YD

中华人民共和国通信行业标准

YD/T 1757-2008

电信网和互联网管理
安全等级保护检测要求

Classified Management Security Protection Testing Requirements for Telecom Network and Internet

2008-01-14 发布　　2008-01-14 实施

中华人民共和国信息产业部　发布

目　　次

前　言

本标准是“电信网和互联网安全防护体系”系列标准之一。该系列标准的结构及名称如下：

1. YD/T 1728-2008　电信网和互联网安全防护管理指南；
2. YD/T 1729-2008　电信网和互联网安全等级保护实施指南；
3. YD/T 1730-2008　电信网和互联网安全风险评估实施指南；
4. YD/T 1731-2008　电信网和互联网灾难备份及恢复实施指南；
5. YD/T 1732-2008　固定通信网安全防护要求；
6. YD/T 1733-2008　固定通信网安全防护检测要求；
7. YD/T 1734-2008　移动通信网安全防护要求；
8. YD/T 1735-2008　移动通信网安全防护检测要求；
9. YD/T 1736-2008　互联网安全防护要求；
10. YD/T 1737-2008　互联网安全防护检测要求；
11. YD/T 1738-2008　增值业务网——消息网安全防护要求；
12. YD/T 1739-2008　增值业务网——消息网安全防护检测要求；
13. YD/T 1740-2008　增值业务网——智能网安全防护要求；
14. YD/T 1741-2008　增值业务网——智能网安全防护检测要求；
15. YD/T 1742-2008　接入网安全防护要求；
16. YD/T 1743-2008　接入网安全防护检测要求；
17. YD/T 1744-2008　传送网安全防护要求；
18. YD/T 1745-2008　传送网安全防护检测要求；
19. YD/T 1746-2008　IP承载网安全防护要求；
20. YD/T 1747-2008　IP承载网安全防护检测要求；
21. YD/T 1748-2008　信令网安全防护要求；
22. YD/T 1749-2008　信令网安全防护检测要求；
23. YD/T 1750-2008　同步网安全防护要求；
24. YD/T 1751-2008　同步网安全防护检测要求；
25. YD/T 1752-2008　支撑网安全防护要求；
26. YD/T 1753-2008　支撑网安全防护检测要求；
27. YD/T 1754-2008　电信网和互联网物理环境安全等级保护要求；
28. YD/T 1755-2008　电信网和互联网物理环境安全等级保护检测要求；
29. YD/T 1756-2008　电信网和互联网管理安全等级保护要求；
30. YD/T 1757-2008　电信网和互联网管理安全等级保护检测要求；
31. YD/T 1758-2008　非核心生产单元安全防护要求；
32. YD/T 1759-2008　非核心生产单元安全防护检测要求。

本标准与YD/T 1756-2008《电信网和互联网管理安全等级保护要求》配套使用。

随着电信网和互联网的发展，将不断补充和完善电信网和互联网安全防护体系的相关标准。

本标准由中国通信标准化协会提出并归口。

本标准起草单位：信息产业部电信研究院、中国电信集团公司、中国移动通信集团公司、中国网络通信集团公司、中国联合通信有限公司、中国铁通集团有限公司

本标准主要起草人：李　成、魏　薇、杨剑峰、赵　阳、李友国、曾小辛、张　尼、冯　铭

电信网和互联网管理安全等级保护检测要求

1 范围

本标准规定了公众电信网和互联网的管理安全等级保护检测要求。

本标准适用于电信网和互联网安全防护体系中的各种网络和系统。

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。

3 术语和定义

下列术语和定义适用于本标准。

3.1

电信网 Telecom Network

利用有线和/或无线的电磁、光电网络，进行文字、声音、数据、图像或其他任何媒体的信息传递的网络，包括固定通信网、移动通信网等。

3.2

互联网 Internet

泛指由多个计算机网络相互连接而形成的网络，它是在功能和逻辑上组成的大型计算机网络。

3.3

安全等级 Security Classification

安全重要程度的表征。重要程度可从网络受到破坏后，对国家安全、社会秩序、经济运行、公共利益、网络和业务运营商造成的损害来衡量。

3.4

访谈 Interview

检测人员通过与有关人员（个人/群体）进行交流、讨论等活动，检查网络安全等级保护、网络安全风险评估和网络灾难备份及恢复相关措施的落实情况以及相关工作的开展情况的一种方法。

3.5

检查 Examination

检测人员通过对检测对象进行观察、查验和分析等活动，检查网络安全等级保护、网络安全风险评估和网络灾难备份及恢复相关措施的落实情况以及相关工作的开展情况的一种方法。

4 管理安全等级保护检测要求

4.1 第1级要求

不作要求。

4.2 第2级要求

4.2.1 安全管理制度

4.2.1.1 管理制度

4.2.1.1.1 检测方式

访谈、检查。

4.2.1.1.2 检测对象

总体方针、政策性文件和安全策略文件，安全管理制度，操作规程。

4.2.1.1.3 检测实施

a）检查网络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。

b）检查安全管理制度，查看文件是否明确安全管理活动中重要的管理内容。

c）检查是否有日常管理操作的操作规程，如网络维护手册和用户操作规程等，是否规定了管理人员或操作人员执行的重要管理操作。

4.2.1.2 制定和发布

4.2.1.2.1 检测方式

访谈、检查。

4.2.1.2.2 检测对象

安全管理制度、评审记录。

4.2.1.2.3 检测实施

a）访谈安全主管，是否指定或授权专门的部门或人员负责安全管理制度的制定；检查安全管理制度文档；

b）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评审，论证和评审方式如何（如召开评审会、函审、内部审核等）；检查管理制度评审记录，查看是否有相关人员的评审意见；

c）访谈安全主管，安全管理制度以何种方式发布，是否能正确地发布到相关人员手中。

4.2.1.3 评审和修订

4.2.1.3.1 检测方式

访谈、检查。

4.2.1.3.2 检测对象

安全管理制度列表、评审记录。

4.2.1.3.3 检测实施

访谈安全主管，询问是否定期对安全管理制度体系的合理性和适用性进行评审，评审周期多长；发现存在不足或需要改进时是否进行修订，检查是否有相关记录。

4.2.2 安全管理机构

4.2.2.1 岗位设置

4.2.2.1.1 检测方式

访谈、检查。

4.2.2.1.2 检测对象

安全主管、系统管理员、网络管理员、安全管理员、岗位职责文件。

4.2.2.1.3 检测实施

a）访谈相关负责人员，询问是否设立安全主管以及安全管理各个方面的负责人岗位，是否明确各个岗位的职责分工；

b）访谈安全主管，询问设置了哪些工作岗位，是否包含系统管理员、网络管理员和安全管理员等重要岗位，检查岗位职责文件，是否明确各个岗位的职责分工。

4.2.2.2 人员配备

4.2.2.2.1 检测方式

访谈、检查。

4.2.2.2.2 检测对象

人员配备要求管理文档，管理人员名单。

4.2.2.2.3 检测实施

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，包括系统管理员、网络管理员、安全管理员等重要岗位人员）配备情况，数量是否充足；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，是否包括系统管理员、网络管理员、安全管理员等重要岗位人员。

