4.1.3 结果判定

本项要求包括：

a) 5.2.4.1.2 a）没有上级主管部门的，如果有本单位信息安全主管领导的批准，则该项为肯定；

b) 如果5.2.4.1.2 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 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，询问是否根据系统的安全级别选择基本安全措施，是否依据风险分析的结果补充和调整安全措施，具体做过哪些调整；

b) 应检查系统的安全方案，查看方案是否描述系统的安全保护要求，是否详细描述了系统的安全策略，是否详细描述了系统采取的安全措施等内容；

c) 应检查系统的详细设计方案，查看详细设计方案是否对应安全方案进行细化，是否有安全建设方案和安全产品采购方案。

5.2.4.2.3 结果判定

如5.2.4.2.2 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 5.2.4.3。

5.2.4.3.2 测评实施

本项要求包括：

a) 应访谈系统建设负责人，询问信息安全产品的采购情况，是否有产品采购清单指导产品采购，采购过程如何控制；

b) 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。

5.2.4.3.3 结果判定

如果5.2.4.3.2 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。

5.2.4.4 自行软件开发

5.2.4.4.1 测评指标

见GB/T 22239-2008 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，自主开发软件是否在独立的模拟环境中编写、调试和完成；

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；

c) 应检查是否具有软件设计相关文档。

5.2.4.4.3 结果判定

如果5.2.4.4.2 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 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) 应检查是否具有需求分析说明书、软件设计说明书、软件操作手册等软件开发文档和使用指南。

5.2.4.5.3 结果判定

如果 5.2.4.5.2 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 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 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) 应检查测试验收记录是否详细记录了测试时间、人员、现场操作过程和测试验收结果等方面内容；

d) 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 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。

5.2.4.8 系统交付

5.2.4.8.1 测评指标

见 GB/T 22239-2008 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，询问目前的信息系统是否由内部人员独立运行维护，如果是，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说明系统交付的各类设备、软件、文档等；

d) 应检查是否具有系统建设文档、指导用户进行系统运维的文档、系统培训手册等。

5.2.4.8.3 结果判定

如果 5.2.4.8.2 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 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 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 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基础设施进行定期维护，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，询问对机房的出入、服务器开机/关机如何进行管理；

c) 应检查机房安全管理制度，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 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 5.2.5.2。

5.2.5.2.2 测评实施

应检查资产清单，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 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、介质内存储信息被未授权修改以及非法泄漏等；

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) 应检查介质管理记录，查看其是否记录介质归档和查询等情况。

5.2.5.3.3 结果判定

本项要求包括：

a) 如果5.2.5.3.2 a）中在防火、防水、防盗等方面均有措施，则为肯定；

b) 如果5.2.5.3.2 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 5.2.5.4。

5.2.5.4.2 测评实施

本项要求包括：

a) 应访谈资产管理员，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，对各类测试工具进行有效性检查，由何部门/何人负责，维护周期多长；

b) 应访谈资产管理员，询问是否对设备选用的各个环节（选型、采购、发放和领用等）进行审批控制；

c) 应检查设备安全管理制度，查看其内容是否明确对各种软硬件设备的选型、采购、发放和领用等环节进行申报和审批。

5.2.5.4.3 结果判定

如果5.2.5.4.2 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。

5.2.5.5 网络安全管理

5.2.5.5.1 测评指标

见GB/T 22239-2008 5.2.5.5。

5.2.5.5.2 测评实施

本项要求包括：

a) 应访谈安全主管，询问是否指定人员负责维护网络运行日志、监控记录和分析处理报警信息等网络安全管理工作；

b) 应访谈安全管理员，询问是否定期对网络设备进行漏洞扫描，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 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 5.2.5.6。

5.2.5.6.2 测评实施

本项要求包括：

a) 应访谈系统管理员，询问是否根据业务需求和系统安全分析制定系统的访问控制策略，控制分配信息系统、文件及服务的访问权限；是否及时安装最新安全补丁程序和进行漏洞修补，在安装系统补丁前是否对重要文件进行备份；

b) 应访谈安全管理员，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；

c) 应检查系统漏洞扫描报告，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 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 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 5.2.5.8。

5.2.5.8.2 测评实施

本项要求包括：

a) 应访谈系统管理员和数据库管理员，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 a）和b）为肯定，则信息系统符合本单元测评指标要求，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 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的管理职责。

5.2.5.9.3 结果判定

如果 5.2.5.9.2 a）和 b）为肯定，则信息系统符合本单元测评指标要求，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 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，询问现有机房和放置终端计算机设备的办公场地的环境条件是否能够满足信息系统业务需求和安全管理需求，是否具有基本的防震、防风和防雨等能力；**

b) **应检查机房和办公场地是否在具有防震、防风和防雨等能力的建筑内。**

6.1.1.1.3 结果判定

如果6.1.1.1.2 b）为肯定，则信息系统符合本单元测评指标要求，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 6.1.1.2。

6.1.1.2.2 测评实施

本项要求包括：

a) 应访谈物理安全负责人，了解部署了哪些控制人员进出机房的保护措施；

b) **应检查机房安全管理制度，查看是否有关于机房出入方面的规定；**

c) 应检查机房**出入口是否有专人值守，是否有值守记录**及人员进入机房的登记记录；**检查机房是否不存在专人值守之外的其他出入口；**

d) **应检查是否有来访人员进入机房的审批记录，查看审批记录是否包括来访人员的访问范围。**

6.1.1.2.3 结果判定

如果6.1.1.2.2 b）-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。

6.1.1.3 防盗窃和防破坏

6.1.1.3.1 测评指标

见 GB/T 22239-2008 6.1.1.3。

6.1.1.3.2 测评实施

本项要求包括：

a) 应访谈物理安全负责人，了解采取了哪些防止设备、介质等丢失的保护措施；

b) **应访谈机房维护人员，询问关键设备放置位置是否做到安全可控，设备或主要部件是否进行了固定和标记，通信线缆是否铺设在隐蔽处；是否对机房安装的防盗报警设施并定期进行维护检查；**

c) **应访谈资产管理员，介质是否进行了分类标识管理，介质是否存放在介质库或档案室内进行管理；**

d) 应检查关键设备是否放置在机房内或其它不易被盗窃和破坏的可控范围内；检查关键设备或设备的主要部件的固定情况，查看其是否不易被移动或被搬走，是否设置明显的不易除去的标记；

e） **应检查通信线缆铺设是否在隐蔽处；**

f） **应检查机房防盗报警设施是否正常运行，并查看是否有运行和报警记录；**

g） **应检查介质的管理情况，查看介质是否有正确的分类标识，是否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 d）-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。

6.1.1.4 防雷击

6.1.1.4.1 测评指标

见GB/T 22239-2008 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，**询问为防止雷击事件导致重要设备被破坏采取了哪些防护措施，**机房建筑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；**询问机房计算机供电系统是否有交流电源地线；**

b） 应检查机房建筑是否有避雷装置，**是否有交流地线；**

6.1.1.4.3 结果判定

如果6.1.1.4.2 b）为肯定，则信息系统符合本单元测评指标要求，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 6.1.1.5。

6.1.1.5.2 测评实施

本项要求包括：

a） 应访谈物理安全负责人，询问机房是否设置了灭火设备，**是否设置了火灾自动报警系统，是否有人负责维护该系统的运行，**是否制定了有关机房消防的管理制度和消防预案，是否进行了消防培训；

b） **应访谈机房维护人员，询问是否对火灾自动报警系统定期进行检查和维护；**

c） 应检查机房是否设置了灭火设备，灭火设备摆放位置是否合理，其有效期是否合格；**应检查机房火灾自动报警系统是否正常工作，查看是否有运行记录、报警记录、定期检查和维修记录。**

6.1.1.5.3 结果判定

如果6.1.1.5.2 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。

6.1.1.6 防水和防潮

6.1.1.6.1 测评指标

见GB/T 22239-2008 6.1.1.6。

6.1.1.6.2 测评实施

本项要求包括：

a） 应访谈物理安全负责人，询问机房是否部署了防水防潮措施；如果机房内有上/下水管安装，是否避免穿过屋顶和活动地板下，穿过墙壁和楼板的水管是否采取了可靠的保护措施；**在湿度较高的地区或季节是否有人负责机房防水防潮事宜，配备除湿装置；**

b） **应访谈机房维护人员，询问机房是否没有出现过漏水和返潮事件；如果机房内有上/下水管安装，是否经常检查其漏水情况；在湿度较高地区或季节是否有人负责机房防水防潮事宜，使用除湿装置除湿；如果出现机房水蒸气结露和地下积水的转移与渗透现象是否及时采取防范措施；**

c） 应检查穿过主机房墙壁或楼板的管道是否配置套管，管道与套管之间是否采取可靠的密封措施；

d） 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，机房及其环境是否不存在明显的漏水和返潮的威胁；如果出现漏水、渗透和返潮现象，则查看是否能够及时修复解决；

e） **对湿度较高的地区，应检查机房是否有湿度记录，是否有除湿装置并能够正常运行，是否有防止出现机房地下积水的转移与渗透的措施，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 c）-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 6.1.1.7。

6.1.1.7.2 测评实施

本项要求包括：

a） **应访谈物理安全负责人，询问关键设备是否采取用必要的防静电措施，机房是否不存在静电问题或因静电引发的安全事件；**

b） **应检查关键设备是否有安全接地，查看机房是否不存在明显的静电现象。**

6.1.1.7.3 结果判定

如果6.1.1.7.2 b）为肯定，则信息系统符合本单元测评指标要求，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 6.1.1.8。

6.1.1.8.2 测评实施

本项要求包括：

a） 应访谈物理安全负责人，询问机房是否配备了**温湿度自动调节设施，**保证温湿度能够满足计算机设备运行的要求，是否在机房管理制度中规定了温湿度控制的要求，是否有人负责此项工作，**是否定期检查和维护机房的温湿度自动调节设施，询问是否没有出现过温湿度影响系统运行的事件；**

b） 应检查**温湿度自动调节设施**是否能够正常运行，**查看是否有温湿度记录、运行记录和维护记录；**查看机房温湿度是否满足计算站场地的技术条件要求。

6.1.1.8.3 结果判定

如果6.1.1.8.2 b）为肯定，则信息系统符合本单元测评指标要求，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 6.1.1.9。

6.1.1.9.2 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；**是否设置了短期备用电源设备，供电时间是否满足系统关键设备最低电力供应需求；**

b） 应检查机房，查看计算机系统供电线路上的稳压器、过电压防护设备**和短期备用电源设备是否正常运行；**

c） **应检查是否有稳压器、过电压防护设备以及短期备用电源设备等的检查和维护记录。**

6.1.1.9.3 结果判定

如果6.1.1.9.2 b）和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。

6.1.1.10 电磁防护

6.1.1.10.1 测评指标

见 GB/T 22239-2008 6.1.1.10。

6.1.1.10.2 测评实施

本项要求包括：

a） **应访谈物理安全负责人，询问电源线和通信线缆是否隔离铺设，是否没有出现过因电磁干扰等问题引发的故障；**

b） **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 b）为肯定，则信息系统符合本单元测评指标要求，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 6.1.2.1。

6.1.2.1.2 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性能以及目前业务高峰流量情况；

b） **应访谈网络管理员，询问网段划分情况以及划分原则；询问重要的网段有哪些；**

c） **应访谈网络管理员，询问网络中带宽控制情况以及带宽分配的原则；**

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，查看是否有关键网络设备业务处理能力、接入网络及核心网络的带宽满足业务高峰期需要的设计或说明；**

f） **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

本项要求包括：

a） 如果 6.1.2.1.2 d）-f）缺少相应文档资料，则为否定；

b） 如果 6.1.2.1.2 d）-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。

6.1.2.2 访问控制

6.1.2.2.1 测评指标

见 GB/T 22239-2008 6.1.2.2。

6.1.2.2.2 测评实施

本项要求包括：

a） 应访谈安全管理员，询问网络访问控制措施有哪些；**询问访问控制策略的设计原则是什么；**询问网络访问控制设备具备哪些访问控制功能；**询问是否允许拨号访问网络；**

b） **应检查边界网络设备，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；**

c） **应检查边界网络设备，查看其是否限制具有拨号访问权限的用户数量；**

d） **应测试边界网络设备，可通过试图访问未授权的资源，验证访问控制措施是否能对未授权的访问行为进行控制，控制粒度是否至少为单个用户。**

6.1.2.2.3 结果判定

如果 6.1.2.2.2 b）-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。

6.1.2.3 安全审计

6.1.2.3.1 测评指标

见 GB/T 22239-2008 6.1.2.3。

6.1.2.3.2 测评实施

本项要求包括：

a） **应访谈安全审计员，询问边界和关键网络设备是否开启审计功能，审计内容包括哪些项；询问审计记录的主要内容有哪些；**

b） **应检查边界和关键网络设备，查看其审计策略是否包括网络设备运行状况、网络流量、用户行为等；**

c） **应检查边界和关键网络设备，查看其事件审计记录是否包括：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 6.1.2.4.2 b）和 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。

6.1.2.4 边界完整性检查

6.1.2.4.1 测评指标

见 GB/T 22239-2008 6.1.2.4。

6.1.2.4.2 测评实施

本项要求包括：

a） **应访谈安全管理员，询问是否对内部用户私自连接到外部网络的行为；**

b） **应检查边界完整性检查设备，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；**

c） **应测试边界完整性检查设备，验证其是否能够有效发现“非法外联”的行为。**

6.1.2.4.3 结果判定

如果 6.1.2.5.2 b）和 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。

6.1.2.5 入侵防范

6.1.2.5.1 测评指标

见 GB/T 22239-2008 6.1.2.5。

6.1.2.5.2 测评实施

本项要求包括：

a） **应访谈安全管理员，询问网络入侵防范措施有哪些；询问是否有专门设备对网络入侵进行防范；**

b） **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；**

c） **应检查网络入侵防范设备，查看其规则库是否为最新；**

d） **应测试网络入侵防范设备，验证其检测策略是否有效。**

6.1.2.5.3 结果判定

如果 6.1.2.6.2 b）-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。

6.1.2.6 网络设备防护

6.1.2.6.1 测评指标

见 GB/T 22239-2008 6.1.2.6。

6.1.2.6.2 测评实施

本项要求包括：

a) 应访谈网络管理员，询问**边界**和关键网络设备的防护措施有哪些；询问**边界**和关键网络设备的登录和验证方式做过何种配置；询问远程管理的设备是否采取措施防止鉴别信息被窃听；

b) **应访谈网络管理员，询问网络设备的口令策略是什么；**

c) **应检查边界和关键网络设备**，查看是否配置了对登录用户进行身份鉴别的功能，**口令设置是否有复杂度和定期修改要求**；

d) 应检查边界和关键网络设备，查看是否配置了鉴别失败处理功能；

e) 应检查边界和关键网络设备，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；

f) **应检查边界和关键网络设备，查看是否对网络设备管理员登录地址进行限制；**

g) **应对边界和关键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。**

6.1.2.6.3 结果判定

如果6.1.2.6.2 c）-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 6.1.3.1。

6.1.3.1.2 测评实施

本项要求包括：

a) 应访谈系统管理员和数据库管理员，询问操作系统和数据库管理系统的身份标识与鉴别机制采取何种措施实现；

b) **应访谈系统管理员和数据库管理员， 询问对操作系统和数据库管理系统是否采用了远程管理，如果采用了远程管理，查看是否采用了防止鉴别信息在网络传输过程中被窃听的措施；**

c) **应检查关键服务器操作系统和关键数据库管理系统帐户列表，查看管理员用户名分配是否唯一；**

d) **应检查关键服务器操作系统和关键数据库管理系统，查看是否提供了身份鉴别措施，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；**

e) **应检查关键服务器操作系统和关键数据库管理系统，查看是否已配置了鉴别失败处理功能，设置了非法登录次数的限制值；查看是否设置登录连接超时处理功能，如自动退出。**

6.1.3.1.3 结果判定

如果6.1.3.1.2 b）-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 6.1.3.2。

6.1.3.2.2 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) **应检查关键数据库服务器的数据库管理员与操作系统管理员是否由不同管理员担任；**

c) 应检查关键服务器操作系统和关键数据库管理系统，查看匿名/默认用户的访问权限是否已被禁用或者严格限制，是否删除了系统中多余的、过期的以及共享的帐户；

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。

6.1.3.2.3 结果判定

如果6.1.3.2.2 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。

6.1.3.3 安全审计

6.1.3.3.1 测评指标

见 GB/T 22239-2008 6.1.3.3。

6.1.3.3.2 测评实施

本项要求包括：

a) **应访谈安全审计员，询问主机系统的安全审计策略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) **应检查关键服务器操作系统和关键数据库管理系统，查看安全审计配置是否符合安全审计策略的要求；**

c) **应检查关键服务器操作系统和关键数据库管理系统，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；**

d) **应检查关键服务器操作系统和关键数据库管理系统，查看是否对审计记录实施了保护措施，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 b）-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。

6.1.3.4 入侵防范

6.1.3.4.1 测评指标

见 GB/T 22239-2008 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，询问操作系统补丁更新的方式和周期；

b) 应检查关键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；

c) **应检查是否设置了专门的升级服务器实现对关键服务器操作系统补丁的升级；**

d) 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安装。

6.1.3.4.3 结果判定

如果6.1.3.4.2 b)-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。

6.1.3.5 恶意代码防范

6.1.3.5.1 测评指标

见 GB/T 22239-2008 6.1.3.5。

6.1.3.5.2 测评实施

本项要求包括：

a) 应访谈系统安全管理员，询问主机系统是否采取恶意代码实时检测与查杀措施，恶意代码实时检测与查杀措施的部署覆盖范围如何；

b) 应检查关键服务器，查看是否安装了实时检测与查杀恶意代码的软件产品并进行及时更新；

c) **应检查防恶意代码产品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 b）-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。

