YD

中华人民共和国通信行业标准

YD/T 1753-2008

支撑网安全防护检测要求

Security Protection Testing Requirements for Supporting Network

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 1752-2008《支撑网安全防护要求》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、中国铁通集团有限公司、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

本标准主要起草人：李　成、刘迎伟、龙维薇、田　峰、刘险峰、王君珂、徐　楠

支撑网安全防护检测要求

1 范围

本标准规定了支撑网在安全等级保护、安全风险评估、灾难备份及恢复等方面的安全防护检测要求。

本标准适用于公众电信网中的支撑网。

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。

YD/T 1754-2008　　电信网和互联网物理环境安全等级保护要求

YD/T 1756-2008　　电信网和互联网管理安全等级保护要求

3 术语和定义

下列术语和定义适用于本标准。

3.1

支撑网安全等级 Security Classification of Supporting Network

支撑网安全重要程度的表征。重要程度可从支撑网受到破坏后，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。

3.2

支撑网安全等级保护 Classified Security Protection of Supporting Network

对支撑网分等级实施安全保护。

3.3

组织 Organization

组织是由不同作用的个体为实施共同的业务目标而建立的结构，组织的特性在于为完成目标而分工、合作；一个单位是一个组织，某个业务部门也可以是一个组织。

3.4

支撑网安全风险 Security Risk of Supporting Network

人为或自然的威胁可能利用支撑网中存在的脆弱性导致安全事件的发生及其对组织造成的影响。

3.5

支撑网安全风险评估 Security Risk Assessment of Supporting Network

指运用科学的方法和手段，系统地分析支撑网所面临的威胁及其存在的脆弱性，评估安全事件一旦发生可能造成的危害程度，提出有针对性的抵御威胁的防护对策和安全措施。防范和化解支撑网安全风险，或者将风险控制在可接受的水平，为最大限度地为保障支撑网的安全提供科学依据。

3.6

支撑网资产 Asset of Supporting Network

支撑网中具有价值的资源，是安全防护保护的对象。支撑网中的资产可能是以多种形式存在，无形的、有形的、硬件、软件，包括物理布局、通信设备、物理线路、数据、软件、文档、规程、业务、人员、管理等各种类型的资源，如网络管理系统、计费系统等。

3.7

支撑网资产价值 Asset Value of Supporting Network

支撑网中资产的重要程度或敏感程度。资产价值是资产的属性，也是进行资产识别的主要内容。

3.8

支撑网威胁 Threat of Supporting Network

可能导致对支撑网产生危害的不希望事故潜在起因，它可能是人为的，也可能是非人为的；可能是无意失误，也可能是恶意攻击。常见的支撑网威胁有黑客入侵、硬件故障、人为操作失误、火灾、水灾等等。

3.9

支撑网脆弱性 Vulnerability of Supporting Network

支撑网脆弱性是支撑网中存在的弱点、缺陷与不足，不直接对资产造成危害，但可能被威胁所利用从而危害资产的安全。

3.10

支撑网灾难 Disaster of Supporting Network

由于各种原因，造成支撑网故障或瘫痪，使支撑网的功能停顿或服务水平不可接受、达到特定的时间的突发性事件。

3.11

支撑网灾难备份 Backup for Disaster Recovery of Supporting Network

为了支撑网灾难恢复而对相关网络要素进行备份的过程。

3.12

支撑网灾难恢复 Disaster Recovery of Supporting Network

为了将支撑网从灾难造成的故障或瘫痪状态恢复到正常运行状态或部分正常运行状态、并将其功能从灾难造成的不正常状态恢复到可接受状态，而设计的活动和流程。

3.13

访谈 Interview

检测人员通过与支撑网有关人员（个人/群体）进行交流、讨论等活动，检查支撑网安全等级保护、支撑网安全风险评估和支撑网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。

3.14

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，检查支撑网安全等级保护、支撑网安全风险评估和支撑网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。

3.15

测试 Testing

检测人员通过对检测对象按照预定的方法/工具使其产生特定行为的活动，查看、分析输出结果，检查支撑网安全等级保护、支撑网安全风险评估和支撑网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 支撑网安全防护检测概述

4.1 支撑网安全防护检测范围

支撑网是独立于业务网之外的用于支持网络及设备维护、业务运营和账务管理的综合信息系统所组成的网络。

本标准文件中支撑网的安全防护范围包括：网管系统和业务运营支撑系统。本标准中的网管系统覆盖以下网络：固定通信网、移动通信网、消息网、智能网、接入网、传送网、IP承载网、信令网、同步网。本标准中的业务运营支撑系统包括：计费系统、营业系统、账务系统。

4.2 支撑网安全防护检测对象

本标准文件中支撑网的定级对象为各类网管系统和业务运营支撑系统,可按照全国、省和地市将各个系统分为不同级别。安全等级保护的检测对象确定以后，风险评估的检测对象、灾难备份及恢复的检测对象应与安全等级保护的检测对象相一致。

4.3 支撑网安全防护检测内容

按照支撑网安全防护检测的需要，将支撑网安全防护检测分为支撑网安全等级保护检测、支撑网安全风险评估检测和支撑网灾难备份及恢复检测等3个部分。

支撑网安全防护检测要求包括以下内容：

——支撑网安全等级保护检测

主要包括业务安全检测、网络安全检测、主机安全检测、应用安全检测、数据安全及备份恢复检测、物理环境安全检测、管理安全检测等。

——支撑网安全风险评估检测

主要包括安全风险评估范围检测、安全风险评估内容检测、安全风险评估要素检测、安全风险评估赋值原则检测、安全风险评估计算方法检测、安全风险评估文件类型检测和安全风险评估文件记录检测等。