4.2.2.3 授权和审批

4.2.2.3.1 检测方式

访谈、检查。

4.2.2.3.2 检测对象

关键活动的批准人、授权管理文件、审批文档、审批记录。

4.2.2.3.3 检测实施

a）访谈安全主管，对系统投入运行、网络系统接入和重要资源的访问等关键活动是否有相应的审批部门及批准人；检查授权审批管理文件，查看文件是否明确审批事项、审批部门、审批人等。

b）访谈安全主管，询问针对关键活动是否建立审批流程，是否由批准人签字确认；检查关键活动的审批记录。

4.2.2.4 沟通和合作

4.2.2.4.1 检测方式

访谈、检查。

4.2.2.4.2 检测对象

会议文件，会议记录，外联单位说明文档。

4.2.2.4.3 检测实施

a）访谈安全主管，询问各类管理人员之间、组织内部机构之间以及网络安全职能部门内部的沟通、合作机制；访谈安全主管，询问是否召开过部门间协调会议，组织其他部门人员共同协助处理网络安全有关问题；检查部门间协调会议以及网络安全职能部门内部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。

b）访谈安全主管，询问是否经常与相关外部单位联系，联系方式有哪些；检查外联单位说明文档，查看外联单位是否包含相关外部单位，是否说明外联单位的联系人和联系方式等内容。

4.2.2.5 审核和检查

4.2.2.5.1 检测方式

访谈、检查。

4.2.2.5.2 检测对象

安全检查制度，安全检查报告，安全检查记录。

4.2.2.5.3 检测实施

访谈安全管理人员，询问是否组织人员定期对网络进行安全检查，检查周期多长，检查人员有哪些；安全检查包含哪些内容，是否包括用户账号情况、系统漏洞情况、数据备份情况等。

4.2.3 人员安全管理

4.2.3.1 人员录用

4.2.3.1.1 检测方式

访谈、检查。

4.2.3.1.2 检测对象

人员审查文档或记录、考核文档或记录、保密协议、审查记录。

4.2.3.1.3 检测实施

a）访谈人事负责人,是否指定或授权专门的部门或人员负责人员录用。

b）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、专业资格进行审查；检查是否具有人员录用时对被录用人身份、背景、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；是否对技术人员的技术技能进行考核，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。

c）访谈人事工作人员，询问是否与从事关键岗位的人员签署保密协议，查看保密协议。

4.2.3.2 人员离岗

4.2.3.2.1 检测方式

访谈、检查。

4.2.3.2.2 检测对象

人员离岗管理文档、人员离岗记录。

4.2.3.2.3 检测实施

a）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，是否要求及时终止离岗员工的所有访问权限。

b）访谈安全主管，询问人员离岗时是否取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备等。

c）访谈安全主管，询问人员离岗是否办理了严格的离岗手续，检查人员离岗记录。

4.2.3.3 人员考核

4.2.3.3.1 检测方式

访谈、检查。

4.2.3.3.2 检测对象

人员考核记录。

4.2.3.3.3 检测实施

访谈安全主管，询问是否定期对各个岗位人员进行安全技能及安全知识的考核；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。

4.2.3.4 安全意识教育和培训

4.2.3.4.1 检测方式

访谈、检查。

4.2.3.4.2 检测对象

安全教育计划、培训计划、培训记录。

4.2.3.4.3 检测实施

a）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意识教育、岗位技能培训和相关安全技术培训；检查是否具有安全教育和各类培训记录，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。

b）访谈安全主管，询问对违反违背安全策略和规定的人员是否有相应的惩戒措施；访谈各类人员，考查其对安全责任和惩戒措施等的理解程度。

c）访谈安全主管，是否制定了安全教育和培训计划，是否对网络安全基础知识、岗位操作规程等进行培训；检查安全教育和培训计划相关文档。

4.2.3.5 外部人员访问管理

4.2.3.5.1 检测方式

访谈、检查。

4.2.3.5.2 检测对象

外部人员访问授权或审批文档，外部人员访问记录。

4.2.3.5.3 检测实施

访谈安全管理人员，询问对外部人员访问受控区域（如访问主机房、重要服务器或设备、保密文档等）前是否得到授权或审批，批准后是否由专人全程陪同或监督，并登记备案；检查外部人员访问受控区域的授权或审批记录，查看记录是否描述了外部人员访问受控区域的进入时间、离开时间、访问区域、访问设备或信息及陪同人等信息。

4.2.4 安全建设管理

4.2.4.1 定级

4.2.4.1.1 检测方式

访谈、检查。

4.2.4.1.2 检测对象

网络定级文档。

4.2.4.1.3 检测实施

a）检查定级文档，查看是否明确网络边界和定级；

b）检查定级文档，查看是否明确描述网络边界划分的方法和确定安全保护等级的理由；

c）访谈安全主管，询问定级结果是否经相关部门批准。

4.2.4.1.4 安全方案设计

4.2.4.1.5 检测方式

访谈、检查。

4.2.4.1.6 检测对象

安全方案、安全详细设计方案、专家论证和审定文档、批准记录。

4.2.4.1.7 检测实施

a）访谈网络建设负责人，询问是否根据网络的安全等级保护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）检查网络安全方案文档，是否包括对网络的安全保护要求、策略和措施等内容。

c）检查网络详细设计方案文档，是否应对安全方案进行细化，形成能指导安全系统建设、安全产品采购和使用的具体设计方法。

d）访谈网络建设负责人，是否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，相关的安全方案在实施前是否经过批准后；检查专家论证和审定文档，检查安全方案实施的批准记录。

