GB

中华人民共和国国家标准

GB/T XXXX-200X

信息系统安全等级保护
测评准则

Evaluation and Testing Criteria for Classified Security 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　　发布

目　录

前　言

本标准是我国实施信息安全等级保护，进行信息系统安全测试评估的基础性技术规范。

本标准的附录 A 和附录 B 为资料性附录。

本标准由全国信息安全标准化技术委员会提出并归口。

本标准起草单位：公安部信息安全等级保护评估中心。

本标准主要起草人：朱建平 谢朝海 曲洁 刘静 黄洪 陈冠直 袁曙光。

引　言

本标准是我国实施信息安全等级保护的重要标准之一，提出了为验证计算机信息系统是否满足信息安全等级保护而必须执行的测评工作要求，用以指导测评机构从信息安全等级保护的角度对信息系统进行测试评估。

为了进一步提高信息安全的保障能力和防护水平，维护国家安全、公共利益和社会稳定，保障和促进信息化建设的健康发展，1994 年国务院颁布的《中华人民共和国计算机信息系统安全保护条例》规定“计算机信息系统实行安全等级保护，安全等级的划分标准和安全等级保护的具体办法，由公安部会同有关部门制定”。2004 年公安部等四部委联合签发的《关于信息安全等级保护工作的实施意见》（公通字[2004]66 号）要求抓紧建立信息安全等级保护制度，定期对信息系统的安全状况进行检测评估。2006 年公安部等四部委联合签发的《信息安全等级保护管理办法（试行）》（公通字[2006]7 号）进一步要求信息系统运营、使用单位应按照相关技术标准对信息系统进行安全测评，符合要求的，方可投入使用。本标准依据上述有关国家政策法规、部门规章的要求，从安全控制测评和系统整体测评两大方面提出信息系统分等级进行安全测试评估的技术要求。

信息安全等级保护要求不同安全等级的信息系统应具有不同的安全保护能力，通过在安全技术和安全管理上选用与安全等级相适应的安全控制来实现。安全技术上的安全控制分别从物理安全、网络安全、主机系统安全、应用安全和数据安全等层面对信息系统的运行和资源实施保护。安全管理上的安全控制分别从安全管理机构、安全管理制度、人员安全管理、系统建设管理和系统运维管理等方面对信息系统的运行和资源实施管理。本标准的安全控制测评就是对安全技术和安全管理上各个层面的安全控制分别提出不同安全等级的测试评估要求。

分布在信息系统中的安全技术和安全管理上不同的安全控制，通过连接、交互、依赖、协调、协同等相互关联关系，共同作用于信息系统的安全功能，使信息系统的整体安全功能与信息系统的结构以及安全控制间、层面间和区域间的相互关联关系密切相关。因此，本标准在安全控制测评的基础上，提出了系统整体测评的要求，描述了安全控制间、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功能影响的测试评估要求。

如果没有特殊指定，本标准中的信息系统仅指计算机信息系统，对基础信息网络和其他信息系统的信息安全等级保护测试评估可以参照本标准执行。

信息系统安全等级保护

测评准则

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，包括第一级、第二级、第三级和第四级信息系统安全控制测评要求和系统整体测评要求。本标准没有规定第五级信息系统安全控制测评的具体内容要求。

本标准适用于测评机构、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，用以评价信息系统是否达到与其安全等级相适应的保护要求。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。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

GB/T xxx-2005 信息系统安全等级保护基本要求

3 术语和定义

GB/T 5271.8-2001 和 **GB/T xxx-2005 信息系统安全等级保护基本要求**所确立的以及下列术语和定义适用于本标准。

3.1

等级测评 evaluation and testing for classified security protection

测评机构、信息系统的主管部门及运营使用单位针对信息系统的安全保护情况进行的信息安全等级保护相关标准要求的符合性测试评定工作。

3.2

测评单元 evaluation and testing unit

安全控制测评的最小工作单位，由测评项、测评方式、测评对象、测评实施和结果判定等组成，分别描述测评目的和内容、测评使用的方式方法、测试过程中涉及的测评对象、具体测试实施取证过程要求和测评证据的结果判定规则与方法。

3.3

测评强度 evaluation and testing intensity

测评的广度和深度，体现测评工作的实际投入程度。

3.4

访谈 interview

测评人员通过与信息系统有关人员（个人/群体）进行交流、讨论等活动，获取证据以证明信息系统安全等级保护措施是否有效的一种方法。

3.5

检查 examine

不同于行政执法意义上的监督检查，是指测评人员通过对测评对象进行观察、查验、分析等活动，获取证据以证明信息系统安全等级保护措施是否有效的一种方法。

3.6

测试 test

测评人员通过对测评对象按照预定的方法/工具使其产生特定的行为等活动，查看、分

析输出结果，获取证据以证明信息系统安全等级保护措施是否有效的一种方法。

3.7

被测系统 information system under evaluation and testing

处在信息安全等级保护安全测试评估之下的信息系统。

3.8

安全控制间安全测评 evaluation and testing between security controls

测评分析在同一区域和层面内两个或者两个以上不同安全控制之间由于存在连接、交互、依赖、协调、协同等相互关联关系而产生的安全功能增强、补充或削弱等关联作用对信息系统整体安全保护能力的影响。

3.9

层面间安全测评 evaluation and testing between lays

测评分析在同一区域内两个或者两个以上不同层面之间由于存在连接、交互、依赖、协调、协同等相互关联关系而产生的安全功能增强、补充或削弱等关联作用对信息系统安全保护能力的影响。

3.10

区域间安全测评 evaluation and testing between areas

测评分析两个或者两个以上不同物理逻辑区域之间由于存在连接、交互、依赖、协调、协同等相互关联关系而产生的安全功能增强、补充或削弱等关联作用对信息系统安全保护能力的影响。

4 总则

4.1 测评原则

a) 客观性和公正性原则

虽然测评工作不能完全摆脱个人主张或判断，但测评人员应当没有偏见，在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式和解释，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，都应基于结果适用于目前的系统，并且能够反映出目前系统的安全状态基础之上。

c) 可重复性和可再现性原则

不论谁执行测评，依照同样的要求，使用同样的测评方式，对每个测评实施过程的重复执行应该得到同样的结果。可再现性和可重复性的区别在于，前者与不同测评者测评结果的一致性有关，后者与同一测评者测评结果的一致性有关。

d) 结果完善性原则

测评所产生的结果应当证明是良好的判断和对测评项的正确理解。测评过程和结果应当服从正确的测评方法以确保其满足了测评项的要求。

4.2 测评内容

4.2.1 基本内容

对信息系统安全等级保护状况进行测试评估，应包括两个方面的内容：一是安全控制测评，主要测评信息安全等级保护要求的基本安全控制在信息系统中的实施配置情况；二是系统整体测评，主要测评分析信息系统的整体安全性。其中，安全控制测评是信息系统整体安全测评的基础。

对安全控制测评的描述，使用测评单元方式组织。测评单元分为安全技术测评和安全管

理测评两大类。安全技术测评包括：物理安全、网络安全、主机系统安全、应用安全和数据安全等五个层面上的安全控制测评；安全管理测评包括：安全管理机构、安全管理制度、人员安全管理、系统建设管理和系统运维管理等五个方面的安全控制测评。

系统整体测评涉及到信息系统的整体拓扑、局部结构，也关系到信息系统的具体安全功能实现和安全控制配置，与特定信息系统的实际情况紧密相关，内容复杂且充满系统个性。因此，全面地给出系统整体测评要求的完整内容、具体实施方法和明确的结果判定方法是很困难的。测评人员应根据特定信息系统的具体情况，结合本标准要求，确定系统整体测评的具体内容，在安全控制测评的基础上，重点考虑安全控制间、层面间以及区域间的相互关联关系，测评安全控制间、层面间和区域间是否存在安全功能上的增强、补充和削弱作用以及信息系统整体结构安全性、不同信息系统之间整体安全性等。

4.2.2 测评单元

测评单元是安全控制测评的基本工作单位，由测评项、测评对象、测评方式、测评实施和结果判定组成，如图 1 所示。

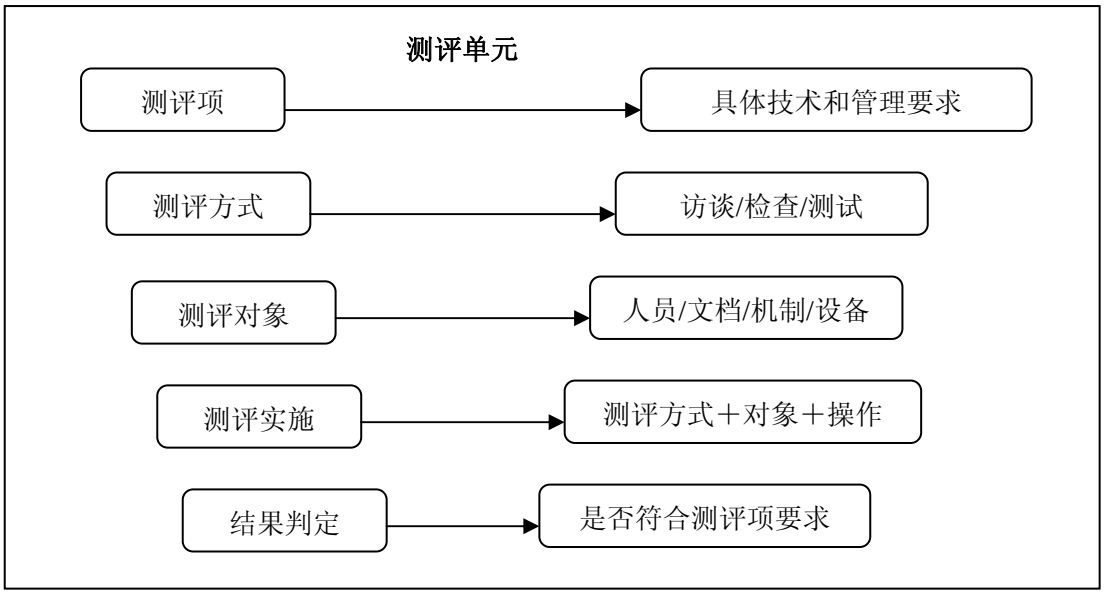

图 1 测评单元构成

测评项描述测评目的和测评内容，与信息安全等级保护要求的基本安全控制要求相一致。

测评方式是指测评人员依据测评目的和测评内容应选取的、实施特定测评操作的方式方法，包括三种基本测评方式：访谈、检查和测试。

测评对象是测评实施过程中涉及到的信息系统的构成成分，是客观存在的人员、文档、机制或者设备等。测评对象是根据该测评单元中的测评项要求提出的，与测评项的要求相适应。一般来说，实施测评时，面临的具体测评对象可以是单个人员、文档、机制或者设备等，也可能是由多个人员、文档、机制或者设备等构成的集合，它们分别需要使用到某个特定安全控制的功能。

测评实施是测评单元的主要组成部分，它是依据测评目的，针对具体测评内容开发出来的具体测评执行实施过程要求。测评实施描述测评过程中涉及到的具体测评方式、内容以及需要实现的和/或应该取得的测评结果。在测评实施过程描述中使用助动词“应（应该）”，表示这些过程是强制性活动，测评人员为作出结论必须完成这些过程；使用助动词“可（可以）”表示这些过程是非强制性活动，对测评人员作出结论没有根本性影响，因此测评人员可根据实际情况选择完成这些过程。

结果判定描述测评人员执行完测评实施过程，产生各种测评证据后，如何依据这些测评证据来判定被测系统是否满足测评项要求的方法和原则。在给出整个测评单元的测评结论前，需要先给出单项测评实施过程的结论。一般来说，单项测评实施过程的结论判定不是直接的，常常需要测评人员的主观判断，通常认为取得正确的、关键性证据，该单项测评实施过程就得到满足。某些安全控制可能在多个具体测评对象上实现（如主机系统的身份鉴别），在测评时发现只有部分测评对象上的安全控制满足要求，它们的结果判定应根据实际情况给出。对某些安全机制的测评要求采取渗透测试，主要是为了使测评强度与信息系统的安全等级相一致，渗透测试的测试结果一般不用到测评单元的结果判定中。如果某项测评实施过程在特定信息系统中不适用或者不能按测评实施过程取得相应证据，而测评人员能够采用其他实施手段取得等同的有效证据，则可判定该测评实施项为肯定。

4.2.3 测评强度

测评强度体现测评工作的实际投入程度，反映出测评的广度和深度。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，测评的深度越深，越需要在细节上展

开，因此就越需要更多的投入。投入越多就越能为测评提供更好的保证，体现测评强度越强。测评的广度和深度落实到访谈、检查和测试等三种基本测评方式上，其含义有所不同，体现出测评实施过程中访谈、检查和测试的投入程度不同。可以通过测评广度和深度来描述访谈、检查和测试三种测评方式的测评强度。

信息安全等级保护要求不同安全等级的信息系统应具有不同的安全保护能力，满足相应安全等级的保护要求。测评验证不同安全等级的信息系统是否达具有相应安全等级的安全保护能力，是否满足相应安全等级的保护要求，需要实施与其安全等级相适应的测评评估，付出相应的工作投入，达到应有的测评强度。信息安全等级保护要求第一级到第四级信息系统的测评强度在总体上可以反映在访谈、检查和测试等三种基本测评方式的测评广度和深度上，体现在具体的测评实施过程中（具体见附录 A）。

4.3 结果重用

在信息系统所有安全控制中，有一些安全控制是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。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、固件组成部分，对于此类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），对其测评必须在信息系统分发到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，系统所属的机构同在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对有效资源可能是一种浪费，因此，可以在一个选定的信息系统中进行测评，而在此场地的其他信息系统直接重用这些测评结果。

4.4 使用方法

从第 5 章到第 8 章，描述了第一级、第二级、第三级和第四级安全控制测评的测试评估要求，分为安全技术测评和安全管理测评两个小节。

信息系统进行信息安全等级保护建设时，可能会选择使用与其安全等级不相同的安全控制来保护信息系统，如安全等级为第三级的信息系统，可能选择使用第二级中安全技术部分上的某些安全控制。因此，测评人员应根据特定信息系统选择使用的安全控制来选择本标准中相应等级安全控制测评中的测评单元。

测评人员在选择完相应测评单元后，应根据信息系统的实际情况，结合第十章系统整体测评的要求，进一步细化测评实施过程，开发相应测评方案。

测评过程中，测评人员应注意测评记录和证据的接收、处理、存储和销毁，保护其在测评期间免遭改变/遗失，并保守秘密。

测评的最终输出是测评报告，测评报告应给出各个测评单元的测评结论，并报告信息系统的整体安全测试评估分析结果。

5 第一级安全控制测评

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 测评项

a） 机房出入应有专人负责，机房设施，进入机房的人员登记在案。

5.1.1.1.2 测评方式

访谈，检查。

5.1.1.1.3 测评对象

物理安全负责人，机房安全管理制度，进出机房的登记记录。

5.1.1.1.4 测评实施

a) 应访谈物理安全负责人，了解具有哪些控制机房进出的能力；
b) 可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) 应检查机房是否有进出机房的登记记录。

5.1.1.1.5 结果判定

a) 5.1.1.1.4 a），至少应包括制订了机房出入的管理制度，指定了专人负责机房出入，对进入的人员登记在案，则该项为肯定；
b) 5.1.1.1.4 a）、c）均为肯定，则信息系统符合本单元测评项要求。

5.1.1.2 防盗窃和防破坏

5.1.1.2.1 测评项

a) 应将主要设备放置在物理受限的范围内；
b) 应对设备或主要部件进行固定，并设置明显的无法除去的标记。

5.1.1.2.2 测评方式

访谈，检查。

5.1.1.2.3 测评对象

物理安全负责人，机房设施，设备管理制度。

5.1.1.2.4 测评实施

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) 可检查是否有设备管理制度文档；
c) 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；
d) 应检查主要设备或设备的主要部件的固定情况，是否不易被移动或被搬走，是否设置明显的无法除去的标记。

5.1.1.2.5 结果判定

a) 5.1.1.2.4 a），至少应该包括制订了设备管理制度，主要设备放置位置做到安全可控,设备或主要部件进行了固定和标记，则该项为肯定；
b) 5.1.1.2.4 a）、c）-d）均为肯定，则信息系统符合本单元测评项要求。

5.1.1.3 防雷击

5.1.1.3.1 测评项

a) 机房建筑应设置避雷装置。

5.1.1.3.2 测评方式

访谈，检查。

5.1.1.3.3 测评对象

物理安全负责人，机房设施，建筑防雷设计/验收文档。

5.1.1.3.4 测评实施

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；
b) 可检查机房是否有建筑防雷设计/验收文档。

5.1.1.3.5 结果判定

a) 5.1.1.3.4 a），至少还应包括符合GB 50057－1994《建筑物防雷设计规范》（GB157《建筑防雷设计规范》）中的计算机机房防雷要求，如果在雷电频繁区域，是否装设浪涌电压吸收装置等，则该项为肯定；
b) 5.1.1.3.4 a）为肯定，则信息系统符合本单元测评项要求。

5.1.1.4 防火

5.1.1.4.1 测评项

a) 应设置灭火设备，并保持灭火设备的良好状态。

5.1.1.4.2 测评方式

访谈，检查。

5.1.1.4.3 测评对象

物理安全负责人，机房设施，机房安全管理制度，机房防火设计/验收文档。

5.1.1.4.4 测评实施

a) 应访谈物理安全负责人，询问机房是否设置了灭火设备，是否制订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，摆放位置是否合理，有效期是否合格；

c) 可检查有关机房消防的管理制度文档，检查机房是否有防火设计/验收文档。

5.1.1.4.5 结果判定

a) 5.1.1.4.4 a）、c）均为肯定，则信息系统符合本单元测评项要求。

5.1.1.5 防水和防潮

5.1.1.5.1 测评项

a) 应对穿过墙壁和楼板的水管增加必要的保护措施，如设置套管；

b) 应采取措施防止雨水通过屋顶和墙壁渗透。

5.1.1.5.2 测评方式

访谈，检查。

5.1.1.5.3 测评对象

物理安全负责人，机房设施，建筑防水和防潮设计/验收文档。

5.1.1.5.4 测评实施

a) 应访谈物理安全负责人，询问机房建设是否有防水防潮措施，是否出现过漏水和返潮事件；如果机房内有上/下水管安装，是否必要的保护措施，如设置套管等；

b) 可检查机房是否有建筑防水和防潮设计/验收文档；

c) 如果有管道穿过主机房墙壁和楼板处，应检查是否采取必要的保护措施，如设置套管等；

d) 应检查机房是否不存在屋顶和墙壁等出现过漏水、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、渗透和返潮现是否能够及时修复解决。

5.1.1.5.5 结果判定

a) 5.1.1.5.4 a）、c）-d）均为肯定，则信息系统符合本单元测评项要求。

5.1.1.6 温湿度控制

5.1.1.6.1 测评项

a) 应设置必要的温、湿度控制设施，使机房温、湿度的变化在设备运行所允许的范围之内。

5.1.1.6.2 测评方式

访谈，检查

5.1.1.6.3 测评对象

物理安全负责人，机房设施，温湿度控制设计/验收文档。

5.1.1.6.4 测评实施

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，是否有人负责此项工作；
b) 可检查机房是否有温湿度控制设计/验收文档；
c) 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GB 2887-89《计算站场地技术条件》的要求。

5.1.1.6.5 结果判定

a) 5.1.1.6.4 a）、c）均为肯定，则信息系统符合本单元测评项要求。

5.1.1.7 电力供应

5.1.1.7.1 测评项

a) 计算机系统供电应与其他供电分开；
b) 应设置稳压器和过电压防护设备。

5.1.1.7.2 测评方式

访谈，检查。

5.1.1.7.3 测评对象

物理安全负责人，机房设施，电力供应安全设计/验收文档。

5.1.1.7.4 测评实施

a) 应访谈物理安全负责人，询问计算机系统供电线路是否与其他供电分开；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) 可检查机房是否有电力供应安全设计/验收文档；
c) 应检查计算机供电线路，查看计算机系统供电是否与其他供电分开；
d) 应检查机房，查看计算机系统供电线路上的稳压器和过电压防护设备是否正常运行。

5.1.1.7.5 结果判定

a) 5.1.1.7.4 a）、c）-d）均为肯定，则信息系统符合本单元测评项要求。

5.1.2 网络安全

5.1.2.1 结构安全与网段划分

5.1.2.1.1 测评项

a) 主要网络设备的业务处理能力应满足基本业务需要；
b) 根据机构业务的特点，在满足基本业务需要的基础上，应合理设计网络接入及核心网络的带宽；
c) 应在业务终端与业务服务器之间进行路由控制，并建立安全的访问路径；
d) 应设计和绘制与当前运行情况相符的网络拓扑结构图。

5.1.2.1.2 测评方式

访谈，检查。

5.1.2.1.3 测评对象

网络结构，网络管理员，边界和关键网络设备，网络拓扑图，网络设计/验收文档。

5.1.2.1.4 测评实施

a) 可访谈网络管理员，询问信息系统中的边界和关键网络设备的业务处理能力是否满足基本业务需求；
b) 可访谈网络管理员，询问目前的网络接入及核心网络的带宽是否满足业务需要；
c) 可访谈网络管理员，询问网络设备上的路由控制策略措施有哪些，这些策略设计的目的是什么；

d） 应检查是否绘制有网络拓扑图，并检查拓扑图是否与当前运行情况一致；

e） 应检查网络设计/验收文档，查看是否有边界和关键网络设备的处理能力是否能满足基本业务需求的能力，网络接入及核心网络的带宽能否满足业务需要的设计或说明；

f） 应检查边界和关键网络设备，查看是否配置路由控制策略（如使用静态路由等）建立安全的访问路径。

5.1.2.1.5 结果判定

a） 如果 5.1.2.1.4 e）中缺少相应的文档，则该项为否定；

b） 5.1.2.1.4 d）-f）均为肯定，则信息系统符合本单元测评项要求。

5.1.2.2 网络访问控制

5.1.2.2.1 测评项

a） 应根据访问控制列表对源地址、目的地址、源端口、目的端口、协议等进行检查，允许/拒绝数据包出入。

5.1.2.2.2 测评方式

访谈，检查。

5.1.2.2.3 测评对象

安全员，边界网络设备。

5.1.2.2.4 测评实施

a） 可访谈安全员，询问采取网络访问控制的措施有哪些；询问访问控制策略的设计原则；询问网络访问控制设备具备的访问控制功能（如是基于状态的，还是基于包过滤等）；

b） 应检查边界网络设备（包括网络安全设备），查看是否有正确的访问控制列表（如 ACL）对数据的源地址、目的地址、源端口、目的端口、协议等进行控制。

5.1.2.2.5 结果判定

a） 5.1.2.2.4 b）为肯定，则信息系统符合本单元测评项要求。

5.1.2.3 拨号访问控制

5.1.2.3.1 测评项

a） 通过访问控制列表对系统资源实现允许或拒绝用户访问，控制粒度为用户组。

5.1.2.3.2 测评方式

访谈，检查。

5.1.2.3.3 测评对象

安全员，边界网络设备。

5.1.2.3.4 测评实施

a） 可访谈安全员，询问网络是否允许拨号访问网络；询问对拨号访问控制的策略是什么，采取何种技术手段实现（如使用防火墙还是使用路由器实现），拨号访问用户的权限分配原则是什么；

b） 应检查边界网络设备（如路由器，防火墙，认证网关），查看是否正确的配置了拨号访问控制列表（对系统资源实现允许或拒绝用户访问），并查看其控制粒度是否为用户组。

5.1.2.3.5 结果判定

a） 5.1.2.3.4 b）为肯定，则信息系统符合本单元测评项要求。

5.1.2.4 网络设备防护

5.1.2.4.1 测评项

a） 应对登录网络设备的用户进行身份鉴别；

b） 应具有登录失败处理功能，如结束会话、限制非法登录次数。

5.1.2.4.2 测评方式

访谈，检查。

5.1.2.4.3 测评对象

网络管理员，边界和关键网络设备（包含安全设备）。

5.1.2.4.4 测评实施

a） 可访谈网络管理员，询问对关键网络设备的防护措施有哪些；询问采取的网络设备的口令策略是什么；询问对关键网络设备的登录和验证方式做过何种特定配置；

b） 应检查边界和关键网络设备上的安全配置，查看是否对登录关键网络设备的用户进行身份鉴别；

c） 应检查边界和关键网络设备上的安全配置，查看是否对鉴别失败采取相应的措施（如是否有鉴别失败后锁定帐号等措施）；查看是否限制非法登录次数。

5.1.2.4.5 结果判定

a） 5.1.2.4.4 b）-c）均为肯定，则信息系统符合本单元测评项要求。

5.1.3 主机系统安全

5.1.3.1 身份鉴别

5.1.3.1.1 测评项

a） 应对登录操作系统和数据库系统的用户进行身份标识和鉴别；

b） 应具有登录失败处理功能，如结束会话、限制非法登录次数。

5.1.3.1.2 测评方式

访谈，检查。

5.1.3.1.3 测评对象

系统管理员，数据库管理员，核心服务器操作系统，核心数据库系统。

5.1.3.1.4 测评实施

a） 应检查服务器操作系统和数据库系统的身份鉴别功能是否具有等级保护一级以上或TCSEC C1级以上的测试报告；

b） 可访谈系统管理员，询问操作系统的身份标识与鉴别机制采取何种措施实现；

c） 应检查核心服务器操作系统，查看是否提供了身份鉴别措施（如用户名和口令等）；

d） 应检查核心服务器操作系统，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；

e） 应测试核心服务器操作系统，验证当进入操作系统时，是否先需要进行标识（如建立账号）；

f） 可访谈数据库管理员，询问数据库的身份标识与鉴别机制采取何种措施实现；

g） 应查看核心数据库系统，查看是否提供了身份鉴别措施（如用户名和口令等）；

h） 应检查核心数据库系统，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；

i） 应测试核心数据库系统，验证当进入数据库系统前是否必须进行标识（如建立账号）。

5.1.3.1.5 结果判定

a） 如果5.1.3.1.4 a）为肯定，则测评实施c）-e）和g）-i）为肯定；

b） 测评实施c）-e）和g）-i）均为肯定，则信息系统符合本单元测评项要求。

5.1.3.2 自主访问控制

5.1.3.2.1 测评项

a） 操作系统和数据库管理系统应依据安全策略控制用户对客体的访问；

b) 自主访问控制的覆盖范围应包括与信息安全直接相关的主体、客体及它们之间的操作；
c) 操作系统和数据库系统自主访问控制的粒度应达到主体为用户组/用户级，客体为文件、数据库表级；
d) 应由授权主体设置对客体访问和操作的权限；
e) 应严格限制默认用户的访问权限。

5.1.3.2.2 测评方式

检查。

5.1.3.2.3 测评对象

核心服务器操作系统，核心数据库系统，安全策略。

5.1.3.2.4 测评实施

a) 应检查服务器操作系统和数据库系统的自主访问控制功能是否具有等级保护一级以上或TCSEC C1级以上的测试报告；
b) 应检查服务器操作系统的安全策略，查看是否明确主体（如用户）以用户和/或用户组的身份规定对客体（如文件）的访问控制，覆盖范围是否包括与信息安全直接相关的主体（如用户）和客体（如文件）及它们之间的操作（如读或写）；
c) 应检查核心服务器操作系统，查看客体（如文件）的所有者是否可以改变其相应访问控制列表的属性，得到授权的用户是否可以改变相应客体访问控制列表的属性；
d) 应查看核心服务器操作系统，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（如限定在有限的范围内）；
e) 应检查数据库系统的安全策略，查看是否明确主体对客体的访问权限（如目录表访问控制/存取控制表访问控制等），是否允许主体（如用户）以用户和/或用户组的身份规定并控制对客体（如数据库表）的访问控制；
f) 应检查核心数据库系统，查看客体（如数据库表、视图、存储过程和触发器等）的所有者是否可以改变其相应访问控制列表的属性，得到授权的用户是否可以改变相应客体访问控制列表的属性；
g) 应检查核心数据库系统，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（如限定在有限的范围内）。

5.1.3.2.5 结果判定

a) 如果5.1.3.2.4 a）为肯定，则测评实施c）、d）、f）和g）为肯定；
b) 5.1.3.2.4 b）-i）均为肯定，则信息系统符合本单元测评项要求。

5.1.3.3 恶意代码防范

5.1.3.3.1 测评项

a) 重要业务处理服务器应安装实时检测与查杀恶意代码的软件产品。

5.1.3.3.2 测评方式

访谈，检查。

5.1.3.3.3 测评对象

系统安全员，重要服务器。

5.1.3.3.4 测评实施

a) 应访谈系统安全员，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情况如何；
b) 应检查重要服务器，查看是否安装实时检测与查杀恶意代码的软件产品（主要是防病毒产品）；查看实时检测与查杀恶意代码软件产品的厂家、名称和恶意代码库版本号。

5.1.3.3.5 结果判定

a) 如果5.1.3.3.4 a）中恶意代码实时检测与查杀措施的部署包括所有重要业务处理服务器，则该项为肯定；

b) 如果5.1.3.2.4 b）中的实时检测与查杀恶意代码软件产品厂家为正规厂家，该恶意代码库版本较新，则该项为肯定；

c) 5.1.3.2.4 a）-b）均为肯定，则信息系统符合本单元测评项要求。

5.1.4 应用安全

5.1.4.1 身份鉴别

5.1.4.1.1 测评项

a) 应对登录应用系统的用户进行身份标识和鉴别；

b) 应具有登录失败处理的功能，如结束会话、限制非法登录次数。

5.1.4.1.2 测评方式

访谈，检查。

5.1.4.1.3 测评对象

系统管理员，关键应用系统。

5.1.4.1.4 测评实施

a) 可访谈系统管理员，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；

b) 应访谈系统管理员，询问应用系统是否具有登录失败处理的功能，是如何进行处理的；

c) 应检查关键应用系统，查看其是否配备身份标识（如建立账号）和鉴别（如口令等）功能；

d) 应检查关键应用系统，查看其是否配备并使用登录失败处理功能（如限制非法登录次数，登录失败次数超过设定值则结束会话等）。

5.1.4.1.5 结果判定

a) 5.1.4.1.4 b）-d）均为肯定，则信息系统符合本单元测评项要求。

5.1.4.2 访问控制

5.1.4.2.1 测评项

a) 应控制应用系统用户对系统功能和用户数据的访问；

b) 应用系统自主访问控制的粒度应达到主体为用户组/用户级；

c) 应由授权主体设置用户对系统功能的操作和对数据访问的权限；

d) 应严格限制默认用户的访问权限。

5.1.4.2.2 测评方式

访谈，检查。

5.1.4.2.3 测评对象

系统管理员，关键应用系统，总体规划/设计文档。

5.1.4.2.4 测评实施

a) 可访谈系统管理员，询问业务系统是否提供访问控制措施，具体措施有哪些；

b) 应检查关键应用系统，查看系统是否提供访问控制机制；

c) 应检查关键应用系统，查看其是否有限制默认用户访问权限的功能，并已配置使用；

d) 应测试关键应用系统，可通过用不同权限的用户登录，查看其权限是否受到应用系统的限制，验证系统权限分离功能是否有效；

e) 应测试关键应用系统，可通过授权主体设置特定用户对系统功能进行操作和对数据进行访问的权限，然后以该用户登录，验证用户权限管理功能是否有效；

f） 应测试关键应用系统，可通过用默认用户登录，验证系统对默认用户访问权限的限制是否有效。

5.1.4.2.5 结果判定

a） 5.1.4.2.4 b）-f）均为肯定，则信息系统符合本单元测评项要求。

5.1.4.3 通信完整性

5.1.4.3.1 测评项

a） 通信双方应约定通信会话的方式，在进行通信时，双方根据会话方式判断对方报文的有效性。

5.1.4.3.2 测评方式

访谈，检查。

5.1.4.3.3 测评对象

安全员，关键应用系统，总体规划/设计文档。

5.1.4.3.4 测评实施

a） 可访谈安全员，询问业务系统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） 应检查设计/验收文档，查看其是否有关于系统是根据校验码（CRC校验）判断对方数据包的有效性的描述；

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。

5.1.4.3.5 结果判定

a） 5.1.4.3.4 b）-c）均为肯定，则信息系统符合本单元测评项要求。

5.1.4.4 软件容错

5.1.4.4.1 测评项

a） 应对通过人机接口输入或通过通信接口输入的数据进行有效性检验；

b） 在故障发生并中断退出时，提供故障类型和故障发生点的信息。

5.1.4.4.2 测评方式

访谈，检查。

5.1.4.4.3 测评对象

系统管理员，关键应用系统。

5.1.4.4.4 测评实施

a） 可访谈系统管理员，询问业务系统是否有保证软件具有容错能力的措施（如对人机接口输入或通过通信接口输入的数据进行有效性检验，在故障发生并中断退出时系统是否提供故障类型和故障发生点的信息等），具体措施有哪些；

b） 应检查关键应用系统，查看业务系统是否有对人机接口输入（如用户界面的数据输入）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，可通过输入的不同（如数据格式或长度等符合、不符合软件设定的要求）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，可通过制造一些故障（如系统异常等），查看系统是否提供故障类型和故障发生点的信息。

5.1.4.4.5 结果判定

a） 5.1.4.4.4 b）-d）均为肯定，则信息系统符合本单元测评项要求。

5.1.4.5 资源控制

5.1.4.5.1 测评项

a） 应对应用系统的最大并发会话连接数进行限制。

5.1.4.5.2 测评方式

访谈，检查。

5.1.4.5.3 测评对象

系统管理员，关键应用系统。

5.1.4.5.4 测评实施

a) 可访谈系统管理员，询问业务系统是否有资源控制的措施（如对应用系统的最大并发会话连接数进行限制等），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) 应测试关键应用系统，可通过对系统用超过最大并发会话连接数进行连接，验证系统能否正确地限制最大并发会话连接数。

5.1.4.5.5 结果判定

a) 5.1.4.5.4 b）-c）均为肯定，则信息系统符合本单元测评项要求。

5.1.4.6 代码安全

5.1.4.6.1 测评项

a) 应对应用程序进行恶意代码扫描，确认不存在恶意代码。

5.1.4.6.2 测评方式

访谈，检查。

5.1.4.6.3 测评对象

相关证明材料，关键应用系统。

5.1.4.6.4 测评实施

a) 可访谈系统管理员，询问业务系统是否有保证质量的措施（如系统是否有程序编写安全规范，开发人员是否参照规范编写代码），具体措施有哪些；

b) 应检查设计/验收文档和相关证明材料（证书），查看是否有对应用程序进行恶意代码扫描，确认不存在恶意代码的声明；

c) 应检查关键应用系统，查看代码的编制是否符合代码安全规范的要求。

5.1.4.6.5 结果判定

a) 5.1.4.6.4 b）-c）均为肯定，则信息系统符合本单元测评项要求。

5.1.5 数据安全

5.1.5.1 数据完整性

5.1.5.1.1 测评项

a) 应能够检测到系统管理数据、鉴别信息和用户数据在传输过程中完整性受到破坏；

b) 应能够检测到系统管理数据、鉴别信息和用户数据在存储过程中未授权的修改与破坏。

5.1.5.1.2 测评方式

访谈，检查。

5.1.5.1.3 测评对象

安全员，关键应用系统，设计/验收文档，相关证明性材料（如证书、检验报告等）。

5.1.5.1.4 测评实施

a) 应访谈安全员，询问业务系统数据在传输和存储过程中是否有完整性保证措施，具体措施有哪些；

b) 应检查操作系统、网络设备、数据库管理系统的设计/验收文档或相关证明性材料（如证书、检验报告等）等，查看其是否能检测/验证到系统管理数据（如 WINDOWS 域管理、目录管理数据）、鉴别信息（如用户名和口令）和用户数据（如用户数据文件）在传输过程中完整性受到破坏；能否检测/验证到系统管理数据（如

WINDOWS 注册表、系统文件）、身份鉴别信息（如用户名和口令存储文件）和用户数据（如用户数据文件）在存储过程中未授权的修改与破坏；如果有相关信息，查看其配置是否正确；

c） 应检查关键应用系统，查看其是否配备检测/验证系统管理数据、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/验证系统管理数据、身份鉴别信息和用户数据在存储过程中未授权修改与破坏的功能。

5.1.5.1.5 结果判定

a） 如果 5.1.5.1.4 b）缺少相关材料，则该项为否定；

b） 5.1.5.1.4 a）-c）均为肯定，则信息系统符合本单元测评项要求。

5.1.5.2 数据保密性

5.1.5.2.1 测评项

a） 网络设备、操作系统、数据库管理系统和应用系统应能防止对身份鉴别信息的未授权的访问。

5.1.5.2.2 测评方式

访谈，检查。

5.1.5.2.3 测评对象

系统管理员、网络管理员、安全员、数据库管理员，操作系统，网络设备，数据库系统，关键应用系统，设计/验收文档。

5.1.5.2.4 测评实施

a） 可访谈网络管理员，询问信息系统中的网络设备能否防止身份鉴别信息（如用户名和口令）在传输过程中未授权的访问；

b） 可访谈系统管理员，询问信息系统中的操作系统能否防止身份鉴别信息（如用户名和口令）在传输过程中未授权的访问；

c） 可访谈数据库管理员，询问信息系统中的数据库管理系统能否防止身份鉴别信息（如用户名和口令）在传输过程中未授权的访问；

d） 可访谈安全员，询问信息系统中的应用系统能否防止身份鉴别信息（如用户名和口令）在传输过程中未授权的访问；

e） 应检查操作系统、网络设备、数据库系统、关键应用系统设计/验收文档，查看其是否有防止身份鉴别信息（如用户名和口令）在传输过程中未授权的访问的描述；

f） 应检查关键应用系统，查看其是否配备防止身份鉴别信息（如用户名和口令）在传输过程中未授权访问的功能。

5.1.5.2.5 结果判定

a) 如果缺少设计/验收文档，5.1.5.2.4 e）为否定；

b) 5.1.5.2.4 e）-f）均为肯定，则信息系统符合本单元测评项要求。

5.1.5.3 数据备份和恢复

5.1.5.3.1 测评项

a） 应提供用户有选择的备份和恢复重要信息的功能。

5.1.5.3.2 测评方式

访谈，检查。

5.1.5.3.3 测评对象

系统管理员、网络管理员、安全员、数据库管理员，关键应用系统，操作系统、网络设备、数据库系统、关键应用系统。

5.1.5.3.4 测评实施

a） 可访谈网络管理员，询问信息系统中的网络设备是否具有对重要数据进行备份的功

能，配置如何；是否提供对重要信息进行恢复的功能；

b) 可访谈系统管理员，询问信息系统中的操作系统是否具有对重要数据进行备份的功能，配置如何；是否提供对重要信息进行恢复的功能；

c) 可访谈数据库管理员，询问信息系统中的数据库管理系统是否具有对重要数据进行备份的功能，配置如何；是否提供对重要信息进行恢复的功能；

d) 可访谈安全员，询问信息系统中的业务系统是否具有对重要数据进行备份的功能，配置如何；是否提供对重要信息进行恢复的功能；

e) 应检查操作系统、网络设备、数据库系统、关键应用系统，查看其是否配置有选择的备份和恢复重要信息恢复的功能，其配置是否正确。

5.1.5.3.5 结果判定

a) 5.1.5.3.4 e）为肯定，则信息系统符合本单元测评项要求。

5.2 安全管理测评

5.2.1 安全管理机构

5.2.1.1 岗位设置

5.2.1.1.1 测评项

a) 应设立系统管理人员、网络管理人员、安全管理人员岗位，定义各个工作岗位的职责。

5.2.1.1.2 测评方式

访谈，检查。

5.2.1.1.3 测评对象

安全主管，岗位职责分工文档。

5.2.1.1.4 测评实施

a) 应访谈安全主管，询问信息系统设置了哪些工作岗位（如机房管理员、系统管理员、网络管理员、安全员等重要岗位），是否明确各个岗位的职责分工；

b) 应检查岗位职责分工文档，查看定义的各个岗位职责是否包括机房管理员、系统管理员、网络管理员、安全员等重要岗位，各个岗位的职责范围是否清晰、明确。

5.2.1.1.5 结果判定

a) 5.2.1.1.4 a）-b）均为肯定，则信息系统符合本单元测评项要求。

5.2.1.2 人员配备

5.2.1.2.1 测评项

a) 应配备一定数量的系统管理人员、网络管理人员、安全管理人员，各个岗位的人员可以兼任。

5.2.1.2.2 测评方式

访谈，检查。

5.2.1.2.3 测评对象

安全主管，管理人员名单。

5.2.1.2.4 测评实施

a) 应访谈安全主管，询问各个安全管理岗位人员配备情况（按照岗位职责文件询问，包括机房管理员、系统管理员、网络管理员和安全员等重要岗位人员），包括数量、专职还是兼职等；

b) 应检查安全管理人员名单，查看其是否明确机房管理员、系统管理员、网络管理员和安全员等重要岗位人员的信息。

5.2.1.2.5 结果判定

a) 5.2.1.2.4 a）-b）均为肯定，则信息系统符合本单元测评项要求。

5.2.1.3 授权和审批

5.2.1.3.1 测评项

a) 应授权审批部门及批准人，对网络、应用、系统等重要资源的访问等关键活动进行审批。

5.2.1.3.2 测评方式

访谈，检查。

5.2.1.3.3 测评对象

安全主管，关键活动的批准人，审批文档。

5.2.1.3.4 测评实施

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) 应访谈关键活动的批准人，询问其对关键活动的审批范围包括哪些（如网络系统、应用系统、数据库管理系统、重要服务器和设备等重要资源的访问），审批程序如何；

c) 应检查经审批的文档，查看是否具有批准人的签字或审批部门的盖章。

5.2.1.3.5 结果判定

a) 5.2.1.3.4 a）-c）均为肯定，则信息系统符合本单元测评项要求。

5.2.1.4 沟通和合作

5.2.1.4.1 测评项

a) 应加强各类管理人员和组织内部机构之间的合作与沟通，定期或不定期召开协调会议，共同协助处理信息安全问题。

5.2.1.4.2 测评方式

访谈，检查。

5.2.1.4.3 测评对象

安全主管，安全管理人员，协调会议文件或会议记录。

5.2.1.4.4 测评实施

a) 应访谈安全主管，询问与组织机构内其他部门之间有哪些合作内容，沟通、合作方式有哪些，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，会议结果如何；

b) 应访谈安全管理人员（从系统管理员和安全员等人员中抽查），询问其与组织机构内其他部门人员，与内部其他管理人员之间的沟通方式和主要沟通内容有哪些；

c) 应检查部门间协调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。

5.2.1.4.5 结果判定

a) 5.2.1.4.4 a）-c）均为肯定，则信息系统符合本单元测评项要求。

5.2.2 安全管理制度

5.2.2.1 管理制度

5.2.2.1.1 测评项

a) 应制定信息安全工作的总体方针、政策性文件和安全策略等，说明机构安全工作的总体目标、范围、方针、原则、责任等；

b) 应建立日常管理活动中常用的安全管理制度，以规范安全管理活动，约束人员的行为。

5.2.2.1.2 测评方式

访谈，检查。

5.2.2.1.3 测评对象

安全主管，总体方针、政策性文件和安全策略文件，安全管理制度清单。

5.2.2.1.4 测评实施

a) 应访谈安全主管，询问是否制定信息安全工作的总体方针、政策性文件和安全策略，是否制定安全管理制度规范日常管理活动；

b) 应检查总体方针、政策性文件和安全策略文件，查看文件是否明确机构安全工作的总体目标、范围、方针、原则、责任等；

c) 应检查安全管理制度清单，查看是否覆盖物理、网络、主机系统、数据、应用和管理等层面。

5.2.2.1.5 结果判定

a) 5.2.2.1.4 a）-c）均为肯定，则信息系统符合本单元测评项要求。

5.2.2.2 制定和发布

5.2.2.2.1 测评项

a) 应授权或指定专门的人员负责制定安全管理制度；

b) 应组织相关人员对制定的安全管理进行论证和审定；

c) 安全管理制度应以某种方式发布到相关人员手中。

5.2.2.2.2 测评方式

访谈，检查。

5.2.2.2.3 测评对象

安全主管，管理人员，评审记录。

5.2.2.2.4 测评实施

a) 应访谈安全主管，询问是否有专人负责制订安全管理制度，负责人是何人；

b) 应访谈管理人员（负责制定管理制度的人员），询问安全管理制度的制定程序，是否对制定的安全管理制度进行论证和审定，论证和审定方式如何（如召开评审会、函审、内部审核等），发布方式有哪些；

c) 应检查管理制度评审记录，查看是否具有相关人员的评审意见。

5.2.2.2.5 结果判定

a) 5.2.2.2.4 a）-c）均为肯定，则信息系统符合本单元测评项要求。

5.2.3 人员安全管理

5.2.3.1 人员录用

5.2.3.1.1 测评项

a) 应保证被录用人具备基本的专业技术水平和安全管理知识；

b) 应对被录用人的身份和专业资格等进行审查；

c) 应对被录用人说明其角色和职责。

5.2.3.1.2 测评方式

访谈，检查。

5.2.3.1.3 测评对象

人事负责人，人事工作人员，人员录用要求管理文档，人员审查文档或记录。

5.2.3.1.4 测评实施

a) 应访谈人事负责人，询问在人员录用时对人员条件有哪些要求，目前录用的安全管理和技术人员是否有能力完成与其职责相对应的工作；

b) 应访谈人事工作人员，询问在人员录用时是否对被录用人的身份和专业资格进行证实，录用后是否对其说明工作职责；

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。

5.2.3.1.5 结果判定

a） 5.2.3.1.4 a）-d）均为肯定，则信息系统符合本单元测评项要求。

5.2.3.2 人员离岗

5.2.3.2.1 测评项

a） 应立即终止由于各种原因即将离岗的员工的所有访问权限；

b） 应取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备。

5.2.3.2.2 测评方式

访谈，检查。

5.2.3.2.3 测评对象

安全主管，安全处理记录。

5.2.3.2.4 测评实施

a） 应访谈安全主管，询问是否及时终止离岗人员所有访问权限，取回各种身份证件、钥匙、徽章等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。

5.2.3.2.5 结果判定

a） 5.2.3.2.4 a）-b）均为肯定，则信息系统符合本单元测评项要求。

5.2.3.3 安全意识教育和培训

5.2.3.3.1 测评项

a） 应对各类人员进行安全意识教育；

b） 应告知人员相关的安全责任和惩戒措施。

5.2.3.3.2 测评方式

访谈。

5.2.3.3.3 测评对象

安全主管，安全员。

5.2.3.3.4 测评实施

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，告知相关的安全知识、安全责任和惩戒措施，以什么形式进行，效果如何；

b） 应访谈安全员，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。

5.2.3.3.5 结果判定

a） 如果5.2.3.3.4 b）访谈人员能够表述清楚询问内容，且安全职责和惩戒措施表述与文件描述一致，则该项为肯定；

b） 5.2.3.3.4 a）-b）均为肯定，则信息系统符合本单元测评项要求。

5.2.3.4 第三方人员访问管理

5.2.3.4.1 测评项

a） 第三方人员应在访问前与机构签署安全责任合同书或保密协议。

5.2.3.4.2 测评方式

访谈，检查。

5.2.3.4.3 测评对象

安全主管，安全责任合同书或保密协议。

5.2.3.4.4 测评实施

a) 应访谈安全主管，询问对第三方人员（如向系统提供服务的系统软、硬件维护人员，业务合作伙伴等）的访问采取哪些管理措施，是否要求第三方人员访问前与机构签署安全责任合同书或保密协议；

b) 应检查安全责任合同书或保密协议，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。

5.2.3.4.5 结果判定

a) 5.2.3.4.4 a）-b）均为肯定，则信息系统符合本单元测评项要求。

5.2.4 系统建设管理

5.2.4.1 系统定级

5.2.4.1.1 测评项

a) 应明确信息系统划分的方法；

b) 应确定信息系统的安全保护等级；

c) 应以书面的形式定义确定了安全保护等级的信息系统的属性，包括使命、业务、网络、硬件、软件、数据、边界、人员等；

d) 应确保信息系统的定级结果经过相关部门的批准。

5.2.4.1.2 测评方式

访谈，检查。

5.2.4.1.3 测评对象

安全主管，系统划分文档，系统定级文档，系统属性说明文档。

5.2.4.1.4 测评实施

a) 应访谈安全主管，询问划分信息系统的方法和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，是否对其进行明确描述；定级结果是否获得了相关部门（如上级主管部门）的批准；

b) 应检查系统划分相关文档，查看文档是否明确描述信息系统划分的方法和理由；

c) 应检查系统定级文档，查看文档是否给出信息系统的安全保护等级，查看定级结果是否有相关部门的批准盖章；

d) 应检查系统属性说明文档，查看文档是否明确了系统使命、业务、网络、硬件、软件、数据、边界、人员等。

5.2.4.1.5 结果判定

a) 5.2.4.1.4 b）没有上级主管部门的，如果有安全主管的批准，则该项为肯定；

b) 5.2.4.1.4 a）-d）均为肯定，则信息系统符合本单元测评项要求。

5.2.4.2 安全方案设计

5.2.4.2.1 测评项

a) 应根据系统的安全级别选择基本安全措施，依据风险评估的结果补充和调整安全措施；

b) 应以书面的形式描述对系统的安全保护要求和策略、安全措施等内容，形成系统的安全方案；

c) 应对安全方案进行细化，形成能指导安全系统建设和安全产品采购的详细设计方案。

5.2.4.2.2 测评方式

访谈，检查。

5.2.4.2.3 测评对象

系统建设负责人，安全方案，详细设计方案。

5.2.4.2.4 测评实施

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，是否依据风险评估的结果补充和调整安全措施，做过哪些调整；
b) 应访谈系统建设负责人，询问系统选择和调整基本安全措施是否依据系统安全级别和风险评估的结果；
c) 应访谈系统建设负责人，询问是否制定系统的安全方案并根据安全方案制定出系统详细设计方案指导安全系统建设和安全产品采购；
d) 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对应的安全措施等内容；
e) 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。

5.2.4.2.5 结果判定

a) 5.2.4.2.4a）-e）均为肯定，则信息系统符合本单元测评项要求。

5.2.4.3 产品采购

5.2.4.3.1 测评项

a) 应确保安全产品的使用符合国家的有关规定。

5.2.4.3.2 测评方式

访谈。

5.2.4.3.3 测评对象

系统建设负责人。

5.2.4.3.4 测评实施

a) 应访谈系统建设负责人，询问系统信息安全产品的采购情况，是否有相关要求，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（边界安全设备、重要服务器操作系统、数据库等）是否符合国家的有关规定。

5.2.4.3.5 结果判定

a) 5.2.4.3.4b）为肯定，则信息系统符合本单元测评项要求。

5.2.4.4 自行软件开发

5.2.4.4.1 测评项

a) 应确保开发环境与实际运行环境物理分开；
b) 应确保系统开发文档由专人负责保管，系统开发文档的使用受到控制。

5.2.4.4.2 测评方式

访谈，检查。

5.2.4.4.3 测评对象

系统建设负责人，文档使用控制记录。

5.2.4.4.4 测评实施

a) 应访谈系统建设负责人，询问系统是否自主开发软件，自主开发是否有相应的控制措施，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，询问系统开发文档是否由专人负责保管，负责人是何人，如何控制使用（如限制使用人员范围并做使用登记等）；
c) 应检查软件开发环境与系统运行环境在物理上是否是分开的；
d) 应检查是否具有系统开发文档的使用控制记录。

5.2.4.4.5 结果判定

a) 5.2.4.4.4a）-d）均为肯定，则信息系统符合本单元测评项要求。

5.2.4.5 外包软件开发

5.2.4.5.1 测评项

a) 应与软件开发单位签订协议，明确知识产权的归属和安全方面的要求；

b) 应根据协议的要求检测软件质量；

c) 应在软件安装之前检测软件包中可能存在的恶意代码。

5.2.4.5.2 测试方法

访谈，检查。

5.2.4.5.3 测试对象

系统建设负责人，软件开发协议。

5.2.4.5.4 测评实施

a) 应访谈系统建设负责人，询问在外包软件前是否对软件开发单位以书面形式（如软件开发安全协议）规范软件开发单位的责任、开发过程中的安全行为、开发环境要求和软件质量等相关内容；

b) 应访谈系统建设负责人，询问软件交付前是否对软件功能和性能等进行验收检测，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；

c) 应检查软件开发协议是否规定知识产权归属、安全行为等内容。

5.2.4.5.5 结果判定

a) 5.2.4.5.4 a）－c）均为肯定，则信息系统符合本单元测评项要求。

5.2.4.6 工程实施

5.2.4.6.1 测评项

a) 应与工程实施单位签订与安全相关的协议，约束工程实施单位的行为。

5.2.4.6.2 测试方法

访谈，检查。

5.2.4.6.3 测试对象

系统建设负责人，工程安全建设协议。

5.2.4.6.4 测评实施

a) 应访谈系统建设负责人，询问是否以书面形式（如工程安全建设协议）约束工程实施方的工程实施行为；

b) 应检查工程安全建设协议，查看其内容是否覆盖工程实施方的责任、任务要求和质量要求等方面内容，约束工程实施行为。

5.2.4.6.5 结果判定

a) 5.2.4.6.4 a）－b）均为肯定，则信息系统符合本单元测评项要求。

5.2.4.7 测试验收

5.2.4.7.1 测评项

a) 应对系统进行安全性测试验收；

b) 应在测试验收前根据设计方案或合同要求等制订测试验收方案，测试验收过程中详细记录测试验收结果，形成测试验收报告；

c) 应组织相关部门和相关人员对系统测试验收报告进行审定，没有疑问后由双方签字。

5.2.4.7.2 测试方法

访谈，检查。

5.2.4.7.3 测试对象

系统建设负责人，系统测试方案，系统测试记录，系统测试报告，系统验收报告。

5.2.4.7.4 测评实施

a) 应访谈系统建设负责人，询问在信息系统正式运行前，是否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，询问是否对测试过程（包括测试前、测试中和测试后）进行文档化要求，是否对测试报告进行符合性审定；

c) 应检查工程测试方案，查看其是否对参与测试部门、人员和现场操作过程等进行要求；查看测试记录是否详细记录了测试时间、人员、现场操作过程和测试结果等方面内容；查看测试报告是否提出存在问题及改进意见等；

d) 应检查是否具有系统验收报告。

5.2.4.7.5 结果判定

a) 5.2.4.7.4 a）—d）均为肯定，则信息系统符合本单元测评项要求。

5.2.4.8 系统交付

5.2.4.8.1 测评项

a) 应明确系统的交接手续，并按照交接手续完成交接工作；

b) 应由系统建设方完成对委托建设方的运维技术人员的培训；

c) 应由系统建设方提交系统建设过程中的文档和指导用户进行系统运行维护的文档。

5.2.4.8.2 测试方法

访谈，检查。

5.2.4.8.3 测试对象

系统建设负责人，系统交付清单。

5.2.4.8.4 测评实施

a) 应访谈系统建设负责人，询问交接手续是什么，系统交接工作是否按照该手续办理，是否根据交付清单对所交接的设备、文档、软件等进行清点，交付清单是否满足合同的有关要求；

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，系统建设方是否对运维技术人员进行过培训，针对哪些方面进行过培训，系统是否具有支持其独立运行维护的文档；

c) 应检查系统交付清单，查看其是否具有系统建设文档（如系统建设方案）、指导用户进行系统运维的文档（如服务器操作规程书）以及系统培训手册等文档名称。

5.2.4.8.5 结果判定

a) 5.2.4.8.4 a）—c）均为肯定，则信息系统符合本单元测评项要求。

5.2.4.9 安全服务商选择

5.2.4.9.1 测评项

a) 应确保安全服务商的选择符合国家的有关规定。

5.2.4.9.2 测试方法

访谈。

5.2.4.9.3 测试对象

系统建设负责人。

5.2.4.9.4 测评实施

a) 应访谈系统建设负责人，询问对信息系统进行安全规划、设计、实施、维护、测评等服务的安全服务单位是否符合国家有关规定。

5.2.4.9.5 结果判定

a) 5.2.4.9.4 a）为肯定，则信息系统符合本单元测评项要求。

5.2.5 系统运维管理

5.2.5.1 环境管理

5.2.5.1.1 测评项

a) 应对机房供配电、空调、温湿度控制等设施指定专人或专门的部门定期进行维护管理；
b) 应配备机房安全管理人员，对机房的出入、服务器的开机或关机等工作进行管理；
c) 应建立机房安全管理制度，对有关机房物理访问，物品带进、带出机房和机房环境安全等方面的管理作出规定。

5.2.5.1.2 测评方式

访谈，检查。

5.2.5.1.3 测评对象

物理安全负责人，机房安全管理制度。

5.2.5.1.4 测评实施

a) 应访谈物理安全负责人，询问是否指定专人或部门负责机房基本设施（如空调、供配电设备等）的定期维护管理，由何部门/何人负责，维护周期多长；
b) 应访谈物理安全负责人，询问是否指定人员负责机房安全管理工作，对机房的出入管理是否要求制度化；
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。

5.2.5.1.5 结果判定

a) 5.2.5.1.4 a）-c）均为肯定，则信息系统符合本单元测评项要求。

5.2.5.2 资产管理

5.2.5.2.1 测评项

a) 应建立资产安全管理制度，规定信息系统资产管理的责任人员或责任部门；
b) 应编制并保存与信息系统相关的资产、资产所属关系、安全级别和所处位置等信息的资产清单。

5.2.5.2.2 测评方式

访谈，检查。

5.2.5.2.3 测评对象

安全主管，物理安全负责人，资产清单，资产安全管理制度。

5.2.5.2.4 测评实施

a) 应访谈安全主管，询问是否指定资产管理的责任人员或部门，由何部门/何人负责；
b) 应访谈物理安全负责人，询问是否对资产管理要求文档化；
c) 应检查资产安全管理制度，查看是否明确资产管理的责任部门、责任人等方面要求；
d) 应检查资产清单，查看其内容是否覆盖资产责任人、所属级别、所处位置和所属部门等方面。

5.2.5.2.5 结果判定

a) 5.2.5.2.4 a）-d）均为肯定，则信息系统符合本单元测评项要求。

5.2.5.3 介质管理

5.2.5.3.1 测评项

a) 应确保介质存放在安全的环境中，并对各类介质进行控制和保护，以防止被盗、被毁、被未授权修改以及信息的非法泄漏；
b) 应有介质的存储、归档、登记和查询记录，并根据备份及存档介质的目录清单定期盘点。

5.2.5.3.2 测评方式

访谈，检查。

5.2.5.3.3 测评对象

资产管理员，介质管理记录。

5.2.5.3.4 测评实施

a) 应访谈资产管理员，询问介质的存放环境是否有保护措施，防止其被盗、被毁、被未授权修改以及信息的非法泄漏；

b) 应访谈资产管理员，询问是否对介质的使用管理要求文档化，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的存储、归档、借用等情况。