6.1.3.6 资源控制

6.1.3.6.1 测评指标

见 GB/T 22239-2008 6.1.3.6。

6.1.3.6.2 测评实施

本项要求包括：

a) **应检查关键服务器操作系统，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) **应检查关键服务器操作系统，查看是否设置了单个用户对系统资源的最大或最小使用限度；**

c) **应检查能够访问关键服务器的终端是否设置了操作超时锁定的配置。**

6.1.3.6.3 结果判定

如果 6.1.3.6.2 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 6.1.4.1。

6.1.4.1.2 测评实施

本项要求包括：

a) 应访谈应用系统管理员，询问应用系统是否提供专用的登录控制模块对登录的用户进行身份标识和鉴别，具体措施有哪些；**系统采取何种措施防止身份鉴别信息被冒用；**

b) 应访谈应用系统管理员，询问应用系统是否具有登录失败处理功能；

c) **应访谈应用系统管理员，询问应用系统对用户标识是否具有唯一性；**

d) **应检查设计或验收文档，查看其是否有系统采用了保证唯一标识的措施的描述；**

e) 应检查关键应用系统，查看其是否提供身份标识和鉴别功能；**查看其身份鉴别信息是否具有不易被冒用的特点；其鉴别信息复杂度检查功能是否能保证系统中不存在弱口令等；**

f) 应检查关键应用系统，查看其提供的登录失败处理功能，是否根据安全策略配置了相关参数；

g) **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，验证其身份标识和鉴别功能是否有效；**

h) **应测试关键应用系统，验证其登录失败处理功能是否有效。**

6.1.4.1.3 结果判定

本项要求包括：

a) 如果6.1.4.1.2 d）中相关文档有系统采用了保证用户唯一性标识的措施的描述，则为肯定；

b) 如果6.1.4.1.2 d）-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。

6.1.4.2 访问控制

6.1.4.2.1 测评指标

见 GB/T 22239-2008 6.1.4.2。

6.1.4.2.2 测评实施

本项要求包括：

a) 应访谈应用系统管理员，询问应用系统是否提供访问控制措施，以及具体措施和访问控制策略有哪些，**访问控制的粒度如何；**

b) 应检查关键应用系统，查看系统是否提供访问控制机制；**是否依据安全策略控制用户对客体的访问；**

c) **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；**

d) 应检查关键应用系统，查看其是否有由授权用户设置其它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；

e) **应检查关键应用系统，查看系统是否授予不同帐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；

g) 应测试关键应用系统，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帐户的访问权限。

6.1.4.2.3 结果判定

如果6.1.4.2.2 b）-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。

6.1.4.3 安全审计

6.1.4.3.1 测评指标

见 GB/T 22239-2008 6.1.4.3。

6.1.4.3.2 测评实施

本项要求包括：

a) **应访谈安全审计员，询问应用系统是否有安全审计功能；对事件进行审计的选择要求和策略是什么；对审计日志的处理方式有哪些；**

b) **应检查关键应用系统，查看其当前审计范围是否覆盖到每个用户；**

c) **应检查关键应用系统，查看其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；**

d) **应检查关键应用系统，查看其审计记录信息是否包括事件发生的日期与时间、触发事件的主体与客体、事件的类型、事件成功或失败、身份鉴别事件中请求的来源、事件的结果等内容；**

e) **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；**

f) **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 b）-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。

6.1.4.4 通信完整性

6.1.4.4.1 测评指标

见 GB/T 22239-2008 6.1.4.4。

6.1.4.4.2 测评实施

本项要求包括：

a) 应访谈安全管理员，询问应用系统是否具有在数据传输过程中保护其完整性的措施，具体措施是什么；

b) 应检查设计或验收文档，查看其是否有关于保护通信完整性的说明，**如果有则查看文档中描述的保护措施是否与依据验证码判断对方数据包的有效性的措施相一致；**

c) **应测试关键应用系统，可通过获取通信双方的数据包，查看其是否有验证码。**

6.1.4.4.3 结果判定

如果6.1.4.4.2 b）和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。

6.1.4.5 通信保密性

6.1.4.5.1 测评指标

见 GB/T 22239-2008 6.1.4.5。

6.1.4.5.2 测评实施

本项要求包括：

a) **应访谈安全管理员，询问应用系统数据在通信过程中是否采取保密措施，具体措施有哪些，关键应用系统的通信是否都采取了上述措施；**

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；系统在通信过程中，对敏感信息字段进行加密的功能是否有效。**

6.1.4.5.3 结果判定

如果6.1.4.5.2 b）为肯定，则信息系统符合本单元测评指标要求，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 6.1.4.6。

6.1.4.6.2 测评实施

本项要求包括：

a) 应访谈应用系统管理员，询问应用系统是否具有保证软件容错能力的措施，具体措施有哪些；

b) 应检查关键应用系统，查看应用系统是否对人机接口输入或通信接口输入的数据进行有效性检验；

c) 应测试关键应用系统，可通过对人机接口输入的不同长度或格式的数据，查看系统的反应，验证系统人机接口有效性检验功能是否正确；

d) **应测试关键应用系统，验证其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 b）-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。

6.1.4.7 资源控制

6.1.4.7.1 测评指标

见 GB/T 22239-2008 6.1.4.7。

6.1.4.7.2 测评实施

本项要求包括：

a) **应访谈应用系统管理员，询问应用系统是否有资源控制的措施，具体措施有哪些；**

b) **应检查关键应用系统，查看系统是否有最大并发会话连接数的限制；**

c) **应检查关键应用系统，查看系统是否对单个帐户的多重并发会话进行限制；**

d) **应测试重要应用系统，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。**

6.1.4.7.3 结果判定

如果6.1.4.7.2 b）-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。

6.1.5 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 6.1.5.1。

6.1.5.1.2 测评实施

本项要求包括：

a) 应访谈安全管理员，询问应用系统**的鉴别信息**和重要业务数据在传输过程中是否有完整性保证措施，具体措施有哪些；

b) 应检查关键**主机操作系统、**关键**网络设备操作系统、**关键**数据库管理系统和**关键应用系统，查看其是否配备检测**鉴别信息**和重要业务数据在传输过程中完整性受到破坏的功能。

6.1.5.1.3 结果判定

如果 6.1.5.1.2 b）为肯定，则信息系统符合本单元测评指标要求，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 6.1.5.2。

6.1.5.2.2 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鉴别信息否采用加密或其他有效措施实现存储保密性；**

b) **应访谈系统管理员，询问关键主机操作系统的鉴别信息否采用加密或其他有效措施实现存储保密性；**

c) **应访谈数据库管理员，询问关键数据库管理系统的鉴别信息否采用加密或其他有效措施实现存储保密性；**

d) **应访谈安全管理员，询问关键应用系统的鉴别信息否采用加密或其他有效措施实现存储保密性；**

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

6.1.5.2.3 结果判定

如果 6.1.5.2.2 e）为肯定，则信息系统符合本单元测评指标要求，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 6.1.5.3。

6.1.5.3.2 测评实施

本项要求包括：

a) 应访谈网络管理员，询问是否对网络设备中的配置文件进行备份，备份策略是什么；当其受到破坏时，恢复策略是什么；**是否提供关键网络设备、通信线路的硬件冗余；**

b) 应访谈系统管理员，询问是否对操作系统中的重要信息进行备份，备份策略是什么；当其受到破坏时，恢复策略是什么；**是否提供关键服务器的硬件冗余；**

c) 应访谈数据库管理员，询问是否对数据库管理系统中的关键数据进行备份，备份策略是什么；当其受到破坏时，恢复策略是什么；

d) 应访谈安全管理员，询问是否对应用系统中的应用程序进行备份，备份策略是什么；当其受到破坏时，恢复策略是什么；

e) 应检查关键主机操作系统、关键网络设备、关键数据库管理系统和关键应用系统，查看其是否提供备份和恢复功能，其配置是否正确，并且查看其备份结果是否与备份策略一致；

f) **应检查关键网络设备、通信线路和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 e）和 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 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 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、建设和管理等层面的**重要管理内容**；

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 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 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，询问是否有**专门的部门或人员**负责制定安全管理制度；

b) 应访谈安全管理制度制、修订人员，询问安全管理制度的**制定程序**和发布方式，**是否对制定的安全管理制度进行论证和审定，论证和评审方式如何**；

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 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 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，评审周期多长，发现存在不足或需要改进的是否进行修订；**

b) **应检查安全管理制度评审记录，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。**

6.2.1.3.3 结果判定

如果6.2.1.3.2 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 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，询问设置了哪些工作岗位，各个岗位的职责分工是否明确；**询问是否设立安全管理各个方面的负责人；**

b) **应访谈安全主管、安全管理某方面的负责人，询问其岗位职责包括哪些内容；**

c) 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、机房管理员**、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 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。

6.2.2.2 人员配备

6.2.2.2.1 测评指标

见GB/T 22239-2008 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人员的配备情况，**包括数量、专职还是兼职**等；

b) 应检查安全管理各岗位人员信息表，查看其是否明确机房管理员、系统管理员、**数据库管理员**、网络管理员、安全管理员等重要岗位人员的信息，**确认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6.2.2.2.2a)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 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，审批部门是何部门，批准人是何人，他们的审批活动是否得到授权；

b) 应访谈安全主管，询问其对关键活动的审批范围包括哪些，**审批程序如何**；

c) **应检查审批管理制度文档，查看文档中是否明确对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批的审批部门和批准人，是否明确审批程序**；

d) **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 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。

6.2.2.4 沟通和合作

6.2.2.4.1 测评指标

见GB/T 22239-2008 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，询问是否经常与公安机关、电信公司和兄弟单位联系，联系和合作方式有哪些，**与组织机构内其他部门之间通过哪些方式进行交流和沟通，信息安全职能部门内部各类管理人员之间通过哪些方式进行交流和沟通**；

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) **应检查是否有组织机构内部人员联系表；**

d) 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。

6.2.2.4.3 结果判定

如果6.2.2.4.2 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。

6.2.2.5 审核和检查

6.2.2.5.1 测评指标

见GB/T 22239-2008 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，检查周期多长；**

b) **应检查安全管理员定期实施安全检查的文档或记录，查看记录的时间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。**

6.2.2.5.3 结果判定

如果6.2.2.5.2 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 6.2.3.1。

6.2.3.1.2 测评实施

本项要求包括：

a) 应访谈安全主管，询问是否有专门的部门或人员负责人员的录用工作，由何部门/何人负责；

b) 应访谈人事管理相关人员，询问在人员录用时对人员条件有哪些要求，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，录用后是否与从事关键岗位的人员签署保密协议**；

c) 应检查人员录用要求管理文档，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、**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；

e) **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；**

f) **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 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。

6.2.3.2 人员离岗

6.2.3.2.1 测评指标

见 GB/T 22239-2008 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**对即将离岗人员有哪些控制方法，**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) **应访谈人事管理相关人员，询问调离手续包括哪些；**

c) 应检查是否具有对离岗人员的安全处理记录（如交还身份证件、设备等的登记记录）；

d) **应检查是否具有按照离职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 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 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，询问是否有人负责定期对各个岗位人员进行安全技能及安全知识的考核，考核周期多长；**

b) **应检查考核文档，查看考核人员是否包括各个岗位的人员，考核日期与考核周期是否一致。**

6.2.3.3.3 结果判定

如果 6.2.3.3.2 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 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，具体的培训方式有哪些；**是否对违反安全策略和规定的人员进行惩戒，如何惩戒**；

b) 应访谈安全管理员、**系统管理员和网络管理员**，考查其对工作相关的信息安全基础知识、安全责任和惩戒措施等的理解程度；

c) **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；**

d) **应检查是否具有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 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。

6.2.3.5 外部人员访问管理

6.2.3.5.1 测评指标

见 GB/T 22239-2008 6.2.3.5。

6.2.3.5.2 测评实施

本项要求包括：

a) 应访谈安全管理员，询问对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）采取了哪些安全措施，是否经有关部门或负责人批准才能访问，**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，查看是否有对外部人员访问机房等重要区域应经过相关部门或负责人批准的内容；

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 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 6.2.4.1。

6.2.4.1.2 测评实施

本项要求包括：

a) 应访谈安全主管，询问确定信息系统安全保护等级的方法是否参照定级指南的指导，定级过程是否有书面描述，定级结果是否获得了相关部门的批准；

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，查看定级结果是否有相关部门的批准盖章。

6.2.4.1.3 结果判定

本项要求包括：

a) 6.2.4.1.2 a）没有上级主管部门的，如果有本单位信息安全主管领导的批准，则该项为肯定；

b) 如果6.2.4.1.2 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 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，询问是否根据系统的安全级别选择基本安全措施，是否依据风险分析的结果补充和调整安全措施，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) 应检查系统的安全方案，查看方案是否描述系统的安全保护要求，是否详细描述了系统的安全策略，是否详细描述了系统采取的安全措施等内容；

d) 应检查系统的详细设计方案，查看详细设计方案是否对应安全方案进行细化，是否有安全建设方案和安全产品采购方案，**查看方案是否有经过安全主管领导或管理部门的批准盖章；**

e) **应检查专家论证文档，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 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 6.2.4.3。

6.2.4.3.2 测评实施

本项要求包括：

a) **应访谈安全主管，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，询问信息安全产品的采购情况，是否有产品采购清单指导产品采购，采购过程如何控制；

c) **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；**

d) **应检查系统使用的有关信息安全产品是否符合国家的有关规定；**

e) **应检查密码产品的使用情况是否符合密码产品使用、管理的相关规定。**

6.2.4.3.3 结果判定

如果 6.2.4.3.2 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。

6.2.4.4 自行软件开发

6.2.4.4.1 测评指标

见GB/T 22239-2008 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，自主开发软件是否在独立的模拟环境中编写、调试和完成；

b) 应访谈系统建设负责人，询问软件设计相关文档**和使用指南**是否由专人负责保管，负责人是何人；

c) **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，是否明确软件开发相关文档的管理等；**

d) 应检查是否具有软件设计的相关文档（应用软件设计程序文件、源代码文档等）**、软件使用指南或操作手册和维护手册等**。

6.2.4.4.3 结果判定

如果6.2.4.4.2 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。

6.2.4.5 外包软件开发

6.2.4.5.1 测评指标

见 GB/T 22239-2008 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，**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**；

b) 应检查是否具有需求分析说明书、软件设计说明书、软件操作手册**、软件源代码文档**等软件开发文档和使用指南；

c) **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。**

6.2.4.5.3 结果判定

如果 6.2.4.5.2 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。

6.2.4.6 工程实施

6.2.4.6.1 测评指标

见 GB/T 22239-2008 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，询问是否有专门部门或人员负责工程实施管理工作，由何部门/何人负责，是否**按照工程实施方案的要求**对工程实施过程进行进度和质量控制；

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 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 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，**是否根据设计方案或合同要求组织相关部门和人员对系统测试验收报告进行审定；**

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

c) 应检查测试验收记录是否详细记录了测试时间、人员、现场操作过程和测试验收结果等方面内容；

d) 应检查是否具有系统测试验收报告，**是否有对测试验收报告的审定文档，查看文档是否有相关人员的审定意见**。

6.2.4.7.3 结果判定

如果 6.2.4.7.2 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。

6.2.4.8 系统交付

6.2.4.8.1 测评指标

见 GB/T 22239-2008 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，询问目前的信息系统是否由内部人员独立运行维护，如果是，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说明系统交付的各类设备、软件、文档等；

d) 应检查是否具有系统建设文档、指导用户进行系统运维的文档、系统培训手册等；

e) **应检查培训记录，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 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 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，查看是否包括服务内容、服务期限、双方签字或盖章等。

6.2.4.9.3 结果判定

如果 6.2.4.9.2 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 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基础设施进行定期维护，由何部门或何人负责，维护周期多长，**是否有机房管理员负责机房出入等环境安全管理工作**；

b) **应访谈安全主管，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；**

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

d) **应检查是否具有机房基础设施维护记录**。

6.2.5.1.3 结果判定

如果6.2.5.1.2 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。

6.2.5.2 资产管理

6.2.5.2.1 测评指标

见GB/T 22239-2008 6.2.5.2。

6.2.5.2.2 测评实施

本项要求包括：

a) **应访谈安全主管，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) **应检查资产安全管理制度，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 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 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、介质内存储信息被未授权修改以及非法泄漏等，**是否有专人管理**；

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，**是否对介质进行分类和标识管理**；

c) **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；**

d) 应检查介质管理记录，查看其是否记录介质的归档、查询和**借用**等情况；

e) **应检查介质，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

本项要求包括：

a) 如果6.2.5.3.2 a）中在防火、防水、防盗等方面均有措施并有介质管理员，则该项为肯定；

b) 如果6.2.5.3.2 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。

6.2.5.4 设备管理

6.2.5.4.1 测评指标

见GB/T 22239-2008 6.2.5.4。

6.2.5.4.2 测评实施

本项要求包括：

a) 应访谈资产管理员，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，对各类测试工具进行有效性检查，由何部门/何人负责，维护周期多长；

b) 应访谈资产管理员，询问是否对设备选用的各个环节（选型、采购、发放和领用**及信息处理设备带离机构**等）进行审批控制；

c) **应访谈安全审计员，询问对关键设备（包括备份和冗余设备）的操作是否建立日志，日志文件如何管理，是否定期检查管理情况；**

d) 应检查设备安全管理制度，查看其内容是否明确对各种软硬件设备的选型、采购、发放和领用**以及带离机构**等环节进行申报和审批；

e) **应检查设备使用管理文档，查看其内容是否覆盖终端计算机、便携机和网络设备等使用、操作原则、注意事项等方面；**

f) **应检查关键设备（包括备份和冗余设备）的操作规程，查看其内容是否覆盖服务器如何启动、停止、加电、断电等操作。**

6.2.5.4.3 结果判定

如果6.2.5.4.2 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。

6.2.5.5 网络安全管理

6.2.5.5.1 测评指标

见GB/T 22239-2008 6.2.5.5。

6.2.5.5.2 测评实施

本项要求包括：

a) 应访谈安全主管，询问是否指定人员负责维护网络运行日志、监控记录和分析处理报警信息等网络安全管理工作，**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**；

b) **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；**

c) 应访谈安全管理员，询问是否定期对网络设备进行漏洞扫描，扫描周期多长，发现漏洞是否及时修补；

d) 应检查网络漏洞扫描报告，**查看其内容是否包含网络存在的漏洞、严重级别和结果处理等方面**，检查扫描时间间隔与扫描周期是否一致；

e) **应检查网络安全管理制度，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) **应检查是否具有内部网络外联的授权批准书；**

g) **应检查是否具有网络设备配置文件的备份文件；**

h) **应检查是否具有网络审计日志，检查日志是否在规定的保存时间范围内。**

6.2.5.5.3 结果判定

如果6.2.5.5.2 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 6.2.5.6。

6.2.5.6.2 测评实施

本项要求包括：

a) 应访谈系统管理员，询问是否根据业务需求和系统安全分析制定系统的访问控制策略，控制分配信息系统、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安装安全补丁程序，在安装系统补丁前是否对重要文件进行备份，**采取什么方式进行，是否先在测试环境中测试通过再安装；**

c) 应访谈安全管理员，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；

d) **应检查系统安全管理制度，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) **应检查是否有详细操作日志(包括重要的日常操作、运行维护记录、参数的设置和修改等内容)；**

f) **应检查是否有定期对运行日志和审计结果进行分析的记录；**

g) 应检查系统漏洞扫描报告，**查看其内容是否包含系统存在的漏洞、严重级别和结果处理等方面，**检查扫描时间间隔与扫描周期是否一致。

6.2.5.6.3 结果判定

如果6.2.5.6.2 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。

6.2.5.7 恶意代码防范管理

6.2.5.7.1 测评指标

见GB/T 22239-2008 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) **应检查恶意代码防范管理文档，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；**

d) **应检查是否具有恶意代码检测记录。**

6.2.5.7.3 结果判定

如果6.2.5.7.2 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。

6.2.5.8 密码管理

6.2.5.8.1 测评指标

见 GB/T 22239-2008 6.2.5.8。

6.2.5.8.2 测评实施

应访谈安全管理员，询问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 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，询问是否制定变更方案指导系统执行变更；**