——支撑网灾难备份及恢复检测

主要包括冗余系统、冗余设备及冗余链路检测、备份数据检测、人员和技术支持能力检测、运行维护管理能力检测和灾难恢复预案检测等。

4.4 支撑网安全防护检测结果判定

支撑网安全防护检测包括对支撑网的安全等级保护、安全风险评估、灾难备份及恢复三个部分的检测，应对三个部分的检测结果分别进行判定，并根据检测结果分别出具检测报告。

支撑网安全防护检测应采取打分的方式进行量化操作，对每一个检测项打分，属于判断结果为“是”或“否”的检测项，结果为“是”则评5分，为“否”则评1分。其他检测项可根据具体实施情况进行评估，并参照表1将评估结果换算成评分。

表1 实施情况评分方法

评估结果	评 分
实施很好	5
实施较好	4
实施一般	3
实施较差	2
实施很差	1

对于安全等级保护，将同一子类检测项的评分结果进行算术平均得到该安全等级保护子类的分数，然后再将各子类的分数进行加权平均得到整个支撑网的安全等级保护的总分数。支撑网安全等级保护中各子类的权重见表2。对于安全风险评估和灾难备份及恢复检测，可将所有检测项目进行算术平均得到最终总分数。

表2 支撑网安全等级保护各子类的权重

权重（%）	等级保护子类
10	业务安全
10	网络安全
10	主机安全
10	应用安全
10	数据安全及备份恢复
20	物理环境安全
30	管理安全

根据各项总分数对支撑网的安全等级保护、安全风险评估和灾难备份及恢复检测结果分别进行等级化评定，总分数和评定等级的关系见表3。

表3 总分数和评定等级的关系

总分数 x	评定等级
$4.5 \leqslant x \leqslant 5$	很好
$3.5 \leqslant x < 4.5$	较好
$2.5 \leqslant x < 3.5$	一般
$1.5 \leqslant x < 2.5$	较差
$1 \leqslant x < 1.5$	很差

5 支撑网安全等级保护检测要求

5.1 第1级要求

不作要求。

5.2 第2级要求

5.2.1 业务安全

5.2.1.1 检测方式

访谈、检查。

5.2.1.2 检测对象

计费系统运行记录，计费信息备份数据。

5.2.1.3 检测实施

a）查看计费系统运行记录，全年中断时间是否符合电信运营企业的相关要求；

b）检查计费系统运行记录，查看计费系统中断后是否当对中断期间未采集的数据进行补采；

c）访谈系统管理员，询问是否对计费信息等数据进行备份，计费数据在系统中保存的时间是否符合相关要求（至少3个月）；查看是否有计费信息备份数据；

d）访谈系统管理员，是否出现过账单错误、重复、丢失、被修改的故障。

5.2.2 网络安全

5.2.2.1 结构安全

5.2.2.1.1 检测方式

访谈、检查。

5.2.2.1.2 检测对象

网络设备、网络拓扑图、网络配置数据。

5.2.2.1.3 检测实施

a）访谈网络管理员，检查网络设备，查看关键网络设备是否具备冗余空间保障的业务处理能力，满足业务高峰期需要；

b）访谈网络管理员，询问接入网络和核心网络的带宽是否满足业务高峰期需要；

c）检查网络拓扑结构图，是否与当前运行情况相符；

d）访谈网络管理员，询问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，查看具体的网络划分情况。

5.2.2.2 访问控制

5.2.2.2.1 检测方式

访谈、检查。

5.2.2.2.2 检测对象

网络设备，访问控制设备。

5.2.2.2.3 检测实施

a）访谈网络管理员，询问是否在网络边界部署访问控制设备，是否启用访问控制功能，查看访问控制配置数据；

b）访谈网络管理员，询问是否能根据会话状态信息为数据流提供明确的允许/拒绝访问的能力，控制粒度是否可为网段级，查看配置数据；

c）访谈网络管理员，询问是否按用户和系统之间的允许访问规则，决定允许或拒绝用户对受控系统进行资源访问，控制粒度是否为单个用户，查看用户访问控制配置数据。

5.2.2.3 安全审计

5.2.2.3.1 检测方式

访谈、检查。

5.2.2.3.2 检测对象

网络设备，网络设备运行状况日志、网络流量日志、用户行为日志，审计记录。

5.2.2.3.3 检测实施

a）访谈网络管理员，询问是否对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录；检查各项日志记录。

b）访谈网络管理员，询问是否有审计记录；检查审计记录，查看是否包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息。

5.2.2.4 边界完整性检查

5.2.2.4.1 检测方式

访谈、检查。

5.2.2.4.2 检测对象

网络设备，用户行为审计记录。

5.2.2.4.3 检测实施

访谈网络管理员，询问是否能够对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进行检查；查看是否具备用户行为的审计记录。

5.2.2.5 入侵防范

5.2.2.5.1 检测方式

访谈、检查。

5.2.2.5.2 检测对象

网络设备、监视记录。

5.2.2.5.3 检测实施

访谈网络管理员，询问是否可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碎片攻击和网络蠕虫攻击等；查看是否具备网络攻击监视记录。

5.2.2.6 网络设备防护

5.2.2.6.1 检测方式

访谈、检查、测试。

5.2.2.6.2 检测对象

网络设备，网络设备用户标识。

5.2.2.6.3 检测实施

a）访谈网络管理员，询问是否对登录网络设备的用户进行身份鉴别；

b）访谈网络管理员，询问是否对网络设备的管理员登录地址进行限制；

c）访谈网络管理员，询问是否对网络设备用户做惟一标识；

d）访谈网络管理员，询问用户口令是否足够复杂度，是否定期更换；

e）访谈网络管理员，询问是否具有登录失败处理功能，是否可采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施，通过测试检验该功能；

f）访谈网络管理员，询问当对网络设备进行远程管理时，是否采取必要措施防止鉴别信息在网络传输过程中被窃听。

5.2.3 主机安全

5.2.3.1 身份鉴别

5.2.3.1.1 检测方式

访谈、检查。

5.2.3.1.2 检测对象

主机设备、操作系统、数据库。

5.2.3.1.3 检测实施

a）访谈网络管理员，询问是否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）访谈网络管理员，询问操作系统和数据库系统管理用户身份标识应具有不易被冒用的特点，口令是否有复杂度要求并定期更换；检查用户身份标识，检查口令更改记录。