5.2.5.3.5 结果判定

a) 如果5.2.5.3.4 a）中在防火、防水、防盗等方面均有措施，则该项为肯定；

b) 5.2.5.3.4 a）-c）均为肯定，则信息系统符合本单元测评项要求。

5.2.5.4 设备管理

5.2.5.4.1 测评项

a) 应对信息系统相关的各种设施、设备、线路等指定专人或专门的部门定期进行维护管理；

b) 应对信息系统的各种软硬件设备的选型、采购、发放或领用等过程的申报、审批和专人负责作出规定；

c) 应按操作规程实现服务器的启动/停止、加电/断电等操作，并根据业务系统的要求维护好系统配置和服务设定；

d) 应对终端计算机、工作站、便携机、系统和网络等设备的操作和使用过程进行规范化管理。

5.2.5.4.2 测评方式

访谈，检查。

5.2.5.4.3 测评对象

资产管理员，设备审批管理文档，设备使用管理文档，服务器操作规程。

5.2.5.4.4 测评实施

a) 应访谈资产管理员，询问是否对各类设施、设备指定专人或专门部门进行定期维护，由何部门/何人维护，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、采购和发放等）进行审批控制，设备的操作和使用是否要求规范化管理；

c) 应检查设备使用管理文档，查看其内容是否对终端计算机、便携机、网络设备等使用、操作原则、注意事项等方面作出规定；

d) 应检查设备审批、发放管理文档，查看其内容是否对设备选型、采购和发放等环节的申报和审批作出规定；

e) 应检查服务器操作规程，查看其内容是否覆盖服务器如何启动、停止、加电和断电等操作。

5.2.5.4.5 结果判定

a) 5.2.5.4.4 a）-e）均为肯定，则信息系统符合本单元测评项要求。

5.2.5.5 监控管理

5.2.5.5.1 测评项

a) 应了解服务器的CPU、内存、进程、磁盘使用情况。

5.2.5.5.2 测评方式

访谈。

5.2.5.5.3 测评对象

安全主管，系统运维负责人。

5.2.5.5.4 测评实

a) 应访谈系统运维负责人，询问是否经常查看主要服务器的各项资源指标，如CPU、内存、进程和磁盘等使用情况。

5.2.5.5.5 结果判定

a) 5.2.5.5.4 a）为肯定，则信息系统符合本单元测评项要求。

5.2.5.6 网络安全管理

5.2.5.6.1 测评项

a) 应指定专人对网络进行管理，负责运行日志、网络监控记录的日常维护和报警信息分析和处理工作；

b) 应根据厂家提供的软件升级版本对网络设备进行更新，并在更新前对现有的重要文件进行备份；

c) 应进行网络系统漏洞扫描，对发现的网络系统安全漏洞进行及时的修补。

5.2.5.6.2 测试方法

访谈，检查。

5.2.5.6.3 测试对象

安全主管，网络管理员，网络漏洞扫描报告。

5.2.5.6.4 测评实施

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；

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、配置数据等）进行备份；是否对网络设备进行过漏洞扫描，对扫描出的漏洞是否及时修补；

c) 应检查网络漏洞扫描报告，查看其内容是覆盖网络存在的漏洞、漏洞级别、原因分析和改进意见等方面。

5.2.5.6.5 结果判定

a) 5.2.5.6.4 a）-c）均为肯定，则信息系统符合本单元测评项要求。

5.2.5.7 系统安全管理

5.2.5.7.1 测评项

a) 应指定专人对系统进行管理，删除或者禁用不使用的系统缺省账户；

b) 应定期安装系统的最新补丁程序，并根据厂家提供的可能危害计算机的漏洞进行及时修补，并在安装系统补丁前对现有的重要文件进行备份；

c) 应根据业务需求和系统安全分析确定系统的访问控制策略，系统访问控制策略用于控制分配信息系统、文件及服务的访问权限。

5.2.5.7.2 测试方法

访谈。

5.2.5.7.3 测试对象

安全主管，安全员，系统管理员。

5.2.5.7.4 测评实施

a) 应访谈安全主管，询问是否指定专人负责系统安全管理；

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和进行漏洞修补，在安

装系统补丁前是否对重要文件（系统配置、系统用户数据等）进行备份；对不常用的系统缺省用户是否采取了一定的处理手段阻止其继续使用（如删除或禁用）；

c） 应访谈安全员，询问是否制定系统访问控制策略。

5.2.5.7.5 结果判定

a） 5.2.5.7.4 a）-c）均为肯定，则信息系统符合本单元测评项要求。

5.2.5.8 恶意代码防范管理

5.2.5.8.1 测评项

a） 应提高所有用户的防病毒意识，告知及时升级防病毒软件；

b） 应在读取移动存储设备（如软盘、移动硬盘、光盘）上的数据以及网络上接收文件或邮件之前，先进行病毒检查，对外来计算机或存储设备接入网络系统之前也要进行病毒检查。

5.2.5.8.2 测试方法

访谈。

5.2.5.8.3 测试对象

系统运维负责人。

5.2.5.8.4 测评实施

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，如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。

5.2.5.8.5 结果判定

a） 5.2.5.8.4 a）为肯定，则信息系统符合本单元测评项要求。

5.2.5.9 备份与恢复管理

5.2.5.9.1 测评项

a） 应识别需要定期备份的重要业务信息、系统数据及软件系统等；

b） 应规定备份信息的备份方式（如增量备份或全备份等）、备份频度（如每日或每周等）、存储介质、保存期等。

5.2.5.9.2 测试方法

访谈，检查。

5.2.5.9.3 测试对象

系统管理员，数据库管理员，备份管理文档。

5.2.5.9.4 测评实施

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；对其备份工作是否以文档形式规范了备份方式、频度、介质和保存期等内容；

b） 应检查备份管理文档，查看其是否规定备份方式、频度、介质和保存期等方面内容。

5.2.5.9.5 结果判定

a） 5.2.5.9.4 a）—b）为肯定，则信息系统符合本单元测评项要求。

5.2.5.10 安全事件处置

5.2.5.10.1 测评项

a） 所有用户均有责任报告自己发现的安全弱点和可疑事件，但任何情况下用户均不应尝试验证弱点；

b） 应制定安全事件报告和处置管理制度，规定安全事件的现场处理、事件报告和后期恢复的管理职责。

5.2.5.10.2 测试方法

访谈，检查。

5.2.5.10.3 测试对象

系统运维负责人，安全事件报告和处置管理制度。

5.2.5.10.4 测评实施

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，查看其是否明确与安全事件有关的工作职责，包括报告单位（人）、接报单位（人）和处置单位等职责。

5.2.5.10.5 结果判定

a) 5.2.5.10.4 a）—b）为肯定，则信息系统符合本单元测评项要求。

6 第二级安全控制测评

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 测评项

a) 机房和办公场地应选择在具有防震、防风和防雨等能力的建筑内。

6.1.1.1.2 测评方式

访谈，检查。

6.1.1.1.3 测评对象

物理安全负责人，机房，办公场地，机房场地设计/验收文档。

6.1.1.1.4 测评实施

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；

b) 应检查机房和办公场地的设计/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；

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。

6.1.1.1.5 结果判定

a) 6.1.1.1.4 a）-c）均为肯定，则信息系统符合本单元测评项要求。

6.1.1.2 物理访问控制

6.1.1.2.1 测评项

a) 机房出入口应有专人值守，鉴别进入的人员身份并登记在案；

b) 应批准进入机房的来访人员，限制和监控其活动范围。

6.1.1.2.2 测评方式

访谈，检查。

6.1.1.2.3 测评对象

物理安全负责人，机房值守人员，机房，机房安全管理制度，值守记录，进入机房的登记记录，来访人员进入机房的审批记录。

6.1.1.2.4 测评实施

a) 应访谈物理安全负责人，了解具有哪些控制机房进出的能力；

b) 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，是否对进入机房的人员记录在案；

c） 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；
d） 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专人值守之外的出入口；
e） 应检查机房，是否有进入机房的人员身份鉴别措施，如戴有可见的身份辨识标识；
f） 应检查是否有来访人员进入机房的审批记录。

6.1.1.2.5 结果判定

a） 6.1.1.2.4 a），至少应包括制订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，则该项为肯定；
b） 6.1.1.2.4 c），至少应包括制订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，则该项为肯定；
c） 6.1.1.2.4 a）-f）均为肯定，则信息系统符合本单元测评项要求。

6.1.1.3 防盗窃和防破坏

6.1.1.3.1 测评项

a） 应将主要设备放置在物理受限的范围内；
b） 应对设备或主要部件进行固定，并设置明显的无法除去的标记；
c） 应将通信线缆铺设在隐蔽处，如铺设在地下或管道中等；
d） 应对介质分类标识，存储在介质库或档案室中；
e） 应安装必要的防盗报警设施，以防进入机房的盗窃和破坏行为。

6.1.1.3.2 测评方式

访谈，检查。

6.1.1.3.3 测评对象

物理安全负责人，机房维护人员，资产管理员，机房设施，设备管理制度文档，通信线路布线文档，报警设施的安装测试/验收报告。

6.1.1.3.4 测评实施

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设施进行定期维护检查；
c） 应访谈资产管理员，在介质管理中，是否进行了分类标识，是否存放在介质库或档案室中；
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，是否不易被移动或被搬走，是否设置明显的无法除去的标记；
e） 应检查通信线缆铺设是否在隐蔽处（如铺设在地下或管道中等）；
f） 应检查机房防盗报警设施是否正常运行，并查看运行和报警记录；
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中；
h） 应检查是否有设备管理制度文档，通信线路布线文档，介质管理制度文档，介质清单和使用记录，机房防盗报警设施的安装测试/验收报告。

6.1.1.3.5 结果判定

a） 6.1.1.3.4 a），至少应该包括制订了设备管理制度，主要设备放置位置做到安全可控,设备或主要部件进行了固定和标记，通信线缆铺设在隐蔽处，介质分类标识

并存储在介质库或档案室，机房安装了防止进入盗窃和破坏的防盗报警设施，则该项为肯定；

b） 6.1.1.3.4 a）-h）均为肯定，则信息系统符合本单元测评项要求。

6.1.1.4 防雷击

6.1.1.4.1 测评项

a） 机房建筑应设置避雷装置；

b） 应设置交流电源地线。

6.1.1.4.2 测评方式

访谈，检查。

6.1.1.4.3 测评对象

物理安全负责人，机房维护人员，机房设施（避雷装置，交流电源地线），建筑防雷设计/验收文档。

6.1.1.4.4 测评实施

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；询问机房计算机系统接地（交流工作接地、安全保护接地、防雷接地）是否符合GB50174－93《电子计算机机房设计规范》的要求；

c） 应检查机房是否有建筑防雷设计/验收文档，查看是否有地线连接要求的描述。

6.1.1.4.5 结果判定

a） 6.1.1.4.4 a），至少还应包括符合GB 50057－1994《建筑物防雷设计规范》（GB157《建筑防雷设计规范》）中的计算机机房防雷要求，如果在雷电频繁区域，是否装设浪涌电压吸收装置等，则该项为肯定；

b） 6.1.1.4.4 b），要求地线的引线应和大楼的钢筋网及各种金属管道绝缘，交流工作接地的接地电阻不应大于4Ω，安全保护地的接地电阻不应大于4Ω；防雷保护地（处在有防雷设施的建筑群中可不设此地）的接地电阻不应大于10Ω的要求，则该项为肯定；

c） 6.1.1.4.4 a）-c）均为肯定，则信息系统符合本单元测评项要求。

6.1.1.5 防火

6.1.1.5.1 测评项

a） 应设置灭火设备和火灾自动报警系统，并保持灭火设备和火灾自动报警系统的良好状态。

6.1.1.5.2 测评方式

访谈，检查。

6.1.1.5.3 测评对象

物理安全负责人，机房值守人员，机房设施，机房安全管理制度，机房防火设计/验收文档，火灾自动报警系统设计/验收文档。

6.1.1.5.4 测评实施

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，是否制订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火灾自动报警系统；

c） 应检查机房是否设置了灭火设备，摆放位置是否合理，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；

d） 应检查是否有有关机房消防的管理制度文档，机房防火设计/验收文档，火灾自动报警系统的设计/验收文档。

6.1.1.5.5 结果判定

a） 6.1.1.5.4 a）-d）均为肯定，则信息系统符合本单元测评项要求。

6.1.1.6 防水和防潮

6.1.1.6.1 测评项

a） 水管安装，不得穿过屋顶和活动地板下；

b） 应对穿过墙壁和楼板的水管增加必要的保护措施，如设置套管；

c） 应采取措施防止雨水通过屋顶和墙壁渗透；

d） 应采取措施防止室内水蒸气结露和地下积水的转移与渗透。

6.1.1.6.2 测评方式

访谈，检查。

6.1.1.6.3 测评对象

物理安全负责人，机房维护人员，机房设施（上下水装置，除湿装置），建筑防水和防潮设计/验收文档。

6.1.1.6.4 测评实施

a） 应访谈物理安全负责人，询问机房建设是否有防水防潮措施；如果机房内有上下水管安装，是否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，是否经常检查是否有漏水情况；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） 应检查机房是否有建筑防水和防潮设计/验收文档，是否能够满足机房防水和防潮的需求；

d） 如果有管道穿过主机房墙壁和楼板处，应检查是否置套管，管道与套管之间是否采取可靠的密封措施；

e） 应检查机房是否不存在屋顶和墙壁等出现过漏水、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、渗透和返潮现是否能够及时修复解决；

f） 如果在湿度较高地区或季节，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。

6.1.1.6.5 结果判定

a） 如果6.1.1.6.4 d）、f）中“如果”条件不成立，则该项为不适用；

b） 6.1.1.6.4 a）-f）均为肯定，则信息系统符合本单元测评项要求。

6.1.1.7 防静电

6.1.1.7.1 测评项

a) 应采用必要的接地等防静电措施。

6.1.1.7.2 测评方式

访谈，检查。

6.1.1.7.3 测评对象

物理安全负责人，机房维护人员，机房设施，防静电设计/验收文档。

6.1.1.7.4 测评实施

a) 应访谈物理安全负责人，询问机房是否采用必要的接地防静电措施，是否有控制机房湿度的措施；

b) 应访谈机房维护人员，询问是否经常检查机房湿度，并控制在GB2887中的规定的范围内；询问机房是否存在静电问题或因静电引起的故障事件；

c) 应检查机房是否有防静电设计/验收文档；

d) 应检查机房是否有安全接地，查看机房的相对湿度是否符合GB2887中的规定，查看机房是否明显存在静电现象。

6.1.1.7.5 结果判定

a) 6.1.1.7.4 a）-d）均为肯定，则信息系统符合本单元测评项要求。

6.1.1.8 温湿度控制

6.1.1.8.1 测评项

a) 应设置温、湿度自动调节设施，使机房温、湿度的变化在设备运行所允许的范围之内。

6.1.1.8.2 测评方式

访谈，检查。

6.1.1.8.3 测评对象

物理安全负责人，机房维护人员，机房设施，温湿度控制设计/验收文档，温湿度记录、运行记录和维护记录。

6.1.1.8.4 测评实施

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；

b) 应访谈机房维护人员，询问是否定期检查和维护机房的温湿度自动调节设施，询问是否出现过温湿度影响系统运行的事件；

c) 应检查机房是否有温湿度控制设计/验收文档；

d) 应检查温湿度自动调节设施是否能够正常运行，查看温湿度记录、运行记录和维护记录；查看机房温湿度是否满足GB 2887-89《计算站场地技术条件》的要求。

6.1.1.8.5 结果判定

a) 6.1.1.8.4 a）-d）均为肯定，则信息系统符合本单元测评项要求。

6.1.1.9 电力供应

6.1.1.9.1 测评项

a) 计算机系统供电应与其他供电分开；

b) 应设置稳压器和过电压防护设备；

c) 应提供短期的备用电力供应（如UPS设备）。

6.1.1.9.2 测评方式

访谈，检查。

6.1.1.9.3 测评对象

物理安全负责人，机房维护人员，机房设施（*供电线路，稳压器，过电压防护设备，短期备用电源设备*），电力供应安全设计/验收文档，检查和维护记录。

6.1.1.9.4 测评实施

a） 应访谈物理安全负责人，询问计算机系统供电线路是否与其他供电分开；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（如UPS），供电时间是否满足系统最低电力供应需求；

b） 应访谈机房维护人员，询问是对在计算机系统供电线路上的稳压器、过电压防护设备、短期备用电源设备等进行定期检查和维护；是否能够控制电源稳压范围满足计算机系统运行正常；

c） 应检查机房是否有电力供应安全设计/验收文档，查看文档中是否标明单独为计算机系统供电，配备稳压器、过电压防护设备以及短期备用电源设备等要求；

d） 应检查计算机供电线路，查看计算机系统供电是否与其他供电分开；

e） 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；

f） 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电源设备的检查和维护记录。

6.1.1.9.5 结果判定

a） 6.1.1.9.4 a）-g）均为肯定，则信息系统符合本单元测评项要求。

6.1.1.10 电磁防护

6.1.1.10.1 测评项

a） 应采用接地方式防止外界电磁干扰和设备寄生耦合干扰；

b） 电源线和通信线缆应隔离，避免互相干扰。

6.1.1.10.2 测评方式

访谈，检查。

6.1.1.10.3 测评对象

物理安全负责人，机房维护人员，机房设施，电磁防护设计/验收文档。

6.1.1.10.4 测评实施

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）；

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；是否出现过因外界电磁干扰等问题引发的故障；

c） 应检查机房是否有电磁防护设计/验收文档；

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。

6.1.1.10.5 结果判定

a） 6.1.1.10.4 a）-e）均为肯定，则信息系统符合本单元测评项要求。

6.1.2 网络安全

6.1.2.1 结构安全与网段划分

6.1.2.1.1 测评项

a） 网络设备的业务处理能力应具备冗余空间，要求满足业务高峰期需要；

b） 应设计和绘制与当前运行情况相符的网络拓扑结构图；

c） 应根据机构业务的特点，在满足业务高峰期需要的基础上，合理设计网络带宽；

d） 应在业务终端与业务服务器之间进行路由控制建立安全的访问路径；

e） 应根据各部门的工作职能、重要性、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、网段分配地址段；

f） 重要网段应采取网络层地址与数据链路层地址绑定措施，防止地址欺骗。

6.1.2.1.2 测评方式

访谈，检查，测试。

6.1.2.1.3 测评对象

网络管理员，边界和重要网络设备，网络拓扑图，网络设计/验收文档。

6.1.2.1.4 测评实施

a) 可访谈网络管理员，询问信息系统中的边界和关键网络设备的性能以及目前业务高峰流量情况；

b) 可访谈网络管理员，询问网段划分情况以及划分的原则；询问重要的网段有哪些，对重要网段的保护措施有哪些；

c) 可访谈网络管理员，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) 可访谈网络管理员，询问网络设备上的路由控制策略措施有哪些，这些策略设计的目的是什么；

e) 应检查网络拓扑图，查看与当前运行情况是否一致；

f） 应检查网络设计/验收文档，查看是否有边界和重要网络设备能满足基本业务需求，网络接入及核心网络的带宽能否满足业务高峰期的需要等方面的设计或说明；

g) 应检查网络设计/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） 应检查边界和重要网络设备，查看是否配置路由控制策略（如使用静态路由等）建立安全的访问路径；

i） 应检查边界和重要网络设备，查看对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（如对重要服务器采用 IP 地址和 MAC 地址绑定措施）；

j） 应测试网络拓扑结构，可通过网络拓扑结构自动发现、绘制工具，验证实际的网络拓扑结构和网络拓扑结构图是否一致；

k） 应测试业务终端与业务服务器之间的访问路径，可通过使用路由跟踪工具（如 tracert 等工具），验证业务终端与业务服务器之间的访问路径的是否安全（如访问路径是否固定等）；

l) 应测试重要网段，验证其采取的网络地址与数据链路地址绑定措施是否有效（如试图使用非绑定地址，查看是否能正常访问等）。

6.1.2.1.5 结果判定

a) 如果 6. 1. 2. 1. 4 f）-g）中缺少相应的文档，则该项为否定；

b) 6. 1. 2. 1. 4 e）-l）均为肯定，则信息系统符合本单元测评项要求。

6.1.2.2 网络访问控制

6.1.2.2.1 测评项

a） 应能根据会话状态信息（包括数据包的源地址、目的地址、源端口号、目的端口号、协议、出入的接口、会话序列号、发出信息的主机名等信息，并应支持地址通配符的使用），为数据流提供明确的允许/拒绝访问的能力。

6.1.2.2.2 测评方式

访谈，检查，测试。

6.1.2.2.3 测评对象

安全员，边界网络设备（包括网络安全设备）。

6.1.2.2.4 测评实施

a) 可访谈安全员，询问采取的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的访问控制功能（如是基于状态的，还是基于包过滤等）；

b) 应检查边界网络设备，查看其是否根据会话状态信息（如包括数据包的源地址、目的地址、源端口号、目的端口号、协议、出入的接口、会话序列号、发出信息的主机名等信息，并应支持地址通配符的使用）对数据流进行控制；

c) 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的控制（如可以使用扫描工具探测等）。

6.1.2.2.5 结果判定

a) 6. 1. 2. 2. 4 b）-c）均为肯定，则信息系统符合本单元测评项要求。

6.1.2.3 拨号访问控制

6.1.2.3.1 测评项

a) 应在基于安全属性的允许远程用户对系统访问的规则的基础上，对系统所有资源允许或拒绝用户进行访问，控制粒度为单个用户；

b) 应限制具有拨号访问权限的用户数量。

6.1.2.3.2 测评方式

访谈，检查，测试。

6.1.2.3.3 测评对象

安全员，边界网络设备。

6.1.2.3.4 测评实施

a) 可访谈安全员，询问网络是否允许拨号访问网络；询问对拨号访问控制的策略是什么，采取何种技术手段实现（如使用防火墙还是路由器实现），采取的拨号访问用户的权限分配原则是什么；

b) 应检查边界网络设备（如路由器，防火墙，认证网关），查看是否配置了正确的拨号访问控制列表（对系统资源实现允许或拒绝用户访问），控制粒度是否为单个用户；查看其能否限制拨号访问权限的用户数量；

c) 应测试边界网络设备，可通过试图非授权的访问，验证拨号访问措施能否有效对系统资源实现允许或拒绝用户访问的控制；

d) 应测试边界网络设备，可使用测试网络连接数工具，验证其限制具有拨号访问权限的用户数量的功能是否有效。

6.1.2.3.5 结果判定

a) 6. 1. 2. 3. 4 b）-d）均为肯定，则信息系统符合本单元测评项要求。

6.1.2.4 网络安全审计

6.1.2.4.1 测评项

a) 应对网络系统中的网络设备运行状况、网络流量、用户行为等事件进行日志记录；

b) 对于每一个事件，其审计记录应包括：事件的日期和时间、用户、事件类型、事件是否成功，及其他与审计相关的信息。

6.1.2.4.2 测评方式

访谈，检查，测试。

6.1.2.4.3 测评对象

审计员，边界和重要网络设备（包括安全设备）审计记录，审计策略。

6.1.2.4.4 测评实施

a) 可访谈审计员，询问是否对网络系统中的边界和重要网络设备进行审计，审计包括哪些项；询问审计记录的主要内容有哪些；询问对审计记录的处理方式；

b) 应检查边界和重要网络设备的审计记录，查看是否有网络系统中的网络设备运行状况、网络流量、用户行为等事件的记录；

c) 应检查边界和重要网络设备的事件审计策略，查看是否包括：事件的日期和时间、用户、事件类型、事件成功情况，及其他与审计相关的信息。

d) 应测试边界和重要网络设备的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（如产生相应的事件，观察审计的记录看是否对这些事件的准确记录）。

6.1.2.4.5 结果判定

a) 6.1.2.4.4 b）-d）均为肯定，则信息系统符合本单元测评项要求。

6.1.2.5 边界完整性检查

6.1.2.5.1 测评项

a) 应能够检测内部网络中出现的内部用户未通过准许私自联到外部网络的行为（即“非法外联”行为）。

6.1.2.5.2 测评方式

访谈，检查，测试。

6.1.2.5.3 测评对象

安全员，边界完整性检查设备/工具，边界完整性检查工具运行日志。

6.1.2.5.4 测评实施

a) 可访谈安全员，询问是否有对内部用户未通过准许私自联到外部网络的行为进行监控的措施，具体是什么措施；询问网络内是否使用边界完整性检查设备/工具对网络进行监控；询问网络内“非法外联”的情况；

b) 应检查边界完整性检查工具运行日志，查看运行是否正常（查看是否持续对网络进行监控）；

c) 应检查边界完整性检查设备/工具的配置，查看是否正确配置对网络的内部用户未通过准许私自联到外部网络的行为进行有效监控；

d) 应测试边界完整性检查工具，是否能有效的发现“非法外联”的行为（如产生非法外联的动作，查看边界完整性检查工具是否能够及时发现该行为）。

6.1.2.5.5 结果判定

a) 6.1.2.5.4 b）-d）均为肯定，则信息系统符合本单元测评项要求。

6.1.2.6 网络入侵防范

6.1.2.6.1 测评项

a) 应在网络边界处监视以下攻击行为：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、网络蠕虫攻击等入侵事件的发生。

6.1.2.6.2 测评方式

访谈，检查，测试。

6.1.2.6.3 测评对象

安全员，网络入侵防范设备。

6.1.2.6.4 测评实施

a) 可访谈安全员，询问网络入侵防范措施有哪些；询问是否有专门的设备对网络入侵进行防范；询问采取什么方式进行网络入侵防范规则库升级；

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，查看其生产厂商是否为正规厂商，规则库是否为最新；
d） 应测试网络入侵防范设备，验证其监控策略是否有效（如模拟产生攻击动作，查看网络入侵防范设备的反应）。

6.1.2.6.5 结果判定

a） 6.1.2.6.4 b）-d）均为肯定，则信息系统符合本单元测评项要求。

6.1.2.7 恶意代码防范

6.1.2.7.1 测评项

a） 应在网络边界及核心业务网段处对恶意代码进行检测和清除；
b） 应维护恶意代码库的升级和检测系统的更新；
c） 应支持恶意代码防范的统一管理。

6.1.2.7.2 测评方式

访谈，检查。

6.1.2.7.3 测评对象

安全员，防恶意代码产品，网络设计/验收文档，恶意代码产品运行日志。

6.1.2.7.4 测评实施

a） 可访谈安全员，询问系统中的网络防恶意代码防范措施是什么；询问恶意代码库的更新策略，询问防恶意代码产品的有哪些主要功能；询问系统是否发生过恶意代码入侵的安全事件；
b） 应检查网络设计/验收文档，查看其是否有在网络边界及核心业务网段处是否有对恶意代码采取相关措施（如是否有防病毒网关）；检查防恶意代码产品是否有实时更新的功能的描述；
c） 应检查恶意代码产品运行日志，查看是否持续运行；
d） 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的措施；
e） 应检查防恶意代码产品，查看是否为正规厂商生产，运行是否正常，恶意代码库是否为最新版本；
f） 应检查防恶意代码产品的配置策略，查看是否支持恶意代码防范的统一管理（如查看是否为分布式部署，集中管理等）。

6.1.2.7.5 结果判定

a） 如果6.1.2.7.4 b）中缺少相应的文档，则该项为否定；
b） 6.1.2.7.4 b）-f）均为肯定，则信息系统符合本单元测评项要求。

6.1.2.8 网络设备防护

6.1.2.8.1 测评项

a） 应对登录网络设备的用户进行身份鉴别；
b） 应对网络设备的管理员登录地址进行限制；
c） 网络设备用户的标识应唯一；
d） 身份鉴别信息应具有不易被冒用的特点，例如口令长度、复杂性和定期的更新等；
e） 应具有登录失败处理功能，如结束会话、限制非法登录次数，当网络登录连接超时，自动退出。

6.1.2.8.2 测评方式

访谈，检查，测试。

6.1.2.8.3 测评对象

网络管理员，边界和重要网络设备（包括安全设备）。

6.1.2.8.4 测评实施

a) 可访谈网络管理员，询问对关键网络设备的防护措施有哪些；询问对关键网络设备的登录和验证方式做过何种特定配置；

b) 应访谈网络管理员，询问网络设备的口令策略是什么；

c) 应检查边界和重要网络设备上的安全设置，查看其是否有对鉴别失败采取相应的措施的设置；查看其是否有限制非法登录次数的功能；

d) 应检查边界和重要网络设备上的安全设置，查看是否对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；查看是否对网络上的对等实体进行身份鉴别；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) 应测试边界和重要网络设备的安全设置，验证鉴别失败处理措施（如模拟失败登录，观察网络设备的动作等），限制非法登录次数（如模拟非法登录，观察网络设备的动作等），对网络设备的管理员登录地址进行限制（如使用任意地址登录，观察网络设备的动作等）等功能是否有效；

f) 应测试边界和重要网络设备的安全设置，验证其网络登录连接超自动退出的设置是否有效（如长时间连接无任何操作，观察观察网络设备的动作等）；

g) 应对边界和重要网络设备进行渗透测试，通过使用各种渗透测试技术（如口令猜解等）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。

6.1.2.8.5 结果判定

a) 如网络设备的口令策略为口令长度6位以上，口令复杂（如规定字符应混有大、小写字母、数字和特殊字符），口令生命周期，新旧口令的替换要求（规定替换的字符数量）或为了便于记忆使用了令牌；则6.1.2.8.4 b）满足测评要求；

b) 6.1.2.8.4 b）-f）均为肯定，则信息系统符合本单元测评项要求。

6.1.3 主机系统安全

6.1.3.1 身份鉴别

6.1.3.1.1 测评项

a) 操作系统和数据库系统用户的身份标识应具有唯一性；

b) 应对登录操作系统和数据库系统的用户进行身份标识和鉴别；

c) 操作系统和数据库系统身份鉴别信息应具有不易被冒用的特点，例如口令长度、复杂性和定期更新等；

d) 应具有登录失败处理功能，如结束会话、限制非法登录次数，当登录连接超时，自动退出。

6.1.3.1.2 测评方式

访谈，检查，测试。

6.1.3.1.3 测评对象

系统管理员，数据库管理员，重要服务器操作系统，重要数据库系统，服务器操作系统文档，数据库系统文档。

6.1.3.1.4 测评实施

a) 应检查服务器操作系统和数据库系统身份鉴别功能是否具有《信息安全等级保护操作系统安全技术要求》和《信息安全等级保护数据库管理系统安全技术要求》第二级以上或TCSEC C2级以上的测试报告；

b) 可访谈系统管理员，询问操作系统的身份标识与鉴别机制采取何种措施实现；

c) 可访谈数据库管理员，询问数据库的身份标识与鉴别机制采取何种措施实现；

d) 应检查服务器操作系统文档和数据库系统文档，查看用户身份标识的唯一性是由什

么属性来保证的（如用户名或者 UID 等）；

e) 应检查重要服务器操作系统和重要数据库系统，查看是否提供了身份鉴别措施（如用户名和口令等），其身份鉴别信息是否具有不易被冒用的特点，例如，口令足够长，口令复杂（如规定字符应混有大、小写字母、数字和特殊字符），更新周期短，或为了便于记忆使用了令牌；

f) 应检查重要服务器操作系统和重要数据库系统，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；

g) 应测试重要服务器操作系统和重要数据库系统，可通过错误的用户名和口令试图登录系统，验证鉴别失败处理功能是否有效；

h) 应测试重要服务器操作系统和重要数据库系统，当进入系统时，是否先需要进行标识（如建立账号），而没有进行标识的用户不能进入系统；

i) 应测试重要服务器操作系统和重要数据库系统，添加一个新用户，其用户标识为系统原用户的标识（如用户名或 UID），查看是否不会成功。

6.1.3.1.5 结果判定

a) 如果6.1.3.1.4 a）为肯定，则测评实施h）和i）为肯定；

b) 6.1.3.1.4 e）-i）均为肯定，则信息系统符合本单元测评项要求。

6.1.3.2 自主访问控制

6.1.3.2.1 测评项

a) 应依据安全策略控制主体对客体的访问；

b) 自主访问控制的覆盖范围应包括与信息安全直接相关的主体、客体及它们之间的操作；

c) 自主访问控制的粒度应达到主体为用户级，客体为文件、数据库表级；

d) 应由授权主体设置对客体访问和操作的权限；

e) 应严格限制默认用户的访问权限。

6.1.3.2.2 测评方式

检查，测试。

6.1.3.2.3 测评对象

重要服务器操作系统，重要数据库系统，安全策略。

6.1.3.2.4 测评实施

a) 应检查服务器操作系统和数据库系统的自主访问控制功能是否具有《信息安全等级保护 操作系统安全技术要求》和《信息安全等级保护 数据库管理系统安全技术要求》第二级以上或TCSEC C2级以上的测试报告；

b) 应检查服务器操作系统和数据库系统的安全策略，查看是否明确主体（如用户）以用户和/或用户组的身份规定对客体(如文件或系统设备,目录表和存取控制表访问控制等）的访问控制，覆盖范围是否包括与信息安全直接相关的主体（如用户）和客体（如文件，数据库表等）及它们之间的操作（如读、写或执行）；

c) 应检查服务器操作系统和数据库系统的安全策略，查看是否明确主体（如用户）具有非敏感标记（如角色），并能依据非敏感标记规定对客体的访问；

d) 应检查重要服务器操作系统和重要数据库系统的访问控制列表，查看授权用户中是否不存在过期的帐号和无用的帐号等；访问控制列表中的用户和权限，是否与安全策略相一致；

e） 应检查重要服务器操作系统和重要数据库系统，查看客体（如文件,数据库表、视图、存储过程和触发器等）的所有者是否可以改变其相应访问控制列表的属性，得到授权的用户是否可以改变相应客体访问控制列表的属性；

f） 应查看重要服务器操作系统和重要数据库系统，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（如限定在有限的范围内）；

g） 应测试重要服务器操作系统和重要数据库系统，依据系统访问控制的安全策略，试图以未授权用户身份/角色访问客体，验证是否不能进行访问。

6.1.3.2.5 结果判定

a） 如果6.1.3.2.4 a）为肯定，则测评实施e）和g）为肯定；

b） 6.1.3.2.4 b）-g）均为肯定，则信息系统符合本单元测评项要求。

6.1.3.3 安全审计

6.1.3.3.1 测评项

a） 安全审计应覆盖到服务器上的每个操作系统用户和数据库用户；

b） 安全审计应记录系统内重要的安全相关事件，包括重要用户行为、系统资源的异常使用和重要系统命令的使用等；

c） 安全相关事件的记录应包括日期和时间、类型、主体标识、客体标识、事件的结果等；

d） 审计记录应受到保护避免受到未预期的删除、修改或覆盖等。

6.1.3.3.2 测评方式

访谈，检查，测试。

6.1.3.3.3 测评对象

安全审计员，重要服务器操作系统，重要数据库系统。

6.1.3.3.4 测评实施

a） 可访谈安全审计员，询问主机系统是否设置安全审计；询问主机系统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） 应检查重要服务器操作系统和重要数据库系统，查看当前审计范围是否覆盖到每个用户；

c） 应检查重要服务器操作系统和重要数据库系统，查看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、自主访问控制的所有操作记录、重要用户行为（如用超级用户命令改变用户身份，删除系统表）、系统资源的异常使用、重要系统命令的使用（如删除客体）等；

d） 应检查重要服务器操作系统和重要数据库系统，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、身份鉴别事件中请求的来源（如末端标识符）、事件的结果等内容；

e) 应检查重要服务器操作系统和重要数据库系统，查看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，能否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) 应测试主要服务器操作系统和主要数据库系统，在系统上以某个用户试图产生一些重要的安全相关事件（如鉴别失败等），测试安全审计的覆盖情况和记录情况与要求是否一致；

g) 应测试主要服务器操作系统和主要数据库系统，在系统上以某个系统用户试图删除、修改或覆盖审计记录，测试安全审计的保护情况与要求是否一致。

6.1.3.3.5 结果判定

a） 6.1.3.3.4 b）-g）均为肯定，则信息系统符合本单元测评项要求。

6.1.3.4 系统保护

6.1.3.4.1 测评项

a) 系统应提供在管理维护状态中运行的能力，管理维护状态只能被系统管理员使用。

6.1.3.4.2 测评方式

访谈，检查，测试。

6.1.3.4.3 测评对象

系统管理员，重要服务器操作系统。

6.1.3.4.4 测评实施

a) 应检查服务器操作系统的系统保护（资源利用）功能是否具有《信息安全等级保护操作系统安全技术要求》和《信息安全等级保护 数据库管理系统安全技术要求》第二级以上或 TCSEC C2 级以上的测试报告；

b) 应访谈系统管理员，询问重要服务器的维护工作是在什么样的状态进行的，进入该维护状态是否只有系统管理员才能登录使用；

c) 应检查重要服务器操作系统是否提供不同于正常运行状态的管理维护状态（如 WINDOWS 2000 提供安全模式，Linux 提供安全启动模式和单用户运行模式等）；

d) 应检查重要服务器操作系统进行管理维护状态时，是否只有系统管理员才能登录使用，使用其他用户（如审计员）用户不能登录；

e) 应测试重要服务器操作系统，通过其他非系统管理员试图登录其管理维护状态，验证是否只有系统管理员才能登录使用，而其他用户不能使用。

6.1.3.4.5 结果判定

a) 如果6.1.3.4.4 a）为肯定，则测评实施b）-e）为肯定；

b) 如果6.1.3.4.4 b）中的重要服务器的维护工作只能在系统管理员登录使用的管理维护状态进行，则该项为肯定；

c) 6.1.3.4.4 b）-e）均为肯定，则信息系统符合本单元测评项要求。

6.1.3.5 剩余信息保护

6.1.3.5.1 测评项

a) 应保证操作系统和数据库管理系统用户的鉴别信息所在的存储空间，被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中；

b) 应确保系统内的文件、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。

6.1.3.5.2 测评方式

访谈，检查。

6.1.3.5.3 测评对象

系统管理员，数据库管理员，重要服务器操作系统维护/操作手册，重要数据库系统维护/操作手册。

6.1.3.5.4 测评实施

a) 应检查服务器操作系统和数据库系统的剩余信息保护（用户数据保密性保护/客体重用）功能是否具有《信息安全等级保护 操作系统安全技术要求》和《信息安全等级保护 数据库管理系统安全技术要求》第二级以上的测试报告；

b) 应与系统管理员访谈，询问操作系统用户的鉴别信息存储空间，被释放或再分配给其他用户前是否得到完全清除；系统内的文件、目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是否得到完全清除；

c) 应与数据库管理员访谈，询问数据库管理员用户的鉴别信息存储空间，被释放或再分配给其他用户前是否得到完全清除；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是否得到完全清除；

d) 应检查重要操作系统和重要数据库系统维护操作手册，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；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。

6.1.3.5.5 结果判定

a) 如果 6.1.3.5.4 a）为肯定，则测评实施 b）-d）为肯定；

a) 6.1.3.5.4 b）-d）均为肯定，则信息系统符合本单元测评项要求。

6.1.3.6 恶意代码防范

6.1.3.6.1 测评项

a) 服务器和重要终端设备（包括移动设备）应安装实时检测和查杀恶意代码的软件产品；

b) 主机系统防恶意代码产品应具有与网络防恶意代码产品不同的恶意代码库。

6.1.3.6.2 测评方式

访谈，检查。

6.1.3.6.3 测评对象

系统安全员，重要服务器系统，重要终端系统，网络防恶意代码产品，主机安全设计/验收文档。

6.1.3.6.4 测评实施

a) 应访谈系统安全员，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情况如何；

b) 应检查主机恶意代码防范方面的设计/验收文档，查看描述的安装范围是否包括服务器和终端设备（包括移动设备）；

c) 应检查重要服务器系统和重要终端系统，查看是否安装实时检测与查杀恶意代码的软件产品；查看检测与查杀恶意代码软件产品的厂家、版本号和恶意代码库名称；

d) 应检查网络防恶意代码产品，查看厂家、版本号和恶意代码库名称。

6.1.3.6.5 结果判定

a) 如果6.1.3.6.4 a）中恶意代码实时检测与查杀措施的部署到服务器和重要终端，则该项为肯定；

b) 6.1.3.6.4 a）-c）均为肯定，检查发现主机系统防恶意代码产品与网络防恶意代码产品使用不同的恶意代码库（如厂家、版本号和恶意代码库名称不相同等），则信息系统符合本单元测评项要求。

6.1.3.7 资源控制

6.1.3.7.1 测评项

a) 应限制单个用户的会话数量；

b) 应通过设定终端接入方式、网络地址范围等条件限制终端登录。

6.1.3.7.2 测评方式

检查，测试。

6.1.3.7.3 测评对象

重要服务器操作系统。

6.1.3.7.4 测评实施

a) 应检查重要服务器操作系统，查看是否限制单个用户的多重并发会话数量；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) 应测试重要服务器操作系统，任选一个用户，登录服务器，试图发出多重并发会话，

验证系统是否限制单个用户的会话数量；

c） 应测试重要服务器操作系统，任选一个用户帐户，登录服务器，用不同的终端接入方式、网络地址试图登录服务器，验证重要服务器操作系统是否通过终端接入方式、网络地址范围等条件限制终端登录。

6.1.3.7.5 结果判定

a） 6.1.3.7.4 a）-c）均为肯定，则信息系统符合本单元测评项要求。

6.1.4 应用安全

6.1.4.1 身份鉴别

6.1.4.1.1 测评项

a） 应用系统用户的身份标识应具有唯一性；

b） 应对登录的用户进行身份标识和鉴别；

c） 系统用户的身份鉴别信息应具有不易被冒用的特点，例如口令长度、复杂性和定期的更新等；

d） 应具有登录失败处理功能，如结束会话、限制非法登录次数，当登录连接超时，自动退出。

6.1.4.1.2 测评方式

访谈，检查，测试。

6.1.4.1.3 测评对象

系统管理员，重要应用系统，总体规划/设计文档。

6.1.4.1.4 测评实施

a) 可访谈系统管理员，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（如复杂性混有大、小写字母、数字和特殊字符，设定口令周期等）；

b) 可访谈系统管理员，询问应用系统是否具有登录失败处理的功能，是如何进行处理的；

c) 可访谈系统管理员，询问应用系统对用户标识是否具有唯一性（如UID、用户名或其他信息在系统中是唯一的，用该标识能唯一识别该用户）；

d） 应检查总体规划/设计文档，查看其是否有系统采取了唯一标识（如用户名、UID或其他属性）的说明；

e） 应检查重要应用系统，查看其是否配备身份标识（如建立账号）和鉴别（如口令等）功能；查看其身份鉴别信息是否具有不易被冒用的特点，例如复杂性（如规定字符应混有大、小写字母、数字和特殊字符）或为了便于记忆使用了令牌；

f） 应检查重要应用系统，查看其是否配备并使用登录失败处理功能（如登录失败次数超过设定值，系统自动退出等）；

g） 应测试重要应用系统，可通过注册用户，并登录系统，查看登录是否成功，验证其身份标识和鉴别功能是否有效；

h） 应测试重要应用系统，验证其登录失败处理，非法登录次数限制，登录连接超时自动退出等功能是否有效。

6.1.4.1.5 结果判定

a） 如果6.1.4.1.4 c）中相关文档中对用户进行唯一性标识的描述，则该项为肯定；

b） 6.1.4.1.4 d）-h）均为肯定，则信息系统符合本单元测评项要求。

6.1.4.2 访问控制

6.1.4.2.1 测评项

a） 应依据安全策略控制用户对客体的访问；

b） 自主访问控制的覆盖范围应包括与信息安全直接相关的主体、客体及它们之间的操作；

c） 自主访问控制的粒度应达到主体为用户级，客体为文件、数据库表级；

d） 应由授权主体设置用户对系统功能和用户数据访问和操作的权限；

e） 应实现应用系统特权用户的权限分离，例如将管理与审计的权限分配给不同的应用系统用户；

f） 权限分离应采用最小授权原则，分别授予不同用户各自为完成自己承担任务所需的最小权限，并在它们之间形成相互制约的关系；

g） 应用系统的设计应采用二层以上结构，将提供数据显示功能与数据处理功能在物理或者逻辑上分离；

h） 应严格限制默认用户的访问权限。

6.1.4.2.2 测评方式

访谈，检查，测试。

6.1.4.2.3 测评对象

系统管理员，重要应用系统。

6.1.4.2.4 测评实施

a） 应访谈系统管理员，询问业务系统是否提供访问控制措施，具体措施有哪些，自主访问控制的粒度如何；

b） 应检查重要应用系统，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（如文件和数据库中的数据）的访问；

c） 应检查重要应用系统，查看其自主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；自主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（如数据库表、视图、存储过程等）；

d） 应检查重要应用系统，查看应用系统是否有对授权主体进行系统功能操作和对数据访问权限进行设置的功能；

e） 应检查重要应用系统，查看其特权用户的权限是否分离（如将系统管理员、安全员和审计员的权限分离），权限之间是否相互制约；

f） 应检查重要应用系统，查看其是否有限制默认用户访问权限的功能，并已配置使用；

g） 应测试重要应用系统，可通过用不同权限的用户登录，查看其权限是否受到应用系统的限制，验证系统权限分离功能是否有效；

h） 应测试重要应用系统，可通过授权主体设置特定用户对系统功能进行操作和对数据进行访问的权限，然后以该用户登录，验证用户权限管理功能是否有效；

i） 应测试重要应用系统，可通过用默认用户（默认密码）登录，并用该用户进行操作（包括合法、非法操作），验证系统对默认用户访问权限的限制是否有效。

6.1.4.2.5 结果判定

a） 6.1.4.2.4 b）-i）均为肯定，则信息系统符合本单元测评项要求。

6.1.4.3 安全审计

6.1.4.3.1 测评项

a） 安全审计应覆盖到应用系统的每个用户；

b） 安全审计应记录应用系统重要的安全相关事件，包括重要用户行为和重要系统功能的执行等；

c） 安全相关事件的记录应包括日期和时间、类型、主体标识、客体标识、事件的结果等；

d） 审计记录应受到保护避免受到未预期的删除、修改或覆盖等。

6.1.4.3.2 测评方式

访谈，检查，测试。

6.1.4.3.3 测评对象

审计员，重要应用系统。

6.1.4.3.4 测评实施

a) 可访谈安全审计员，询问应用系统是否设置安全审计；询问应用系统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) 应检查重要应用系统，查看其当前审计范围是否覆盖到每个用户；

c) 应检查重要应用系统，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、自主访问控制的所有操作记录、重要用户行为（如用超级用户命令改变用户身份，删除系统表）、重要系统命令的使用（如删除客体）等；

d) 应检查重要应用系统，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（如末端标识符）、事件的结果等内容；

e) 应检查重要应用系统，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，能否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) 应测试重要应用系统，可通过非法终止审计功能或修改其配置，验证审计功能是否受到保护；

g) 应测试重要应用系统，在系统上以某个用户试图产生一些重要的安全相关事件（如鉴别失败等），测试安全审计的覆盖情况和记录情况与要求是否一致；

h) 应测试重要应用系统，在系统上以某个系统用户试图删除、修改或覆盖审计记录，测试安全审计的保护情况与要求是否一致。

6.1.4.3.5 结果判定

a) 6.1.4.3.4 b）-h）均为肯定，则信息系统符合本单元测评项要求。

6.1.4.4 剩余信息保护

6.1.4.4.1 测评项

a) 应保证用户的鉴别信息所在的存储空间，被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中；

b) 应确保系统内的文件、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。

6.1.4.4.2 测评方式

访谈，检查。

6.1.4.4.3 测评对象

系统管理员，总体规划/设计文档。

6.1.4.4.4 测评实施

a) 可访谈系统管理员，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) 应检查总体规划/设计文档，查看其是否有关于系统是否有将鉴别信息所在的存储空间，被释放或再分配给其他用户前完全清除（无论这些信息是存放在硬盘上还是在内存中）的描述；

c) 应检查总体规划/设计文档，查看其是否有系统内的文件、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是否完全清除的描述。

6.1.4.4.5 结果判定

a) 如果6.1.4.4.4 b）-c）缺少相关材料，则该项为否定；

b) 6.1.4.4.4 b）-c）均为肯定，则信息系统符合本单元测评项要求。

6.1.4.5 通信完整性

6.1.4.5.1 测评项

a) 通信双方应约定单向的校验码算法，计算通信数据报文的校验码，在进行通信时，双方根据校验码判断对方报文的有效性。

6.1.4.5.2 测评方式

访谈，检查，测试。

6.1.4.5.3 测评对象

安全员，设计/验收文档，重要应用系统。

6.1.4.5.4 测评实施

a) 可访谈安全员，询问业务系统是否有数据在传输过程中进行完整性保证的操作，具体措施是什么；

b) 应检查设计/验收文档，查看其是否有通信完整性的说明，如果有则查看其是否有系统是根据校验码判断对方数据包的有效性的描述；

c) 应测试重要应用系统，可通过获取通信双方的数据包，查看其是否有验证码。

6.1.4.5.5 结果判定

a) 6.1.4.5.4 b）-c）均为肯定，则信息系统符合本单元测评项要求。

6.1.4.6 通信保密性

6.1.4.6.1 测评项

a) 当通信双方中的一方在一段时间内未作任何响应，另一方应能够自动结束会话；

b) 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；

c) 在通信过程中，应对敏感信息字段进行加密。

6.1.4.6.2 测评方式

访谈，测试。

6.1.4.6.3 测评对象

安全员，重要应用系统。

6.1.4.6.4 测评实施

a) 可访谈安全员，询问业务系统数据在存储和传输过程中是否采取保密措施（如在通信双方建立会话之前利用密码技术进行会话初始化验证，在通信过程中对敏感信息字段进行加密等），具体措施有哪些，是否所有应用系统的通信都采取了上述措施；

b) 应测试重要应用系统，查看当通信双方中的一方在一段时间内未作任何响应，另一方是否能自动结束会话；系统是否能在通信双方建立连接之前，利用密码技术进行会话初始化验证（如SSL建立加密通道前是否利用密码技术进行会话初始验证）；

c) 应测试重要应用系统，通过通信双方中的一方在一段时间内未作任何响应，查看另一方是否能自动结束会话，测试当通信双方中的一方在一段时间内未作任何响应，另一方是否能自动结束会话的功能是否有效；

d) 应测试重要应用系统，通过查看通信双方数据包的内容，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。

6.1.4.6.5 结果判定

a) 6.1.4.6.4 b）-d）均为肯定，则信息系统符合本单元测评项要求。

6.1.4.7 软件容错

6.1.4.7.1 测评项

a) 应对通过人机接口输入或通过通信接口输入的数据进行有效性检验；

b) 应对通过人机接口方式进行的操作提供“回退”功能，即允许按照操作的序列进行回退；

c) 在故障发生时，应继续提供一部分功能，确保能够实施必要的措施。

6.1.4.7.2 测评方式

访谈，检查，测试。

6.1.4.7.3 测评对象

安全员，重要应用系统。

6.1.4.7.4 测评实施

a) 可访谈系统管理员，询问业务系统是否有保证软件具有容错能力的措施（如对人机接口输入或通过通信接口输入的数据进行有效性检验等），具体措施有哪些；

b) 应检查重要应用系统，查看业务系统是否对人机接口输入（如用户界面的数据输入）或通信接口输入的数据进行有效性检验；是否允许按照操作的序列进行回退（如撤消操作）；是否在故障发生时继续提供一部分功能，确保能够实施必要的措施（如对重要数据的保存）；

c) 应测试重要应用系统，可通过输入的不同（如数据格式或长度等符合、不符合软件设定的要求），验证系统人机接口有效性检验功能是否正确；

d) 应测试重要应用系统，可通过多步操作，然后回退，验证系统能否按照操作的序列进行正确的回退；可通过给系统人为制造一些故障（如系统异常），验证系统能否在故障发生时继续提供一部分功能，并能实施必要的措施。

6.1.4.7.5 结果判定

a) 6.1.4.7.4 b）-d）均为肯定，则信息系统符合本单元测评项要求。

6.1.4.8 资源控制

6.1.4.8.1 测评项

a) 应限制单个用户的多重并发会话；

b) 应对应用系统的最大并发会话连接数进行限制；

c) 应对一个时间段内可能的并发会话连接数进行限制。

6.1.4.8.2 测评方式

访谈，检查，测试。

6.1.4.8.3 测评对象

系统管理员，重要应用系统。

6.1.4.8.4 测评实施

a) 可访谈系统管理员，询问业务系统是否有资源控制的措施（如对应用系统的最大并发会话连接数进行限制，是否禁止同一用户账号在同一时间内并发登录，是否对一个时间段内可能的并发会话连接数进行限制，对一个访问用户或一个请求进程占用的资源分配最大限额和最小限额等），具体措施有哪些；

b) 应检查重要应用系统，查看系统是否有最大并发会话连接数的限制；

c) 应测试重要应用系统，可通过对系统进行进行超过最大并发会话连接数进行连接，验证系统能否正确地限制最大并发会话连接数；

d) 应测试重要应用系统，可通过在一个时间段内，用超过设定的并发连接数对系统进行连接，查看能否连接成功，验证系统对一个时间段内可能的并发会话连接数进行限制的功能是否正确。

6.1.4.8.5 结果判定

a) 6.1.4.8.4 b）-d）均为肯定，则信息系统符合本单元测评项要求。

6.1.4.9 代码安全

6.1.4.9.1 测评项

a) 应对应用程序进行恶意代码扫描；

b) 应对应用程序进行安全脆弱性分析。

6.1.4.9.2 测评方式

访谈，检查。

6.1.4.9.3 测评对象

系统管理员，重要应用系统，总体规划/设计文档，相关证明材料（证书）。

6.1.4.9.4 测评实施

a) 可访谈系统管理员，询问业务系统是否有保证质量的措施（如系统是否有程序编写安全规范，开发人员是否参照规范编写代码），具体措施有哪些；

b) 应检查设计/验收文档和相关证明材料（证书），查看是否有对应用程序进行恶意代码扫描，确认不存在恶意代码的声明；

c) 应检查设计/验收文档和相关证明材料（证书），查看是否对应用程序进行安全脆弱性分析，确认存在的脆弱性不会被利用的声明；

d) 应检查重要应用系统，查看代码的编制是否与代码安全规范要求一致。

6.1.4.9.5 结果判定

a) 如果6.1.4.9.4 b）-c）缺少相关材料，则该项为否定；

b) 6.1.4.9.4 b）-d）均为肯定，则信息系统符合本单元测评项要求。

6.1.5 数据安全

6.1.5.1 数据完整性

6.1.5.1.1 测评项

a) 应能够检测到系统管理数据、鉴别信息和用户数据在传输过程中完整性受到破坏；

b) 应能够检测到系统管理数据、鉴别信息和用户数据在存储过程中完整性受到破坏。

6.1.5.1.2 测评方式

访谈，检查。

6.1.5.1.3 测评对象

安全员，重要应用系统，设计/验收文档，相关证明性材料（如证书、检验报告等）。

6.1.5.1.4 测评实施

a) 可访谈安全员，询问业务系统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) 应检查操作系统、网络设备、数据库管理系统的设计/验收文档或相关证明性材料（如证书、检验报告等）等，查看其是否有能检测/验证到系统管理数据（如WINDOWS 域管理、目录管理数据）、鉴别信息（如用户名和口令）和用户数据（如用户数据文件）在传输过程中完整性受到破坏；能否检测/验证到系统管理数据（如WINDOWS 注册表、系统文件）、身份鉴别信息（如用户名和口令存储文件）和用户数据（如用户数据文件）在存储过程中未授权的修改与破坏；能否检测到系统管理数据、鉴别信息和用户数据在操作过程中完整性受到破坏；如果有相关信息，查看其配置如何；

c) 应检查重要应用系统，查看其是否配备检测/验证系统管理数据、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/验证系统管理数据、身份鉴别信息和用户数据在存储过程中未授权修改与破坏的功能；是否具备检测/验

证系统管理数据、鉴别信息和用户数据在操作过程中完整性受到破坏的功能。

6.1.5.1.5 结果判定

a) 如果 6.1.5.1.4 b）缺少相关材料，则该项为否定；

b) 6.1.5.1.4 b）-c）均为肯定，则信息系统符合本单元测评项要求。

6.1.5.2 数据保密性

6.1.5.2.1 测评项

a) 网络设备、操作系统、数据库系统和应用系统的鉴别信息、敏感的系统管理数据和敏感的用户数据应采用加密或其他有效措施实现传输保密性；

b) 网络设备、操作系统、数据库系统和应用系统的鉴别信息、敏感的系统管理数据和敏感的用户数据应采用加密或其他保护措施实现存储保密性；

c) 当使用便携式和移动式设备时，应加密或者采用可移动磁盘存储敏感信息。

6.1.5.2.2 测评方式

访谈，检查，测试。

6.1.5.2.3 测评对象

系统管理员、网络管理员、安全员、数据库管理员，操作系统，网络设备，数据库系统，重要应用系统，设计/验收文档。

6.1.5.2.4 测评实施

a) 可访谈网络管理员，询问信息系统中的网络设备的鉴别信息、敏感的系统管理数据和敏感的用户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保护措施实现存储保密性；

b) 可访谈系统管理员，询问信息系统中的操作系统的鉴别信息、敏感的系统管理数据和敏感的用户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保护措施实现存储保密性；

c) 可访谈数据库管理员，询问信息系统中的数据库管理系统的鉴别信息、敏感的系统管理数据和敏感的用户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保护措施实现存储保密性；

d) 可访谈安全员，询问信息系统中的应用系统的鉴别信息、敏感的系统管理数据和敏感的用户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保护措施实现存储保密性；

e) 可访谈安全员，询问当使用便携式和移动式设备时，是否加密或者采用可移动磁盘存储敏感信息；

f) 可访谈安全员，询问系统采用的密码算法和密钥是否符合国家密码管理规定；

g) 应检查操作系统、网络设备、数据库系统、重要应用系统设计/验收文档，查看其是否有关于其鉴别信息、敏感的系统管理数据和敏感的用户数据采用加密或其他有效措施实现传输保密性描述，是否有采用加密或其他保护措施实现存储保密性的描述；

h) 应检查重要应用系统，查看其鉴别信息、敏感的系统管理数据和敏感的用户数据是否采用加密或其他有效措施实现传输保密性描述，是否采用加密或其他保护措施实现存储保密性；

i) 应测试重要应用系统，通过用嗅探工具获取系统传输数据报，查看其是否采用加密或其他有效措施实现传输保密性。

6.1.5.2.5 结果判定

a) 如果缺少设计/验收文档，6.1.5.2.4 g）为否定；

b) 6.1.5.2.4 g）-i）均为肯定，则信息系统符合本单元测评项要求。

6.1.5.3 数据备份和恢复

6.1.5.3.1 测评项

a) 应提供自动备份机制对重要信息进行有选择的数据备份；

b) 应提供恢复重要信息的功能；

c) 应提供重要网络设备、通信线路和服务器的硬件冗余。

6.1.5.3.2 测评方式

访谈，检查。

6.1.5.3.3 测评对象

系统管理员、网络管理员、安全员、数据库管理员，重要应用系统，重要应用系统设计/验收文档。

6.1.5.3.4 测评实施

a) 可访谈网络管理员，询问信息系统中的网络设备是否提供用户有选择的备份重要信息的功能；是否提供重要网络设备、通信线路和服务器的硬件冗余；

b) 可访谈系统管理员，询问信息系统中的操作系统是否提供用户有选择的备份重要信息的功能；

c) 可访谈数据库管理员，询问信息系统中的数据库管理系统是否提供用户有选择的备份重要信息的功能；

d) 应检查重要应用系统设计/验收文档，查看其是否有描述应用系统提供用户有选择的备份重要信息的功能的描述；

e) 应检查操作系统、网络设备、数据库系统、关键应用系统，查看其是否配置有选择的备份和恢复重要信息恢复的功能，其配置是否正确；

f) 应检查重要网络设备、通信线路和服务器是否提供硬件冗余。

6.1.5.3.5 结果判定

a) 如果缺少设计/验收文档，6.1.5.3.4 d）为否定；

b) 6.1.5.3.4 d）-f）均为肯定，则信息系统符合本单元测评项要求。

6.2 安全管理测评

6.2.1 安全管理机构

6.2.1.1 岗位设置

6.2.1.1.1 测评项

a) 应设立信息安全管理工作的职能部门，设立安全主管人、安全管理各个方面的负责人，定义各负责人的职责；

b) 应设立系统管理人员、网络管理人员、安全管理人员岗位，定义各个工作岗位的职责；

c) 应制定文件明确安全管理机构各个部门和岗位的职责、分工和技能要求。

6.2.1.1.2 测评方式

访谈，检查。

6.2.1.1.3 测评对象

安全主管，安全管理某方面的负责人，部门、岗位职责文件。

6.2.1.1.4 测评实施

a) 应访谈安全主管，询问是否设立安全管理机构（即信息安全管理工作的职能部门，可以由其它部门兼职）；机构内部门设置情况如何，是否明确机构内各部门的职责分工；

b) 应访谈安全主管，询问是否设立安全管理各个方面的负责人，设置了哪些工作岗位（如安全主管、安全管理各个方面的负责人、机房管理员、系统管理员、网络管理员和安全员等重要岗位），是否明确各个岗位的职责分工；

c) 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；

d) 应检查部门、岗位职责文件，查看文件是否明确安全管理机构的职责，是否明确机构内各部门的职责和分工，部门职责是否涵盖物理、网络和系统等各个方面；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、网络管理员和安全员等各个岗位，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。

6.2.1.1.5 结果判定

a) 如果6.2.1.1.4 c）被访谈人员表述与文件描述一致，则该项为肯定；

b) 6.2.1.1.4 a）-d）均为肯定，则信息系统符合本单元测评项要求。

6.2.1.2 人员配备

6.2.1.2.1 测评项

a) 应配备一定数量的系统管理人员、网络管理人员、安全管理人员等；

b) 安全管理人员不能兼任网络管理员、系统管理员、数据库管理员等。

6.2.1.2.2 测评方式

访谈，检查。

6.2.1.2.3 测评对象

安全主管，人员配备要求的相关文档，管理人员名单。

6.2.1.2.4 测评实施

a) 应访谈安全主管，询问各个安全管理岗位人员（按照岗位职责文件询问，包括机房管理员、系统管理员、数据库管理员、网络管理员、安全员等重要岗位人员）配备情况，包括数量、专职还是兼职等；

b) 应检查人员配备要求的相关文档，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、安全员等重要岗位人员；

c) 应检查管理人员名单，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、安全员等重要岗位人员的信息，确认安全员是否没有兼任网络管理员、系统管理员、数据库管理员等。