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 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 6.2.5.10。

6.2.5.10.2 测评实施

本项要求包括：

a) 应访谈系统管理员、数据库管理员**和网络管理员**，询问是否识别出需要定期备份的业务信息、系统数据及软件系统，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 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 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) **应访谈系统运维负责人，询问是否根据本系统已发生的和需要防止发生的安全事件对系统的影响程度划分不同等级，划分为几级，划分方法是否参照了国家相关管理部门的技术资料，主要参照哪些；**

c) 应检查安全事件报告和处置管理制度，查看其**是否明确本系统已发生的和需要防止发生的安全事件类型，**是否明确安全事件的现场处理、事件报告和后期恢复的管理职责；

d) **应检查安全事件定级文档，查看其是否明确安全事件的定义、安全事件等级划分的原则、等级描述等方面内容；**

e) **应检查安全事件记录分析文档，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，是否采取措施避免其再次发生。**

6.2.5.11.3 结果判定

如果 6.2.5.11.2 a）-e）为肯定，则信息系统符合本单元测评指标要求，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 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；**

d) **应检查是否具有应急预案培训记录。**

6.2.5.12.3 结果判定

如果6.2.5.12.2 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 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，询问现有机房和放置终端计算机设备的办公场地的环境条件是否能够满足信息系统业务需求和安全管理需求，是否具有基本的防震、防风和防雨等能力；**询问机房场地是否符合选址要求；**

b) **应访谈机房维护人员，询问是否存在因机房和办公场地环境条件引发的安全事件或安全隐患；如果某些环境条件不能满足，是否及时采取了补救措施；**

c) 应检查机房和办公场地是否在具有防震、防风和防雨等能力的建筑内；

d) **应检查机房场地是否不在建筑物的高层或地下室，以及用水设备的下层或隔壁。**

7.1.1.1.3 结果判定

如果7.1.1.1.2 c）和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。

7.1.1.2 物理访问控制

7.1.1.2.1 测评指标

见 GB/T 22239-2008 7.1.1.2。

7.1.1.2.2 测评实施

本项要求包括：

a) 应访谈物理安全负责人，了解部署了哪些控制人员进出机房的保护措施；

b) **应访谈物理安全负责人，如果业务或安全管理需要，是否对机房进行了划分区域管理，是否对各个区域都有专门的管理要求；**

c) **应访谈机房值守人员，询问是否认真执行有关机房出入的管理规定，是否对进入机房的人员记录在案；**

d) 应检查机房安全管理制度，查看是否有关于机房出入方面的规定；

e) 应检查机房出入口是否有专人值守，是否有值守记录以及进出机房的人员登记记录；检查机房是否不存在值守人员控制之外的其他出入口；

f) 应检查是否有来访人员进入机房的审批记录，查看审批记录是否包括来访人员的访问范围；

g) **应检查机房区域划分是否合理，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) **应检查重要区域配置的电子门禁系统是否有验收文档或产品安全认证资质；**

i) **应检查电子门禁系统是否正常工作（不考虑断电后的工作情况）；查看是否有电子门禁系统运行和维护记录；查看监控进入机房重要区域的电子门禁系统记录，是否能够鉴别和记录进入人员的身份。**

7.1.1.2.3 结果判定

本项要求包括：

a) 如果有机房安全管理制度，指定了专人在机房出入口值守，对进入的人员登记在案并进行身份鉴别，对来访人员须经批准、限制和监控其活动范围，重要区域配置了电子门禁系统进行管理，则7.1.1.2.2 d）为肯定；

b) 如果7.1.1.2.2 d）-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。

7.1.1.3 防盗窃和防破坏

7.1.1.3.1 测评指标

见 GB/T 22239-2008 7.1.1.3。

7.1.1.3.2 测评实施

本项要求包括：

a) 应访谈物理安全负责人，采取了哪些防止设备、介质等丢失的保护措施；

b) 应访谈机房维护人员，询问**主要**设备放置位置是否做到安全可控，设备或主要部件是否进行了固定和标记，通信线缆是否铺设在隐蔽处；是否对机房安装的防盗报警系统和**监控报警系统**定期进行维护检查；

c) 应访谈资产管理员，介质是否进行了分类标识管理，介质是否存放在介质库或档案室内进行管理；

d) 应检查**主要**设备是否放置在机房内或其它不易被盗窃和破坏的可控范围内；检查**主要**设备或设备的主要部件的固定情况，查看其是否不易被移动或被搬走，是否设置明显的不易除去的标记；

e) 应检查通信线缆铺设是否在隐蔽处；

f) 应检查介质的管理情况，查看介质是否有正确的分类标识，是否存放在介质库或档案室中，**并且进行分类存放（满足磁介质、纸介质等的存放要求）**；

g) 应检查机房防盗报警设施是否正常运行，并查看是否有运行和报警记录；**应检查机房的摄像、传感等监控报警系统是否正常运行，并查看是否有运行记录、监控记录和报警记录；**

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 d）-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 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，询问为防止雷击事件采取了哪些防护措施，机房建筑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；**询问机房计算机系统接地是否设置了专用地线；是否在电源和信号线上安装避雷装置；**

b) 应检查机房建筑是否有避雷装置，是否有交流地线；

c) **应检查机房是否安装防雷保安器等装置。**

7.1.1.4.3 结果判定

如果7.1.1.4.2 b）和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。

7.1.1.5 防火

7.1.1.5.1 测评指标

见GB/T 22239-2008 7.1.1.5。

7.1.1.5.2 测评实施

本项要求包括：

a) 应访谈物理安全负责人，询问机房是否设置了灭火设备，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，**是否有专人负责维护该系统的运行，是否制定了有关机房消防的管理制度和消防预案，是否进行了消防培训；

b) 应访谈物理安全负责人，询问**机房及相关的工作房间和辅助房是否采用具有耐火等级的建筑材料；**

c) 应访谈机房维护人员，询问是否对火灾自动消防系统定期进行检查和维护；

d) 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**

摆放位置是否合理，其有效期是否合格；应检查**自动消防系统**是否正常工作，查看是否有运行记录、报警记录、定期检查和维修记录；

e) **应检查机房及相关的工作房间和辅助房是否采用具有耐火等级的建筑材料；**

f) **应检查机房是否采取区域隔离防火措施，将重要设备与其他设备隔离开。**

7.1.1.5.3 结果判定

如果7.1.1.5.2 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。

7.1.1.6 防水和防潮

7.1.1.6.1 测评指标

见GB/T 22239-2008 7.1.1.6。

7.1.1.6.2 测评实施

本项要求包括：

a) 应访谈物理安全负责人，询问机房是否部署了防水防潮措施；如果机房内有上下水管安装，是否避免穿过屋顶和活动地板下，穿过墙壁和楼板的水管是否采取了的保护措施；在湿度较高地区或季节是否有人负责机房防水防潮事宜，配备除湿装置；

b) 应访谈机房维护人员，询问机房是否没有出现过漏水和返潮事件；如果机房内有上下水管安装，是否经常检查其漏水情况；如果出现机房水蒸气结露和地下积水的转移与渗透现象是否及时采取防范措施；

c) 应检查穿过主机房墙壁或楼板的管道是否采取必要的防渗防漏等防水保护措施；

d) 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，机房及其环境是否不存在明显的漏水和返潮的威胁；如果出现漏水、渗透和返潮现象，则查看是否能够及时修复解决；

e) 对湿度较高的地区，应检查机房是否有湿度记录，是否有除湿装置并能够正常运行，是否有防止出现机房地下积水的转移与渗透的措施，是否有防水防潮处理记录**和除湿装置运行记录；**

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，是否有人负责其运行管理工作。**

7.1.1.6.3 结果判定

如果7.1.1.6.2 c）-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 7.1.1.7。

7.1.1.7.2 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**主要**设备是否采取必要的防静电措施，是否不存在静电问题或因静电引发的安全事件；**在静电较强地区的机房是否采取了有效的防静电措施，存在静电时是否及时采取消除静电的措施；**

b) 应检查主要设备是否有安全接地，查看机房是否不存在明显的静电现象；

c) **应检查机房是否采用了防静电地板；**

d) **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。**

7.1.1.7.3 结果判定

如果 7.1.1.7.2 b）-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。

7.1.1.8 温湿度控制

7.1.1.8.1 测评指标

见GB/T 22239-2008 7.1.1.8。

7.1.1.8.2 测评实施

本项要求包括：

a) 应访谈物理安全负责人，询问机房是否配备了温湿度自动调节设施，保证温湿度能够满足计算机设备运行的要求，是否在机房管理制度中规定了温湿度控制的要求，是否有人负责此项工作，是否定期检查和维护机房的温湿度自动调节设施，询问是否没有出现过温湿度影响系统运行的事件；

b) 应检查温湿度自动调节设施是否能够正常运行，查看是否有温湿度记录、运行记录和维护记录；查看机房温湿度是否满足计算站场地的技术条件要求。

7.1.1.8.3 结果判定

如果7.1.1.8.2 b）为肯定，则信息系统符合本单元测评指标要求，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 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；是否设置了短期备用电源设备，供电时间是否满足系统最低电力供应需求；**是否安装了冗余或并行的电力电缆线路；是否建立备用供电系统；**

b) 应检查机房，查看计算机系统供电线路上的稳压器、过电压防护设备和短期备用电源设备是否正常运行，**查看供电电压是否正常；**

c) 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**等电源设备的检查和维护记录，**冗余或并行的电力电缆线路切换记录，备用供电系统运行记录；以及上述计算机系统供电的运行记录，是否能够符合系统正常运行的要求；**

d) **应测试安装的冗余或并行的电力电缆线路，是否能够进行双路供电切换；**

e) **应测试备用供电系统是否能够在规定时间内正常启动和正常供电。**

7.1.1.9.3 结果判定

如果7.1.1.9.2 b）-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 7.1.1.10。

7.1.1.10.2 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**有防止外界电磁干扰和设备寄生耦合干扰的措施（包括设备外壳有良好的接地，电源线和通信线缆隔离等）；是否对处理秘密级信息的设备和磁介质采取了防止电磁泄漏的措施；**

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) **应检查关键设备和磁介质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 b）-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 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 7.1.2.1。

7.1.2.1.2 测评实施

本项要求包括：

a) 应访谈网络管理员，询问**主要**网络设备的性能以及目前业务高峰流量情况；

b) 应访谈网络管理员，询问网段划分情况以及划分的原则；询问重要网段有哪些，**其具体的部署位置，与其他网段的隔离措施有哪些；**

c) 应访谈网络管理员，询问网络中带宽控制情况以及带宽分配的原则；

d) **应访谈网络管理员，询问网络设备的路由控制策略有哪些，这些策略设计的目的是什么；**

e) 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；

f) 应检查网络设计或验收文档，查看是否有**主要**网络设备业务处理能力、接入网络及核心网络的带宽满足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；

g) 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；

h) **应检查边界和主要网络设备，查看是否配置路由控制策略以建立安全的访问路径；**

i) **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；**

j) **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

本项要求包括：

a) 如果 7.1.2.1.2 e）-g）缺少相应文档资料，则为否定；

b) 如果 7.1.2.1.2 e）-j）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 7.1.2.2。

7.1.2.2.2 测评实施

本项要求包括：

a) 应访谈安全管理员，询问网络访问控制措施有哪些；询问访问控制策略的设计原则是什么；询问是否允许拨号访问网络；

b) 应检查边界网络设备，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；**

c) **应检查边界网络设备，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；**

d) **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；**

e) **应检查边界和主要网络设备，查看重要网段是否采取了网络地址与数据链路地址绑定的措施；**

f) **应检查边界网络设备，查看重要网段是否采取一定的技术手段防止地址欺骗；**

g) 应检查边界网络设备查看其是否限制具有拨号访问权限的用户数量；

h) 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**；

i) **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是否不存在明显的弱点。**

7.1.2.2.3 结果判定

如果 7.1.2.2.2 b）-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。

7.1.2.3 安全审计

7.1.2.3.1 测评指标

见 GB/T 22239-2008 7.1.2.3。

7.1.2.3.2 测评实施

本项要求包括：

a) 应访谈安全审计员，询问边界和主要网络设备是否开启安全审计功能，审计内容包括哪些项；询问审计内容是什么；**对审计记录的处理方式有哪些；**

b) 应检查边界和**主要**网络设备，查看审计策略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；

c) 应检查边界和**主要**网络设备，查看事件审计记录是否包括：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；

d) **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；**

e) **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 b）-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。

7.1.2.4 边界完整性检查

7.1.2.4.1 测评指标

见 GB/T 22239-2008 7.1.2.4。

7.1.2.4.2 测评实施

本项要求包括：

a) 应访谈安全管理员，询问是否对内部用户私自连接到外部网络的行为以及**非授权设备私自接入到内部网络的行为**进行监控；

b) 应检查边界完整性检查设备，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；**

c) **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；**

d) **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 b）-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。

7.1.2.5 入侵防范

7.1.2.5.1 测评指标

见 GB/T 22239-2008 7.1.2.5。

7.1.2.5.2 测评实施

本项要求包括：

a) 应访谈安全管理员，询问网络入侵防范措施有哪些，是否有专门设备对网络入侵进行防范；**询问网络入侵防范规则库的升级方式；**

b) 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；

c) **应检查网络入侵防范设备，查看入侵事件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；**

d) 应检查网络入侵防范设备，查看其规则库是否为最新；

e) 应测试网络入侵防范设备，验证其检测策略是否有效；

f) **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 b）-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。

7.1.2.6 恶意代码防范

7.1.2.6.1 测评指标

见GB/T 22239-2008 7.1.2.6。

7.1.2.6.2 测评实施

本项要求包括：

a) **应访谈安全管理员，询问网络恶意代码防范措施是什么；询问恶意代码库的更新策略；**

b) **应检查网络设计或验收文档，查看其是否有在网络边界处对恶意代码采取相关措施的描述，防恶意代码产品是否有实时更新功能的描述；**

c) **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；**

d) **应检查防恶意代码产品，查看其运行是否正常，恶意代码库是否为最新版本。**

7.1.2.6.3 结果判定

本项要求包括：

a) 如果7.1.2.6.2 b）缺少相应文档资料，则为否定；

b) 如果7.1.2.6.2 b）-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。

7.1.2.7 网络设备防护

7.1.2.7.1 测评指标

见GB/T 22239-2008 7.1.2.7。

7.1.2.7.2 测评实施

本项要求包括：

a) 应访谈网络管理员，询问**主要**网络设备的防护措施有哪些；询问**主要**网络设备的登录和验证方式做过何种特定配置；询问远程管理的设备是否采取措施防止鉴别信息被泄漏；**询问网络特权用户的权限如何分配；**

b) 应访谈网络管理员，询问网络设备的口令策略是什么；

c) 应检查边界和**主要**网络设备，查看是否配置了登录用户身份鉴别功能，口令设置是否有复杂度和定期修改要求；

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，查看是否配置了鉴别失败处理功能；

f) 应检查边界和**主要**网络设备，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；

g) 应检查边界和**主要**网络设备，查看是否对**边界和主要**网络设备的管理员登录地址进行限制；**查看是否设置网络登录连接超时，并自动退出；查看是否实现设备特权用户的权限分离；**

h) 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 c）-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 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 7.1.3.1。

7.1.3.1.2 测评实施

本项要求包括：

a) 应访谈系统管理员和数据库管理员，询问操作系统和数据库管理系统的身份标识与鉴别机制采取何种措施实现；

b) 应访谈系统管理员和数据库管理员，询问对操作系统和数据库管理系统是否采用了远程管理，如采用了远程管理，查看是否采用了防止鉴别信息在网络传输过程中被窃听的措施；

c) 应检查**主要**服务器操作系统和**主要**数据库管理系统帐户列表，查看管理员用户名分配是否唯一；

d) 应检查**主要**服务器操作系统和**主要**数据库管理系统，查看是否提供了身份鉴别措施，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了要求和限制；

e) **应检查主要服务器操作系统和主要数据库管理系统，查看身份鉴别是否采用两个及两个以上身份鉴别技术的组合来进行身份鉴别；**

f) 应检查**主要**服务器操作系统和**主要**数据库管理系统，查看是否已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；

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 b）-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 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，查看匿名/默认用户的访问权限是否已被禁用或者严格限制，是否删除了系统中多余的、过期的以及共享的帐户；

c) 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；

d) 应检查**主要**数据库服务器的数据库管理员与操作系统管理员是否由不同管理员担任；

e) **应检查主要服务器操作系统和主要数据库管理系统，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；**

f) **应检查主要服务器操作系统和主要数据库管理系统，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 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。

7.1.3.3 安全审计

7.1.3.3.1 测评指标

见GB/T 22239-2008 7.1.3.3。

7.1.3.3.2 测评实施

本项要求包括：

a) 应访谈安全审计员，询问主机系统的安全审计策略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，查看安全审计配置是否符合安全审计策略的要求；

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，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；

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，查看是否对审计记录实施了保护措施，使其避免受到未预期的删除、修改或覆盖等；

e) **应检查主要服务器和重要终端操作系统，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；**

f) **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帐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 b）-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。

7.1.3.4 剩余信息保护

7.1.3.4.1 测评指标

见GB/T 22239-2008 7.1.3.4。

7.1.3.4.2 测评实施

本项要求包括：

a) **应检查主要操作系统和主要数据库管理系统维护操作手册，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 a）为肯定，则信息系统符合本单元测评指标要求，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 7.1.3.5。

7.1.3.5.2 测评实施

本项要求包括：

a) **应访谈系统管理员，询问是否采取入侵防范措施，入侵防范内容是否包括主机运行监视、特定进程监控、入侵行为检测和完整性检测等方面内容；**
b) **应检查入侵防范系统，查看是否能够记录攻击者的源 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）；**
c) **应检查重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；**
d) 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；
e) 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；
f) 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安装。

7.1.3.5.3 结果判定

如果 7.1.3.5.2 b）-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。

7.1.3.6 恶意代码防范

7.1.3.6.1 测评指标

见 GB/T 22239-2008 7.1.3.6。

7.1.3.6.2 测评实施

本项要求包括：

a) 应访谈系统安全管理员，询问主机系统是否采取恶意代码实时检测与查杀措施，恶意代码实时检测与查杀措施的部署覆盖范围如何；
b) 应检查**主要**服务器，查看是否安装了实时检测与查杀恶意代码的软件产品并进行及时更新；
c) 应检查防恶意代码产品是否实现了统一管理；
d) **应检查网络防恶意代码产品，查看其厂家名称、产品版本号和恶意代码库名称等，查看其是否与主机防恶意代码产品有不同的恶意代码库。**