4.2.4.2 产品采购

4.2.4.2.1 检测方式

访谈、检查。

4.2.4.2.2 检测对象

安全产品、密码产品。

4.2.4.2.3 检测实施

a）访谈系统建设负责人，询问是否采用了安全产品，安全产品的采购和使用是否符合国家有关规定；

b）访谈系统建设负责人，询问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；

c）访谈系统建设负责人，询问是否有专门的部门负责产品的采购，由何部门负责。

4.2.4.3 自行软件开发

4.2.4.3.1 检测方法

访谈、检查。

4.2.4.3.2 检测对象

软件开发管理制度，软件设计文档，软件使用指南。

4.2.4.3.3 检测实施

a）访谈系统建设负责人，询问是否自行开发软件，开发环境与实际运行环境是否物理分开；

b）检查是否具备制定软件开发管理制度，查看其是否说明开发过程的控制方法和人员行为准则；

c）访谈系统建设负责人，询问是否提供软件设计的相关文档和使用指南，是否由专人负责保管；检查是否具有软件设计文档和软件使用指南。

4.2.4.4 外包软件开发

4.2.4.4.1 检测方法

访谈、检查。

4.2.4.4.2 检测对象

软件开发文档，软件使用指南。

4.2.4.4.3 检测实施

a）访谈网络建设负责人，询问软件交付前是否依据开发需求对软件功能和性能等进行验收检测；

b）访谈网络建设负责人，开发单位是否提供软件设计的相关文档和使用指南，检查软件设计的相关文档和使用指南；

c）访谈网络建设负责人，应在软件安装之前检测软件包中可能存在的恶意代码，查看检测记录。

4.2.4.5 工程实施

4.2.4.5.1 检测方法

访谈、检查。

4.2.4.5.2 检测对象

工程实施方案、工程实施管理制度。

4.2.4.5.3 检测实施

a）访谈网络建设负责人，是否指定或授权专门的部门或人员负责工程实施过程的管理。

b）访谈网络建设负责人，是否制定详细的工程实施方案控制工程实施过程；检查工程实施方案，查看其是否覆盖工程时间限制、进度控制和质量控制等方面内容。

4.2.4.6 测试验收

4.2.4.6.1 检测方法

访谈、检查。

4.2.4.6.2 检测对象

测试验收方案、测试验收结果记录、测试验收报告。

4.2.4.6.3 检测实施

a）访谈系统建设负责人，询问在系统正式运行前，是否根据设计方案或合同要求对系统进行独立的安全性测试；检查网络测试验收报告。

b）访谈网络建设负责人，在测试验收前是否根据设计方案或合同要求等制订测试验收方案，在测试验收过程中是否详细记录测试验收结果，并形成测试验收报告；检查测试验收方案、测试验收结果记录和测试验收报告。

c）访谈网络建设负责人，是否组织相关部门和相关人员对网络测试验收报告进行审定，并签字确认；检查网络测试验收报告。

4.2.4.7 交付

4.2.4.7.1 检测方法

访谈、检查。

4.2.4.7.2 检测对象

交付清单，培训记录。

4.2.4.7.3 检测实施

a）访谈网络建设负责人，询问交接手续是什么，是否有交付清单，是否根据交付清单对所交接的设备、文档、软件等进行清点。

b）访谈网络建设负责人，询问目前的运维技术人员是否进行过技能培训，检查培训记录。

c）检查网络交付清单，查看其是否具有网络建设文档（如网络建设方案）、指导用户进行网络运维的文档（如服务器操作规程书）等文档名称。

4.2.4.8 安全服务商的选择

4.2.4.8.1 检测方式

访谈、检查。

4.2.4.8.2 检测对象

安全服务器、安全相关协议、安全服务合同。

4.2.4.8.3 检测实施

a）访谈安全主管，是否使用安全服务商提供的安全服务器，是否按国家有关规定选择安全服务商；

b）检查与安全服务商签订的安全相关协议查看，查看其中是否明确约定相关责任；

c）访谈安全主管，是否要求安全服务商提供技术支持和服务承诺，是否与其签订服务合同。

4.2.4.9 备案

4.2.4.9.1 检测方式

访谈、检查。

4.2.4.9.2 检测对象

备案相关记录。

4.2.4.9.3 检测实施

访谈安全主管，询问是否有专门的人员或部门负责管理网络定级、属性等文档，由何部门/何人负责；访谈文档管理员，询问对网络定级、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）；检查是否具有网络定级、属性等相关材料的使用控制记录。

4.2.5 安全运维制度

4.2.5.1 环境管理

4.2.5.1.1 检测方式

访谈、检查。

4.2.5.1.2 检测对象

维护文档、机房出入记录、服务器开关机记录。

4.2.5.1.3 检测实施

a）访谈系统管理员，询问是否应指定专门的部门或人员定期对机房供配电、空调、温湿度控制等设施进行维护管理；检查维护管理文档。

b）访谈系统管理员，询问是否配备机房安全管理人员，是否对机房的出入、服务器的开机或关机等工作进行管理；检查机房出入记录、服务器开关机记录。

c）访谈系统管理员，询问是否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；检查机房安全管理制度文档。

d）访谈安全管理人员，询问是否加强对办公环境的保密性管理，工作人员调离办公室是否立即交还

该办公室钥匙，是否不在办公区接待来访人员等。

4.2.5.2 资产管理

4.2.5.2.1 检测方式

访谈、检查。

4.2.5.2.2 检测对象

资产清单、资产安全管理制度文档。

4.2.5.2.3 检测实施

a）访谈资产管理员，是否编制与网络相关的资产清单；检查资产清单，是否包括资产责任部门、重要程度和所处位置等内容。

b）访谈资产管理员，是否建立资产安全管理制度；检查资产安全管理制度文档，是否规定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。

4.2.5.3 介质管理

4.2.5.3.1 检测方式

访谈、检查。

4.2.5.3.2 检测对象

介质管理记录、介质安全管理制度、各类介质。

4.2.5.3.3 检测实施

a）访谈资产管理员，询问介质是否存放在安全的环境中，是否对各类介质进行控制和保护，并实行存储环境专人管理，查看介质存放地点，是否按照符合相关要求。

b）访谈资产管理员，询问是否对介质归档和查询等过程进行记录，并根据存档介质的目录清单定期盘点；检查介质管理记录，查看其是否记录介质的归档、查询等情况。

c）访谈资产管理员，询问是否对需要送出维修或销毁的介质，清除其中的敏感数据。

d）访谈资产管理员，询问是否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；检查介质，查看是否对其进行了分类，并具有不同标识。