c）访谈网络管理员，询问是否启用登录失败处理功能，是否采取结束会话、限制非法登录次数和自动退出等措施。

d）访谈网络管理员，询问当对服务器进行远程管理时，是否采取必要措施，防止鉴别信息在网络传输过程中被窃听。

e）访谈网络管理员，询问是否为操作系统和数据库系统的不同用户分配不同的用户名，确保用户名具有惟一性。

5.2.3.2 访问控制

5.2.3.2.1 检测方式

访谈、检查。

5.2.3.2.2 检测对象

主机设备、操作系统、数据库。

5.2.3.2.3 检测实施

a）访谈网络管理员，询问是否启用访问控制功能，依据安全策略控制用户对资源的访问；

b）访谈网络管理员，询问是否实现操作系统和数据库系统特权用户的权限分离；

c）访谈网络管理员，询问是否限制默认账户的访问权限，重命名系统默认账户，修改这些账户的默认口令；

d）访谈网络管理员，询问是否及时删除多余的、过期的账户，避免共享账户的存在。

5.2.3.3 安全审计

5.2.3.3.1 检测方式

访谈、检查。

5.2.3.3.2 检测对象

主机设备，操作系统，数据库，审计记录。

5.2.3.3.3 检测实施

a）访谈网络管理员，询问审计范围是否覆盖到服务器上的每个操作系统用户和数据库用户；

b）访谈网络管理员，询问是否审计内容是否包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件；

c）检查审计记录，是否包括事件的日期、时间、类型、主体标识、客体标识和结果等；

d）访谈网络管理员，询问是否保护审计记录，避免受到未预期的删除、修改或覆盖等。

5.2.3.4 入侵防范

5.2.3.4.1 检测方式

访谈、检查。

5.2.3.4.2 检测对象

主机设备，操作系统。

5.2.3.4.3 检测实施

访谈网络管理员，询问操作系统是否遵循最小安装的原则，仅安装需要的组件和应用程序，保持系统补丁及时得到更新。

5.2.3.5 恶意代码防范

5.2.3.5.1 检测方式

访谈、检查。

5.2.3.5.2 检测对象

主机设备，防恶意代码软件，防恶意代码软件更新记录，恶意代码库更新记录。

5.2.3.5.3 检测实施

a）访谈网络管理员，询问是否安装防恶意代码软件，是否及时更新防恶意代码软件版本和恶意代码库；检查防恶意代码软件和恶意代码库的更新记录；

b）访谈网络管理员，询问是否支持防恶意代码软件的统一管理。

5.2.3.6 资源控制

5.2.3.6.1 检测方式

访谈、检查、测试。

5.2.3.6.2 检测对象

主机设备、安全策略。

5.2.3.6.3 检测实施

a）访谈网络管理员，询问是否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；

b）访谈网络管理员，询问是否根据安全策略设置登录终端的操作超时锁定，通过测试检验该功能；

c）访谈网络管理员，询问是否限制单个用户对系统资源的最大或最小使用限度，查看配置数据。

5.2.4 应用安全

5.2.4.1 身份鉴别

5.2.4.1.1 检测方式

访谈、检查、测试。

5.2.4.1.2 检测对象

应用软件。

5.2.4.1.3 检测实施

a）访谈网络管理员，询问是否提供专用的登录控制模块对登录用户进行身份标识和鉴别；

b）访谈网络管理员，询问是否提供用户身份标识惟一和鉴别信息复杂度检查功能，是否能保证应用系统中不存在重复用户身份标识，身份鉴别信息不易被冒用；

c）访谈网络管理员，询问是否提供登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施，通过测试检验该功能；

d）访谈网络管理员，询问是否启用身份鉴别、用户身份标识惟一性检查、用户身份鉴别信息复杂度检查以及登录失败处理功能，并根据安全策略配置相关参数，查看安全策略配置参数。

5.2.4.2 访问控制

5.2.4.2.1 检测方式

访谈、检查。

5.2.4.2.2 检测对象

应用软件。

5.2.4.2.3 检测实施

a）访谈网络管理员，询问是否提供访问控制功能，依据安全策略控制用户对文件、数据库表等客体的访问；

b）访谈网络管理员，询问访问控制的覆盖范围是否包括与资源访问相关的主体、客体及它们之间的操作；

c）访谈网络管理员，询问是否由授权主体配置访问控制策略，并严格限制默认账户的访问权限；

d）访谈网络管理员，询问是否授予不同账户为完成各自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。

5.2.4.3 安全审计

5.2.4.3.1 检测方式

访谈、检查。

5.2.4.3.2 检测对象

应用软件，审计记录。

5.2.4.3.3 检测实施

a）访谈网络管理员，询问是否提供覆盖到每个用户的安全审计功能，对应用系统重要安全事件进行审计；

b）访谈网络管理员，询问是否保证无法删除、修改或覆盖审计记录；

c）检查审计记录的内容，查看是否至少包括事件日期、时间、发起者信息、类型、描述和结果等。

5.2.4.4 通信完整性

5.2.4.4.1 检测方式

访谈、检查。

5.2.4.4.2 检测对象

应用软件，软件设计文档。

5.2.4.4.3 检测实施

访谈网络管理员，询问是否采用校验码技术保证通信过程中数据的完整性，查看软件设计文档，是否具备该功能。

5.2.4.5 通信保密性

5.2.4.5.1 检测方式

访谈、检查。

5.2.4.5.2 检测对象

应用软件。

5.2.4.5.3 检测实施

a）访谈网络管理员，询问在通信双方建立连接之前，应用系统是否利用密码技术进行会话初始化验证，查看软件使用手册或设计文档；

b）访谈网络管理员，询问是否对通信过程中的敏感信息字段进行加密。

5.2.4.6 软件容错

5.2.4.6.1 检测方式

访谈、检查。

5.2.4.6.2 检测对象

应用软件。

5.2.4.6.3 检测实施

访谈网络管理员，询问是否提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的数据格式或长度符合系统设定要求。