7.1.3.6.3 结果判定

如果7.1.3.6.2 b）-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。

7.1.3.7 资源控制

7.1.3.7.1 测评指标

见 GB/T 22239-2008 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，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**主要**服务器操作系统，查看是否设置了单个用户对系统资源的最大或最小使用限度；
c) **应检查主要服务器操作系统，查看是否在服务水平降低到预先规定的最小值时，能检测和报警；**
d) **应检查主要服务器操作系统，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；**
e) 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。

7.1.3.7.3 结果判定

如果 7.1.3.7.2 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 7.1.4.1。

7.1.4.1.2 测评实施

本项要求包括：

a) 应访谈应用系统管理员，询问应用系统是否采取身份标识和鉴别措施，具体措施有哪些；系统采取何种措施防止身份鉴别信息被冒用；

b) 应访谈应用系统管理员，询问应用系统是否具有登录失败处理功能；

c) 应检查设计或验收文档，查看其是否有系统采用了保证唯一标识的措施的描述；

d) **应检查操作规程和操作记录，查看其是否有添加、删除用户和修改用户权限的操作规程、操作记录和审批记录；**

e) **应检查主要应用系统，查看其是否采用了两个及两个以上身份鉴别技术的组合来进行身份鉴别；**

f) 应检查**主要**应用系统，查看其是否提供身份标识和鉴别功能；查看其身份鉴别信息是否具有不易被冒用的特点；其鉴别信息复杂度检查功能是否能保证系统中不存在弱口令等；

g) 应检查**主要**应用系统，查看其提供的登录失败处理功能，是否根据安全策略配置了相关参数；

h) 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，查看是否成功，验证其身份标识和鉴别功能是否有效；

i) 应测试**主要**应用系统，验证其登录失败处理功能是否有效；

j) **应渗透测试主要应用系统，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

本项要求包括：

a) 如果7.1.4.1.2 c）中相关文档有系统采用了保证用户唯一性标识的措施的描述，则为肯定；

b) 如果7.1.4.1.2 d）缺少相应文档资料，则为否定；

c) 如果7.1.4.1.2 c）-j）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 7.1.4.2。

7.1.4.2.2 测评实施

本项要求包括：

a) 应访谈应用系统管理员，询问应用系统是否提供访问控制措施，以及具体措施和访问控制策略有哪些，访问控制的粒度如何；

b) 应检查**主要**应用系统，查看系统是否提供访问控制机制；是否依据安全策略控制用户对客体的访问；

c) 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；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；

d) 应检查**主要**应用系统，查看其是否有由授权用户设置其它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；

e) 应检查**主要**应用系统，查看系统是否授予不同帐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帐户的访问权限；

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 b）-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 7.1.4.3。

7.1.4.3.2 测评实施

本项要求包括：

a) 应访谈安全审计员，询问应用系统是否有安全审计功能，对事件进行审计的策略是什么，对审计日志的保护措施有哪些；

b) 应检查**主要**应用系统，查看其当前审计范围是否覆盖到每个用户；

c) 应检查**主要**应用系统，查看其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；

d) 应检查**主要**应用系统，查看其审计记录信息是否包括事件发生的日期与时间、触发事件的主体与客体、事件的类型、事件成功或失败、身份鉴别事件中请求的来源、事件的结果等内容；

e) **应检查主要应用系统，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分析功能，并能根据需要生成审计报表；**

f) 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；

g) 应测试**主要**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。

7.1.4.3.3 结果判定

如果7.1.4.3.2 b）-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。

7.1.4.4 剩余信息保护

7.1.4.4.1 测评指标

见 GB/T 22239-2008 7.1.4.4。

7.1.4.4.2 测评实施

本项要求包括：

a) **应访谈应用系统管理员，询问系统是否采取措施保证对存储介质中的残余信息进行删除（无论这些信息是存放在硬盘上还是在内存中），具体措施有哪些；**

b) **应检查设计或验收文档，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；**

c) **应检查设计或验收文档，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；**

d) **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

本项要求包括：

a) 如果7.1.4.4.2 b）和c）缺少相应文档资料，则为否定；

b) 如果7.1.4.4.2 b）-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。

7.1.4.5 通信完整性

7.1.4.5.1 测评指标

见GB/T 22239-2008 7.1.4.5。

7.1.4.5.2 测评实施

本项要求包括：

a) 应访谈安全管理员，询问应用系统是否具有在数据传输过程中保护其完整性的措施，具体措施是什么；

b) 应检查设计或验收文档，查看其是否有关于保护通信完整性的说明，**如果有则查看其是否有用密码技术来保证通信过程中数据的完整性的描述；**

c) 应测试**主要**应用系统，可通过获取通信双方的数据包，查看通信报文是否含有**加密**的验证码。

7.1.4.5.3 结果判定

如果7.1.4.5.2 b）和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。

7.1.4.6 通信保密性

7.1.4.6.1 测评指标

见GB/T 22239-2008 7.1.4.6。

7.1.4.6.2 测评实施

本项要求包括：

a) 应访谈安全管理员，询问应用系统数据在通信过程中是否采取保密措施，具体措施有哪些；

b) 应测试**主要**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；**查看系统在通信过程中，对整个报文或会话过程进行加密的功能是否有效。**

7.1.4.6.3 结果判定

如果7.1.4.6.2 b）为肯定，则信息系统符合本单元测评指标要求，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 7.1.4.7。

7.1.4.7.2 测评实施

本项要求包括：

a) **应访谈安全员，询问系统是否具有抗抵赖的措施，具体措施有哪些；**

b) **应测试主要应用系统，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；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 b）为肯定，则信息系统符合本单元测评指标要求，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 7.1.4.8。

7.1.4.8.2 测评实施

本项要求包括：

a) 应访谈应用系统管理员，询问应用系统是否具有保证软件容错能力的措施，具体措施有哪些；

b) 应检查**主要**应用系统，查看应用系统是否对人机接口输入或通信接口输入的数据进行有效性检验；

c) 应测试**主要**应用系统，可通过对人机接口输入的不同长度或格式的数据，查看系统的反应，验证系统人机接口有效性检验功能是否正确；

d) 应测试**主要应用系统，验证其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 b）-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。

7.1.4.9 资源控制

7.1.4.9.1 测评指标

见GB/T 22239-2008 7.1.4.9。

7.1.4.9.2 测评实施

本项要求包括：

a) 应访谈应用系统管理员，询问应用系统是否有资源控制的措施，具体措施有哪些；

b) 应检查**主要**应用系统，查看是否限制单个帐户的多重并发会话；系统是否有最大并发会话连接数的限制，**是否对一个时间段内可能的并发会话连接数进行限制；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；**

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

d) **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；**

e) **应测试主要应用系统，可通过对系统进行超过规定的单个帐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帐户的多重并发会话数；**

f) **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；**

g) 应测试重要应用系统，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。

7.1.4.9.3 结果判定

如果7.1.4.9.2 b）-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 7.1.5.1。

7.1.5.1.2 测评实施

本项要求包括：

a) 应访谈安全管理员，询问应用系统数据在**存储和**传输过程中是否有完整性保证措施，具体措施有哪些；**在检测到完整性错误时是否能恢复，恢复措施有哪些；**

b) 应检查**主要**主机操作系统、**主要**网络设备操作系统、**主要**数据库管理系统和**主要**应用系统，查看其是否配备检测**系统管理数据**、鉴别信息和重要业务数据在传输过程中完整性受到破坏的功能；**是否配备检测系统管理数据、鉴别信息和用户数据在存储过程中完整性受到破坏的功能；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 b）为肯定，则信息系统符合本单元测评指标要求，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 7.1.5.2。

7.1.5.2.2 测评实施

本项要求包括：

a) 应访谈网络管理员，询问**主要**网络设备的**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保密性，**是否采用加密或其他有效措施实现存储保密性；

b) 应访谈系统管理员，询问**主要**主机操作系统的**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保密性，**是否采用加密或其他有效措施实现存储保密性；

c) 应访谈数据库管理员，询问**主要**数据库管理系统的**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保密性，**是否采用加密或其他有效措施实现存储保密性；

d) 应访谈安全管理员，询问**主要**应用系统的**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保密性，**是否采用加密或其他有效措施实现存储保密性；

e) 应检查**主要**主机操作系统、**主要**网络设备操作系统、**主要**数据库管理系统和**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；

f) **应测试主要应用系统，通过用嗅探工具获取系统传输数据包，查看其是否采用了加密或其他有效措施实现传输保密性。**

7.1.5.2.3 结果判定

如果 7.1.5.2.2 e）和 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。

7.1.5.3 备份和恢复

7.1.5.3.1 测评指标

见 GB/T 22239-2008 7.1.5.3。

7.1.5.3.2 测评实施

本项要求包括：

a) 应访谈网络管理员，询问是否对网络设备中的配置文件进行备份，备份策略是什么；**完全数据备份是否每天一次，备份介质是否场外存放；是否提供异地数据备份功能；**当其受到破坏时，恢复策略是什么；是否提供**主要**网络设备、通信线路的硬件冗余；

b) 应访谈系统管理员，询问是否对操作系统中的重要信息进行备份，备份策略是什么；**完全数据备份是否每天一次，备份介质是否场外存放；是否提供异地数据备份功能；**当其受到破坏时，恢复策略是什么；是否提供**主要**服务器的硬件冗余；

c) 应访谈数据库管理员，询问是否对数据库管理系统中的**主要**数据进行备份，备份策略是什么；

完全数据备份是否每天一次，备份介质是否场外存放；是否提供异地数据备份功能；当其受到破坏时，恢复策略是什么；

d) 应访谈安全管理员，询问是否对应用系统中的应用程序进行备份，备份策略是什么；当其受到破坏时，恢复策略是什么；**完全数据备份是否每天一次，备份介质是否场外存放；是否提供异地数据备份功能**；

e) **应检查设计或验收文档，查看其是否有关于主要主机操作系统、网络设备操作系统、数据库管理系统和应用系统配置有本地和异地数据备份和恢复功能及策略的描述；**

f) 应检查**主要**主机操作系统、**主要**网络设备、**主要**数据库管理系统和**主要**应用系统，查看其是否提供备份和恢复功能，其配置是否正确，并且查看其备份结果是否与备份策略一致；

g) 应检查**主要**网络设备、**主要**通信线路和**主要**数据处理系统是否采用硬件冗余、软件配置等技术手段提供系统的高可用性；

h) **应检查网络拓扑结构是否不存在关键节点的单点故障。**

7.1.5.3.3 结果判定

本项要求包括：

a) 如果 7.1.5.3.2 e）缺少相应文档资料，则为否定；

b) 如果 7.1.5.3.2 e）-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。

7.2 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 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、建设和管理等层面的**各类管理内容**；

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 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 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，询问是否有专门的部门或人员负责制定安全管理制度；

b) 应访谈安全管理制度制、修订人员，询问安全管理制度的制定程序和发布方式，是否对制定的安全管理制度进行论证和审定，论证和评审方式如何，**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，是否有版本标识，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，查看收发是否通过正式、有效的方式（如正式发文、领导签署和单位盖章等），是否有发布范围要求。**

7.2.1.2.3 结果判定

如果7.2.1.2.2 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 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，评审周期多长，是否定期或不定期对安全管理制度进行检查、审定，由何部门或何人负责；**

b) **应访谈安全管理制度制、修订人员，询问对安全管理制度的安全检查及修订情况，评审、修订程序如何；**

c) **应访谈安全管理制度制、修订人员，询问系统发生重大安全事故、出现新的安全漏洞以及技术基础结构和组织结构等发生变更时是否对安全管理制度进行审定，对需要改进的制度是否进行修订；**

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；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 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。

7.2.2 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 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）；机构内部门设置情况如何，是否明确各部门的职责分工；**

c) 应访谈安全主管，询问信息系统设置了哪些工作岗位，各个岗位的职责分工是否明确；询问是否设立安全管理各个方面的负责人；

d) **应访谈安全主管、安全管理某方面的负责人、系统管理员、网络管理员和安全管理员，询问其岗位职责包括哪些内容；**

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、机房管理员、系统管理员、网络管理员、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；**查看文件是否明确各个岗位人员应具有的技能要求**；

f) **应检查信息安全管理委员会或领导小组最高领导是否具有委任授权书，查看授权书中是否有本单位主管领导的授权签字；**

g) **应检查信息安全管理委员会职责文件，查看是否明确委员会职责和其最高领导岗位的职责；**

h) **应检查安全管理各部门和信息安全管理委员会或领导小组是否具有日常管理工作执行情况的文件或工作记录。**

7.2.2.1.3 结果判定

如果7.2.2.1.2 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。

7.2.2.2 人员配备

7.2.2.2.1 测评指标

见GB/T 22239-2008 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人员的配备情况，包括数量、专职还是兼职等，**对关键事务的管理人员配备情况如何**；

b) **应检查人员配备要求管理文档，查看是否明确应配备哪些安全管理人员，是否包括机房管理员、系统管理员、数据库管理员、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；查看是否明确对哪些关键事务的管理人员应配备2人或2人以上共同管理，是否明确对配备人员的具体要求；**

c) 应检查安全管理各岗位人员信息表，查看其是否明确机房管理员、系统管理员、数据库管理员、网络管理员、安全管理员等重要岗位人员的信息，**确认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 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 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，审批部门是何部门，批准人是何人，他们的审批活动是否得到授权；**询问是否定期审查、更新审批项目，审查周期多长；**

b) 应访谈安全主管，询问其对重要活动的审批范围包括哪些，审批程序如何；

c) **应检查审批管理制度文档，查看文档中是否明确审批事项、需逐级审批的事项、审批部门、批准人及审批程序等，是否明确对系统变更、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；**

d) **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；**

e) **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 a）-e）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 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，询问是否建立与外单位（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）的沟通、合作机制，与外单位和其他部门有哪些合作内容，沟通、合作方式有哪些；与组织机构内其它部门之间及内部各部门管理人员之间是否建立沟通、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，组织其它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安全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安全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) 应检查是否有组织机构内部人员联系表；

g) **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；**

h) **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 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。

7.2.2.5 审核和检查

7.2.2.5.1 测评指标

见GB/T 22239-2008 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进行全面安全检查，检查周期多长，检查内容有哪些；**

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，检查周期多长；**询问系统全面安全检查情况，检查周期多长，检查人员有哪些，检查程序如何，是否对检查结果进行通报，通报形式、范围如何；**

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文件要求是否一致。**

7.2.2.5.3 结果判定

如果7.2.2.5.2 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 7.2.3.1。

7.2.3.1.2 测评实施

本项要求包括：

a) 应访谈安全主管，询问是否有专门的部门或人员负责人员的录用工作，由何部门/何人负责；

b) 应访谈人事管理相关人员，询问在人员录用时对人员条件有哪些要求，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，**是否与被录用人员都签署保密协议**；

c) **应访谈人事管理相关人员，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；**

d) 应检查人员录用要求管理文档，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、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；

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的签字等内容；

h) **应检查岗位安全协议，查看是否有岗位安全责任、违约责任、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 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。

7.2.3.2 人员离岗

7.2.3.2.1 测评指标

见 GB/T 22239-2008 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，询问对即将离岗人员有哪些控制方法，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) 应访谈人事管理相关人员，询问调离手续包括哪些，**是否要求关键岗位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) 应检查是否具有对离岗人员的安全处理记录（如交还身份证件、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；

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 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 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，询问是否有人负责定期对各个岗位人员进行安全技能及安全知识的考核；

b) 应访谈人事管理相关人员员，询问对各个岗位人员的考核情况，考核周期多长，考核内容有哪些；**询问对人员的安全审查情况，审查人员是否包含所有岗位人员，审查内容有哪些；对关键岗位人员的审查和考核是否有特殊要求；**

c) 应检查考核文档**和记录**，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，是否有对关键岗位人员特殊的考核内容**；查看记录日期与考核周期是否一致；

d) **应检查人员安全审查记录，查看记录的审查人员是否包括各个岗位的人员，是否有对关键岗位人员特殊的安全审查内容。**

7.2.3.3.3 结果判定

如果 7.2.3.3.2 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。

7.2.3.4 安全意识教育和培训

7.2.3.4.1 测评指标

见 GB/T 22239-2008 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，具体的培训方式有哪些；是否对违反安全策略和规定的人员进行惩戒，如何惩戒；

b) 应访谈安全管理员、系统管理员、网络管理员和**数据库管理员**，考查其对工作相关的信息安全基础知识、安全责任和惩戒措施等的理解程度；

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) 应检查是否具有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 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。

7.2.3.5 外部人员访问管理

7.2.3.5.1 测评指标

见GB/T 22239-2008 7.2.3.5。

7.2.3.5.2 测评实施

本项要求包括：

a) 应访谈安全管理员，询问对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）采取了哪些安全措施，是否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）和外部人员离开的条件等；**

c) **应检查外部人员访问重要区域的批准文档，查看是否有外部人员访问重要区域的书面申请，是否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、**访问设备或信息**及陪同人等。

7.2.3.5.3 结果判定

如果7.2.3.5.2 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 7.2.4.1。

7.2.4.1.2 测评实施

本项要求包括：

a) 应访谈安全主管，询问确定信息系统安全保护等级的方法是否参照定级指南的指导，定级过程是否有书面描述；**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，**定级结果是否获得了相关部门的批准；

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，查看是否说明定级的方法和理由，查看定级结果是否有相关部门的批准盖章；

c) **应检查专家论证文档，查看是否有专家对定级结果的论证意见。**

7.2.4.1.3 结果判定

本项要求包括：

a) 如果7.2.4.1.2 a）单位没有上级主管部门，但定级结果有本单位信息安全主管领导的批准，则为肯定；

b) 如果7.2.4.1.2 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 7.2.4.2。

7.2.4.2.2 测评实施

本项要求包括：

a) **应访谈安全主管，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，询问是否根据系统的安全级别选择基本安全措施，是否依据风险分析的结果补充和调整安全措施，具体做过哪些调整；

c) **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，是否经过论证和审定，是否**

经过审批，是否根据等级测评、安全评估的结果定期调整和修订，维护周期多长；

d) **应检查系统的安全建设工作计划，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) 应检查专家论证文档，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，查看维护记录日期间隔与维护周期是否一致。**

7.2.4.2.3 结果判定

如果7.2.4.2.2 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 7.2.4.3。

7.2.4.3.2 测评实施

本项要求包括：

a) 应访谈安全主管，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，询问信息安全产品的采购情况，**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，采购过程如何控制，**是否定期审定和更新候选产品名单，审定周期多长；**

c) 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；

d) **应检查产品采购管理文档，查看内容是否明确需要的产品性能指标，确定产品的候选范围，通过招投标等方式确定采购产品及人员行为准则等方面；**

e) 应检查系统使用的有关信息安全产品是否符合国家的有关规定；

f) 应检查密码产品的使用情况是否符合密码产品使用、管理的相关规定；

g) **应检查是否具有产品选型测试结果记录、候选产品名单审定记录或更新的候选产品名单。**

7.2.4.3.3 结果判定

如果 7.2.4.3.2 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。

7.2.4.4 自行软件开发

7.2.4.4.1 测评指标

见 GB/T 22239-2008 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编写、调试和完成；

b) 应访谈系统建设负责人，询问软件设计相关文档和使用指南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，询问其是否参照代码编写安全规范进行软件开发，开发之后是否交给测试人员测试软件；**