4.2.5.4 设备管理

4.2.5.4.1 检测方式

访谈、检查。

4.2.5.4.2 检测对象

设备维护文档、线路维护文档、设备审批管理文档、设备操作规程、审批记录。

4.2.5.4.3 检测实施

a）访谈资产管理员，询问网络相关的各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理，由何部门/何人维护，维护周期多长；检查设备、线路维护文档。

b）访谈资产管理员，询问是否应建立基于申报、审批和专人负责的设备安全管理制度，是否对设备选用的各个环节（选型、采购、发放、领用等）进行规范化管理；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、发放和领用等环节的申报和审批作出规定。

c）访谈系统管理员，询问是否对终端计算机、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，按操作规程实现关键设备（包括备份和冗余设备）的启动/停止、加电/断电等操作；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。

d）应访谈系统管理员，询问信息处理设备是否经过审批才能带离机房或办公地点；检查相关审批记录。

4.2.5.5 网络安全管理

4.2.5.5.1 检测方法

访谈、检查。

4.2.5.5.2 检测对象

网络安全管理制度文档、软件版本升级记录、重要文件备份记录、网络漏洞扫描报告、配置文件备份记录。

4.2.5.5.3 检测实施

a）访谈安全主管，询问是否指定人员负责网络运行日志、网络监控记录的日常维护和报警信息分析和处理工作。

b）访谈安全管理人员，询问是否建立网络安全管理制度，检查网络安全管理制度文档，查看其是否包含网络安全配置、日志保存时间、安全策略、升级与打补丁、口令更新周期等方面的规定。

c）访谈安全管理人员，询问是否根据厂家提供的软件升级版本对网络设备进行更新，并在更新前对现有的重要文件进行备份；检查软件版本升级记录、软件升级时的重要文件备份记录。

d）访谈安全管理人员，询问是否定期对网络系统进行漏洞扫描，对发现的网络系统安全漏洞是否进行及时的修补；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。

e）访谈安全管理人员，询问是否对网络设备的配置文件进行定期备份；检查配置文件备份记录。

4.2.5.6 系统安全管理

4.2.5.6.1 检测方法

访谈、检查。

4.2.5.6.2 检测对象

系统的访问控制策略文档、系统漏洞扫描报告、系统安全管理制度、系统操作日志、运行日志，审计记录。

4.2.5.6.3 检测实施

a）访谈系统管理员，询问是否根据业务需求和系统安全分析确定系统的访问控制策略。

b）访谈系统管理员，询问是否定期进行漏洞扫描，对发现的系统安全漏洞及时进行修补；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。

c）访谈系统管理员，询问是否安装系统的最新补丁程序，在安装系统补丁前，是否在测试环境中测试通过，并对重要文件进行备份后，方实施系统补丁程序的安装。

d）访谈系统管理员，询问是否建立系统安全管理制度；检查系统安全管理制度文档，查看其是否对系统安全策略、安全配置、日志管理和日常操作流程等方面作出规定。

e）访谈系统管理员，询问是否依据操作手册对系统进行维护；检查系统操作日志，是否包括重要的日常操作、运行维护记录、参数的设置和修改等内容，是否能够杜绝未经授权的操作。

f）访谈系统管理员，询问是否应定期对运行日志和审计数据进行分析，以便及时发现异常行为；检

查运行日志和审计记录。

4.2.5.7 恶意代码、病毒防范管理

4.2.5.7.1 检测方法

访谈、检查。

4.2.5.7.2 检测对象

恶意代码、病毒防范管理制度、病毒检测记录、病毒库升级记录。

4.2.5.7.3 检测实施

a）访谈网络运维负责人，询问是否对员工进行基本恶意代码、病毒防范意识教育，如告知应及时升级防病毒软件，在读取移动存储设备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应进行病毒检查。

b）访谈网络运维负责人，询问是否指定专人对恶意代码、病毒进行检测，并保存记录；检查是否具有恶意代码检测记录。

c）检查恶意代码、病毒防范管理制度，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。

4.2.5.8 密码管理

4.2.5.8.1 检测方法

访谈、检查。

4.2.5.8.2 检测对象

密码技术和产品。

4.2.5.8.3 检测实施

访谈安全主管，如采用了密码技术和产品，是否符合国家密码管理规定。

4.2.5.9 变更管理

4.2.5.9.1 检测方法

访谈、检查。

4.2.5.9.2 检测对象

变更方案、变更申请书、变更管理制度。

4.2.5.9.3 检测实施

a）访谈网络运维负责人，询问是否制定变更方案指导网络执行变更；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。

b）访谈网络运维负责人，询问重要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；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；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。

4.2.5.10 备份与恢复管理

4.2.5.10.1 检测方法

访谈、检查。

4.2.5.10.2 检测对象

备份管理文档、备份和恢复策略文档。

4.2.5.10.3 检测实施

a）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重要业务信息、系统数据及软件系统；

b）检查备份管理文档，是否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；

c）检查数据的备份策略和恢复策略文档，是否考虑了数据的重要性和数据对系统运行的影响，是否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。

4.2.5.11 安全事件处置

4.2.5.11.1 检测方法

访谈、检查。

4.2.5.11.2 检测对象

安全事件报告和处置管理制度、安全事件定级文档、安全事件报告和处理程序文档。

4.2.5.11.3 检测实施

a）访谈系统管理人员、网络管理人员、安全管理人员，询问是否被告知在发现安全脆弱性和可疑事件时应及时报告，是否曾经尝试验证脆弱性。

b）访谈安全管理人员，询问是否制定安全事件报告和处置管理制度；检查安全事件报告和处置管理制度，是否明确安全事件类型，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）访谈安全管理人员，询问是否对根据安全事件对本网络产生的影响，对本网络安全事件进行等级划分；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。

d）访谈安全管理人员，询问是否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；检查安全事件报告和处理程序文档。