5.2.4.7 资源控制

5.2.4.7.1 检测方式

访谈、检查、测试。

5.2.4.7.2 检测对象

应用软件。

5.2.4.7.3 检测实施

a）访谈网络管理员，询问当应用系统的通信双方中的一方在一段时间内未作任何响应，另一方是否能够自动结束会话，通过测试检验该功能；

b）访谈网络管理员，询问是否能够对应用系统的最大并发会话连接数进行限制，通过测试检验该功能；

c）访谈网络管理员，询问是否能够对单个账户的多重并发会话进行限制，通过测试检验该功能。

5.2.5 数据安全及备份恢复

5.2.5.1 数据完整性

5.2.5.1.1 检测方式

访谈、检查。

5.2.5.1.2 检测对象

鉴别信息，重要业务数据。

5.2.5.1.3 检测实施

访谈网络管理员，询问是否能够检测到鉴别信息和重要业务数据在传输过程中完整性受到破坏。

5.2.5.2 数据保密性

5.2.5.2.1 检测方式

访谈、检查。

5.2.5.2.2 检测对象

鉴别信息。

5.2.5.2.3 检测实施

访谈网络管理员，询问是否采用加密或其他保护措施实现鉴别信息的存储保密性。

5.2.5.3 备份和恢复

5.2.5.3.1 检测方式

访谈、检查。

5.2.5.3.2 检测对象

重要信息的备份和恢复记录，关键网络设备，通信线路，数据处理系统。

5.2.5.3.3 检测实施

a）访谈网络管理员，询问是否对重要信息进行备份和恢复；检查重要信息备份和恢复记录；

b）访谈网络管理员，询问是否提供关键网络设备、通信线路和数据处理系统的硬件冗余，保证系统的可用性。

5.2.6 物理环境安全

与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》中的第2级要求的内容相同。

5.2.7 管理安全

与YD/T 1757-2008《电信网和互联网管理安全等级保护检测要求》中的第2级要求的内容相同。

5.3 第3.1级要求

5.3.1 业务安全

与5.2.1的检测内容相同。

5.3.2 网络安全

5.3.2.1 结构安全

除按照5.2.2.1的要求进行检测外，还应按照本节内容进行检测。

5.3.2.1.1 检测方式

访谈、检查。

5.3.2.1.2 检测对象

网络设备。

5.3.2.1.3 检测实施

a）访谈网络管理员，询问在业务终端与业务服务器之间是否进行路由控制建立安全的访问路径；

b）访谈网络管理员，询问是否避免将重要网段部署在网络边界处且直接连接外部信息系统，重要网段与其他网段之间是否采取可靠的技术隔离手段，询问采用何种具体手段；

c）访谈网络管理员，询问是否按照对业务服务的重要次序来指定带宽分配优先级别，在网络发生拥堵的时候是否优先保护重要主机，查看配置数据。

5.3.2.2 访问控制

除按照5.2.2.2的要求进行检测外，还应按照本节内容进行检测。

5.3.2.2.1 检测方式

访谈、检查、测试。

5.3.2.2.2 检测对象

网络设备。

5.3.2.2.3 检测实施

a）访谈网络管理员，询问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；

b）访谈网络管理员，询问是否在会话处于非活跃一定时间或会话结束后终止网络连接，通过测试检测该功能；

c）访谈网络管理员，询问是否限制网络最大流量数及网络连接数，查看相关配置数据；

d） 访谈网络管理员，询问重要网段是否采取技术手段防止地址欺骗，查看软件使用手册或设计文档，是否具备此功能。

5.3.2.3 安全审计

除按照5.2.2.3的要求进行检测外，还应按照本节内容进行检测。

5.3.2.3.1 检测方式

访谈、检查。

5.3.2.3.2 检测对象

网络设备、审计记录。

5.3.2.3.3 检测实施

a）访谈网络管理员，询问是否能够根据记录数据进行分析，并生成审计报表；检查审计记录；

b）访谈网络管理员，询问是否对审计记录进行保护，避免受到未预期的删除、修改或覆盖等。

5.3.2.4 边界完整性检查

除按照5.2.2.4的要求进行检测外，还应按照本节内容进行检测。

5.3.2.4.1 检测方式

访谈、检查。

5.3.2.4.2 检测对象

网络设备。

5.3.2.4.3 检测实施

访谈网络管理员，询问是否能够对非授权设备私自联到内部网络的行为进行检查，准确定出位置，并对其进行有效阻断。

5.3.2.5 入侵防范

除按照5.2.2.5的要求进行检测外，还应按照本节内容进行检测。

5.3.2.5.1 检测方式

访谈、检查。

5.3.2.5.2 检测对象

网络设备、入侵事件记录。

5.3.2.5.3 检测实施

访谈网络管理员，询问当检测到攻击行为时，是否能记录攻击源IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时是否提供报警，检查入侵事件记录和告警信息。