6.2.1.2.5 结果判定

a) 如果6.2.1.2.4 a）设置的安全员没有兼任网络管理员、系统管理员、数据库管理员等，则该项为肯定；

b) 6.2.1.2.4 a）-c）均为肯定，则信息系统符合本单元测评项要求。

6.2.1.3 授权和审批

6.2.1.3.1 测评项

a) 应授权审批部门及批准人，对关键活动进行审批；

b) 应列表说明须审批的事项、审批部门和可批准人。

6.2.1.3.2 测评方式

访谈，检查。

6.2.1.3.3 测评对象

安全主管，关键活动的批准人，审批事项列表，审批文档。

6.2.1.3.4 测评实施

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） 应访谈关键活动的批准人，询问其对关键活动的审批范围包括哪些（如网络系统、应用系统、数据库管理系统、重要服务器和设备等重要资源的访问，重要管理制度的制定和发布，人员的配备、培训和产品的采购等），审批程序如何；

c） 应检查审批事项列表，查看列表是否明确须审批事项、审批部门、批准人及审批程序等；

d） 应检查经审批的文档，查看是否具有批准人的签字和审批部门的盖章。

6.2.1.3.5 结果判定

a） 6.2.1.3.4 a）-d）均为肯定，则信息系统符合本单元测评项要求。

6.2.1.4 沟通和合作

6.2.1.4.1 测评项

a） 应加强各类管理人员和组织内部机构之间的合作与沟通，定期或不定期召开协调会议，共同协助处理信息安全问题；

b） 信息安全职能部门应定期或不定期召集相关部门和人员召开安全工作会议，协调安全工作的实施；

c） 应加强与兄弟单位、公安机关、电信公司的合作与沟通，以便在发生安全事件时能够得到及时的支持。

6.2.1.4.2 测评方式

访谈，检查。

6.2.1.4.3 测评对象

安全主管，安全管理人员，会议文件，会议记录，外联单位说明文档。

6.2.1.4.4 测评实施

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，联系方式有哪些，与组织机构内其他部门之间有哪些合作内容，沟通、合作方式有哪些；

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部署安全工作的实施，参加会议的部门和人员有哪些，会议结果如何；

c） 应访谈安全管理人员（从系统管理员和安全员等人员中抽查），询问其与外单位人员，与组织机构内其他部门人员，与内部各部门管理人员之间的沟通方式和主要沟通内容有哪些；

d） 应检查部门间协调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；

e） 应检查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、会议结果等的描述；

f） 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、电信公司及兄弟公司，是否说明外联单位的联系人和联系方式等内容。

6.2.1.4.5 结果判定

a） 6.2.1.4.4 a）-f）均为肯定，则信息系统符合本单元测评项要求。

6.2.1.5 审核和检查

6.2.1.5.1 测评项

a） 应由安全管理人员定期进行安全检查，检查内容包括用户账号情况、系统漏洞情况、系统审计情况等。

6.2.1.5.2 测评方式

访谈，检查。

6.2.1.5.3 测评对象

安全主管，安全员，安全检查记录。

6.2.1.5.4 测评实施

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安全检查，检查周期多长，是否明确检查内容；

b) 应访谈安全员，询问安全检查包含哪些内容，检查人员有哪些，检查程序是否按照系统相关策略和要求进行，检查结果如何；

c) 应检查安全检查记录，查看记录时间与检查周期是否一致，文档中是否有检查内容、检查人员、检查结果等的描述。

6.2.1.5.5 结果判定

a) 6.2.1.5.4 a）-c）均为肯定，则信息系统符合本单元测评项要求。

6.2.2 安全管理制度

6.2.2.1 管理制度

6.2.2.1.1 测评项

a) 应制定信息安全工作的总体方针和政策性文件，说明机构安全工作的总体目标、范围、方针、原则、责任等；

b) 应对安全管理活动中重要的管理内容建立安全管理制度，以规范安全管理活动，约束人员的行为方式；

c) 应对要求管理人员或操作人员执行的重要管理操作，建立操作规程，以规范操作行为，防止操作失误。

6.2.2.1.2 测评方式

访谈，检查。

6.2.2.1.3 测评对象

安全主管，总体方针、政策性文件和安全策略文件，安全管理制度清单，操作规程。

6.2.2.1.4 测评实施

a) 应访谈安全主管，询问是否制定信息安全工作的总体方针、政策性文件和安全策略等，是否对重要管理内容建立安全管理制度，是否对重要管理操作制定操作规程；

b) 应检查信息安全工作的总体方针、政策性文件和安全策略文件，查看文件是否明确机构安全工作的总体目标、范围、方针、原则、责任等；

c) 应检查安全管理制度清单，查看是否覆盖物理、网络、主机系统、数据、应用和管理等层面；

d) 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。

6.2.2.1.5 结果判定

a) 6.2.2.1.4 a）-d）均为肯定，则信息系统符合本单元测评项要求。

6.2.2.2 制定和发布

6.2.2.2.1 测评项

a) 应在信息安全职能部门的总体负责下，组织相关人员制定；

b) 应保证安全管理制度具有统一的格式风格，并进行版本控制；

c) 应组织相关人员对制定的安全管理进行论证和审定；

d) 安全管理制度应经过管理层签发后按照一定的程序以文件形式发布。

6.2.2.2.2 测评方式

访谈，检查。

6.2.2.2.3 测评对象

安全主管，制度制定和发布要求管理文档，评审记录，安全管理制度。

6.2.2.2.4 测评实施

a) 应访谈安全主管，询问安全管理制度是否在信息安全职能部门的总体负责下统一制定，参与制定人员有哪些；

b) 应访谈安全主管，询问安全管理制度的制定程序，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（如召开评审会、函审、内部审核等），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) 应检查安全管理制度文档，查看是否有版本标识，是否有管理层的签字或盖章；查看其格式是否统一。

6.2.2.2.5 结果判定

a) 6.2.2.2.4 a）-e）均为肯定，则信息系统符合本单元测评项要求。

6.2.2.3 评审和修订

6.2.2.3.1 测评项

a) 应定期对安全管理制度进行评审和修订，对存在不足或需要改进的安全管理制度进行修订。

6.2.2.3.2 测评方式

访谈，检查。

6.2.2.3.3 测评对象

安全主管，安全管理制度列表，评审记录。

6.2.2.3.4 测评实施

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

b) 应检查是否具有需要定期评审的安全管理制度列表；

c) 应检查安全管理制度评审记录，查看记录日期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。

6.2.2.3.5 结果判定

a) 6.2.2.3.4 a）-c）均为肯定，则信息系统符合本单元测评项要求。

6.2.3 人员安全管理

6.2.3.1 人员录用

6.2.3.1.1 测评项

a) 应保证被录用人具备基本的专业技术水平和安全管理知识；

b) 应对被录用人声明的身份、背景、专业资格和资质等进行审查；

c) 应对被录用人所具备的技术技能进行考核；

d) 应对被录用人说明其角色和职责；

e) 应签署保密协议。

6.2.3.1.2 测评方式

访谈，检查。

6.2.3.1.3 测评对象

人事负责人，人事工作人员，人员录用要求管理文档，人员审查文档或记录，考核文档或记录，保密协议。

6.2.3.1.4 测评实施

a) 应访谈人事负责人，询问在人员录用时对人员条件有哪些要求，目前录用的安全管理和技术人员是否有能力完成与其职责相对应的工作；

b) 应访谈人事工作人员，询问在人员录用时是否对被录用人的身份、背景、专业资格和资质进行审查，录用后是否与其签署保密协议，是否对其说明工作职责；

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、专业资格或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；

e) 应检查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。

6.2.3.1.5 结果判定

a) 6.2.3.1.4 a）-f）均为肯定，则信息系统符合本单元测评项要求。

6.2.3.2 人员离岗

6.2.3.2.1 测评项

a) 应立即终止由于各种原因即将离岗的员工的所有访问权限；

b) 应取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备；

c) 应经机构人事部门办理严格的调离手续，并承诺调离后的保密义务后方可离开。

6.2.3.2.2 测评方式

访谈，检查。

6.2.3.2.3 测评对象

安全主管，人事工作人员，安全处理记录，保密承诺文档。

6.2.3.2.4 测评实施

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

b) 应访谈人事工作人员，询问调离手续包括哪些，是否要求调离人员承诺相关保密义务后方可离开；

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) 应检查保密承诺文档，查看是否有调离人员的签字。

6.2.3.2.5 结果判定

a) 6.2.3.2.4 a）-d）均为肯定，则信息系统符合本单元测评项要求。

6.2.3.3 人员考核

6.2.3.3.1 测评项

a) 应定期对各个岗位的人员进行安全技能及安全认知的考核；

b) 应对关键岗位的人员进行全面、严格的安全审查；

c) 应对违背安全策略和规定的人员进行惩戒。

6.2.3.3.2 测评方式

访谈。

6.2.3.3.3 测评对象

安全主管，人事工作人员。

6.2.3.3.4 测评实施

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） 应访谈人事工作人员，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，审查内容有哪些（如操作行为、社会关系、社交活动等），是否全面；

c） 应访谈人事工作人员，询问对违背安全策略和规定的人员有哪些惩戒措施。

6.2.3.3.5 结果判定

a） 如果6.2.3.3.4 b）被访谈人员表述审查内容包含社会关系、社交活动、操作行为等各个方面，则该项为肯定；

b） 如果6.2.3.3.4 c）被访谈人员表述与文件描述一致，则该项为肯定；

c） 6.2.3.3.4 a）-c）均为肯定，则信息系统符合本单元测评项要求。

6.2.3.4 安全意识教育和培训

6.2.3.4.1 测评项

a） 应对各类人员进行安全意识教育；

b） 应告知人员相关的安全责任和惩戒措施；

c） 应制定安全教育和培训计划，对信息安全基础知识、岗位操作规程等进行培训；

d） 应对安全教育和培训的情况和结果进行记录并归档保存。

6.2.3.4.2 测评方式

访谈，检查。

6.2.3.4.3 测评对象

安全主管，安全员，系统管理员，网络管理员，培训计划，培训记录。

6.2.3.4.4 测评实施

a） 应访谈安全主管，询问是否制定安全教育和培训计划并按计划对各个岗位人员进行安全教育和培训，以什么形式进行，效果如何；

b） 应访谈安全员、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目的、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；查看记录与培训计划是否一致。

6.2.3.4.5 结果判定

a） 如果6.2.3.4.4 b）访谈人员能够表述清楚询问内容，且安全职责、惩戒措施和岗位操作规程表述与文件描述一致，则该项为肯定；

b） 6.2.3.4.4 a）-d）均为肯定，则信息系统符合本单元测评项要求。

6.2.3.5 第三方人员访问管理

6.2.3.5.1 测评项

a） 第三方人员应在访问前与机构签署安全责任合同书或保密协议；

b） 对重要区域的访问，必须经过有关负责人的批准，并由专人陪同或监督下进行，并记录备案。

6.2.3.5.2 测评方式

访谈，检查。

6.2.3.5.3 测评对象

安全主管，安全管理人员，安全责任合同书或保密协议，第三方人员访问管理文档，登记记录。

6.2.3.5.4 测评实施

a) 应访谈安全主管，询问对第三方人员（如向系统提供服务的系统软、硬件维护人员，业务合作伙伴、评估人员等）的访问采取哪些管理措施，是否要求第三方人员访问前与机构签署安全责任合同书或保密协议；

b) 应访谈安全管理人员，询问对第三方人员访问重要区域（如访问主机房等）采取哪些措施，是否经有关负责人批准才能访问，是否由专人陪同或监督，是否进行记录并备案管理；

c) 应检查安全责任合同书或保密协议，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。

d) 应检查第三方人员访问管理文档，查看是否规定对第三方人员访问哪些重要区域应经过负责人批准；

e) 应检查第三方人员访问重要区域的登记记录，查看记录是否描述了第三方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。

6.2.3.5.5 结果判定

a) 6.2.3.5.4 a）-e）均为肯定，则信息系统符合本单元测评项要求。

6.2.4 系统建设管理

6.2.4.1 系统定级

6.2.4.1.1 测评项

a) 应明确信息系统划分的方法；

b) 应确定信息系统的安全保护等级；

c) 应以书面的形式定义确定了安全保护等级的信息系统的属性，包括使命、业务、网络、硬件、软件、数据、边界、人员等；

d) 应确保信息系统的定级结果经过相关部门的批准。

6.2.4.1.2 测评方式

访谈，检查。

6.2.4.1.3 测评对象

安全主管，系统划分文档，系统定级文档，系统属性说明文档。

6.2.4.1.4 测评实施

a) 应访谈安全主管，询问划分信息系统的方法和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，是否对其进行明确描述；定级结果是否获得了相关部门（如上级主管部门）的批准；

b) 应检查系统划分相关文档，查看文档是否明确描述信息系统划分的方法和理由；

c) 应检查系统定级文档，查看文档是否给出信息系统的安全保护等级，是否给出安全等级保护措施组成SxCyGz值；查看定级结果是否有相关部门的批准盖章；

d) 应检查系统属性说明文档，查看文档是否明确了系统使命、业务、网络、硬件、软件、数据、边界、人员等。

6.2.4.1.5 结果判定

a) 6.2.4.1.4 a）没有上级主管部门的，如果有安全主管的批准，则该项为肯定；

b) 6.2.4.1.4 a）-e）均为肯定，则信息系统符合本单元测评项要求。

6.2.4.2 安全方案设计

6.2.4.2.1 测评项

a) 应根据系统的安全级别选择基本安全措施，依据风险评估的结果补充和调整安全措施；

b） 应以书面的形式描述对系统的安全保护要求和策略、安全措施等内容，形成系统的安全方案；

c） 应对安全方案进行细化，形成能指导安全系统建设和安全产品采购的详细设计方案；

d） 应组织相关部门和有关安全技术专家对安全设计方案的合理性和正确性进行论证和审定；

e） 应确保安全设计方案必须经过批准，才能正式实施。

6.2.4.2.2 测评方式

访谈，检查。

6.2.4.2.3 测评对象

系统建设负责人，安全方案，详细设计方案，专家论证文档。

6.2.4.2.4 测评实施

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，是否依据风险评估的结果补充和调整安全措施，做过哪些调整；

b） 应访谈系统建设负责人，询问是否制定系统的安全方案并根据安全方案制定出系统详细设计方案指导安全系统建设和安全产品采购，是否组织相关部门和有关安全技术专家对安全设计方案进行论证和审定，安全设计方案是否经过安全主管领导或管理层的批准；

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对应的安全措施等内容；

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。

6.2.4.2.5 结果判定

a） 6.2.4.2.4 a）-e）均为肯定，则信息系统符合本单元测评项要求。

6.2.4.3 产品采购

6.2.4.3.1 测评项

a） 应确保安全产品的使用符合国家的有关规定；

b） 应确保密码产品的使用符合国家密码主管部门的要求；

c） 应指定或授权专门的部门负责产品的采购。

6.2.4.3.2 测评方式

访谈，检查。

6.2.4.3.3 测评对象

安全主管，系统建设负责人，信息安全产品。

6.2.4.3.4 测评实施

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，询问系统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（边界安全设备、重要服务器操作系统、数据库等）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，如《商用密码管理条例》规定任何单位只能使用经过国家密码管理机构认可的商用密码产品，商用密码产品发生故障，必须有国家密码管理机构指定的单位维修，报废商用密码产品应向国家密码管理机构备案等。

6.2.4.3.5 结果判定

a） 如果6.2.4.3.4 c）访谈说明没有采用密码产品，则测评实施c）、e）为不适用；

b） 6.2.4.3.4 a）-e）均为肯定，则信息系统符合本单元测评项要求。

6.2.4.4 自行软件开发

6.2.4.4.1 测评项

a） 应确保开发环境与实际运行环境物理分开；

b） 应确保提供软件设计的相关文档和使用指南；

c） 应确保系统开发文档由专人负责保管，系统开发文档的使用受到控制。

6.2.4.4.2 测评方式

访谈，检查。

6.2.4.4.3 测评对象

系统建设负责人，软件设计的相关文档和使用指南，文档使用控制记录。

6.2.4.4.4 测评实施

a） 应访谈系统建设负责人，询问系统是否自主开发软件，自主开发是否有相应的控制措施，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，询问系统开发文档是否由专人负责保管，负责人是何人，如何控制使用（如限制使用人员范围并做使用登记等）；

c） 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）和软件使用指南或操作手册和维护手册等；

d） 应检查软件开发环境与系统运行环境在物理上是否是分开的；

e） 应检查是否具有系统开发文档的使用控制记录。

6.2.4.4.5 结果判定

a） 6.2.4.4.4 a）-e）均为肯定，则信息系统符合本单元测评项要求。

6.2.4.5 外包软件开发

6.2.4.5.1 测评项

a） 应与软件开发单位签订协议，明确知识产权的归属和安全方面的要求；

b） 应根据协议的要求检测软件质量；

c） 应在软件安装之前检测软件包中可能存在的恶意代码；

d） 应确保提供软件设计的相关文档和使用指南。

6.2.4.5.2 测试方法

访谈，检查。

6.2.4.5.3 测试对象

系统建设负责人，软件开发安全协议，软件开发文档。

6.2.4.5.4 测评实施

a） 应访谈系统建设负责人，询问在外包软件前是否对软件开发单位以书面文档形式（如软件开发安全协议）规范软件开发单位的责任、开发过程中的安全行为、开发环境要求和软件质量等相关内容，是否具有能够独立的对软件进行日常维护和使用所需的文档；

b） 应访谈系统建设负责人，询问软件交付前是否依据开发协议的技术指标对软件功能和性能等进行验收检测，验收检测是否是由开发商和委托方共同参与，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；

c） 应检查软件开发协议是否规定知识产权归属、安全行为等内容；

d） 应检查是否具有需求分析说明书、软件设计说明书和软件操作手册等开发文档。

6.2.4.5.5 结果判定

a） 6.2.4.5.4 a）—d）均为肯定，则信息系统符合本单元测评项要求。

6.2.4.6 工程实施

6.2.4.6.1 测评项

a） 应与工程实施单位签订与安全相关的协议，约束工程实施单位的行为；

b） 应指定或授权专门的人员或部门负责工程实施过程的管理；

c） 应制定详细的工程实施方案控制实施过程。

6.2.4.6.2 测试方法

访谈，检查。

6.2.4.6.3 测试对象

系统建设负责人，工程安全建设协议，工程实施方案。

6.2.4.6.4 测评实施

a） 应访谈系统建设负责人，询问是否以书面形式（如工程安全建设协议）约束工程实施方的工程实施行为；

b） 应访谈系统建设负责人，询问是否指定专门人员或部门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；

c） 应检查工程安全建设协议，查看其内容是否覆盖工程实施方的责任、任务要求和质量要求等方面内容，约束工程实施行为；

d） 应检查工程实施方案，查看其内容是否覆盖工程时间限制、进度控制和质量控制等方面内容。

6.2.4.6.5 结果判定

a) 6.2.4.6.4 a）—d）均为肯定，则信息系统符合本单元测评项要求。

6.2.4.7 测试验收

6.2.4.7.1 测评项

a) 应对系统进行安全测试验收；

b) 应在测试验收前根据设计方案或合同要求等制订测试验收方案，测试验收过程中详细记录测试验收结果，形成测试验收报告；

c) 应组织相关部门和相关人员对系统测试验收报告进行审定，没有疑问后由双方签字。

6.2.4.7.2 测试方法

访谈，检查。

6.2.4.7.3 测试对象

系统建设负责人，系统测试方案，系统测试记录，系统测试报告，系统验收报告。

6.2.4.7.4 测评实施

a) 应访谈系统建设负责人，询问在信息系统正式运行前，是否根据设计方案或合同要求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，询问是否对测试过程（包括测试前、测试中和测试后）进行文档化要求，是否根据设计方案或合同要求组织相关部门和人员对测试报告进行符合性审定；

c) 应检查工程测试方案，查看其是否对参与测试部门、人员和现场操作过程等进行要求；查看测试记录是否详细记录了测试时间、人员、现场操作过程和测试结果等方

面内容；查看测试报告是否提出存在问题及改进意见等；

d) 应检查是否具有系统验收报告。

6.2.4.7.5 结果判定

a) 6.2.4.7.4 a）—d）均为肯定，则信息系统符合本单元测评项要求。

6.2.4.8 系统交付

6.2.4.8.1 测评项

a) 应明确系统的交接手续，并按照交接手续完成交接工作；

b) 应由系统建设方完成对委托建设方的运维技术人员的培训；

c) 应由系统建设方提交系统建设过程中的文档和指导用户进行系统运行维护的文档；

d) 应由系统建设方进行服务承诺，并提交服务承诺书，确保对系统运行维护的支持。

6.2.4.8.2 测试方法

访谈，检查。

6.2.4.8.3 测试对象

系统建设负责人，系统交付清单，服务承诺书，培训记录。

6.2.4.8.4 测评实施

a) 应访谈系统建设负责人，询问交接手续是什么，系统交接工作是否按照该手续办理，是否根据交接清单对所交接的设备、文档、软件等进行清点，交接清单是否满足合同的有关要求；

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进行运行维护，如果是，系统建设实施方是否对运维技术人员进行过培训，针对哪些方面进行过培训，是否以书面形式承诺对系统运行维护提供一定的技术支持服务，系统是否具有支持其独立运行维护的文档；

c) 应检查系统交付清单，查看其是否具有系统建设文档（如系统建设方案）、指导用户进行系统运维的文档（如服务器操作规程书）以及系统培训手册等文档名称；

d) 应检查是否具有系统建设方的服务承诺书和对系统进行的培训记录。

6.2.4.8.5 结果判定

a) 6.2.4.8.4 a）—d）均为肯定，则信息系统符合本单元测评项要求。

6.2.4.9 安全服务商选择

6.2.4.9.1 测评项

a) 应确保安全服务商的选择符合国家的有关规定。

6.2.4.9.2 测试方法

访谈。

6.2.4.9.3 测试对象

系统建设负责人。

6.2.4.9.4 测评实施

a) 应访谈系统建设负责人，询问对信息系统进行安全规划、设计、实施、维护、测评等服务的安全服务单位是否符合国家有关规定。

6.2.4.9.5 结果判定

a) 6.2.4.9.4 a）为肯定，则信息系统符合本单元测评项要求。

6.2.5 系统运维管理

6.2.5.1 环境管理

6.2.5.1.1 测评项

a) 应对机房供配电、空调、温湿度控制等设施指定专人或专门的部门定期进行维护管理，维护周期多长；

b） 应配备机房安全管理人员，对机房的出入、服务器的开机或关机等工作进行管理；
c） 应建立机房安全管理制度，对有关机房物理访问，物品带进、带出机房和机房环境安全等方面作出规定；
d） 应对机房来访人员实行登记、备案管理，同时限制来访人员的活动范围；
e） 应加强对办公环境的保密性管理，包括如工作人员调离办公室应立即交还该办公室钥匙和不在办公区接待来访人员等。

6.2.5.1.2 测评方式

访谈，检查。

6.2.5.1.3 测评对象

物理安全负责人，机房安全管理制度，机房进出登记表。

6.2.5.1.4 测评实施

a） 应访谈物理安全负责人，询问是否对机房基本设施（如空调、供配电设备等）进行定期维护，由何部门/何人负责，维护周期多长；
b） 应访谈物理安全负责人，询问是否指定人员负责机房安全管理工作，对机房的出入管理是否要求进行制度化和文档化；
c） 应访谈物理安全负责人，询问是否对保证办公环境的保密性采取相应措施，如人员调离后权力收回等；
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、带出机房和机房环境安全等方面；
e） 应检查机房进出登记表，查看其是否记录外来人员进出时间、人员姓名和访问原因等方面内容。

6.2.5.1.5 结果判定

a） 6.2.5.1.4 a）-e）均为肯定，则信息系统符合本单元测评项要求。

6.2.5.2 资产管理

6.2.5.2.1 测评项

a） 应建立资产安全管理制度，规定信息系统资产管理的责任人员或责任部门；
b） 应编制并保存与信息系统相关的资产、资产所属关系、安全级别和所处位置等信息的资产清单；
c） 应根据资产的重要程度对资产进行定性赋值和标识管理，根据资产的价值选择相应的管理措施。

6.2.5.2.2 测评方式

访谈，检查。

6.2.5.2.3 测评对象

安全主管，资产管理员，资产清单，资产安全管理制度，设备。

6.2.5.2.4 测评实施

a） 应访谈安全主管，询问是否指定资产管理的责任人员或部门，由何部门/何人负责；
b） 应访谈物理安全负责人，询问是否对资产管理要求文档化；
c） 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赋值和标识管理，不同类别的资产是否采取不同的管理措施；
d） 应检查资产清单，查看其内容是否覆盖资产责任人、所属级别、所处位置和所属部门等方面；
e） 应检查资产安全管理制度，询问是否明确资产管理的责任部门、责任人等方面要求；
f） 应检查资产清单中的设备，查看其是否具有相应标识。

6.2.5.2.5 结果判定

a) 6.2.5.2.4 a）-f）均为肯定，则信息系统符合本单元测评项要求。

6.2.5.3 介质管理

6.2.5.3.1 测评项

a) 应确保介质存放在安全的环境中，并对各类介质进行控制和保护，以防止被盗、被毁、被未授权的修改以及信息的非法泄漏；

b) 应有介质的存储、归档、登记和查询记录，并根据备份及存档介质的目录清单定期盘点；

c) 对于需要送出维修或销毁的介质，应首先清除介质中的敏感数据，防止信息的非法泄漏；

d) 应根据所承载数据和软件的重要程度对介质进行分类和标识管理，并实行存储环境专人管理。

6.2.5.3.2 测评方式

访谈，检查。

6.2.5.3.3 测评对象

资产管理员，介质管理记录，各类介质。

6.2.5.3.4 测评实施

a) 应访谈资产管理员，询问介质的存放环境是否有保护措施，防止其被盗、被毁、被未授权修改以及信息的非法泄漏，是否有专人管理；

b) 应访谈资产管理员，询问是否对介质的使用管理要求文档化，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介质之前是否做过安全处理（如清除其中的敏感数据）；

d) 应检查介质管理记录，查看其是否记录介质的存储、归档和借用等情况；

e) 应检查介质，查看是否对其进行了分类，并具有不同标识。

6.2.5.3.5 结果判定

a) 如果6.2.5.3.4 a）中在防火、防水、防盗等方面均有措施，则该项为肯定；

b) 6.2.5.3.4 a）-e）均为肯定，则信息系统符合本单元测评项要求。

6.2.5.4 设备管理

6.2.5.4.1 测评项

a) 应对信息系统相关的各种设施、设备、线路等指定专人或专门的部门定期进行维护管理；

b) 应对信息系统的各种软硬件设备的选型、采购、发放或领用等过程的申报、审批和专人负责作出规定；

c) 应对终端计算机、工作站、便携机、系统和网络等设备的操作和使用进行规范化管理；

d) 应对带离机房或办公地点的信息处理设备进行控制；

e) 应按操作规程实现服务器的启动/停止、加电/断电等操作，加强对服务器操作的日志文件管理和监控管理，按安全策略的要求对网络及设备进行配置，并对其定期进行检查。

6.2.5.4.2 测评方式

访谈，检查。

6.2.5.4.3 测评对象

资产管理员，系统管理员，审计员，服务器操作规程，设备审批、发放管理文档，设备

使用管理文档，服务器操作日志。

6.2.5.4.4 测评实施

a) 应访谈资产管理员，询问是否对各类设施、设备指定专人或专门部门进行定期维护，由何部门/何人维护，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、发放等）进行审批控制，是否对设备带离机构进行审批控制，设备的操作和使用是否要求规范化管理；

c) 应访谈系统管理员，询问其对服务器是否进行正确配置，对服务器的操作是否按操作规程进行；

d) 应访谈审计员，询问对服务器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；

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) 应检查设备审批、发放管理文档，查看其内容是否对设备选型、采购和发放等环节的申报和审批作出规定；

g) 应检查服务器操作规程，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。

6.2.5.4.5 结果判定

a) 6.2.5.4.4 a）-g）均为肯定，则信息系统符合本单元测评项要求。

6.2.5.5 监控管理

6.2.5.5.1 测评项

a) 应了解服务器的CPU、内存、进程、磁盘使用情况。

6.2.5.5.2 测评方式

访谈。

6.2.5.5.3 测评对象

安全主管，系统运维负责人。

6.2.5.5.4 测评实

a) 应访谈系统运维负责人，询问是否经常查看主要服务器的各项资源指标，如CPU、内存、进程和磁盘等使用情况。

6.2.5.5.5 结果判定

a) 6.2.5.5.4 a）为肯定，则信息系统符合本单元测评项要求。

6.2.5.6 网络安全管理

6.2.5.6.1 测评项

a) 应指定专人对网络进行管理，负责运行日志、网络监控记录的日常维护和报警信息分析和处理工作；

b) 应根据厂家提供的软件升级版本对网络设备进行更新，并在更新前对现有的重要文件进行备份；

c) 应进行网络系统漏洞扫描，对发现的网络系统安全漏洞进行及时的修补；

d) 应保证所有与外部系统的连接均应得到授权和批准；

e) 应建立网络安全管理制度，对网络安全配置和审计日志等作出规定；

f) 应对网络设备的安全策略、授权访问、最小服务、升级与打补丁、维护记录、日志等方面做出具体规定；

g) 应规定网络审计日志的保存时间以便为可能的安全事件调查提供支持。

6.2.5.6.2 测试方法

访谈，检查。

6.2.5.6.3 测试对象

安全主管，安全员，网络管理员，审计员，网络漏洞扫描报告，网络安全管理制度，系统外联授权书，网络审计日志。

6.2.5.6.4 测评实施

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；

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、配置数据等）进行备份，采取什么方式进行备份；是否对网络设备进行过漏洞扫描，对扫描出的漏洞是否及时修补；

c) 应访谈安全员，询问系统网络的外联种类有哪些（互联网、合作伙伴企业网、上级部门网络等），是否都得到授权与批准，由何部门/何人批准；

d) 应访谈审计员，询问是否规定网络审计日志的保存时间，多长时间；

e) 应检查网络漏洞扫描报告，查看其内容是否覆盖网络存在的漏洞、严重级别、原因分析和改进意见等方面；

f) 应检查网络安全管理制度，查看其是否覆盖网络设备的安全策略、授权访问、最小服务、升级与打补丁、维护记录、日志内容、日志保存时间等方面内容；

g) 应检查是否具有内部网络外联的授权批准书；

h) 应检查在规定的保存时间范围内是否存在网络审计日志。

6.2.5.6.5 结果判定

h) 6.2.5.6.4 a）-h）均为肯定，则信息系统符合本单元测评项要求。

6.2.5.7 系统安全管理

6.2.5.7.1 测评项

a) 应指定专人对系统进行管理，删除或者禁用不使用的系统缺省账户；

b) 应建立系统安全管理制度，对系统安全配置、系统帐户及审计日志等方面作出规定；

c) 应定期安装系统的最新补丁程序，并根据厂家提供的可能危害计算机的漏洞进行及时修补，并在安装系统补丁前对现有的重要文件进行备份；

d) 应根据业务需求和系统安全分析确定系统的访问控制策略，系统访问控制策略用于控制分配信息系统、文件及服务的访问权限；

e) 应对系统账户进行分类管理，权限设定应当遵循最小授权要求；

f) 应对系统的安全策略、授权访问、最小服务、升级与打补丁、维护记录、日志等方面做出具体要求；

g) 应规定系统审计日志的保存时间以便为可能的安全事件调查提供支持；

h) 应进行系统漏洞扫描，对发现的系统安全漏洞进行及时的修补。

6.2.5.7.2 测试方法

访谈，检查。

6.2.5.7.3 测试对象

安全主管，安全员，系统管理员，系统审计员，系统安全管理制度，系统审计日志，系统漏洞扫描报告。

6.2.5.7.4 测评实施

a) 应访谈安全主管，询问是否指定专人负责系统安全管理；

b) 应访谈系统管理员，询问是否对系统安全进行制度化管理；

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（系统配置、系统用户数据等）进行备份，采取什么方式进行；是否对系统进行过漏洞扫描，发现漏洞是否及时修补；

d） 应访谈安全员，询问是否根据业务需求和系统安全分析确定系统访问控制策略；

e） 应访谈系统管理员，询问对系统用户是否进行分类，不同类别的用户是否只具有完成其工作的最低权限；对不常用的系统缺省用户是否采取了一定的处理手段阻止其继续使用（如删除或禁用）；

f） 应访谈审计员，询问是否规定系统审计日志的保存时间，多长时间；

g） 应检查在规定的保存时间范围内是否存在系统审计日志；

h） 应检查系统漏洞扫描报告，查看其内容是否覆盖系统存在的漏洞、严重级别、原因分析和改进意见等方面；

i） 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、授权访问、最小服务、升级与打补丁、维护记录、日志、系统帐户等方面做出具体要求。

6.2.5.7.5 结果判定

a） 6.2.5.7.4 a）-i）均为肯定，则信息系统符合本单元测评项要求。

6.2.5.8 恶意代码防范管理

6.2.5.8.1 测评项

a） 应提高所有用户的防病毒意识，告知及时升级防病毒软件；

b） 应在读取移动存储设备（如软盘、移动硬盘、光盘）上的数据以及网络上接收文件或邮件之前，先进行病毒检查，对外来计算机或存储设备接入网络系统之前也要进行病毒检查；

c） 应指定专人对网络和主机的进行恶意代码检测并保存检测记录；

d） 应对防恶意代码软件的授权使用、恶意代码库升级、定期汇报等作出明确管理规定。

6.2.5.8.2 测试方法

访谈，检查。

6.2.5.8.3 测试对象

系统运维负责人，恶意代码防范管理文档，恶意代码检测记录。

6.2.5.8.4 测评实施

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，如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；

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，并保存记录；

c） 应检查恶意代码防范管理文档，查看其内容是否对防恶意代码软件的授权使用、恶意代码库升级、定期汇报等方面作出规定；

d） 应检查是否具有恶意代码检测记录。

6.2.5.8.5 结果判定

a） 6.2.5.8.4 a）—d）均为肯定，则信息系统符合本单元测评项要求。

6.2.5.9 密码管理

6.2.5.9.1 测评项

a） 密码算法和密钥的使用应符合国家密码管理规定。

6.2.5.9.2 测试方法

访谈。

6.2.5.9.3 测试对象

安全员。

6.2.5.9.4 测评实施

a） 应访谈安全员，询问密码算法和密钥的使用是否遵照国家密码管理规定。

6.2.5.9.5 结果判定

a） 6.2.5.9.4 a）为肯定，则信息系统符合本单元测评项要求。

6.2.5.10 变更管理

6.2.5.10.1 测评项

a） 应确认系统中将发生的变更，并制定变更方案；

b） 建立变更管理制度，重要系统变更前，应向主管领导申请，审批后方可实施变更；

c） 系统变更情况应向所有相关人员通告。

6.2.5.10.2 测试方法

访谈，检查。

6.2.5.10.3 测试对象

系统运维负责人，变更方案，变更管理制度，系统变更申请书。

6.2.5.10.4 测评实施

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，变更是否要求制度化管理；

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，查看其是否对变更类型、变更原因、变更过程、变更前评估等方面进行说明；

d） 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；

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。

6.2.5.10.5 结果判定

a） 6.2.5.10.4 a）—e）均为肯定，则信息系统符合本单元测评项要求。

6.2.5.11 备份与恢复管理

6.2.5.11.1 测评项

a） 应识别需要定期备份的重要业务信息、系统数据及软件系统等；

b） 应规定备份信息的备份方式（如增量备份或全备份等）、备份频度（如每日或每周等）、存储介质、保存期等；

c） 应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略，备份策略应指明备份数据的放置场所、文件命名规则、介质替换频率和将数据离站运输的方法；

d） 应指定相应的负责人定期维护和检查备份及冗余设备的状况，确保需要接入系统时能够正常运行；

e） 根据备份方式，规定备份及冗余设备的安装、配置和启动的流程。

6.2.5.11.2 测试方法

访谈，检查。

6.2.5.11.3 测试对象

系统管理员，数据库管理员，网络管理员，备份管理文档，备份和恢复策略文档，备份设备操作流程文档。

6.2.5.11.4 测评实施

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；对其的备份工作是否以文档形式规

范了备份方式、频度、介质、保存期等内容，数据备份和恢复策略是否文档化；

b） 应访谈系统管理员、数据库管理员和网络管理员，询问其对备份和冗余设备的安装、配置和启动工作是否根据一定的流程进行，是否指定专人对备份和冗余设备的有效性定期维护和检查，多长时间检查一次；

c） 应检查是否具有规定备份方式、频度、介质、保存期的文档；

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） 应检查备份设备操作流程文档，查看其是否规定备份和冗余设备的安装、配置、启动、关闭等操作流程。

6.2.5.11.5 结果判定

a） 6.2.5.11.4 a）－e）均为肯定，则信息系统符合本单元测评项要求。

6.2.5.12 安全事件处置

6.2.5.12.1 测评项

a） 所有用户均有责任报告自己发现的安全弱点和可疑事件，但任何情况下用户均不应尝试验证弱点；

b） 应制定安全事件报告和处置管理制度，规定安全事件的现场处理、事件报告和后期恢复的管理职责；

c） 应分析信息系统的类型、网络连接特点和信息系统用户特点，了解本系统和同类系统已发生的安全事件，识别本系统需要防止发生的安全事件，事件可能来自攻击、错误、故障、事故或灾难；

d） 应根据国家相关管理部门对计算机安全事件等级划分方法，根据安全事件在本系统产生的影响，将本系统计算机安全事件进行等级划分；

e） 应记录并保存所有报告的安全弱点和可疑事件，分析事件原因，监督事态发展，采取措施避免安全事件发生。

6.2.5.12.2 测试方法

访谈，检查。

6.2.5.12.3 测试对象

系统运维负责人，安全事件报告和处置管理制度，安全事件定级文档，安全事件记录分析文档。

6.2.5.12.4 测评实施

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，是否对所报告的安全事件进行记录并保存；

b） 应访谈系统运维负责人，询问是否对安全事件处置进行制度化管理；

c） 应访谈系统运维负责人，询问本系统已发生的和需要防止发生的安全事件主要有哪几类，对识别出的安全事件是否根据其对系统的影响程度划分不同等级，划分为几级；

d） 应检查安全事件报告和处置管理制度，查看其内容是否明确与安全事件有关的工作职责，包括报告单位（人）、接报单位（人）和处置单位等职责；

e） 应检查安全事件定级文档，查看其内容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；

f） 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。

6.2.5.12.5 结果判定

a） 6.2.5.12.4 a）－f）为肯定，则信息系统符合本单元测评项要求。

6.2.5.13 应急预案管理

6.2.5.13.1 测评项

a) 应在统一的应急预案框架下制定不同事件的应急预案，应急预案框架应包括启动预案的条件、应急处理流程、系统恢复流程和事后教育和培训等内容；

b) 应对系统相关的人员进行培训使之了解如何及何时使用应急预案中的控制手段及恢复策略，对应急预案的培训至少每年举办一次。

6.2.5.13.2 测试方法

访谈，检查。

6.2.5.13.3 测试对象

系统运维负责人，应急响应预案文档。

6.2.5.13.4 测评实施

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，培训内容是什么，多长时间举办一次；

b) 应检查应急响预案文档，查看其内容是否覆盖启动预案的条件、应急处理流程、系统恢复流程和事后教育等内容。

6.2.5.13.5 结果判定

a) 6.2.5.13.4 a）—b）均为肯定，则信息系统符合本单元测评项要求。

7 第三级安全控制测评

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 测评项

a) 机房和办公场地应选择在具有防震、防风和防雨等能力的建筑内；

b) 机房场地应避免设在建筑物的高层或地下室，以及用水设备的下层或隔壁；

c) 机房场地应当避开强电场、强磁场、强震动源、强噪声源、重度环境污染、易发生火灾、水灾、易遭受雷击的地区。

7.1.1.1.2 测评方式

访谈，检查。

7.1.1.1.3 测评对象

物理安全负责人，机房维护人员，机房，办公场地，机房场地设计/验收文档

7.1.1.1.4 测评实施

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；

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/验收文档，查看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；查看是否有机房场地的选址说明；查看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避免在建筑物的高层或地下室，以及用水设备的下层或隔壁；

f) 应检查机房场地是否避免设在强电场、强磁场、强震动源、强噪声源、重度环境污染、易发生火灾、水灾、易遭受雷击的地区；

g） 如果机房和办公场地的显示器、打印机等设备有敏感或密级信息输出，应检查设备摆放位置是否为不易被无关人员看到的隐蔽位置。

7.1.1.1.5 结果判定

a） 如果7.1.1.1.4 a）中机房场地的选址符合不在建筑物的高层或地下室，以及用水设备的下层或隔壁；不在强电场、强磁场、强震动源、强噪声源、重度环境污染、易发生火灾、水灾、易遭受雷击的地区等要求，则该项为肯定；

b） 如果7.1.1.1.4 g）中“如果”条件不成立，则该项为不适用；

c） 7.1.1.1.4 a）-g）均为肯定，则信息系统符合本单元测评项要求。

7.1.1.2 物理访问控制

7.1.1.2.1 测评项

a） 机房出入口应有专人值守，鉴别进入的人员身份并登记在案；

b） 应批准进入机房的来访人员，限制和监控其活动范围；

c） 应对机房划分区域进行管理，区域和区域之间设置物理隔离装置，在重要区域前设置交付或安装等过度区域；

d） 应对重要区域配置电子门禁系统，鉴别和记录进入的人员身份并监控其活动。

7.1.1.2.2 测评方式

访谈，检查。

7.1.1.2.3 测评对象

物理安全负责人，机房值守人员，机房设施（电子门禁系统），机房安全管理制度，值守记录，进入机房的登记记录，来访人员进入机房的审批记录，电子门禁系统记录。

7.1.1.2.4 测评实施

a） 应访谈物理安全负责人，了解具有哪些控制机房进出的能力；

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制度，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；检查机房是否存在电子门禁系统控制之外的出入口；

f） 应检查机房是否有进入机房的人员身份鉴别措施，如戴有可见的身份辨识标识；

g） 应检查是否有来访人员进入机房的审批记录；

h） 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；是否对不同区域设置不同机房或者同一机房的不同区域之间设置有效的物理隔离装置（如隔墙等）；

i） 应检查机房或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资质；

j） 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）；查看电子门禁系统运行、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的人员身份。

7.1.1.2.5 结果判定

a） 如果有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，机房或重要区域配置了电子门禁系统，则7.1.1.2.4 a）为肯定；

b) 如果7.1.1.2.4 b）认为没有必要对机房进行划分区域管理（如果安全管理需要，计算机设备宜采用分区布置，如可分为主机区、存贮器区、数据输入区、数据输出区、通信区和监控调度区等），则测评实施h）不适用；

c) 如果有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，电子门禁系统管理，则7.1.1.2.4 d）为肯定；

d) 7.1.1.2.4 a）- j）均为肯定，则信息系统符合本单元测评项要求。

7.1.1.3 防盗窃和防破坏

a) 应将主要设备放置在物理受限的范围内；

b) 应对设备或主要部件进行固定，并设置明显的无法除去的标记；

c) 应将通信线缆铺设在隐蔽处，如铺设在地下或管道中等；

d) 应对介质分类标识，存储在介质库或档案室中；

e) 设备或存储介质携带出工作环境时，应受到监控和内容加密；

f) 应利用光、电等技术设置机房的防盗报警系统，以防进入机房的盗窃和破坏行为；

g) 应对机房设置监控报警系统。

7.1.1.3.1 测评项

7.1.1.3.2 测评方式

访谈，检查。

7.1.1.3.3 测评对象

物理安全负责人，机房维护人员，资产管理员，机房设施，设备管理制度文档，通信线路布线文档，防盗报警系统和监控报警系统的安装测试/验收报告。

7.1.1.3.4 测评实施

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；是否设置了冗余或并行的通信线路；是否对机房安装的防盗报警系统和监控报警系统进行定期维护检查

c) 应访谈资产管理员，在介质管理中，是否进行了分类标识，是否存放在介质库或档案室中；询问对设备或存储介质携带出工作环境是否规定了审批程序、内容加密、专人检查等安全保护的措施；

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，是否不易被移动或被搬走，是否设置明显的无法除去的标记；

e) 应检查通信线缆铺设是否在隐蔽处（如铺设在地下或管道中等）；

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），红外报警等措施；

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

h) 应检查有关设备或存储介质携带出工作环境的审批记录，以及专人对内容加密进行检查的记录；

i) 应检查是否有设备管理制度文档，通信线路布线文档，介质管理制度文档，介质清单和使用记录，机房防盗报警设施的安全资质材料、安装测试/验收报告；查看文档中的条文是否与设备放置位置、设备或主要部件保护、通信线缆铺设等实际情况一致。

7.1.1.3.5 结果判定

a) 如果有设备管理制度，主要设备放置位置做到安全可控,设备或主要部件进行了固定和标记，通信线缆铺设在隐蔽处，介质分类标识并存储在介质库或档案室，机房安装了防止进入盗窃和破坏的利用光、电等技术设置的机房防盗报警系统；设备或存储介质携带出工作环境的审批程序、内容加密、专人检查等措施；机房设置了摄像、传感等监控报警系统，则7.1.1.3.4 a）为肯定；

b) 7.1.1.3.4 a）-i）均为肯定，则信息系统符合本单元测评项要求。

7.1.1.4 防雷击

7.1.1.4.1 测评项

a) 机房建筑应设置避雷装置；

b) 应设置防雷保安器，防止感应雷；

c) 应设置交流电源地线。

7.1.1.4.2 测评方式

访谈，检查。

7.1.1.4.3 测评对象

物理安全负责人，机房维护人员，机房设施，建筑防雷设计/验收文档。

7.1.1.4.4 测评实施

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增加有资质的避雷装置，以避免感应雷击；

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；询问机房计算机系统接地（交流工作接地、安全保护接地）是否符合GB50174－93《电子计算机机房设计规范》的要求；

c) 应检查机房是否有建筑防雷设计/验收文档，机房接地设计/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增加有资质的避雷装置,以避免感应雷击。

7.1.1.4.5 结果判定

a) 如果计算机机房防雷符合GB 50057－1994《建筑物防雷设计规范》（GB157《建筑防雷设计规范》）要求，而且如果是在雷电频繁区域，装设浪涌电压吸收装置等，则7.1.1.4.4 a）为肯定；

b) 如果地线的引线和大楼的钢筋网及各种金属管道绝缘,交流工作接地的接地电阻不大于4Ω，安全保护地的接地电阻不大于4Ω；防雷保护地（处在有防雷设施的建筑群中可不设此地）的接地电阻不大于10Ω的要求，则7.1.1.4.4 b）为肯定；

c) 7.1.1.4.4 a）-d）均为肯定，则信息系统符合本单元测评项要求。

7.1.1.5 防火

7.1.1.5.1 测评项

a) 应设置火灾自动消防系统，自动检测火情、自动报警，并自动灭火；

b) 机房及相关的工作房间和辅助房，其建筑材料应具有耐火等级；

c) 机房采取区域隔离防火措施，将重要设备与其他设备隔离开。

7.1.1.5.2 测评方式

访谈，检查

7.1.1.5.3 测评对象

物理安全负责人，机房值守人员，机房设施，机房安全管理制度，机房防火设计/验收

文档，自动消防系统设计/验收文档。

7.1.1.5.4 测评实施

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，是否制订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（喷水不适用于机房）；

c) 应检查机房是否设置了自动检测火情（如使用温感、烟感探测器）、自动报警、自动灭火的自动消防系统，摆放位置是否合理，有效期是否合格；应检查自动消防系统是否正常工作，查看运行记录、报警记录、定期检查和维修记录；

d) 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/验收文档；检查是否有机房自动消防系统的设计/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；

e) 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。

7.1.1.5.5 结果判定

a) 7.1.1.5.4 a）-e）均为肯定，则信息系统符合本单元测评项要求。

7.1.1.6 防水和防潮

7.1.1.6.1 测评项

a) 水管安装，不得穿过屋顶和活动地板下；

b) 应对穿过墙壁和楼板的水管增加必要的保护措施，如设置套管；

c) 应采取措施防止雨水通过屋顶和墙壁渗透；

d) 应采取措施防止室内水蒸气结露和地下积水的转移与渗透。

7.1.1.6.2 测评方式

访谈，检查。

7.1.1.6.3 测评对象

物理安全负责人，机房维护人员，机房设施，建筑防水和防潮设计/验收文档，机房湿度记录，除湿装置运行记录。

7.1.1.6.4 测评实施

a) 应访谈物理安全负责人，询问机房建设是否有防水防潮措施；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，如设置套管；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，是否经常检查是否有漏水情况；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采取防范措施；

c) 应检查机房是否有建筑防水和防潮设计/验收文档，是否与机房防水防潮的实际情况一致；

d) 如果有管道穿过主机房墙壁和楼板处，应检查是否有必要的保护措施，如设置套管等；

e) 应检查机房是否不存在屋顶和墙壁等出现过漏水、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；

f) 如果在湿度较高地区或季节，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，与机房湿度记录情况是否一致。

7.1.1.6.5 结果判定

a) 如果7.1.1.6.4 d），f）中“如果”条件不成立，则该项为不适用；

b) 7.1.1.6.4 a）-f）均为肯定，则信息系统符合本单元测评项要求。

7.1.1.7 防静电

7.1.1.7.1 测评项

a) 应采用必要的接地等防静电措施；

b) 应采用防静电地板。

7.1.1.7.2 测评方式

访谈，检查。

7.1.1.7.3 测评对象

物理安全负责人，机房维护人员，机房设施，防静电设计/验收文档，湿度记录。

7.1.1.7.4 测评实施

a) 应访谈物理安全负责人，询问机房是否采用必要的接地等防静电措施，是否有控制机房湿度的措施；在静电较强地区的机房是否采取了有效的防静电措施；

b) 应访谈机房维护人员，询问是否经常检查机房湿度，并控制在GB2887中的规定的范围内；询问机房是否存在静电问题或因静电引起的故障事件；如果存在静电时是否及时采取消除静电的措施；

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

d) 应检查机房是否有安全接地，查看机房的相对湿度的记录是否符合GB2887中的规定，查看机房是否不存在明显的静电现象；

e) 如果在静电较强的地区，应检查机房是否了采用了如防静电地板、防静电工作台、以及静电消除剂和静电消除器等措施。

7.1.1.7.5 结果判定

a) 7.1.1.7.4 e）中有效的防静电措施，可以包括如防静电地板、防静电工作台，或静电消除剂和静电消除器等措施的部分或全部，则该项为肯定；

b) 如果7.1.1.7.4 e）中“如果”条件不成立，则该项为不适用；

c) 7.1.1.7.4 a）-e）均为肯定，则信息系统符合本单元测评项要求。

7.1.1.8 温湿度控制

7.1.1.8.1 测评项

a) 应设置恒温恒湿系统，使机房温、湿度的变化在设备运行所允许的范围之内。

7.1.1.8.2 测评方式

访谈，检查。

7.1.1.8.3 测评对象

物理安全负责人，机房维护人员，机房设施，温湿度控制设计/验收文档，温湿度记录、运行记录和维护记录。

7.1.1.8.4 测评实施

a) 应访谈物理安全负责人，询问机房是否配备了恒温恒湿系统，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；

b) 应访谈机房维护人员，询问是否定期检查和维护机房的温湿度自动调节设施，询问是否出现过温湿度影响系统运行的事件；

c） 应检查机房是否有温湿度控制设计/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合；

d） 应检查恒温恒湿系统是否能够正常运行，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GB 2887-89《计算站场地技术条件》的要求。

7.1.1.8.5 结果判定

a） 7.1.1.8.4 a）-d）均为肯定，则信息系统符合本单元测评项要求。

7.1.1.9 电力供应

7.1.1.9.1 测评项

a） 计算机系统供电应与其他供电分开；

b） 应设置稳压器和过电压防护设备；

c） 应提供短期的备用电力供应（如UPS设备）；

d） 应设置冗余或并行的电力电缆线路；

e） 应建立备用供电系统（如备用发电机），以备常用供电系统停电时启用。

7.1.1.9.2 测评方式

访谈，检查，测试。

7.1.1.9.3 测评对象

物理安全负责人，机房维护人员，机房设施，电力供应安全设计/验收文档，检查和维护记录。

7.1.1.9.4 测评实施

a） 应访谈物理安全负责人，询问计算机系统供电线路是否与其他供电分开；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（如UPS），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（如双路供电方式）；是否建立备用供电系统（如备用发电机）；

b） 应访谈机房维护人员，询问是对在计算机系统供电线路上的稳压器、过电压防护设备、短期备用电源设备等进行定期检查和维护；是否能够控制电源稳压范围满足计算机系统运行正常；

c） 应访谈机房维护人员，询问冗余或并行的电力电缆线路（如双路供电方式）在双路供电切换时是否能够对计算机系统正常供电；是否定期检查备用供电系统（如备用发电机），是否能够在规定时间内正常启动和正常供电；

d） 应检查机房是否有电力供应安全设计/验收文档，查看文档中是否标明单独为计算机系统供电，配备稳压器、过电压防护设备、备用电源设备以及冗余或并行的电力电缆线路等要求；查看与机房电力供应实际情况是否一致；

e） 应检查计算机供电线路，查看计算机系统供电是否与其他供电分开；

f） 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；

g） 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电源设备的检查和维护记录，以及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；

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

i） 应测试备用供电系统(如备用发电机)是否能够在规定时间内正常启动和正常供电。

7.1.1.9.5 结果判定

a） 7.1.1.9.4 a）-i）均为肯定，则信息系统符合本单元测评项要求。

7.1.1.10 电磁防护

7.1.1.10.1 测评项

a) 应采用接地方式防止外界电磁干扰和设备寄生耦合干扰；

b) 电源线和通信线缆应隔离，避免互相干扰；

c) 对重要设备和磁介质实施电磁屏蔽。

7.1.1.10.2 测评方式

访谈，检查。

7.1.1.10.3 测评对象

物理安全负责人，机房维护人员，机房设施，电磁防护设计/验收文档。

7.1.1.10.4 测评实施

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采取了防止电磁泄露的措施；

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，是否安装了满足BMB4-2000《电磁干扰器技术要求和测试方法》要求的二级电磁干扰器；

c) 应检查机房是否有电磁防护设计/验收文档，查看其描述内容与实际情况是否一致；

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) 应检查使用电磁干扰器的涉密设备开机，是否同时开启电磁干扰器。

7.1.1.10.5 结果判定

a) 7.1.1.10.4 a）-f）均为肯定，则信息系统符合本单元测评项要求。

7.1.2 网络安全

7.1.2.1 结构安全与网段划分

7.1.2.1.1 测评项

a) 网络设备的业务处理能力应具备冗余空间，要求满足业务高峰期需要；

b) 应设计和绘制与当前运行情况相符的网络拓扑结构图；

c) 应根据机构业务的特点，在满足业务高峰期需要的基础上，合理设计网络带宽；

d) 应在业务终端与业务服务器之间进行路由控制建立安全的访问路径；

e) 应根据各部门的工作职能、重要性、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、网段分配地址段；

f) 重要网段应采取网络层地址与数据链路层地址绑定措施，防止地址欺骗；

g) 应按照对业务服务的重要次序来指定带宽分配优先级别，保证在网络发生拥堵的时候优先保护重要业务数据主机。

7.1.2.1.2 测评方式

访谈，检查，测试。

7.1.2.1.3 测评对象

网络管理员，边界和主要网络设备，网络拓扑结构，网络拓扑图，网络设计/验收文档。

7.1.2.1.4 测评实施

a) 可访谈网络管理员，询问信息系统中的边界和主要网络设备的性能以及目前业务高峰流量情况；

b) 可访谈网络管理员，询问网段划分情况以及划分的原则；询问重要的网段有哪些，对重要网段的保护措施有哪些；

c) 可访谈网络管理员，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) 可访谈网络管理员，询问网络设备上的路由控制策略措施有哪些，这些策略设计的目的是什么；
e) 应检查网络拓扑图，查看其与当前运行情况是否一致；
f) 应检查网络设计/验收文档，查看是否有边界和主要网络设备能满足基本业务需求，网络接入及核心网络的带宽能满足业务高峰期的需要，是否不存在带宽瓶颈等方面的设计或描述；
g) 应检查网络设计/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（如使用静态路由等）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网络地址与数据链路地址绑定的措施（如对重要服务器采用IP地址和MAC地址绑定措施）；
j) 应检查边界和主要网络设备，查看是否有对带宽进行控制的策略（如路由、交换设备上的QOS策略配置情况，专用的带宽管理设备的配置策略等），这些策略能否保证在网络发生拥堵的时候优先保护重要业务（如重要业务的主机的优先级要高于非重要业务的主机）；
k） 应测试网络拓扑结构，可通过网络拓扑结构自动发现、绘制工具，验证实际的网络拓扑结构和网络拓扑结构图是否一致；
l) 应测试业务终端与业务服务器之间的访问路径，可通过使用路由跟踪工具（如tracert等工具），验证业务终端与业务服务器之间的访问路径是否安全（如访问路径是否固定等）；
m) 应测试重要网段，验证其采取的网络地址与数据链路地址绑定措施是否有效（如试图使用非绑定地址，查看是否能正常访问等）；
n) 应测试网络带宽分配策略，可通过使用带宽测试工具，测试网络带宽分配是否有效。

7.1.2.1.5 结果判定

a) 如果 7. 1. 2. 1. 4 f）-g）中缺少相应的文档，则该项为否定；
b) 7. 1. 2. 1. 4 e）-n）均为肯定，则信息系统符合本单元测评项要求。

7.1.2.2 网络访问控制

7.1.2.2.1 测评项

a） 应能根据会话状态信息（包括数据包的源地址、目的地址、源端口号、目的端口号、协议、出入的接口、会话序列号、发出信息的主机名等信息，并应支持地址通配符的使用），为数据流提供明确的允许/拒绝访问的能力；
b） 应对进出网络的信息内容进行过滤，实现对应用层HTTP、FTP、TELNET、SMTP、POP3等协议命令级的控制；
c） 应依据安全策略允许或者拒绝便携式和移动式设备的网络接入；
d） 应在会话处于非活跃一定时间或会话结束后终止网络连接；
e） 应限制网络最大流量数及网络连接数。

7.1.2.2.2 测评方式

访谈，检查，测试。

7.1.2.2.3 测评对象

安全员，边界网络设备（包括网络安全设备）。

7.1.2.2.4 测评实施

a) 可访谈安全员，询问采取的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；

b) 应检查边界网络设备，查看其是否根据会话状态信息（如包括数据包的源地址、目的地址、源端口号、目的端口号、协议、出入的接口、会话序列号、发出信息的主机名等信息，并应支持地址通配符的使用）对数据流进行控制；

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，查看是否能设置会话处于非活跃的时间或会话结束后自动终止网络连接；查看是否能设置网络最大流量数及网络连接数；

e) 应检查主要网络设备，查看是否有访问控制措施（如 VLAN，访问控制列表，MAC 地址绑定）控制便携式和移动式设备接入网络；

f) 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（如可以使用扫描工具来探测等）；

g) 应测试主要网络设备，可通过试图用移动设备接入网络，验证网络设备的访问控制策略是否有效；

h) 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（如 http 隧道等），验证网络访问控制措施是否不存在明显的弱点。

7.1.2.2.5 结果判定

a) 7.1.2.2.4 b）-g）均为肯定，则信息系统符合本单元测评项要求；

7.1.2.3 拨号访问控制

7.1.2.3.1 测评项

a) 应在基于安全属性的允许远程用户对系统访问的规则的基础上，对系统所有资源允许或拒绝用户进行访问，控制粒度为单个用户；

b) 应限制具有拨号访问权限的用户数量；

c) 应按用户和系统之间的允许访问规则，决定允许用户对受控系统进行资源访问。

7.1.2.3.2 测评方式

访谈，检查，测试。

7.1.2.3.3 测评对象

安全员，边界网络设备（包括网络安全设备）。

7.1.2.3.4 测评实施

a) 可访谈安全员，询问是否允许拨号访问网络；询问对拨号访问控制的策略是什么，采取什么技术手段实现拨号访问控制（如使用防火墙还是使用路由器实现），采取的拨号访问用户的权限分配原则是什么；询问对保护访问的认证方式有哪些；

b) 应检查边界网络设备（如路由器，防火墙，认证网关），查看是否正确的配置了拨号访问控制列表（对系统资源实现允许或拒绝访问），控制粒度是否为单个用户；查看其能否限制拨号访问权限的用户数量；

c) 应测试边界网络设备，可通过试图非授权的访问，验证拨号访问措施能否有效对系统资源实现允许或拒绝用户访问的控制；

d) 应测试边界网络设备，可使用测试拨号连接数工具，验证其限制具有拨号访问权限的用户数量的功能是否有效。

7.1.2.3.5 结果判定

a) 7.1.2.3.4 b）-d）为肯定，则信息系统符合本单元测评项要求。

7.1.2.4 网络安全审计

7.1.2.4.1 测评项

a) 应对网络系统中的网络设备运行状况、网络流量、用户行为等进行全面的监测、记录；

b) 对于每一个事件，其审计记录应包括：事件的日期和时间、用户、事件类型、事件是否成功，及其他与审计相关的信息；

c) 安全审计应可以根据记录数据进行分析，并生成审计报表；

d) 安全审计应可以对特定事件，提供指定方式的实时报警；

e) 审计记录应受到保护避免受到未预期的删除、修改或覆盖等。

7.1.2.4.2 测评方式

访谈，检查，测试。

7.1.2.4.3 测评对象

审计员，边界和主要网络设备。

7.1.2.4.4 测评实施

a) 可访谈审计员，询问网络系统中的边界和关键网络设备是否设置安全审计，包括哪些项；询问审计记录的主要内容有哪些；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，查看审计记录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，查看是否可以对特定事件，按照指定方式进行实时报警（如声音、EMAIL、短信等）；

e) 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（如对审计记录进行分类、排序、查询、统计、分析和组合查询等），并能根据需要生成审计报表；

f) 应测试边界和主要网络设备，可通过以某个用户试图产生一些重要的安全相关事件（如鉴别失败等），验证安全审计的覆盖情况和记录情况与要求是否一致；

g) 应测试边界和主要网络设备，可通过以某个系统用户试图删除、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。

