YD

中华人民共和国通信行业标准

YD/T 1743-2008

接入网安全防护检测要求

Security Protection Testing Requirements for Access 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 1742-2008《接入网安全防护要求》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：刘　谦、唐建军、曹一生、钟　星、贾　川

接入网安全防护检测要求

1 范围

本标准规定了接入网在安全等级保护、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接入网。

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检测要求

YD/T 1756—2008　　电信网和互联网管理安全等级保护检测要求

3 术语和定义

下列术语和定义适用于本标准。

3.1

接入网安全等级 Security Classification of Transport Network

接入网安全重要程度的表征。重要程度可从接入网受到破坏后，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

接入网安全等级保护 Classified Security Protection of Transport Network

对接入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

接入网安全风险 Security Risk of Transport Network

人为或自然的威胁可能利用接入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

接入网安全风险评估 Security Risk Assessment of Transport Network

指运用科学的方法和手段，系统地分析接入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。为进一步提出有针对性的抵御威胁的防护对策和安全措施，防范和化解接入网安全风险，将风险控制在可接受的水平，为最大限度地保障接入网的安全提供科学依据。

3.6

接入网资产 Asset

接入网中具有价值的资源，是安全防护保护的对象。接入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，如接入网的设备（DSLAM、OLT、ONU、以太网交换机、综合接入系统、无线接入的基站等）、接入网的光/电缆线路、接入网的网络布局等。

3.7

接入网资产价值 Asset Value

接入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

接入网威胁 Threat

可能导致对接入网产生危害的不希望事件潜在起因，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。常见的接入网络威胁有光纤/缆中断、设备失效、火灾、水灾等。

3.9

接入网脆弱性 Vulnerability

脆弱性是接入网中存在的弱点、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及资产的安全。

3.10

接入网灾难 Disaster of Transport Network

由于各种原因，造成接入网故障或瘫痪，使接入网支持的业务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

接入网灾难备份 Backup for Disaster Recovery of Transport Network

为了接入网灾难恢复而对相关网络要素进行备份的过程。

3.12

接入网灾难恢复 Disaster Recovery of Transport Network

为了将接入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，并将其支持的业务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

检测人员通过与接入网有关人员（个人/群体）进行交流、讨论等活动，检查接入网安全等级保护、接入网安全风险评估和接入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，检查接入网安全等级保护、接入网安全风险评估和接入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，检查接入网安全等级保护、接入网安全风险评估和接入网灾难备份及恢复相关措施的落实情况以及相关工作开展情况的一种方法。

4 缩略语

下列缩略语适用于本标准。

ACL	Access Control List	访问控制列表
DSL	Digital Subscriber Line	数字用户线
DSLAM	Digital Subscriber Line Access Multiplexer	数字用户线接入复用器
IP	Internet Protocol	互联网协议
LMDS	Local Multi-point Distribution System	本地多点分配系统
MAC	Media Access Control	媒质接入控制
OLT	Optical Line Terminal	光线路终端
ONU	Optical Network Unit	光网络单元
PON	Passive Optical Network	无源光网络
PWLAN	Public Wireless Local Area Network	公众无线局域网
SNI	Service Node Interface	业务节点接口
UNI	User Network Interface	用户网络接口

5 接入网安全防护检测概述

5.1 接入网安全防护检测范围

接入网由三个接口所定界，即网络侧经由SNI与业务节点相连，用户侧经由UNI与用户设备或者用户驻地网相连，网管方面经由网管接口与电信管理网相连。接入网包括各种有线和无线接入系统以及网元管理系统。

接入网的安全防护的检测范围特指本地网下不同区域（如：区、县等）内的接入网，包括各种有线接入系统（如：DSL系统、PON系统、以太网接入系统、综合接入系统等）和无线接入系统（如：LMDS、3.5GHz固定无线接入系统、5.8GHz固定无线接入系统、PWLAN系统、基于802.16d的WiMAX系统等）。