4.2.5.12 应急预案管理

4.2.5.12.1 检测方法

访谈、检查。

4.2.5.12.2 检测对象

应急预案、应急预案培训记录。

4.2.5.12.3 检测实施

a）访谈网络运维负责人，询问是否制定不同事件的应急预案；检查应急预案。

b）访谈网络运维负责人，询问是否对网络相关人员进行应急预案培训，应急预案培训是否至少一年一次；检查应急预案培训记录。

4.3 第3.1级要求

4.3.1 安全管理制度

4.3.1.1 管理制度

除按照4.2.1.1的要求进行检测外，还应按照本节内容进行检测。

4.3.1.1.1 检测方式

访谈、检查。

4.3.1.1.2 检测对象

安全管理制度文档。

4.3.1.1.3 检测实施

a）访谈安全主管，询问是否应对安全管理活动中的各类管理内容建立安全管理制度；检查安全管理制度，是否覆盖各类安全管理活动。

b）应谈安全主管，询问是否形成由安全策略、管理制度、操作规程等构成的全面的安全管理制度体系。检查安全管理制度相关文档是否由安全策略、管理制度、操作规程等构成。

4.3.1.2 制定和发布

除按照4.2.1.2的要求进行检测外，还应按照本节内容进行检测。

4.3.1.2.1 检测方式

访谈、检查。

4.3.1.2.2 检测对象

制度制定和发布要求管理文档、安全管理制度、收发登记记录。

4.3.1.2.3 检测实施

a）访谈安全主管，询问安全管理制度是否按照统一的格式标准或要求制定；应检查安全管理制度文档，查看各项制度文档格式是否统一，是否有版本标识。

b）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是否通过正式、有效的方式发布。

c）检查安全管理制度文档，查看是否注明发布范围；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。

4.3.1.3 评审和修订

除按照4.2.1.3的要求进行检测外，还应按照本节内容进行检测。

4.3.1.3.1 检测方式

访谈、检查。

4.3.1.3.2 检测对象

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。

4.3.1.3.3 检测实施

a）访谈安全主管，询问安全小组是否定期对安全管理制度体系的合理性和适用性进行评审，评审周期多长。

b）访谈安全主管，询问是否定期或不定期地对安全管理制度进行评审，由何部门/何人负责；访谈负责定期评审的人员，询问定期对安全管理制度的评审、修订情况，评审周期多长，评审、修订程序如何；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。

4.3.2 安全管理机构

4.3.2.1 岗位设置

除按照4.2.2.1的要求进行检测外，还应按照本节内容进行检测。

4.3.2.1.1 检测方式

访谈、检查。

4.3.2.1.2 检测对象

安全管理制度文档。

4.3.2.1.3 检测实施

a）访谈安全主管，询问是否设立了安全管理工作的职能部门。

b）访谈安全主管，询问是否应成立指导和管理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。

c）检查安全管理制度文档，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。

4.3.2.2 人员配备

除按照4.2.2.2的要求进行检测外，还应按照本节内容进行检测。

4.3.2.2.1 检测方式

访谈、检查。

4.3.2.2.2 检测对象

安全管理人员名单。

4.3.2.2.3 检测实施

a）访谈安全主管，询问是否配备专职的安全管理员；检查安全管理人员名单，确认安全管理人员是否是专职人员。

b）访谈安全主管，询问关键事务岗位是否配备多人共同管理；检查安全管理人员名单和职责列表，确认关键事务岗位是否由多人共同管理。

4.3.2.3 授权和审批

除按照4.2.2.3的要求进行检测外，还应按照本节内容进行检测。

4.3.2.3.1 检测方式

访谈、检查。

4.3.2.3.2 检测对象

授权审批管理文件、授权文档、审批文档、审批记录。

4.3.2.3.3 检测实施

a）访谈关键活动的批准人，询问是否根据各个部门和岗位的职责明确授权审批事项。

b）访谈安全主管，询问是否针对系统变更、重要操作、物理访问和系统接入等事项建立审批程序，按照审批程序执行审批过程，对重要活动建立逐级审批制度；应检查授权审批管理文件，查看文件是否明确审批程序。

c）访谈安全主管，询问是否定期审查审批事项，审查周期多长，是否及时更新需授权和审批的项目、审批部门和审批人等信息；检查授权审批管理文件，查看文件是否说明定期审查审批的事项、及时更新需审批的项目、审查周期等内容；检查审批记录，查看记录日期是否与审查周期一致。

d）访谈安全主管，询问是否记录审批过程并保存审批文档；检查是否有记录项目授权审批过程的文档。

4.3.2.4 沟通和合作

除按照4.2.2.4的要求进行检测外，还应按照本节内容进行检测。

4.3.2.4.1 检测方式

访谈、检查。

4.3.2.4.2 检测对象

会议记录文件、外联单位说明文档、安全顾问名单。

4.3.2.4.3 检测实施

a）访谈安全主管，询各类管理人员之间、组织内部机构之间以及网络安全职能部门内部是否定期或不定期召开协调会议，共同协作处理网络安全问题；检查会议记录文件，查看是否有会议内容、会议时间、参加人员和结果等的描述。

b）访谈安全主管，询问是否建立与相关外部单位的沟通、合作，与外联单位有哪些合作内容，沟通、合作方式有哪些；应检查外联单位说明文档，是否说明外联单位的联系人、联系方式、合作内容等。

c）访谈安全主管，询问是否聘请网络安全专家作为常年的安全顾问，指导网络安全建设，参与安全规划和安全评审等；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网络安全建设、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。

4.3.2.5 审核和检查

除按照4.2.2.5的要求进行检测外，还应按照本节内容进行检测。

4.3.2.5.1 检测方式

访谈、检查。

4.3.2.5.2 检测对象

安全检查制度、安全检查报告、安全检查过程记录。

4.3.2.5.3 检测实施

a）访谈安全主管，询问是否由内部人员或上级单位定期进行全面安全检查；检查安全检查制度文档，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。

b）访谈安全管理人员，询问是否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；检查是否有安全检查报告，报告中是否有检查数据汇总表等的描述。

c）检查安全审核和安全检查制度文档，查看文档是否规定安全审核和安全检查的内容、程序和周期等；应检查安全审核和安全检查过程记录，查看报告日期与检查周期是否一致，查看记录的检查程序与文件要求是否一致。