7.1.2.4.5 结果判定

a) 7.1.2.4.4 b）-g）均为肯定，则信息系统符合本单元测评项要求。

7.1.2.5 边界完整性检查

7.1.2.5.1 测评项

a) 应能够检测内部网络中出现的内部用户未通过准许私自联到外部网络的行为（即“非法外联”行为）；

b) 应能够对非授权设备私自联到网络的行为进行检查，并准确定出位置，对其进行有效阻断；

c) 应能够对内部网络用户私自联到外部网络的行为进行检测后准确定出位置，并对其进行有效阻断。

7.1.2.5.2 测评方式

访谈，检查，测试。

7.1.2.5.3 测评对象

安全员，边界完整性检查设备，边界完整性检查设备运行日志。

7.1.2.5.4 测评实施

a) 可访谈安全员，询问是否有对内部用户未通过准许私自联到外部网络的行为、对非授权设备私自联到网络的行为进行监控的措施，具体采取什么措施；询问网络内“非法外联”的情况；

b) 应检查边界完整性检查设备运行日志，查看运行是否正常（查看是否持续对网络进行监控）；

c) 应检查边界完整性检查设备，查看是否设置了同时对非法联接到内网和非法联接到外网的行为进行监控；查看是否对发现的非法联接行为进行有效的阻断；

d) 应测试边界完整性检查设备，测试是否能有效的发现“非法外联”的行为（如产生非法外联的动作，查看边界完整性检查设备是否能够发现该行为）；

e) 应测试边界完整性检查设备，测试是否确定出“非法外联”设备的位置，并对其进行有效阻断（如产生非法外联的动作，查看边界完整性检查设备是否能够准确定位并阻断）；

f) 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联到网络的行为进行检查，并准确定出位置，对其进行有效阻断（如产生非法接入的动作，查看测试边界完整性检查设备是否能准确的发现，准确的定位并产生阻断）。

7.1.2.5.5 结果判定

a) 7.1.2.5.4 b）-f）均为肯定，则信息系统符合本单元测评项要求。

7.1.2.6 网络入侵防范

7.1.2.6.1 测评项

a) 应在网络边界处应监视以下攻击行为：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、网络蠕虫攻击等入侵事件的发生；

b) 当检测到入侵事件时，应记录入侵的源IP、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时提供报警。

7.1.2.6.2 测评方式

访谈，检查，测试。

7.1.2.6.3 测评对象

安全员，网络入侵防范设备。

7.1.2.6.4 测评实施

a) 可访谈安全员，询问网络入侵防范措施有哪些；是否有专门的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，查看其生产厂商是否为正规厂商，规则库是否为最新；

e) 应测试网络入侵防范设备，验证其监控策略是否有效（如模拟产生攻击动作，查看网络入侵防范设备的反应）；

f) 应测试网络入侵防范设备，验证其报警策略是否有效（如模拟产生攻击动作，查看网络入侵防范设备是否能实时报警）。

7.1.2.6.5 结果判定

a) 7.1.2.6.4 b）-f）均为肯定，则信息系统符合本单元测评项要求。

7.1.2.7 恶意代码防范

7.1.2.7.1 测评项

a) 应在网络边界及核心业务网段处对恶意代码进行检测和清除；
b) 应维护恶意代码库的升级和检测系统的更新；
c) 应支持恶意代码防范的统一管理。

7.1.2.7.2 测评方式

访谈，检查。

7.1.2.7.3 测评对象

安全员，防恶意代码产品，设计/验收文档，恶意代码产品运行日志。

7.1.2.7.4 测评实施

a) 可访谈安全员，询问系统中的网络防恶意代码防范措施是什么；询问恶意代码库的更新策略；询问防恶意代码产品的有哪些主要功能；询问系统是否发生过针对恶意代码入侵的安全事件；
b) 应检查设计/验收文档，查看其是否有在网络边界及核心业务网段处有对恶意代码采取相关措施（如是否有防病毒网关），防恶意代码产品是否有实时更新的功能的描述；
c) 应检查恶意代码产品运行日志，查看是否持续运行；
d) 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的措施；
e) 应检查防恶意代码产品，查看是否为正规厂商生产，运行是否正常，恶意代码库是否为最新版本；
f) 应检查防恶意代码产品的配置策略，查看是否支持恶意代码防范的统一管理（如查看是否为分布式部署，集中管理等）。

7.1.2.7.5 结果判定

a) 如果7.1.2.7.4 b）中缺少相应的文档，则该项为否定；
b) 7.1.2.7.4 b）-f）均为肯定，则信息系统符合本单元测评项要求。

7.1.2.8 网络设备防护

7.1.2.8.1 测评项

a) 应对登录网络设备的用户进行身份鉴别；
b) 应对网络上的对等实体进行身份鉴别；
c) 应对网络设备的管理员登录地址进行限制；
d) 网络设备用户的标识应唯一；
e) 身份鉴别信息应具有不易被冒用的特点，例如口令长度、复杂性和定期的更新等；
f) 应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；
g) 应具有登录失败处理功能，如结束会话、限制非法登录次数，当网络登录连接超时，自动退出；
h) 应实现设备特权用户的权限分离，例如将管理与审计的权限分配给不同的网络设备用户。

7.1.2.8.2 测评方式

访谈，检查，测试。

7.1.2.8.3 测评对象

网络管理员，边界和主要网络设备。

7.1.2.8.4 测评实施

a) 可访谈网络管理员，询问对关键网络设备的防护措施有哪些；询问对关键网络设备的登录和验证方式做过何种特定配置；

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上的安全设置，查看其是否有对鉴别失败采取相应的措施的设置；查看是否有限制非法登录次数的功能；

d） 应检查边界和主要网络设备上的安全设置，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；查看是否对网络上的对等实体进行身份鉴别；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（如同时使用口令和地址绑定等）；

e） 应测试边界和主要网络设备的安全设置，验证鉴别失败处理措施（如模拟失败登录，观察网络设备的动作等），限制非法登录次数（如模拟非法登录，观察网络设备的动作等），对网络设备的管理员登录地址进行限制（如使用任意地址登录，观察网络设备的动作等）等功能是否有效；

f） 应测试边界和主要网络设备的安全设置，验证其网络登录连接超自动退出的设置是否有效（如长时间连接无任何操作，观察观察网络设备的动作等）；

g） 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（如口令猜解等）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。

7.1.2.8.5 结果判定

a） 如网络设备的口令策略为口令长度8位以上，口令复杂（如规定字符应混有大、小写字母、数字和特殊字符），口令生命周期，新旧口令的替换要求（规定替换的字符数量）或为了便于记忆使用了令牌；则7.1.2.8.4 b）满足测评要求；

b） 7.1.2.8.4 b）-g）均为肯定，则信息系统符合本单元测评项要求。

7.1.3 主机系统安全

7.1.3.1 身份鉴别

7.1.3.1.1 测评项

a） 操作系统和数据库系统用户的身份标识应具有唯一性；

b） 应对登录操作系统和数据库系统的用户进行身份标识和鉴别；

c） 应对同一用户采用两种或两种以上组合的鉴别技术实现用户身份鉴别；

d） 操作系统和数据库系统用户的身份鉴别信息应具有不易被冒用的特点，例如口令长度、复杂性和定期更新等；

e） 应具有登录失败处理功能，如结束会话、限制非法登录次数，当登录连接超时，自动退出；

f） 应具有鉴别警示功能；

g） 重要的主机系统应对与之相连的服务器或终端设备进行身份标识和鉴别。

7.1.3.1.2 测评方式

访谈，检查，测试。

7.1.3.1.3 测评对象

系统管理员，数据库管理员，主要服务器操作系统，主要数据库系统，服务器操作系统文档，数据库系统文档。

7.1.3.1.4 测评实施

a） 应检查服务器操作系统和数据库系统身份鉴别功能是否具有《信息安全等级保护操作系统安全技术要求》和《信息安全等级保护数据库管理系统安全技术要求》第二级以上或TCSEC C2级以上的测试报告；

b） 可访谈系统管理员，询问操作系统的身份标识与鉴别机制采取何种措施实现，目前系统提供了哪些身份鉴别措施和鉴别失败处理措施；

c） 可访谈数据库管理员，询问数据库的身份标识与鉴别机制采取何种措施实现，目前系统提供了哪些身份鉴别措施和鉴别失败处理措施；

d） 应检查服务器操作系统文档和数据库系统文档，查看用户身份标识的唯一性是由什么属性来保证的（如用户名或者 UID 等）；

e） 应检查主要服务器操作系统和主要数据库系统，查看是否提供了身份鉴别措施（如用户名和口令等），其身份鉴别信息是否具有不易被冒用的特点，例如，口令足够长，口令复杂（如规定字符应混有大、小写字母、数字和特殊字符），口令生命周期，新旧口令的替换要求（如规定替换的字符数量）或为了便于记忆使用了令牌；

f） 应检查主要服务器操作系统和主要数据库系统，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（如采用用户名/口令、挑战应答、动态口令、物理设备、生物识别技术和数字证书方式的身份鉴别技术中的任意两个组合）；

g） 应检查主要服务器操作系统和主要数据库系统，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，对超过限制值的登录终止其鉴别会话或临时封闭帐号；查看是否设置网络登录连接超时，并自动退出；查看是否设置鉴别警示信息；

h） 应检查主要服务器操作系统，查看服务器操作系统是否对与之相连的服务器或终端设备进行身份标识和鉴别；

i） 应测试主要服务器操作系统和主要数据库系统，可通过错误的用户名和口令试图登录系统，验证鉴别失败处理功能是否有效；

j) 应测试主要服务器操作系统和主要数据库系统，当进入系统时，是否先需要进行标识（如建立账号），而没有进行标识的用户不能进入系统；

k） 应测试主要服务器操作系统和主要数据库系统，添加一个新用户，其用户标识为系统原用户的标识（如用户名或 UID），查看是否不会成功；

l） 应测试主要服务器操作系统和主要数据库系统，删除一个用户标识，然后再添加一个新用户，其用户标识和所删除的用户标识一样（如用户名/UID），查看是否不能成功；

m） 应测试主要服务器操作系统，可通过使用未进行身份标识和鉴别的主机连接该服务器，验证主机系统能否正确地对与之相连的服务器或终端设备进行身份标识和鉴别；

n） 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，查看能否破解用户口令，破解口令后能否登录进入系统；

o） 应渗透测试主要服务器操作系统，验证已存在的账号（如安装一些服务后会系统会增加新应的账号）是否不能与系统进行交互式登录管理；

p） 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，例如，认证程序存在的 BUG，社会工程或其他手段等。

7.1.3.1.5 结果判定

a） 如果7.1.3.1.4 a）为肯定，则测评实施j）、k）和l）为肯定；

b） 如果不采用用户名/口令方式的进行身份鉴别，则7.1.3.1.4 n）不适用；

c） 如果7.1.3.1.4 o）中能破解口令，则该项为否定；

d） 如果7.1.3.1.4 p）中没有常见的绕过认证方式进行系统登录的方法，则该项为肯定；

e） 7.1.3.1.4 e）-m）均为肯定，则信息系统符合本单元测评项要求。

7.1.3.2 自主访问控制

7.1.3.2.1 测评项

a) 应依据安全策略控制主体对客体的访问；

b) 自主访问控制的覆盖范围应包括与信息安全直接相关的主体、客体及它们之间的操作；

c) 自主访问控制的粒度应达到主体为用户级，客体为文件、数据库表级；

d) 应由授权主体设置对客体访问和操作的权限；

e) 权限分离应采用最小授权原则，分别授予不同用户各自为完成自己承担任务所需的最小权限，并在他们之间形成相互制约的关系；

f) 应实现操作系统和数据库系统特权用户的权限分离；

g) 应严格限制默认用户的访问权限。

7.1.3.2.2 测评方式

检查，测试。

7.1.3.2.3 测评对象

主要服务器操作系统，主要数据库系统，安全策略。

7.1.3.2.4 测评实施

a) 应检查服务器操作系统和数据库系统的自主访问控制功能是否具有《信息安全等级保护 操作系统安全技术要求》和《信息安全等级保护 数据库管理系统安全技术要求》第二级以上或TCSEC C2级以上的测试报告；

b) 应检查服务器操作系统和数据库系统的安全策略，查看是否明确主体（如用户）以用户和/或用户组的身份规定对客体（如文件或系统设备，目录表和存取控制表访问控制等）的访问控制，覆盖范围是否包括与信息安全直接相关的主体（如用户）和客体（如文件，数据库表等）及它们之间的操作（如读、写或执行）；

c) 应检查服务器操作系统和数据库系统的安全策略，查看是否明确主体（如用户）具有非敏感标记（如角色），并能依据非敏感标记规定对客体的访问；

d) 应检查主要服务器操作系统和主要数据库系统的访问控制列表，查看授权用户中是否不存在过期的帐号和无用的帐号等；访问控制列表中的用户和权限，是否与安全策略相一致；

e) 应检查主要服务器操作系统和主要数据库系统，查看客体（如文件，数据库表、视图、存储过程和触发器等）的所有者是否可以改变其相应访问控制列表的属性，得到授权的用户是否可以改变相应客体访问控制列表的属性；

f) 应检查主要服务器操作系统和主要数据库系统，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（如系统管理员只能对系统进行维护，安全管理员只能进行策略配置和安全设置，安全审计员只能维护审计信息等）；

g) 应检查主要服务器操作系统和主要数据库系统，查看在系统管理员、安全管理员、安全审计员之间是否设置了相互制约关系（如系统管理员、安全管理员等不能对审计日志，安全审计员管理不了审计数据的开启、关闭、删除等重要事件的审计日志等）；

h) 应查看主要服务器操作系统和主要数据库系统，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（如限定在有限的范围内）；

i) 应测试主要服务器操作系统和主要数据库系统，依据系统访问控制的安全策略，试图以未授权用户身份/角色访问客体，验证是否不能进行访问。

7.1.3.2.5 结果判定

a) 如果7.1.3.2.4 a）为肯定，则测评实施e）和i）为肯定；

b) 7.1.3.2.4 b）-i）均为肯定，则信息系统符合本单元测评项要求。

7.1.3.3 强制访问控制

7.1.3.3.1 测评项

a) 应对重要信息资源和访问重要信息资源的所有主体设置敏感标记；

b) 强制访问控制的覆盖范围应包括与重要信息资源直接相关的所有主体、客体及它们之间的操作；

c) 强制访问控制的粒度应达到主体为用户级，客体为文件、数据库表级。

7.1.3.3.2 测评方式

访谈，检查，测试。

7.1.3.3.3 测评对象

主要服务器操作系统，主要数据库系统，服务器操作系统文档，数据库系统文档。

7.1.3.3.4 测评实施

a) 应检查服务器操作系统和数据库系统的强制访问控制是否具有《信息安全等级保护操作系统安全技术要求》和《信息安全等级保护 数据库管理系统安全技术要求》第三级以上的测试报告；

b) 应检查主要服务器操作系统和主要数据库系统，查看是否能对重要信息资源和访问重要信息资源的所有主体设置敏感标记，这些敏感标记是否构成多级安全模型的属性库，主体和客体的敏感标记是否以默认方式生成或由安全员建立、维护和管理；

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

d) 应检查服务器操作系统和主要数据库系统文档，查看强制访问控制是否与用户身份鉴别、标识等安全功能密切配合，并且控制粒度达到主体为用户级，客体为文件和数据库表级；

e) 应测试主要服务器操作系统和主要数据库系统，依据系统文档描述的强制访问控制模型，以授权用户和非授权用户身份访问客体，验证是否只有授权用户可以访问客体，而非授权用户不能访问客体；

f) 应渗透测试主要服务器操作系统和主要数据库系统，可通过非法终止强制访问模块，非法修改强制访问相关规则，使用假冒身份等方式，测试强制访问控制是否安全、可靠。

7.1.3.3.5 结果判定

a) 如果7.1.3.3.4 a）为肯定，则测评实施b）、c）和f）为肯定；

b) 7.1.3.3.4 b）-e）均为肯定，则信息系统符合本单元测评项要求。

7.1.3.4 安全审计

7.1.3.4.1 测评项

a) 安全审计应覆盖到服务器和客户端上的每个操作系统用户和数据库用户；

b) 安全审计应记录系统内重要的安全相关事件，包括重要用户行为、系统资源的异常使用和重要系统命令的使用；

c) 安全相关事件的记录应包括日期和时间、类型、主体标识、客体标识、事件的结果等；

d) 安全审计应可以根据记录数据进行分析，并生成审计报表；

e） 安全审计应可以对特定事件，提供指定方式的实时报警；

f） 审计进程应受到保护避免受到未预期的中断；

g） 审计记录应受到保护避免受到未预期的删除、修改或覆盖等。

7.1.3.4.2 测评方式

访谈，检查，测试。

7.1.3.4.3 测评对象

安全审计员，主要服务器操作系统，重要终端操作系统，主要数据库系统。

7.1.3.4.4 测评实施

a） 可访谈安全审计员，询问主机系统是否设置安全审计；询问主机系统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） 应检查主要服务器操作系统、重要终端操作系统和主要数据库系统，查看当前审计范围是否覆盖到每个用户；

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系统，查看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、自主访问控制的所有操作记录、重要用户行为（如用超级用户命令改变用户身份，删除系统表）、系统资源的异常使用、重要系统命令的使用（如删除客体）等；

d） 应检查主要服务器操作系统、重要终端操作系统和主要数据库系统，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、身份鉴别事件中请求的来源（如末端标识符）、事件的结果等内容；

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

f） 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系统，查看能否对特定事件指定实时报警方式（如声音、EMAIL、短信等）；

g) 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系统，查看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，能否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；

h） 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系统，可通过非法终止审计功能或修改其配置，验证审计功能是否受到保护；

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

j） 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系统，在系统上以某个系统用户试图删除、修改或覆盖审计记录，测试安全审计的保护情况与要求是否一致。

7.1.3.4.5 结果判定

a） 7.1.3.4.4 b）-j）均为肯定，则信息系统符合本单元测评项要求。

7.1.3.5 系统保护

7.1.3.5.1 测评项

a） 系统因故障或其他原因中断后，应能够以手动或自动方式恢复运行。

7.1.3.5.2 测评方式

访谈，测试。

7.1.3.5.3 测评对象

系统管理员，主要服务器操作系统。

7.1.3.5.4 测评实施

a) 应访谈系统管理员，询问哪些故障或其他原因会导致服务器系统中断，中断后能否以手动或自动方式恢复运行，相应操作规程有哪些；

b) 应测试主要服务器操作系统，可通过人为制造一些故障（如断电等），验证服务器系统因故障或其他原因中断后，能否以手动或自动方式恢复运行。

7.1.3.5.5 结果判定

a) 如果系统管理员能够描述出主要故障或其他原因，以及相应操作规程，则7.1.3.5.4 b）为肯定；

b) 7.1.3.5.4 a）-b）为肯定，则信息系统符合本单元测评项要求。

7.1.3.6 剩余信息保护

7.1.3.6.1 测评项

a) 应保证操作系统和数据库管理系统用户的鉴别信息所在的存储空间，被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中；

b) 应确保系统内的文件、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。

7.1.3.6.2 测评方式

访谈，检查。

7.1.3.6.3 测评对象

系统管理员，数据库管理员，主要服务器操作系统维护/操作手册，主要数据库系统维护/操作手册。

7.1.3.6.4 测评实施

a) 应检查服务器操作系统和数据库系统的剩余信息保护（用户数据保密性保护/客体重用）功能是否具有《信息安全等级保护 操作系统安全技术要求》和《信息安全等级保护 数据库管理系统安全技术要求》第二级以上的测试报告；

b) 应与系统管理员访谈，询问操作系统用户的鉴别信息存储空间，被释放或再分配给其他用户前是否得到完全清除；系统内的文件、目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是否得到完全清除；

c) 应与数据库管理员访谈，询问数据库管理员用户的鉴别信息存储空间，被释放或再分配给其他用户前是否得到完全清除；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是否得到完全清除；

d) 应检查主要操作系统和主要数据库系统维护操作手册，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；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。

7.1.3.6.5 结果判定

b) 如果 7.1.3.6.4 a）为肯定，则测评实施 b）-d）为肯定；

c) 7.1.3.6.4 b）-d）均为肯定，则信息系统符合本单元测评项要求。

7.1.3.7 入侵防范

7.1.3.7.1 测评项

a) 应进行主机运行监视，包括监视主机的CPU、硬盘、内存、网络等资源的使用情况；

b) 应设定资源报警阈值，以便在资源使用超过规定数值时发出报警；

c) 应进行特定进程监控，限制操作人员运行非法进程；

d) 应进行主机账户监控，限制对重要账户的添加和更改；
e) 应检测各种已知的入侵行为，记录入侵的源IP、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时提供报警；
f) 应能够检测重要程序完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施。

7.1.3.7.2 测评方式

访谈，检查，测试。

7.1.3.7.3 测评对象

系统管理员，主要服务器系统。

7.1.3.7.4 测评实施

a) 应与系统管理员访谈，询问主机系统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、资源使用超过值报警、特定进程监控、入侵行为检测、完整性检测等方面内容；
b) 应与系统管理员访谈，询问入侵防范产品的厂家、版本和在主机系统中的安装部署情况；询问是否进行过部署的改进或者更换过产品，是否按要求（如定期或实时）进行产品升级；
c) 应检查主要服务器系统，查看是否进行主机运行监视，监视的内容是否包括主机的CPU、硬盘、内存、网络等资源的使用情况，并给出资源使用历史记录；
d) 应检查主要服务器系统，查看是否设定资源报警阈值（如 CPU、硬盘、内存、网络等资源的报警阈值）以便在资源使用超过规定数值时发出报警，并查看报警方式有哪些；
e) 应检查主要服务器系统，查看是否对特定进程（包括主要的系统进程，如 WINDOWS 的 Explorer 进程）进行监控，是否可以设定非法进程列表；
f) 应检查主要服务器系统，查看是否对主机账户（如系统管理员）进行控制，以限制对重要账户的添加和更改等；
g) 应检查主要服务器系统，查看能否记录攻击者的源 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、EMAIL 等）；
h) 应测试主要服务器系统，试图运行非法进程，验证其能否限制非法进程的运行；试图添加或更改重要账户，验证主机能否限制重要账户的添加和更改；
i) 应测试主要服务器系统，试图破坏重要程序（如执行系统任务的重要程序）的完整性，验证主机能否检测到重要程序的完整性受到破坏。

7.1.3.7.5 结果判定

a) 如果 7.1.3.7.4 b）中的厂家为正规厂家（如有销售许可），版本号较新，改进合理，定期升级，则该项为肯定；
b) 7.1.3.7.4 a）-f）均为肯定，则信息系统符合本单元测评项要求。

7.1.3.8 恶意代码防范

7.1.3.8.1 测评项

a) 服务器和终端设备（包括移动设备）均应安装实时检测和查杀恶意代码的软件产品；
b) 主机系统防恶意代码产品应具有与网络防恶意代码产品不同的恶意代码库；
c) 应支持恶意代码防范的统一管理。

7.1.3.8.2 测评方式

访谈，检查，测试。

7.1.3.8.3 测评对象

系统安全员，主要服务器系统，主要终端系统，网络防恶意代码产品，主机安全设计/

验收文档。

7.1.3.8.4 测评实施

a) 应访谈系统安全员，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情况如何，因何改进过部署或者更换过产品，是否按要求（如定期或实时）进行产品升级；

b) 应检查主机恶意代码防范方面的设计/验收文档，查看描述的安装范围是否包括服务器和终端设备（包括移动设备）；

c) 应检查主要服务器系统和主要终端系统，查看是否安装实时检测与查杀恶意代码的软件产品，查看实时检测与查杀恶意代码的软件产品是否支持恶意代码防范的统一管理功能，查看检测与查杀恶意代码软件产品的厂家、版本号和恶意代码库名称；

d) 应检查网络防恶意代码产品，查看厂家、版本号和恶意代码库名称。

7.1.3.8.5 结果判定

c) 如果7.1.3.8.4 a）中恶意代码实时检测与查杀措施的部署到所有服务器和重要终端，则该项为肯定；

d) 7.1.3.8.4 a）-c）均为肯定，检查发现主机系统防恶意代码产品与网络防恶意代码产品使用不同的恶意代码库（如厂家、版本号和恶意代码库名称不相同等），则信息系统符合本单元测评项要求。

7.1.3.9 资源控制

7.1.3.9.1 测评项

a) 应限制单个用户的多重并发会话；

b) 应对最大并发会话连接数进行限制；

c) 应对一个时间段内可能的并发会话连接数进行限制；

d) 应通过设定终端接入方式、网络地址范围等条件限制终端登录；

e) 应根据安全策略设置登录终端的操作超时锁定和鉴别失败锁定，并规定解锁或终止方式；

f) 应禁止同一用户账号在同一时间内并发登录；

g) 应限制单个用户对系统资源的最大或最小使用限度；

h) 当系统的服务水平降低到预先规定的最小值时，应能检测和报警；

i) 应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。

7.1.3.9.2 测评方式

检查，测试。

7.1.3.9.3 测评对象

主要服务器操作系统。

7.1.3.9.4 测评实施

a) 应检查主要服务器操作系统，查看是否限制单个用户的多重并发会话数量；查看是否设置登录终端的操作超时锁定和鉴别失败锁定，以及是否规定解锁或终止方式；查看是否配置了终端接入方式、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，查看是否对一个时间段内可能的并发会话连接数进行限制，是否禁止同一用户账号在同一时间内并发登录，是否限制单个用户对系统资源（如 CPU、内存和硬盘等）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，报警的方式有哪些，能否已根据安全策略设定主体（如进程）的服务优先级，并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；

d) 应测试主要服务器操作系统，任选一个用户，登录服务器，试图发出多重并发会话，验证系统是否限制单个用户的多重并发会话；试图在一段时间内建立一些并发会话连接，验证系统是否对一定时间段内的并发会话连接数进行限制；

e) 应测试重要服务器操作系统，任选一个用户帐户，登录服务器，用不同的终端接入方式、网络地址试图登录服务器，验证重要服务器操作系统是否通过终端接入方式、网络地址范围等条件限制终端登录。

f) 应测试主要服务器操作系统，试图使服务水平降低到预先规定的最小值，验证系统能否正确检测和报警；

g) 应测试主要服务器操作系统，任选一个用户，登录服务器，在一定时间内不进行任何动作，验证主要服务器操作系统能否对操作超时的终端进行锁定；任选一个用户，可通过多次失败登录服务器，验证服务器能否对鉴别失败的终端进行锁定，锁定后能否按照规定的解锁或终止方式进行解锁或终止。

7.1.3.9.5 结果判定

a) 7.1.3.9.4 a）-g）均为肯定，则信息系统符合本单元测评项要求。

7.1.4 应用安全

7.1.4.1 身份鉴别

7.1.4.1.1 测评项

a) 系统用户的身份标识应具有唯一性；

b) 应对登录的用户进行身份标识和鉴别；

c) 系统用户的身份鉴别信息应具有不易被冒用的特点，例如口令长度、复杂性和定期的更新等；

d) 应对同一用户采用两种或两种以上组合的鉴别技术实现用户身份鉴别；

e) 应具有登录失败处理功能，如结束会话、限制非法登录次数，当登录连接超时，自动退出；

f) 应具有鉴别警示功能；

g) 应用系统应及时清除存储空间中动态使用的鉴别信息。

7.1.4.1.2 测评方式

访谈，检查，测试。

7.1.4.1.3 测评对象

系统管理员，主要应用系统，设计/验收文档，操作规程和操作记录。

7.1.4.1.4 测评实施

a) 可访谈系统管理员，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（如复杂性混有大、小写字母、数字和特殊字符，口令周期等）；

b) 可访谈系统管理员，询问应用系统是否具有登录失败处理的功能，是如何进行处理的；询问应用系统对用户标识在整个生命周期内是否具有唯一性（如UID、用户名或其他信息在系统中是唯一的，用该标识在整个生命周期内能唯一识别该用户）；

c) 应检查设计/验收文档，查看文档中是否有系统采取了唯一标识（如用户名、UID或其他属性）的描述；

d) 应检查操作规程和操作记录，查看其是否有身份标识和鉴别的操作规程、审批记录和操作记录；

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（如采用用户名/口令、挑战应答、动态口令、物理设备、生物识别技

术中的任意两个组合）；对有抗抵赖要求的系统，查看其是否采用数字证书方式的身份鉴别技术；

f) 应检查主要应用系统，查看其是否配备身份标识（如建立账号）和鉴别（如口令等）功能；查看其其身份鉴别信息是否具有不易被冒用的特点，例如复杂性（如规定字符应混有大、小写字母、数字和特殊字符）或为了便于记忆使用了令牌；

g) 应检查主要应用系统，查看其是否配备并使用登录失败处理功能（如登录失败次数超过设定值，系统自动退出等）；

h) 应测试主要应用系统，可通过注册用户，并登录系统，查看登录是否成功，验证其身份标识和鉴别功能是否有效；可通过删除一个用户再重新注册相同标识的用户，查看能否成功，验证身份标识在整个生命周期内是否具有唯一性；

i) 应测试主要应用系统，验证其登录失败处理，非法登录次数限制，登录连接超时自动退出等功能是否有效；

j) 应测试主要应用系统，验证其是否及时清除存储空间中动态使用的鉴别信息（如登录系统，退出系统后重新登录系统，查看上次登录的鉴别信息是否存在）；

k) 应测试主要应用系统，验证其是否有鉴别警示功能（如系统有三次登录失败则锁定该用户的限制，则应给用户必要的提示）；

l) 应渗透测试主要应用系统，测试身份鉴别信息是否不易被冒用（如通过暴力破解或其他手段进入系统，对WEB系统可采用SQL注入等绕过身份鉴别的方法）。

7.1.4.1.5 结果判定

a) 如果7.1.4.1.4 c）中相关文档有用户唯一性标识的描述，则该项为肯定；

b) 如果7.1.4.1.4 d）中缺少相应的文档，则该项为否定；

c) 7.1.4.1.4 c）-k）均为肯定，则信息系统符合本单元测评项要求。

7.1.4.2 访问控制

7.1.4.2.1 测评项

a) 应依据安全策略控制用户对客体的访问；

b) 自主访问控制的覆盖范围应包括与信息安全直接相关的主体、客体及它们之间的操作；

c) 自主访问控制的粒度应达到主体为用户级，客体为文件、数据库表级；

d) 应由授权主体设置对系统功能操作和对数据访问的权限；

e) 应实现应用系统特权用户的权限分离，例如将管理与审计的权限分配给不同的应用系统用户；

f) 权限分离应采用最小授权原则，分别授予不同用户各自为完成自己承担任务所需的最小权限，并在它们之间形成相互制约的关系；

g) 应严格限制默认用户的访问权限。

7.1.4.2.2 测评方式

访谈，检查，测试。

7.1.4.2.3 测评对象

系统管理员，主要应用系统。

7.1.4.2.4 测评实施

a) 可访谈系统管理员，询问业务系统是否提供访问控制措施，具体措施有哪些，自主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（如文件和数据库中的数据）的访问；

c) 应检查主要应用系统，查看其自主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；自主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（如数据库表、视图、存储过程等）；

d) 应检查主要应用系统，查看应用系统是否有对授权主体进行系统功能操作和对数据访问权限进行设置的功能；

e) 应检查主要应用系统，查看其特权用户的权限是否分离（如将系统管理员、安全员和审计员的权限分离），权限之间是否相互制约（如系统管理员、安全管理员等不能对审计日志进行管理，安全审计员不能管理审计功能的开启、关闭、删除等重要事件的审计日志等）；

f) 应检查主要应用系统，查看其是否有限制默认用户访问权限的功能，并已配置使用；

g) 应测试主要应用系统，可通过用不同权限的用户登录，查看其权限是否受到应用系统的限制，验证系统权限分离功能是否有效；

h) 应测试主要应用系统，可通过授权主体设置特定用户对系统功能进行操作和对数据进行访问的权限，然后以该用户登录，验证用户权限管理功能是否有效；

i) 应测试主要应用系统，可通过用默认用户（默认密码）登录，并用该用户进行操作（包括合法、非法操作），验证系统对默认用户访问权限的限制是否有效；

j) 应渗透测试主要应用系统，测试自主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（如试图绕过系统访问控制机制等操作）。

7.1.4.2.5 结果判定

a) 7.1.4.2.4 b）-j）均为肯定，则信息系统符合本单元测评项要求。

7.1.4.3 安全审计

7.1.4.3.1 测评项

a) 安全审计应覆盖到应用系统的每个用户；

b) 安全审计应记录应用系统重要的安全相关事件，包括重要用户行为、系统资源的异常使用和重要系统功能的执行等；

c) 安全相关事件的记录应包括日期和时间、类型、主体标识、客体标识、事件的结果等；

d) 安全审计应可以根据记录数据进行分析，并生成审计报表；

e) 安全审计应可以对特定事件，提供指定方式的实时报警；

f) 审计进程应受到保护避免受到未预期的中断；

g) 审计记录应受到保护避免受到未预期的删除、修改或覆盖等。

7.1.4.3.2 测评方式

访谈，检查，测试。

7.1.4.3.3 测评对象

安全审计员，主要应用系统。

7.1.4.3.4 测评实施

a) 可访谈安全审计员，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、自主访问控制的所有操作记录、重要用户行为（如用超级用户命令改变用户身份，删除系统表）、系统资源的异常使用、重要系统命令的使用（如删除客体）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（如末端标识符）、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工具（如对审计记录进行分类、排序、查询、统计、分析和组合查询等），并能根据需要生成审计报表；

f) 应检查主要应用系统，查看其能否对特定事件指定实时报警方式（如声音、EMAIL、短信等）；

g) 应测试主要应用系统，可通过非法终止审计功能或修改其配置，验证审计功能是否受到保护；

h) 应测试主要应用系统，在系统上以某个用户试图产生一些重要的安全相关事件（如鉴别失败等），测试安全审计的覆盖情况和记录情况与要求是否一致；

i) 应测试主要应用系统，在系统上以某个系统用户试图删除、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。

7.1.4.3.5 结果判定

a) 7.1.4.3.4 b）-i）均为肯定，则信息系统符合本单元测评项要求。

7.1.4.4 剩余信息保护

7.1.4.4.1 测评项

a) 应保证用户的鉴别信息所在的存储空间，被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中；

b) 应确保系统内的文件、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。

7.1.4.4.2 测评方式

访谈，检查，测试。

7.1.4.4.3 测评对象

系统管理员，设计/验收文档。

7.1.4.4.4 测评实施

a) 可访谈系统管理员，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/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/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）。

7.1.4.4.5 结果判定

a) 如果7.1.4.4.4 b）-c）缺少相关材料，则该项为否定；

b) 7.1.4.4.4 b）-d）均为肯定，则信息系统符合本单元测评项要求。

7.1.4.5 通信完整性

7.1.4.5.1 测评项

a) 通信双方应约定密码算法，计算通信数据报文的报文验证码，在进行通信时，双方根据校验码判断对方报文的有效性。

7.1.4.5.2 测评方式

访谈，检查，测试。

7.1.4.5.3 测评对象

安全员，主要应用系统，设计/验收文档。

7.1.4.5.4 测评实施

a) 可访谈安全员，询问业务系统是否有数据在传输过程中进行完整性保证的操作，具体措施是什么；

b) 应检查设计/验收文档，查看其是否有通信完整性的说明，如果有则查看其是否有系统是根据校验码判断对方数据包的有效性的，用密码计算通信数据报文的报文验证码的描述；

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验证码。

7.1.4.5.5 结果判定

a) 7.1.4.5.4 b）-c）均为肯定，则信息系统符合本单元测评项要求。

7.1.4.6 通信保密性

7.1.4.6.1 测评项

a) 当通信双方中的一方在一段时间内未作任何响应，另一方应能够自动结束会话；

b) 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；

c) 在通信过程中，应对整个报文或会话过程进行加密；

d) 应选用符合国家有关部门要求的密码算法。

7.1.4.6.2 测评方式

访谈，检查，测试。

7.1.4.6.3 测评对象

安全员，主要应用系统，相关证明材料（证书）。

7.1.4.6.4 测评实施

a) 可访谈安全员，询问业务系统数据在存储和传输过程中是否采取保密措施（如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，在通信过程中对敏感信息字段进行加密等），具体措施有哪些；

b) 应检查相关证明材料（证书），查看应用系统采用的密码算法是否符合国家有关部门要求；

c) 应测试主要应用系统，查看当通信双方中的一方在一段时间内未作任何响应，另一方是否能自动结束会话；系统是否能在通信双方建立会话之前，利用密码技术进行会话初始化验证（如SSL建立加密通道前是否利用密码技术进行会话初始验证）；在通信过程中，是否对整个报文或会话过程进行加密；

d) 应测试主要应用系统，通过通信双方中的一方在一段时间内未作任何响应，查看另一方是否能自动结束会话，测试当通信双方中的一方在一段时间内未作任何响应，另一方是否能自动结束会话的功能是否有效；

e) 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。

7.1.4.6.5 结果判定

a) 如果7.1.4.6.4 b）缺少相关材料，则该项为否定；

b) 7.1.4.6.4 b）-e）均为肯定，则信息系统符合本单元测评项要求。

7.1.4.7 抗抵赖

7.1.4.7.1 测评项

a) 应具有在请求的情况下为数据原发者或接收者提供数据原发证据的功能；

b) 应具有在请求的情况下为数据原发者或接收者提供数据接收证据的功能。

7.1.4.7.2 测评方式

访谈，测试。

7.1.4.7.3 测评对象

安全员，主要应用系统。

7.1.4.7.4 测评实施

a) 可访谈安全员，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或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或接收者提供数据接收证据的功能。

7.1.4.7.5 结果判定

a) 7.1.4.7.4 b）为肯定，则信息系统符合本单元测评项要求。

7.1.4.8 软件容错

7.1.4.8.1 测评项

a) 应对通过人机接口输入或通过通信接口输入的数据进行有效性检验；

b) 应对通过人机接口方式进行的操作提供“回退”功能，即允许按照操作的序列进行回退；

c) 应有状态监测能力，当故障发生时，能实时检测到故障状态并报警；

d) 应有自动保护能力，当故障发生时，自动保护当前所有状态。

7.1.4.8.2 测评方式

访谈，检查，测试。

7.1.4.8.3 测评对象

系统管理员，主要应用系统。

7.1.4.8.4 测评实施

a) 可访谈系统管理员，询问业务系统是否有保证软件具有容错能力的措施（如对人机接口输入或通过通信接口输入的数据进行有效性检验等），具体措施有哪些；

b) 应检查主要应用系统，查看业务系统是否对人机接口输入（如用户界面的数据输入）或通信接口输入的数据进行有效性检验；是否允许按照操作的序列进行回退（如撤消操作）；是否在故障发生时继续提供一部分功能，确保能够实施必要的措施（如对重要数据的保存）；

c) 应测试主要应用系统，可通过输入的不同（如数据格式或长度等符合、不符合软件设定的要求），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，可通过多步操作，然后回退，验证系统能否按照操作的序列进行正确的回退；

e) 应测试主要应用系统，可通过给系统人为制造一些故障（如系统异常），验证系统能否在故障发生时实时检测到故障状态并报警，能否自动保护当前所有状态。

7.1.4.8.5 结果判定

a) 7.1.4.8.4 b）-e）均为肯定，则信息系统符合本单元测评项要求。

7.1.4.9 资源控制

7.1.4.9.1 测评项

a) 应限制单个用户的多重并发会话；
b) 应对应用系统的最大并发会话连接数进行限制；
c) 应对一个时间段内可能的并发会话连接数进行限制；
d) 应根据安全策略设置登录终端的操作超时锁定和鉴别失败锁定，并规定解锁或终止方式；
e) 应禁止同一用户账号在同一时间内并发登录；
f) 应对一个访问用户或一个请求进程占用的资源分配最大限额和最小限额；
g) 应根据安全属性（用户身份、访问地址、时间范围等）允许或拒绝用户建立会话连接；
h) 当系统的服务水平降低到预先规定的最小值时，应能检测和报警；
i) 应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。

7.1.4.9.2 测评方式

访谈，检查，测试。

7.1.4.9.3 测评对象

系统管理员，主要应用系统。

7.1.4.9.4 测评实施

a) 可访谈系统管理员，询问业务系统是否有资源控制的措施（如对应用系统的最大并发会话连接数进行限制，是否禁止同一用户账号在同一时间内并发登录，是否对一个时间段内可能的并发会话连接数进行限制，对一个访问用户或一个请求进程占用的资源分配最大限额和最小限额等），具体措施有哪些；
b) 应检查主要应用系统，查看是否有限制单个用户的多重并发会话；系统是否有最大并发会话连接数的限制，是否有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) 应检查主要应用系统，查看是否根据安全策略设置登录终端的操作超时锁定和鉴别失败锁定，并规定解锁或终止方式；是否禁止同一用户账号在同一时间内并发登录；是否对一个访问用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，查看是否根据安全属性（用户身份、访问地址、时间范围等）允许或拒绝用户建立会话连接；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单个用户的多重并发会话连接，验证系统能否正确地限制单个用户的多重并发会话数；可通过对系统进行超过最大并发会话连接数进行连接，验证系统能否正确地限制最大并发会话连接数；
f) 应测试主要应用系统，可通过在一个时间段内，用超过设定的并发连接数对系统进行连接，查看能否连接成功，验证系统对一个时间段内可能的并发会话连接数进行限制的功能是否正确；
g) 应测试主要应用系统，可通过设置登录终端的操作超时锁定和鉴别失败锁定，并规定解锁或终止方式，制造操作超时和鉴别失败，验证系统能否锁定，解锁或终止方式是否和设定的方式相同；
h) 应测试主要应用系统，可通过按照安全属性（用户身份、访问地址、时间范围等）设定允许或拒绝某个用户建立会话连接，然后用该用户进行对应的操作，验证查看

系统能否正确地根据安全属性允许或拒绝用户建立会话连接；试图使服务水平降低到预先规定的最小值，验证系统能否正确检测并报警。

7.1.4.9.5 结果判定

a) 7.1.4.9.4 b）-h）均为肯定，则信息系统符合本单元测评项要求。

7.1.4.10 代码安全

7.1.4.10.1 测评项

a) 应制定应用程序代码编写安全规范，要求开发人员参照规范编写代码；

b) 应对应用程序代码进行代码复审，识别可能存在的恶意代码；

c) 应对应用程序代码进行安全脆弱性分析；

d) 应对应用程序代码进行穿透性测试。

7.1.4.10.2 测评方式

访谈，检查，测试。

7.1.4.10.3 测评对象

系统管理员，设计/验收文档，相关证明材料（证书），主要应用系统。

7.1.4.10.4 测评实施

a) 可访谈系统管理员，询问业务系统是否有保证质量的措施（如系统是否有应用程序代码编写安全规范，开发人员是否参照规范编写代码），具体措施有哪些；

b) 应检查设计/验收文档和其他相关文档，查看是否有应用程序代码编写安全规范；

c) 应检查设计/验收文档和相关证明材料（证书），查看是否有对应用程序代码进行代码复审；

d) 应检查设计/验收文档和相关证明材料（证书），查看是否对应用程序代码进行安全脆弱性分析；

e) 应检查设计/验收文档和相关证明材料（证书），查看是否有对应用程序代码进行穿透性测试的声明；

f) 应检查主要应用系统，查看应用程序代码的编制与代码安全规范要求是否一致；

g) 应测试主要应用系统，可通过对代码进行穿透性测试（如内存溢出等），查看是否成功。

7.1.4.10.5 结果判定

a) 如果7.1.4.10.4 b）-e）缺少相关材料，则该项为否定；

b) 7.1.4.10.4 b）-g）均为肯定，则信息系统符合本单元测评项要求。

7.1.5 数据安全

7.1.5.1 数据完整性

7.1.5.1.1 测评项

a) 应能够检测到系统管理数据、鉴别信息和用户数据在传输过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施；

b) 应能够检测到系统管理数据、鉴别信息和用户数据在存储过程中完整性受到破，并在检测到完整性错误时采取必要的恢复措施；

c) 应能够检测到重要系统的完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施。

7.1.5.1.2 测评方式

访谈，检查。

7.1.5.1.3 测评对象

安全员，主要应用系统，设计/验收文档，相关证明性材料（如证书、检验报告等）。

7.1.5.1.4 测评实施

a) 可访谈安全员，询问业务系统数据在存储、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) 应检查操作系统、网络设备、数据库管理系统的设计/验收文档或相关证明性材料（如证书、检验报告等）等，查看其是否有能检测/验证到系统管理数据（如WINDOWS 域管理、目录管理数据）、鉴别信息（如用户名和口令）和用户数据（如用户数据文件）在传输过程中完整性受到破坏，能检测到系统管理数据、身份鉴别信息和用户数据（如防火墙的访问控制规则）在存储过程中完整性受到破坏，能检测到重要系统完整性受到破坏，在检测到完整性错误时采取必要的恢复措施的描述；如果有相关信息，查看其配置是否正确；

c) 应检查主要应用系统，查看其是否配备检测/验证系统管理数据、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/验证系统管理数据、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/验证重要系统/模块完整性受到破坏的功能；在检测/验证到完整性错误时能采取必要的恢复措施；

d) 应检查主要应用系统，查看其是否配备检测系统完整性受到破坏的功能；并在检测到完整性错误时采取必要的恢复措施。

7.1.5.1.5 结果判定

a) 如果 7. 1. 5. 1. 4 b）缺少相关材料，则该项为否定；

b) 7. 1. 5. 1. 4 b）-d）均为肯定，则信息系统符合本单元测评项要求。

7.1.5.2 数据保密性

7.1.5.2.1 测评项

a) 网络设备、操作系统、数据库系统和应用系统的鉴别信息、敏感的系统管理数据和敏感的用户数据应采用加密或其他有效措施实现传输保密性；

b) 网络设备、操作系统、数据库系统和应用系统的鉴别信息、敏感的系统管理数据和敏感的用户数据应采用加密或其他保护措施实现存储保密性；

c) 当使用便携式和移动式设备时，应加密或者采用可移动磁盘存储敏感信息；

d) 用于特定业务通信的通信信道应符合相关的国家规定。

7.1.5.2.2 测评方式

访谈，检查，测试。

7.1.5.2.3 测评对象

系统管理员、网络管理员、安全员、数据库管理员，主要应用系统，设计/验收文档，相关证明性材料（如证书等）。

7.1.5.2.4 测评实施

a) 可访谈网络管理员，询问信息系统中的网络设备的鉴别信息、敏感的系统管理数据和敏感的用户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保护措施实现存储保密性；

b) 可访谈系统管理员，询问信息系统中的操作系统的鉴别信息、敏感的系统管理数据和敏感的用户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保护措施实现存储保密性；

c) 可访谈数据库管理员，询问信息系统中的数据库管理系统的鉴别信息、敏感的系统管理数据和敏感的用户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保护措施实现存储保密性；

d) 可访谈安全员，询问信息系统中的应用系统的鉴别信息、敏感的系统管理数据和敏

感的用户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保护措施实现存储保密性；

e) 可访谈安全员，询问当使用便携式和移动式设备时，是否加密或者采用可移动磁盘存储敏感信息；

f) 应检查操作系统、网络设备、数据库系统、关键应用系统的设计/验收文档，查看其是否有关于鉴别信息、敏感的系统管理数据和敏感的用户数据采用加密或其他有效措施实现传输保密性描述，是否有采用加密或其他保护措施实现存储保密性的描述；

g) 应检查相关证明性材料（如证书或其他相关材料等），查看其是否有特定业务通信的通信信道符合相关的国家规定的说明；

h) 应检查主要应用系统，查看其鉴别信息、敏感的系统管理数据和敏感的用户数据是否采用加密或其他有效措施实现传输保密性描述，是否采用加密或其他保护措施实现存储保密性；

i) 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。

7.1.5.2.5 结果判定

a) 如果 7.1.5.2.4 f）缺少相关材料，则该项为否定；

b) 如果没有相关证明性材料（如证书、检验报告等），7.1.5.2.4 g）为否定；

c) 7.1.5.2.4 f）-i）均为肯定，则信息系统符合本单元测评项要求。

7.1.5.3 数据备份和恢复

7.1.5.3.1 测评项

a) 应提供自动备份机制对重要信息进行本地和异地备份；

b) 应提供恢复重要信息的功能；

c) 应提供重要网络设备、通信线路和服务器的硬件冗余；

d) 应提供重要业务系统的本地系统级热备份。

7.1.5.3.2 测评方式

访谈，检查。

7.1.5.3.3 测评对象

系统管理员，网络管理员，数据库管理员，操作系统，网络设备，数据库系统，主要应用系统，设计/验收文档。

7.1.5.3.4 测评实施

a) 可访谈网络管理员，询问信息系统中的网络设备是否提供自动备份机制对重要信息进行本地和异地备份功能；是否提供对重要信息进行恢复的功能；是否提供重要网络设备、通信线路和服务器的硬件冗余；

b) 可访谈系统管理员，询问信息系统中的操作系统是否提供自动备份机制对重要信息进行本地和异地备份功能；是否提供对重要信息进行恢复的功能；

c) 可访谈数据库管理员，询问信息系统中的数据库管理系统是否提供自动备份机制对重要信息进行本地和异地备份功能；是否提供重要业务系统的本地系统级热备份；是否提供对重要信息进行恢复的功能；

d) 应检查设计/验收文档，查看其是否有关于操作系统、网络设备、数据库系统、应用系统配置有本地系统级热备份和重要信息恢复功能的描述；

e) 应检查操作系统、网络设备、数据库系统、主要应用系统，查看其是否配置有本地/异地备份和重要信息恢复的功能，其配置是否正确；

f) 应检查重要网络设备、通信线路和服务器是否提供硬件冗余；

g） 应检查重要业务系统是否配备本地系统级热备份的功能。

7.1.5.3.5 结果判定

a) 如果没有设计/验收文档，7.1.5.3.4 d） 则该项为否定；

b) 7.1.5.3.4 d）-e）均为肯定，则信息系统符合本单元测评项要求。

7.2 安全管理测评

7.2.1 安全管理机构

7.2.1.1 岗位设置

7.2.1.1.1 测评项

a） 应设立信息安全管理工作的职能部门，设立安全主管人、安全管理各个方面的负责人，定义各负责人的职责；

b） 应设立系统管理人员、网络管理人员、安全管理人员岗位，定义各个工作岗位的职责；

c） 应成立指导和管理信息安全工作的委员会或领导小组，其最高领导应由单位主管领导委任或授权；

d） 应制定文件明确安全管理机构各个部门和岗位的职责、分工和技能要求。

7.2.1.1.2 测评方式

访谈，检查。

7.2.1.1.3 测评对象

安全主管，安全管理某方面的负责人，领导小组日常管理工作的负责人，系统管理员，网络管理员，安全员，部门、岗位职责文件，委任授权书，工作记录。

7.2.1.1.4 测评实施

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，是否明确各部门职责分工；

c） 应访谈安全主管，询问是否设立安全管理各个方面的负责人，设置了哪些工作岗位（如安全主管、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、安全员等重要岗位），是否明确各个岗位的职责分工；

d） 应访谈安全主管、安全管理某方面的负责人、信息安全管理委员会或领导小组日常管理工作的负责人、系统管理员、网络管理员和安全员，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是否具有单位主管领导对其最高领导的委任授权书；

g） 应检查信息安全管理委员会职责文件，查看是否明确描述委员会的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（如会议记录/纪要和信息安全工作决策文档等）。

7.2.1.1.5 结果判定

a） 如果7.2.1.1.4 d）被访谈人员表述与文件描述一致，则该项为肯定；

b） 7.2.1.1.4 a）-h）均为肯定，则信息系统符合本单元测评项要求。

7.2.1.2 人员配备

7.2.1.2.1 测评项

a） 应配备一定数量的系统管理人员、网络管理人员、安全管理人员等；

b） 应配备专职安全管理人员不可兼任；

c） 关键岗位应定期轮岗。

7.2.1.2.2 测评方式

访谈，检查。

7.2.1.2.3 测评对象

安全主管，人员配备要求管理文档，管理人员名单。

7.2.1.2.4 测评实施

a） 应访谈安全主管，询问各个安全管理岗位人员（按照岗位职责文件询问，包括机房管理员、系统管理员、数据库管理员、网络管理员、安全员等重要岗位人员）配备情况，包括数量、专职还是兼职等；

b） 应访谈安全主管，询问对哪些关键岗位实行定期轮岗，定期轮岗情况如何，轮岗周期多长，轮岗手续如何；

c） 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、安全员等重要岗位人员并明确应配备专职的安全员；查看是否明确对哪些关键岗位（应有列表）实行定期轮岗并明确轮岗周期、轮岗手续等相关内容；

d） 应检查管理人员名单，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、安全员等重要岗位人员的信息，确认安全员是否是专职人员。

7.2.1.2.5 结果判定

a） 如果7.2.1.2.4 a）设置的安全员是专职的，则该项为肯定；

b） 7.2.1.2.4 a）-d）均为肯定，则信息系统符合本单元测评项要求。

7.2.1.3 授权和审批

7.2.1.3.1 测评项

a） 应授权审批部门及批准人，对关键活动进行审批；

b） 应列表说明须审批的事项、审批部门和可批准人；

c） 应建立各审批事项的审批程序，按照审批程序执行审批过程；

d） 应建立关键活动的双重审批制度；

e） 不再适用的权限应及时取消授权；

f） 应定期审查、更新需授权和审批的项目；

g） 应记录授权过程并保存授权文档。

7.2.1.3.2 测评方式

访谈，检查。

7.2.1.3.3 测评对象

安全主管，关键活动的批准人，授权管理文件，审批文档，审批记录，审查记录，消除授权记录。

7.2.1.3.4 测评实施

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） 应访谈关键活动的批准人，询问其对关键活动的审批范围包括哪些（如网络系统、应用系统、数据库管理系统、重要服务器和设备等重要资源的访问，重要管理制度的制定和发布，人员的配备、培训，产品的采购，第三方人员的访问、管理，与合作单位的合作项目等），审批程序如何；

c） 应检查授权管理文件，查看文件是否包含需审批事项列表，列表是否明确审批事项和双重审批事项、审批部门、批准人及审批程序等（如列表说明哪些事项应经过信息安全领导小组审批，哪些事项应经过安全管理机构审批，哪些关键活动应经过哪些部门双重审批等），文件是否说明应定期审查、更新需审批的项目和审查周期等；

d） 应检查经双重审批的文档，查看是否具有双重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；

f） 应检查审查记录，查看记录日期是否与审查周期一致；

g） 应检查是否具有对不再适用的权限及时取消授权的记录。

7.2.1.3.5 结果判定

a） 7.2.1.3.4 a）-g）均为肯定，则该测评项符合要求。

7.2.1.4 沟通和合作

7.2.1.4.1 测评项

a） 应加强各类管理人员和组织内部机构之间的合作与沟通，定期或不定期召开协调会议，共同协助处理信息安全问题；

b） 信息安全职能部门应定期或不定期召集相关部门和人员召开安全工作会议，协调安全工作的实施；

c） 信息安全领导小组或者安全管理委员会定期召开例会，对信息安全工作进行指导、决策；

d） 应加强与兄弟单位、公安机关、电信公司的合作与沟通，以便在发生安全事件时能够得到及时的支持；

e） 应加强与供应商、业界专家、专业的安全公司、安全组织的合作与沟通，获取信息安全的最新发展动态，当发生紧急事件的时候能够及时得到支持和帮助；

f） 应文件说明外联单位、合作内容和联系方式；

g） 应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。

7.2.1.4.2 测评方式

访谈，检查。

7.2.1.4.3 测评对象

安全主管，安全管理人员，会议文件，会议记录，外联单位说明文档，安全顾问名单。

7.2.1.4.4 测评实施

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），与组织机构内其它部门之间及内部各部门管理人员之间的沟通、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；

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部署安全工作的实施，参加会议的部门和人员有哪些，会议结果如何；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) 应访谈安全管理人员（从系统管理员和安全员等人员中抽查），询问其与外单位人员，与组织机构内其他部门人员，与内部各部门管理人员之间的沟通方式和主要沟通内容有哪些；

e) 应检查部门间协调会议文件或会议记录，查看是否有会议内容、会议时间、参加人员和结果等的描述；

f) 应检查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；

g) 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；

h) 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、兄弟单位、供应商、业界专家、专业的安全公司、安全组织等，是否说明外联单位的联系人和联系方式等内容；

i) 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，查看由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，是否具有由安全顾问签字的相关建议。

7.2.1.4.5 结果判定

a) 7.2.1.4.4 a）-i）均为肯定，则信息系统符合本单元测评项要求。

7.2.1.5 审核和检查

7.2.1.5.1 测评项

a) 应由安全管理人员定期进行安全检查，检查内容包括用户账号情况、系统漏洞情况、系统审计情况等；

b) 应由安全管理部门组织相关人员定期进行全面检查，检查内容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；

c) 应由安全管理部门组织相关人员定期分析、评审异常行为的审计记录，发现可疑行为，形成审计分析报告，并采取必要的应对措施；

d) 应制定安全检查表格实施安全检查，汇总安全检查数据，形成安全检查报告，并对安全检查结果进行通报；

e) 应制定安全审核和安全检查制度规范安全审核和安全检查工作，定期按照程序进行安全审核和安全检查活动。

7.2.1.5.2 测评方式

访谈，检查。

7.2.1.5.3 测评对象

安全主管，安全员，安全检查制度，安全检查报告，审计分析报告，安全检查过程记录，安全检查表格。

7.2.1.5.4 测评实施

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安全检查，检查周期多长，是否定期分析、评审异常行为的审计记录；

b) 应访谈安全员，询问安全检查包含哪些内容，检查人员有哪些，检查程序是否按照系统相关策略和要求进行，是否制定安全检查表格实施安全检查，检查结果如何，是否对检查结果进行通报，通报形式、范围如何；

c) 应检查安全检查制度文档，查看文档是否规定检查内容、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，是否包括用户账号情况、系统漏洞情况、系统审计情况等；

d） 应检查安全检查报告，查看报告日期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；

e） 应检查安全检查过程记录，查看记录的检查程序与文件要求是否一致；

f） 应检查审计分析报告，查看报告日期与检查周期是否一致，报告中是否有分析人员、异常问题和分析结果等的描述，是否对发现的问题提出相应的措施；

g） 应检查是否具有安全检查表格。

7.2.1.5.5 结果判定

a） 7.2.1.5.4 a）-g）均为肯定，则信息系统符合本单元测评项要求。

7.2.2 安全管理制度

7.2.2.1 管理制度

7.2.2.1.1 测评项

a） 应制定信息安全工作的总体方针、政策性文件和安全策略等，说明机构安全工作的总体目标、范围、方针、原则、责任等；

b） 应对安全管理活动中的各类管理内容建立安全管理制度，以规范安全管理活动，约束人员的行为方式；

c） 应对要求管理人员或操作人员执行的日常管理操作，建立操作规程，以规范操作行为，防止操作失误；

d） 应形成由安全政策、安全策略、管理制度、操作规程等构成的全面的信息安全管理制度体系；

e） 应由安全管理职能部门定期组织相关部门和相关人员对安全管理制度体系的合理性和适用性进行审定。

7.2.2.1.2 测评方式

访谈，检查。

7.2.2.1.3 测评对象

安全主管，总体方针、政策性文件和安全策略文件，安全管理制度清单，操作规程，评审记录。

7.2.2.1.4 测评实施

a） 应访谈安全主管，询问机构的制度体系是否由安全政策、安全策略、管理制度、操作规程等构成，是否定期对安全管理制度体系进行评审，评审周期多长；

b） 应检查信息安全工作的总体方针、政策性文件和安全策略文件，查看文件是否明确机构安全工作的总体目标、范围、方针、原则、责任等，是否明确信息系统的安全策略；

c） 应检查安全管理制度清单，查看是否覆盖物理、网络、主机系统、数据、应用、管理等层面；

d） 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；

e） 应检查是否具有安全管理制度体系的评审记录，查看记录日期与评审周期是否一致，是否记录了相关人员的评审意见。

7.2.2.1.5 结果判定

a） 7.2.2.1.4 a）-e）均为肯定，则信息系统符合本单元测评项要求。

7.2.2.2 制定和发布

7.2.2.2.1 测评项

a） 应在信息安全领导小组的负责下，组织相关人员制定；

b） 应保证安全管理制度具有统一的格式风格，并进行版本控制；

c） 应组织相关人员对制定的安全管理制度进行论证和审定；

d) 安全管理制度应经过管理层签发后按照一定的程序以文件形式发布；

e) 安全管理制度应注明发布范围，并对收发文进行登记。

7.2.2.2.2 测评方式

访谈，检查。

7.2.2.2.3 测评对象

安全主管，制度制定和发布要求管理文档，评审记录，安全管理制度，收发登记记录。

7.2.2.2.4 测评实施

a) 应访谈安全主管，询问安全管理制度是否在信息安全领导小组或委员会的总体负责下统一制定，参与制定人员有哪些；

b) 应访谈安全主管，询问安全管理制度的制定程序，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（如召开评审会、函审、内部审核等），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) 应检查安全管理制度文档，查看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，查看收发是否符合规定程序和发布范围要求。