5.2 接入网安全防护检测内容

按照接入网安全防护检测的需要，将接入网安全防护检测分为接入网安全等级保护检测、接入网安全安全风险评估检测和接入网灾难备份及恢复检测等三个部分。

接入网安全防护检测要求包括以下一些内容：

——接入网安全等级保护检测

主要包括网络安全检测、设备安全检测、物理环境安全检测、管理安全检测等；

——接入网安全风险评估检测

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

——接入网灾难备份及恢复检测

主要包括备份数据检测、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。

5.3 接入网安全防护检测结果判定原则

接入网安全防护检测包括对接入网的安全等级保护、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，检测报告中应具体说明安全防护工作的优势和不足。

对每一个部分中的每一个评测项，应根据具体实施情况进行等级化评价（分5级：很好、较好、一般、较差、很差）。参见表1将各评测项的评价等级换算成评分，各评测项的分数经过一定的算法（例如加权平均）分别得到安全等级保护、安全风险评估、灾难备份及恢复三个部分的总分数，根据总分数分别对安全等级保护、安全风险评估、灾难备份及恢复三个部分的评测结果进行等级化评定，总分数和评定等级的关系见表2。在计算总分数过程中，应充分考虑到各评测项在安全防护检测要求中所占的比重，例如，表3给出了安全等级保护子类所占的比重。

表1 评测项评分方法

评价结果	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

表2 总分数和评定等级的关系

总分数 x	评定等级
$x \geq 4.5$	很好
$3.5 \leq x < 4.5$	较好
$2.5 \leq x < 3.5$	一般
$1.5 \leq x < 2.5$	较差
$x < 1.5$	很差

表3 安全等级保护子类所占的比重

比 重	安全等级保护子类
30%	网络安全
20%	设备安全
10%	物理环境安全
40%	管理安全

6 接入网安全等级保护检测要求

6.1 第1级要求

不作要求。

6.2 第2级要求

6.2.1 接入网网络安全

6.2.1.1 网络拓扑安全

6.2.1.1.1 检测方式

访谈，检查。

6.2.1.1.2 检测对象

网络拓扑图，现场、记录文档。

6.2.1.1.3 检测实施

a） 应访谈网络管理员，询问是否有网络拓扑图，是否有光缆/管道的在线监测措施，是否有光缆/管道的使用状态记录；

b） 应检查光缆/管道的使用年限，查看其是否超过设计使用年限，对于超过设计使用年限要求的光缆/管道应检查是否具有在线监测措施，是否定期记录光缆/管道使用状态；

c） 应检查网络拓扑图，查看其与当前运行情况是否一致。

6.2.1.2 网络访问控制安全

6.2.1.2.1 检测方式

访谈，检查，测试。

6.2.1.2.2 检测对象

设计/验收文档，网络中运行的设备。

6.2.1.2.3 检测实施

a） 应访谈网络管理员，询问接入网是否满足访问控制安全的要求；

b） 应查看设计/验收文档，测试网络中运行的设备是否保证用户在二层域的隔离；

c） 应查看设计/验收文档，测试网络中运行的设备是否能对二层广播风暴进行抑制；

d） 应查看设计/验收文档、检查网管，查看网络中运行的设备是否提供用户 MAC 地址或用户账户或 IP 地址与物理端口（如：DSLAM 线路口、ONU/ONT 物理端口、以太网交换机物理端口、无线接入系统远端站物理端口等）的动态对应列表；

e） 应查看设计/验收文档，测试网络中运行的设备是否具有用户带宽限制、用户端口申请 IP 地址数量的限制、用户端口 MAC 地址数量限制等功能；

f） 应查看设计/验收文档、检查网管，查看网络中运行的设备是否能够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；