4.3.3 人员安全管理

4.3.3.1 人员录用

除按照4.2.3.1的要求进行检测外，还应按照本节内容进行检测。

4.3.3.1.1 检测方式

访谈、检查。

4.3.3.1.2 检测对象

人员录用要求管理文档、人员审查文档或记录、保密协议、岗位安全协议。

4.3.3.1.3 检测实施

a）访谈人事负责人，询问在人员录用时是否对被录用人资质进行审查；检查人员录用要求管理文档，查看是否要求对被录用人资质进行审查；检查是否有人员资质审查文档或记录。

b）访谈人事负责人，询问是否要求被录用人签订保密协议；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。

c）访谈人事负责人，询问是否从内部人员中选拔从事关键岗位的人员，并签署岗位安全协议；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。

4.3.3.2 人员离岗

除按照4.2.3.2的要求进行检测外，还应按照本节内容进行检测。

4.3.3.2.1 检测方式

访谈、检查。

4.3.3.2.2 检测对象

人员离岗管理文档、保密承诺文档。

4.3.3.2.3 检测实施

访谈人事工作人员，询问关键岗位人员离岗是否须承诺调离后的保密义务后方可离开；检查人员离岗管理文档，是否要求离岗人员承诺保密义务；应检查保密承诺文档，查看是否有调离人员的签字。

4.3.3.3 人员考核

除按照4.2.3.3的要求进行检测外，还应按照本节内容进行检测。

4.3.3.3.1 检测方式

访谈、检查。

4.3.3.3.2 检测对象

人员考核记录。

4.3.3.3.3 检测实施

a）访谈人事工作人员，询问是否对关键岗位的人员进行全面、严格的安全审查和技能考核；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。

b）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。

4.3.3.4 安全意识教育和培训

除按照4.2.3.4的要求进行检测外，还应按照本节内容进行检测。

4.3.3.4.1 检测方式

访谈、检查。

4.3.3.4.2 检测对象

技术人员、管理人员、安全管理制度、安全教育培训计划、安全教育培训记录。

4.3.3.4.3 检测实施

a）访谈各类技术人员和管理人员，考查其对工作相关的网络安全基础知识、安全责任和惩戒措施等的理解程度，被访谈人员对询问内容的表述是否清楚，是否与文件描述一致；检查安全管理制度，查看是否规定了安全责任和惩戒措施。

b）访谈安全管理人员，是否针对不同岗位制定不同的培训计划；检查安全教育培训计划，查看其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，培训内容是否包含网络安全基础知识、岗位操作规程等。

c）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。

4.3.3.5 外部人员访问管理

除按照4.2.3.5的要求进行检测外，还应按照本节内容进行检测。

4.3.3.5.1 检测方式

访谈、检查。

4.3.3.5.2 检测对象

外部人员访问管理文档、外部人员访问批准文档、外部人员访问登记记录。

4.3.3.5.3 检测实施

a）访谈安全主管，询问对外部人员（如向网络提供服务的软、硬件维护人员，业务合作伙伴、评估人员等）访问受控区域前是否需提出书面申请；检查外部人员访问受控区域批准文档，查看是否有外部人员访问受控区域的书面申请，是否有批准人允许访问的批准签字等。

b）检查外部人员访问管理文档，查看是否明确外部人员包括哪些人员，允许外部人员访问的范围（区域、系统、设备、信息等内容），外部人员进入条件（对哪些受控区域的访问须提出书面申请批准后方可进入），外部人员进入的访问控制（由专人全程陪同或监督等）和外部人员的离开条件等；检查外部人员访问受控区域的登记记录，查看记录是否描述了外部人员访问重要区域的进入时间、离开时间、访问区域、访问设备或信息及陪同人等信息。

4.3.4 安全建设管理

4.3.4.1 定级

除按照4.2.4.1的要求进行检测外，还应按照本节内容进行检测。

4.3.4.1.1 检测方式

访谈、检查。

4.3.4.1.2 检测对象

网络定级文档、专家论证文档。

4.3.4.1.3 检测实施

a）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网络定级结果进行论证和审定。

b）检查网络定级文档，查看定级结果是否分级上报至全国或地区的主管部门，是否获得了上级主管部门的批准。

4.3.4.2 安全方案设计

除按照4.2.4.2的要求进行检测外，还应按照本节内容进行检测。

4.3.4.2.1 检测方式

访谈、检查。

4.3.4.2.2 检测对象

安全建设工作计划、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，

相关文档维护记录。

4.3.4.2.3 检测实施

a）访谈安全主管或网络建设负责人，询问是否指定和授权专门的部门对网络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；检查网络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。

b）访谈网络建设负责人，询问是否根据网络的等级划分情况，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。

c）访谈网络建设负责人，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、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，并且经过批准后才正式实施；检查网络总体安全策略、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。

d）访谈网络建设负责人，询问是根据等级测评、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；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。

4.3.4.3 产品采购

除按照4.2.4.3的要求进行检测外，还应按照本节内容进行检测。

4.3.4.3.1 检测方式

访谈、检查。

4.3.4.3.2 检测对象

产品采购管理制度、产品选型测试结果记录、候选产品名单、候选产品名单审定记录。

4.3.4.3.3 检测实施

访谈网络建设负责人，询问网络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，是否定期审定和更新候选产品名单，审定周期多长；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。