7.2.2.2.5 结果判定

a) 7.2.2.2.4 a）-f）均为肯定，则信息系统符合本单元测评项要求。

7.2.2.3 评审和修订

7.2.2.3.1 测评项

a) 应定期对安全管理制度进行评审和修订，对存在不足或需要改进的安全管理制度进行修订；

b) 当发生重大安全事故、出现新的安全漏洞以及技术基础结构发生变更时，应对安全管理制度进行检查、审定和修订；

c) 每个制度文档应有相应负责人或负责部门，负责对明确需要修订的制度文档的维护。

7.2.2.3.2 测评方式

访谈，检查。

7.2.2.3.3 测评对象

安全主管，管理人员，安全管理制度列表，评审记录，安全管理制度对应负责人或负责部门的清单。

7.2.2.3.4 测评实施

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，由何部门/何人负责；

b) 应访谈管理人员（负责定期评审、修订和日常维护的人员），询问定期对安全管理制度的评审、修订情况和日常维护情况，评审周期多长，评审、修订程序如何，维护措施如何；

c) 应访谈管理人员（负责人员），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) 应检查安全管理制度评审记录，查看记录日期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；

e） 应检查是否具有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对安全管理制度进行审定的记录；

f） 应检查是否具有需要定期修订的安全管理制度列表，查看列表是否注明评审周期；

g） 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。

7.2.2.3.5 结果判定

a） 7.2.2.3.4 a）-g）均为肯定，则信息系统符合本单元测评项要求。

7.2.3 人员安全管理

7.2.3.1 人员录用

7.2.3.1.1 测评项

a） 应保证被录用人具备基本的专业技术水平和安全管理知识；

b） 应对被录用人的身份、背景、专业资格和资质进行审查；

c） 应对被录用人所具备的技术技能进行考核；

d） 应对被录用人说明其角色和职责；

e） 应签署保密协议；

f） 对从事关键岗位的人员应从内部人员选拔，并定期进行信用审查；

g） 对从事关键岗位的人员应签署岗位安全协议。

7.2.3.1.2 测评方式

访谈，检查。

7.2.3.1.3 测评对象

人事负责人，人事工作人员，人员录用要求管理文档，人员审查文档或记录，考核文档或记录，保密协议，岗位安全协议，审查记录。

7.2.3.1.4 测评实施

a） 应访谈人事负责人，询问在人员录用时对人员条件有哪些要求，目前录用的安全管理和技术人员是否有能力完成与其职责相对应的工作；

b） 应访谈人事工作人员，询问在人员录用时是否对被录用人的身份、背景、专业资格和资质进行审查，对技术人员的技术技能进行考核，录用后是否与其签署保密协议，是否对其说明工作职责；

c） 应访谈人事负责人，询问对从事关键岗位的人员是否从内部人员中选拔，是否要求其签署岗位安全安全协议，是否定期对关键岗位人员进行信用审查，审查周期多长；

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；

i） 应检查信用审查记录，查看是否记录了审查内容和审查结果等，查看审查时间与审查周期是否一致。

7.2.3.1.5 结果判定

a） 7.2.3.1.4 a）-i）均为肯定，则信息系统符合本单元测评项要求。

7.2.3.2 人员离岗

7.2.3.2.1 测评项

a) 应立即终止由于各种原因即将离岗的员工的所有访问权限；
b) 应取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备；
c) 应经机构人事部门办理严格的调离手续，并承诺调离后的保密义务后方可离开。

7.2.3.2.2 测评方式

访谈，检查。

7.2.3.2.3 测评对象

安全主管，人事工作人员，人员离岗管理文档，保密承诺文档。

7.2.3.2.4 测评实施

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、徽章等以及机构提供的软硬件设备等；
b) 应访谈人事工作人员，询问调离手续包括哪些，是否要求调离人员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，查看是否规定了调离手续和离岗要求等；
d) 应检查是否具有交还身份证件和设备等的记录；
e) 应检查保密承诺文档，查看是否有调离人员的签字。

7.2.3.2.5 结果判定

a) 7.2.3.2.4 a）-e）均为肯定，则信息系统符合本单元测评项要求。

7.2.3.3 人员考核

7.2.3.3.1 测评项

a) 应对所有人员进行全面、严格的安全审查；
b) 应定期对各个岗位的人员进行安全技能及安全认知的考核；
c) 应对考核结果进行记录并保存；
d) 应对违背安全策略和规定的人员进行惩戒。

7.2.3.3.2 测评方式

访谈，检查。

7.2.3.3.3 测评对象

安全主管，人事工作人员，人员考核记录。

7.2.3.3.4 测评实施

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) 应访谈人事工作人员，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（如操作行为、社会关系、社交活动等），是否全面；
c) 应访谈人事工作人员，询问对违背安全策略和规定的人员有哪些惩戒措施；
d) 应检查考核记录，查看记录的考核人员是否包括各个岗位的人员，考核内容是否包含安全知识、安全技能等；查看记录日期与考核周期是否一致。

7.2.3.3.5 结果判定

a) 如果7.2.3.3.4 b）被访谈人员表述审查内容包含社会关系、社交活动、操作行为等各个方面，则该项为肯定；
b) 如果7.2.3.3.4 c）被访谈人员表述与文件描述一致，则该项为肯定；
c) 7.2.3.3.4 a）-d）均为肯定，则信息系统符合本单元测评项要求。

7.2.3.4 安全意识教育和培训

7.2.3.4.1 测评项

a) 应对各类人员进行安全意识教育；

b) 应告知人员相关的安全责任和惩戒措施；

c) 应制定安全教育和培训计划，对信息安全基础知识、岗位操作规程等进行培训；

d) 应针对不同岗位制定不同培训计划；

e) 应对安全教育和培训的情况和结果进行记录并归档保存。

7.2.3.4.2 测评方式

访谈，检查。

7.2.3.4.3 测评对象

安全主管，安全员，系统管理员，网络管理员，数据库管理员，培训计划，培训记录。

7.2.3.4.4 测评实施

a) 应访谈安全主管，询问是否制定安全教育和培训计划并按计划对各个岗位人员进行安全教育和培训，以什么形式进行，效果如何；

b) 应访谈安全员、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目的、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；查看记录与培训计划是否一致。

7.2.3.4.5 结果判定

a) 如果7.2.3.4.4 b）访谈人员能够表述清楚询问内容，且安全职责、惩戒措施和岗位操作规程表述与文件描述一致，则该项为肯定；

b) 7.2.3.4.4 a）-d）均为肯定，则信息系统符合本单元测评项要求。

7.2.3.5 第三方人员访问管理

7.2.3.5.1 测评项

a) 第三方人员应在访问前与机构签署安全责任合同书或保密协议；

b) 对重要区域的访问，须提出书面申请，批准后由专人全程陪同或监督，并记录备案；

c) 对第三方人员允许访问的区域、系统、设备、信息等内容应进行书面的规定，并按照规定执行。

7.2.3.5.2 测评方式

访谈，检查。

7.2.3.5.3 测评对象

安全主管，安全管理人员，安全责任合同书或保密协议，第三方人员访问管理文档，访问批准文档，登记记录。

7.2.3.5.4 测评实施

a) 应访谈安全主管，询问对第三方人员（如向系统提供服务的系统软、硬件维护人员，业务合作伙伴、评估人员等）的访问采取哪些管理措施，是否要求第三方人员访问前与机构签署安全责任合同书或保密协议；

b) 应访谈安全管理人员，询问对第三方人员访问重要区域（如访问主机房、重要服务器或设备、保密文档等）采取哪些措施，是否经有关负责人书面批准，是否由专人全程陪同或监督，是否进行记录并备案管理；

c） 应检查安全责任合同书或保密协议，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。

d） 应检查第三方人员访问管理文档，查看是否明确第三方人员包括哪些人员，允许第三方人员访问的范围（区域、系统、设备、信息等内容），第三方人员进入条件（对哪些重要区域的访问须提出书面申请批准后方可进入），第三方人员进入的访问控制（由专人全程陪同或监督等）和第三方人员的离开条件等；

e） 应检查第三方人员访问重要区域批准文档，查看是否有第三方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；

f） 应检查第三方人员访问重要区域的登记记录，查看记录是否描述了第三方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。

7.2.3.5.5 结果判定

a） 7.2.3.5.4 a）-f）均为肯定，则该测评项符合要求。

7.2.4 系统建设管理

7.2.4.1 系统定级

7.2.4.1.1 测评项

a） 应明确信息系统划分的方法；

b） 应确定信息系统的安全保护等级；

c） 应以书面的形式定义确定了安全保护等级的信息系统的属性，包括使命、业务、网络、硬件、软件、数据、边界、人员等；

d） 应以书面的形式说明确定一个信息系统为某个安全保护等级的方法和理由；

e） 应组织相关部门和有关安全技术专家对信息系统的定级结果的合理性和正确性进行论证和审定；

f） 应确保信息系统的定级结果经过相关部门的批准。

7.2.4.1.2 测评方式

访谈，检查。

7.2.4.1.3 测评对象

安全主管，系统划分文档，系统定级文档，专家论证文档，系统属性说明文档。

7.2.4.1.4 测评实施

a） 应访谈安全主管，询问划分信息系统的方法和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，是否对其进行明确描述；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（如上级主管部门）的批准；

b） 应检查系统划分文档，查看文档是否明确描述信息系统划分的方法和理由；

c） 应检查系统定级文档，查看文档是否给出信息系统的安全保护等级，是否明确描述确定信息系统为某个安全保护等级的方法和理由，是否给出安全等级保护措施组成SxCyGz值；查看定级结果是否有相关部门的批准盖章；

d） 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；

e） 应检查系统属性说明文档，查看文档是否明确了系统使命、业务、网络、硬件、软件、数据、边界、人员等。

7.2.4.1.5 结果判定

a） 7.2.4.1.4 a）没有上级主管部门的，如果有安全主管的批准，则该项为肯定；

b） 7.2.4.1.4 b）-e）均为肯定，则信息系统符合本单元测评项要求。

a）

7.2.4.2 安全方案设计

7.2.4.2.1 测评项

a) 应根据系统的安全级别选择基本安全措施，依据风险评估的结果补充和调整安全措施；

b) 应指定和授权专门的部门对信息系统的安全建设进行总体规划，制定近期和远期的安全建设工作计划；

c) 应根据信息系统的等级划分情况，统一考虑安全保障体系的总体安全策略、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，并形成配套文件；

d) 应组织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合理性和正确性进行论证和审定；

e) 应确保总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等文件必须经过批准，才能正式实施；

f) 应根据安全测评、安全评估的结果定期调整和修订总体安全策略、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。

7.2.4.2.2 测评方式

访谈，检查。

7.2.4.2.3 测评对象

安全主管，系统建设负责人，总体安全策略文档，安全技术框架，安全管理策略文档，总体建设规划书，详细设计方案，专家论证文档，维护记录。

7.2.4.2.4 测评实施

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/何人负责；

b) 应访谈系统建设负责人，询问是否制定近期和远期的安全建设工作计划，是否根据系统的安全级别选择基本安全措施，是否依据风险评估的结果补充和调整安全措施，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，统一考虑安全保障体系的总体安全策略、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；

d) 应访谈系统建设负责人，询问是否组织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、安全管理策略等相关配套文件进行论证和审定，并经过管理部门的批准；

e) 应访谈系统建设负责人，询问是否根据安全测评、安全评估的结果定期调整和修订总体安全策略、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，维护周期多长；

f) 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；

g) 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；

h) 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；

i） 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，查看记录日期与维护周期是否一致。

7.2.4.2.5 结果判定

a） 7.2.4.3.4 a）-i）均为肯定，则信息系统符合本单元测评项要求。

7.2.4.3 产品采购

7.2.4.3.1 测评项

a） 应确保安全产品的使用符合国家的有关规定；

b） 应确保密码产品的使用符合国家密码主管部门的要求；

c） 应指定或授权专门的部门负责产品的采购；

d） 应制定产品采购方面的管理制度明确说明采购过程的控制方法和人员行为准则；

e） 应预先对产品进行选型测试，确定产品的候选范围，并定期审定和更新候选产品名单；

7.2.4.3.2 测评方式

访谈，检查。

7.2.4.3.3 测评对象

安全主管，系统建设负责人，产品采购管理制度，产品选型测试结果记录，候选产品名单审定记录。

7.2.4.3.4 测评实施

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，询问系统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制度，查看内容是否明确采购过程的控制方法（如采购前对产品做选型测试，明确需要的产品性能指标，确定产品的候选范围，通过招投标方式确定采购产品等）和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（边界安全设备、重要服务器操作系统、数据库等）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，例如《商用密码管理条例》规定任何单位只能使用经过国家密码管理机构认可的商用密码产品，商用密码产品发生故障，必须有国家密码管理机构指定的单位维修，报废商用密码产品应向国家密码管理机构备案，《计算机信息系统保密工作暂行规定》规定涉密系统配置合格的保密专用设备，所采取的保密措施应与所处理信息的密级要求相一致等；

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。

7.2.4.3.5 结果判定

a） 如果7.2.4.4.4 c）访谈说明没有采用密码产品，则测评实施c）、f）为不适用；

b） 7.2.4.4.4 a）-g）均为肯定，则信息系统符合本单元测评项要求。

7.2.4.4 自行软件开发

7.2.4.4.1 测评项

a） 应确保开发环境与实际运行环境物理分开；

b） 应确保系统开发文档由专人负责保管，系统开发文档的使用受到控制；
c） 应制定开发方面的管理制度明确说明开发过程的控制方法和人员行为准则；
d） 应确保开发人员和测试人员的分离，测试数据和测试结果受到控制；
e） 应确保提供软件设计的相关文档和使用指南；
f） 应确保对程序资源库的修改、更新、发布进行授权和批准；

7.2.4.4.2 测评方式

访谈，检查。

7.2.4.4.3 测评对象

系统建设负责人，软件设计相关文档和使用指南，审批文档或记录，文档使用控制记录。

7.2.4.4.4 测评实施

a） 应访谈系统建设负责人，询问系统是否自主开发软件，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，软件开发是否有相应的控制措施，是否要求开发人员不能做测试人员（即二者分离），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，询问系统开发文档是否由专人负责保管，负责人是何人，如何控制使用（如限制使用人员范围并做使用登记等），测试数据和测试结果是否受到控制；
c） 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、源代码说明文档等)和软件使用指南或操作手册和维护手册等；
d） 应检查软件开发环境与系统运行环境在物理上是否是分开的；
e） 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；
f） 应检查是否具有系统软件开发相关文档（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。

7.2.4.4.5 结果判定

a） 7.2.4.5.4 a）-f）均为肯定，则信息系统符合本单元测评项要求。

7.2.4.5 外包软件开发

7.2.4.5.1 测评项

a） 应与软件开发单位签订协议，明确知识产权的归属和安全方面的要求；
b） 应根据协议的要求检测软件质量；
c） 应在软件安装之前检测软件包中可能存在的恶意代码；
d） 应要求开发单位提供技术培训和服务承诺；
e） 应要求开发单位提供软件设计的相关文档和使用指南。

7.2.4.5.2 测试方法

访谈，检查。

7.2.4.5.3 测试对象

系统建设负责人，软件开发安全协议，软件开发文档，软件培训文档。

7.2.4.5.4 测评实施

a） 应访谈系统建设负责人，询问在外包软件前是否对软件开发单位以书面文档形式（如软件开发安全协议）规范软件开发单位的责任、开发过程中的安全行为、开发环境要求、软件质量、开发后的服务承诺等内容；
b） 应访谈系统建设负责人，询问是否具有独立对软件进行日常维护和使用所需的文档，开发单位是否为软件的正常运行和维护提供过技术支持，以何种方式进行；
c） 应访谈系统建设负责人，询问软件交付前是否依据开发协议的技术指标对软件功能

和性能等进行验收检测，验收检测是否是由开发商和委托方共同参与；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；

d) 应检查软件开发协议，查看其是否规定知识产权归属、安全行为等内容；

e) 应检查是否具有需求分析说明书、软件设计说明书、软件操作手册等开发文档以及用户培训计划、程序员培训手册等后期技术支持文档。

7.2.4.5.5 结果判定

a) 7.2.4.6.4 a）—e）均为肯定，则信息系统符合本单元测评项要求。

7.2.4.6 工程实施

7.2.4.6.1 测评项

a) 应与工程实施单位签订与安全相关的协议，约束工程实施单位的行为；

b) 应指定或授权专门的人员或部门负责工程实施过程的管理；

c) 应制定详细的工程实施方案控制实施过程，并要求工程实施单位能正式地执行安全工程过程；

d) 应制定工程实施方面的管理制度明确说明实施过程的控制方法和人员行为准则。

7.2.4.6.2 测试方法

访谈，检查。

7.2.4.6.3 测试对象

系统建设负责人，工程安全建设协议，工程实施方案，工程实施管理制度。

7.2.4.6.4 测评实施

a) 应访谈系统建设负责人，询问是否以书面形式（如工程安全建设协议）约束工程实施方的工程实施行为；

b) 应访谈系统建设负责人，询问是否指定专门人员或部门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，是否将控制方法和工程人员行为规范制度化，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；

c) 应检查工程安全建设协议，查看其是否规定工程实施方的责任、任务要求、质量要求等方面内容，约束工程实施行为；

d) 应检查工程实施方案，查看其是否规定工程时间限制、进度控制、质量控制等方面内容，工程实施过程是否按照实施方案形成各种文档，如阶段性工程报告；

e) 应检查工程实施管理制度，查看其是否规定工程实施过程的控制方法（如内部阶段性控制或外部监理单位控制）、实施参与人员的各种行为等方面内容。

7.2.4.6.5 结果判定

a) 7.2.4.7.4 a）—e）均为肯定，则信息系统符合本单元测评项要求。

7.2.4.7 测试验收

7.2.4.7.1 测评项

a) 应对系统进行安全性测试验收；

b) 应在测试验收前根据设计方案或合同要求等制订测试验收方案，测试验收过程中详细记录测试验收结果，形成测试验收报告；

c) 应委托公正的第三方测试单位对系统进行测试，并出具测试报告；

d) 应制定系统测试验收方面的管理制度明确说明系统测试验收的控制方法和人员行为准则；

e) 应指定或授权专门的部门负责系统测试验收的管理，并按照管理制度的要求完成系统测试验收工作；

f) 应组织相关部门和相关人员对系统测试验收报告进行审定，没有疑问后由双方签字。

7.2.4.7.2 测试方法

访谈，检查。

7.2.4.7.3 测试对象

系统建设负责人，测试方案，测试记录，测试报告，验收报告，验收测试管理制度。

7.2.4.7.4 测评实施

a) 应访谈系统建设负责人，询问在信息系统正式运行前，是否委托第三方测试机构根据设计方案或合同要求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，询问是否指定专门部门负责测试验收工作，由何部门负责，是否对测试过程（包括测试前、测试中和测试后）进行文档化要求和制度化要求；

c) 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测试报告进行符合性审定；

d) 应检查工程测试方案，查看其是否对参与测试部门、人员、现场操作过程等进行要求；查看测试记录是否详细记录了测试时间、人员、操作过程、测试结果等方面内容；查看测试报告是否提出存在问题及改进意见等；

e) 应检查是否具有系统验收报告；

f) 应检查验收测试管理制度是否对系统验收测试的过程控制、参与人员的行为等进行规定。

7.2.4.7.5 结果判定

a) 7.2.4.8.4 a）—f）均为肯定，则信息系统符合本单元测评项要求。

7.2.4.8 系统交付

7.2.4.8.1 测评项

a) 应明确系统的交接手续，并按照交接手续完成交接工作；

b) 应由系统建设方完成对委托建设方的运维技术人员的培训；

c) 应由系统建设方提交系统建设过程中的文档和指导用户进行系统运行维护的文档；

d) 应由系统建设方进行服务承诺，并提交服务承诺书，确保对系统运行维护的支持；

e) 应制定系统交付方面的管理制度明确说明系统交付的控制方法和人员行为准则；

f) 应指定或授权专门的部门负责系统交付的管理工作，并按照管理制度的要求完成系统交付工作。

7.2.4.8.2 测试方法

访谈，检查。

7.2.4.8.3 测试对象

系统建设负责人，系统交付清单，服务承诺书，系统培训记录，系统交付管理制度。

7.2.4.8.4 测评实施

a) 应访谈系统建设负责人，询问交接手续是什么，系统交接工作是否由专门部门按照该手续办理，是否根据交付清单对所交接的设备、文档、软件等进行清点，交付清单是否满足合同的有关要求；是否对交付工作进行制度化要求；

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，系统建设实施方是否对运维技术人员进行过培训，针对哪些方面进行过培训，是否以书面形式承诺对系统运行维护提供一定的技术支持服务，是否按照服务承诺书的要求进行过技术支持，以何形式进行，系统是否具有支持其独立运行维护所需的文档；

c) 应检查系统交付清单，查看其是否具有系统建设文档（如系统建设方案）、指导用户进行系统运维的文档（如服务器操作规程书）以及系统培训手册等文档名称；

d) 应检查是否具有系统建设方的服务承诺书和对系统进行的培训记录；

e） 应检查系统交付管理制度，查看其是否规定了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。

7.2.4.8.5 结果判定

a) 7. 2. 4. 9. 4 a）—e）均为肯定，则信息系统符合本单元测评项要求。

7.2.4.9 系统备案

7.2.4.9.1 测评项

a） 应将系统定级、系统属性等材料指定专门的人员或部门负责管理，并控制这些材料的使用；

b） 应将系统等级和系统属性等资料报系统主管部门备案；

c） 应将系统等级、系统属性、等级划分理由及其他要求的备案材料报相应公安机关备案。

7.2.4.9.2 测评方式

访谈，检查。

7.2.4.9.3 测评对象

安全主管，文档管理员，备案记录。

7.2.4.9.4 测评实施

a） 应访谈安全主管，询问是否有专门的人员或部门负责管理系统定级、系统属性等文档，由何部门/何人负责；

b） 应访谈文档管理员，询问对系统定级、系统属性等文档采取哪些控制措施（如限制使用范围、使用登记记录等）；

c） 应检查是否具有将系统定级文档和系统属性说明文件等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、系统属性和等级划分理由等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文档和系统属性说明文件等相关材料的使用控制记录。

7.2.4.9.5 结果判定

7.2.4.2.4 c）-e）为肯定，则信息系统符合本单元测评项要求。

7.2.4.10 安全服务商选择

7.2.4.10.1 测评项

a） 应确保安全服务商的选择符合国家的有关规定。

7.2.4.10.2 测试方法

访谈。

7.2.4.10.3 测试对象

系统建设负责人。

7.2.4.10.4 测评实施

a） 应访谈系统建设负责人，询问对信息系统进行安全规划、设计、实施、维护、测评等服务的安全服务单位是否符合国家有关规定。

7.2.4.10.5 结果判定

a） 7. 2. 4. 10. 4 a）为肯定，则信息系统符合本单元测评项要求。

7.2.5 系统运维管理

7.2.5.1 环境管理

7.2.5.1.1 测评项

a） 应对机房供配电、空调、温湿度控制等设施指定专人或专门的部门定期进行维护管理；

b） 应配备机房安全管理人员，对机房的出入、服务器的开机或关机等工作进行管理；
c） 应建立机房安全管理制度，对有关机房物理访问，物品带进、带出机房和机房环境安全等方面作出规定；
d） 应加强对办公环境的保密性管理，包括如工作人员调离办公室应立即交还该办公室钥匙和不在办公区接待来访人员等；
e） 应有指定的部门负责机房安全，并配置电子门禁系统，对机房来访人员实行登记记录和电子记录双重备案管理；
f） 应对办公环境的人员行为，如工作人员离开座位应确保终端计算机退出登录状态和桌面上没有包含敏感信息的纸档文件等作出规定。

7.2.5.1.2 测评方式

访谈，检查。

7.2.5.1.3 测评对象

物理安全负责人，机房值守人员，机房工作人员，机房安全管理制度，办公环境管理文档，设备维护记录，机房进出登记表，机房电子门禁系统及其电子记录。

7.2.5.1.4 测评实施

a） 应访谈物理安全负责人，询问是否指定专人或部门对机房基本设施（如空调、供配电设备等）进行定期维护，由何部门/何人负责，维护周期多长；
b） 应访谈物理安全负责人，询问是否指定人员负责机房安全管理工作，对机房进出管理是否要求制度化和文档化；
c） 应访谈机房值守人员，询问对外来人员进出机房是否采用人工记录和电子记录双重控制；
d） 应访谈工作人员，询问对办公环境的保密性要求事项；
e） 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、机房环境安全等方面；
f） 应检查办公环境管理文档，查看其内容是否对工作人员离开座位后的保密行为（如清理桌面文件和屏幕锁定等）、人员调离办公室后的行为等方面进行规定；
g） 应检查机房进出登记表，查看是否记录外来人员进出时间、人员姓名、访问原因等内容；查看是否具有电子门禁系统，电子记录文档是否有时间、人员等信息；
h） 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。

7.2.5.1.5 结果判定

a） 如果7.2.5.1.4 c）中访谈人员能够表述出针对办公环境保密性注意事项（如离开座位后应退出登录，并收好敏感性文件等），则该项为肯定；
b） 7.2.5.1.4 a）-h）均为肯定，则信息系统符合本单元测评项要求。

7.2.5.2 资产管理

7.2.5.2.1 测评项

a） 应建立资产安全管理制度，规定信息系统资产管理的责任人员或责任部门，并规范资产管理和使用的行为；
b） 应编制并保存与信息系统相关的资产、资产所属关系、安全级别和所处位置等信息的资产清单；
c） 应根据资产的重要程度对资产进行定性赋值和标识管理，根据资产的价值选择相应的管理措施；
d） 应规定信息分类与标识的原则和方法，并对信息的使用、存储和传输作出规定。

7.2.5.2.2 测评方式

访谈，检查。

7.2.5.2.3 测评对象

安全主管，物理安全负责人，资产管理员，资产清单，资产安全管理制度，信息分类标识文档，设备。

7.2.5.2.4 测评实施

a) 应访谈安全主管，询问是否指定资产管理的责任人员或部门,由何部门/何人负责；
b) 应访谈物理安全负责人，询问是否对资产管理要求文档化和制度化；
c) 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赋值和标识管理，不同类别的资产是否采取不同的管理措施；
d) 应检查资产清单，查看其内容是否覆盖资产责任人、所属级别、所处位置、所属部门等方面；
e) 应检查资产安全管理制度，查看其内容是否覆盖资产使用、借用、维护等方面；
f) 应检查信息分类文档，查看其内容是否规定了分类标识的原则和方法（如根据信息的重要程度、敏感程度或用途不同进行分类）；
g) 应检查资产清单中的设备，查看其是否具有相应标识。

7.2.5.2.5 结果判定

a) 如果7.2.5.2.4 c）中访谈人员能够描述出不同的资产管理措施，则该项为肯定；
b) 如果7.2.5.2.4 g）中设备标识与信息分类标识文档中所要求的一致，则该项为肯定；
c) 7.2.5.2.4 a）-g）均为肯定，则信息系统符合本单元测评项要求。

7.2.5.3 介质管理

7.2.5.3.1 测评项

a) 应建立介质安全管理制度，对介质的存放环境、使用、维护和销毁等方面作出规定；
b) 应有介质的归档和查询记录，并对存档介质的目录清单定期盘点；
c) 对于需要送出维修或销毁的介质，应首先清除介质中的敏感数据，防止信息的非法泄漏；
d) 应根据数据备份的需要对某些介质实行异地存储，存储地的环境要求和管理方法应与本地相同；
e) 应根据所承载数据和软件的重要程度对介质进行分类和标识管理，并实行存储环境专人管理；
f) 应对介质的物理传输过程中人员选择、打包、交付等情况进行控制；
g) 应对存储介质的使用过程、送出维修以及销毁进行严格的管理，保密性较高的信息存储介质未经批准不得自行销毁；
h) 必要时应对重要介质的数据和软件采取加密存储，对带出工作环境的存储介质进行内容加密和监控管理；
i) 应对存放在介质库中的介质定期进行完整性和可用性检查，确认其数据或软件没有受到损坏或丢失。

7.2.5.3.2 测评方式

访谈，检查。

7.2.5.3.3 测评对象

资产管理员，介质管理记录，介质安全管理制度，各类介质，介质存放地，异地存放地。

7.2.5.3.4 测评实施

a) 应访谈资产管理员，询问介质的存放环境是否有保护措施，防止其被盗、被毁、被未授权修改以及信息的非法泄漏，是否有专人管理；

b) 应访谈资产管理员，询问是否对介质的使用管理要求制度化和文档化，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（如送出维修或销毁）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是否对数据进行净化处理；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（如采用防拆包装置）、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、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；

h) 应检查介质本地存放地的实际环境条件是否安全，异地存放地的环境要求和管理要求是否与本地相同，是否有专人对存放地进行管理。

7.2.5.3.5 结果判定

a) 7.2.5.3.4 a）-h）均为肯定，则信息系统符合本单元测评项要求。

7.2.5.4 设备管理

7.2.5.4.1 测评项

a) 应对信息系统相关的各种设备、线路等指定专人或专门的部门定期进行维护管理；

b) 应对信息系统的各种软硬件设备的选型、采购、发放或领用等过程建立基于申报、审批和专人负责的管理制度；

c) 应对终端计算机、工作站、便携机、系统和网络等设备的操作和使用进行规范化管理；

d) 应对带离机房或办公地点的信息处理设备进行控制；

e) 应按操作规程实现服务器的启动/停止、加电/断电等操作，加强对服务器操作的日志文件管理和监控管理，并对其定期进行检查；

f) 应建立配套设施、软硬件维护方面的管理制度，对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等；

g) 应在安全管理机构统一安全策略下对服务器进行系统配置和服务设定，并实施配置管理。

7.2.5.4.2 测评方式

访谈，检查。

7.2.5.4.3 测评对象

资产管理员，系统管理员，审计员，设备审批管理文档，设备操作规程，设备使用管理文档，设施、软硬件维护管理制度，设备维护记录，服务器操作日志，配置文档。

7.2.5.4.4 测评实施

a) 应访谈资产管理员，询问是否对各类设施、设备指定专人或专门部门进行定期维护，由何部门/何人维护，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（如选型、采购、发放等）进行审批控制，是否对设备带离机构进行审批控制，设备的操作和使用是否要求规范化管理；

c) 应访谈系统管理员，询问其是否在统一安全策略下，对服务器进行正确配置，对服务器的操作是否按操作规程进行；

d) 应访谈系统管理员，询问其是否对软硬件维护进行制度化管理；

e) 应访谈审计员，询问对服务器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；

f) 应检查设备审批、发放管理文档，查看其是否对设备选型、采购、发放以及带离机构等环节的申报和审批作出规定；查看是否具有设备的选型、采购、发放等过程的申报材料和审批报告；

g) 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；

h) 应检查服务器操作规程，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；

i) 应检查软硬件维护制度，查看其是否覆盖维护人员的责任、涉外维修和服务的审批、维修过程的监督控制等方面。

7.2.5.4.5 结果判定

a) 7.2.5.4.4 a）-i）均为肯定，则信息系统符合本单元测评项要求。

7.2.5.5 监控管理

7.2.5.5.1 测评项

a) 应进行主机运行监视，包括监视主机的CPU、硬盘、内存和网络等资源的使用情况；

b) 应对分散或集中的安全管理系统的访问授权、操作记录、日志等方面进行有效管理；

c) 应严格管理运行过程文档，其中包括责任书、授权书、许可证、各类策略文档、事故报告处理文档、安全配置文档、系统各类日志等，并确保文档的完整性和一致性。

7.2.5.5.2 测评方式

访谈，检查。

7.2.5.5.3 测评对象

系统运维负责人，监控记录文档。

7.2.5.5.4 测评实施

a) 应访谈系统运维负责人，询问其是否监控主要服务器的各项资源指标，如CPU、内存、进程和磁盘等使用情况；

b) 应访谈系统运维负责人，询问目前信息系统是否由机构自身负责运行维护，如果是，系统运行所产生的文档如何进行管理（如责任书、授权书、许可证、各类策略文档、事故报告处理文档、安全配置文档、系统各类日志等）；

c) 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。

7.2.5.5.5 结果判定

a) 7.2.5.5.4 a）-c）均为肯定，则信息系统符合本单元测评项要求。

7.2.5.6 网络安全管理

7.2.5.6.1 测评项

a) 应指定专人对网络进行管理，负责运行日志、网络监控记录的日常维护和报警信息分析和处理工作；

b) 应根据厂家提供的软件升级版本对网络设备进行更新，并在更新前对现有的重要文件进行备份；

c） 应进行网络系统漏洞扫描，对发现的网络系统安全漏洞进行及时的修补；
d） 应保证所有与外部系统的连接均应得到授权和批准；
e） 应建立网络安全管理制度，对网络安全配置、网络用户以及日志等方面作出规定；
f） 应对网络设备的安全策略、授权访问、最小服务、升级与打补丁、维护记录、日志以及配置文件的生成、备份、变更审批、符合性检查等方面做出具体要求；
g） 应规定网络审计日志的保存时间以便为可能的安全事件调查提供支持；
h） 应明确各类用户的责任、义务和风险，并按照机构制定的审查和批准程序建立用户和分配权限，定期检查用户实际权限与分配权限的符合性；
i） 应对日志的备份、授权访问、处理、保留时间等方面做出具体规定，使用统一的网络时间，以确保日志记录的准确；
j） 应通过身份鉴别、访问控制等严格的规定限制远程管理账户的操作权限和登录行为；
k） 应定期检查违反规定拨号上网或其他违反网络安全策略的行为。

7.2.5.6.2 测试方法

访谈，检查。

7.2.5.6.3 测试对象

安全主管，安全员，网络管理员，审计员，网络漏洞扫描报告，网络安全管理制度，系统外联授权书，网络审计日志。

7.2.5.6.4 测评实施

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；
b） 应访谈安全员，询问是否对网络安全的管理工作（包括网络安全配置、网络用户、日志等方面）制度化；
c） 应访谈安全员，询问网络的外联种类有哪些（互联网、合作伙伴企业网、上级部门网络等），是否都得到授权与批准，由何部门/何人批准；是否定期检查违规联网的行为；
d） 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（帐户数据和配置数据等）进行备份，采取什么方式进行；是否对网络设备进行过漏洞扫描，对扫描出的漏洞是否及时修补；
e） 应检查网络漏洞扫描报告，查看其内容是否覆盖网络存在的漏洞、严重级别、原因分析、改进意见等方面；
f） 应检查网络安全管理制度，查看其内容是否覆盖网络安全配置（包括网络设备的安全策略、授权访问、最小服务、升级与打补丁）、网络帐户（用户责任、义务、风险、权限审批、权限分配、帐户注销等）、审计日志以及配置文件的生成、备份、变更审批、符合性检查等方面；
g） 应检查是否具有内部网络所有外联的授权批准书；
h） 应检查在规定的保存时间范围内是否存在网络审计日志；

7.2.5.6.5 结果判定

a） 7.2.5.6.4 a）-h）均为肯定，则信息系统符合本单元测评项要求。

7.2.5.7 系统安全管理

7.2.5.7.1 测评项

a） 应指定专人对系统进行管理，删除或者禁用不使用的系统缺省账户；

b） 应制定系统安全管理制度，对系统安全配置、系统帐户以及审计日志等方面作出规定；

c） 应对能够使用系统工具的人员及数量进行限制和控制；

d） 应定期安装系统的最新补丁程序，并根据厂家提供的可能危害计算机的漏洞进行及时修补，并在安装系统补丁前对现有的重要文件进行备份；

e） 应根据业务需求和系统安全分析确定系统的访问控制策略，系统访问控制策略用于控制分配信息系统、文件及服务的访问权限；

f） 应对系统账户进行分类管理，权限设定应当遵循最小授权要求；

g） 应对系统的安全策略、授权访问、最小服务、升级与打补丁、维护记录、日志以及配置文件的生成、备份、变更审批、符合性检查等方面做出具体要求；

h） 应规定系统审计日志的保存时间以便为可能的安全事件调查提供支持；

i） 应进行系统漏洞扫描，对发现的系统安全漏洞进行及时的修补；

j） 应明确各类用户的责任、义务和风险，对系统账户的登记造册、用户名分配、初始口令分配、用户权限及其审批程序、系统资源分配、注销等作出规定；

k） 应对于账户安全管理的执行情况进行检查和监督，定期审计和分析用户账户的使用情况，对发现的问题和异常情况进行相关处理。

7.2.5.7.2 测试方法

访谈，检查。

7.2.5.7.3 测试对象

安全主管，安全员，系统管理员，审计员，系统安全管理制度，系统审计日志，系统漏洞扫描报告。

7.2.5.7.4 测评实施

a） 应访谈安全主管，询问是否指定专人负责系统安全管理；

b） 应访谈系统管理员，询问对系统工具的使用（如脆弱性扫描工具）是否采取措施控制不同使用人员及数量；

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，是否在测试环境中测试其对应用系统的影响；在安装系统补丁前是否对重要文件（系统配置、系统用户数据等）进行备份，采取什么方式进行；是否对系统进行过漏洞扫描，发现漏洞是否进行及时修补；

d） 应访谈安全员，询问是否将系统安全管理工作（包括系统安全配置、系统帐户、审计日志等）制度化；

e） 应访谈系统管理员，询问对不常用的系统缺省用户是否采取了一定的处理手段阻止其继续使用（如删除或禁用）；是否对系统帐户安全管理情况是否定期进行检查和分析，发现问题如何处理；

f） 应访谈审计员，询问是否规定系统审计日志保存时间，多长时间；

g） 应检查在规定的保存时间范围内是否存在系统审计日志；

h） 应检查系统漏洞扫描报告，查看其内容是否覆盖系统存在的漏洞、严重级别、原因分析、改进意见等方面；

i） 应检查系统安全管理制度，查看其内容是否覆盖系统安全配置（包括系统的安全策略、授权访问、最小服务、升级与打补丁）、系统帐户（用户责任、义务、风险、权限审批、权限分配、帐户注销等）、审计日志以及配置文件的生成、备份、变更审批、符合性检查等方面。

7.2.5.7.5 结果判定

a） 7.2.5.7.4 a）-i）均为肯定，则信息系统符合本单元测评项要求。

7.2.5.8 恶意代码防范管理

7.2.5.8.1 测评项

a) 应提高所有用户的防病毒意识，告知及时升级防病毒软件；

b) 应在读取移动存储设备（如软盘、移动硬盘、光盘）上的数据以及网络上接收文件或邮件之前，先进行病毒检查，对外来计算机或存储设备接入网络系统之前也要进行病毒检查；

c) 应指定专人对网络和主机进行恶意代码检测并保存检测记录；

d) 应建立恶意代码防范管理制度，对防恶意代码软件的授权使用、恶意代码库升级、定期汇报等作出明确管理规定；

e) 应建立恶意代码集中防护的安全管理中心，确保整个网络统一配置、统一升级、统一控制；

f) 应定期检查信息系统内各种产品的恶意代码库的升级情况并进行记录，对主机防病毒产品、防病毒网关和邮件防病毒网关上截获的危险病毒或恶意代码进行及时分析处理，并形成书面的报表和总结汇报。

7.2.5.8.2 测试方法

访谈，检查。

7.2.5.8.3 测试对象

系统运维负责人，安全员，恶意代码防范管理制度，恶意代码检测记录，恶意代码升级记录，恶意代码分析报告，恶意代码集中防范管理中心。

7.2.5.8.4 测评实施

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，如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；

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，并保存记录；

c) 应访谈安全员，询问是否将恶意代码防范管理工作（包括防恶意代码软件的授权使用、代码库升级和防范工作情况汇报等）制度化，对其执行情况是否进行检查，检查周期多长；

d) 应访谈安全员，询问是否建立恶意代码防护管理中心，对整个系统的恶意代码管理工作是否实行统一集中管理（统一升级、检测、分析等），是否对恶意代码库的升级情况进行记录，对截获的危险病毒或恶意代码是否进行及时分析处理，并形成书面的报表和总结汇报；

e) 应访谈工作人员，询问其是否熟知恶意代码基本的防范手段，主要包括哪些；

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

g) 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；

h) 应检查是否具有恶意代码集中防范管理中心。

7.2.5.8.5 结果判定

a) 如果 7.2.5.8.4 e）中访谈人员回答内容与测评实施 a）回答内容基本一致，则该项为肯定；

b) 7.2.5.8.4 a）—h）均为肯定，则信息系统符合本单元测评项要求。

7.2.5.9 密码管理

7.2.5.9.1 测评项

a) 应建立密码使用管理制度，密码算法和密钥的使用应符合国家密码管理规定。

7.2.5.9.2 测试方法

访谈，检查。

7.2.5.9.3 测试对象

安全员，密码管理制度。

7.2.5.9.4 测评实施

a) 应访谈安全员，询问密码算法和密钥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。

7.2.5.9.5 结果判定

a) 7.2.5.9.4 a）—b）均为肯定，则信息系统符合本单元测评项要求。

7.2.5.10 变更管理

7.2.5.10.1 测评项

a) 应确认系统中将发生的变更，并制定变更方案；

b) 应建立变更管理制度，重要系统变更前，应向主管领导申请，变更方案经过评审、审批后方可实施变更；

c) 系统变更情况应向所有相关人员通告；

d) 应建立变更控制的申报和审批文件化程序，变更影响分析应文档化，变更实施过程应记录，所有文档记录应妥善保存；

e) 中止变更并从失败变更中恢复程序应文档化，应明确过程控制方法和人员职责，必要时恢复过程应经过演练。

7.2.5.10.2 测试方法

访谈，检查。

7.2.5.10.3 测试对象

系统运维负责人，变更方案，系统变更申请书，变更管理制度，变更申报和审批程序文档，变更失败恢复程序文档，变更方案评审记录，变更过程记录文档。

7.2.5.10.4 测评实施

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，变更过程是否文档化并保存，是否修改相关的操作流程（如系统配置发生变更后，相应的操作流程是否修改）；

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；变更方案是否经过评审；

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) 应检查重要系统的变更申请书，查看其是否有主管领导的批准；

e) 应检查系统变更方案，查看其是否对变更类型、变更原因、变更过程、变更前评估等方面进行规定；

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。

7.2.5.10.5 结果判定

a） 如果系统没有发生过变更，则7.2.5.10.4 i）不适用；

b） 7.2.5.10.4 a）－i）均为肯定，则信息系统符合本单元测评项要求。

7.2.5.11 备份与恢复管理

7.2.5.11.1 测评项

a） 应识别需要定期备份的重要业务信息、系统数据及软件系统等；

b） 应规定备份信息的备份方式（如增量备份或全备份等）、备份频度（如每日或每周等）、存储介质、保存期等；

c） 应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略，备份策略应指明备份数据的放置场所、文件命名规则、介质替换频率和将数据离站运输的方法；

d） 应指定相应的负责人定期维护和检查备份及冗余设备的状况，确保需要接入系统时能够正常运行；

e） 根据设备备份方式，规定备份及冗余设备的安装、配置和启动的流程；

f） 应建立控制数据备份和恢复过程的程序，备份过程应记录，所有文件和记录应妥善保存；

g） 应根据系统级备份所采用的方式和产品，建立备份设备的安装、配置、启动、操作及维护过程控制的程序，记录设备运行过程状况，所有文件和记录应妥善保存；

h） 应定期执行恢复程序，检查和测试备份介质的有效性，确保可以在恢复程序规定的时间内完成备份的恢复。

7.2.5.11.2 测试方法

访谈，检查。

7.2.5.11.3 测试对象

系统管理员，数据库管理员，网络管理员，备份管理文档，备份和恢复策略文档，备份设备操作流程文档，备份和恢复程序文档，备份过程记录文档。

7.2.5.11.4 测评实施

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；对其备份工作是否以文档形式规范了备份方式、频度、介质、保存期等内容，数据备份和恢复策略是否文档化，备份和恢复过程是否文档化；

b） 应访谈系统管理员、数据库管理员和网络管理员，询问其对备份及冗余设备的安装、配置和启动工作是否根据一定的流程进行，是否记录操作过程，是否保存记录文档，是否指定专人对备份设备的有效性定期维护和检查，多长时间检查一次；

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

d） 应检查是否具有规定备份方式、频度、介质、保存期的文档；

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） 应检查备份设备操作流程文档，查看其是否备份及冗余设备的安装、配置、启动、关闭等操作流程；

g） 应检查备份过程记录文档，查看其内容是否覆盖备份时间、备份内容、备份操作、备份介质存放等内容。

7.2.5.11.5 结果判定

a) 7.2.5.11.4 a）—g）均为肯定，则信息系统符合本单元测评项要求。

7.2.5.12 安全事件处置

7.2.5.12.1 测评项

a) 所有用户均有责任报告自己发现的安全弱点和可疑事件，但任何情况下用户均不应尝试验证弱点；

b) 应制定安全事件报告和处置管理制度，规定安全事件的现场处理、事件报告和后期恢复的管理职责；

c) 应分析信息系统的类型、网络连接特点和信息系统用户特点，了解本系统和同类系统已发生的安全事件，识别本系统需要防止发生的安全事件，事件可能来自攻击、错误、故障、事故或灾难；

d) 应根据国家相关管理部门对计算机安全事件等级划分方法，根据安全事件在本系统产生的影响，将本系统计算机安全事件进行等级划分；

e) 应制定安全事件报告和响应处理程序，确定事件的报告流程，响应和处置的范围、程度，以及处理方法等；

f) 应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训，制定防止再次发生的补救措施，过程形成的所有文件和记录均应妥善保存；

g) 对造成系统中断和造成信息泄密的安全事件应采用不同的处理程序和报告程序。

7.2.5.12.2 测试方法

访谈，检查。

7.2.5.12.3 测试对象

系统运维负责人，工作人员，安全事件记录分析文档，安全事件报告和处置管理制度，安全事件报告和处理程序文档。

7.2.5.12.4 测评实施

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，安全事件的报告和响应处理过程是否制度化和文档化，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，询问本系统已发生的和需要防止发生的安全事件主要有哪几类，对识别出的安全事件是否根据其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) 应访谈工作人员，询问其不同安全事件的报告流程；

d) 应检查安全事件报告和处置管理制度，查看其是否明确与安全事件有关的工作职责，包括报告单位（人）、接报单位（人）和处置单位等职责；

e) 应检查安全事件定级文档，查看其内容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；

f) 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；

g) 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，是否明确具体报告方式、报告内容、报告人等方面内容。

7.2.5.12.5 结果判定

a) 如果 7.2.5.12.4 c）中访谈回答与 g）中描述一致，则该项为肯定；

b) 7.2.5.12.4 a）—g）为肯定，则信息系统符合本单元测评项要求。

7.2.5.13 应急预案管理

7.2.5.13.1 测评项

a) 应在统一的应急预案框架下制定不同事件的应急预案，应急预案框架应包括启动预案的条件、应急处理流程、系统恢复流程和事后教育和培训等内容；

b) 应从人力、设备、技术和财务等方面确保应急计划的执行有足够的资源保障；

c) 应对系统相关的人员进行培训使之了解如何及何时使用应急预案中的控制手段及恢复策略，对应急预案的培训至少每年举办一次；

d) 应急预案应定期演练，根据不同的应急恢复内容，确定演练的周期；

e) 应规定应急预案需要定期审查和根据实际情况更新的内容，并按照执行。

7.2.5.13.2 测试方法

访谈，检查。

7.2.5.13.3 测试对象

系统运维负责人，应急响应预案文档，应急预案培训记录，应急预案演练记录，应急预案审查记录。

7.2.5.13.4 测评实施

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，培训内容是什么，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并更新；

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) 应检查应急响应预案文档，查看其内容是否覆盖启动预案的条件、应急处理流程、系统恢复流程、事后教育等内容；

d) 应检查是否具有应急预案培训记录、演练记录和审查记录。

7.2.5.13.5 结果判定

a) 7.2.5.13.4 a）－d）均为肯定，则信息系统符合本单元测评项要求。

8 第四级安全控制测评

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 测评项

a) 机房和办公场地应选择在具有防震、防风和防雨等能力的建筑内；

b) 机房场地应避免设在建筑物的高层或地下室，以及用水设备的下层或隔壁；

c) 机房场地应当避开强电场、强磁场、强震动源、强噪声源、重度环境污染、易发生火灾、水灾、易遭受雷击的地区。

8.1.1.1.2 测评方式

访谈，检查。

8.1.1.1.3 测评对象

物理安全负责人，机房维护人员，机房，办公场地，机房场地设计/验收文档。

8.1.1.1.4 测评实施

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；

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/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避免在建筑物的高层或地下室，以及用水设备的下层或隔壁；

f） 应检查机房场地是否避免设在强电场、强磁场、强震动源、强噪声源、重度环境污染、易发生火灾、水灾、易遭受雷击的地区；

g） 如果机房和办公场地的终端显示器、打印机等设备有敏感或密级信息输出，应检查设备摆放位置是否为不易被无关人员看到的隐蔽位置。

8.1.1.1.5 结果判定

a） 8.1.1.1.4 c），机房场地的选址符合不在建筑物的高层或地下室，以及用水设备的下层或隔壁；不在强电场、强磁场、强震动源、强噪声源、重度环境污染、易发生火灾、水灾、易遭受雷击的地区等要求，则该项为肯定；

b） 如果8.1.1.1.4 g）中“如果”条件不成立，则该项为不适用；

c） 8.1.1.1.4 a）-g）均为肯定，则信息系统符合本单元测评项要求。

8.1.1.2 物理访问控制

8.1.1.2.1 测评项

a） 机房出入口配置电子门禁系统，由专人值守，鉴别进入的人员身份并登记在案；

b） 应批准进入机房的来访人员，限制和监控其活动范围；

c） 应对机房划分区域进行管理，区域和区域之间设置物理隔离装置，在重要区域前设置交付或安装等过度区域；

d） 应对重要区域配置第二道电子门禁系统，控制、鉴别和记录进入的人员身份并监控其活动。

8.1.1.2.2 测评方式

访谈，检查。

8.1.1.2.3 测评对象

物理安全负责人，机房值守人员，机房，机房设施（电子门禁系统），机房安全管理制度，进入机房的登记记录，来访人员进入机房的审批记录，电子门禁系统记录。

8.1.1.2.4 测评实施

a） 应访谈物理安全负责人，了解具有哪些控制机房进出的能力；

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；检查机房是否存在电子门禁系统控制之外的出入口；

f） 应检查机房，是否有进入机房的人员身份鉴别措施，如戴有可见的身份辨识标识；

g） 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；

h) 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度区域;是否对不同区域设置不同机房或者同一机房的不同区域之间设置有效的物理隔离装置（如隔墙等）；

i) 应检查机房或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；

j) 应检查每道电子门禁系统是否都能正常工作；查看每道电子门禁系统运行、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的人员身份；

k) 应检查视频监控设备是否正常工作，是否能够监视和记录进入的人员活动情况，查看运行和维护记录，监视记录是否保存足够的时间。

8.1.1.2.5 结果判定

a) 8.1.1.2.4 a），至少应包括制订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，视频监控设备，该测评实施才为肯定；

b) 如果8.1.1.2.4 b）认为没有必要对机房进行划分区域管理（如果安全管理需要，计算机设备宜采用分区布置，如可分为主机区、存贮器区、数据输入区、数据输出区、通信区和监控调度区等），则测评实施h）不适用；

c) 8.1.1.2.4 d），至少应包括制订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，该测评实施才为肯定；

d) 8.1.1.2.4 a）- k）均为肯定，则信息系统符合本单元测评项要求。

8.1.1.3 防盗窃和防破坏

8.1.1.3.1 测评项

a) 应将主要设备放置在物理受限的范围内；

b) 应对设备或主要部件进行固定，并设置明显的无法除去的标记；

c) 应将通信线缆铺设在隐蔽处，如铺设在地下或管道中等；

d) 应对介质分类标识，存储在介质库或档案室中；

e) 设备或存储介质携带出工作环境时，应受到监控和内容加密；

f) 应利用光、电等技术设置机房的防盗报警系统，以防进入机房的盗窃和破坏行为；

g) 应对机房设置监控报警系统。

8.1.1.3.2 测评方式

访谈，检查。

8.1.1.3.3 测评对象

物理安全负责人，机房维护人员，资产管理员，机房设施，设备管理制度文档，通信线路布线文档，防盗报警系统和监控报警系统的安装测试/验收报告。

8.1.1.3.4 测评实施

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进行定期维护检查；

c) 应访谈资产管理员，在介质管理中，是否进行了分类标识，是否存放在介质库或档案室中；询问对设备或存储介质携带出工作环境是否规定了审批程序、内容加密、专人检查等安全保护的措施；

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，是否不易被移动或被搬走，是否设置明显的无法除去的标记；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（如铺设在地下或管道中等）；

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；是否有异地保存的措施；

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

h) 应检查有关设备或存储介质携带出工作环境的审批记录，以及专人对内容加密进行检查的记录；各种有关的记录是否保存足够的时间；

i) 应检查是否有设备管理制度文档，通信线路布线文档，介质管理制度文档，介质清单和使用记录，机房防盗报警设施的安全资质材料、安装测试/验收报告；查看文档中的条文是否与设备放置位置、设备或主要部件保护、通信线缆铺设等实际情况一致。

8.1.1.3.5 结果判定

a) 8.1.1.3.4 a）中至少应该包括制订了设备管理制度，主要设备放置位置做到安全可控，设备或主要部件进行了固定和标记，通信线缆铺设在隐蔽处，介质分类标识并存储在介质库或档案室，机房安装了防止进入盗窃和破坏的利用光、电等技术设置的机房防盗报警系统；设备或存储介质携带出工作环境的审批程序、内容加密、专人检查等措施；机房设置了摄像、传感等监控报警系统，该测评实施才为肯定；

b) 8.1.1.3.4 a）-i）均为肯定，则信息系统符合本单元测评项要求。

8.1.1.4 防雷击

8.1.1.4.1 测评项

a) 机房建筑应设置避雷装置；

b) 应设置防雷保安器，防止感应雷；

c) 应设置交流电源地线。

8.1.1.4.2 测评方式

访谈，检查，测试。

8.1.1.4.3 测评对象

物理安全负责人，机房维护人员，机房设施，建筑防雷设计/验收文档。

8.1.1.4.4 测评实施

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增加有资质的避雷装置，以避免感应雷击；

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；询问机房计算机系统接地（交流工作接地、安全保护接地、防雷接地）是否符合GB50174—93《电子计算机机房设计规范》的要求；

c) 应检查机房是否有建筑防雷设计/验收文档，机房接地设计/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增加有资质的避雷装置，以避免感应雷击；

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，是否达到了GB50174—93《电子计算机机房设计规范》的接地电阻要求。

8.1.1.4.5　结果判定

a）　8.1.1.4.4 a）至少还应包括符合GB 50057－1994《建筑物防雷设计规范》（GB157《建筑防雷设计规范》）中的计算机机房防雷要求，如果在雷电频繁区域，是否装设浪涌电压吸收装置等，则该项为肯定；

b）　8.1.1.4.4 b），要求地线的引线应和大楼的钢筋网及各种金属管道绝缘，交流工作接地的接地电阻不应大于4Ω，安全保护地的接地电阻不应大于4Ω；防雷保护地（处在有防雷设施的建筑群中可不设此地）的接地电阻不应大于10Ω的要求，则该项为肯定；

c）　8.1.1.4.4 a）-e）均为肯定，则信息系统符合本单元测评项要求。

8.1.1.5　防火

8.1.1.5.1　测评项

a）　应设置火灾自动消防系统，自动检测火情、自动报警，并自动灭火；

b）　机房及相关的工作房间和辅助房，其建筑材料应具有耐火等级；

c）　机房采取区域隔离防火措施，将重要设备与其他设备隔离开。

8.1.1.5.2　测评方式

访谈，检查。

8.1.1.5.3　测评对象

物理安全负责人，机房值守人员，机房设施，机房安全管理制度，机房防火设计/验收文档，自动消防系统设计/验收文档。

8.1.1.5.4　测评实施

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，是否制订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（喷水不适用于机房）；是否能够做到随时注意防止和消灭火灾隐患；

c）　应检查机房是否设置了自动检测火情（如使用温感、烟感探测器）、自动报警、自动灭火的自动消防系统，摆放位置是否合理，有效期是否合格；应检查自动消防系统是否正常工作，查看运行记录、报警记录、定期检查和维修记录；

d）　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/验收文档；检查是否有机房自动消防系统的设计/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；

e）　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。

8.1.1.5.5　结果判定

a）　8.1.1.5.4 a）-e）均为肯定，则信息系统符合本单元测评项要求。

8.1.1.6　防水和防潮

8.1.1.6.1　测评项

a）　水管安装，不得穿过屋顶和活动地板下；

b）　应对穿过墙壁和楼板的水管增加必要的保护措施，如设置套管；

c）　应采取措施防止雨水通过屋顶和墙壁渗透；

d）　应采取措施防止室内水蒸气结露和地下积水的转移与渗透；

e）　应安装对水敏感的检测仪表或元件，对机房进行防水检测和报警。

8.1.1.6.2 测评方式

访谈，检查。

8.1.1.6.3 测评对象

物理安全负责人，机房维护人员，机房设施，建筑防水和防潮设计/验收文档，防水检测报警系统设计/验收文档，机房湿度记录，除湿装置运行记录。

8.1.1.6.4 测评实施

a) 应访谈物理安全负责人，询问机房建设是否有防水防潮措施；如果机房内有上下水管安装，是否穿过屋顶和活动地板下，穿过墙壁和楼板的水管是否采取必要的保护措施，如设置套管；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，是否经常检查是否有漏水情况；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采取防范措施；

c) 应检查机房是否有建筑防水和防潮设计/验收文档，是否能够满足机房防水和防潮的需求，是否机房防水防潮的实际情况一致；

d) 如果有管道穿过主机房墙壁和楼板处，应检查是否有必要的保护措施，如设置套管等；

e) 应检查机房是否不存在屋顶和墙壁等出现过漏水、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、渗透和返潮现是否能够及时修复解决；

f) 如果在湿度较高地区或季节，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，与机房湿度记录情况是否一致；

g) 如果机房受到漏水威胁很高，应检查是否设置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以及运行记录，是否有人负责此项工作。

8.1.1.6.5 结果判定

a) 如果8.1.1.6.4 d），f），g）中“如果”条件不成立，则该项为不适用；

b) 8.1.1.6.4 a）-g）均为肯定，则信息系统符合本单元测评项要求。

8.1.1.7 防静电

8.1.1.7.1 测评项

a) 应采用必要的接地等防静电措施；

b) 应采用防静电地板；

c) 应采用静电消除器等装置，减少静电的产生。

8.1.1.7.2 测评方式

访谈，检查。

8.1.1.7.3 测评对象

物理安全负责人，机房维护人员，机房设施，防静电设计/验收文档，湿度记录，除湿操作记录。

8.1.1.7.4 测评实施

a) 应访谈物理安全负责人，询问机房是否采用必要的接地等防静电措施，是否有控制机房湿度的措施；在静电较强地区的机房是否采取了有效的防静电措施；

b） 应访谈机房维护人员，询问是否经常检查机房湿度，并控制在GB2887中的规定的范围内；询问机房是否存在静电问题或因静电引起的故障事件；如果存在静电时是否及时采取消除静电的措施；

c） 应检查机房是否有防静电设计/验收文档，与实际情况是否一致；

d） 应检查机房是否有安全接地，查看机房的相对湿度的记录是否符合GB2887中的规定，查看机房是否不存在明显的静电现象；

e） 如果在静电较强的地区，应检查机房是否了采用了如防静电地板、防静电工作台、以及静电消除剂和静电消除器等措施；应查看使用静电消除剂或静电消除器等的除湿操作记录；

f） 在静电较强的地区，应测试机房的相对湿度是否符合GB2887中的规定。

8.1.1.7.5 结果判定

a） 8.1.1.7.4 e）中有效的防静电措施，可以包括如防静电地板、防静电工作台，或静电消除剂和静电消除器等措施的部分或全部，则该项为肯定；

b） 如果8.1.1.7.4 e）中“如果”条件不成立，则该项为不适用；

c） 8.1.1.7.4 a）-f）均为肯定，则信息系统符合本单元测评项要求。

8.1.1.8 温湿度控制

8.1.1.8.1 测评项

a） 应设置恒温恒湿系统，使机房温、湿度的变化在设备运行所允许的范围之内。

8.1.1.8.2 测评方式

访谈，检查。

8.1.1.8.3 测评对象

物理安全负责人，机房维护人员，机房设施，温湿度控制设计/验收文档，温湿度记录、运行记录和维护记录。

8.1.1.8.4 测评实施

a） 应访谈物理安全负责人，询问机房是否配备了恒温恒湿系统，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；

b） 应访谈机房维护人员，询问是否定期检查和维护机房的温湿度自动调节设施，询问是否出现过温湿度影响系统运行的事件；

c） 应检查机房是否有温湿度控制设计/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合；

d） 应检查恒温恒湿系统是否能够正常运行，查看温湿度记录、运行记录和维护记录；查看机房温、湿度是否满足GB 2887-89《计算站场地技术条件》的要求。

8.1.1.8.5 结果判定

a） 8.1.1.8.4 a）-d）均为肯定，则信息系统符合本单元测评项要求。

8.1.1.9 电力供应

8.1.1.9.1 测评项

a） 计算机系统供电应与其他供电分开；

b） 应设置稳压器和过电压防护设备；

c） 应提供短期的备用电力供应（如UPS设备）；

d） 应设置冗余或并行的电力电缆线路；

e） 应建立备用供电系统（如备用发电机），以备常用供电系统停电时启用。

8.1.1.9.2 测评方式

访谈，检查。

8.1.1.9.3 测评对象

物理安全负责人，机房维护人员，机房设施，电力供应安全设计/验收文档，检查和维护记录。

8.1.1.9.4 测评实施

a) 应访谈物理安全负责人，询问计算机系统供电线路是否与其他供电分开；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（如UPS），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（如双路供电方式）；是否建立备用供电系统（如备用发电机）；

b) 应访谈机房维护人员，询问是对在计算机系统供电线路上的稳压器、过电压防护设备、短期备用电源设备等进行定期检查和维护；是否能够控制电源稳压范围满足计算机系统运行正常；

c) 应访谈机房维护人员，询问冗余或并行的电力电缆线路（如双路供电方式）在双路供电切换时是否能够对计算机系统正常供电；是否定期检查备用供电系统（如备用发电机），是否能够在规定时间内正常启动和正常供电；

d) 应检查机房是否有电力供应安全设计/验收文档，查看文档中是否标明单独为计算机系统供电，配备稳压器、过电压防护设备、备用电源设备以及冗余或并行的电力电缆线路等要求；查看与机房电力供应实际情况是否一致；

e) 应检查计算机供电线路，查看计算机系统供电是否与其他供电分开；

f) 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；

g) 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电源设备的检查和维护记录，以及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。