5.3.2.6 网络设备防护

除按照5.2.2.6的要求进行检测外，还应按照本节内容进行检测。

5.3.2.6.1 检测方式

访谈、检查。

5.3.2.6.2 检测对象

网络设备。

5.3.2.6.3 检测实施

访谈网络管理员，询问是否实现设备特权用户的权限分离。

5.3.2.7 恶意代码防范

5.3.2.7.1 检测方式

访谈、检查。

5.3.2.7.2 检测对象

网络设备、恶意代码库。

5.3.2.7.3 检测实施

a）访谈网络管理员，询问是否是否在网络边界处对恶意代码进行检测和清除；

b）访谈网络管理员，询问是否维护恶意代码库的升级和检测系统的更新，检查恶意代码苦的升级记录和系统更新记录。

5.3.3 主机安全

5.3.3.1 身份鉴别

与5.2.3.1的检测内容相同。

5.3.3.2 访问控制

除按照5.2.3.2的要求进行检测外，还应按照本节内容进行检测。

5.3.3.2.1 检测方式

访谈、检查。

5.3.3.2.2 检测对象

主机设备。

5.3.3.2.3 检测实施

a）访谈网络管理员，询问是否根据管理用户的角色分配权限，实现管理用户的权限分离，仅授予管理用户所需的最小权限，检查用户权限设置数据；

b）访谈网络管理员，询问是否对重要信息资源设置敏感标记，检查具体标记；

c）访谈网络管理员，询问是否依据安全策略严格控制用户对有敏感标记重要信息资源的操作。

5.3.3.3 安全审计

除按照5.2.3.3的要求进行检测外，还应按照本节内容进行检测。

5.3.3.3.1 检测方式

访谈、检查。

5.3.3.3.2 检测对象

主机设备、审计报表。

5.3.3.3.3 检测实施

a）访谈网络管理员，询问是否能够根据记录数据进行分析，并生成审计报表；

b）访谈网络管理员，询问是否能保护审计进程，避免受到未预期的中断。

5.3.3.4 入侵防范

除按照5.2.3.4的要求进行检测外，还应按照本节内容进行检测。

5.3.3.4.1 检测方式

访谈、检查。

5.3.3.4.2 检测对象

主机设备，入侵记录，完整性测试记录，恢复记录。

5.3.3.4.3 检测实施

a）访谈网络管理员，询问是否能够检测到对重要服务器进行入侵的行为，是否能够记录入侵的源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，检查入侵记录；

b）访谈网络管理员，询问是否能够对重要程序的完整性进行检测，并在检测到完整性受到破坏后具有恢复的措施，检查完整性测试和恢复记录。

5.3.3.5 恶意代码防范

除按照5.2.3.5的要求进行检测外，还应按照本节内容进行检测。

5.3.3.5.1 检测方式

访谈、检查。

5.3.3.5.2 检测对象

主机设备、防恶意代码产品。

5.3.3.5.3 检测实施

访谈网络管理员，询问主机防恶意代码产品是否具有与网络防恶意代码产品不同的恶意代码库，查看主机上的防恶意代码产品。

5.3.3.6 资源控制

除按照5.2.3.6的要求进行检测外，还应按照本节内容进行检测。

5.3.3.6.1 检测方式

访谈、检查、测试。

5.3.3.6.2 检测对象

主机设备。

5.3.3.6.3 检测实施

a）访谈网络管理员，询问是否过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；

b）访谈网络管理员，询问是否根据安全策略设置登录终端的操作超时锁定，测试终端登录操作超时的情况；

c）访谈网络管理员，询问是否限制单个用户对系统资源的最大或最小使用限度。

5.3.4 应用安全

5.3.4.1 身份鉴别

与5.2.4.1的检测内容相同。

5.3.4.2 访问控制

除按照5.2.4.2的要求进行检测外，还应按照本节内容进行检测。

5.3.4.2.1 检测方式

访谈、检查。

5.3.4.2.2 检测对象

应用软件、重要信息资源。

5.3.4.2.3 检测实施

a）访谈网络管理员，询问是否具有对重要信息资源设置敏感标记的功能，查看具体设置；

b）访谈网络管理员，询问是否依据安全策略严格控制用户对有敏感标记重要信息资源的操作。

5.3.4.3 安全审计

除按照5.2.4.3的要求进行检测外，还应按照本节内容进行检测。

5.3.4.3.1 检测方式

访谈、检查。

5.3.4.3.2 检测对象

应用软件、审计记录。

5.3.4.3.3 检测实施

a）访谈网络管理员，询问是否无法单独中断审计进程；

b）访谈网络管理员，询问是否提供对审计记录数据进行统计、查询、分析及生成审计报表的功能，查看审计记录；

c）访谈网络管理员，询问是否强化对涉及金额的数据以及涉及用户信息数据访问的审计，查看审计记录。

5.3.4.4 通信完整性

除按照5.2.4.4的要求进行检测外，还应按照本节内容进行检测。

5.3.4.4.1 检测方式

访谈、检查。

5.3.4.4.2 检测对象

应用软件、软件设计文档。

5.3.4.4.3 检测实施

访谈网络管理员，询问是否采用密码技术保证通信过程中数据的完整性，查看软件设计文档，是否具备该功能。

5.3.4.5 通信保密性

与5.2.4.5的检测内容相同。

5.3.4.6 软件容错

除按照5.2.4.6的要求进行检测外，还应按照本节内容进行检测。

5.3.4.6.1 检测方式

访谈、检查、测试。

5.3.4.6.2 检测对象

应用软件。

5.3.4.6.3 检测实施

访谈网络管理员，询问是否应提供自动保护功能，当故障发生时自动保护当前所有状态，是否保证系统能够进行恢复，通过测试检验容错功能。

5.3.4.7 资源控制

除按照5.2.4.7的要求进行检测外，还应按照本节内容进行检测。

5.3.4.7.1 检测方式

访谈、检查、测试。

5.3.4.7.2 检测对象

应用软件。

5.3.4.7.3 检测实施

a）访谈网络管理员，询问是否能够对一个时间段内可能的并发会话连接数进行限制，通过测试检验是否具备并发会话连接数限制功能；

b）访谈网络管理员，询问是否能够对一个访问账户或一个请求进程占用的资源分配最大限额和最小限额，通过测试检验是否具备资源限额功能；

c）访谈网络管理员，询问是否能够对系统服务水平降低到预先规定的最小值进行检测和报警，查看报警信息；

d）访谈网络管理员，询问是否提供服务优先级设定功能，并在安装后根据安全策略设定访问账户或请求进程的优先级，根据优先级分配系统资源，查看服务优先设定功能的配置数据。