g） 应查看设计/验收文档，测试网络中运行的设备是否能对接入到共享物理媒质网络（如：无线接入、PON 等）的用户端设备进行认证；

h） 应查看设计/验收文档，测试网络中采用共享物理媒质网络（如：无线接入、PON 等）的运行的设备是否启用数据加密功能；

i） 应查看设计/验收文档，查看网络中运行设备的远程管理系统是否具有一定安全机制，避免对用户端设备的非法远程配置；

j） 应查看设计/验收文档，查看网络中负责重要用户接入的设备是否开启了双归属功能。

6.2.2 接入网设备安全

6.2.2.1 检测方式

访谈，检查。

6.2.2.2 检测对象

设备入网检测报告，设备入网证，安全检测报告。

6.2.2.3 检测实施

应访谈相关技术支持人员和管理人员，检查设备（主要包括DSL系统、PON系统、以太网接入系统、综合接入系统、LMDS、3.5GHz固定无线接入系统、5.8GHz固定无线接入系统、PWLAN系统、基于802.16d的WiMAX系统等）是否有入网检测报告、设备入网证、安全检测报告等。

6.2.3 接入网物理环境安全

6.2.3.1 有机房的接入网设备物理环境安全

应满足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》中第2级的检测要求。

6.2.3.2 无机房的接入网设备物理环境安全

6.2.3.2.1 检测方式

访谈，检查。

6.2.3.2.2 检测对象

设备放置场地，设计/验收文档，安全管理制度。

6.2.3.2.3 检测实施

a） 应访谈物理安全负责人，询问放置设备的环境条件是否能够满足无机房接入网设备物理环境安全管理需求；

b） 应检查设计/验收文档，查看设备放置地点的承重是否满足设计要求；

c） 应检查设备放置场地是否避免设在强电场、强磁场、易发生火灾、水灾、泥石流、易遭受雷击等的地区；

d） 应检查设计/验收文档，查看设备机箱是否具备防雨、雪、风砂、日照、雷击的措施；

e） 应检查安全管理制度，查看是否有机箱钥匙管理方面的规定；

f） 应检查设计/验收文档，查看设备机箱是否具有环境、电源的告警监测系统；

g） 对重要设备应检查备用电力供应系统（如UPS设备或蓄电池等）是否正常运行。

6.2.4 接入网管理安全

应满足YD/T 1757-2008《电信网和互联网管理安全等级保护检测要求》中第2级的检测要求。

6.3 第3.1级要求

应满足6.2的检测要求。

6.4 第3.2级要求

应满足6.2的检测要求。

6.5 第4级要求

同第3.2级要求。

6.6 第5级要求

待补充。

7 接入网安全风险评估检测要求

7.1 安全风险评估范围

7.1.1 检测方式

访谈，检查。

7.1.2 检测对象

风险评估报告。

7.1.3 检测实施

应访谈风险评估负责人，询问进行接入网风险评估时选择的风险评估范围是什么；检查风险评估报告，查看接入网风险评估范围是否与要求一致。

7.2 安全风险评估内容

7.2.1 检测方式

访谈，检查。

7.2.2 检测对象

风险评估报告。

7.2.3 检测实施

a） 应访谈接入网风险评估负责人、查看风险评估报告，检查接入网风险评估是否覆盖了技术安全和管理安全；

b） 应访谈接入网风险评估负责人、查看风险评估报告，检查接入网风险评估中技术安全是否覆盖了网络安全、设备安全和物理环境安全等方面；

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

7.3 安全风险评估要素

7.3.1 检测方式

访谈，检查。

7.3.2 检测对象

风险评估报告。

7.3.3 检测实施

a） 应访谈风险评估负责人，询问进行接入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，检查接入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） 应访谈风险评估负责人，询问进行接入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，检查接入网风险评估报告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） 应访谈风险评估负责人，询问进行接入网风险评估时评估了哪些资产；查看风险评估报告，检查接入网风险评估时的资产是否包含了各种接入设备（包括各种有线接入系统（如：DSL系统、PON系统、以太网接入系统、综合接入系统等）和无线接入系统（如：LMDS、3.5GHz固定无线接入系统、5.8GHz固定无线接入系统、PWLAN系统、基于802.16d的WiMAX系统等）和物理环境设备包括机房、电力供应系统、电磁防护系统、防火、防水和防潮系统、防静电系统、防雷击系统、温湿度控制系统等，各种设备的系统软件，设备中的重要数据，设备维护人员，各种管理规定和设备文档等。