4.3.4.4 自行软件开发

除按照4.2.4.4的要求进行检测外，还应按照本节内容进行检测。

4.3.4.4.1 检测方式

访谈、检查。

4.3.4.4.2 检测对象

代码编写安全规范、程序资源库修改、更新和发布的记录及审批文档。

4.3.4.4.3 检测实施

a）访谈网络建设负责人，询问开发人员和测试人员是否分离，测试数据和测试结果是否受到控制。

b）检查是否具备代码编写安全规范，开发人员是否参照规范编写代码。

c）访谈网络建设负责人，询问是否对程序资源库的修改、更新、发布进行授权和批准；查看是否具备程序资源库修改、更新和发布的记录及审批文档。

4.3.4.5 外包软件开发

与 4.2.4.5 的检测内容相同。

4.3.4.6 工程实施

除按照4.2.4.6的要求进行检测外，还应按照本节内容进行检测。

4.3.4.6.1 检测方法

访谈、检查。

4.3.4.6.2 检测对象

工程实施方案、工程实施管理制度。

4.3.4.6.3 检测实施

a）访谈网络建设负责人，询问工程实施单位能正确地执行安全工程过程。

b）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。

4.3.4.7 测试验收

除按照4.2.4.7的要求进行检测外，还应按照本节内容进行检测。

4.3.4.7.1 检测方法

访谈、检查。

4.3.4.7.2 检测对象

网络安全性测试报告、验收测试管理制度、验收报告。

4.3.4.7.3 检测实施

a）访谈网络建设负责人，询问在网络正式运行前，是否委托第三方测试机构对网络进行独立的安全性测试；检查是否具有网络安全性测试报告。

b）检查验收测试管理制度，查看是否包含网络测试验收的控制方法和人员行为准则。

c）访谈网络建设负责人，询问是否指定或授权专门的部门负责测试验收的管理，是否按照管理规定的要求完成测试验收工作。检查是否具有验收报告。

4.3.4.8 交付

除按照4.2.4.8的要求进行检测外，还应按照本节内容进行检测。

4.3.4.8.1 检测方法

访谈、检查。

4.3.4.8.2 检测对象

网络交付管理制度、试运行报告、应急预防方案/措施。

4.3.4.8.3 检测实施

a）检查网络交付管理制度，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行为准则等方面内容。

b）访谈网络建设负责人，询问是否指定或授权专门的部门负责网络交付的管理工作，并按照管理规定的要求完成交付工作。

c）访谈网络建设负责人，询问在正式投入使用前，是否根据实际情况进行了试运行，试运行期间是否制定相关应急预防措施；检查是否制定了相关文档，是否具有试运行报告、应急预防方案/措施。

d）访谈网络建设负责人，并通过实际操作检查在正式投入使用后，是否对建设、开发过程中涉及安

全要求的配置、口令等内容重新修改、设定。

4.3.4.9 安全服务商的选择

与4.2.4.9的检测内容相同。

4.3.4.10 备案

除按照4.2.4.10的要求进行检测外，还应按照本节内容进行检测。

4.3.4.10.1 检测方式

访谈、检查。

4.3.4.10.2 检测对象

备案记录。

4.3.4.10.3 检测实施

访谈安全主管，询问是否将网络定级、属性、定级理由等材料分级上报至全国或地区主管部门；检查备案记录或备案文档。

4.3.4.11 等级测评

4.3.4.11.1 检测方式

访谈、检查。

4.3.4.11.2 检测对象

等级评测记录、整改记录、测评单位资质证明。

4.3.4.11.3 检测实施

a）访谈安全主管，询问在网络运行过程中，是否至少每年对网络进行一次等级测评，发现不符合相应等级保护标准要求的是否及时整改；检查是否具备等级评测记录、整改记录。

b）访谈安全主管，询问是否在网络发生变更时及时对网络进行等级测评，发现级别发生变化的是否及时调整级别并进行安全改造，发现不符合相应等级保护标准要求的是否及时整改；检查网络等级评测记录，是否能反映网络发生的变更、级别的变化；检查整改记录。

c）访谈安全主管，询问是否选择具有国家相关技术资质和安全资质的测评单位进行等级测评；检查测评单位的资质证明。

d）访谈安全主管，询问是否指定或授权专门的部门或人员负责等级测评的管理。

4.3.5 安全运维管理

4.3.5.1 环境管理

除按照4.2.5.1的要求进行检测外，还应按照本节内容进行检测。

4.3.5.1.1 检测方式

访谈、检查。

4.3.5.1.2 检测对象

机房安全管理制度、办公环境管理文档、机房进出登记表、机房电子门禁系统及其电子记录。

4.3.5.1.3 检测实施

a）访谈安全主管，是否有指定的部门负责机房安全，机房是否配置电子门禁系统，是否机房来访人员实行登记记录和电子记录双重备案管理；检查机房安全管理制度是否指定专门的部门负责机房安全；检查是否具备机房来访人员登记记录和电子记录。

b）检查办公环境管理文档，是否要求工作人员离开座位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。

4.3.5.2 资产管理

除按照4.2.5.2的要求进行检测外，还应按照本节内容进行检测。

4.3.5.2.1 检测方式

访谈、检查。

4.3.5.2.2 检测对象

资产、资产清单、资产标识、资产安全管理制度。

4.3.5.2.3 检测实施

a）访谈资产管理员，询问是否依据资产的重要程度对资产进行分类和标识管理；检查是否根据资产的价值是否采取相应的管理措施；应检查资产清单中的资产，查看其是否具有相应标识，资产标识是否与资产分类标识文档中所要求的一致。

b）访谈安全主管，询问是否对信息分类与标识方法作出规定，并对信息的使用、传输和存储等进行规范化管理。检查资产安全管理制度，查看其内容是否按信息分类与标识的原则和方法对信息资产的使用、传输和存储作出规定。

4.3.5.3 介质管理

除按照4.2.5.3的要求进行检测外，还应按照本节内容进行检测。

4.3.5.3.1 检测方式

访谈、检查。

4.3.5.3.2 检测对象

介质管理记录、介质安全管理制度、各类介质以及介质存放地。

4.3.5.3.3 检测实施

a）检查是否具备介质安全管理制度，查看是否对介质的存放环境、使用、维护和销毁等方面作出规定。

b）检查是否具备介质安全管理制度，查看是否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应。

c）访谈资产管理员，询问是否对存储介质的使用过程进行严格的管理，是否对带出工作环境的存储介质进行内容加密和监控管理，对保密性较高的存储介质未经批准是否从未自行销毁。

d）访谈资产管理员，询问是否根据数据备份的需要对某些介质实行异地存储，检查存储地的环境要求和管理方法是否与本地相同。

访谈资产管理员，询问是否对重要介质中的数据和软件采取加密存储。

4.3.5.4 设备管理

除按照4.2.5.4的要求进行检测外，还应按照本节内容进行检测。

4.3.5.4.1 检测方式

访谈、检查。

4.3.5.4.2 检测对象

设施、软硬件维护管理制度。

4.3.5.4.3 检测实施

访谈系统管理员，询问是否建立配套设施、软硬件维护方面的管理制度，是否对其维护进行有效的管理；检查设备维护管理制度，查看是否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。