5.3.5 数据安全及备份恢复

5.3.5.1 数据完整性

除按照5.2.5.1的要求进行检测外，还应按照本节内容进行检测。

5.3.5.1.1 检测方式

访谈、检查。

5.3.5.1.2 检测对象

数据，系统管理数据，鉴别信息数据，重要业务数据。

5.3.5.1.3 检测实施

a）访谈网络管理员，询问是否能够检测到系统管理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，采用何种检测手段和恢复措施；

b）访谈网络管理员，询问是否能够检测到系统管理数据、鉴别信息和重要业务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，采用何种检测手段和恢复措施。

5.3.5.2 数据保密性

除按照5.2.5.2的要求进行检测外，还应按照本节内容进行检测。

5.3.5.2.1 检测方式

访谈、检查。

5.3.5.2.2 检测对象

数据，系统管理数据，鉴别信息数据，重要业务数据，软件设计文档。

5.3.5.2.3 检测实施

a）访谈网络管理员，询问是否采用加密或其他有效措施实现系统管理数据、鉴别信息和重要业务数据传输保密性，查看软件设计说明文档，检查是否具备数据加密功能；

b）访谈网络管理员，询问是否采用加密或其他保护措施实现系统管理数据和重要业务数据存储保密性，查看软件设计说明文档，检查是否具备数据加密功能。

5.3.5.3 备份和恢复

除按照5.2.5.3的要求进行检测外，还应按照本节内容进行检测。

5.3.5.3.1 检测方式

访谈、检查、测试。

5.3.5.3.2 检测对象

数据、支撑网网络拓扑。

5.3.5.3.3 检测实施

a）访谈网络管理员，询问是否提供本地数据备份与恢复功能，备份介质场外存放，对数据备份和恢复功能进行测试；

b）访谈网络管理员，询问是否具备异地数据备份功能，采用何种方式；

c）访谈网络管理员，询问是否采用冗余技术设计网络拓扑结构，避免关键节点存在单点故障，查看网络拓扑图，是否具有冗余设计。

5.3.6 物理环境安全

与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》中的第3.1级要求的内容相同。

5.3.7 管理安全

与YD/T 1757-2008《电信网和互联网管理安全等级保护检测要求》中的第3.1级要求的内容相同。

5.4 第3.2级要求

5.4.1 业务安全

除按照5.3.1的要求进行检测外，还应按照本节内容进行检测。

5.4.1.1 检测方式

访谈、检查。

5.4.1.2 检测对象

营业系统服务器，计费系统服务器，账务系统服务器。

5.4.1.3 检测实施

访谈网络管理员，询问营业系统、计费系统、账务系统的服务器是否在异址（可为同城不同地点的机房）进行容灾备份。

5.4.2 网络安全

与第5.3.2的检测内容相同。

5.4.3 主机安全

与第5.3.3的检测内容相同。

5.4.4 应用安全

与第5.3.4的检测内容相同。

5.4.5 数据安全及备份恢复

与第5.3.5的检测内容相同。

5.4.6 物理环境安全

与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》中的第3.2级要求的内容相同。

5.4.7 管理安全

与YD/T 1757-2008《电信网和互联网管理安全等级保护检测要求》中的第3.2级要求的内容相同。

5.5 第4级要求

同第3.2级要求。

5.6 第5级要求

待补充。

6 支撑网安全风险评估检测要求

6.1 安全风险评估范围

6.1.1 检测方式

访谈、检查。

6.1.2 检测对象

风险评估报告，风险评估负责人。

6.1.3 检测实施

应访谈风险评估负责人，询问进行支撑网风险评估时，选择的风险评估范围是什么，是否对支撑网风险评估范围作出合理的边界划分。

6.2 安全风险评估内容

6.2.1 检测方式

访谈、检查。

6.2.2 检测对象

风险评估报告，风险评估负责人。

6.2.3 检测实施

a）访谈支撑网风险评估负责人、查看风险评估报告，检查支撑网风险评估是否覆盖了技术安全和管理安全；

b）访谈支撑网风险评估负责人、查看风险评估报告，检查支撑网风险评估中技术安全是否覆盖了业务安全、网络安全、主机安全、应用安全、数据安全即备份恢复和物理环境安全等方面；

c）访谈支撑网风险评估负责人、查看风险评估报告，检查支撑网风险评估中管理安全是否覆盖了安全管理制度、安全管理机构、人员安全管理、安全建设管理、安全运维管理等方面。

6.3 安全风险评估要素

6.3.1 检测方式

访谈、检查。

6.3.2 检测对象

风险评估报告，风险评估负责人，历史记录。

6.3.3 检测实施

a）访谈风险评估负责人，询问进行支撑网风险评估时采用了哪些风险评估的要素；查看风险评估报告，检查支撑网风险评估时是否包含了资产、脆弱性、威胁、安全措施、风险和残余风险等要素。

b）访谈风险评估负责人，询问进行支撑网风险评估时考虑了哪些风险评估要素的相关属性；查看风险评估报告，检查支撑网风险评估报告时是否包含了与评估要素密切相关的业务战略、资产价值、安全需求和安全事件等属性。

c）访谈风险评估负责人，询问进行支撑网风险评估时评估了哪些资产；检查风险评估报告，查看风险评估报告中资产是否包含了各类设备（网管系统、营业系统、计费系统、账务系统）的硬件和软件、设备中的各种重要数据（配置数据、用户信息、账单等）、网络和业务运营商向用户提供的服务（如账单服务等）、各类人员（管理人员及技术人员等）、纸质文件和规章制度等。

d）访谈风险评估负责人，询问计算支撑网各资产的资产价值时考虑了哪些因素；检查风险评估报告，查看风险评估报告中资产价值的计算是否主要考虑了社会影响力、资产价值和可用性等因素，同时采用了合理的计算方法。