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，是否明确软件开发相关文档的管理等；

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；**

f) 应检查是否具有软件设计的相关文档（应用软件设计程序文件、源代码文档等）、软件使用指南或操作手册和维护手册等；

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（软件设计和开发程序文件、测试数据、测试结果、维护手册等）的使用控制记录。**

7.2.4.4.3 结果判定

如果7.2.4.4.2 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。

7.2.4.5 外包软件开发

7.2.4.5.1 测评指标

见 GB/T 22239-2008 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，**检测工具是否是第三方的商业产品**；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；

b) 应检查是否具有需求分析说明书、软件设计说明书、软件操作手册、软件源代码文档等软件开发文档和使用指南；

c) 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 7.2.4.5.4 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。

7.2.4.6 工程实施

7.2.4.6.1 测评指标

见 GB/T 22239-2008 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，询问是否有专门部门或人员负责工程实施管理工作，由何部门/何人负责，是否按照工程实施方案的要求对工程实施过程进行进度和质量控制，**是否要求工程实施单位提供其能够安全实施系统建设的资质证明和能力保证；**

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；

c) **应检查是否具有按照实施方案形成的阶段性工程报告等文档；**

d) **应检查工程实施管理制度，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。**

7.2.4.6.3 结果判定

如果 7.2.4.6.2 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 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对系统测试验收报告进行审定；

c) 应检查工程测试验收方案，查看其是否明确说明参与测试的部门、人员、测试验收的内容、现场操作过程等内容；

d) 应检查测试验收记录是否详细记录了测试时间、人员、现场操作过程和测试验收结果等方面内容；

e) **应检查是否具有系统安全性测试报告，查看报告是否给出测试通过的结论（如果报告中提出了存在的问题，则检查是否有针对这些问题的改进报告），是否有第三方测试机构的签字或盖章**；

f) 应检查是否具有系统测试验收报告，是否有对测试验收报告的审定文档，查看文档是否有相关人员的审定意见；

g) **应检查测试验收管理文档是否包括系统测试验收的过程控制方法、参与人员的行为规范等内容。**

7.2.4.7.3 结果判定

如果 7.2.4.7.2 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。

7.2.4.8 系统交付

7.2.4.8.1 测评指标

见 GB/T 22239-2008 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，**系统交接时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，询问目前的信息系统是否由内部人员独立运行维护，如果是，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**分类详细列项**系统交付的各类设备、软件、文档等；

d) 应检查是否具有系统建设文档、指导用户进行系统运维的文档、系统培训手册等；

e) **应检查系统交付管理文档，查看其是否包括交付过程的控制方法和对交付参与人员的行为限制等方面内容；**

f) 应检查培训记录，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 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 7.2.4.9。

7.2.4.9.2 测评实施

本项要求包括：

a) **应访谈安全主管，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；**

b) **应访谈文档管理员，询问对系统定级相关备案文档采取哪些控制措施；**

c) **应检查是否具有将系统等级相关材料报主管部门备案的记录或备案文档；**

d) **应检查是否具有将系统等级相关备案材料报相应公安机关备案的记录或证明；**

e) **应检查是否具有系统定级相关材料的使用控制记录。**

7.2.4.9.3 结果判定

如果7.2.4.9.2 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。

7.2.4.10 安全服务商选择

7.2.4.10.1 测评指标

见 GB/T 22239-2008 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，查看是否包括服务内容、服务期限、双方签字或盖章等。

7.2.4.10.3 结果判定

如果 7.2.4.10.2 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 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基础设施进行定期维护，由何部门或何人负责，维护周期多长，是否有**专门的部门**和人员负责机房环境安全管理工作；

b) 应访谈安全主管，询问为保证办公环境的保密性采取了哪些控制措施；

c) 应检查机房安全管理制度，查看其内容是否覆盖机房物理访问、物品带进和带出机房、机房环境安全等方面；

d) **应检查办公环境管理文档，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、人员调离办公室时立即收回钥匙、不在办公区接待来访人员等方面内容；**

e) **应检查机房基础设施维护记录，查看是否记录维护日期、维护人、维护设备、故障原因、维护结果等方面内容**。

7.2.5.1.3 结果判定

如果7.2.5.1.2 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。

7.2.5.2 资产管理

7.2.5.2.1 测评指标

见 GB/T 22239-2008 7.2.5.2。

7.2.5.2.2 测评实施

本项要求包括：

a) 应访谈安全主管，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) **应访谈资产管理员，询问是否依据资产的重要程度对资产进行分类和标识管理，不同类别的资产是否采取不同的管理措施；**

c) 应检查资产清单，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；

d) 应检查资产安全管理制度，查看其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、**传输、存储**、维护等方面；

e) **应检查信息分类文档，查看其内容是否明确了信息分类标识的原则和方法。**

7.2.5.2.3 结果判定

如果7.2.5.2.2 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。

7.2.5.3 介质管理

7.2.5.3.1 测评指标

见 GB/T 22239-2008 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、介质内存储信息被未授权修改以及非法泄漏等，是否有专人管理；

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，**是否定期对其完整性（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**根据所承载数据和软件的重要性**对介质进行分类和标识管理；

c) 应访谈资产管理员，询问**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，**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；**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；**

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) 应检查介质管理记录，查看其是否记录介质的**存储**、归档、查询和借用等情况；

f) **应检查介质管理制度，查看其内容是否覆盖介质的存放环境、使用、维护和销毁等方面；**

g) 应检查介质，查看是否对其进行了分类，并具有不同标识。

7.2.5.3.3 结果判定

如果7.2.5.3.2 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。

7.2.5.4 设备管理

7.2.5.4.1 测评指标

见GB/T 22239-2008 7.2.5.4。

7.2.5.4.2 测评实施

本项要求包括：

a) 应访谈资产管理员，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，对各类测试工具进行有效性检查，由何部门/何人负责，维护周期多长；

b) 应访谈资产管理员，询问是否对设备选用的各个环节（选型、采购、发放和领用、**涉外维修和服务**及信息处理设备带离机构等）进行审批控制；

c) 应访谈安全审计员，询问对**主要**设备（包括备份和冗余设备）的操作是否建立日志，日志文件如何管理，是否定期检查管理情况；

d) 应检查设备安全管理制度，查看其内容是否明确对各种软硬件设备的选型、采购、发放和领用以及带离机构等环节进行申报和审批；

e) **应检查配套设施、软硬件维护方面的管理制度，查看其是否对配套设施、软硬件维护进行有效的管理，包括明确维护人员的责任、涉外维修和服务的审批、维修过程的监督控制管理等；**

f) 应检查设备使用管理文档，查看其内容是否覆盖终端计算机、便携机和网络设备等使用、操作原则、注意事项等方面；

g) 应检查**主要**设备（包括备份和冗余设备）的操作规程，查看其内容是否覆盖服务器如何启动、停止、加电、断电等操作；

h) **应检查是否具有设备的选型、采购、发放和领用以及带离机构等的申报材料和审批报告；**

i) **应检查是否具有设备维护记录和主要设备的操作日志。**

7.2.5.4.3 结果判定

如果7.2.5.4.2 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。

7.2.5.5 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 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，询问是否建立安全管理中心，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管理中心，安全管理中心是否对设备状态、恶意代码、补丁升级、安全审计等安全相关事项进行集中管理；**

d) **应检查监控记录，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；**

e) **应检查监测分析报告，查看是否包括监测的异常现象、处理措施等。**

7.2.5.5.3 结果判定

如果7.2.5.5.2 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。

7.2.5.6 网络安全管理

7.2.5.6.1 测评指标

见GB/T 22239-2008 7.2.5.6。

7.2.5.6.2 测评实施

本项要求包括：

a) 应访谈安全主管，询问是否指定**专人**负责维护网络运行日志、监控记录和分析处理报警信息等网络安全管理工作；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；

b) 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（帐户数据、设备配置文件等）进行备份，采取什么方式；

c) **应访谈网络管理员，询问是否实现网络设备的最小服务配置，对配置文件是否进行定期离线备份，采取什么方式；是否定期检查拨号上网等违反网络安全策略的行为；**

d) 应访谈安全管理员，询问是否定期对网络设备进行漏洞扫描，扫描周期多长，发现漏洞是否及时修补；

e) 应检查网络漏洞扫描报告，查看其内容是否包含网络存在的漏洞、严重级别和结果处理等方面，检查扫描时间间隔与扫描周期是否一致；

f) 应检查网络安全管理制度，查看其是否覆盖网络安全配置、安全策略、升级与打补丁、**最小服**

务、授权访问、日志保存时间、口令更新周期、**文件备份**等方面内容，**查看安全策略是否包括允许或者拒绝便携式和移动式设备的网络接入；**

g) 应检查是否具有内部网络外联的授权批准书；

h) 应检查是否具有网络设备配置文件的**离线备份文件**；

i) 应检查是否具有网络审计日志，检查日志是否在规定的保存时间范围内。

7.2.5.6.3 结果判定

如果7.2.5.6.2 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 7.2.5.7。

7.2.5.7.2 测评实施

本项要求包括：

a) 应访谈安全主管，询问是否**指定专人对系统进行管理，对系统管理员用户是否进行分类，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**；

b) 应访谈系统管理员，询问是否根据业务需求和系统安全分析制定系统的访问控制策略，控制分配信息系统、文件及服务的访问权限；

c) 应访谈系统管理员，询问是否定期对系统安装安全补丁程序，在安装系统补丁前是否对重要文件进行备份，采取什么方式进行，是否先在测试环境中测试通过再安装；

d) 应访谈安全管理员，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；

e) 应检查系统安全管理制度，查看其内容是否覆盖系统安全策略、安全配置、日志管理、日常操作流程等具体内容；

f) 应检查是否有详细操作日志(包括重要的日常操作、运行维护记录、参数的设置和修改等内容)；

g) 应检查是否有定期对运行日志和审计结果进行分析的**分析报告，查看报告是否能够记录帐户的连续多次登录失败、非工作时间的登录、访问受限系统或文件的失败尝试、系统错误等非正常事件；**

h) 应检查系统漏洞扫描报告，查看其内容是否包含系统存在的漏洞、严重级别和结果处理等方面，检查扫描时间间隔与扫描周期是否一致。

7.2.5.7.3 结果判定

如果7.2.5.7.2 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。

7.2.5.8 恶意代码防范管理

7.2.5.8.1 测评指标

见GB/T 22239-2008 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；

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) 应检查恶意代码防范管理文档，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 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 7.2.5.9。

7.2.5.9.2 测评实施

本项要求包括：

a) 应访谈安全管理员，询问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管理制度。

7.2.5.9.3 结果判定

如果7.2.5.9.2 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 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，询问是否制定变更方案指导系统执行变更，**目前系统发生过哪些变更，变更方案是否经过评审，变更过程是否文档化**；

b) 应访谈系统运维负责人，询问重要系统变更前是否**根据申报和审批程序**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) **应访谈系统运维负责人，询问变更失败后的恢复程序、工作方法和人员职责是否文档化，恢复过程是否经过演练；**

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、变更前评估等方面内容；

e) 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；

f) **应检查变更管理制度，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；**

g) **应检查变更控制的申报、审批程序，查看其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；**

h) **应检查变更失败恢复程序，查看其是否规定变更失败后的恢复流程；**

i) **应检查是否具有变更方案评审记录和变更过程记录文档。**

7.2.5.10.3 结果判定

如果 7.2.5.10.2 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。

7.2.5.11 备份与恢复管理

7.2.5.11.1 测评指标

见GB/T 22239-2008 7.2.5.11。

7.2.5.11.2 测评实施

本项要求包括：

a) 应访谈系统管理员、数据库管理员和网络管理员，询问是否识别出需要定期备份的业务信息、

系统数据及软件系统，主要有哪些；

b) **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；**

c) 应检查**备份和恢复管理制度**，查看其是否明确备份方式、备份频度、存储介质和保存期等方面内容；

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

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。**

7.2.5.11.3 结果判定

如果7.2.5.11.2 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。

7.2.5.12 安全事件处置

7.2.5.12.1 测评指标

见 GB/T 22239-2008 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，**不同安全事件是否采取不同的处理和报告程序**；

b) 应访谈系统运维负责人，询问是否根据本系统已发生的和需要防止发生的安全事件对系统的影响程度划分不同等级，划分为几级，划分方法是否参照了国家相关管理部门的技术资料，主要参照哪些；

c) 应检查安全事件报告和处置管理制度，查看其是否明确本系统已发生的和需要防止发生的安全事件类型，是否明确安全事件的现场处理、事件报告和后期恢复的管理职责；

d) 应检查安全事件定级文档，查看其是否明确安全事件的定义、安全事件等级划分原则、等级描述等方面内容；

e) 应检查安全事件记录分析文档，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，**不同安全事件是否采取不同措施避免其再次发生**；

f) **应检查安全事件报告和处理程序文档，查看其是否根据不同安全事件制定不同的处理和报告程序，及响应和处置的范围、程度、处理方法，是否明确具体报告方式、报告内容、报告人等方面内容。**

7.2.5.12.3 结果判定

如果 7.2.5.12.2 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。

7.2.5.13 应急预案管理

7.2.5.13.1 测评指标

见 GB/T 22239-2008 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，**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**；

b) **应访谈系统运维负责人，询问是否具有应急预案小组，是否具备应急设备并能正常工作，应急预案执行所需资金是否做过预算并能够落实；**

c) 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；

d) 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；

e) **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；**

f) 应检查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 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 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 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，询问现有机房和办公场地（放置终端计算机设备）的环境条件是否能够满足信息系统业务需求和安全管理需求，是否具有基本的防震、防风和防雨等能力；询问机房场地是否符合选址要求，**机房与办公场地是否尽量安排在一起或物理位置较近的地方；**

b) 应访谈机房维护人员，询问是否存在因机房和办公场地环境条件引发的安全事件或安全隐患；如果某些环境条件不能满足，是否及时采取了补救措施；

c) **应检查机房和办公场地的设计或验收文档，是否有机房和办公场地所在建筑能够具有防震、防风和防雨等能力的说明；是否有机房场地的选址说明；是否与机房和办公场地实际情况相符合；**

d) 应检查机房和办公场地是否在具有防震、防风和防雨等能力的建筑内；

e) 应检查机房场地是否不在建筑物的高层或地下室，以及用水设备的下层或隔壁。

8.1.1.1.3 结果判定

如果 8.1.1.1.2 c）-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 8.1.1.2。

8.1.1.2.2 测评实施

本项要求包括：

a) 应访谈物理安全负责人，了解部署了哪些控制人员进出机房的保护措施；

b) 应访谈物理安全负责人，如果业务或安全管理需要，是否对机房进行了划分区域管理，是否对各个区域都有专门的管理要求；**是否严格控制来访人员进入或一般不允许来访人员进入；**

c) 应访谈机房值守人员，询问是否认真执行有关机房出入的管理制度，是否对进入机房的**来访人员**记录在案；

d) 应检查机房安全管理制度，查看是否有关于机房出入方面的规定；

e) 应检查机房出入口是否有专人值守，是否有值守记录以及进出机房的来访人员登记记录；检查机房是否不存在电子门禁系统控制之外的其他出入口；

f） 应检查是否有来访人员进入机房的审批记录，**进出机房的有关记录是否保存足够的时间；**

g） 应检查机房区域划分是否合理，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） 应检查机房和重要区域配置的电子门禁系统是否有验收文档或产品安全认证资质；

i） **应检查每道电子门禁系统是否都能正常工作；查看是否有每道电子门禁系统的运行和维护记录；查看监控进入机房的电子门禁系统记录，是否能够鉴别和记录进入人员的身份。**