4.3.5.5 监控管理

4.3.5.5.1 检测方式

访谈、检查。

4.3.5.5.2 检测对象

监控记录、安全事件分析报告、安全管理记录。

4.3.5.5.3 检测实施

a）访谈网络运维负责人，询问是否对通信线路、主机、网络设备和应用软件的运行状况、网络流量、用户行为等进行监测和报警，形成记录并妥善保存；检查是否具备监控记录。

b）访谈网络运维负责人，询问是否组织相关人员定期对监测和报警记录进行分析、评审，发现可疑行为，形成分析报告，并采取必要的应对措施；检查是否具备安全事件分析报告。

c）访谈网络运维负责人，是否建立安全管理中心，对设备状态、恶意代码、补丁升级、安全审计等安全相关事项进行集中管理；检查是否具备安全管理记录。

4.3.5.6 网络安全管理

除按照4.2.5.5的要求进行检测外，还应按照本节内容进行检测。

4.3.5.6.1 检测方式

访谈、检查。

4.3.5.6.2 检测对象

离线备份记录、安全检查记录。

4.3.5.6.3 检测实施

a）访谈网络运维负责人，询问是否实现设备的最小服务配置，并对配置文件进行定期离线备份；检查是否具备离线备份记录，备份周期是否与要求一致。

b）访谈网络运维负责人，询问是否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。

c）访谈网络运维负责人，询问是否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；检查是否具备相应的安全检查记录。

4.3.5.7 系统安全管理

除按照4.2.5.6的要求进行检测外，还应按照本节内容进行检测。

4.3.5.7.1 检测方法

访谈、检查。

4.3.5.7.2 检测对象

网络安全管理制度。

4.3.5.7.3 检测实施

访谈安全主管、安全员，询问是否指定专人对系统进行管理；检查网络安全管理制度文档，查看是否划分系统管理员角色，明确各个角色的权限、责任和风险，权限设定应当遵循最小授权原则。

4.3.5.8 恶意代码、病毒防范管理

除按照4.2.5.7的要求进行检测外，还应按照本节内容进行检测。

4.3.5.8.1 检测方法

访谈、检查。

4.3.5.8.2 检测对象

恶意代码、病毒库升级记录，恶意代码、病毒分析报告。

4.3.5.8.3 检测实施

访谈安全员，询问是否定期检查网络内各种产品的恶意代码库的升级情况并进行记录，是否主机防病毒产品、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；检查是否具备恶意代码库升级记录，病毒或恶意代码分析报告。

4.3.5.9 密码管理

除按照4.2.5.8的要求进行检测外，还应按照本节内容进行检测。

4.3.5.9.1 检测方法

访谈、检查。

4.3.5.9.2 检测对象

密码使用管理制度。

4.3.5.9.3 检测实施

检查是否具备密码使用管理制度。

4.3.5.10 变更管理

除按照4.2.5.9的要求进行检测外，还应按照本节内容进行检测。

4.3.5.10.1 检测方法

访谈、检查。

4.3.5.10.2 检测对象

变更方案、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、变更恢复演练记录。

4.3.5.10.3 检测实施

a）访谈网络运维负责人，询问是否具有建立变更管理制度，变更和变更方案是否有评审过程；检查是否具备变革管理制度；检查是否具备变更和变更方案的评审记录。

b）访谈网络运维负责人，询问是否具有变更控制的申报和审批文件化程序，是否对变更影响进行分析并文档化；检查是否具备变更控制的申报和审批文件，检查变更记录，是否记录变更实施过程。

c）检查是否具备中止变更并从失败变更中恢复的程序文档，是否明确过程控制方法和人员职责。访谈网络运维负责人，询问是否对恢复过程进行演练，检查是否变更恢复演练记录。

4.3.5.11 备份与恢复管理

除按照4.2.5.10的要求进行检测外，还应按照本节内容进行检测。

4.3.5.11.1 检测方法

访谈、检查。

4.3.5.11.2 检测对象

备份和恢复策略文档、备份和恢复记录文档、介质有效性测试记录。

4.3.5.11.3 检测实施

a）访谈系统管理员，询问是否具有备份与恢复管理相关的安全管理制度；检查是否具有备份与恢复策略文档。

b）访谈系统管理员，询问是否具有控制数据备份和恢复过程的程序，是否对备份过程进行记录；检查是否具有数据备份和恢复记录。

c）访谈系统管理员，询问是否定期执行恢复程序，检查和测试备份介质的有效性；检查是否具有介质有效性测试记录。

4.3.5.12 安全事件处置

除按照4.2.5.11的要求进行检测外，还应按照本节内容进行检测。

4.3.5.12.1 检测方法

访谈、检查。

4.3.5.12.2 检测对象

安全事件报告流程，安全事件响应处理程序，安全事件记录分析文档，安全事件处理记录，安全事件处理报告。

4.3.5.12.3 检测实施

a）检查是否具备安全事件的报告，查看其是否包含安全事件的报告流程；检查是否具备安全事件响应处理程序，查看其是否包含响应和处置的范围、程度，以及处理方法等。

b）检查安全事件记录分析文档，查看其是否分析和鉴定安全事件产生的原因。

c）访谈系统管理员，询问是否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；检查相应的安全事件处理记录和报告。

4.3.5.13 应急预案管理

除按照4.2.5.12的要求进行检测外，还应按照本节内容进行检测。

4.3.5.13.1 检测方法

访谈、检查。

4.3.5.13.2 检测对象

应急预案演练记录、应急预案审查记录。

4.3.5.13.3 检测实施

a）访谈网络运维负责人，询问是否从人力、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。

b）访谈网络运维负责人，询问是否定期对应急预案进行演练；检查是否具备应急预案演练记录，查看演练周期是否符合规定。

c）访谈网络运维负责人，询问是否对应急预案定期审查，是否根据实际情况更新的内容，是否能按实际内容执行；检查是否具有应急预案审查记录，查看是否有应急预案和灾难恢复计划中不适用内容的修订、和更新记录，检查记录是否说明修订和更新的原因以及相关审查结果。

4.4 第3.2级要求

与第3.1级要求相同。

4.5 第 4 级要求

同第 3.2 级要求。

4.6 第 5 级要求

待补充。

参 考 文 献

国家标准	信息安全技术信息系统安全等级保护基本要求（报批搞）
YD/T 1728-2008	电信网和互联网安全防护管理指南
YD/T 1729-2008	电信网和互联网安全等级保护实施指南
YD/T 1730-2008	电信网和互联网安全风险评估实施指南
YD/T 1730-2008	电信网和互联网灾难备份及恢复实施指南