e）访谈风险评估负责人，询问识别了支撑网各资产的脆弱性时考虑了哪些方面的脆弱性；检查风险评估报告，查看风险评估报告中脆弱性识别是否包含了技术脆弱性和管理脆弱性等方面，技术脆弱性是否包含了业务/应用脆弱性、网络脆弱性、设备脆弱性和物理环境脆弱性，管理脆弱性是否包含安全管理机构方面的脆弱性、人员管理方面脆弱性、建设管理方面的脆弱性、运维管理方面的脆弱性。

f）访谈风险评估负责人，询问识别了支撑网各资产的脆弱性时考虑了哪些方面的脆弱性；检查风险评估报告，查看风险评估报告中威胁识别是否依据了已有安全事件报告数据、检测工具检测数据和国内外同行业报告数据等多个方面综合考虑。

g）访谈风险评估负责人，询问对支撑网存在哪些威胁；检查风险评估报告，查看风险评估报告中威胁是否包含了网络设备自身的威胁、环境威胁、人员威胁和管理制度中的隐患造成的威胁。

h）访谈风险评估负责人，询问威胁识别依据了哪些历史数据；查看风险评估报告，检查支撑网风险评估中威胁识别是否依据了已有安全事件报告数据、检测工具检测数据和国内外同行业报告数据等多个方面。

i）访谈风险评估负责人，询问风险值的计算采用了哪种计算方法；查看风险评估报告，检查支撑网风险评估中风险值的计算是否主要考虑了资产、威胁和脆弱性等因素，是否采用了合理的计算方法。

j）访谈风险评估负责人，询问如何确定的风险阈值；查看风险评估报告，检查支撑网风险评估中确定的风险阈值是否合理，是否与资产所在网络或系统的安全等级相结合。

k）访谈风险评估负责人，询问对于不可接受的风险，是否制定了相应的风险处理计划；查看风险评估报告，检查支撑网风险评估中对于不可接受的风险，是否制定了相应的风险处理计划，采用风险处理计划以后，风险值是否满足阈值要求。

6.4 安全风险评估赋值原则

6.4.1 检测方式

访谈、检查。

6.4.2 检测对象

风险评估报告，风险评估负责人

6.4.3 检测实施

a）访谈风险评估负责人，询问支撑网风险评估时对资产的赋值遵循了什么样的原则；查看风险评估报告，检查支撑网各资产的赋值是否从资产的社会影响力、资产价值和可用性3个方面和5个等级进行赋值。

b）访谈风险评估负责人，询问支撑网风险评估时对脆弱性的赋值遵循了什么样的原则；查看风险评估报告，检查支撑网脆弱性的赋值是否考虑赋值对象对资产损害程度等因素，是否按照5个等级进行赋值。

c）访谈风险评估负责人，询问支撑网风险评估时对威胁的赋值遵循了什么样的原则；查看风险评估报告，检查支撑网威胁的赋值是否依据威胁发生的频率，同时是否按照5个等级进行赋值。

6.5 安全风险评估计算方法

6.5.1 检测方式

访谈、检查。

6.5.2 检测对象

风险评估报告，风险评估负责人

6.5.3 检测实施

a）访谈风险评估负责人，询问支撑网风险评估中采用了什么样的方法计算资产价值；查看风险评估报告，检查支撑网资产价值的计算方法是否合理，是否有对于所采用计算方法的理论分析。

b）访谈风险评估负责人，询问支撑网风险评估中采用了什么样的方法计算风险值；查看风险评估报告，检查支撑网风险值的计算方法是否合理，是否具有对于所采用计算方法的理论分析。

6.6 安全风险评估文件类型

6.6.1 检测方式

访谈、检查。

6.6.2 检测对象

风险评估方案，风险评估程序，资产识别清单，重要资产清单，脆弱性列表，威胁列表，已有安全措施确认表，风险评估报告，风险评估记录，风险处理计划等风险评估文件。

6.6.3 检测实施

a）访谈风险评估负责人，询问是否制定了风险评估方案；查看此文件，检查是否包括风险评估的目标、范围、人员、评估方法、评估结果的形式和实施进度等内容。

b）访谈风险评估负责人，询问是否制定了风险评估程序；查看此文件，检查是否包括风险评估的目的、职责、过程、相关的文件要求，以及实施本次评估所需要的各种资产、威胁、脆弱性识别和判断依据等内容。

c）访谈风险评估负责人，询问是否制定了资产识别清单；查看此文件，检查是否根据组织在风险评估程序文件中所确定的资产分类方法进行资产识别，形成资产识别清单，明确资产的责任人/部门等内容。

d）访谈风险评估负责人，询问是否制定了重要资产清单；查看此文件，检查是否根据资产识别和赋值的结果，形成重要资产列表，包括重要资产名称、描述、类型、重要程度、责任人/部门等内容。

e）访谈风险评估负责人，询问是否根据威胁识别和赋值的结果，制定了威胁列表；查看此文件，检查是否包括威胁名称、种类、来源、动机及出现的频率等内容。

f）访谈风险评估负责人，询问是否根据脆弱性识别和赋值的结果，形成脆弱性列表；查看此文件，检查是否包括具体脆弱性的名称、描述、类型及严重程度等。

g）访谈风险评估负责人，询问是否根据已采取的安全措施确认的结果，形成已有安全措施确认表；查看此文件，检查是否包括已有安全措施名称、类型、功能描述及实施效果等。

h）访谈风险评估负责人，询问是否有风险评估报告；查看此文件，检查是否对整个风险评估过程和结果进行总结，详细说明被评估对象，风险评估方法，资产、威胁、脆弱性的识别结果，风险分析、风险统计和结论等内容。

i）访谈风险评估负责人，询问是否有风险处理计划；查看此文件，检查是否对评估结果中不可接受的风险制定风险处理计划，选择适当的控制目标及安全措施，明确责任、进度、资源，并通过对残余风险的评价以确定所选择安全措施的有效性。