8.1.1.2.3 结果判定

本项要求包括：

a） 如果8.1.1.2.2 a）访谈回答内容包括：指定了专人在机房出入口值守，对进入的来访人员登记在案并进行身份鉴别，对来访人员须经批准、限制和监控其活动范围，机房配置了电子门禁系统，重要区域配置了第二道电子门禁系统，则为肯定；

b） 如果8.1.1.2.2 d）检查结果包括：制定了机房出入的管理制度，指定了专人在机房出入口值守，对进入的来访人员登记在案并进行身份鉴别，对来访人员须经批准、限制和监控其活动范围，两道电子门禁系统的管理，则为肯定；

c） 如果8.1.1.2.2 a）、d）- 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。

8.1.1.3 防盗窃和防破坏

8.1.1.3.1 测评指标

见GB/T 22239-2008 8.1.1.3。

8.1.1.3.2 测评实施

本项要求包括：

a） 应访谈物理安全负责人，采取了哪些防止设备、介质等丢失的保护措施；

b） 应访谈机房维护人员，询问主要设备放置位置是否做到安全可控，设备或主要部件是否进行了固定和标记，通信线缆是否铺设在隐蔽处；是否对机房安装的防盗报警系统和监控报警系统定期进行维护检查；

c） 应访谈资产管理员，介质是否进行了分类标识管理，介质是否存放在介质库或档案室内进行管理；

d） 应检查主要设备是否放置在机房内或其它不易被盗窃和破坏的可控范围内；检查主要设备或设备的主要部件的固定情况，查看其是否不易被移动或被搬走，是否设置明显的不易除去的标记；**是否有设备物理位置图，是否经常检查设备物理位置的变化；**

e） 应检查通信线缆铺设是否在隐蔽处；

f） 应检查介质的管理情况，查看介质是否有正确的分类标识，是否存放在介质库或档案室中；

g） 应检查机房防盗报警设施是否正常运行，并查看是否有运行和报警记录；应检查机房的摄像、传感等监控报警系统是否正常运行，并查看是否有运行记录、监控记录和报警记录；

h） **应检查是否有通信线路布线文档、介质清单和使用记录，**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；

i） **应检查通信线缆铺设情况，查看通信线缆铺设实际情况是否与相关文档的条文相一致。**

8.1.1.3.3 结果判定

如果8.1.1.3.2 d）-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。

8.1.1.4 防雷击

8.1.1.4.1 测评指标

见GB/T 22239-2008 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，询问为防止雷击事件导致重要设备被破坏采取了哪些防护措施，机房建筑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；询问机房计算机系统接地是否设置了专用地线，是否在电源和信号线上安装避雷装置；

b) **应访谈机房维护人员，询问机房建筑避雷装置是否有人定期进行检查和维护；询问机房交流工作接地、安全保护接地和防雷接地等是否符合机房设计相关国家标准的要求；**

c) **应检查机房是否有建筑防雷设计或验收文档，查看是否有地线连接要求的描述，与实际情况是否一致；**

d) 应检查机房是否在电源和信号线上安装避雷装置；

e) **应测试机房安全保护地、防雷保护地、交流工作地的接地电阻，是否达到接地电阻的相关国家标准要求。**

8.1.1.4.3 结果判定

如果8.1.1.4.2 c）-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 8.1.1.5。

8.1.1.5.2 测评实施

本项要求包括：

a) 应访谈物理安全负责人，询问机房是否设置了灭火设备，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，是否有专人负责维护该系统的运行，是否制定了有关机房消防的管理制度和消防预案，是否进行了消防培训；

b) 应访谈物理安全负责人，询问机房及相关的工作房间和辅助房是否采用具有耐火等级的建筑材料；

c) 应访谈机房维护人员，询问是否对火灾自动消防系统定期进行检查和维护；

d) **应访谈机房值守人员，询问对机房出现的消防安全隐患是否能够及时报告并得到排除；是否参加过机房灭火设备的使用培训，是否能够正确使用灭火设备和自动消防系统；是否能够做到随时注意防止和消灭火灾隐患；**

e) 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，自动消防系统摆放位置是否合理，其有效期是否合格；应检查自动消防系统是否正常工作，查看是否有运行记录、报警记录、定期检查和维修记录；

f) **应检查是否有机房消防方面的管理制度文档；检查是否有机房防火设计或验收文档；检查是否有机房自动消防系统的设计或验收文档，文档是否与现有消防配置状况一致；检查是否有机房及相关房间的建筑材料、区域隔离防火措施的验收文档或消防检查验收文档；**

g) 应检查机房及相关的工作房间和辅助房是否采用具有耐火等级的建筑材料；

h) 应检查机房是否采取区域隔离防火措施，将重要设备与其他设备隔离开。

8.1.1.5.3 结果判定

如果8.1.1.5.2 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。

8.1.1.6 防水和防潮

8.1.1.6.1 测评指标

见GB/T 22239-2008 8.1.1.6。

8.1.1.6.2 测评实施

本项要求包括：

a) 应访谈物理安全负责人，询问机房是否部署了防水防潮措施；如果机房内有上/下水管安装，是否避免穿过屋顶和活动地板下，穿过墙壁和楼板的水管是否采取了保护措施；在湿度较高地区或季节是否有人负责机房防水防潮事宜，配备除湿装置；

b) 应访谈机房维护人员，询问机房是否没有出现过漏水和返潮事件；如果机房内有上/下水管安装，是否经常检查其漏水情况；如果出现机房水蒸气结露和地下积水的转移与渗透现象是否及时采取防范措施；

c) **应检查机房是否有建筑防水和防潮设计或验收文档，文档是否与机房防水防潮的实际情况相一致；**

d) 应检查穿过主机房墙壁或楼板的管道是否采取必要的防渗防漏等防水保护措施；

e) 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，机房及其环境是否不存在明显的漏水和返潮的威胁；如果出现漏水、渗透和返潮现象，则查看是否能够及时修复解决；

f) 对湿度较高的地区，应检查机房是否有湿度记录，是否有除湿装置并能够正常运行，是否有防止出现机房地下积水的转移与渗透的措施，是否有防水防潮处理记录和除湿装置运行记录；

g) 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，是否有人负责其运行管理工作。

8.1.1.6.3 结果判定

如果8.1.1.6.2 c）-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。

8.1.1.7 防静电

8.1.1.7.1 测评指标

见GB/T 22239-2008 8.1.1.7。

8.1.1.7.2 测评实施

本项要求包括：

a) 应访谈物理安全负责人，询问机房主要设备是否采取必要的接地防静电措施，是否不存在静电问题或因静电引发的安全事件；在静电较强地区的机房是否采取了有效的防静电措施，存在静电时是否及时采取消除静电的措施；

b) **应检查机房是否有防静电设计或验收文档，查看其描述内容与实际情况是否一致；**

c) 应检查主要设备是否有安全接地，查看机房是否不存在明显的静电现象；

d) 应检查机房是否采用了防静电地板；

e) 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

本项要求包括：

a) 8.1.1.7.2 e）有效的防静电措施，可以包括如防静电工作台、静电消除剂和静电消除器等措施的部分或全部；

b) 如果8.1.1.7.2 b）-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。

8.1.1.8 温湿度控制

8.1.1.8.1 测评指标

见GB/T 22239-2008 8.1.1.8。

8.1.1.8.2 测评实施

本项要求包括：

a) 应访谈物理安全负责人，询问机房是否配备了温湿度自动调节设施，保证温湿度能够满足计算机设备运行的要求，是否在机房管理制度中规定了温湿度控制的要求，是否有人负责此项工作，是否定期检查和维护机房的温湿度自动调节设施；询问是否没有出现过温湿度影响系统运行的事件；

b) **应检查机房是否有温湿度控制设计或验收文档，是否能够满足系统运行需要，是否与当前实际情况相符；**

c) 应检查温湿度自动调节设施是否能够正常运行，查看是否有温湿度记录、运行记录和维护记录；查看机房温湿度是否满足计算站场地的技术条件要求。

8.1.1.8.3 结果判定

如果8.1.1.8.2 b）和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。

8.1.1.9 电力供应

8.1.1.9.1 测评指标

见 GB/T 22239-2008 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；是否设置了短期备用电源设备，供电时间是否满足系统最低电力供应需求；是否安装了冗余或并行的电力电缆线路；是否建立备用供电系统；

b) **应访谈机房维护人员，询问冗余或并行的电力电缆线路在双路供电切换时是否能够对计算机系统正常供电；备用供电系统是否能够在规定时间内正常启动和正常供电；**

c) **应检查机房是否有电力供应安全设计或验收文档，查看文档中是否标明配备稳压器、过电压防护设备、备用电源设备、冗余或并行的电力电缆线路以及备用供电系统等要求；查看与机房电力供应实际情况是否一致；**

d) 应检查机房，查看计算机系统供电线路上的稳压器、过电压防护设备和短期备用电源设备是否正常运行，查看供电电压是否正常；

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，冗余或并行的电力电缆线路切换记录，备用供电系统运行记录；以及上述计算机系统供电的运行记录，是否能够符合系统正常运行的要求；

f) 应测试安装的冗余或并行的电力电缆线路，是否能够进行双路供电切换；

g) 应测试备用供电系统是否能够在规定时间内正常启动和正常供电。

8.1.1.9.3 结果判定

如果8.1.1.9.2 c）-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。

8.1.1.10 电磁防护

8.1.1.10.1 测评指标

见 GB/T 22239-2008 8.1.1.10。

8.1.1.10.2 测评实施

本项要求包括：

a) 应访谈物理安全负责人，询问是否有防止外界电磁干扰和设备寄生耦合干扰的措施；是否对处理秘密级信息的设备和磁介质采取了防止电磁泄漏的措施；**是否在必要时对机房采用了电子屏蔽或安装屏蔽机房；**

b) **应访谈机房维护人员，询问是否对设备外壳做了良好的接地；是否做到电源线和通信线缆隔离；是否出现过因电磁防护问题引发的故障；处理秘密级信息的设备是否为低辐射设备；重**

要设备和磁介质是否存放在具有电磁屏蔽功能的容器中；

c) **应检查机房是否有电子屏蔽或屏蔽机房设计或验收文档；是否有电子屏蔽或屏蔽机房的管理制度文档；**

d) 应检查机房设备外壳是否有安全接地；

e) 应检查机房布线，查看是否做到电源线和通信线缆隔离；

f) 应检查关键设备和磁介质是否存放在具有电磁屏蔽功能的容器中；

g) **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；**

h) **对屏蔽机房，应检查是否有定期测试电磁泄漏的报告；**

i) **对屏蔽机房，应测试机房的电磁泄漏状况。**

8.1.1.10.3 结果判定

如果8.1.1.10.2 c）-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。

8.1.2 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 8.1.2.1。

8.1.2.1.2 测评实施

本项要求包括：

a) 应访谈网络管理员，询问网络设备的性能以及目前业务高峰流量情况；

b) 应访谈网络管理员，询问网段划分情况以及划分原则；询问重要网段有哪些，其具体的部署位置，与其他网段的隔离措施有哪些；

c) 应访谈网络管理员，询问网络的带宽情况；询问网络中带宽控制情况以及带宽分配的原则；

d) 应访谈网络管理员，询问网络设备的路由控制策略有哪些，这些策略设计的目的是什么；

e) 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；

f) 应检查网络设计或验收文档，查看是否有网络设备业务处理能力、接入网络及核心网络的带宽满足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；

g) 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；

h) 应检查边界和网络设备，查看是否配置路由控制策略以建立安全的访问路径；

i) 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；

j) 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

本项要求包括：

a) 如果 8.1.2.1.2 e）-g）缺少相应文档资料，则为否定；

b) 如果 8.1.2.1.2 e）-j）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 8.1.2.2。

8.1.2.2.2 测评实施

本项要求包括：

a) 应访谈安全管理员，询问网络访问控制措施有哪些；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**；询问是否不允许远程拨号访问网络；

b) **应检查网络设计或验收文档，查看其是否有根据数据的敏感标记允许或拒绝数据通过，不提供拨号访问网络功能的描述；**

c) **应检查边界网络设备，查看是否有相应的访问控制措施来实现禁止数据带通用协议通过；**

d) **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；**

e) **应检查边界网络设备，查看是否禁用远程拨号访问功能；**

f) **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 b）-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。

8.1.2.3 安全审计

8.1.2.3.1 测评指标

见 GB/T 22239-2008 8.1.2.3。

8.1.2.3.2 测评实施

本项要求包括：

a) 应访谈安全审计员，询问对边界和网络设备是否实现集中安全审计，审计内容包括哪些项；询问审计内容是什么，对审计记录的处理方式有哪些；

b) 应检查边界和网络设备，查看审计策略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；

c) 应检查边界和网络设备，查看审计记录是否包括：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；

d) 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；

e) **应检查边界和网络设备，查看其审计跟踪设置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) **应检查边界和主要网络设备，查看时钟是否保持一致；**

g) 应测试边界和网络设备，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。

8.1.2.3.3 结果判定

如果 8.1.2.3.2 b）-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。

8.1.2.4 边界完整性检查

8.1.2.4.1 测评指标

见 GB/T 22239-2008 8.1.2.4。

8.1.2.4.2 测评实施

本项要求包括：

a) 应访谈安全管理员，询问是否对内部用户私自连接到外部网络的行为以及非授权设备私自接入到内部网络的行为进行监控；

b) 应检查边界完整性检查设备，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；

c) 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；

d) 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 b）-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。

8.1.2.5 入侵防范

8.1.2.5.1 测评指标

见 GB/T 22239-2008 8.1.2.5。

8.1.2.5.2 测评实施

本项要求包括：

a) 应访谈安全管理员，询问网络入侵防范措施有哪些；询问是否有专门设备对网络入侵进行防范；询问网络入侵防范规则库的升级方式；

b) 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；

c) 应检查网络入侵防范设备，查看入侵事件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**；

d) 应检查网络入侵防范设备，查看其规则库是否为最新；

e) 应测试网络入侵防范设备，验证其检测策略是否有效；

f) 应测试网络入侵防范设备，验证其报警策略是否有效。

8.1.2.5.3 结果判定

如果8.1.2.5.2 b）-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。

8.1.2.6 恶意代码防范

8.1.2.6.1 测评指标

见 GB/T 22239-2008 8.1.2.6。

8.1.2.6.2 测评实施

本项要求包括：

a) 应访谈安全管理员，询问网络恶意代码防范措施是什么；询问恶意代码库的更新策略；

b) 应检查网络设计或验收文档，查看其是否有在网络边界及核心业务网段处对恶意代码采取相关措施的描述，防恶意代码产品是否有实时更新功能的描述；

c) 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；

d) 应检查防恶意代码产品，查看其运行是否正常，恶意代码库是否为最新版本。

8.1.2.6.3 结果判定

本项要求包括：

a) 如果8.1.2.6.2 b）缺少相应文档资料，则为否定；

b) 如果8.1.2.6.2 b）-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。

8.1.2.7 网络设备防护

8.1.2.7.1 测评指标

见 GB/T 22239-2008 8.1.2.7。

8.1.2.7.2 测评实施

本项要求包括：

a) 应访谈网络管理员，询问网络设备的防护措施有哪些，询问网络设备的登录和验证方式做过何种特定配置；询问网络特权用户的权限如何分配；
b) 应访谈网络管理员，询问网络设备的口令策略是什么；
c) 应检查边界和主要网络设备，查看是否配置了登录用户身份鉴别功能，口令设置是否有复杂度和定期修改要求；
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**且其中一种是不可伪造的；**
e) 应检查边界和网络设备，查看是否配置了鉴别失败处理功能；
f) 应检查边界和网络设备，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；
g) 应检查边界和网络设备，查看是否对网络设备的管理员登录地址进行限制；查看是否设置网络登录连接超时，并自动退出；查看是否实现设备特权用户的权限分离；
h) 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 c）-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 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 8.1.3.1。

8.1.3.1.2 测评实施

本项要求包括：

a) 应访谈系统管理员和数据库管理员，询问操作系统和数据库管理系统的身份标识与鉴别机制采取何种措施实现；
b) 应访谈系统管理员和数据库管理员，询问对操作系统和数据库管理系统是否采用了远程管理，如采用了远程管理，查看是否采用了防止鉴别信息在网络传输过程中被窃听的措施；
c) 应检查服务器操作系统和数据库管理系统帐户列表，查看管理员用户名分配是否唯一；
d) 应检查服务器操作系统和数据库管理系统，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；
e) 应检查服务器操作系统和数据库管理系统，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**；
f) 应检查服务器操作系统和数据库管理系统，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；查看是否配置网络登录连接超时自动退出的功能；
g) **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。**
h) 应渗透测试服务器操作系统，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；
i) 应渗透测试服务器操作系统，测试是否存在绕过认证方式进行系统登录的方法。

8.1.3.1.3 结果判定

如果8.1.3.1.2 c）-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 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 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 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，查看匿名/默认用户的访问权限是否已被禁用或者严格限制，是否删除了系统中多余的、过期的和共享的帐户；

c) 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；

d) 应检查数据库服务器的数据库管理员与操作系统管理员是否由不同管理员担任。

e) 应检查服务器操作系统和数据库管理系统，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；

f) **应检查主要服务器操作系统和主要数据库管理系统，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；访问控制的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 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。

8.1.3.4 可信路径

8.1.3.4.1 测评指标

见 GB/T 22239-2008 8.1.3.4。

8.1.3.4.2 测评实施

本项要求包括：

a) **应访谈安全管理员，询问在什么情况下起用可信路径进行初始登录；目前系统提供了哪些方式的可信路径；**

b) **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；**

c) **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；**

d) **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；**

e) **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 b）-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。

8.1.3.5 安全审计

8.1.3.5.1 测评指标

见GB/T 22239-2008 8.1.3.5。

8.1.3.5.2 测评实施

本项要求包括：

a) 应访谈安全审计员，询问主机系统的安全审计策略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，查看安全审计配置是否符合安全审计策略的要求；

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，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；

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，查看是否对审计记录实施了保护措施，使其避免受到未预期的删除、修改或覆盖等。

e) 应检查主要服务器和重要终端操作系统，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；

f) **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，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；**

g) 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，可试图通过非审计员的其他帐户来中断审计进程，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 b）-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。

8.1.3.6 剩余信息保护

8.1.3.6.1 测评指标

见GB/T 22239-2008 8.1.3.6。

8.1.3.6.2 测评实施

本项要求包括：

a) 应检查操作系统和数据库管理系统维护操作手册，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 a）为肯定，则信息系统符合本单元测评指标要求，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 8.1.3.7。

8.1.3.7.2 测评实施

本项要求包括：

a) 应访谈系统管理员，询问是否采取入侵防范措施，入侵防范内容是否包括主机运行监视、特定

进程监控、入侵行为检测和完整性检测等方面内容；

b) 应检查入侵防范系统，查看是否能够记录攻击者的源 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）；

c) 应检查重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；

d) 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；

e) 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；

f) 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安装。

8.1.3.7.3 结果判定

如果 8.1.3.7.2 b）-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 8.1.3.8。

8.1.3.8.2 测评实施

本项要求包括：

a) 应访谈系统安全管理员，询问主机系统是否采取恶意代码实时检测与查杀措施，恶意代码实时检测与查杀措施的部署覆盖范围如何；

b) 应检查主要服务器，查看是否安装了实时检测与查杀恶意代码的软件产品并进行及时更新；

c) 应检查防恶意代码产品是否实现了统一管理；

d) 应检查网络防恶意代码产品，查看其厂家名称、产品版本号和恶意代码库名称等，查看其是否与主机防恶意代码产品有不同的恶意代码库。

8.1.3.8.3 结果判定

如果8.1.3.8.2 b）-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。

8.1.3.9 资源控制

8.1.3.9.1 测评指标

见 GB/T 22239-2008 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，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) 应检查服务器操作系统，查看是否设置了单个用户对系统资源的最大或最小使用限度；

c) 应检查服务器操作系统，查看是否在服务水平降低到预先规定的最小值时，能检测和报警；

d) 应检查主要服务器操作系统，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；

e) 应检查能够访问服务器的终端是否设置了操作超时锁定的配置。

8.1.3.9.3 结果判定

如果 8.1.3.9.2 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 8.1.4.1。

8.1.4.1.2 测评实施

本项要求包括：

a) 应访谈应用系统管理员，询问应用系统是否提供专用的登录控制模块对用户进行身份标识和鉴别，具体措施有哪些；系统采取何种措施防止身份鉴别信息被冒用；
b) 应访谈应用系统管理员，询问应用系统是否具有登录失败处理功能；
c) 应检查设计或验收文档，查看其是否有系统采用了保证唯一标识的措施的描述；
d) 应检查操作规程和操作记录，查看其是否有添加、删除用户和修改用户权限的操作规程、操作记录和审批记录；
e) 应检查应用系统，查看其是否采用了两个及两个以上身份鉴别技术的组合来进行身份鉴别，**并且保证至少有一种是不可伪造的；**
f) 应检查应用系统，查看其是否提供身份标识和鉴别功能；查看其身份鉴别信息是否具有不易被冒用的特点；查看其鉴别信息复杂度检查功能是否能够保证系统中不存在弱口令等；
g) 应检查应用系统，查看其提供的登录失败处理功能，是否根据安全策略配置了相关参数；
h) 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，查看登录是否成功，验证其身份标识和鉴别功能是否有效；
i) 应测试应用系统，验证其登录失败处理功能是否有效；
j) 应渗透测试应用系统，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

本项要求包括：

a) 如果8.1.4.1.2 c）中相关文档有系统采用了保证用户唯一性标识的措施的描述，则为肯定；
b) 如果8.1.4.1.2 d）缺少相应文档资料，则为否定；
c) 如果8.1.4.1.2 c）-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。