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

i) 应测试备用供电系统(如备用发电机)是否能够在规定时间内正常启动和正常供电。

8.1.1.9.5 结果判定

a) 8.1.1.9.4 a）-i）均为肯定，则信息系统符合本单元测评项要求。

8.1.1.10 电磁防护

8.1.1.10.1 测评项

a) 应采用接地方式防止外界电磁干扰和设备寄生耦合干扰；

b) 电源线和通信线缆应隔离，避免互相干扰；

c) 对重要设备和磁介质实施电磁屏蔽；

d) 对机房实施电磁屏蔽。

8.1.1.10.2 测评方式

访谈，检查。

8.1.1.10.3 测评对象

物理安全负责人，机房维护人员，机房设施，电磁防护设计/验收文档，电子屏蔽装置或屏蔽机房设计/验收文档，电磁泄露测试报告。

8.1.1.10.4 测评实施

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采取了防止电磁泄露的措施；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，是否安装了满足BMB4-2000《电磁干扰器技术要求和测试方法》要求的二级电磁干扰器；

c） 应检查机房是否有电磁防护设计/验收文档，与实际情况是否一致；是否有电子屏蔽或屏蔽机房设计/验收文档；是否有电子屏蔽或屏蔽机房的管理制度文档；

d） 应检查机房是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） 应检查使用电磁干扰器的涉密设备开机，是否同时开启电磁干扰器；

g） 如果对机房采用了电子屏蔽，应检查在机房有设备运行时是否开启了电子屏蔽装置；如果安装了屏蔽机房，应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，屏蔽机房是否定期测试电磁泄露，应查看电磁泄露测试报告；

h） 如果对机房采用了电子屏蔽或安装了屏蔽机房，应测试屏蔽机房的电磁泄露状况（参考标准GB12190-90 高性能屏蔽效能的测量方法）。

8.1.1.10.5 结果判定

a） 如果8.1.1.10.4 g）、h）、中“如果”条件不成立，则该项为不适用；

b） 8.1.1.10.4 a）-h）均为肯定，则信息系统符合本单元测评项要求。

8.1.2 网络安全

8.1.2.1 结构安全与网段划分

8.1.2.1.1 测评项

a） 网络设备的业务处理能力应具备冗余空间，要求满足业务高峰期需要；

b） 应设计和绘制与当前运行情况相符的网络拓扑结构图；

c） 应根据机构业务的特点，在满足业务高峰期需要的基础上，合理设计网络带宽；

d） 应在业务终端与业务服务器之间进行路由控制建立安全的访问路径；

e） 应根据各部门的工作职能、重要性、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、网段分配IP地址段；

f） 重要网段应采取网络层地址与数据链路层地址绑定措施，防止地址欺骗；

g） 应按照对业务服务的重要次序来指定带宽分配优先级别，保证在网络发生拥堵的时候优先保护重要业务数据主机。

8.1.2.1.2 测评方式

访谈，检查，测试。

8.1.2.1.3 测评对象

网络管理员，边界和主要网络设备，网络拓扑结构，网络拓扑图，网络设计/验收文档。

8.1.2.1.4 测评实施

a) 可访谈网络管理员，询问信息系统中的边界和主要网络设备的性能以及目前业务高峰流量情况；

b) 可访谈网络管理员，询问网段划分情况以及划分的原则；询问重要的网段有哪些，对重要网段的保护措施有哪些；

c) 可访谈网络管理员，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) 可访谈网络管理员，询问网络设备上的路由控制策略措施有哪些，这些策略设计的目的是什么；

e) 应检查网络拓扑图，查看与当前运行情况是否一致；

f) 应检查网络设计/验收文档，查看是否有边界和主要网络设备是否有能满足基本业务需求的能力，目前的网络接入及核心网络的带宽能否满足业务高峰期的需要，是否不存在带宽瓶颈等方面的设计或描述；

g) 应检查设计/验收文档，查看是否有是否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（如使用静态路由等）建立安全的访问路径；

i) 应检查边界和主要网络设备，查看对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（如对重要服务器采用IP地址和MAC地址绑定措施）；

j) 应检查边界和主要网络设备，查看是否有对带宽进行控制的策略（如路由、交换设备上的QOS策略配置情况，专用的带宽管理设备的配置策略等），并且这些策略能否保证在网络发生拥堵的时候优先保护重要业务（如重要业务的主机的优先级要高于非重要业务的主机）；

k) 应测试网络拓扑结构，可通过网络拓扑结构自动发现、绘制工具，验证实际的网络拓扑结构和网络拓扑结构图是否一致；

l) 应测试业务终端与业务服务器之间的访问路径，可通过使用路由跟踪工具（如tracert等工具），验证业务终端与业务服务器之间的访问路径的是否安全（如访问路径是否固定等）；

m) 应测试重要网段，验证其采取的网络地址与数据链路地址绑定措施是否有效（如试图使用非绑定地址，观察是否能正常访问等）；

n) 应测试网络带宽分配策略，可通过使用带宽测试工具，验证网络带宽分配是否有效。

8.1.2.1.5 结果判定

a) 如果 8. 1. 2. 1. 4 f）-g）中缺少相应的文档，则该项为否定；

b) 8. 1. 2. 1. 4 e）-n）均为肯定，则信息系统符合本单元测评项要求。

8.1.2.2 网络访问控制

8.1.2.2.1 测评项

a) 应不允许数据带通用协议通过；

b) 应禁止便携式和移动式设备接入网络。

8.1.2.2.2 测评方式

访谈，检查，测试。

8.1.2.2.3 测评对象

安全员，边界和主要网络设备。

8.1.2.2.4 测评实施

a) 可访谈安全员，询问采取网络访问控制的措施有哪些；询问访问控制策略的设计原则；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；

b) 应检查主要网络设备，查看是否有相应的访问控制措施（如 VLAN，访问控制列表，MAC 地址绑定）禁止便携式和移动式设备接入网络；

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) 应测试边界和主要网络设备，可通过试图用移动设备接入网络，测试网络设备的访问控制措施是否有效；

e) 应测试边界和主要网络设备，可通过发送带通用协议的数据（如使用 http 隧道工具），测试访问控制措施是否有效阻断这种连接。

8.1.2.2.5 结果判定

a) 8.1.2.2.4 b）-e）均为肯定，则信息系统符合本单元测评项要求。

8.1.2.3 拨号访问控制

8.1.2.3.1 测评项

a） 应不开放远程拨号访问功能（如远程拨号用户或移动VPN用户）。

8.1.2.3.2 测评方式

访谈，检查。

8.1.2.3.3 测评对象

安全员，边界网络设备，设计/验收文档。

8.1.2.3.4 测评实施

a） 可访谈安全员，询问网络是否允许拨号访问；询问对拨号访问控制的策略是什么，采取何种技术手段实现（如使用防火墙还是使用路由器实现），采取的拨号访问用户的权限分配原则是什么；询问对保护访问的认证方式有哪些；

b） 应检查设计/验收文档，查看其是否有网络不提供拨号访问功能的描述；

c） 应检查边界网络设备，查看是否禁用掉远程拨号访问功能。

8.1.2.3.5 结果判定

a） 如果8.1.2.3.4 b）中缺少相应的文档，则该项为否定；

b） 8.1.2.3.4 b）-c）均为肯定，则信息系统符合本单元测评项要求。

8.1.2.4 网络安全审计

8.1.2.4.1 测评项

a） 对网络系统中的网络设备运行状况、网络流量、用户行为等进行全面的监测、记录；

b） 对于每一个事件，其审计记录应包括：事件的日期和时间、用户、事件类型、事件是否成功，及其他与审计相关的信息；

c） 安全审计应可以根据记录数据进行分析，并生成审计报表；

d） 安全审计应可以对特定事件，提供指定方式的实时报警；

e） 审计记录应受到保护避免受到未预期的删除、修改或覆盖等；

f） 安全审计应能跟踪监测到可能的安全侵害事件，并终止违规进程；

g） 审计员应能够定义审计跟踪极限的阈值，当存储空间接近极限时，能采取必要的措施（如报警并导出），当存储空间被耗尽时，终止可审计事件的发生；

h） 安全审计应根据信息系统的统一安全策略，实现集中审计；

i） 网络设备时钟应与时钟服务器时钟保持同步。

8.1.2.4.2 测评方式

访谈，检查，测试。

8.1.2.4.3 测评对象

审计员，边界和主要网络设备（包括安全设备）。

8.1.2.4.4 测评实施

a） 可访谈审计员，询问是否对网络系统中的边界和关键网络设备的审计包括哪些项；询问审计记录的主要内容有哪些；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，查看审计策略是否对网络系统中的网络设备运行状况、网络流量、用户行为等进行全面的监测、记录；

c） 应检查边界和主要网络设备，查看事件审计策略是否包括：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，查看是否可以对特定事件，是否提供指定方式的实时报警（如声音、EMAIL、短信等）；

e） 应检查边界和主要网络设备，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（如对审计记录进行分类、排序、查询、统计、分析和组合查询等），并能根据需要生成审计报表；

f） 应检查边界和主要网络设备，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，能否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；

g） 应测试边界和主要网络设备，可通过以某个用户试图产生一些重要的安全相关事件（如鉴别失败等），验证安全审计的覆盖情况和记录情况与要求是否一致；

h） 应测试边界和主要网络设备，可通过以某个系统用户试图删除、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；

i） 应测试边界和主要的网络设备，验证其能否跟踪监测到可能的安全侵害事件，并终止违规进程的功能是否正确（如产生一定的安全侵害事件，查看安全审计能否检测到该事件，并终止其进程）。

8.1.2.4.5 结果判定

a) 8. 1. 2. 4. 4 b）-i）均为肯定，则信息系统符合本单元测评项要求。

8.1.2.5 边界完整性检查

8.1.2.5.1 测评项

a） 应能够检测内部网络中出现的内部用户未通过准许私自联到外部网络的行为（即“非法外联”行为）；

b） 应能够对非授权设备私自联到网络的行为进行检查，并准确定位、有效阻断；

c） 应能够对内部网络用户私自联到外部网络的行为进行检查后准确定出位置，并对其进行有效阻断；

d） 应能够根据信息流控制策略和信息流的敏感标记，阻止重要信息的流出。（网络设备标记，指定路由信息标记）。

8.1.2.5.2 测评方式

访谈，检查，测试。

8.1.2.5.3 测评对象

安全员，边界完整性检查设备，边界完整性检查设备运行日志。

8.1.2.5.4 测评实施

a） 可访谈安全员，询问是否有对内部用户未通过准许私自联到外部网络的行为、对非授权设备私自联到网络的行为进行监控的措施，，措施是什么；询问网络内是否使用边界完整性检查设备对网络进行监控；询问网络内“非法外联”的情况；

b） 应检查边界完整性检查工具运行日志，查看运行是否正常（查看看是否持续对网络进行监控）；

c） 应检查边界完整性检查设备/工具，查看是否设置了同时对非法联接到内网和非法联接到外网的行为进行监控；查看是否对发现的非法联接行为进行有效的阻断

d） 应该检查边界网络设备，查看是否设置相关措施能够根据信息流控制策略和信息流的敏感标记，阻止重要信息的流出（网络设备标记，指定路由信息标记）；

e） 应测试边界完整性检查设备，测试是否能有效的发现“非法外联”的行为（如产生非法外联的动作，查看边界完整性检查设备是否能够发现该行为）；

f） 应测试边界完整性检查设备，测试是否确定出“非法外联”设备的位置，并对其进行有效阻断（如产生非法外联的动作，查看边界完整性检查设备是否能够准确定位并阻断）；

g） 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联到网络的行为进行

检查，并准确定出位置，对其进行有效阻断（如产生非法接入的动作，查看测试边界完整性检查设备是否能准确的发现，准确的定位并产生阻断）。

8.1.2.5.5 结果判定

a) 8.1.2.5.4 b）-g）均为肯定，则信息系统符合本单元测评项要求。

8.1.2.6 网络入侵防范

8.1.2.6.1 测评项

a) 在网络边界处应监视以下攻击行为：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、网络蠕虫攻击等入侵事件的发生；

b) 当检测到入侵事件时，应记录入侵的源IP、攻击的类型、攻击的目的、攻击的时间等，并发出安全警告（如可采取屏幕实时提示、E-mail告警、声音告警等几种方式）及自动采取相应动作。

8.1.2.6.2 测评方式

访谈，检查，测试。

8.1.2.6.3 测评对象

安全员，网络入侵防范设备。

8.1.2.6.4 测评实施

a) 可访谈安全员，询问网络入侵防范措施有哪些；是否有专门的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、网络蠕虫攻击等入侵事件；

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（如采取屏幕实时提示、E-mail告警、声音告警等）；

d) 应检查网络入侵防范设备，查看其生产厂商是否为正规厂商，规则库是否为最新；

e) 应测试网络入侵防范设备，验证其监控策略是否有效（如模拟产生攻击动作，查看网络入侵防范设备的反应）；

f) 应测试网络入侵防范设备，验证其报警策略是否有效（如模拟产生攻击动作，查看网络入侵防范设备是否能实时报警）。

8.1.2.6.5 结果判定

a) 8.1.2.6.4 b）-f）均为肯定，则信息系统符合本单元测评项要求。

8.1.2.7 恶意代码防范

8.1.2.7.1 测评项

a) 应在网络边界及核心业务网段处对恶意代码进行检测和清除；

b) 应维护恶意代码库的升级和检测系统的更新；

c) 应支持恶意代码防范的统一管理。

8.1.2.7.2 测评方式

访谈，检查。

8.1.2.7.3 测评对象

安全员，防恶意代码产品，设计/验收文档， 恶意代码产品运行日志。

8.1.2.7.4 测评实施

a) 可访谈安全员，询问系统中的网络防恶意代码防范措施是什么；询问恶意代码库的更新策略；询问防恶意代码产品的有哪些主要功能；询问系统是否发生过针对恶意代码入侵的安全事件；

b） 应检查设计/验收文档，查看其是否有在网络边界及核心业务网段处是否有对恶意代码的采取相关措施（如是否有防病毒网关），防恶意代码产品是否有实时更新的功能的描述；

c） 应检查恶意代码产品运行日志，查看是否持续运行；

d） 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的措施；

e） 应检查防恶意代码产品，查看是否为正规厂商生产，运行是否正常，恶意代码库是否为最新版本；

f） 应检查防恶意代码产品的配置策略，查看是否支持恶意代码防范的统一管理（如查看是否为分布式部署，集中管理等）。

8.1.2.7.5 结果判定

a） 如果8.1.2.7.4 b）中缺少相应的文档，则该项为否定；

b） 8.1.2.7.4 b）-f）均为肯定，则信息系统符合本单元测评项要求。

8.1.2.8 网络设备防护

8.1.2.8.1 测评项

a） 应对登录网络设备的用户进行身份鉴别；

b） 应对网络上的对等实体进行身份鉴别；

c） 应对网络设备的管理员登录地址进行限制；

d） 网络设备用户的标识应唯一；

e） 身份鉴别信息应具有不易被冒用的特点，例如口令长度、复杂性和定期的更新等；

f） 应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；

g） 网络设备用户的身份鉴别信息至少有一种应是不可伪造的，例如以公私钥对、生物特征等作为身份鉴别信息；

h） 应具有登录失败处理功能，如结束会话、限制非法登录次数，当网络登录连接超时，自动退出；

i） 应实现设备特权用户的权限分离，例如将管理与审计的权限分配给不同的网络设备用户。

8.1.2.8.2 测评方式

访谈，检查，测试。

8.1.2.8.3 测评对象

网络管理员，边界和主要网络设备（包括安全设备）。

8.1.2.8.4 测评实施

a） 可访谈网络管理员，询问对关键网络设备的防护措施有哪些，询问对关键网络设备的登录和验证方式做过何种特定配置；

b） 应访谈网络管理员，询问采取的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的安全设置，查看其是否有对鉴别失败采取相应的措施的设置；查看是否有限制非法登录次数的功能；

d） 应检查边界和主要网络设备的安全设置，查看是否对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；查看是否对网络上的对等实体进行身份鉴别；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） 应测试边界和主要网络设备的安全设置，验证鉴别失败处理措施是否有效（如模拟失败登录，观察网络设备的动作等），限制非法登录次数（如模拟非法登录，观察网络设备的动作等），对网络设备的管理员登录地址进行限制（如使用任意地址登录，观察网络设备的动作等）等功能是否有效；

f） 应测试边界和主要网络设备的安全设置，验证其网络登录连接超自动退出的设置是否有效（如长时间连接无任何操作，观察观察网络设备的动作等）；

g） 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（如口令猜解等）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。

8.1.2.8.5 结果判定

a） 如果网络设备的口令策略为口令长度8位以上，口令复杂（如规定字符应混有大、小写字母、数字和特殊字符），口令生命周期，新旧口令的替换要求（规定替换的字符数量）或为了便于记忆使用了令牌；则8.1.2.8.4 b）满足测评要求；

b） 8.1.2.8.4 b）-f）均为肯定，则信息系统符合本单元测评项要求。

8.1.3 主机系统安全

8.1.3.1 身份鉴别

8.1.3.1.1 测评项

a） 操作系统和数据库系统用户的身份标识应具有唯一性；

b） 应对登录操作系统和数据库系统的用户进行身份标识和鉴别；

c） 应对同一用户采用两种或两种以上组合的鉴别技术实现用户身份鉴别；

d） 操作系统和数据库系统用户的身份鉴别信息应具有不易被冒用的特点，例如口令长度、复杂性和定期更新等；

e） 操作系统和数据库系统用户的身份鉴别信息至少有一种应是不可伪造的，例如以公私钥对、生物特征等作为身份鉴别信息；

f） 应具有登录失败处理功能，如结束会话、限制非法登录次数，当登录连接超时，自动退出；

g） 应具有鉴别警示功能；

h） 重要的主机系统应对与之相连的服务器或终端设备进行身份标识和鉴别。

8.1.3.1.2 测评方式

访谈，检查，测试。

8.1.3.1.3 测评对象

系统管理员，数据库管理员，主要服务器操作系统，主要数据库系统，服务器操作系统文档，数据库系统文档。

8.1.3.1.4 测评实施

a） 应检查服务器操作系统和数据库系统身份鉴别功能是否具有《信息安全等级保护操作系统安全技术要求》和《信息安全等级保护数据库管理系统安全技术要求》第二级以上或TCSEC C2级以上的测试报告；

b） 可访谈系统管理员，询问操作系统的身份标识与鉴别机制采取何种措施实现，目前系统提供了哪些身份鉴别措施和鉴别失败处理措施；

c） 可访谈数据库管理员，询问数据库的身份标识与鉴别机制采取何种措施实现，目前系统提供了哪些身份鉴别措施和鉴别失败处理措施；

d） 应检查服务器操作系统文档和数据库系统文档，查看用户身份标识的唯一性是由什么属性来保证的（如用户名或者 UID 等）；

e） 应检查主要服务器操作系统和主要数据库系统，查看是否提供了身份鉴别措施（如用户名和口令等），身份鉴别信息是否具有不易被冒用的特点，例如，口令足够长，口令复杂（如规定字符应混有大、小写字母、数字和特殊字符），口令生命周期，新旧口令的替换要求（如规定替换的字符数量）或为了便于记忆使用了令牌；

f） 应检查主要服务器操作系统和主要数据库系统，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（如采用用户名/口令、挑战应答、动态口令、

物理设备、生物识别技术和数字证书方式的身份鉴别技术中的任意两个组合），并且有一种是不易伪造的（如数字证书或生物识别技术）；

g) 应检查主要服务器操作系统和主要数据库系统，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，对超过限制值的登录终止其鉴别会话，并封闭帐号；查看是否设置网络登录连接超时，并自动退出；

h) 应检查重要服务器操作系统，查看服务器操作系统是否对与之相连的服务器或终端设备进行身份标识和鉴别；

i) 应测试主要服务器操作系统和主要数据库系统，可通过错误的用户名和口令试图登录系统，验证鉴别失败处理功能是否有效；

j) 应测试主要服务器操作系统和主要数据库系统，当进入系统时，是否先需要进行标识（如建立账号），而没有进行标识的用户不能进入系统；

k) 应测试主要服务器操作系统和主要数据库系统，添加一个新用户，其用户标识为系统原用户的标识（如用户名或 UID），查看是否不会成功；

l) 应测试主要服务器操作系统和主要数据库系统，删除一个用户标识，然后再添加一个新用户，其用户标识和所删除的用户标识一样（如用户名/UID），查看是否不能成功；

m) 应测试主要服务器操作系统，可通过使用未进行身份标识和鉴别的主机连接该服务器，验证主机系统能否正确地对与之相连的服务器或终端设备进行身份标识和鉴别；

n) 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，查看能否破解用户口令，破解口令后能否登录进入系统；

o) 应渗透测试主要服务器操作系统，验证已存在的账号（如安装一些服务后会系统会增加新应的账号）是否不能与系统进行交互式登录管理；

p) 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，例如，认证程序存在的安全漏洞，社会工程或其他手段等。

8.1.3.1.5 结果判定

a) 如果8.1.3.1.4 a）为肯定，则测评实施j）、k）和l）为肯定；

b) 如果不采用用户名/口令方式的进行身份鉴别，则8.1.3.1.4 n）不适用；

c) 如果8.1.3.1.4 o）中能破解口令，则该项为否定；

d) 如果8.1.3.1.4 p）中没有常见的绕过认证方式进行系统登录的方法，则该项为肯定；

e) 8.1.3.1.4 e）-m）均为肯定，则信息系统符合本单元测评项要求。

8.1.3.2 自主访问控制

8.1.3.2.1 测评项

a) 应依据安全策略控制用户对客体的访问；

b) 自主访问控制的覆盖范围应包括与信息安全直接相关的主体、客体及它们之间的操作；

c) 自主访问控制的粒度应达到主体为用户级，客体为文件、数据库表/记录、字段级；

d) 应由授权主体设置对客体访问和操作的权限；

e) 应实现操作系统和数据库系统特权用户的权限分离；

f) 权限分离应采用最小授权原则，分别授予不同用户各自为完成自己承担任务所需的最小权限，并在他们之间形成相互制约的关系；

g) 应禁止默认用户访问。

8.1.3.2.2 测评方式

检查，测试。

8.1.3.2.3 测评对象

主要服务器操作系统，主要数据库系统，安全策略。

8.1.3.2.4 测评实施

a) 应检查服务器操作系统和数据库系统的自主访问控制功能是否具有《信息安全等级保护 操作系统安全技术要求》和《信息安全等级保护 数据库管理系统安全技术要求》第二级以上或TCSEC C2级以上的测试报告；

b) 应检查服务器操作系统和数据库系统的安全策略，查看是否明确主体（如用户）以用户和/或用户组的身份规定对客体(如文件或系统设备,目录表和存取控制表访问控制等）的访问控制，覆盖范围是否包括与信息安全直接相关的主体（如用户）和客体（如文件，数据库表等）及它们之间的操作（如读、写或执行）；

c) 应检查服务器操作系统和数据库系统的安全策略，查看是否明确主体（如用户）具有非敏感标记（如角色），并能依据非敏感标记规定对客体的访问；

d) 应检查主要服务器操作系统和主要数据库系统的访问控制列表，查看授权用户中是否不存在过期的帐号和无用的帐号等；访问控制列表中的用户和权限，是否与安全策略相一致；

e) 应检查主要服务器操作系统和主要数据库系统，查看客体（如文件,数据库表、记录、字段等）的所有者是否可以改变其相应访问控制列表的属性，得到授权的用户是否可以改变相应客体访问控制列表的属性；

f) 应检查主要服务器操作系统和主要数据库系统，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(如系统管理员只能对系统进行维护,安全管理员只能进行策略配置和安全设置,安全审计员只能维护审计信息等)；

g) 应检查主要服务器操作系统和主要数据库系统，查看在系统管理员、安全管理员、安全审计员之间是否设置了相互制约关系（如系统管理员、安全管理员等不能对审计日志，安全审计员管理不了审计数据的开启、关闭、删除等重要事件的审计日志等)；

h) 应查看主要服务器操作系统和主要数据库系统，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（如限定在有限的范围内）；

i) 应查看主要服务器操作系统，查看匿名/默认用户是否已被禁用；

j) 应测试主要服务器操作系统和主要数据库系统，依据系统访问控制的安全策略，试图以未授权用户身份/角色访问客体，验证是否不能进行访问。

8.1.3.2.5 结果判定

a) 如果8.1.3.2.4 a）为肯定，则测评实施e）和j）为肯定；

b) 8.1.3.2.4 b）-j）均为肯定，则信息系统符合本单元测评项要求。

8.1.3.3 强制访问控制

8.1.3.3.1 测评项

a) 应对重要信息资源和访问重要信息资源的所有主体设置敏感标记；

b) 强制访问控制的覆盖范围应包括与重要信息资源直接相关的所有主体、客体及它们之间的操作；

c) 强制访问控制的粒度应达到主体为用户级，客体为文件、数据库表/记录、字段级。

8.1.3.3.2 测评方式

访谈，检查，测试。

8.1.3.3.3 测评对象

主要服务器操作系统，主要数据库系统，服务器操作系统文档，数据库系统文档。

8.1.3.3.4 测评实施

a) 应检查服务器操作系统和数据库系统的强制访问控制是否具有《信息安全等级保护操作系统安全技术要求》和《信息安全等级保护 数据库管理系统安全技术要求》第三级以上的测试报告；

b) 应检查主要服务器操作系统和主要数据库系统，查看是否能对重要信息资源和访问重要信息资源的所有主体设置敏感标记，这些敏感标记是否构成多级安全模型的属性库，主体和客体的敏感标记是否以默认方式生成或由安全员建立、维护和管理；

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

d) 应检查服务器操作系统和主要数据库系统文档，查看强制访问控制是否与用户身份鉴别、标识等安全功能密切配合，并且控制粒度达到主体为用户级，客体为文件和数据库表级；

e) 应测试主要服务器操作系统和主要数据库系统，依据系统文档描述的强制访问控制模型，以授权用户和非授权用户身份访问客体，验证是否只有授权用户可以访问客体，而非授权用户不能访问客体；

f) 应渗透测试主要服务器操作系统和主要数据库系统，可通过非法终止强制访问模块，非法修改强制访问相关规则，使用假冒身份等方式，测试强制访问控制是否安全、可靠。

8.1.3.3.5 结果判定

a) 如果8.1.3.3.4 a）为肯定，则测评实施b）、c）和e）为肯定；

b) 8.1.3.3.4 b）-e）均为肯定，则信息系统符合本单元测评项要求。

8.1.3.4 可信路径

8.1.3.4.1 测评项

a) 在用户进行初始登录和/或鉴别时，系统应在它与用户之间建立一条安全的信息传输通路。

8.1.3.4.2 测评方式

访谈，检查。

8.1.3.4.3 测评对象

安全管理员，主要服务器操作系统，主要数据库系统，服务器操作系统文档，数据库系统文档。

8.1.3.4.4 测评实施

a) 应检查服务器操作系统和数据库系统的可信路径功能是否具有《信息安全等级保护操作系统安全技术要求》和《信息安全等级保护 数据库管理系统安全技术要求》第四级以上的测试报告；

b) 可访谈安全管理员，询问在什么情况下起用可信路径进行初始登录和/或鉴别；目前系统提供了哪些可信路径；

c) 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；

d) 应检查主要服务器操作系统，查看文档声称的可信路径功能是否有效；

e) 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和/或鉴别；目前系统提供了哪些可信路径；

f） 应检查数据库系统文档，查看系统提供了哪些可信路径功能；
g） 应检查主要数据库系统，查看文档声称的可信路径功能是否有效。

8.1.3.4.5 结果判定

a） 如果8.1.3.4.4 a）为肯定，则测评实施d）和g）为肯定；
b） 8.1.3.4.4 d）和g）为肯定，则信息系统符合本单元测评项要求。

8.1.3.5 安全审计

8.1.3.5.1 测评项

a） 安全审计应覆盖到服务器和客户端上的所有用户；
b） 安全审计应记录系统内重要的安全相关事件，包括重要用户行为、系统资源的异常使用和重要系统命令的使用；
c） 安全相关事件的记录应包括日期和时间、类型、主体标识、客体标识、客体敏感标记、事件的结果等；
d） 安全审计应可以根据记录数据进行分析，并生成审计报表；
e） 安全审计应可以对特定事件，提供指定方式的实时报警；
f） 审计进程应受到保护避免受到未预期的中断；
g） 审计记录应受到保护避免受到未预期的删除、修改或覆盖等；
h） 安全审计应能跟踪监测到可能的安全侵害事件，并终止违规进程；
i） 安全审计应根据信息系统的统一安全策略，实现集中审计；
j） 系统设备时钟应与时钟服务器时钟保持同步。

8.1.3.5.2 测评方式

访谈，检查，测试。

8.1.3.5.3 测评对象

安全审计员，主要服务器和重要终端操作系统，主要数据库系统。

8.1.3.5.4 测评实施

a） 可访谈安全审计员，询问主机系统是否设置安全审计；询问主机系统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） 应检查主要服务器操作系统、重要终端操作系统和主要数据库系统，查看当前审计范围是否覆盖到每个用户；
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系统，查看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、自主访问控制的所有操作记录、重要用户行为（如用超级用户命令改变用户身份，删除系统表）、系统资源的异常使用、重要系统命令的使用（如删除客体）等；
d） 应检查主要服务器操作系统、重要终端操作系统和主要数据库系统，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、身份鉴别事件中请求的来源（如末端标识符）、事件的结果等内容；
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浏览和分析审计数据提供专门的审计工具（如对审计记录进行分类、排序、查询、统计、分析和组合查询等），并能根据需要生成审计报表；
f） 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系统，查看能否对特定事件指定实时报警方式（如声音、EMAIL、短信等）；
g） 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系统，查看审计跟踪设置是否定义了审计跟踪极限的阈值，当存储空间接近极限时，能指定采取必要的措施（如报警并导出）；当存储空间被耗尽时，终止可审计事件的发生；
h） 应检查主要服务器、重要终端操作系统和主要数据库系统，查看是否提供集中审计

系统连接的接口，并能根据集中审计系统的要求发送审计数据；

i) 应检查主要服务器和重要终端操作系统的时钟，查看是否与时钟服务器的时间保持同步；

j) 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系统，可通过非法终止审计功能或修改其配置，验证审计功能是否受到保护；

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

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

m) 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系统，产生一些安全侵害事件，查看安全审计能否跟踪监测到这些安全侵害事件，并终止违规进程。

8.1.3.5.5 结果判定

a) 8.1.3.5.4 b）-m）均为肯定，则信息系统符合本单元测评项要求。

8.1.3.6 系统保护

8.1.3.6.1 测评项

a) 系统因故障或其他原因中断后，应能够以手动或自动方式恢复运行；

b) 应对被保护存储单元的访问和操作权限加以控制，当发生对存储单元的未授权执行行为时，系统应能及时报警或者中断执行行为。

8.1.3.6.2 测评方式

访谈，检查，测试。

8.1.3.6.3 测评对象

系统管理员，主要服务器操作系统。

8.1.3.6.4 测评实施

a) 应访谈系统管理员，询问主要服务器操作系统中被保护的存储单元近来是否出现被频繁非法访问或操作，如果出现过，是否重新对访问和操作的权限进行过改进；

b) 应访谈系统管理员，询问哪些故障或其他原因会导致服务器系统中断，中断后能否以手动或自动方式恢复运行，相应操作规程有哪些；

c) 应检查主要服务器操作系统，查看主要服务器操作系统中被保护的存储单元有哪些（如注册表，系统文件），是否对保护存储单元的访问和操作权限加以控制，当发生对存储单元的未授权执行行为时，系统能否及时报警或者中断执行行为，系统报警的方式有哪些；

d) 应测试主要服务器操作系统，可通过人为制造一些故障（如断电等），验证服务器系统因故障或其他原因中断后，能否够以手动或自动方式恢复运行；

e) 应测试主要服务器操作系统，试图非法访问或操作被保护存储单元，查看系统能否及时报警或者中断非法行为。

8.1.3.6.5 结果判定

a) 如果主要服务器操作系统中被保护的存储单元未出现过被频繁非法访问或操作，则8.1.3.6.4 a）为不适用；

b) 如果系统管理员能够描述出主要故障或其他原因，以及相应操作规程，则8.1.3.6.4 b）为肯定；

c) 8.1.3.6.4 a）-e）均为肯定，则信息系统符合本单元测评项要求。

8.1.3.7 剩余信息保护

8.1.3.7.1 测评项

a) 应保证操作系统和数据库管理系统用户的鉴别信息所在的存储空间，被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中；

b) 应确保系统内的文件、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。

8.1.3.7.2 测评方式

访谈，检查。

8.1.3.7.3 测评对象

系统管理员，数据库管理员，主要服务器操作系统维护/操作手册，主要数据库系统维护/操作手册。

8.1.3.7.4 测评实施

a) 应检查服务器操作系统和数据库系统的剩余信息保护（用户数据保密性保护/客体重用）功能是否具有《信息安全等级保护 操作系统安全技术要求》和《信息安全等级保护 数据库管理系统安全技术要求》第二级以上的测试报告；

b) 应与系统管理员访谈，询问操作系统用户的鉴别信息存储空间，被释放或再分配给其他用户前是否得到完全清除；系统内的文件、目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是否得到完全清除；

c) 应与数据库管理员访谈，询问数据库管理员用户的鉴别信息存储空间，被释放或再分配给其他用户前是否得到完全清除；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是否得到完全清除；

d) 应检查主要操作系统和主要数据库系统维护操作手册，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；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。

8.1.3.7.5 结果判定

a) 如果 8.1.3.7.4 a）为肯定，则测评实施 b）-d）为肯定；

b) 8.1.3.7.4 b）-d）均为肯定，则信息系统符合本单元测评项要求。

8.1.3.8 入侵防范

8.1.3.8.1 测评项

a) 应进行主机运行监视，包括监视主机的CPU、硬盘、内存、网络等资源的使用情况；

b) 应设定资源报警域值，以便在资源使用超过规定数值时发出报警；

c) 应进行特定进程监控，限制操作人员运行非法进程；

d) 应进行主机账户监控，限制对重要账户的添加和更改；

e) 应检测各种已知的入侵行为，记录入侵的源IP、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时提供报警；

f) 主机系统应根据安全策略阻止某些指定的入侵事件；

g) 应能够检测重要程序完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施。

8.1.3.8.2 测评方式

访谈，检查，测试。

8.1.3.8.3 测评对象

系统管理员，主要服务器系统。

8.1.3.8.4 测评实施

a) 应访谈系统管理员，询问主机系统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、资源使用超过值报警、特定进程监控、入侵行为检测、完整性检测等方面内容；

b) 应访谈系统管理员，询问入侵防范产品的厂家、版本和在主机系统中的安装部署情况；询问是否进行过部署的改进或者更换过产品，是否按要求（如定期或实时）进行产品升级；

c) 应检查主要服务器系统，查看是否进行主机运行监视，监视的内容是否包括主机的CPU、硬盘、内存、网络等资源的使用情况，并给出资源使用历史记录；

d) 应检查主要服务器系统，查看是否设定资源报警阈值（如 CPU、硬盘、内存、网络等资源的报警阈值）以便在资源使用超过规定数值时发出报警，并查看报警方式有哪些；

e) 应检查主要服务器系统，查看是否对特定进程（包括主要的系统进程，如 WINDOWS 的 Explorer 进程）进行监控，是否可以设定非法进程列表；

f) 应检查主要服务器系统，查看是否对主机账户（如系统管理员）进行控制，以限制对重要账户的添加和更改等；

g) 应检查主要服务器系统，查看能否记录攻击者的源 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、EMAIL 等），在其响应处置方式中是否包含有对某些入侵事件的阻断，并已配置使用；

h) 应测试主要服务器系统，试图运行非法进程，验证其能否限制非法进程的运行；试图添加或更改重要账户，验证主机能否限制重要账户的添加和更改；

i) 应测试主要服务器系统，试图破坏重要程序（如执行系统任务的重要程序）的完整性，验证主机能否检测到重要程序的完整性受到破坏。

8.1.3.8.5 结果判定

a) 如果 8.1.3.8.4 b）中的厂家为正规厂家（如有销售许可），版本号较新，改进合理，定期升级，则该项为肯定；

b) 8.1.3.8.4 a）-i）均为肯定，则信息系统符合本单元测评项要求。

8.1.3.9 恶意代码防范

8.1.3.9.1 测评项

a) 服务器和终端设备（包括移动设备）均应安装实时检测和查杀恶意代码的软件产品；

b) 主机系统防恶意代码产品应具有与网络防恶意代码产品不同的恶意代码库；

c) 应支持恶意代码防范的统一管理。

8.1.3.9.2 测评方式

访谈，检查，测试。

8.1.3.9.3 测评对象

安全员，主要服务器，主要终端，网络防恶意代码产品，主机安全设计/验收文档。

8.1.3.9.4 测评实施

a) 应访谈安全员，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情况如何，因何改进过部署或者更换过产品，是否按要求（如定期或实时）进行产品升级；

b) 应检查主机恶意代码防范方面的设计/验收文档，查看描述的安装范围是否包括服务器和终端设备（包括移动设备）；

c） 应检查主要服务器系统和主要终端系统，查看是否安装实时检测与查杀恶意代码的软件产品，查看实时检测与查杀恶意代码的软件产品是否支持恶意代码防范的统一管理功能，查看检测与查杀恶意代码软件产品的厂家、版本号和恶意代码库名称；

d） 应检查网络防恶意代码产品，查看其厂家、版本号和恶意代码库名称。

8.1.3.9.5 结果判定

a） 如果8.1.3.9.4 a）中恶意代码实时检测与查杀措施的部署到所有服务器和重要终端，则该项为肯定；

b） 8.1.3.9.4 a）-c）均为肯定，检查发现主机系统防恶意代码产品与网络防恶意代码产品使用不同的恶意代码库（如厂家、版本号和恶意代码库名称不相同等），则信息系统符合本单元测评项要求。

8.1.3.10 资源控制

8.1.3.10.1 测评项

a） 应限制单个用户的多重并发会话；

b） 应对最大并发会话连接数进行限制；

c） 应对一个时间段内可能的并发会话连接数进行限制；

d） 应通过设定终端接入方式、网络地址范围等条件限制终端登录；

e） 应根据安全策略设置登录终端的操作超时锁定和鉴别失败锁定，并规定解锁或终止方式；

f） 应禁止同一用户账号在同一时间内并发登录；

g） 应限制单个用户对系统资源的最大或最小使用限度；

h） 当系统的服务水平降低到预先规定的最小值时，应能检测和报警；

i） 应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。

8.1.3.10.2 测评方式

检查，测试。

8.1.3.10.3 测评对象

主要服务器操作系统。

8.1.3.10.4 测评实施

a） 应检查主要服务器操作系统，查看是否限制单个用户的多重并发会话数量；查看是否设置登录终端的操作超时锁定和鉴别失败锁定，以及是否规定解锁或终止方式；查看是否配置了终端接入方式、网络地址范围等条件限制终端登录；

b） 应检查重要服务器操作系统，查看是否对一个时间段内可能的并发会话连接数进行限制，是否禁止同一用户账号在同一时间内并发登录，是否限制单个用户对系统资源（如 CPU、内存和硬盘等）的最大或最小使用限度；

c) 应检查重要服务器操作系统，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，报警的方式有哪些，能否已根据安全策略设定主体（如进程）的服务优先级，并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；

d） 应测试主要服务器操作系统，任选一个用户，登录服务器，试图发出多重并发会话，验证系统是否限制单个用户的多重并发会话；试图在一段时间内建立一些并发会话连接，验证系统是否对一定时间段内的并发会话连接数进行限制；

e） 应测试重要服务器操作系统，任选一个用户帐户，登录服务器，用不同的终端接入方式、网络地址试图登录服务器，验证重要服务器操作系统是否通过终端接入方式、网络地址范围等条件限制终端登录。

f） 应测试主要服务器操作系统，试图使服务水平降低到预先规定的最小值，验证系统能否正确检测和报警；

g） 应测试主要服务器操作系统，任选一个用户，登录服务器，在一定时间内不进行任何动作，验证主要服务器操作系统能否对操作超时的终端进行锁定；任选一个用户，可通过多次失败登录服务器，验证服务器能否对鉴别失败的终端进行锁定，锁定后能否按照规定的解锁或终止方式进行解锁或终止。

8.1.3.10.5 结果判定

a） 8. 1. 3. 10. 4 a）-g）均为肯定，则信息系统符合本单元测评项要求。

8.1.4 应用安全

8.1.4.1 身份鉴别

8.1.4.1.1 测评项

a） 系统用户的身份标识应具有唯一性；

b） 应对登录的用户进行身份标识和鉴别；

c） 应对同一用户采用两种或两种以上组合的鉴别技术实现用户身份鉴别；

d） 系统用户的身份鉴别信息应具有不易被冒用的特点，例如口令长度、复杂性和定期的更新等；

e） 系统用户的身份鉴别信息至少有一种应是不可伪造的，例如以公私钥对、生物特征等作为身份鉴别信息；

f） 应具有登录失败处理功能，如结束会话、限制非法登录次数，当登录连接超时自动退出；

g） 应具有鉴别警示功能；

h） 应用系统应及时清除存储空间中动态使用的鉴别信息。

8.1.4.1.2 测评方式

访谈，检查，测试。

8.1.4.1.3 测评对象

系统管理员，应用系统，设计/验收文档，操作规程。

8.1.4.1.4 测评实施

a) 可访谈系统管理员，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（如复杂性混有大、小写字母、数字和特殊字符，口令周期等）；

b) 可访谈系统管理员，询问应用系统是否具有登录失败处理的功能，是如何进行处理的；询问应用系统对用户标识在整个生命周期内是否具有唯一性（如UID、用户名或其他信息在系统中是唯一的，用该标识在整个生命周期内能唯一识别该用户）；

c） 应检查设计/验收文档，查看系统是否有系统采取了唯一标识（如用户名、UID或其他属性）的说明；

d） 应检查操作规程和操作记录，查看其是否有管理身份标识和鉴别的操作规程、审批记录和操作记录；

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（如采用用户名/口令、挑战应答、动态口令、物理设备、生物识别技术中的任意两个组合），其中应有一种应是不可伪造的（如数字证书或生物识别技术）；对有抗抵赖要求的系统，查看其是否采用数字证书方式的身份鉴别技术；

f） 应检查应用系统，查看其是否配备身份标识（如建立账号）和鉴别（如口令等）功能；查看其其身份鉴别信息是否具有不易被冒用的特点，例如复杂性（如规定字符应混有大、小写字母、数字和特殊字符）或为了便于记忆使用了令牌；

g) 应检查应用系统，查看其是否配备并使用登录失败处理功能（如登录失败次数超过设定值，系统自动退出等）；

h) 应测试应用系统，可通过注册用户，并登录系统，查看登录是否成功，验证其身份标识和鉴别功能是否有效；可通过删除一个用户然后再重新注册相同标识的用户，查看能否成功，验证其身份标识在应用系统整个生命周期内是否具有唯一性；

i) 应测试应用系统，验证其登录失败处理，非法登录次数限制，登录连接超时自动退出等功能是否有效；

j) 应测试应用系统，验证其是否及时清除存储空间中动态使用的鉴别信息（如登录系统，退出系统后重新登录系统，查看上次登录的鉴别信息是否存在）；

k) 应测试应用系统，验证其是否有鉴别警示功能（如系统有三次登录失败则锁定该用户的限制，则应给用户必要的提示）；

l) 应渗透测试应用系统，测试身份鉴别信息是否不易被冒用（如通过暴力破解或其他手段进入系统，对WEB系统可采用SQL注入等绕过身份鉴别的方法）。

8.1.4.1.5 结果判定

a) 如果8.1.4.1.4 d）中相关文档有用户唯一性标识的描述，则该项为肯定；

b) 如果8.1.4.1.4 d）中缺少相应的文档，则该项为否定；

c) 8.1.4.1.4 c）-k）均为肯定，则信息系统符合本单元测评项要求。

8.1.4.2 访问控制

8.1.4.2.1 测评项

a) 应依据安全策略控制用户对客体的访问；

b) 自主访问控制的覆盖范围应包括与信息安全直接相关的主体、客体及它们之间的操作；

c) 自主访问控制的粒度应达到主体为用户级，客体为文件、数据库表级；

d) 应由授权主体设置用户对系统功能操作和对数据访问的权限；

e) 应实现应用系统特权用户的权限分离，例如将管理与审计的权限分配给不同的应用系统用户；

f) 权限分离应采用最小授权原则，分别授予不同用户各自为完成自己承担任务所需的最小权限，并在它们之间形成相互制约的关系；

g) 应用系统的设计应采用二层以上结构，将提供数据显示功能与数据处理功能在物理或者逻辑上分离；

h) 应禁止默认用户访问；

i) 主体和客体具有安全标记，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。

8.1.4.2.2 测评方式

访谈，检查，测试。

8.1.4.2.3 测评对象

系统管理员，应用系统。

8.1.4.2.4 测评实施

a) 可访谈系统管理员，询问业务系统是否提供访问控制措施，具体措施有哪些，自主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（如文件和数据库中的数据）的访问；

c) 应检查应用系统，查看其自主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；自主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（如数据库表、视图、存储过程等）；

d) 应检查应用系统，查看应用系统是否有对授权主体进行系统功能操作和对数据访问权限进行设置的功能；

e) 应检查应用系统，查看其特权用户的权限是否分离（如将系统管理员、安全员和审计员的权限分离），权限之间是否相互制约（如系统管理员、安全管理员等不能对审计日志进行管理，安全审计员不能管理审计功能的开启、关闭、删除等重要事件的审计日志等）；

f) 应检查应用系统，查看其是否有限制默认用户访问权限的功能，并已配置使用；

g) 应检查应用系统，查看其是否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是否有效；

h) 应测试应用系统，可通过用不同权限的用户登录，查看其权限是否受到应用系统的限制，验证系统权限分离功能是否有效；

i) 应测试应用系统，可通过授权主体设置特定用户对系统功能进行操作和对数据进行访问的权限，然后以该用户登录，验证用户权限管理功能是否有效；

j) 应测试应用系统，可通过用默认用户登录（默认密码），并用该用户进行操作（包括合法、非法操作），验证系统对默认用户访问权限的限制是否有效；

k) 应渗透测试应用系统，测试自主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（如试图绕过系统访问控制机制等操作）；

l) 应渗透测试应用系统，通过试图对系统进行绕过访问控制的操作，查看系统自主访问控制是否存在缺陷。

8.1.4.2.5 结果判定

a) 8.1.4.2.4 b）-k）均为肯定，则信息系统符合本单元测评项要求。

8.1.4.3 安全审计

8.1.4.3.1 测评项

a) 安全审计应覆盖到应用系统的每个用户；

b) 安全审计应记录应用系统重要的安全相关事件，包括重要用户行为、系统资源的异常使用和重要系统功能的执行等；

c) 安全相关事件的记录应包括日期和时间、类型、主体标识、客体标识、客体敏感标记、事件的结果等；

d) 安全审计应可以根据记录数据进行分析，并生成审计报表；

e) 安全审计应可以对特定事件，提供指定方式的实时报警；

f) 审计进程应受到保护避免受到未预期的中断；

g) 审计记录应受到保护避免受到未预期的删除、修改或覆盖等；

h) 安全审计应能跟踪监测到可能的安全侵害事件，并终止违规进程；

i) 审计员应能够定义审计跟踪极限的阈值，当存储空间接近极限时，能采取必要的措施（如报警并导出），当存储空间被耗尽时，终止可审计事件的发生；

j) 安全审计应根据信息系统的统一安全策略，实现集中审计。

8.1.4.3.2 测评方式

访谈，检查，测试。

8.1.4.3.3 测评对象

审计员，应用系统。

8.1.4.3.4 测评实施

a) 可访谈安全审计员，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、自主访问控制的所有操作记录、重要用户行为（如用超级用户命令改变用户身份，删除系统表）、系统资源的异常使用、重要系统命令的使用（如删除客体）等；

d) 应检查应用系统，查看安全相关事件的记录是否包括了日期和时间、类型、主体标识、客体标识、客体敏感标记、事件的结果等信息；

e) 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（如末端标识符）、事件的结果等内容；

f) 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工具（如对审计记录进行分类、排序、查询、统计、分析和组合查询等），并能根据需要生成审计报表；

g) 应检查应用系统，查看其能否对特定事件指定实时报警方式（如声音、EMAIL、短信等）；

h) 应检查应用系统，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，能否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；

i) 应检查应用系统，查看其安全审计是否是根据信息系统的统一安全策略，实现集中审计的；

j) 应测试应用系统，可通过非法终止审计功能或修改其配置，验证审计功能是否受到保护；

k) 应测试应用系统，在系统上以某个用户试图产生一些重要的安全相关事件（如鉴别失败等），测试安全审计的覆盖情况和记录情况与要求是否一致；

l) 应测试应用系统，在系统上以某个系统用户试图删除、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；

m) 应测试应用系统，制造一些安全事件，查看安全审计是否能跟踪监测到可能的安全侵害事件，并终止违规进程，验证其功能是否正确。

8.1.4.3.5 结果判定

a) 8.1.4.3.4 b）-m）均为肯定，则信息系统符合本单元测评项要求。

8.1.4.4 剩余信息保护

8.1.4.4.1 测评项

a) 应保证用户的鉴别信息所在的存储空间，被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中；

b) 应确保系统内的文件、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。

8.1.4.4.2 测评方式

访谈，检查，测试。

8.1.4.4.3 测评对象

系统管理员，设计/验收文档。

8.1.4.4.4 测评实施

a) 可访谈管理员，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/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/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）。

8.1.4.4.5 结果判定

a) 如果8.1.4.4.4 b）-c）缺少相关材料，则该项为否定；

b) 8.1.4.4.4 b）-d）均为肯定，则信息系统符合本单元测评项要求。

8.1.4.5 通信完整性

8.1.4.5.1 测评项

a) 通信双方应约定密码算法，计算通信数据报文的报文验证码，在进行通信时，双方根据校验码判断对方报文的有效性。

8.1.4.5.2 测评方式

访谈，测试。

8.1.4.5.3 检查，测评对象

安全员，应用系统，设计/验收文档。

8.1.4.5.4 测评实施

a) 可访谈安全员，询问业务系统是否有数据在传输过程中进行完整性保证的操作，具体措施是什么；

b) 应检查设计/验收文档，查看其是否有通信完整性的说明，如果有则查看其是否有系统是根据校验码判断对方数据包的有效性的，用密码计算通信数据报文的报文验证码的描述；

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是否有验证码。

8.1.4.5.5 结果判定

a) 8.1.4.5.4 b）-c）均为肯定，则信息系统符合本单元测评项要求。

8.1.4.6 通信保密性

8.1.4.6.1 测评项

a) 当通信双方中的一方在一段时间内未作任何响应，另一方应能够自动结束会话；

b) 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；

c) 在通信过程中，应对整个报文或会话过程进行加密；

d) 应选用符合国家有关部门要求的密码算法；

e) 应基于硬件化的设备，产生密钥，进行加解密运算。

8.1.4.6.2 测评方式

访谈，检查，测试。

8.1.4.6.3 测评对象

安全员，应用系统，相关证明材料（证书）。

8.1.4.6.4 测评实施

a) 可访谈安全员，询问业务系统数据在存储和传输过程中是否采取保密措施（如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，在通信过程中对敏感信息字段进行加密等），具体措施有哪些，是否所有应用系统的通信都采取了上述措施；

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要求；

d) 应测试应用系统，查看当通信双方中的一方在一段时间内未作任何响应，另一方是否能自动结束会话；系统是否能在通信双方建立连接之前，利用密码技术进行会话初始化验证（如SSL建立加密通道前是否利用密码技术进行会话初始验证）；在通信过程中，是否对整个报文或会话过程进行加密；

e) 应测试应用系统，通过通信双方中的一方在一段时间内未作任何响应，查看另一方是否能自动结束会话，测试当通信双方中的一方在一段时间内未作任何响应，另一方是否能自动结束会话的功能是否有效；

f) 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。

8.1.4.6.5 结果判定

a) 如果8.1.4.6.4 c）缺少相关材料，则该项为否定；

b) 8.1.4.6.4 b）-f）均为肯定，则信息系统符合本单元测评项要求。

8.1.4.7 抗抵赖

8.1.4.7.1 测评项

a) 应具有在请求的情况下为数据原发者或接收者提供数据原发证据的功能；

b) 应具有在请求的情况下为数据原发者或接收者提供数据接收证据的功能。

8.1.4.7.2 测评方式

访谈，测试。

8.1.4.7.3 测评对象

安全员，应用系统。

8.1.4.7.4 测评实施

a) 可访谈安全员，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或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或接收者提供数据接收证据的功能。

8.1.4.7.5 结果判定

a) 8.1.4.7.4 b）为肯定，则信息系统符合本单元测评项要求。

8.1.4.8 软件容错

8.1.4.8.1 测评项

a) 应对通过人机接口输入或通过通信接口输入的数据进行有效性检验；

b) 应对通过人机接口方式进行的操作提供“回退”功能，即允许按照操作的序列进行回退；

c) 应有状态监测能力，当故障发生时，能实时检测到故障状态并报警；

d) 应有自动保护能力，当故障发生时，自动保护当前所有状态；

e) 应有自动恢复能力，当故障发生时，立即启动新的进程，恢复原来的工作状态。

8.1.4.8.2 测评方式

访谈，检查，测试。

8.1.4.8.3 测评对象

系统管理员，应用系统。

8.1.4.8.4 测评实施

a) 可访谈系统管理员，询问业务系统是否有保证软件具有容错能力的措施（如对人机接口输入或通过通信接口输入的数据进行有效性检验等），具体措施有哪些；

b) 应检查应用系统，查看业务系统是否对人机接口输入（如用户界面的数据输入）或通信接口输入的数据进行有效性检验；是否允许按照操作的序列进行回退（如撤消操作）；是否在故障发生时继续提供一部分功能，确保能够实施必要的措施（如对重要数据的保存）；

c) 应检查应用系统，查看其是否具有状态监控能力，当故障发生时，是否能实时检测到故障状态并报警；系统是否具有自动保护能力，当故障发生时，是否能自动保护当前所有状态；

d) 应检查应用系统，查看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；

e) 应测试应用系统，可通过输入的不同（如数据格式或长度等符合、不符合软件设定的要求），验证系统人机接口有效性检验功能是否正确；

f) 应测试应用系统，可通过多步操作，然后回退，验证系统能否按照操作的序列进行正确的回退；可通过给系统人为制造一些故障（如系统异常），验证系统能否在故障发生时继续提供一部分功能，并能实施必要的措施；

g) 应测试应用系统，通过制造异常事件，验证系统是否能实时检测到故障状态并报警，能否自动保护当前所有状态，是否具有自动恢复能力（当故障发生时，立即启动新的进程，恢复原来的工作状态）。

8.1.4.8.5 结果判定

a) 8.1.4.8.4 b）-g）为肯定，则信息系统符合本单元测评项要求。

8.1.4.9 资源控制

8.1.4.9.1 测评项

a) 应限制单个用户的多重并发会话；

b) 应对最大并发会话连接数进行限制；

c) 应对一个时间段内可能的并发会话连接数进行限制；

d) 应根据安全策略设置登录终端的操作超时锁定和鉴别失败锁定，并规定解锁或终止方式；

e) 应禁止同一用户账号在同一时间内并发登录；

f) 应对一个访问用户或一个请求进程占用的资源分配最大限额和最小限额；

g) 应根据安全属性（用户身份、访问地址、时间范围等）允许或拒绝用户建立会话连接；

h) 当系统的服务水平降低到预先规定的最小值时，应能检测和报警；

i) 应确定访问用户或请求进程的优先级，对全部资源采用优先服务机制。

8.1.4.9.2 测评方式

访谈，检查，测试。

8.1.4.9.3 测评对象

系统管理员，应用系统。

8.1.4.9.4 测评实施

a) 可访谈系统管理员，询问业务系统是否有资源控制的措施（如对应用系统的最大并发会话连接数进行限制，是否禁止同一用户账号在同一时间内并发登录，是否对一个时间段内可能的并发会话连接数进行限制，对一个访问用户或一个请求进程占用的资源分配最大限额和最小限额等），具体措施有哪些；

b) 应检查应用系统，查看是否有限制单个用户的多重并发会话；系统是否有最大并发会话连接数的限制，是否有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，查看是否根据安全策略设置登录终端的操作超时锁定和鉴别失败锁定，并规定解锁或终止方式；是否禁止同一用户账号在同一时间内并发登录；是否对一个访问用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，查看是否根据安全属性（用户身份、访问地址、时间范围等）允许或拒绝用户建立会话连接；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，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单个用户的多重并发会话连接，验证系统能否正确地限制单个用户的多重并发会话数；可通过对系统进行超过最大并发会话连接数进行连接，验证系统能否正确地限制最大并发会话连接数；

f) 应测试应用系统，可通过在一个时间段内，用超过设定的并发连接数对系统进行连接，查看能否连接成功，验证系统对一个时间段内可能的并发会话连接数进行限制的功能是否正确；

g) 应测试应用系统，可通过设置登录终端的操作超时锁定和鉴别失败锁定，并规定解锁或终止方式，制造操作超时和鉴别失败，验证系统能否锁定，解锁或终止方式是否和设定的方式相同；

h) 应测试应用系统，可通过按照安全属性（用户身份、访问地址、时间范围等）设定允许或拒绝某个用户建立会话连接，然后用该用户进行对应的操作，验证查看系统能否正确地根据安全属性允许或拒绝用户建立会话连接；试图使服务水平降低到预先规定的最小值，验证系统能否正确检测并报警。

8.1.4.9.5 结果判定

a) 8.1.4.9.4 b）-h）肯定，则信息系统符合本单元测评项要求。

8.1.4.10 代码安全

8.1.4.10.1 测评项

a) 应制定应用程序代码编写安全规范，要求开发人员参照规范编写代码；

b) 应对应用程序代码进行代码复审，识别可能存在的恶意代码；

c) 应对应用程序代码进行安全脆弱性分析；

d) 应对应用程序代码进行穿透性测试；

e) 应对应用程序代码进行严格的代码复审，识别可能存在的隐蔽信道。

8.1.4.10.2 测评方式

访谈，检查。

8.1.4.10.3 测评对象

系统管理员，应用系统，设计/验收文档，相关证明材料（证书）。

8.1.4.10.4 测评实施

a) 可访谈系统管理员，询问业务系统是否有保证质量的措施（如系统是否应用程序代码编写安全规范，开发人员是否参照规范编写代码），具体措施有哪些；

b） 应检查设计/验收文档和其他相关文档，查看是否有应用程序代码编写安全规范；
c） 应检查设计/验收文档和相关证明材料（证书），查看是否有对应用程序代码进行代码复审；
d） 应检查设计/验收文档和相关证明材料（证书），查看是否对应用代码进行安全脆弱性分析；
e） 应检查设计/验收文档和相关证明材料（证书），查看是否有对应用代码进行穿透性测试的声明；
f） 应检查设计/验收文档和相关证明材料（证书），查看是否有对应用代码进行严格的代码复审，识别可能存在的隐蔽信道的声明；
g） 应检查应用系统，查看应用程序代码的编制与代码安全规范要求是否一致。