j）访谈风险评估负责人，询问是否有风险评估记录；查看此文件，检查风险评估过程中的各种现场记录是否可复现评估过程，是否能够作为产生歧义后解决问题的依据。

6.7 安全风险评估文件记录

6.7.1 检测方式

访谈、检查。

6.7.2 检测对象

风险评估方案，风险评估程序，资产识别清单，重要资产清单，脆弱性列表，威胁列表，已有安全措施确认表，风险评估报告，风险评估记录，风险处理计划等风险评估文件。

6.7.3 检测实施

a）访谈风险评估负责人，询问风险评估文件发布以前是否需要批准；应查看风险评估文件，检查文件发布以前是否得到批准。

b）访谈风险评估负责人，询问风险评估文件的更改和现行修订状态是如何进行识别的；应查看风险评估文件，检查文件的更改和现行修订状态是否是可识别的。

c）访谈风险评估负责人，询问风险评估文件的版本如何管理；应查看风险评估文件，检查是否有版本划分以及相应的版本使用说明。

d）访谈风险评估负责人，询问作废文件是如何管理的；应查看风险评估文件，检查是否对于作废文件作了标识。

e）访谈风险评估负责人，询问如何对文件进行控制；应查看风险评估文件，检查是否规定其标识、储存、保护、检索、保存期限以及处置所需的控制。

7 支撑网灾难备份及恢复检测要求

7.1 第1级要求

不作要求。

7.2 第2级要求

7.2.1 冗余系统、冗余设备及冗余链路

7.2.1.1 检测方式

访谈、检查。

7.2.1.2 检测对象

支撑网系统设计/验收文档，支撑网设备，演练文档。

7.2.1.3 检测实施

a）检查重要服务器、重要部件、重要数据库是否采用本地双机备份的方式进行容灾保护。

b）检查演练文档，查看支撑网网络灾难演练的恢复时间是否满足行业管理和企业应急预案的相关要求。

7.2.2 数据备份

7.2.2.1 检测方式

访谈、检查。

7.2.2.2 检测对象

支撑网设计/验收文档，支撑网设备。

7.2.2.3 检测实施

a）访谈支撑网安全管理人员，询问系统的关键数据（如网络拓扑配置数据、业务支撑系统的用户资料 、费率表）是否提供本地备份；

b）检查设计/验收文档，查看支撑网是否支持关键数据定期备份，查看数据备份日志，记录备份周期。

7.2.3 人员和技术支持能力

7.2.3.1 检测方式

访谈、检查。

7.2.3.2 检测对象

机房管理人员，技术支持人员，安全管理人员，历史值班记录，培训记录。

7.2.3.3 检测实施

a）检查是否有安全管理人员，应访谈安全管理人员，询问并察看历史值班记录，是否安排机房管理人员、数据备份人员和相关的软硬件支持人员（不要求是专职人员）。

b）检查培训记录，查看技术人员是否定期得到灾难备份及恢复方面的技能培训。

7.2.4 运行维护管理能力

7.2.4.1 检测方式

访谈、检查。

7.2.4.2 检测对象

管理制度、安全管理人员。

7.2.4.3 检测实施

a）访谈安全管理人员，询问是否有相应的介质存取、验证和转储管理制度，是否可确保备份数据授权访问；

b）检查支撑网相关管理制度，查看其是否按介质特性对备份数据进行定期的有效性验证；

c）检查支撑网相关管理制度，查看其是否具有相关服务器设备的灾难备份及恢复的管理制度。

7.2.5 灾难恢复预案

7.2.5.1 检测方式

访谈、检查。

7.2.5.2 检测对象

灾难恢复预案，设计/验收文档，演练记录，管理制度，安全管理人员。

7.2.5.3 检测实施

a）检查支撑网灾难恢复预案设计/验收文档，查看其是否具备完整的支撑网灾难恢复预案；

b）检查支撑网灾难恢复教育和培训计划，访谈相关人员是否具备实际操作能力；

c）检查支撑网灾难恢复预案演练记录，查看其是否已经过灾难恢复预案演练以及灾难恢复预案演练的效果是否达到设计要求。

7.3 第3.1级要求

7.3.1 冗余系统、冗余设备及冗余链路

与7.2.1的检测内容相同。

7.3.2 数据备份

与7.2.2的检测内容相同。

7.3.3 人员和技术支持能力

与7.2.3的检测内容相同。

7.3.4 运行维护管理能力

与7.2.4的检测内容相同。

7.3.5 灾难恢复预案

与7.2.5的检测内容相同。

7.4 第3.2级要求

7.4.1 冗余系统、冗余设备及冗余链路

除按照7.3.1的要求进行检测外，还应检测本节内容。

7.4.1.1 检测方式

访谈、检查。

7.4.1.2 检测对象

支撑网系统设计/验收文档，支撑网设备。

7.4.1.3 检测实施

a）检查重要服务器、重要部件、重要数据库是否采用异地备份的方式进行容灾保护；

b）检查关键设备之间是否提供多条物理链路。

7.4.2 数据备份

除按照7.3.2的要求进行检测外，还应检测本节内容。

7.4.2.1 检测方式

访谈、检查。

7.4.2.2 检测对象

支撑网设计/验收文档，支撑网设备。

7.4.2.3 检测实施

访谈支撑网安全管理人员，询问系统的关键数据是否提供异地备份。

7.4.3 人员和技术支持能力

与7.3.3的检测内容相同。

7.4.4 运行维护管理能力

与7.3.4的检测内容相同。

7.4.5 灾难恢复预案

除按照7.3.5节的要求进行检测外，还应检测本节内容。

7.4.5.1 检测方式

访谈、检查。

7.4.5.2 检测对象

管理制度，灾难恢复预案管理制度。

7.4.5.3 检测实施

检查支撑网管理制度，查看其是否具有灾难恢复预案管理制度。

7.5 第4级要求

同第3.2级要求。

7.6 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 1731-2008　电信网和互联网灾难备份及恢复实施指南