8.1.4.2 安全标记

8.1.4.2.1 测评指标

见GB/T 22239-2008 8.1.4.2。

8.1.4.2.2 测评实施

本项要求包括：

a) **应访谈应用系统管理员，询问应用系统是否提供所有主体和客体设置敏感标记的功能；**
b) **应检查设计或验收文档，查看文档中是否有应用系统敏感标记的说明；**
c) **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；**
d) **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 b）-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。

8.1.4.3 访问控制

8.1.4.3.1 测评指标

见GB/T 22239-2008 8.1.4.3。

8.1.4.3.2 测评实施

本项要求包括：

a) 应访谈应用系统管理员，询问应用系统是否提供访问控制措施，以及具体措施和访问控制策略有哪些，访问控制的粒度如何；
b) 应检查应用系统，查看系统是否提供访问控制机制；是否依据安全策略控制用户对客体的访问；

c) 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；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；

d) 应检查应用系统，查看其是否有由授权用户设置其它用户访问系统功能和用户数据的权限的功能；

e) 应检查应用系统，查看系统是否授予不同帐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) **应检查应用系统，查看其是否不存在默认帐户，如果有是否禁止了默认帐户的访问**；

g) **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；**

h) 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；

i) 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帐户的访问；

j) 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 b）-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。

8.1.4.4 可信路径

8.1.4.4.1 测评指标

见GB/T 22239-2008 8.1.4.4。

8.1.4.4.2 测评实施

本项要求包括：

a) **应访谈应用系统管理员，询问在系统对用户进行身份鉴别和用户对系统进行访问时能否在系统与用户之间建立一条安全的信息传输路径；**

b) **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应能够建立一条安全的信息传输路径的说明；**

c) **应测试应用系统，可通过获取并查看系统对用户进行身份鉴别和用户对系统进行访问的通信数据包，验证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 b）和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。

8.1.4.5 安全审计

8.1.4.5.1 测评指标

见GB/T 22239-2008 8.1.4.5。

8.1.4.5.2 测评实施

本项要求包括：

a) 应访谈安全审计员，询问应用系统是否设置安全审计功能，对事件进行审计的选择要求和策略是什么，对审计日志的保护措施有哪些；

b) 应检查应用系统，查看其当前审计范围是否覆盖到每个用户；

c) 应检查应用系统，查看其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；

d) 应检查应用系统，查看其审计记录信息是否包括事件发生的日期与时间、触发事件的主体与客体、事件的类型、事件成功或失败、身份鉴别事件中请求的来源、事件的结果等内容；

e) 应检查应用系统，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分析功能，并能根据需要生成审计报表；

f) **应检查应用系统，查看其安全审计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；**

g) 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；

h) 应测试应用系统，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。

8.1.4.5.3 结果判定

如果8.1.4.5.2 b）-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。

8.1.4.6 剩余信息保护

8.1.4.6.1 测评指标

见GB/T 22239-2008 8.1.4.6。

8.1.4.6.2 测评实施

本项要求包括：

a) 应访谈应用系统管理员，询问系统是否采取措施保证对存储介质中的残余信息进行删除（无论这些信息是存放在硬盘上还是在内存中），具体措施有哪些；

b) 应检查设计或验收文档，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；

c) 应检查设计或验收文档，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如何进行完全清除的描述；

d) 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

本项要求包括：

a) 如果8.1.4.6.2 b）和c）缺少相应文档资料，则为否定；

b) 如果8.1.4.6.2 b）-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。

8.1.4.7 通信完整性

8.1.4.7.1 测评指标

见GB/T 22239-2008 8.1.4.7。

8.1.4.7.2 测评实施

本项要求包括：

a) 应访谈安全管理员，询问应用系统是否具有在数据传输过程中保护其完整性的措施，具体措施是什么；

b) 应检查设计或验收文档，查看其是否有关于保护通信完整性的说明，如果有则查看其是否有用密码技术来保证通信过程中数据的完整性的描述；

c） 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加密的验证码。

8.1.4.7.3 结果判定

如果8.1.4.7.2 b）和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。

8.1.4.8 通信保密性

8.1.4.8.1 测评指标

见 GB/T 22239-2008 8.1.4.8。

8.1.4.8.2 测评实施

本项要求包括：

a） 应访谈安全管理员，询问应用系统数据在通信过程中是否采取保密措施，具体措施有哪些；

b） **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；**

c） **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；**

d） 应测试应用系统，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；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 c）缺少相关文档材料，则为否定；

b） 如果8.1.4.8.2 b）-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。

8.1.4.9 抗抵赖

8.1.4.9.1 测评指标

见 GB/T 22239-2008 8.1.4.9。

8.1.4.9.2 测评实施

本项要求包括：

a） 应访谈安全管理员，询问系统是否具有抗抵赖的措施，具体措施有哪些；

b） 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 b）为肯定，则信息系统符合本单元测评指标要求，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 8.1.4.10。

8.1.4.10.2 测评实施

本项要求包括：

a） 应访谈应用系统管理员，询问应用系统是否具有保证软件容错能力的措施，具体措施有哪些；

b） 应检查应用系统，查看应用系统是否对人机接口输入或通信接口输入的数据进行有效性检验；

c） 应测试应用系统，可通过对人机接口输入的不同长度或格式的数据，查看系统的反应，验证系统人机接口有效性检验功能是否正确；

d） 应测试应用系统，验证其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；

e) **应测试应用系统，验证其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 b）-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。

8.1.4.11 资源控制

8.1.4.11.1 测评指标

见 GB/T 22239-2008 8.1.4.11。

8.1.4.11.2 测评实施

本项要求包括：

a) 应访谈应用系统管理员，询问应用系统是否有资源控制的措施，具体措施有哪些；

b) 应检查应用系统，查看是否限制单个帐户的多重并发会话；系统是否有最大并发会话连接数的限制，是否对一个时间段内可能的并发会话连接数进行限制；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，保证优先级低的主体处理能力不会影响到优先级高的主体的处理能力；

c) 应检查应用系统，查看是否对一个访问帐户或一个请求进程占用的资源分配最大限额和最小限额；

d) 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，是否对全部资源采用优先服务机制；**

e) 应测试应用系统，可通过对系统进行超过规定的单个帐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帐户的多重并发会话数；

f) 应测试应用系统，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；

g) 应测试重要应用系统，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。

8.1.4.11.3 结果判定

如果8.1.4.11.2 b）-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 8.1.5.1。

8.1.5.1.2 测评实施

本项要求包括：

a) 应访谈安全管理员，询问应用系统数据在存储和传输过程中是否有完整性保证措施，具体措施有哪些；在检测到完整性错误时是否能恢复，恢复措施有哪些；

b) **应访谈管理人员（系统管理员、网络管理员、安全管理员、数据库管理员），询问信息系统中的操作系统、网络设备、数据库管理系统和应用系统等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，破坏数据的完整性；并询问具体的专用通信协议或安全通信协议服务是什么；**

c) 应检查操作系统、网络设备、数据库管理系统和应用系统，查看其是否配备检测系统管理数据、鉴别信息和用户数据在传输过程中完整性受到破坏的功能；是否配备检测系统管理数据、身份鉴别信息和用户数据在存储过程中完整性受到破坏的功能；是否配备检测重要系统/模块完整性受到破坏的功能；在检测到完整性错误时能否采取必要的恢复措施；

d) **应检查操作系统、网络设备、数据库管理系统和应用系统中是否为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 c）和 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。

8.1.5.2 数据保密性

8.1.5.2.1 测评指标

见 GB/T 22239-2008 8.1.5.2。

8.1.5.2.2 测评实施

本项要求包括：

a) 应访谈网络管理员，询问网络设备的管理数据、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保密性，是否采用加密或其他有效措施实现存储保密性；

b) 应访谈系统管理员，询问主机操作系统的管理数据、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保密性，是否采用加密或其他有效措施实现存储保密性；

c) 应访谈数据库管理员，询问数据库管理系统的管理数据、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保密性，是否采用加密或其他有效措施实现存储保密性；

d) 应访谈安全管理员，询问应用系统的管理数据、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保密性，是否采用加密或其他有效措施实现存储保密性；

e) 应检查主机操作系统、网络设备操作系统、数据库管理系统和应用系统，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；

f) **应检查操作系统、网络设备、数据库管理系统和应用系统中是否为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；**

g) 应测试应用系统，通过用嗅探工具获取系统传输数据包，查看其是否采用了加密或其他有效措施实现传输保密性。

8.1.5.2.3 结果判定

如果 8.1.5.2.2 e）-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。

8.1.5.3 备份和恢复

8.1.5.3.1 测评指标

见 GB/T 22239-2008 8.1.5.3。

8.1.5.3.2 测评实施

本项要求包括：

a) 应访谈网络管理员，询问是否对网络设备中的配置文件进行备份，备份策略是什么；完全数据备份是否每天一次，备份介质是否场外存放；是否提供异地**实时**数据备份功能；当其受到破坏时，恢复策略是什么；是否提供主要网络设备、通信线路的硬件冗余；

b) 应访谈系统管理员，询问是否对操作系统中的重要信息进行备份，备份策略是什么；完全数据备份是否每天一次，备份介质是否场外存放；是否提供异地**实时**数据备份功能；当其受到破坏时，恢复策略是什么；是否提供主要服务器的硬件冗余；

c) 应访谈数据库管理员，询问是否对数据库管理系统中的主要数据进行备份，备份策略是什么；完全数据备份是否每天一次，备份介质是否场外存放；是否提供异地**实时**数据备份功能；当其受到破坏时，恢复策略是什么；

d) 应访谈安全管理员，询问是否对应用系统中的应用程序进行备份，备份策略是什么；当其受到破坏时，恢复策略是什么；完全数据备份是否每天一次，备份介质是否场外存放；是否提供异地**实时**数据备份功能；

e) 应检查设计或验收文档，查看其是否有关于主要主机操作系统、网络设备操作系统、数据库管理系统和应用系统配置有本地和异地**实时**数据备份和恢复功能及策略的描述；

f) 应检查主要主机操作系统、主要网络设备、主要数据库管理系统和主要应用系统，查看其是否提供备份和恢复功能，其配置是否正确，并且查看其备份结果是否与备份策略一致；

g) 应检查主要网络设备、主要通信线路和主要数据处理系统是否采用硬件冗余、软件配置等技术手段提供系统的高可用性；

h) 应检查网络拓扑结构是否不存在关键节点的单点故障；

i) **应检查是否建立异地灾难备份中心，配备灾难恢复所需的通信线路、网络设备和数据处理设备，将备份数据实时备份至灾难备份中心，提供业务应用的实时切换；**

j) **应测试业务应用系统，验证其异地切换功能是否有效。**

8.1.5.3.3 结果判定

本项要求包括：

a) 如果 8.1.5.3.2 e）缺少相应文档资料，则为否定；

b) 如果 8.1.5.3.2 e）-j）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 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、建设和管理等层面的各类管理内容；

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 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 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，询问是否有专门的部门或人员负责制定安全管理制度；

b) 应访谈安全管理制度制、修订人员，询问安全管理制度的制定程序和发布方式，是否对制定的安全管理制度进行论证和审定，论证和评审方式如何，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如何控制使用，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**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，查看收发是否通过正式、有效的方式（如正式发文、领导签署和单位盖章等），是否有发布范围要求。

8.2.1.2.3 结果判定

如果8.2.1.2.2 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 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，评审周期多长，**是否有部门或人员负责制度的日常维护，**定期或不定期对安全管理制度进行检查、审定，由何部门或何人负责；

b） 应访谈安全管理制度制、修订人员，询问对安全管理制度的**日常维护情况，**安全检查及修订情况，评审、修订程序如何；

c） **应访谈安全管理制度制、修订人员，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；**

d） 应访谈安全管理制度制、修订人员，询问系统发生重大安全事故、出现新的安全漏洞以及技术基础结构和组织结构等发生变更时是否对安全管理制度进行审定，对需要改进的制度是否进行修订；

e） **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**；

f） **应检查是否具有所有安全管理制度对应相应负责人或者负责部门的清单；**

g） 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；

h） 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。

8.2.1.3.3 结果判定

如果8.2.1.3.2 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。

8.2.2 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 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）；机构内部门设置情况如何，是否明确各部门的职责分工；

c） 应访谈安全主管，询问信息系统设置了哪些工作岗位，各个岗位的职责分工是否明确；询问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，询问其岗位职责包括哪些内容；
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、机房管理员、系统管理员、网络管理员、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；查看文件是否明确各个岗位人员应具有的技能要求；
f) 应检查信息安全管理委员会或领导小组最高领导是否具有委任授权书，查看授权书中是否有本单位主管领导的授权签字；
g) 应检查信息安全管理委员会职责文件，查看是否明确委员会职责和其最高领导岗位的职责；
h) 应检查安全管理各部门和信息安全管理委员会或领导小组是否具有日常管理工作执行情况的文件或工作记录。

8.2.2.1.3 结果判定

如果8.2.2.1.2 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。

8.2.2.2 人员配备

8.2.2.2.1 测评指标

见GB/T 22239-2008 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人员的配备情况，包括数量、专职还是兼职等，对关键事务的管理人员配备情况如何；
b) 应检查人员配备要求管理文档，查看是否明确应配备哪些安全管理人员，是否包括机房管理员、系统管理员、数据库管理员、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；查看是否明确对哪些关键事务的管理人员应配备2人或2人以上共同管理，是否明确对配备人员的具体要求；
c) 应检查安全管理各岗位人员信息表，查看其是否明确机房管理员、系统管理员、数据库管理员、网络管理员和安全管理员等重要岗位人员的信息，确认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 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 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，审批部门是何部门，批准人是何人，他们的审批活动是否得到授权；询问是否定期审查、更新审批项目，审查周期多长；
b) 应访谈安全主管，询问其对关键活动的审批范围包括哪些，审批程序如何；
c) 应检查审批管理制度文档，查看文档中是否明确审批事项、需逐级审批的事项、审批部门、批准人及审批程序等，是否明确对系统变更、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；
d) 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；

e） 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 a）-e）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 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，询问是否建立与外单位（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）的沟通、合作机制，与外单位和其他部门有哪些合作内容，沟通、合作方式有哪些；与组织机构内其它部门之间及内部各部门管理人员之间是否建立沟通、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，组织其它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安全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安全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） 应检查是否有组织机构内部人员联系表；

g） 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；

h） 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 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。

8.2.2.5 审核和检查

8.2.2.5.1 测评指标

见GB/T 22239-2008 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进行全面安全检查，检查周期多长，检查内容有哪些；

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，检查周期多长；询问系统全面安全检查情况，检查周期多长，检查人员有哪些，检查程序如何，是否对检查结果进行通报，通报形式、范围如何；

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文件要求是否一致。

8.2.2.5.3 结果判定

如果8.2.2.5.2 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 8.2.3.1。

8.2.3.1.2 测评实施

本项要求包括：

a) 应访谈安全主管，询问是否有专门的部门或人员负责人员的录用工作，由何部门/何人负责；

b) 应访谈人事管理相关人员，询问在人员录用时对人员条件有哪些要求，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，是否与被录用人员都签署保密协议；

c) 应访谈人事管理相关人员，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；

d) 应检查人员录用要求管理文档，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、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；

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的签字等内容；

h) 应检查岗位安全协议，查看是否有岗位安全责任、违约责任、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 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。

8.2.3.2 人员离岗

8.2.3.2.1 测评指标

见 GB/T 22239-2008 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有哪些控制方法，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) 应访谈人事管理相关人员，询问调离手续包括哪些，是否要求**所有人员**调离时须承诺相关保密义务后方可离开，**对于某些关键岗位人员调离是否采取更加严格的处理措施，如重新评估确定其调离后可能存在的安全风险，保密承诺要求更加严格等**；

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**、人员离岗控制程序、**人员调离手续等相关内容**；**

d) 应检查是否具有对离岗人员的安全处理记录（如交还身份证件、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 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 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，询问是否有人负责定期对各个岗位人员进行安全技能及安全知识的考核；

b) 应访谈人事管理相关人员员，询问对各个岗位人员的考核情况，考核周期多长，考核内容有哪些；询问对人员的安全审查情况，审查人员是否包含所有岗位人员，审查内容有哪些；对关键岗位人员的审查和考核是否有特殊要求；

c) **应访谈人事管理相关人员员，询问是否对安全保密制度执行情况进行检查或考核，考核方式有哪些；**

d) **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；**

e) 应检查考核文档和记录，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，是否有对关键岗位人员特殊的考核内容；查看记录日期与考核周期是否一致；

f) **应检查人员安全审查记录，查看记录的审查人员是否包括各个岗位的人员，是否有对关键岗位人员特殊的安全审查内容。**

8.2.3.3.3 结果判定

如果 8.2.3.3.2 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。

8.2.3.4 安全意识教育和培训

8.2.3.4.1 测评指标

见 GB/T 22239-2008 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，具体的培训方式有哪些；是否对违反安全策略和规定的人员进行惩戒，如何惩戒；

b) 应访谈安全管理员、系统管理员、网络管理员和数据库管理员，考查其对工作相关的信息安全基础知识、安全责任和惩戒措施等的理解程度；

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） 应检查是否具有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 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 8.2.3.5。

8.2.3.5.2 测评实施

本项要求包括：

a） 应访谈安全管理员，询问对外部人员访问重要区域（如访问机房、重要服务器或设备区、**保密文档存放区**等）采取了哪些安全措施，是否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**外部人员包括哪些人员**，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，**对哪些关键区域不允许外部人员访问等）**，外部人员进入的访问控制措施（由专人全程陪同或监督等）和外部人员离开的条件等；

c） 应检查外部人员访问重要区域的批准文档，查看是否有外部人员访问重要区域的书面申请，是否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、访问设备或信息及陪同人等信息。

8.2.3.5.3 结果判定

如果8.2.3.5.2 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 8.2.4.1。

8.2.4.1.2 测评实施

本项要求包括：

a） 应访谈安全主管，询问确定信息系统安全保护等级的方法是否参照定级指南的指导，定级过程是否有书面描述；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，定级结果是否获得了相关部门的批准；

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，查看是否说明定级的方法和理由，查看定级结果是否有相关部门的批准盖章；

c） 应检查专家论证文档，查看是否有专家对定级结果的论证意见。

8.2.4.1.3 结果判定

本项要求包括：

a） 如果8.2.4.1.2 a）单位没有上级主管部门，但定级结果有本单位信息安全主管领导的批准，则该项为肯定；

b） 如果8.2.4.1.2 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 8.2.4.2。

8.2.4.2.2 测评实施

本项要求包括：

a) 应访谈安全主管，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，询问是否根据系统的安全级别选择基本安全措施，是否依据风险分析的结果补充和调整安全措施，具体做过哪些调整；

c) 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，是否经过论证和审定，是否经过审批，是否根据等级测评、安全评估的结果定期调整和修订，维护周期多长；

d) 应检查系统的安全建设工作计划，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) 应检查专家论证文档，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，查看维护记录日期间隔与维护周期是否一致。