8.1.4.10.5 结果判定

a） 如果8.1.4.10.4 b）-f）缺少相关材料，则该项为否定；
b） 8.1.4.10.4 b）-g）均为肯定，则信息系统符合本单元测评项要求。

8.1.5 数据安全

8.1.5.1 数据完整性

8.1.5.1.1 测评项

a） 应能够检测到系统管理数据、鉴别信息和用户数据在传输过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施；
b） 应能够检测到系统管理数据、鉴别信息和用户数据在存储过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施；
c） 应能够检测重要系统完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施；
d） 应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。

8.1.5.1.2 测评方式

访谈，检查。

8.1.5.1.3 测评对象

系统管理员、网络管理员、安全员、数据库管理员，应用系统，设计/验收文档，相关证明性材料（如证书、检验报告等）。测评实施

a） 可访谈安全员，询问业务系统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；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、数据库管理系统的设计/验收文档或相关证明性材料（如证书、检验报告等）等，查看其是否有能检测/验证到系统管理数据（如WINDOWS 域管理、目录管理数据）、鉴别信息（如用户名和口令）和用户数据（如用户数据文件）在传输过程中完整性受到破坏；能否检测到系统管理数据、身份鉴别信息和用户数据（如防火墙的访问控制规则）在存储过程中完整性受到破坏；能否检测到重要系统完整性受到破坏；在检测到完整性错误时采取必要的恢复措施，具体的恢复措施有哪些；
d） 应检查应用系统，查看其是否配备检测/验证系统管理数据、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/验证系统管理数据、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/验证重要系统/模块完整性受到破坏的功能；在检测/验证到完整性错误时能采取的具体恢复措施有哪些；

e） 应检查操作系统、网络设备、数据库管理系统和应用系统中为重要通信提供的、具体的专用通信协议或安全通信协议服务是否正在运行使用。

8.1.5.1.5 结果判定

a) 如果操作系统、网络设备、数据库管理系统和应用系统中任意一种能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），则 8. 1. 5. 1. 4 b）为肯定；

b) 如果 8. 1. 5. 1. 4 c）缺少相关材料，则该项为否定；

c） 8. 1. 5. 1. 4 b）-e）均为肯定，则信息系统符合本单元测评项要求。

8.1.5.2 数据保密性

8.1.5.2.1 测评项

a） 网络设备、操作系统、数据库系统和应用系统的鉴别信息、敏感的系统管理数据和敏感的用户数据应采用加密或其他有效措施实现传输保密性；

b） 网络设备、操作系统、数据库系统和应用系统的鉴别信息、敏感的系统管理数据和敏感的用户数据应采用加密或其他保护措施实现存储保密性；

c） 当使用便携式和移动式设备时，应加密或者采用可移动磁盘存储敏感信息；

d） 用于特定业务通信的通信信道应符合相关的国家规定；

e） 网络设备、操作系统、数据库管理系统和应用系统应为重要通信提供专用协议或安全通信协议服务，避免来自基于通用协议的攻击，破坏数据保密性。

8.1.5.2.2 测评方式

访谈，检查，测试。

8.1.5.2.3 测评对象

系统管理员、网络管理员、安全员、数据库管理员，操作系统，网络设备，数据库系统，应用系统，设计/验收文档，相关证明性材料（如证书、检验报告等）。

8.1.5.2.4 测评实施

a) 可访谈网络管理员，询问信息系统中的网络设备的鉴别信息、敏感的系统管理数据和敏感的用户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保护措施实现存储保密性；

b) 可访谈系统管理员，询问信息系统中的操作系统的鉴别信息、敏感的系统管理数据和敏感的用户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保护措施实现存储保密性；

c) 可访谈数据库管理员，询问信息系统中的数据库管理系统的鉴别信息、敏感的系统管理数据和敏感的用户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保护措施实现存储保密性；

d) 可访谈安全员，询问信息系统中的应用系统的鉴别信息、敏感的系统管理数据和敏感的用户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保护措施实现存储保密性；

e) 可访谈安全员，询问系统采用的密码算法和密钥是否符合国家密码管理规定；

f) 可访谈安全员，询问当使用便携式和移动式设备时，是否加密或者采用可移动磁盘存储敏感信息；

g) 应检查操作系统、网络设备、数据库系统、应用系统的设计/验收文档，查看其是否有关于应用系统的鉴别信息、敏感的系统管理数据和敏感的用户数据采用加密或

其他有效措施实现传输保密性描述，是否有采用加密或其他保护措施实现存储保密性的描述；

h) 应检查相关证明性材料（如证书或其他相关材料等），查看其是否有特定业务通信的通信信道、密码算法和密钥符合相关国家规定的说明。

i) 应检查应用系统，查看其鉴别信息、敏感的系统管理数据和敏感的用户数据是否采用加密或其他有效措施实现传输保密性描述，是否采用加密或其他保护措施实现存储保密性；

j) 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。

8.1.5.2.5 结果判定

a) 如果 8. 1. 5. 2. 4 g）缺少相关材料，则该项为否定；

b) 如果没有相关证明性材料（如证书、检验报告等），8. 1. 5. 2. 4 h） 为否定；

c) 8. 1. 5. 2. 4 g）-i）均为肯定，则信息系统符合本单元测评项要求。

8.1.5.3 数据备份和恢复

8.1.5.3.1 测评项

a） 应提供自动备份机制实现数据实时本地和异地备份；

b） 应提供恢复数据的功能；

c） 应提供重要网络设备、通信线路和服务器的硬件冗余；

d） 应提供重要业务系统的本地和异地系统级热备份；

e） 应提供自动机制在灾难发生时实现自动业务切换和恢复。

8.1.5.3.2 测评方式

访谈，检查，测试。

8.1.5.3.3 测评对象

系统管理员、网络管理员、安全员、数据库管理员，操作系统，网络设备，数据库系统，业务系统，业务系统设计/验收文档。

8.1.5.3.4 测评实施

a) 可访谈网络管理员，询问信息系统中的网络设备是否提供自动备份机制对重要信息进行本地和异地备份功能；是否提供重要网络设备、通信线路和服务器的硬件冗余；是否提供自动机制在灾难发生时实现自动业务切换和恢复的功能；

b) 可访谈系统管理员，询问信息系统中的操作系统是否提供自动备份机制对重要信息进行本地和异地备份功能；是否提供自动机制在灾难发生时实现自动业务切换和恢复的功能；

c) 可访谈数据库管理员，询问信息系统中的数据库管理系统是否提供自动备份机制对重要信息进行本地和异地备份功能；是否提供重要业务系统的本地和异地系统级热备份；是否提供自动机制在灾难发生时实现自动业务切换和恢复的功能；

d) 应检查设计/验收文档，查看其是否有关于重要业务系统的本地和异地系统级热备份的描述；是否有关于在灾难发生时业务自动切换和恢复的功能的描述；

e） 应检查操作系统、网络设备、数据库系统、业务系统，查看其是否配备重要业务系统的本地和异地系统级热备份，配置是否正确；

f） 应检查重要网络设备、通信线路和服务器是否提供硬件冗余；

g) 应检查重要业务系统是否配备了本地系统级热备份的功能；是否配备自动机制在灾难发生时实现自动业务切换和恢复功能；

h) 应测试重要业务系统，验证其本地系统级热备份功能是否有效，在灾难发生时自动业务切换和恢复功能是否有效。

8.1.5.3.5 结果判定

a) 如果没有设计/验收文档，则 8.1.5.3.4 d）为否定；

b) 8.1.5.3.4 d）-h）均为肯定，则信息系统符合本单元测评项要求。

8.2 安全管理测评

8.2.1 安全管理机构

8.2.1.1 岗位设置

8.2.1.1.1 测评项

a) 应设立信息安全管理工作的职能部门，设立安全主管人、安全管理各个方面的负责人，定义各负责人的职责；

b) 应设立系统管理人员、网络管理人员、安全管理人员岗位，定义各个工作岗位的职责；

c) 应成立指导和管理信息安全工作的委员会或领导小组，其最高领导应由单位主管领导委任或授权；

d) 应制定文件明确安全管理机构各个部门和岗位的职责、分工和技能要求。

8.2.1.1.2 测评方式

访谈，检查。

8.2.1.1.3 测评对象

安全主管，安全管理各个方面的负责人，领导小组日常管理工作的负责人，系统管理员，网络管理员，安全员，部门、岗位职责文件，委任授权书，工作记录。

8.2.1.1.4 测评实施

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，是否明确各部门职责分工；

c) 应访谈安全主管，询问是否设立安全管理各个方面的负责人，设置了哪些工作岗位（如安全主管、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、安全员等重要岗位），是否明确各个岗位的职责分工；

d) 应访谈安全主管、安全管理各个方面的负责人、信息安全管理委员会或领导小组日常管理工作的负责人、系统管理员、网络管理员和安全员，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是否具有单位主管领导对其最高领导的委任授权书；

g) 应检查信息安全管理委员会职责文件，查看是否明确描述委员会的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（如会议记录/纪要和信息安全工作决策文档等）。

8.2.1.1.5 结果判定

a) 如果8.2.1.1.4 d）被访谈人员表述与文件描述一致，则该项为肯定；

b) 8.2.1.1.4 a）-h）均为肯定，则信息系统符合本单元测评项要求。

8.2.1.2 人员配备

8.2.1.2.1 测评项

a) 应配备一定数量的系统管理人员、网络管理人员和安全管理人员等；
b) 应配备专职安全管理人员，不可兼任；
c) 关键区域或部位的安全管理人员应按照机要人员条件配备；
d) 关键岗位应定期轮岗；
e) 关键事务应配备多人共同管理。

8.2.1.2.2 测评方式

访谈，检查。

8.2.1.2.3 测评对象

安全主管，人员配备要求的相关文档，管理人员名单。

8.2.1.2.4 测评实施

a) 应访谈安全主管，询问各个安全管理岗位人员（按照岗位职责文件询问，包括机房管理员、系统管理员、数据库管理员、网络管理员和安全员等重要岗位人员）配备情况，包括数量、专职还是兼职等；
b) 应访谈安全主管，询问对哪些关键岗位实行定期轮岗（如中心机房的安全员和关键服务器的安全员等），定期轮岗情况如何，轮岗周期多长，轮岗手续如何；
c) 应访谈安全主管，询问其对关键区域或部位的安全员配备是否有一定条件要求（如中心机房的安全员、关键服务器的安全员、机密资料的管理员等），对关键事务的管理人员配备情况如何（如密钥管理等人员），是否配备2人或2人以上共同管理，相互监督和制约；
d) 应检查人员配备要求的相关文档，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、网络管理员和安全员等重要岗位人员并明确应配备专职的安全员；查看是否明确对哪些关键岗位（应有列表）实行定期轮岗并明确轮岗周期、轮岗手续等相关内容；查看是否明确对哪些关键区域或部位的安全员应按照机要人员的条件配备；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；
e) 应检查管理人员名单，查看其是否明确机房管理员、系统管理员、数据库管理员、网络管理员和安全员等重要岗位人员的信息，确认安全员是否是专职人员。

8.2.1.2.5 结果判定

a) 如果8.2.1.2.4 a）设置的安全员是专职的，则该项为肯定；
b) 8.2.1.2.4 a）-e）均为肯定，则信息系统符合本单元测评项要求。

8.2.1.3 授权和审批

8.2.1.3.1 测评项

a) 应授权审批部门及批准人，对关键活动进行审批；
b) 应列表说明须审批的事项、审批部门和可批准人；
c) 应建立各审批事项的审批程序，按照审批程序执行审批过程；
d) 应建立关键活动的双重审批制度；
e) 不再适用的权限应及时取消授权；
f) 应定期审查、更新需授权和审批的项目；
g) 应记录授权过程并保存授权文档。

8.2.1.3.2 测评方式

访谈，检查。

8.2.1.3.3 测评对象

安全主管，关键活动的批准人，授权管理文件，审批文档，审批记录，审查记录，消除授权记录。

8.2.1.3.4 测评实施

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) 应访谈关键活动的批准人，询问其对关键活动的审批范围包括哪些（如网络系统、应用系统、数据库管理系统、重要服务器和设备等重要资源的访问，重要管理制度的制定和发布，人员的配备、培训，产品的采购，第三方人员的访问、管理，与合作单位的合作项目等），审批程序如何；

c) 应检查授权管理文件，查看文件是否包含需审批事项列表，列表是否明确审批事项和双重审批事项、审批部门、批准人及审批程序等（如列表说明哪些事项应经过信息安全领导小组审批，哪些事项应经过安全管理机构审批，哪些关键活动应经过哪些部门双重审批等），文件是否说明应定期审查、更新需审批的项目和审查周期等；

d) 应检查经双重审批的文档，查看是否具有双重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；

f) 应检查审查记录，查看记录日期是否与审查周期一致；

g) 应检查是否具有对不再适用的权限及时取消授权的记录。

8.2.1.3.5 结果判定

a) 8.2.1.3.4 a）-g）均为肯定，则该测评项符合要求。

8.2.1.4 沟通和合作

8.2.1.4.1 测评项

a) 应加强各类管理人员和组织内部机构之间的合作与沟通，定期或不定期召开协调会议，共同协助处理信息安全问题；

b) 信息安全职能部门应定期或不定期召集相关部门和人员召开安全工作会议，协调安全工作的实施；

c) 信息安全领导小组或者安全管理委员会定期召开例会，对信息安全工作进行指导、决策；

d) 应加强与兄弟单位、公安机关、电信公司的合作与沟通，以便在发生安全事件时能够得到及时的支持；

e) 应加强与供应商、业界专家、专业的安全公司、安全组织的合作与沟通，获取信息安全的最新发展动态，当发生紧急事件的时候能够及时得到支持和帮助；

f) 应文件说明外联单位、合作内容和联系方式；

g) 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。

8.2.1.4.2 测评方式

访谈，检查。

8.2.1.4.3 测评对象

安全主管，安全管理人员，会议文件，会议记录，外联单位说明文档，安全顾问名单。

8.2.1.4.4 测评实施

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），与组织机构内其它部门之间及内

部各部门管理人员之间的沟通、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；

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部署安全工作的实施，参加会议的部门和人员有哪些，会议结果如何；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) 应访谈安全管理人员（从系统管理员和安全员等人员中抽查），询问其与外单位人员，与组织机构内其他部门人员，与内部各部门管理人员之间的沟通方式和主要沟通内容有哪些；

e) 应检查部门间协调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、会议结果等的描述；

g) 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；

h) 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、兄弟公司、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联系人、联系方式等内容；

i) 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，检查由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，查看是否具有由安全顾问签字的相关建议。

8.2.1.4.5 结果判定

a) 8.2.1.4.4 a）-i）均为肯定，则信息系统符合本单元测评项要求。

8.2.1.5 审核和检查

8.2.1.5.1 测评项

a) 应由安全管理人员定期进行安全检查，检查内容包括用户账号情况、系统漏洞情况、系统审计情况等；

b) 应由安全管理部门组织相关人员定期进行全面安全检查，检查内容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；

c) 应由安全管理部门组织相关人员定期分析、评审异常行为的审计记录，发现可疑行为，形成审计分析报告，并采取必要的应对措施；

d) 应制定安全检查表格实施安全检查，汇总安全检查数据，形成安全检查报告，并对安全检查结果进行通报；

e) 应制定安全审核和安全检查制度规范安全审核和安全检查工作，定期按照程序进行安全审核和安全检查活动。

8.2.1.5.2 测评方式

访谈，检查。

8.2.1.5.3 测评对象

安全主管，安全员，安全检查制度，安全检查报告，审计分析报告，安全检查过程记录，安全检查表格。

8.2.1.5.4 测评实施

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安全检查，检查周期多长，是否定期分析、评审异常行为的审计记录；

b) 应访谈安全员，询问安全检查包含哪些内容，检查人员有哪些，检查程序是否按照系统相关策略和要求进行，是否制定安全检查表格实施安全检查，检查结果如何，是否对检查结果进行通报，通报形式、范围如何；

c) 应检查安全检查制度文档，查看文档是否规定检查内容、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，内容是否包括用户账号情况、系统漏洞情况、系统审计情况等；

d) 应检查安全检查报告，查看报告日期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；

e) 应检查安全检查过程记录，查看记录的检查程序与文件要求是否一致；

f) 应检查审计分析报告，查看报告日期与检查周期是否一致，报告中是否有分析人员、异常问题和分析结果等的描述，是否对发现的问题提出相应的措施；

g) 应检查是否具有安全检查表格。

8.2.1.5.5 结果判定

a) 8.2.1.5.4 a）-g）均为肯定，则信息系统符合本单元测评项要求。

8.2.2 安全管理制度

8.2.2.1 管理制度

8.2.2.1.1 测评项

a) 应制定信息安全工作的总体方针、政策性文件和安全策略等，说明机构安全工作的总体目标、范围、方针、原则、责任等；

b) 应对安全管理活动中的各类管理内容建立安全管理制度，以规范安全管理活动，约束人员的行为方式；

c) 应对要求管理人员或操作人员执行的日常管理操作，建立操作规程，以规范操作行为，防止操作失误；

d) 应形成由安全政策、安全策略、管理制度、操作规程等构成的全面的信息安全管理制度体系；

e) 应由安全管理职能部门定期组织相关部门和相关人员对安全管理制度体系的合理性和适用性进行审定。

8.2.2.1.2 测评方式

访谈，检查。

8.2.2.1.3 测评对象

安全主管，总体方针、政策性文件和安全策略文件，安全管理制度清单，操作规程，评审记录。

8.2.2.1.4 测评实施

a) 应访谈安全主管，询问机构的制度体系是否由安全政策、安全策略、管理制度、操作规程等构成，是否定期对安全管理制度体系进行评审，评审周期多长；

b) 应检查信息安全工作的总体方针、政策性文件和安全策略文件，查看文件是否明确机构安全工作的总体目标、范围、方针、原则、责任等，是否明确信息系统的安全策略；

c) 应检查安全管理制度清单，查看是否覆盖物理、网络、主机系统、数据、应用和管理等层面；

d) 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；
e) 应检查是否具有安全管理制度体系的评审记录，查看记录日期与评审周期是否一致，是否记录了相关人员的评审意见。

8.2.2.1.5 结果判定

a) 8.2.2.1.4 a）-e）均为肯定，则信息系统符合本单元测评项要求。

8.2.2.2 制定和发布

8.2.2.2.1 测评项

a) 应在信息安全领导小组的负责下，组织相关人员制定；
b) 应保证安全管理制度具有统一的格式风格，并进行版本控制；
c) 应组织相关人员对制定的安全管理进行论证和审定；
d) 安全管理制度应经过管理层签发后按照一定的程序以文件形式发布；
e) 安全管理制度应注明发布范围，并对收发文进行登记；
f) 安全管理制度应注明密级，进行密级管理。

8.2.2.2.2 测评方式

访谈，检查。

8.2.2.2.3 测评对象

安全主管，管理人员，制度制定和发布要求管理文档，评审记录，安全管理制度，收发登记记录。

8.2.2.2.4 测评实施

a) 应访谈安全主管，询问安全管理制度是否在信息安全领导小组或委员会的总体负责下统一制定，参与制定人员有哪些；
b) 应访谈安全主管，询问安全管理制度的制定程序，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（如召开评审会、函审、内部审核等），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) 应检查安全管理制度文档，查看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，查看收发是否符合规定程序和发布范围要求。

8.2.2.2.5 结果判定

a) 8.2.2.2.4 a）-f）均为肯定，则信息系统符合本单元测评项要求。

8.2.2.3 评审和修订

8.2.2.3.1 测评项

a) 应定期对安全管理制度进行评审和修订，对存在不足或需要改进的安全管理制度进行修订；
b) 当发生重大安全事故、出现新的安全漏洞以及技术基础结构发生变更时，应对安全管理制度进行检查、审定和修订；
c) 每个制度文档应有相应负责人或负责部门，负责对明确需要修订的制度文档的维护；
d) 评审和修订的操作范围应考虑安全管理制度的相应密级。

8.2.2.3.2 测评方式

访谈，检查。

8.2.2.3.3 测评对象

安全主管，管理人员，安全管理制度列表，评审记录，安全管理制度对应负责人或负责部门的清单。

8.2.2.3.4 测评实施

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，由何部门/何人负责；
b) 应访谈管理人员（负责定期评审、修订和日常维护的人员），询问定期对安全管理制度的评审、修订情况和日常维护情况，评审周期多长，评审、修订程序如何，维护措施如何；
c) 应访谈管理人员（负责人员），询问系统发生重大安全事故、出现新的安全漏洞以技术基础结构和组织机构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) 应访谈管理人员（负责定期评审、修订的人员），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；
e) 应检查安全管理制度评审记录，查看记录日期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；
f) 应检查是否具有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等发生变更时对安全管理制度进行审定的记录；
g) 应检查是否具有需要定期修订的安全管理制度列表，查看列表是否注明评审周期；
h) 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。

8.2.2.3.5 结果判定

a) 8.2.2.3.4 a）-h）均为肯定，则信息系统符合本单元测评项要求。

8.2.3 人员安全管理

8.2.3.1 人员录用

8.2.3.1.1 测评项

a) 应保证被录用人具备基本的专业技术水平和安全管理知识；
b) 应对被录用人声明的身份、背景、专业资格和资质等进行审查；
c) 应对被录用人所具备的技术技能进行考核；
d) 应对被录用人说明其角色和职责；
e) 应签署保密协议；
f) 对从事关键岗位的人员应从内部人员选拔，并定期进行信用审查；
g) 对从事关键岗位的人员应签署岗位安全协议。

8.2.3.1.2 测评方式

访谈，检查。

8.2.3.1.3 测评对象

人事负责人，人事工作人员，人员录用要求管理文档，人员审查文档或记录，考核文档或记录，保密协议，岗位安全协议，审查记录。

8.2.3.1.4 测评实施

a) 应访谈人事负责人，询问在人员录用时对人员条件有哪些要求，目前录用的安全管理和技术人员是否有能力完成与其职责相对应的工作；
b) 应访谈人事工作人员，询问在人员录用时是否对被录用人的身份、背景、专业资格和资质进行审查，对技术人员的技术技能进行考核，录用后是否与其签署保密协议，是否对其说明工作职责；

c） 应访谈人事负责人，询问对从事关键岗位的人员是否从内部人员中选拔，是否要求其签署岗位安全安全协议，是否定期对关键岗位人员进行信用审查，审查周期多长；
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） 应检查技能考核文档或记录，查看是否记录考核内容和考核结果等；
g） 应检查保密协议，查看是否有保密范围、保密责任、违约责任、协议的有效期限和责任人签字等内容；
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的签字等内容；
i） 应检查信用审查记录，查看是否记录了审查内容和审查结果等，查看审查时间与审查周期是否一致。

8.2.3.1.5 结果判定

a） 8.2.3.1.4 a）-i）均为肯定，则信息系统符合本单元测评项要求。

8.2.3.2 人员离岗

8.2.3.2.1 测评项

a） 应立即终止由于各种原因即将离岗的员工的所有访问权限；
b） 应取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备；
c） 应经机构人事部门办理严格的调离手续，并承诺调离后的保密义务后方可离开；
d） 关键岗位的人员调离应按照机要人员的有关管理办法进行。

8.2.3.2.2 测评方式

访谈，检查。

8.2.3.2.3 测评对象

安全主管，人事工作人员，人员离岗要求文档，保密承诺文档，机要人员管理办法，执行记录。

8.2.3.2.4 测评实施

a） 应访谈安全主管，询问是否及时终止离岗人员所有访问权限，取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备等；
b） 应访谈人事工作人员，询问调离手续包括哪些，对关键岗位的人员调离是否按照机要人员的有关管理办法执行，是否要求调离人员在脱密期满并承诺相关保密义务后方可离开；
c） 应检查人员离岗要求文档，查看是否规定了调离手续和离岗要求等；
d） 应检查是否具有交还身份证件和设备等的记录；
e） 应检查保密承诺文档，查看是否有调离人员的签字；
f） 应检查机要人员的有关管理办法，查看是否说明机要人员条件、机要人员调离手续等相关内容；
g） 应检查关键岗位人员调离的执行记录，查看记录与管理办法要求是否一致。

8.2.3.2.5 结果判定

a） 8.2.3.2.4 a）-g）均为肯定，则信息系统符合本单元测评项要求。

8.2.3.3 人员考核

8.2.3.3.1 测评项

a） 应对所有人员实施全面、严格的安全审查；
b） 应定期对各个岗位的人员进行安全技能及安全认知的考核；

c） 应对考核结果进行记录并保存；

d） 应对违背安全策略和规定的人员进行惩戒。

8.2.3.3.2 测评方式

访谈，检查。

8.2.3.3.3 测评对象

安全主管，人事工作人员，人员考核记录。

8.2.3.3.4 测评实施

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） 应访谈人事工作人员，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（如操作行为、社会关系、社交活动等），是否全面；

c） 应访谈人事工作人员，询问对违背安全策略和规定的人员有哪些惩戒措施；

d） 应检查考核记录，查看记录的考核人员是否包括各个岗位的人员，考核内容是否包含安全知识、安全技能等；查看记录日期与考核周期是否一致。

8.2.3.3.5 结果判定

a） 如果8.2.3.3.4 b）被访谈人员表述审查内容包含社会关系、社交活动、操作行为等各个方面，则该项为肯定；

b） 如果8.2.3.3.4 c）被访谈人员表述与文件描述一致，则该项为肯定；

c） 8.2.3.3.4 a）-d）均为肯定，则信息系统符合本单元测评项要求。

8.2.3.4 安全意识教育和培训

8.2.3.4.1 测评项

a） 应对各类人员进行安全意识教育；

b） 应告知人员相关的安全责任和惩戒措施；

c） 应制定安全教育和培训计划，对信息安全基础知识、岗位操作规程等进行培训；

d） 应针对不同岗位制定不同培训计划；

e） 应对安全教育和培训的情况和结果进行记录并归档保存。

8.2.3.4.2 测评方式

访谈，检查。

8.2.3.4.3 测评对象

安全主管，安全员，系统管理员，网络管理员，数据库管理员，培训计划，培训记录。

8.2.3.4.4 测评实施

a） 应访谈安全主管，询问是否制定安全教育和培训计划并按计划对各个岗位人员进行安全教育和培训，以什么形式进行，效果如何；

b） 应访谈安全员、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目的、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；查看记录与培训计划是否一致。

8.2.3.4.5 结果判定

a） 如果8.2.3.4.4 b）访谈人员能够表述清楚询问内容，且安全职责、惩戒措施和岗位操作规程表述与文件描述一致，则该项为肯定；

b） 8.2.3.4.4 a）-d）均为肯定，则信息系统符合本单元测评项要求。

8.2.3.5 第三方人员访问管理

8.2.3.5.1 测评项

a） 第三方人员应在访问前与机构签署安全责任合同书或保密协议；

b） 对重要区域的访问，须提出书面申请，批准后由专人全程陪同或监督，并记录备案；

c） 对第三方人员允许访问的区域、系统、设备、信息等内容应进行书面的规定，并按照规定执行；

d） 对关键区域不允许第三方人员访问。

8.2.3.5.2 测评方式

访谈，检查。

8.2.3.5.3 测评对象

安全主管，安全管理人员，安全责任合同书或保密协议，第三方人员访问管理文档，访问批准文档，登记记录。

8.2.3.5.4 测评实施

a） 应访谈安全主管，询问对第三方人员（如向系统提供服务的系统软、硬件维护人员，业务合作伙伴、评估人员等）的访问采取哪些管理措施，是否要求第三方人员访问前与机构签署安全责任合同书或保密协议；

b） 应访谈安全管理人员，询问对第三方人员访问重要区域（如访问主机房、重要服务器或设备、保密文档等）采取哪些措施，是否经有关负责人书面批准，是否由专人全程陪同或监督，是否进行记录并备案管理；

c） 应检查安全责任合同书或保密协议，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；

d） 应检查第三方人员访问管理文档，查看是否明确第三方人员包括哪些人员，允许第三方人员访问的范围（区域、系统、设备、信息等内容），第三方人员进入条件（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第三方人员访问），第三方人员进入的访问控制（由专人全程陪同或监督等）和第三方人员的离开条件等；

e） 应检查第三方人员访问重要区域批准文档，查看是否有第三方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；

f） 应检查第三方人员访问重要区域的登记记录，查看记录是否描述了第三方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。

8.2.3.5.5 结果判定

a） 8.2.3.5.4 a）-f）均为肯定，则该测评项符合要求。

8.2.4 系统建设管理

8.2.4.1 系统定级

8.2.4.1.1 测评项

a） 应明确信息系统划分的方法；

b） 应确定信息系统的安全保护等级；

c） 应以书面的形式定义确定了安全保护等级的信息系统的属性，包括使命、业务、网络、硬件、软件、数据、边界、人员等；

d） 应以书面的形式说明确定信息系统为某个安全保护等级的方法和理由；

e） 应组织相关部门和有关安全技术专家对信息系统定级结果的合理性和正确性进行论证和审定；

f） 应确保信息系统的定级结果经过相关部门的批准。

8.2.4.1.2 测评方式

访谈，检查。

8.2.4.1.3 测评对象

安全主管，系统划分文档，系统定级文档，专家论证文档，系统属性说明文档。

8.2.4.1.4 测评实施

a) 应访谈安全主管，询问划分信息系统的方法和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，是否对其进行明确描述；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，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（如上级主管部门）的批准；

b) 应检查系统划分文档，查看文档是否明确描述信息系统划分的方法和理由；

c) 应检查系统定级文档，查看文档是否给出信息系统的安全保护等级，是否明确描述确定信息系统为某个安全保护等级的方法和理由，是否给出安全等级保护措施组成SxCyGz值；查看定级结果是否有相关部门的批准盖章；

d) 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；

e) 应检查系统属性说明文档，查看文档是否明确了系统使命、业务、网络、硬件、软件、数据、边界、人员等。

8.2.4.1.5 结果判定

a) 8.2.4.1.4 a）没有上级主管部门的，如果有安全主管的批准，则该项为肯定；

b) 8.2.4.1.4 b）-e）均为肯定，则信息系统符合本单元测评项要求。

8.2.4.2 安全方案设计

8.2.4.2.1 测评项

a) 应根据系统的安全级别选择基本安全措施，依据风险评估的结果补充和调整安全措施；

b) 应指定和授权专门的部门对信息系统的安全建设进行总体规划，制定近期和远期的安全建设工作计划；

c) 应根据信息系统的等级划分情况，统一考虑安全保障体系的总体安全策略、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，并形成配套文件；

d) 应组织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合理性和正确性进行论证和审定；

e) 应确保总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等文件必须经过批准，才能正式实施；

f) 应根据安全测评、安全评估的结果定期调整和修订总体安全策略、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。

8.2.4.2.2 测评方式

访谈，检查。

8.2.4.2.3 测评对象

安全主管，系统建设负责人，总体安全策略文档，安全技术框架，安全管理策略文档，总体建设规划书，详细设计方案，专家论证文档，维护记录。

8.2.4.2.4 测评实施

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，有何部门/何人负责；

b) 应访谈系统建设负责人，询问是否制定近期和远期的安全建设工作计划，是否根据系统的安全级别选择基本安全措施，是否依据风险评估的结果补充和调整安全措施，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，统一考虑安全保障体系的总体安全策略、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；

d) 应访谈系统建设负责人，询问是否组织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、安全管理策略等相关配套文件进行论证和审定，并经过管理部门的批准；

e) 应访谈系统建设负责人，询问是否根据安全测评、安全评估的结果定期调整和修订总体安全策略、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，维护周期多长；

f) 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；

g) 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；

h) 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；

i) 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，查看记录日期与维护周期是否一致。

8.2.4.2.5 结果判定

a) 8.2.4.3.4 a）-i）均为肯定，则信息系统符合本单元测评项要求。

8.2.4.3 产品采购

8.2.4.3.1 测评项

a) 应确保安全产品的使用符合国家的有关规定；

b) 应确保密码产品的使用符合国家密码主管部门的要求；

c) 应指定或授权专门的部门负责产品的采购；

d) 应制定产品采购方面的管理制度明确说明采购过程的控制方法和人员行为准则；

e) 应预先对产品进行选型测试，确定产品的候选范围，并定期审定和更新候选产品名单；

f) 应对重要部位的产品委托专业测评单位进行专项测试，根据测试结果选用产品。

8.2.4.3.2 测评方式

访谈，检查。

8.2.4.3.3 测评对象

安全主管，系统建设负责人，产品采购管理制度，产品选型测试结果记录，更新候选产品名单。

8.2.4.3.4 测评实施

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，询问系统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制度，查看内容是否明确采购过程的控制方法（如采购前对产品做选型测试，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，通过招投标方式确定采购产品等）和人员行为准则；

e） 应检查系统使用的有关信息安全产品（边界安全设备、重要服务器操作系统、数据库等）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（如《商用密码管理条例》规定任何单位只能使用经过国家密码管理机构认可的商用密码产品，商用密码产品发生故障，必须有国家密码管理机构指定的单位维修，报废商用密码产品应向国家密码管理机构备案等；《计算机信息系统保密工作暂行规定》规定涉密系统配置合格的保密专用设备，所采取的保密措施应与所处理信息的密级要求相一致等；

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。

8.2.4.3.5 结果判定

a） 如果8.2.4.4.4 c）访谈说明没有采用密码产品，则测评实施c）、f）为不适用；

b） 8.2.4.4.4 a）-g）均为肯定，则信息系统符合本单元测评项要求。

8.2.4.4 自行软件开发

8.2.4.4.1 测评项

a） 应确保开发环境与实际运行环境物理分开；

b） 应确保系统开发文档由专人负责保管，系统开发文档的使用受到控制；

c） 应制定开发方面的管理制度明确说明开发过程的控制方法和人员行为准则；

d） 应确保开发人员和测试人员的分离，测试数据和测试结果受到控制；

e） 应确保提供软件设计的相关文档和使用指南；

f） 应确保对程序资源库的修改、更新、发布进行授权和批准；

g） 应确保开发人员为专职人员，开发人员的开发活动受到控制、监视和审查。

8.2.4.4.2 测评方式

访谈，检查。

8.2.4.4.3 测评对象

系统建设负责人，软件设计相关文档和使用指南，软件开发管理制度，审批文档或记录，文档使用控制记录，审查记录。

8.2.4.4.4 测评实施

a） 应访谈系统建设负责人，询问系统是否自主开发软件，是否对程序资源库的修改、更新、发布进行授权和批准，软件开发是否有相应的控制措施，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，软件开发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，系统开发文档是否由专人负责保管，负责人是何人，如何控制使用（如限制使用人员范围并做使用登记等），测试数据和测试结果是否受到控制；

c） 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）和软件使用指南或操作手册和维护手册等；

d） 应检查软件开发环境与系统运行环境在物理上是否是分开的；

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

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

g） 应检查是否具有系统软件开发相关文档（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。

h） 应检查对开发人员的审查记录，查看是否记录审查结果等。

8.2.4.4.5 结果判定

a） 8.2.4.5.4 a）-h）均为肯定，则信息系统符合本单元测评项要求。

8.2.4.5 外包软件开发

8.2.4.5.1 测评项

a) 应与软件开发单位签订协议，明确知识产权的归属和安全方面的要求；

b) 应根据协议的要求检测软件质量；

c) 应在软件安装之前检测软件包中可能存在的恶意代码；

d) 应要求开发单位提供技术培训和服务承诺；

e) 应要求开发单位提供软件设计的相关文档和使用指南；

f) 应要求开发单位提供软件源代码，并审查软件中可能存在的后门。

8.2.4.5.2 测试方法

访谈，检查。

8.2.4.5.3 测试对象

系统建设负责人，软件开发安全协议，软件开发文档，软件培训文档，软件源代码文档。

8.2.4.5.4 测评实施

a） 应访谈系统建设负责人，询问在外包软件前是否对软件开发单位以书面文档形式（如软件开发安全协议）规范软件开发单位的责任、开发过程中的安全行为、开发环境要求、软件质量以及开发后的服务承诺等相关内容；

b） 应访谈系统建设负责人，询问是否具有能够独立的对软件进行日常维护和使用所需的文档，开发单位是否为软件的正常运行和维护提供过技术支持，以何种方式进行；

c） 应访谈系统建设负责人，询问软件交付前是否依据开发协议的技术指标对软件功能和性能等进行验收检测，验收检测是否是由开发商和委托方共同完成，软件安装之前是否检测软件中的恶意代码和可能的后门，检测工具是否是第三方的商业产品；

d） 应检查软件开发协议是否规定知识产权归属、安全行为等内容；查看是否具有需求分析说明书、软件设计说明书、软件操作手册、软件源代码文档等开发文档和用户培训计划、程序员培训手册等后期技术支持文档。

8.2.4.5.5 结果判定

a） 8.2.4.6.4 a）—d）均为肯定，则信息系统符合本单元测评项要求。

8.2.4.6 工程实施

8.2.4.6.1 测评项

a） 应与工程实施单位签订与安全相关的协议，约束工程实施单位的行为；

b） 应指定或授权专门的人员或部门负责工程实施过程的管理；

c） 应制定详细的工程实施方案控制实施过程，并要求工程实施单位能正式地执行安全工程过程；

d） 应制定工程实施方面的管理制度明确说明实施过程的控制方法和人员行为准则；

e） 应通过工程监理控制项目的实施过程。

8.2.4.6.2 测试方法

访谈，检查。

8.2.4.6.3 测试对象

系统建设负责人，工程安全建设协议，工程实施方案，工程实施管理制度，工程监理报告。

8.2.4.6.4 测评实施

a) 应访谈系统建设负责人，询问是否以书面形式（如工程安全建设协议）约束工程实施方的工程实施行为；

b) 应访谈系统建设负责人，询问是否指定专门人员或部门负责工程实施管理，是否由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，是否将控制方法和工程人员行为规范制度化，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；

c) 应检查工程安全建设协议，查看其内容是否规定工程实施方的责任、任务要求、质量要求等方面内容，约束工程实施行为；

d) 应检查工程实施管理制度，查看其是否规定实施过程的控制方法（如内部阶段性控制或外部监理单位控制）、实施参与人员的各种行为等方面内容，是否做过改进；

e) 应检查工程监理实施过程是否形成各种文档，如阶段性工程监理报告。

8.2.4.6.5 结果判定

a) 如果 8.2.4.7.4 d）因没有出现过重大问题而没有做过制度内容的改进，则该项为不适用；

b) 8.2.4.7.4 a）一e）均为肯定，则信息系统符合本单元测评项要求。

8.2.4.7 测试验收

8.2.4.7.1 测评项

a) 应对系统进行安全性测试验收；

b) 应在测试验收前根据设计方案或合同要求等制订测试验收方案，测试验收过程中详细记录测试验收结果，形成测试验收报告；

c) 应委托公正的第三方测试单位对系统进行测试，并出具测试报告；

d) 应制定系统测试验收方面的管理制度明确说明系统测试验收的控制方法和人员行为准则；

e) 应指定或授权专门的部门负责系统测试验收的管理，并按照管理制度的要求完成系统测试验收工作；

f) 应组织相关部门和相关人员对系统测试验收报告进行审定，没有疑问后由双方签字。

8.2.4.7.2 测试方法

访谈，检查。

8.2.4.7.3 测试对象

系统建设负责人，测试方案，测试记录，测试报告，验收报告，验收测试管理制度。

8.2.4.7.4 测评实施

a) 应访谈系统建设负责人，询问在信息系统正式运行前，是否委托第三方测试机构根据设计方案或合同要求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，询问是否指定专门部门负责测试验收工作，由何部门负责，是否对测试过程（包括测试前、测试中和测试后）进行文档化和制度化要求；

c) 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测试报告进行符合性审定；

d） 应检查工程测试方案，查看其是否对参与测试部门、人员、现场操作过程等进行要求；查看测试记录是否详细记录了测试时间、人员、操作过程、测试结果等方面内容；查看测试报告是否提出存在问题及改进意见等；

e） 应检查是否具有系统验收报告；

f） 应检查验收测试管理制度是否对系统验收测试的过程控制、参与人员的行为等进行规定，是否根据实际工作中出现的问题而做过相应改进。

8.2.4.7.5 结果判定

a) 如果 8.2.4.8.4 f）因没有出现过重大问题而没有做过制度内容的改进，则该项为不适用；

b) 8.2.4.8.4 a）—f）均为肯定，则信息系统符合本单元测评项要求。

8.2.4.8 系统交付

8.2.4.8.1 测评项

a) 应明确系统的交接手续，并按照交接手续完成交接工作；

b) 应由系统建设方完成对委托建设方的运维技术人员的培训；

c) 应由系统建设方提交系统建设过程中的文档和指导用户进行系统运行维护的文档；

d) 应由系统建设方进行服务承诺，并提交服务承诺书，确保对系统运行维护的支持；

e) 应制定系统交付方面的管理制度明确说明系统交付的控制方法和人员行为准则；

f) 应指定或授权专门的部门负责系统交付的管理工作，并按照管理制度的要求完成系统交付工作。

8.2.4.8.2 测试方法

访谈，检查。

8.2.4.8.3 测试对象

系统建设负责人，系统交付清单，服务承诺书，系统培训记录，系统交付管理制度。

8.2.4.8.4 测评实施

a) 应访谈系统建设负责人，询问交接手续是什么，系统交接工作是否由专门部门按照该手续办理，是否根据交付清单对所交接的设备、文档、软件等进行清点，交付清单是否满足合同的有关要求；是否对交付工作的控制方法和人员行为准则进行制度化要求，交接工作是否由于出现管理上的问题而进行交接手续或制度要求的改进；

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，系统建设实施方是否对运维技术人员进行过培训，针对哪些方面进行过培训，是否以书面形式承诺对系统运行维护提供一定的技术支持服务，是否按照服务承诺书的要求进行过技术支持，以何形式进行，系统是否具有支持其独立运行维护所需的文档；

c） 应检查系统交付清单，查看其是否具有系统建设文档（如系统建设方案）、指导用户进行系统运维的文档（如服务器操作规程书）以及系统培训手册等文档名称；

d) 应检查是否具有系统建设方的服务承诺书和对系统进行的培训记录；

e) 应检查系统交付管理制度是否规定了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，是否做过改进。

8.2.4.8.5 结果判定

a) 如果 8.2.4.9.4 a）、d）中因没有出现交接工作中的问题而没有对相关文档做过改进，则以上两项不适用；

b) 8.2.4.9.4 a）—d）均为肯定，则信息系统符合本单元测评项要求。

8.2.4.9 系统备案

8.2.4.9.1 测评项

a) 应将系统定级、系统属性等材料指定专门的人员或部门负责管理，并控制这些材料的使用；

b) 应将系统等级和系统属性等资料报系统主管部门备案；

c) 应将系统等级、系统属性、等级划分理由及其他要求的备案材料报相应公安机关备案。

8.2.4.9.2 测评方式

访谈，检查。

8.2.4.9.3 测评对象

安全主管，文档管理员，备案记录。

8.2.4.9.4 测评实施

a) 应访谈安全主管，询问是否有专门的人员或部门负责管理系统定级、系统属性等文档，由何部门/何人负责；

b) 应访谈文档管理员，询问对系统定级、系统属性等文档备案采取哪些控制措施（如限制使用范围、使用登记记录等）；

c) 应检查是否具有将系统定级文档和系统属性说明文件等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、系统属性和等级划分理由等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文档和系统属性说明文件等相关材料的使用控制记录。

8.2.4.9.5 结果判定

8.2.4.2.4 c）-e）为肯定，则信息系统符合本单元测评项要求。

8.2.4.10 安全服务商选择

8.2.4.10.1 测评项

a) 应确保安全服务商的选择符合国家的有关规定。

8.2.4.10.2 测试方法

访谈。

8.2.4.10.3 测试对象

系统建设负责人。

8.2.4.10.4 测评实施

a) 应访谈系统建设负责人，询问对信息系统进行安全规划、设计、实施、维护、测评等服务的安全服务单位是否符合国家有关规定。

8.2.4.10.5 结果判定

a) 8. 2. 4. 10. 4 a）为肯定，则信息系统符合本单元测评项要求。

8.2.5 系统运维管理

8.2.5.1 环境管理

8.2.5.1.1 测评项

a) 应对机房供配电、空调、温湿度控制等设施指定专人或专门的部门定期进行维护管理；

b) 应配备机房安全管理人员，对机房的出入、服务器的开机或关机等工作进行管理；

c) 应建立机房安全管理制度，对有关机房物理访问，物品带进、带出机房和机房环境安全等方面作出规定；

d) 加强对办公环境的保密性管理，包括如工作人员调离办公室应立即交还该办公室钥匙和不在办公区接待来访人员等；

e) 应对办公环境的人员行为，如工作人员离开座位应确保终端计算机退出登录状态和桌面上没有包含敏感信息的纸档文件等作出规定；

f) 应有指定的部门负责机房安全，并配置电子门禁系统和专职警卫，对机房来访人员实行登记记录、电子记录和监控录像三重备案管理；

g) 应对机房和办公环境实行统一策略的安全管理，出入人员应经过相应级别授权，对进入重要安全区域的活动行为应实时监视和记录。

8.2.5.1.2 测评方式

访谈，检查。

8.2.5.1.3 测评对象

物理安全负责人，机房值守人员，工作人员，机房安全管理制度，办公环境管理文档，设备维护记录，机房进出登记表，机房电子门禁系统及其电子记录，摄像监控系统。

8.2.5.1.4 测评实施

a) 应访谈物理安全负责人，询问是否指定专人或部门对机房基本设施（如空调、供配电设备等）进行定期维护，由何部门/何人负责，维护周期多长；

b) 应访谈物理安全负责人，询问是否指定人员负责机房安全管理工作，对机房进出管理是否要求制度化和文档化；

c) 应访谈机房值守人员，询问对外来人员进出机房是否采用人工记录、电子记录和监控录像三重控制管理；

d) 应访谈物理安全负责人，询问办公环境是否和机房实行统一安全管理，出入是否要经过相应级别的授权控制；

e) 应访谈工作人员，询问对办公环境的保密性要求事项，其出入授权级别如何；

f) 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；

g) 应检查办公环境管理文档，查看其是否对工作人员离开座位后的保密行为（如清理桌面文件和屏幕锁定等）和人员调离办公室后的行为等方面作出规定；

h) 应检查机房进出登记表，查看是否记录外来人员进出时间、人员姓名、访问原因等内容；查看是否具有电子门禁系统和专职警卫值守，电子记录文档是否有时间和人员等信息；

i) 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、故障原因和维护结果等方面内容。

8.2.5.1.5 结果判定

a) 如果8.2.5.1.4 c）中访谈人员能够表述出针对办公环境保密性注意事项（如离开座位后应退出登录，并收好敏感性文件等），且其出入级别为相应级（如普通员工级）则该项为肯定；

b) 8.2.5.1.4 a）-i）均为肯定，则信息系统符合本单元测评项要求。

8.2.5.2 资产管理

8.2.5.2.1 测评项

a) 应建立资产安全管理制度，规定信息系统资产管理的责任人员或责任部门，并规范资产管理和使用的行为；

b) 应编制并保存与信息系统相关的资产所属关系、安全级别和所处位置等信息的资产清单；

c） 应根据资产的重要程度对资产进行定性赋值和标识管理，根据资产的价值选择相应的管理措施；

d） 应规定信息分类与标识的原则和方法，并对信息的使用、存储和传输作出规定；

e） 应根据信息分类与标识的原则和方法，在信息的存储、传输等过程中对信息进行标识。

8.2.5.2.2 测评方式

访谈，检查。

8.2.5.2.3 测评对象

安全主管，物理安全负责人，资产管理员，资产清单，信息分类标识文档，资产安全管理制度，设备。

8.2.5.2.4 测评实施

a） 应访谈安全主管，询问是否指定资产管理的责任人员或部门,由何部门/何人负责；

b） 应访谈物理安全负责人，询问是否对资产管理要求文档化和制度化；

c） 应访谈资产管理员，询问是否根据资产清单定期对资产进行一致性清查，并对资产清单进行维护更新；是否对资产进行赋值和标识管理，不同类别的资产是否采取不同的管理措施；

d） 应访谈资产管理员，询问对信息的操作（包括信息使用、存储和传输等方面）是否要求进行标识；

e） 应检查资产清单，查看其内容是否覆盖资产责任人、所属级别、所处位置和所属部门等方面，清单内容是否因资产所属发生变化或资产增减而进行过改变；

f） 应检查资产安全管理制度，查看其内容是否覆盖了资产使用、借用、维护等方面；

g） 应检查信息分类文档，查看其是否规定了分类标识的原则和方法（如根据数据的重要程度、敏感程度或用途不同进行分类），是否根据分类文档所描述的信息种类规定不同信息的使用、传输、存储等方面内容；

h） 应检查资产清单中的设备，查看其是否具有相应标识。

8.2.5.2.5 结果判定

a） 如果8.2.5.2.4 c）中访谈人员能够描述出不同的资产管理措施，则该项为肯定；

b） 如果8.2.5.2.4 e）中因没有发生过资产变化而使资产清单没有改变，则该项为不适用；

c） 如果测评实施8.2.5.2.4 h）中设备标识与信息分类标识文档中所要求的一致，则该项为肯定；

d） 8.2.5.2.4 a）-h）均为肯定，则信息系统符合本单元测评项要求。

8.2.5.3 介质管理

8.2.5.3.1 测评项

a） 应建立介质安全管理制度，对介质的存放环境、使用、维护和销毁等方面作出规定；

b） 应有介质的归档和查询记录，并对存档介质的目录清单定期盘点；

c） 对于需要送出维修或销毁的介质，应采用多次读写覆盖，清除介质中的敏感或秘密数据，防止信息的非法泄漏，对无法执行删除操作的受损介质必须销毁；

d） 应根据数据备份的需要对某些介质实行异地存储，存储地的环境要求和管理方法应与本地相同；

e） 应根据所承载数据和软件的重要程度对介质进行分类和标识管理，并实行存储环境专人管理；

f） 应对介质的物理传输过程中人员选择、打包、交付等情况进行控制；

g） 应对存储介质的使用过程、送出维修以及销毁建立严格的管理制度，保密性较高的信息存储介质未经批准不得自行销毁，销毁时必须做到双人监销，销毁记录应妥善保存；

h） 重要数据存储在本地或带出工作环境必须采取加密方式存储，并进行监控管理；

i） 应对存放在介质库中的介质定期进行完整性和可用性检查，确认其数据或软件没有受到损坏或丢失。

8.2.5.3.2 测评方式

访谈，检查。

8.2.5.3.3 测评对象

资产管理员，介质管理记录，介质安全管理制度，各类介质，介质存放地，异地存放地。

8.2.5.3.4 测评实施

a） 应访谈资产管理员，询问介质的存放环境是否具有保护措施，防止其被盗、被毁、被未授权修改以及信息的非法泄漏，是否有专人管理；

b） 应访谈资产管理员，询问是否对介质的使用管理进行制度化和文档化，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和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（如送出维修或销毁）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，对介质的销毁和维修是否执行严格的控制（如双人在场，销毁过程进行记录，介质送出前要经过多次读写覆盖等）；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（如采用防拆包装置）、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、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；是否具有介质销毁过程记录；

g） 应检查介质，查看是否对其进行了分类，并具有不同标识；

h） 应检查介质本地存放地的实际环境条件是否是安全的，异地存放地的环境要求和管理要求是否与本地相同，是否有专人对存放地进行管理。

8.2.5.3.5 结果判定

a） 8.2.5.3.4 a）-h）均为肯定，则信息系统符合本单元测评项要求。

8.2.5.4 设备管理

8.2.5.4.1 测评项

a） 应对信息系统相关的各种设施、设备、线路等指定专人或专门的部门定期进行维护管理；

b） 应对信息系统的各种软硬件设备的选型、采购、发放或领用等过程建立基于申报、审批和专人负责的管理制度；

c） 应对终端计算机、工作站、便携机、系统和网络等设备的操作和使用进行规范化管理；

d） 应对带离机房或办公地点的信息处理设备进行控制；

e） 应按操作规程实现服务器的启动/停止、加电/断电等操作，加强对服务器操作的日志文件管理和监控管理，并对其定期进行检查；

f） 应建立配套设施、软硬件维护方面的管理制度，对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等；

g） 应在安全管理机构统一安全策略下对服务器的进行系统配置和服务设定，并实施配置管理。

8.2.5.4.2 测评方式

访谈，检查。

8.2.5.4.3 测评对象

资产管理员，系统管理员，审计员，设备操作规程，设备审批管理制度，设备使用管理文档，设备维护记录，软硬件维护制度，服务器操作日志，配置文档。

8.2.5.4.4 测评实施

a） 应访谈资产管理员，询问是否对各类设施、设备指定专人或专门部门进行定期维护，由何部门/何人维护，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、发放等）进行审批控制，是否对设备带离机构进行审批控制，设备的操作和使用是否要求规范化管理；

c） 应访谈系统管理员，询问其对服务器是否在统一安全策略下进行正确配置，对服务器的操作是否按操作规程进行；

d） 应访谈审计员，询问对服务器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；

e） 应检查设备审批、发放制度，查看其内容是否覆盖对设备选型、采购、发放以及带离机构等环节的申报和审批规定；查看是否具有对设备的选型、采购、发放等过程的申报材料和审批报告；

f） 应检查设备使用管理文档，查看其是否对终端计算机、便携机、网络设备等使用、操作原则、注意事项等方面作出规定；

g） 应检查服务器操作规程，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） 应检查软硬件维护制度，查看其是否覆盖维护人员的责任、涉外维修和服务的审批、维修过程的监督控制等方面。

8.2.5.4.5 结果判定

a） 8.2.5.4.4 a）-h）均为肯定，则信息系统符合本单元测评项要求。

8.2.5.5 监控管理

8.2.5.5.1 测评项

a） 应进行主机运行监视，包括监视主机的CPU、硬盘、内存和网络等资源的使用情况；

b） 应对分散或集中的安全管理系统的访问授权、操作记录、日志等方面进行有效管理；

c） 应严格管理运行过程文档，其中包括责任书、授权书、许可证、各类策略文档、事故报告处理文档、安全配置文档、系统各类日志等，并确保文档的完整性和一致性；

d） 应定期或不定期对保密制度执行情况进行监督检查；

e） 应建立安全管理中心，对恶意代码、补丁和审计等进行集中管理。

8.2.5.5.2 测评方式

访谈，检查。

8.2.5.5.3 测评对象

系统运维负责人，监控记录文档，安全管理中心。

8.2.5.5.4 测评实施

a) 应访谈系统运维负责人，询问其是否监视主要服务器的各项资源指标，如CPU、内存、进程和磁盘等使用情况；

b) 应访谈系统运维负责人，询问目前信息系统是否由机构自身负责运行维护，如果是，系统运行所产生的文档如何进行管理（责任书、授权书、许可证、各类策略文档、事故报告处理文档、安全配置文档、系统各类日志等）；

c) 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；

d) 应访谈系统运维负责人，询问是否根据要求对运行安全保密问题开展过检查；

e) 应检查是否具有安全管理中心，对恶意代码、补丁和审计等进行集中管理。

8.2.5.5.5 结果判定

a) 8.2.5.5.4 a）-e）均为肯定，则信息系统符合本单元测评项要求。

8.2.5.6 网络安全管理

8.2.5.6.1 测评项

a) 应指定专人对网络进行管理，负责运行日志、网络监控记录的日常维护和报警信息分析和处理工作；

b) 应根据厂家提供的软件升级版本对网络设备进行更新，并在更新前对现有的重要文件进行备份；

c) 应进行网络系统漏洞扫描，对发现的网络系统安全漏洞进行及时的修补；

d) 应保证所有与外部系统的连接均应得到授权和批准；

e) 应建立网络安全管理制度，对网络安全配置、网络用户以及日志等方面作出规定；

f) 应对网络设备的安全策略、授权访问、最小服务、升级与打补丁、维护记录、日志及配置文件的生成、备份、变更审批、符合性检查等方面做出具体规定；

g) 应规定网络审计日志的保存时间以便为可能的安全事件调查提供支持；

h) 应明确各类用户的责任、义务和风险，并按照机构制定的审查和批准程序建立用户和分配权限，定期检查用户实际权限与分配权限的符合性；

i) 应对日志的备份、授权访问、处理、保留时间等方面做出具体规定，使用统一的网络时间，以确保日志记录的准确；

j) 应通过身份鉴别、访问控制等严格的规定限制远程管理账户的操作权限和登录行为；

k) 应定期检查违反规定拨号上网或其他违反网络安全策略的行为；

l) 应严格控制网络管理用户的授权，授权程序中要求必须有两人在场，并经双重认可后方可操作，操作过程应当有不可更改的审计日志。

8.2.5.6.2 测试方法

访谈，检查。

8.2.5.6.3 测试对象

安全主管，安全员，网络管理员，审计员，网络漏洞扫描报告，网络安全管理制度，系统外联授权书，网络审计日志。

8.2.5.6.4 测评实施

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；

b) 应访谈安全员，询问是否对网络安全的管理工作（包括网络安全配置、网络用户、日志等方面）制度化；

c) 应访谈安全员，询问网络的外联种类有哪些（互联网、合作伙伴企业网、上级部门网络等），是否都得到授权与批准，由何部门/何人批准；是否定期检查违规联网的行为；

d) 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（帐户数据和配置数据等）进行备份，采取什么方式进行；是否对网络设备进行过漏洞扫描，对扫描出的漏洞是否及时修补；

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，查看其内容是否覆盖网络存在的漏洞、严重级别、原因分析、改进意见等方面；

g) 应检查网络安全管理制度，查看其内容是否覆盖网络安全配置（包括网络设备的安全策略、授权访问、最小服务、升级与打补丁）、网络帐户（用户责任、义务、风险、权限审批、权限分配、帐户注销等）、审计日志以及配置文件的生成、备份、变更审批、符合性检查等方面；

h) 应检查是否具有内部网络所有外联的授权批准书；

i) 应检查在规定的保存时间范围内是否存在网络审计日志。

8.2.5.6.5 结果判定

a) 如果8.2.5.6.4 e）中有关现场操作的访谈回答为必须两人以上，经双重认可方能操作，并要形成审计日志，则该测评项为肯定；

b) 8.2.5.6.4 a）-i）均为肯定，则信息系统符合本单元测评项要求。

8.2.5.7 系统安全管理

8.2.5.7.1 测评项

a) 应指定专人对系统进行管理，删除或者禁用不使用的系统缺省账户；

b) 应制定系统安全管理制度，对系统安全配置、系统帐户以及审计日志等方面作出规定；

c) 应对能够使用系统工具的人员及数量进行限制和控制；

d) 应定期安装系统的最新补丁程序，并根据厂家提供的可能危害计算机的漏洞进行及时修补，并在安装系统补丁前对现有的重要文件进行备份；

e) 应根据业务需求和系统安全分析确定系统的访问控制策略，系统访问控制策略用于控制分配信息系统、文件及服务的访问权限；

f) 应对系统账户进行分类管理，权限设定应当遵循最小授权要求；

g) 应对系统的安全策略、授权访问、最小服务、升级与打补丁、维护记录、日志及配置文件的生成、备份、变更审批、符合性检查等方面做出具体规定；

h) 应规定系统审计日志的保存时间以便为可能的安全事件调查提供支持；

i) 应进行系统漏洞扫描，对发现的系统安全漏洞进行及时的修补；

j) 应明确各类用户的责任、义务和风险，对系统账户的登记造册、用户名分配、初始口令分配、用户权限及其审批程序、系统资源分配、注销等作出规定；

k) 应对于账户安全管理的执行情况进行检查和监督，定期审计和分析用户账户的使用情况，对发现的问题和异常情况进行相关处理。

8.2.5.7.2 测试方法

访谈，检查。

8.2.5.7.3 测试对象

安全主管，安全员，系统管理员，系统审计员，系统安全管理制度，系统审计日志，系统漏洞扫描报告。

8.2.5.7.4 测评实施

a) 应访谈安全主管，询问是否指定专人负责系统安全管理；
b) 应访谈系统管理员，询问对系统工具的使用（如脆弱性扫描工具）是否采取措施控制不同使用人员及数量；
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，是否在测试环境中测试其对应用系统的影响；在安装系统补丁前是否对重要文件（系统配置、系统用户数据等）进行备份，采取什么方式进行；是否对系统进行过漏洞扫描，发现漏洞是否进行及时修补；
d) 应访谈安全员，询问是否将系统安全管理工作（包括系统安全配置、系统帐户、审计日志等）制度化；
e) 应访谈系统管理员，询问对不常用的系统缺省用户是否采取了一定的处理手段阻止其继续使用（如删除或禁用）；是否对系统帐户安全管理情况是否定期进行检查和分析，发现问题如何处理；
f) 应访谈审计员，询问是否规定系统审计日志保存时间，多长时间；
g) 应检查在规定的保存时间范围内是否存在系统审计日志；
h) 应检查系统漏洞扫描报告，查看其内容是否覆盖系统存在的漏洞、严重级别、原因分析、改进意见等方面；
i) 应检查系统安全管理制度，查看其内容是否覆盖系统安全配置（包括系统的安全策略、授权访问、最小服务、升级与打补丁）、系统帐户（用户责任、义务、风险、权限审批、权限分配、帐户注销等）、审计日志以及配置文件的生成、备份、变更审批、符合性检查等方面。