8.2.4.2.3 结果判定

如果8.2.4.2.2 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 8.2.4.3。

8.2.4.3.2 测评实施

本项要求包括：

a) 应访谈安全主管，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，询问信息安全产品的采购情况，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，采购过程如何控制，是否定期审定和更新候选产品名单，审定周期多长；

c) 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；

d) 应检查产品采购管理文档，查看内容是否明确**对重要部位的产品委托专业测评单位进行专项测试，**明确需要的产品性能指标，确定产品的候选范围，通过招投标等方式确定采购产品及人员的行为准则等方面；

e) 应检查系统使用的有关信息安全产品是否符合国家的有关规定；

f) 应检查密码产品的使用情况是否符合密码产品使用、管理的相关规定；

g) 应检查是否具有产品选型测试结果记录**（包括对重要部位的产品委托专业测评单位进行专项测试的结果记录）**、候选产品名单审定记录或更新的候选产品名单。

8.2.4.3.3 结果判定

如果8.2.4.3.2 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 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），**开发人员有哪些人，是否是专职人员，**自主开发软件是否在独立的模拟环境中编写、调试和完成；

b) 应访谈系统建设负责人，**询问对开发人员的开发活动采取哪些控制措施，是否有专人监控、审查，**软件设计相关文档和使用指南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，询问其是否参照代码编写安全规范进行软件开发，开发之后是否交给测试人员测试软件；

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，是否明确软件开发相关文档的管理等；

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；

f) 应检查是否具有软件设计的相关文档（应用软件设计程序文件、源代码文档等）、软件使用指南或操作手册和维护手册等；

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（软件设计和开发程序文件、测试数据、测试结果、维护手册等）的使用控制记录；

i) **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 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。

8.2.4.5 外包软件开发

8.2.4.5.1 测评指标

见 GB/T 22239-2008 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，检测工具是否是第三方的商业产品；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；

b) 应检查是否具有需求分析说明书、软件设计说明书、软件操作手册、软件源代码文档等软件开发文档和使用指南；

c) 应检查软件源代码审查记录，查看是否包括对可能存在的后门**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 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。

8.2.4.6 工程实施

8.2.4.6.1 测评指标

见GB/T 22239-2008 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，询问是否有专门的部门或人员负责工程实施管理工作，由何部门/何人负责，**是否由第三方工程监理单位按照系统建设文档的要求对工程实施过程进行进度和质量控制**，是否要求工程实施单位提供其能够安全实施系统建设的资质证明和能力保证；

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；

c) 应检查是否具有按照实施方案形成的阶段性工程报告等文档；

d) **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**；

e) 应检查工程实施管理制度，查看其是否包括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。

8.2.4.6.3 结果判定

如果8.2.4.6.2 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 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对系统测试验收报告进行审定；

c) 应检查工程测试验收方案，查看其是否明确说明参与测试的部门、人员、测试验收的内容、现场操作过程等内容；

d) 应检查测试验收记录是否详细记录了测试时间、人员、现场操作过程和测试验收结果等方面内容；

e) 应检查是否具有系统安全性测试报告，查看报告是否给出测试通过的结论（如果报告中提出了存在的问题，则检查是否有针对这些问题的改进报告），是否有第三方测试机构的签字或盖章；

f) 应检查是否具有系统测试验收报告，是否有对测试验收报告的审定文档，查看文档是否有相关人员的审定意见；

g) 应检查测试验收管理文档是否包括系统测试验收的过程控制方法、参与人员的行为规范等内容。

8.2.4.7.3 结果判定

如果8.2.4.7.2 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。

8.2.4.8 系统交付

8.2.4.8.1 测评指标

见GB/T 22239-2008 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，系统交接时是否根据交付

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，询问目前的信息系统是否由内部人员独立运行维护，如果是，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分类详细列项系统交付的各类设备、软件、文档等；

d) 应检查是否具有系统建设文档、指导用户进行系统运维的文档、系统培训手册等；

e) 应检查系统交付管理文档，查看其是否包括交付过程的控制方法和对交付参与人员的行为限制等方面内容；

f) 应检查培训记录，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 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 8.2.4.9。

8.2.4.9.2 测评实施

本项要求包括：

a) 应访谈安全主管，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；

b) 应访谈文档管理员，询问对系统定级相关备案文档采取哪些控制措施；

c) 应检查是否具有将系统等级相关材料报主管部门备案的记录或备案文档；

d) 应检查是否具有将系统等级相关备案材料报相应公安机关备案的记录或证明；

e) 应检查是否具有系统定级相关材料的使用控制记录。

8.2.4.9.3 结果判定

如果 8.2.4.9.2 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。

8.2.4.10 安全服务商选择

8.2.4.10.1 测评指标

见 GB/T 22239-2008 8.2.4.11。

8.2.4.10.2 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，查看文档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，查看是否包括服务内容、服务期限、双方签字或盖章等。

8.2.4.10.3 结果判定

如果 8.2.4.10.2 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 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基础设施进行定期维护，由何部门或何人负责，维护周期多长，是否有专门的部门和人员负责机房环境安全管理工作；

b) **应访谈系统运维负责人，询问办公环境是否和机房实行统一安全管理，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控制，机房是否有摄像监控系统；**

c) 应访谈安全主管，询问为保证办公环境的保密性采取了哪些控制措施；

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

e) 应检查办公环境管理文档，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、人员调离办公室时立即收回钥匙、不在办公区接待来访人员等方面内容；

f) 应检查机房基础设施维护记录，查看是否记录维护日期、维护人、维护设备、故障原因、维护结果等方面内容；

g) **应检查机房的摄像监控系统是否可以实时监控，是否有监控记录**。

8.2.5.1.3 结果判定

如果8.2.5.1.2 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 8.2.5.2。

8.2.5.2.2 测评实施

本项要求包括：

a) 应访谈安全主管，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) 应访谈资产管理员，询问是否依据资产的重要程度对资产进行分类和标识管理，不同类别的资产是否采取不同的管理措施；

c) 应检查资产清单，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；

d) 应检查资产安全管理制度，查看其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、传输、存储、维护等方面；

e) 应检查信息分类文档，查看其内容是否明确了信息分类标识的原则和方法。

8.2.5.2.3 结果判定

如果8.2.5.2.2 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。

8.2.5.3 介质管理

8.2.5.3.1 测评指标

见 GB/T 22239-2008 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、介质内存储信息被未授权修改以及非法泄漏等，是否有专人管理；

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，是否对其完整性（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，是否根据所承载的数据和软件的重要性对介质进行分类和标识管理；

c) 应访谈资产管理员，询问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；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；

d) 应访谈资产管理员，询问对送出维修的介质在送出之前**是否采用多次读写覆盖、清除敏感或秘密数据等保密处理措施**，对保密性较高的介质销毁前是否有领导批准，**是否采取双人监控，对无法执行删除操作的受损介质是否要求销毁，销毁时是否送符合国家保密部门规定的部门销毁；**

e) 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；

f) 应检查介质管理记录，查看其是否记录介质的存储、归档、查询和借用等情况；

g) 应检查介质管理制度，查看其内容是否覆盖介质的存放环境、使用、维护和销毁等方面；

h) 应检查介质，查看是否对其进行了分类，并具有不同标识；

i) **应检查介质异地存放地的环境要求和管理要求是否与本地相同**；

j) **应检查保密性介质销毁过程记录，查看其是否有双人监控的签字确认，是否严格执行销毁过程**。

8.2.5.3.3 结果判定

如果8.2.5.3.2 a）-j）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 8.2.5.4。

8.2.5.4.2 测评实施

本项要求包括：

a) 应访谈资产管理员，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，对各类测试工具进行有效性检查，由何部门/何人负责，维护周期多长；

b) 应访谈资产管理员，询问是否对设备选用的各个环节（选型、采购、发放和领用、涉外维修和服务及信息处理设备带离机构等）进行审批控制；

c) 应访谈安全审计员，询问对设备（包括备份和冗余设备）的操作是否建立日志，日志文件如何管理，是否定期检查管理情况；

d) 应检查设备安全管理制度，查看其内容是否明确对各种软硬件设备的选型、采购、发放和领用以及带离机构等环节进行申报和审批；

e) 应检查配套设施、软硬件维护方面的管理制度，查看其是否对配套设施、软硬件维护进行有效的管理，包括明确维护人员的责任、涉外维修和服务的审批、维修过程的监督控制管理等；

f) 应检查设备使用管理文档，查看其内容是否覆盖终端计算机、便携机和网络设备等使用、操作原则、注意事项等方面；

g) 应检查设备（包括备份和冗余设备）操作规程，查看其内容是否覆盖服务器如何启动、停止、加电、断电等操作；

h) 应检查是否具有设备的选型、采购、发放和领用以及带离机构等的申报材料和审批报告；

i) 应检查是否具有设备维护记录和主要设备的操作日志。

8.2.5.4.3 结果判定

如果8.2.5.4.2 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。

8.2.5.5 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 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，询问是否建立安全管理中心，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管理中心，安全管理中心是否对设备状态、恶意代码、补丁升级、安全审计等安全相关事项进行集中管理；
d) 应检查监控记录，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；
e) 应检查监测分析报告，查看是否包括监测的异常现象、处理措施等。

8.2.5.5.3 结果判定

如果8.2.5.5.2 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。

8.2.5.6 网络安全管理

8.2.5.6.1 测评指标

见GB/T 22239-2008 8.2.5.6。

8.2.5.6.2 测评实施

本项要求包括：

a) 应访谈安全主管，询问是否指定专人负责维护网络运行日志、监控记录和分析处理报警信息等网络安全管理工作；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；
b) 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（帐户数据、设备配置文件等）进行备份，采取什么方式；
c) 应访谈网络管理员，询问是否实现网络设备的最小服务配置**和优化配置**，对配置文件是否进行定期离线备份，采取什么方式；是否定期检查拨号上网等违反网络安全策略的行为；
d) 应访谈安全管理员，询问是否定期对网络设备进行漏洞扫描，扫描周期多长，发现漏洞是否及时修补；
e) **应访谈网络管理员，询问对网络管理用户的现场操作有何要求；**
f) 应检查网络漏洞扫描报告，查看其内容是否包含网络存在的漏洞、严重级别和结果处理等方面，检查扫描时间间隔与扫描周期是否一致；
g) 应检查网络安全管理制度，查看其是否覆盖网络安全配置、安全策略、升级与打补丁、最小服务、**优化配置**、日志保存时间、口令更新周期、**网络帐户（权限审批、权限分配、帐户注销等）**、文件备份等方面内容，**查看安全策略是否禁止便携式和移动式设备的网络接入；**
h) 应检查是否具有内部网络外联的授权批准书；
i) 应检查是否具有网络设备配置文件的离线备份文件；
j) 应检查是否具有网络审计日志，检查日志是否在规定的保存时间范围内。

8.2.5.6.3 结果判定

本项要求包括：

a) 如果8.2.5.6.2 e）访谈回答现场操作必须为两人以上，且经双重认可方能操作，操作过程有不可更改的审计日志，则为肯定；
b) 如果8.2.5.6.2 a）-j）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 8.2.5.7。

8.2.5.7.2 测评实施

本项要求包括：

a) 应访谈安全主管，询问是否指定专人对系统进行管理，对系统管理员用户是否进行分类，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；
b) 应访谈系统管理员，询问是否根据业务需求和系统安全分析制定系统的访问控制策略，控制分配信息系统、文件及服务的访问权限；
c) 应访谈系统管理员，询问是否定期对系统安装安全补丁程序，在安装系统补丁前是否对重要文件进行备份，采取什么方式进行，是否先在测试环境中测试通过再安装；
d) **应访谈系统管理员，询问是否对系统资源的使用进行预测，是否监视系统资源的使用情况，包括处理器、存储设备和输出设备等**；
e) 应访谈安全管理员，询问是否定期对系统进行漏洞扫描，扫描周期多长，发现的漏洞是否及时修补；
f) 应检查系统安全管理制度，查看其内容是否覆盖系统安全策略、安全配置、日志管理、日常操作流程等具体内容；
g) 应检查是否有详细操作日志(包括重要的日常操作、运行维护记录、参数的设置和修改等内容)；
h) 应检查是否有定期对运行日志和审计结果进行分析的分析报告，查看报告是否能够记录帐户的连续多次登录失败、非工作时间的登录、访问受限系统或文件的失败尝试、系统错误等非正常事件；
i) 应检查系统漏洞扫描报告，查看其内容是否包含系统存在的漏洞、严重级别和结果处理等方面，检查扫描时间间隔与扫描周期是否一致。

8.2.5.7.3 结果判定

如果 8.2.5.7.2 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。

8.2.5.8 恶意代码防范管理

8.2.5.8.1 测评指标

见 GB/T 22239-2008 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；
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) 应检查恶意代码防范管理文档，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 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 8.2.5.9。

8.2.5.9.2 测评实施

本项要求包括：

a) 应访谈安全管理员，询问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管理制度。

8.2.5.9.3 结果判定

如果 8.2.5.9.2 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 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，询问是否制定变更方案指导系统执行变更；目前系统发生过哪些变更，变更方案是否经过评审，变更过程是否文档化；

b) 应访谈系统运维负责人，询问重要系统变更前是否根据有关申报和审批程序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，**是否按照申报和审批程序定期对系统变更情况进行一致性检查**；

c) 应访谈系统运维负责人，询问变更失败后的恢复程序、工作方法和职责是否文档化，恢复过程是否经过演练；

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、变更前评估等方面内容；

e) 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；

f) 应检查变更管理制度，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；

g) 应检查变更控制的申报、审批程序，查看其是否覆盖**所有变更类型**、申报流程、审批部门、批准人等方面内容；

h) 应检查变更失败恢复程序，查看其是否规定变更失败后的恢复流程；

i) 应检查是否具有变更方案评审记录和变更过程记录文档。

8.2.5.10.3 结果判定

如果 8.2.5.10.2 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。

8.2.5.11 备份与恢复管理

8.2.5.11.1 测评指标

见 GB/T 22239-2008 8.2.5.11。

8.2.5.11.2 测评实施

本项要求包括：

a) 应访谈系统管理员、数据库管理员和网络管理员，询问是否识别出需要定期备份的业务信息、系统数据及软件系统，主要有哪些；**对特殊备份数据的操作是否要求人员数量，过程是否记录备案；**

b) 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，是否针对问题进行恢复程序的改进或调整其他因素；

c) **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**；

d) 应检查备份和恢复管理制度，查看其是否明确备份方式、备份频度、存储介质和保存期等方面内容；

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

f) 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；**

g) **应检查灾难恢复计划文档，查看其内容是否覆盖恢复计划执行条件和系统恢复流程等方面；**

h) **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 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。

8.2.5.12 安全事件处置

8.2.5.12.1 测评指标

见GB/T 22239-2008 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，**对重大的失、泄密事件是否向公安、安全、保密、机要等国家部门汇报**，不同安全事件是否采取不同的处理和报告程序，**处理涉密事件时是否要求两人或两人以上**；

b) 应访谈系统运维负责人，询问是否根据本系统已发生的和需要防止发生的安全事件对系统的影响程度划分不同等级，划分为几级，划分方法是否参照了国家相关管理部门的技术资料，主要参照哪些；

c) 应检查安全事件报告和处置管理制度，查看其是否明确本系统已发生的和需要防止发生的安全事件类型，是否明确安全事件的现场处理、事件报告和后期恢复的管理职责；

d) 应检查安全事件定级文档，查看其是否明确安全事件的定义、安全事件等级划分的原则、等级描述等方面内容；

e) 应检查安全事件记录分析文档，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，不同安全事件是否采取不同措施避免其再次发生，**涉密事件记录文档中是否至少包括两名工作人员；**

f) 应检查安全事件报告和处理程序文档，查看其是否根据不同安全事件制定不同的处理和报告程序，及响应和处置的范围、程度、处理方法，是否明确具体报告方式、报告内容、报告人等方面内容。

8.2.5.12.3 结果判定

如果 8.2.5.12.2 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。

8.2.5.13 应急预案管理

8.2.5.13.1 测评指标

见 GB/T 22239-2008 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，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，**根据系统变更定期评估并修订预案，目前的预案文档为第几版**；

b) 应访谈系统运维负责人，询问是否具有应急预案小组，是否具备应急设备并能正常工作，应急预案执行所需资金是否做过预算并能够落实；

c） 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；

d） 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；

e） 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；

f） 应检查是否具有应急预案培训记录、演练记录和审查记录，**如果系统有大的变更，检查是否有针对应急预案的评估文档和修订版本**。

8.2.5.13.3 结果判定

如果 8.2.5.13.2 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。

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

国标 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。

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项或部分符合项，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项或部分符合项，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本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项或部分符合项，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。

10.5 系统结构安全测评

在完成安全控制点间、层面间和区域间安全测评后，应进行系统结构安全测评，系统结构安全测评应从信息系统整体结构的安全性和整体安全防范的合理性方面进行分析和测评。

在测评分析信息系统整体结构的安全性时，应掌握信息系统的物理布局、网络拓扑、业务逻辑（业务数据流）、系统实现和集成方式等各种情况，结合业务数据流分析物理布局与网络拓扑之间、网络拓扑与业务逻辑之间、物理布局与业务逻辑之间、不同信息系统之间存在的各种关系，明确物理、网络和应用系统等不同位置上可能面临的威胁、可能暴露的脆弱性等，考虑信息系统的实际情况，综合判定信息系统的整体布局是否清晰、合理、安全有效。

在测评分析信息系统整体安全防范的合理性时，应熟悉信息系统安全保护措施的具体实现方式和部署情况等，结合业务数据流分析不同区域和不同边界与安全保护措施的关系、重要业务和关键信息与安全保护措施的关系等，参照纵深防御的要求，识别信息系统的安全防范是否突出重点、层层深入，综合判定信息系统的整体安全防范措施是否恰当合理、协调一致。

11 等级测评结论

11.1 各层面的测评结论

等级测评报告应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、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。当然，不同环境下，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 整体保护能力的测评结论

等级测评报告应给出信息系统整体保护能力的测评结论，确认信息系统达到相应等级保护要求的程度。

根据各层面的测评结论，结合整体测评的结果，给出信息系统整体安全保护能力的测评结论。整体安全保护能力的测评结论应包括安全技术和安全管理措施的有效性、安全强度的一致性以及整体安全防

御体系的完善程度等方面内容。

附录 A
（资料性附录）
测评力度

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.1 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。

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.2 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。

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 18336-2000 信息技术 信息技术安全性评估准则
[8] Information technology-Security techniques - Information security management systems requirements（ISO/IEC 27001：2005）
[9] Information technology-Security techniques - Code of practice forinformation security management（ISO/IEC 17799：2005）