8.2.5.7.5 结果判定

a) 8.2.5.7.4 a）—i）均为肯定，则信息系统符合本单元测评项要求。

8.2.5.8 恶意代码防范管理

8.2.5.8.1 测评项

a) 应提高所用用户的防病毒意识，告知及时升级防病毒软件；
b) 应在读取移动存储设备（如软盘、移动硬盘、光盘）上的数据以及网络上接收文件或邮件之前，先进行病毒检查，对外来计算机或存储设备接入网络系统之前也要进行病毒检查
c) 应指定专人对网络和主机的进行恶意代码检测并保存检测记录；
d) 应建立恶意代码防范管理制度，对防恶意代码软件的授权使用、恶意代码库升级、定期汇报等作出明确管理规定；
e) 应定期检查信息系统内各种产品的恶意代码库的升级情况并进行记录，对主机防病毒产品、防病毒网关和邮件防病毒网关上截获的危险病毒或恶意代码进行及时分析处理，并形成书面的报表和总结汇报。

8.2.5.8.2 测试方法

访谈，检查。

8.2.5.8.3 测试对象

安全员，恶意代码防范管理制度，恶意代码检测记录，升级记录，分析报告。

8.2.5.8.4 测评实施

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，如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；
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，并保存记录；

c） 应访谈安全员，询问是否将恶意代码防范管理工作（包括软件的授权使用、升级、情况汇报等）制度化，对其执行情况是否进行检查，检查周期多长；

d） 应访谈安全员，询问是否对恶意代码库的升级情况进行记录，对截获的危险病毒或恶意代码是否进行及时分析处理，并形成书面的报表和总结汇报；

e） 应访谈工作人员，询问其是否熟知恶意代码基本的防范手段，主要包括哪些；

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

g） 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。

8.2.5.8.5 结果判定

a） 如果 8.2.5.8.4 e）中访谈人员回答内容与测评实施 a）回答内容基本一致，则该项为肯定；

b） 8.2.5.8.4 a）—g）均为肯定，则信息系统符合本单元测评项要求。

8.2.5.9 密码管理

8.2.5.9.1 测评项

a） 应建立密码使用管理制度，密码算法和密钥的使用应符合国家密码管理规定。

8.2.5.9.2 测试方法

访谈，检查。

8.2.5.9.3 测试对象

安全员，密码管理制度。

8.2.5.9.4 测评实施

a） 应访谈安全员，询问密码算法和密钥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。

8.2.5.9.5 结果判定

a） 8.2.5.9.4 a）—b）均为肯定，则信息系统符合本单元测评项要求。

8.2.5.10 变更管理

8.2.5.10.1 测评项

a） 应确认系统中将发生的变更，并制定变更方案；

b） 应建立变更管理制度，重要系统变更前，应向主管领导申请，变更方案经过评审、审批后方可实施变更；

c） 系统变更情况应向所有相关人员通告；

d） 应建立变更控制的申报和审批文件化程序，变更影响分析应文档化，变更实施过程应记录，所有文档记录应妥善保存；

e） 中止变更并从失败变更中恢复程序应文档化，应明确过程控制方法和人员职责，必要时恢复过程应经过演练；

f） 变更控制的申报和审批程序应控制所有系统变更情况；

g） 应定期检查变更控制的申报和审批程序的执行情况，评估系统现有状况与文档记录的一致性。

8.2.5.10.2 测试方法

访谈，检查。

8.2.5.10.3 测试对象

系统运维负责人，系统变更申请书，变更方案，变更管理制度，变更申报和审批程序，变更失败恢复程序，变更评估报告，变更过程记录文档。

8.2.5.10.4 测评实施

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，变更过程是否文档化并保存，是否修改相关的操作流程（如系统配置发生变更后，相应的操作流程是否修改）；

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) 应检查重要系统的变更申请书，查看其是否有主管领导的批准；

e) 应检查系统变更方案，查看其是否对变更类型、变更原因、变更过程、变更前评估等方面进行规定；

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过程记录文档和变更方案。

8.2.5.10.5 结果判定

a) 如果系统没有发生过变更，则8.2.5.10.4 i）不适用；

b) 8.2.5.10.4 a）—i）均为肯定，则信息系统符合本单元测评项要求。

8.2.5.11 备份与恢复管理

8.2.5.11.1 测评项

a) 应识别需要定期备份的重要业务信息、系统数据及软件系统等；

b) 应规定备份信息的备份方式（如增量备份或全备份等）、备份频度（如每日或每周等）、存储介质、保存期等；

c) 应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略，备份策略应指明备份数据的放置场所、文件命名规则、介质替换频率和将数据离站运输的方法；

d) 应指定相应的负责人定期维护和检查备份及冗余设备的状况，确保需要接入系统时能够正常运行；

e) 根据备份方式，规定备份及冗余设备的安装、配置和启动的流程；

f) 应建立控制数据备份和恢复过程的程序，备份过程应记录，所有文件和记录应妥善保存；

g) 应根据系统级备份所采用的方式和产品，建立备份设备的安装、配置、启动、操作及维护过程控制的程序，记录设备运行过程状况，所有文件和记录应妥善保存；

h) 应定期执行恢复程序，检查和测试备份介质的有效性，确保可以在恢复程序规定的时间内完成备份的恢复；

i) 对需要采取加密或数据隐藏处理的备份数据，进行备份和加密操作时要求两名工作人员在场并登记备案。

8.2.5.11.2 测试方法

访谈，检查。

8.2.5.11.3 测试对象

系统管理员，数据库管理员，网络管理员，备份管理文档，备份和恢复策略文档，备份

设备操作流程文档，备份和恢复程序，备份过程记录文档。

8.2.5.11.4 测评实施

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；对其的备份工作是否以文档形式规范了备份方式、频度、介质、保存期等内容，数据备份和恢复策略是否文档化，备份和恢复过程是否文档化，对特殊备份数据（如保密数据）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，询问其对备份及冗余设备的安装、配置和启动工作是否根据一定的流程进行，是否记录操作过程，是否保存记录文档，是否指定专人对备份设备的有效性定期维护和检查，多长时间检查一次；

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

d) 应检查是否具有规定备份方式、频度、介质、保存期的文档；

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) 应检查备份设备操作流程文档，查看其是否规定备份及冗余设备的安装、配置、启动、关闭等操作流程；

g) 应检查备份过程记录文档，查看其内容是否覆盖备份时间、备份内容、备份操作、备份介质存放等内容；查看是否具有保密数据的备份过程记录文档。

8.2.5.11.5 结果判定

a) 8.2.5.11.4 a）－g）均为肯定，则信息系统符合本单元测评项要求。

8.2.5.12 安全事件处置

8.2.5.12.1 测评项

a) 所有用户均有责任报告自己发现的安全弱点和可疑事件，但任何情况下用户均不应尝试验证弱点；

b) 应制定安全事件报告和处置管理制度，规定安全事件的现场处理、事件报告和后期恢复的管理职责；

c) 应分析信息系统的类型、网络连接特点和信息系统用户特点，了解本系统和同类系统已发生的安全事件，识别本系统需要防止发生的安全事件，事件可能来自攻击、错误、故障、事故或灾难；

d) 应根据国家相关管理部门对计算机安全事件等级划分方法，根据安全事件在本系统产生的影响，将本系统计算机安全事件进行等级划分；

e) 应制定的安全事件报告和响应处理程序，确定事件的报告流程，响应和处置的范围、程度，以及处理方法等；

f) 应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训，制定防止再次发生的补救措施，过程形成的所有文件和记录均应妥善保存；

g) 对造成系统中断和造成信息泄密的安全事件应采用不同的处理程序和报告程序；

h) 可能涉及国家秘密的重大失、泄密事件应按照有关规定向公安、安全、保密等部门汇报；

i) 严格控制参与涉密事件处理和恢复的人员，重要操作要求至少两名工作人员在场并登记备案。

8.2.5.12.2 测试方法

访谈，检查。

8.2.5.12.3 测试对象

系统运维负责人，工作人员，安全事件报告和处置管理制度，安全事件记录文档，安全事件报告和处理程序文档。

8.2.5.12.4 测评实施

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、保密等国家部门汇报，安全事件的报告和响应处理过程是否制度化和文档化，不同安全事件是否采取不同的处理和报告程序，对涉密事件的处理是否要求现场人员数量；

b) 应访谈系统运维负责人，询问本系统已发生的和需要防止发生的安全事件主要有哪几类，对识别出的安全事件是否根据其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) 应访谈工作人员，询问其发生安全事件时的报告流程；

d) 应检查安全事件报告和处置管理制度，查看其是否描述在安全事件处置、报告和恢复等工作中不同部门和人员的职责；

e) 应检查安全事件定级文档，查看其内容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；

f) 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；

g) 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，是否明确具体报告方式、报告内容、报告人等方面内容。

8.2.5.12.5 结果判定

a) 如果 8.2.5.12.4 a）中访谈回答为涉密事件的处理必须两人在现场，则该项为肯定；

b) 如果 8.2.5.12.4 c）中访谈回答与 g）中描述一致，则该项为肯定；

c) 8.2.5.12.4 a）—g）为肯定，则信息系统符合本单元测评项要求。

8.2.5.13 应急预案管理

8.2.5.13.1 测评项

a) 应在统一的应急预案框架下制定不同事件的应急预案，应急预案框架应包括启动预案的条件、应急处理流程、系统恢复流程和事后教育和培训等内容；

b) 应从人力、设备、技术和财务等方面确保应急预案的执行有足够的资源保障；

c) 应对系统相关的人员进行培训使之了解如何及何时使用应急预案中的控制手段及恢复策略，对应急预案的培训至少每年举办一次；

d) 应急预案应定期演练，根据不同的应急恢复内容，确定演练的周期；

e) 应规定应急预案需要定期审查和根据实际情况更新的内容，并按照执行；

f) 应根据信息系统的灾难备份技术措施，制定相应的灾难恢复计划；

g) 应急预案和灾难恢复计划应得到测试以确保各个恢复规程的正确性和预案整体的有效性，测试内容包括运行系统恢复、人员协调、备用系统性能测试、通信连接等，根据测试结果，对不适用的规定进行修改或更新；

h) 应随着信息系统的变更，定期对原有的应急预案重新评估，修订完善。

8.2.5.13.2 测试方法

访谈，检查。

8.2.5.13.3 测试对象

系统运维负责人，应急响应预案文档，应急预案培训记录，应急预案演练记录，应急预

案审查记录，灾难恢复计划文档，应急预案测试方案，测试结果文档。

8.2.5.13.4 测评实施

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和灾难恢复计划，是否对系统相关人员进行应急预案培训，培训内容是什么，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，是否对应急预案和灾难恢复计划进行测试并修改，是否对应急预案定期进行审查并更新，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) 应检查应急响应预案和灾难恢复文档，查看其内容是否覆盖启动预案的条件、应急处理流程、系统恢复流程和事后教育等内容；

d) 应检查是否具有应急预案培训记录、演练记录和审查记录；

e) 应检查应急预案测试方案，查看其内容是否覆盖运行系统恢复、人员协调、备用系统性能测试、通信连接等方面；查看测试结果记录，是否记录测试出现的问题、原因分析和修改意见。

8.2.5.13.5 结果判定

a) 8.2.5.13.4 a）—e）均为肯定，则信息系统符合本单元测评项要求。

9 第五级安全控制测评

第五级信息系统是涉及国家安全、社会秩序、经济建设和公共利益的重要信息系统，国家指定专门部门或者专门机构对其进行专门控管，对第五级信息系统的安全控制进行测评由国家指定的专门部门或者专门机构参照第四级的安全控制测评要求另行规范。

10 系统整体测评

10.1 安全控制间安全测评

安全控制间的安全测评主要考虑同一区域内、同一层面上的不同安全控制间存在的功能增强、补充或削弱等关联作用。安全功能上的增强和补充可以使两个不同强度、不同等级的安全控制发挥更强的综合效能，可以使单个低等级安全控制在特定环境中达到高等级信息系统的安全要求。例如，可以通过物理层面上的物理访问控制来增强其安全防盗窃功能等。安全功能上的削弱会使一个安全控制的引入影响另一个安全控制的功能发挥或者给其带来新的脆弱性。例如，应用安全层面的代码安全与访问控制，如果代码安全没有做好，很可能会使应用系统的访问控制被旁路。

在测评安全控制间的增强和补充作用时，应先根据安全控制的具体实现和部署方式以及信息系统的实际环境，分析出位于物理安全、网络安全、主机系统安全、应用安全和数据安全等同一层面内的哪些安全技术控制间可能存在安全功能上的增强和补充作用，分析出处在安全管理机构、安全管理制度、人员安全管理、系统建设管理和系统运维管理等同一方面内的哪些安全管理控制间可能存在安全功能上的增强和补充作用。如果增强和补充作用是可以进行测评验证的，则应设计出具体测评过程，进行测评验证。最后根据测评分析结果，综合判断安全控制相互作用后，是否发挥出更强的综合效能，使其功能增强或得到补充。

在测评安全控制间的削弱作用时，应先根据安全控制的具体实现方式和部署方式以及信息系统的实际环境，分析出位于物理安全、网络安全、主机系统安全、应用安全和数据安全等同一层面内的哪些安全技术控制间可能会存在安全功能上的削弱作用，分析出处在安全管理机构、安全管理制度、人员安全管理、系统建设管理和系统运维管理等同一方面内的哪些安全管理控制间可能存在安全功能上的削弱作用。如果功能削弱是可以进行测评验证的，则应设计出具体测评过程进行测评验证。最后根据测评分析结果，综合判断安全控制相互作用

后，一个安全控制是否影响另一个安全控制的功能发挥或者给其带来新的脆弱性，使其功能削弱。

如果安全控制间优势互补，使单个低等级安全控制发挥的安全功能达到信息系统相应等级的安全要求，则可认为该安全控制没有影响信息系统的整体安全保护能力。如果安全控制间存在削弱作用，使某个安全控制的功能等级降低到其安全功能已不能达到信息系统相应等级的安全要求，则可认为该安全控制影响到信息系统的整体安全保护能力。

10.2 层面间安全测评

层面间的安全测评主要考虑同一区域内的不同层面之间存在的功能增强、补充和削弱等关联作用。安全功能上的增强和补充可以使两个不同层面上的安全控制发挥更强的综合效能，可以使单个低等级安全控制在特定环境中达到高等级信息系统的安全要求。安全功能上的削弱会使一个层面上的安全控制影响另一个层面安全控制的功能发挥或者给其带来新的脆弱性。

在测评层面间的功能增强和补充作用时，应先根据层面的整合集成方式和信息系统的实际环境，重点研究不同层面上相同或相似的安全控制（如主机系统层面与应用层面上的身份鉴别之间的关系），以及技术与管理上各层面的关联关系，分析出哪些安全控制间可能会存在安全功能上的增强和补充作用。如果增强和补充作用是可以进行测评验证的，则应设计出具体测评过程，进行测评验证。最后根据测评分析结果，综合判断层面间整合后，是否发挥出更强的综合效能，使其功能增强或得到补充。

在测评层面间的功能削弱作用时，应先根据层面的整合集成方式和信息系统的实际环境，分析出哪些安全技术层面间和安全管理方面可能存在安全功能上的削弱作用。如果功能削弱是可以进行测评验证的，则应设计出具体测评过程，进行测评验证。最后根据测评分析结果，综合判断不同层面整合后，一个层面是否影响另一个层面安全功能的发挥或者给其带来新的脆弱性，使其功能削弱。

如果层面间安全功能增强或优势互补，使单个或部分低等级安全控制发挥的安全功能达到信息系统的安全要求，则可认为这些安全控制没有影响信息系统的整体安全保护能力。如果层面间存在削弱作用，使某个或某些安全控制的功能等级降低到其安全功能已不能满足信息系统相应等级的安全要求，则可认为这些安全控制影响到信息系统的整体安全保护能力。

10.3 区域间安全测评

区域间的安全测评主要考虑互连互通（包括物理上和逻辑上的互连互通等）的不同区域之间存在的安全功能增强、补充和削弱等关联作用，特别是有数据交换的两个不同区域。例如，流入某个区域的所有网络数据都已经在另一个区域上做过网络安全审计，则可以认为该区域通过区域互连后具备网络安全审计功能。安全功能上的增强和补充可以使两个不同区域上的安全控制发挥更强的综合效能，可以使单个低等级安全控制在特定环境中达到高等级信息系统的安全要求。安全功能上的削弱会使一个区域上的安全功能影响另一个区域安全功能的发挥或者给其带来新的脆弱性。

在测评区域间的功能增强和补充作用时，应先根据区域间互连互通的集成方式和信息系统的实际环境，特别是区域间的数据流流向和控制方式，分析出哪些区域间可能会存在安全功能上的增强和补充作用。如果增强和补充作用是可以进行测评验证的，则应设计出具体测评过程，进行测评验证。最后根据测评分析结果，综合判断区域间互连互通后，是否发挥出更强的综合效能，使其功能增强或得到补充。

在测评区域间的功能削弱作用时，应先根据区域间互连互通的集成方式和信息系统的实际环境，特别是区域间的数据流流向和控制方式，分析出哪些区域间可能会存在安全功能上的削弱作用。如果功能削弱是可以进行测评验证的，则应设计出具体测评过程，进行测评验

证。最后根据测评分析结果，综合判断不同区域互连互通后，一个区域是否影响另一个区域安全功能的发挥或者给其带来新的脆弱性，使其功能削弱。

如果区域间安全功能增强或优势互补，使单个或部分低等级安全控制发挥的安全功能达到信息系统的安全要求，则可认为这些安全控制没有影响信息系统的整体安全保护能力。如果区域间存在削弱作用，使某个或某些安全控制的功能等级降低到其安全功能已不能满足信息系统相应等级的安全要求，则可认为这些安全控制影响到信息系统的整体安全保护能力。

10.4 系统结构安全测评

系统结构安全测评主要考虑信息系统整体结构的安全性和整体安全防范的合理性。例如，由于信息系统边界上的网络入侵防范设备的管理接口连接方式不当，可能使网络访问控制出现旁路，出现信息系统整体安全防范不当。测评分析信息系统整体结构的安全性，主要是指从信息安全的角度，分析信息系统的物理布局、网络结构和业务逻辑等在整体结构上是否合理、简单、安全有效。测评信息系统整体安全防范的合理性，主要是指从系统的角度，分析研究信息系统安全防范在整体上是否遵循纵深防御的思路，明晰系统边界，确定重点保护对象，在适当的位置部署恰当的安全技术和安全管理措施等。

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、网络和业务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合理、主要关系是否简单、整体是否安全有效等。

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是否恰当合理等。

附录 A

（资料性附录）

测评强度

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安全控制测评的具体测评实施过程要求。为了便于理解、对比不同测评方式的测评强度以及不同级别信息系统安全控制测评的测评强度增强情况，分别编制表 A.1 测评方式的测评强度描述，表 A.2 不同安全等级信息系统的测评强度要求表和表 A.3 安全控制测评强度列表。

A.1 测评方式的测评强度描述

表 A.1 测评方式的测评强度

测评方式	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，可以分为三种：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，可以分为三种：简要的、充分的和全面的。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 信息系统测评强度

为了进一步理解不同等级信息系统在测评强度上的不同，表 A.2 在表 A.1 的基础上，从数量和种类的角度详细分析了不同测评方式在不同安全等级信息系统安全测评中的不同体现。

表 A.2 信息系统测评强度要求

测评强度		信息系统安全等级			
		第一级	第二级	第三级	第四级
访谈	广度	种类和数量上抽样，种类和数量都较少	种类和数量上抽样，种类和数量都较多	数量上抽样，基本覆盖	数量上抽样，基本覆盖
	深度	简要	充分	较全面	全面
检查	广度	种类和数量上抽样，种类和数量都较少	种类和数量上抽样，种类和数量都较多	数量上抽样，基本覆盖	数量上抽样，基本覆盖
	深度	简要	充分	较全面	全面
测试	广度	种类和数量、范围上抽样，种类和数量都较少，范围小	种类和数量、范围上抽样，种类和数量都较多，范围大	数量、范围上抽样，基本覆盖	数量、范围上抽样，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

表 A.3 则针对不同安全等级信息系统，汇总第 5 章到第 8 章中第一级到第四级安全控制测评中的具体测评实施项的变化，描述信息系统测评强度在安全控制测评具体实施过程中的变化情况。

表 A.3 中的‘保持’表示该级安全控制测评保持了与前一级相同或者增强了的测评实施项目（其中项目号为黑体的表示增强了的测评实施项目）；‘新增’表示该级安全控制测评比前一级新增加的测评实施项目；表格中‘--’表示该表格项为空。

表格中的 a)b)c)等实施项目编号是指当前级别下测评单元的测评实施项目编号，与前一级测评单元的测评实施项目编号不存在对应关系，如第三级安全控制测评的‘物理位置的选择’测评单元中‘保持’的测评实施项目编号 a)c)d)等是 7.1.1.1.4 测评实施的项目编号，而不是第二级安全控制测评的‘物理位置的选择’测评单元 6.1.1.1.4 测评实施中的项目编号。

表 A.3 安全控制测评强度对比列表

类	层面	测评单元	测评实施						
			第一级	第二级		第三级		第四级	
				保持	新增	保持	新增	保持	新增
安全技术测评	物理安全	物理位置的选择	--	--	a)b)c)	a)c)d)	b)e)f)g)	a)b)c)d)e)f)g)	--
		物理访问控制	a)b)c)	a)c)d)	b)e)f)	a)c)d)e)f)g)	b)h)i)j)	a)b)c)d)e)f)g)h)i)j)	k)
		防盗窃和防破坏	a)b)c)d)	a)d)h)	b)c)e)f)	a)b)c)d)e)f)g)i)	h)	a)b)c)d)e)f)g)h)i)	--
		防雷击	a)b)	a)c)	b)	a)b)c)	d)	a)b)c)d)	e)
		防火	a)b)c)	a)c)d)	b)	a)b)c)d)	e)	a)b)c)d)e)	--

	防水和防潮	a)b)c)d)	a)c)d)e)	b)f)	a)b)c)d)e)f)	--	a)b)c)d)e)f)	g)
	防静电	--	--	a)b)c)d)	a)b)c)d)	e)	a)b)c)d)e)	f)
	温湿度控制	a)b)c)	a)c)d)	b)	a)b)c)d)	--	a)b)c)d)	--
	电力供应	a)b)c)d)	a)c)d)e)	b)f)	a)b)d)e)f)g)	c)h)i)	a)b)c)d)e)f)g)h)i)	--
	电磁防护	--	--	a)b)c)d)e)	a)b)c)d)e)	f)	a)b)c)d)e)f)	g)h)
网络安全	结构安全与网段划分	a)b)c)d)e)f)	a)b)c)d)e)f)g)h)i)	j)k)l)	a)b)c)d)e)f)g)h)i)k)l)m)	j)n)	a)b)c)d)e)f)g)h)i)j)k)l)m)n)	--
	网络访问控制	a)b)	a)b)	c)	a)b)g)h)	c)d)e)f)	a)d)e)	b)c)
	拨号访问控制	a)b)	a)b)c)	d)	a)b)c)d)	--	a)	b)c)
	网络安全审计	--	--	a)b)c)d)	a)b)c)d)e)	f)g)	a)b)c)d)g)h)i)	e)f)
	边界完整性检查	--	--	a)b)c)d)	a)b)c)d)	e)f)	a)b)c)e)f)g)	d)
	网络入侵防范	--	--	a)b)c)d)	a)b)d)e)	c)f)	a)b)c)d)e)f)	--
	恶意代码防范	--	--	a)b)c)d)e)f)	a)b)c)d)e)f)	--	a)b)c)d)e)f)	--
	网络设备防护	a)b)c)	a)b)c)d)	e)f)g)	a)b)c)d)e)f)g)	--	a)b)c)d)e)f)g)	--
主机安全	身份鉴别	a)b)c)d)e)f)g)h)i)	a)b)c)d)e)f)g)h)	i)	a)b)c)d)e)g)i)j)k)	f)h)l)m)n)o)p)	a)b)c)d)e)f)g)h)i)j)k)l)m)n)o)p)	--
	自主访问控制	a)b)c)d)e)f)g)	a)b)e)f)	c)d)g)	a)b)c)d)e)f)h)i)	g)	a)b)c)d)e)f)g)h)j)	i)
	强制访问控制	--	--	--	--	a)b)c)d)e)f)	a)b)c)d)e)f)	--
	可信路径	--	--	--	--	--	--	a)b)c)d)e)f)g)

		安全审计	--	--	a)b)c)d)e)f)g)	a)b)c)d)g)i)j)	e)f)h)	a)b)c)d)e)f)g)j)k)l)m)	h)i)
		系统保护	--	--	a)b)c)d)e)	--	a)b)	b)d)	a)c)e)
		剩余信息保护	--	--	a)b)c)d)	a)b)c)d)	--	a)b)c)d)	--
		入侵防范	--	--	--	--	a)b)c)d)e)f)g)h)i)	a)b)c)d)e)f)g)h)i)	--
		恶意代码防范	a)b)	a)c)	b)d)	a)b)c)d)	--	a)b)c)d)	--
		资源控制	--	--	a)b)c)	a)d)e)	b)c)f)g)	a)b)c)d)e)f)g)	--
	应用安全	身份鉴别	a)b)c)d)	a)b)e)f)	c)d)g)h)	a)b)c)f)g)h)i)k)l)	d)e)j)	a)b)c)d)e)f)g)h)i)j)k)l)	--
		访问控制	a)b)c)d)e)f)	a)b)f)g)h)i)	c)d)e)	a)b)c)d)e)f)g)h)i)	--	a)b)c)d)e)f)h)i)j)k)	g)l)
		安全审计	--	--	a)b)c)d)e)f)g)h)	a)b)c)d)g)h)i)	e)f)	a)b)c)e)f)g)j)k)l)	d)h)i)m)
		剩余信息保护	--	--	a)b)c)	a)b)c)	d)	a)b)c)d)	--
		通信完整性	a)b)c)	a)b)c)	--	a)b)c)	--	a)b)c)	--
		通信保密性	--	--	a)b)c)d)	a)c)d)e)	b)	a)c)d)e)f)	b)
		抗抵赖	--	--	--	--	a)b)	a)b)	--
		软件容错	a)b)c)d)	a)b)c)	d)	a)b)c)d)	e)	a)b)e)f)g)	c)d)
		资源控制	a)b)c)	a)b)c)	d)	a)b)e)f)	c)d)g)h)	a)b)c)d)e)f)g)h)	--
		代码安全	a)b)c)	a)b)d)	c)	a)b)c)d)f)	e)g)	a)b)c)d)e)g)	f)
	数据安全	数据完整性	a)b)c)	a)b)c)	--	a)b)c)d)	--	a)b)c)d)	e)
		数据保密性	a)b)c)d)e)f)	a)b)c)d)g)h)	e)f)i)	a)b)c)d)f)e)h)i)	g)	a)b)c)d)e)f)g)h)i)j)	
		数据备份和恢复	a)b)c)d)e)	a)b)c)d)e)	f)	a)b)c)e)	d)f)g)	a)b)c)d)e)f)g)	h)

安全管理测评	安全管理机构	岗位设置	a)b)	b)d)	a)c)	b)c)d)e)	a)f)g)h)	a)b)c)d)e)f)g)h)	--
		人员配备	a)b)	a)c)	b)	a)c)d)	b)	a)b)d)e)	c)
		授权和审批	a)b)c)	a)b)d)	c)	a)b)	c)d)e)f)g)	a)b)c)d)e)f)g)	--
		沟通和合作	a)b)c)	a)b)c)d)	e)f)	a)b)d)e)f)h)	c)g)i)	a)b)c)d)e)f)g)h)i)	--
		审核和检查	--	--	a)b)c)	a)b)	c)d)e)f)g)	a)b)c)d)e)f)g)	--
	安全管理制度	管理制度	a)b)c)	a)b)c)	d)	b)c)d)	a)e)	a)b)c)d)e)	--
		制定和发布	a)b)c)	b)d)	a)c)e)	b)c)d)e)	a)f)	a)b)c)d)e)f)	--
		评审和修订	--	--	b)c)	a)b)d)f)	c)e)g)	a)b)c)e)f)g)h)	d)
	人员安全管理	人员录用	a)b)c)d)	a)b)c)d)	e)f)	a)b)d)e)f)g)	c)h)i)	a)b)c)d)e)f)g)h)i)	--
		人员离岗	a)b)	a)c)	b)d)	a)b)d)e)	c)	a)b)c)d)e)	f)g)
		人员考核	--	--	a)b)c)	a)b)c)	d)	a)b)c)d)	--
		安全意识教育和培训	a)b)	a)b)	c)d)	a)b)c)d)	--	a)b)c)d)	--
		第三方人员访问管理	a)b)	a)c)	b)d)e)	a)b)c)f)	d)e)	a)b)c)d)e)f)	--
	系统建设管理	系统定级	a)b)c)d)	a)b)c)d)	--	a)b)c)e)	d)	a)b)c)d)e)	--
		系统备案	--	--	--	--	a)b)c)d)e)	a)b)c)d)e)	--
		安全方案设计	a)b)c)d)e)	a)b)c)d)	e)	b)	a)c)d)e)f)g)h)i)	a)b)c)d)e)f)g)h)i)	--
		产品采购	a)b)	b)d)	a)c)e)	a)b)c)e)f)	d)g)	a)b)c)d)e)f)g)	--
		自行软件开发	a)b)c)d)	a)b)d)e)	c)	a)b)c)d)f)	e)	a)b)c)d)f)g)	e)h)
		外包软件开发	a)b)c)	a)b)c)	d)	a)b)c)d)e)	--	a)b)c)d)	--

		工程实施	a)b)	a)c)	b)d)	a)b) c)d)	e)	a)b)c) d)e)	--
		测试验收	a)b) c)d)	a)b) c)d)	--	a)b)c) d)e)	f)	a)b)c) d)e)f)	--
		系统交付	a)b)c)	a)b)c)	d)	a)b)c) d)	e)	a)b)c) d)e)	--
		安全服务商选择	a)	a)	--	a)	--	a)	--
	系统运维管理	环境管理	a)b)c)	a)b)d)	c)e)	a)b)e) g)	c)d)f) h)	a)b)d)e) f)g)h)i)	c)
		资产管理	a)b)c) d)	a)b)d) e)	c)f)	a)b)c) d)e)g)	f)	a)b)c)e) f)g)h)	d)
		介质管理	a)b)c)	a)b)d)	c)e)	a)b)e) g)	c)d)f) h)	a)b)c)d) e)f)g)h)	--
		设备管理	a)b)c) d)e)	a)b)e) f)g)	c)d)	a)b)c) e)f)g) h)	d)i)	a)b)c)d) e)f)g)h)	--
		监控管理	a)	a)	--	a)	b)c)	a)b)c)	d)e)
		网络安全管理	a)b)c)	a)b)c)	d)e)f) g)	a)b)c) d)e)f) g)	h)i)j) k)	a)b)c)d) e)f)g)h) i)j)k)	l)
		系统安全管理	a)b)c)	a)c)d) e)	b)f)g) h)i)	a)c)d) e)f)g) h)i)	b)	a)b)c)d) e)f)g)h) i)	--
		恶意代码防范管理	a)	a)	b)c)d)	a)b)f)	c)d)e) g)h)	a)b)c)d) e)f)g)	--
		密码管理	--	a)	--	a)	b)	a)b)	--
		变更管理	--	a)b)c) d)e)	--	a)b)d) e)f)	c)g)h) i)	a)b)c)d) e)f)g)h) i)	--
		备份与恢复管理	a) b)	a)c)	b)d)e)	a)b)c) d)e)f)	g)	a)b)c)d) e)f)g)	
		安全事件处置	a) b)	a)d)	b)c)e) f)	a)b)d) e)f)	c)g)	a)b)c)d) e)f)g)	
		应急预案管理	--	--	a) b)	a) c)	b) d)	a)b)c)d)	e)

附录 B

（资料性附录）

关于系统整体测评的进一步说明

信息系统整体安全测评与被测系统组成结构密切相关，本章从信息系统‘水平分区域，垂直分层面’的思路出发对区域和层面进行了较为详细的描述，阐述被测系统在区域、层面间存在的构成关系。通过区域和层面的描述，可以进一步理解系统整体测评的内容和要求，使系统整体测评落实到具体的测试评估内容和过程中，确保系统整体测评能够恰当充分地反映出信息系统的整体安全状况。然后，举例子说明了信息系统整体测评的一些分析测评方法。

B.1 区域和层面

信息系统是由计算机及其相关配套设备、设施(含网络)构成的，按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统，是一个复杂系统。进行安全测评时，需要对这样一个复杂的系统进行合理剖分，恰当描述。‘水平分区域，垂直分层面’的思路是对复杂的信息系统进行剖分、描述的一种可行方法。

B.1.1 区域

信息系统中的计算机、设备和设施等都有其物理和逻辑位置，根据其所处的物理和逻辑位置范围可以把信息系统划分为一个或者多个不同的区域。区域具有一个相对独立的物理、逻辑范围，区域内的信息系统组件一般位于同一局域网内，面临相同或相似的物理、网络、主机、应用和管理等安全环境，采取相同或相似的安全措施，整体对外呈现一定的安全功能，使信息系统在整体安全性上表现出分区域的集成特性。

根据区域所处的网络拓扑逻辑位置，可以把信息系统的区域分为内部区域、边界区域和外部区域三大类。内部区域一般位于信息系统运营使用单位的物理控制范围内的局域网内，是信息系统进行信息处理的主体，是安全测评的一个重点。可以进一步根据业务处理功能，对内部区域进行细分，如终端区域、服务器区域等。边界区域处在两个不同的区域之间，通常是处在内部区域和信息系统外部区域之间（如连接内外区域的防火墙 DMZ 区），也属于信息系统的边界。信息系统外部区域通常是信息系统提供通信的公共网络（如 Internet、PSTN、ISDN、公共无线网络等）和专用网络（如 DDN 等）。在一般意义上，信息系统外部区域不属于信息系统的一个部分，而是信息系统外的其他网络系统。在进行安全测评时，可以暂时不考虑提供通信服务的外部区域的具体实现细节，可以认为外部区域是由通信线路连接网络设备构成的，具有通信能力的抽象线路模型。通过对外部区域模型化抽象处理后，对外部区域的安全测评关注点将放在外部区域的网络安全管理上。

不同区域之间可能需要进行信息交换，特别是有业务交互、数据通信的两个区域。为了进行信息交换，保证信息交换和交换信息的安全，区域之间会产生连接、交互、依赖、协调、协同等相互关联关系，使得区域之间安全功能发生相互作用，进而相互影响。如，在有数据通信的内部区域和边界区域之间，从信息系统外对边界区域构成一定的威胁，进而可以通过边界区域和内部区域之间的数据通信关系，进一步攻击信息系统的内部区域，影响到信息系统内部区域的安全。

不同区域之间相互作用会影响到区域的安全功能，可能使一个区域的安全功能得到增强、补充，或者被削弱，或者出现依赖。发生增强作用说明两个区域发生关联关系后，一个区域已有的安全功能得到进一步增强，发挥更好的安全保护功能，具有更好的安全保护能力。发生补充作用说明两个区域发生关联关系后，一个区域原本没有的一部分安全功能，通过另一个区域的相互作用，得到补充，使其具备这些安全功能。发生削弱作用说明两个区域发生

关联关系后，一个区域已有的安全功能被削弱，不能很好地发挥原有的安全保护功能。出现依赖说明一个区域的安全功能依赖于另一个区域配合，才能发挥应有的作用。依赖作用一般需要在安全控制的实现过程中事先设定，对其进行的安全测评，在安全控制测评单元的测试实施过程中已有体现。

B.1.2 层面

安全控制措施的功能发挥总是作用在信息系统的具体层面上的，这些层面主要包括物理安全、网络安全、主机系统安全、应用安全和数据安全等技术上的五个层面以及安全管理机构、安全管理制度、人员安全管理、系统建设管理和系统运维管理等管理上的五个方面。管理方面通过建立合理的人员组织、恰当的安全管理制度和操作规程等来保障安全技术能够综合有效地实现、正确地运行，在某种意义上，安全管理相当于安全技术的“黏合剂”。

a)物理安全

物理安全是支持信息系统运行的设施环境以及构成信息系统的计算机、设备和介质等物理层面的安全。物理层面构成组件可能分布在被测单位物理控制范围内，也可能位于被测单位物理控制范围外。一般来说，大部分物理层面构成组件位于被测单位（被测系统的运营使用单位）的物理控制范围内，主要分布在机房、介质存放地和终端运行场地等空间范围内。两个或者多个相连相通的不同区域物理空间的物理安全控制措施，因为有空间上的连接连通，可能会发生关联关系，使其安全功能相互作用。

b)网络安全

网络层面构成组件负责支撑信息系统进行网络互联，为信息系统各个构成组件进行通信提供安全传输服务，一般包括计算机、网络设备（包括网络安全设备）、连接线路以及它们构成的网络拓扑等。这些网络构成组件可能位于被测单位的物理控制范围内，也可能处于被测单位物理控制范围外。一般来说，大部分网络层面构成组件位于被测单位的物理控制范围内，形成一个或者多个局域网的形式，它们是网络层面安全保护的重点。位于被测单位的物理控制范围外的网络层面组成部分通常是由通信线路和通信设备共同构成，其中，通信线路包括由骨干网、城域网等网络构成的虚拟逻辑通信线路。

位于被测单位物理控制范围内的局域网上的构成组件，根据其承载业务的情况，按照其物理和逻辑位置，划分到相应的网络区域上。位于同一区域上的不同网络设备，通过协调、协同或者依赖等相互关系，发挥出不同的功能作用，共同作用到一个区域上。

两个不同区域可能需要在网络层面上进行互联互通，交换信息。两个不同区域一般来说有不同权限的用户，面临不同的危险，有不同的安全问题，网络互联互通后，这些安全问题可能会交叉出现，给另一个区域带来相同或相似的安全问题。两个不同区域互联互通的通信线路也可能给它们的通信带来威胁。如果互联互通是经过由骨干网、城域网等网络构成的通信线路，则面临的威胁将会更不确定，更大。为了节约资源，两个不同区域可能需要共用一些网络设备资源，构成网络设备和通信线路共用的情况。网络设备和通信线路共用的两个区域可能不需要直接交换信息，但是，这同样会使得两个不同区域因共用网络设备而出现安全问题交叉的可能，给不同区域带来相同或相似的安全问题。

c)主机系统安全

主机系统层面构成的组件主要有服务器、终端/工作站等所有计算机设备上的操作系统、数据库系统及其相关环境等，它们直接为信息系统对信息进行采集、加工、存储、传输、检索等处理提供环境，包括为信息系统用户提供人机交互的环境。

分布在同一服务器和终端/工作站等主机系统上身份鉴别、访问控制、安全审计、系统资源控制等安全功能，需要相互协作，共同发挥作用，才能保证系统的安全。同时，为了进一步加强操作系统环境的安全，还可以在服务器和终端/工作站上安装主机入侵防范和主机恶意代码防范软件等。这使得操作系统的安全环境变得更为复杂，因此，有必要分析这些安

全控制的引入对其他安全控制的影响。

d）应用安全

从功能上看，大多数应用系统主要是完成三种任务：获取用户输入，将输入存储为数据，按预定的操作规则处理这些数据。在应用系统中，用户一般需要和系统中的数据进行交互。因此，可以根据用户与数据之间所具有的层次把信息系统划分为三种：单层应用体系结构、两层应用体系结构和多层（三层以上）应用体系结构。

在单层应用体系结构中，用户界面、商业规则和数据管理等都在单一的应用层内实现。对数据本身来说，它可以是物理上位于一个远端位置，但是存取数据的逻辑却是应用系统的一部分。在这样的体系结构中，数据处理主要不是通过数据库，而是文件来存取数据，应用系统自己定义如何进行数据的存储、查询、读取等运算逻辑。应用安全和数据安全直接相关。

在两层应用体系结构模型中，商业规则和用户界面仍然结合在一起构成应用系统的客户端。但是数据的存取和管理独立出来由单独的通常是运行在不同的系统上的程序来完成，这样的数据存取和管理程序通常是数据库管理系统，如 MS SQL Server、Sybase 和 Oracle 等。数据库系统的安全相对独立于应用安全，但是应用安全仍然会威胁到数据安全。

在多层应用体系结构模型中，商业规则被进一步从客户端独立出来，运行在一个介于用户界面和数据存储的单独的系统之上。客户端程序提供应用系统的用户界面，用户输入数据，查看反馈回来的请求结果。商业中间层由封装了商业逻辑的组件构成，这些商业逻辑组件模拟日常的商业任务。数据层可以是数据库管理系统，也可以是事务处理或消息队列服务等。数据库系统离前端应用较远，中间有业务逻辑的隔离。应用层面的安全对数据库系统的安全影响较小。

e）数据安全

数据安全构成组件主要为信息系统安全功能数据和用户数据提供安全保护。这些数据可能处于传输和处理过程中，也可能处于存储状态。对于传输和处理过程中的数据，一般有机密性和完整性的安全要求，而对于存储中的数据，还需要有备份恢复的安全要求。

安全功能数据主要用于控制和管理信息系统的安全配置设置，使信息系统的安全功能能得到正确有效的执行。传输中的安全功能数据最常见的是用户鉴别信息，一般来说，它需要通过网络从客户端传输到认证服务器来进行鉴别。存储中的安全功能数据常见的有 ACL 列表、安全检测策略、审计配置等信息。用户数据主要是用于完成应用系统的使命，由应用系统按照应用目标和规则对其进行采集、加工、存储、传输、检索等处理的数据信息。

f）安全管理机构

安全管理机构包括安全管理的岗位设置、人员配备、授权和审批、沟通和合作等方面内容，严格的安全管理应该由相对独立的职能部门和岗位来完成。安全管理机构从组织上保证了信息系统的安全。

g）安全管理制度

在被测系统中，安全管理制度一般是文档化的，被正式制定、评审、发布和修订，内容包括策略、制度、规程、表格和记录等，构成一个塔字结构的文档体系，如图 B.1。

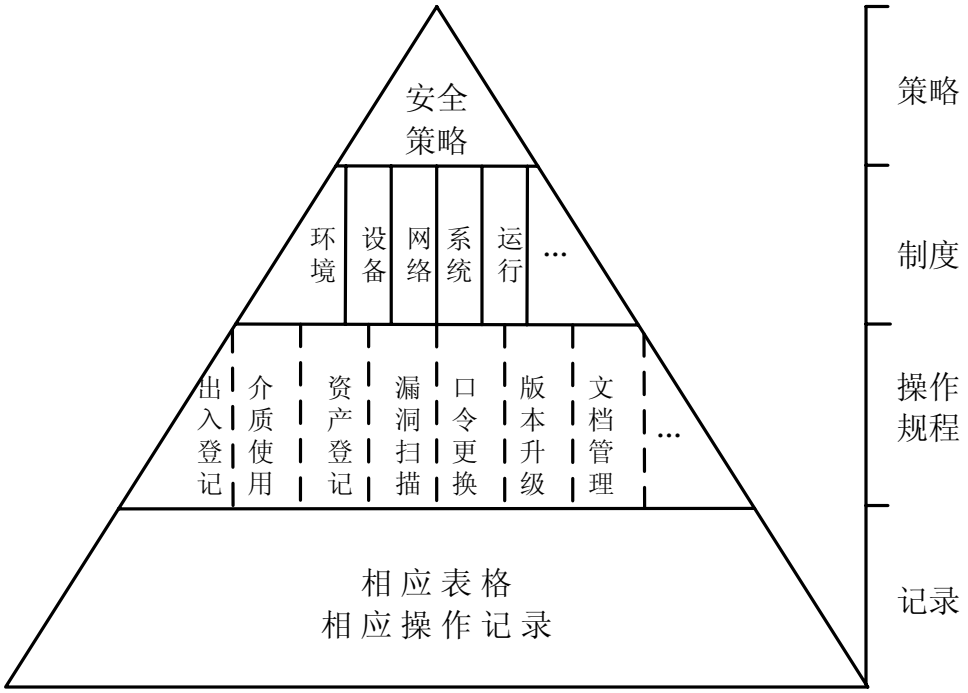

图 B.1 文档结构图

安全管理制度规范了各种安全管理制度的制修订和发布行为。安全管理制度直接关系到各种安全控制技术的正确、安全配置和合理使用。因此，安全管理制度的制修订和发布行为也将间接影响到信息系统的整体安全。

h）人员安全管理

人员安全管理包括信息系统用户、安全管理人员和第三方人员的管理，覆盖人员录用、人员离岗、人员考核、安全意识教育和培训、第三方人员管理等方面内容。工作人员直接运行、管理和维护信息系统的各种设备、设施和相关技术手段，与他们直接发生关联关系。因此，他们的知识结构和工作能力直接影响到信息系统其他层面的安全。

i）系统建设管理

系统建设管理包括系统定级、安全风险分析、安全方案设计、产品采购、自行软件开发、外包软件开发、工程实施、测试验收、系统交付、安全测评、系统备案等信息系统安全等级建设的各个方面。信息系统的安全是一个过程，是一项工程，它不但涉及到当前的运行状态，而且还关系到信息系统安全建设的各个阶段。只有在信息系统安全建设的各个阶段确保安全，才能使得运行中的信息系统有安全保证。

j）系统运维管理

系统运维管理包括运行环境管理、资产管理、介质管理、设备使用管理、运行监控管理、恶意代码防护管理、网络安全管理、系统安全管理、密码管理、变更管理、备份和恢复管理、安全事件处置和应急计划管理等方面内容。系统运维各个方面都直接关系到相关安全控制技术的正确、安全配置和合理使用。对信息系统运维各个方面提出具体的安全要求，可以为工作人员进行正确管理和运行提供工作准绳，直接影响到整个信息系统的安全。

B.2 信息系统测评的组成说明

根据对被测系统区域和层面的分析描述，可以看出，信息系统的安全控制综合集成到信息系统之后，会在层面内、层面间和区域间产生连接、交互、依赖、协调、协同等相互关联关系，共同作用于信息系统的安全功能，使信息系统的整体安全功能与信息系统的结构以及安全控制间、层面间和区域间的相互关联关系密切相关。如果相互关联关系具有相容性质，则综合集成后，安全控制间、层面间和区域间的安全控制可能会产生功能增强、补充等良性

关联作用。如果相互关联关系具有互斥性质，则综合集成后，安全控制间、层面间和区域间的安全控制可能会产生功能削弱的劣性关联作用。

在信息系统在安全控制部署、层面整合和区域互连等系统集成后呈现出的安全集成特性，在安全控制的测评单元中是没有体现的。因此，安全控制测评的基础上，有必要对集成系统和运行环境进行整体测评，以确定安全控制部署、层面整合、区域互连乃至整体系统结构等是否会增强或者削弱信息系统的整体安全保护能力;缺失或者低等级的安全控制是否会影响到系统的整体安全功能,在高等级的信息系统使用低等级的安全控制是否达到相应等级的安全要求等。

在测评内容上，在安全控制测评基础上，信息系统整体安全性测评应重点测评分析不同安全控制的部署、层面的整合和区域的互连后其安全功能的相互作用和对信息系统整体安全功能的影响，具体应包括：安全控制间安全测评、层面间安全测评、区域间安全测评和系统结构安全测评等。因此，整个信息系统的等级测评内容构成可以用图 B.2 表示。

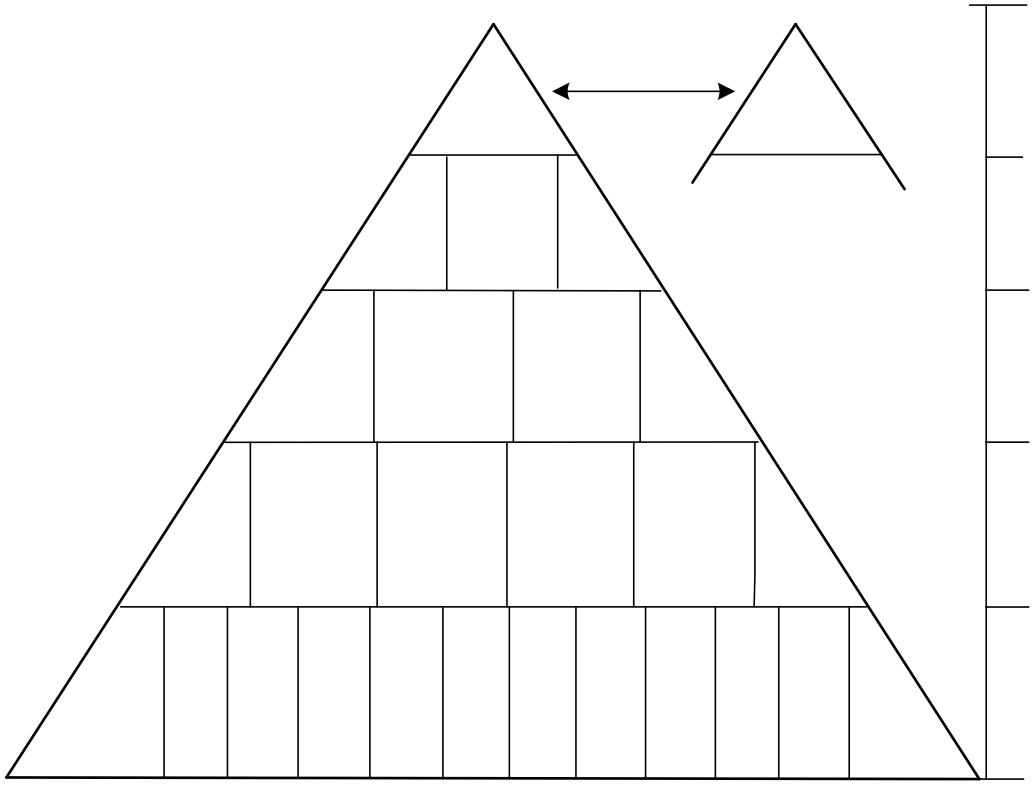

图 B.2 信息系统等级测评内容构成

B.3 系统整体测评举例说明

B.3.1 被测系统和环境概述

某单位被测系统主要由内部局域网的重点工程区、控制信息区、服务区和楼层接入区以及系统边界上的 DMZ 区组成。重点工程区和控制信息区位于屏蔽机房内，服务区和楼层接入区以及系统边界上的 DMZ 区位于中心机房内。与被测系统相连的外部连接包括 Internet、单位专网和国家局的卫星网、控制网、提供短信服务的移动公司、三产公司等。其中，与 Internet、单位专网和国家局的卫星网的连接边界处，设置了防火墙安全防护设备；与控制网连接是通过共用服务器方式进行的;与电信互联的短信服务器以双网卡的方式通过光纤直接到移动公司，移动公司再用无线方式外联；三产公司通过专线直接接入到楼层交换机上。整个网络拓扑结构示意图如图 B.3 所示。

系统结构

外部与 边界与

边界间 内部区域间

物理与 主机系统与 应
网络间 运维管理间 人员

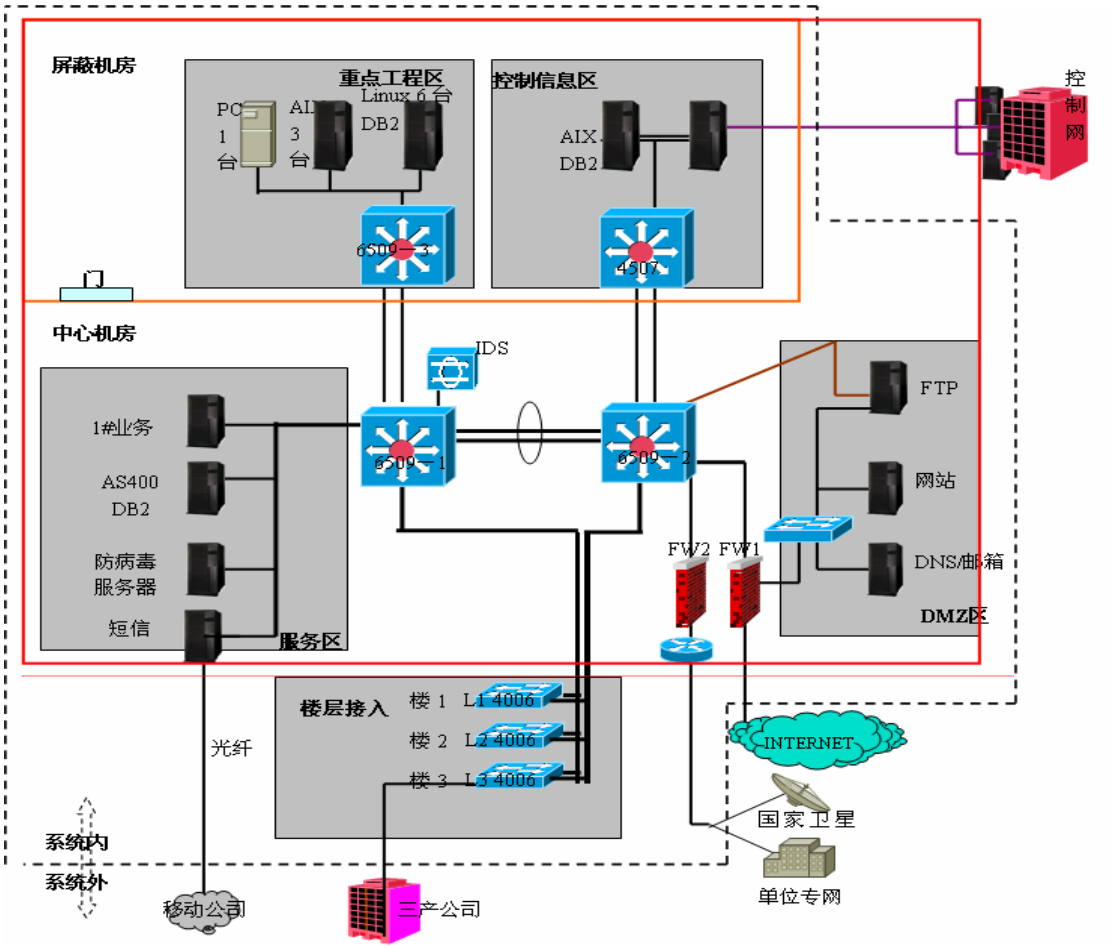

图 B.3 网络拓扑结构示意图

B.3.1 安全控制间安全测评举例

例子 1：物理访问控制与防盗窃安全功能增强（物理安全）

中心机房只有一个出入口，在物理访问控制上安排 24 小时专人值守中心机房的出入口。这显示有助于增强防盗窃安全控制的安全功能。通过专人值守可以能够及时发现并阻止设备被盗窃的现象。

例子 2：身份鉴别、自主访问控制中的安全功能消弱和增强（主机系统安全）

屏蔽机房重点工程区的 3 台 AIX 机器有两台机器 A 和 B 存在信任关系，AIX 机器 A 和 B 上各有一个帐户 a 和 b，建立了帐户的相互协同信任关系。在机器 A 上以帐户 a 登录，就可以毫无阻拦地使用任何以 r*开头的远程调用命令，在机器 B 上执行相当于帐户 b 的权限。测试发现机器 A 帐户 a 的身份鉴别存在薄弱口令，直接影响到机器 B 的安全。另一方面，对这种消弱作用，由于在机器 B 上加强了对帐户 b 的访问控制力度而得到某种程度的安全功能增强。综合判断身份鉴别和自主访问控制安全控制间存在削弱、增强作用，确定主机 A 的身份鉴别已降低到其安全功能不能达到信息系统相应等级的安全要求，可确定该安全控制已影响到信息系统的安全保护能力。

B.3.2 层面间安全测评举例

例子 1：物理安全与主机系统安全

由于加强了屏蔽机房的物理安全，采取限制进入屏蔽机房的人员，对进入机房的外来人员必须单位内部工作人员陪同，监视和限制其主机执行命令等措施，使得在物理上直接访问控制信息区的 AIX 主机变得安全可控。AIX 机器上的本地登录用户的身份鉴别和自主访问控制功能虽然没有满足相应安全等级要求，但考虑物理安全的加强可以增强主机系统这方

面安全功能。因此，可以适当降低强度身份鉴别和自主访问控制功能的要求，主机系统在总体的安全功能上也不会受到影响，仍能满足相应等级的安全要求。

例子 2：主机系统安全与系统运维管理

对屏蔽机房重点工程区的 PC 服务器，在系统运维管理中指定为专人运行维护，只有一个人可以使用该机器，主机系统上只有一个可以在本地登录的帐户。该机器在主机系统安全中的自主访问控制和资源控制虽然没有满足相应安全等级要求，但考虑到通过系统运维管理的加强可以增强主机系统这方面安全功能。因此，可以适当降低自主访问控制和资源控制的要求，主机系统在总体的安全功能上也不会受到影响，仍能满足相应等级的安全要求。

B.3.3 区域间安全测评举例

例子 1：中心机房和屏蔽机房之间

由于屏蔽机房是建设在中心机房内部的，它只有一个出入口，该出入口在中心机房内。因此，在中心机房的出入口上安排 24 小时专人值守等措施，可以解决屏蔽机房区域上的物理访问控制等相应措施的安全功能，使其达到该区域物理安全所要求的安全保护强度。

例子 2：DMZ 区与服务区之间

被测系统在全网部署了统一的网络防病毒服务器，该服务器位于中心机房服务区。在 DMZ 的 FTP 服务器上安装了网络防病毒的客户端。为了使 FTP 服务器上的防病毒客户端软件能够得到及时的、统一的升级服务和其他管理，在 FTP 服务器上安装了双网卡，一个网卡连接到 DMZ 区的交换机上，使用公网 IP 地址；另外一个网卡连接到核心交换机 6509 的服务区上，使用内部网络 IP 地址。DMZ 区上的防火墙 FW1 设置规则禁止任何从 DMZ 区主机上发起的，连接到内部网络服务区的行为，也就是，在网络访问控制上采取的是禁止措施。但是，由于 DMZ 区与服务区除了防火墙 FW1 这一网络通道外，还有 FTP 服务器（双网卡），防火墙 FW1 的访问控制规则被旁路，使得其网络访问控制失效。在实际测评中，可以通过利用 FTP 服务器漏洞，先侵入 FTP 服务器，取得管理控制权限，然后进一步利用其作为跳板，进一步攻击服务区上的机器，得以验证。因此，边界区域 DMZ 区与信息系统内部区域服务区之间存在安全功能的削弱作用，使网络访问控制的功能等级降低，其安全功能已不能满足信息系统安全等级的安全要求，可以确定该措施已影响到信息系统的整体安全保护能力。

B.3.4 系统结构安全测评举例

例子 1：信息系统整体结构的安全性

从被测系统的网络拓扑结构示意图来看，该网络系统有：Internet、单位专网和国家局的卫星网、控制网、提供短信服务的移动公司、三产公司等五处网络上相对独立的出口。在网络结构上，出口过多，不是很合理。可以合并一些出口，如合并移动公司和三产公司，连接到防火墙 FW2 上，使其通过 FW2 的访问控制来访问内部网络的服务区主机。

服务区上的短信服务器使用双网卡方式工作，在安全上是不可取的。如果从移动公司控制了该机器，则完全可以直接进入信息系统的内部网络区域，对信息系统的安全构成严重威胁。

对三产公司不经过访问控制而直接接入内部网络，在安全上是不可取的。这是两个不同信息系统之间的互联互通。这种互联互通如果没有经过严格的网络访问控制，就会直接使得被测系统的安全脆弱性经过网络直接暴露另外一个信息系统。三产公司不同于内部网络用户，其信息系统物理、网络、应用和管理等都不在被测单位的控制范围内。因此，这种连接方式对信息系统带来的威胁是相当大的，可以进一步通过网络测评等来验证。

例子 2：信息系统整体安全防范的合理性

从被测系统的网络拓扑结构示意图来看，虽然内部网络划分了多个区域，但是由于这些区域之间没有采取网络访问控制措施，不同用户通过核心交换机 6509-1 和 6509-2 等，访

问到内部网络的任何一台机器，包括屏蔽机房内的重点工程区和控制信息区上的服务器。这种保护方法不符合纵深防御的要求，没有更好地突出重点，从信息系统外渗透攻击内部网络，只有突破一层防线即全线崩溃。

在边界 DMZ 区上采取的保护手段较单一，也未起用防火墙 FW1 的 NAT 功能，而是在 DMZ 区上采用公网 IP 地址，都将使得整个保护防范能力降低，不满足信息系统业务的安全需要。

移动公司和三产公司的网络接入是信息系统外的接入。对这样的网络接入没有采取一些必要的安全防范手段，使得整个信息系统的安全防范暴露很大的安全问题。通过移动公司和三产公司可以很方便地侵入信息系统内部各区域的主机。信息系统的整体安全防范不是很合理。