d） 应访谈风险评估负责人，询问计算接入网各资产的资产价值时考虑了哪些因素；查看风险评估报告，检查接入网风险评估中计算各资产的资产价值是否主要考虑了社会影响力、资产价值和可用性等因素，同时是否采用了合理的计算方法。

e） 应访谈风险评估负责人，询问识别接入网各资产的脆弱性时考虑了哪些方面的脆弱性；查看风险评估报告，检查接入网风险评估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。

f） 应访谈风险评估负责人，询问识别接入网各资产的脆弱性时考虑了哪些方面的脆弱性；查看风险评估报告，检查接入网风险评估中技术脆弱性是否包含了网络脆弱性、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、人员安全管理方面脆弱性、建设管理方面的脆弱性和运维管理方面的脆弱性。

g） 应访谈风险评估负责人，询问对接入网存在哪些威胁；查看风险评估报告，检查接入网风险评估时威胁识别是否包含了环境威胁和人员威胁。

h） 应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，检查接入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） 应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，检查接入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） 应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，检查接入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） 应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，检查接入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。

7.4 安全风险评估赋值原则

7.4.1 检测方式

访谈，检查。

7.4.2 检测对象

风险评估报告。

7.4.3 检测实施

a） 应访谈风险评估负责人，询问接入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，检查接入网各资产的赋值是否从资产的社会影响力、资产价值和可用性三个方面和5个等级进行赋值。

b） 应访谈风险评估负责人，询问接入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，检查接入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，同时是否按照5个等级进行赋值。

c） 应访谈风险评估负责人，询问接入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，检查接入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。

7.5 安全风险评估计算方法

7.5.1 检测方式

访谈，检查。

7.5.2 检测对象

风险评估报告。

7.5.3 检测实施

a） 应访谈风险评估负责人，询问接入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，检查接入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） 应访谈风险评估负责人，询问接入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，检查接入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。

7.6 安全风险评估文件类型

7.6.1 检测方式

访谈，检查。

7.6.2 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。

7.6.3 检测实施

a） 应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） 应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） 应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） 应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） 应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） 应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、类型及严重程度等内容。

g） 应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内容。

h） 应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） 应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） 应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。

7.7 安全风险评估文件记录

7.7.1 检测方式

访谈，检查。

7.7.2 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。

7.7.3 检测实施

a） 应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） 应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） 应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） 应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，检查是否对作废文件作了标识。

e） 应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。

8 接入网灾难备份及恢复检测要求

8.1 第1级要求

不作要求。

8.2 第2级要求

8.2.1 接入网备份数据

8.2.1.1 检测方式

访谈，检查。

8.2.1.2 检测对象

数据备份服务器，设计/验收文档。

8.2.1.3 检测实施

a） 应访谈接入网安全管理人员，询问是否支持关键数据的本地定期备份；

b） 应检查设计/验收文档，查看接入网是否支持关键数据的本地定期备份；

c） 应检查接入网数据备份服务器，查看其与设计文档是否一致。

8.2.2 接入网人员和技术支持能力

8.2.2.1 检测方式

访谈，检查。

8.2.2.2 检测对象

历史值班记录，培训记录。

8.2.2.3 检测实施

a） 应访谈安全管理人员，询问是否有数据备份人员；

b） 应检查历史值班记录，查看是否有数据备份人员；

c） 应检查在职上班人员，查看是否有数据备份人员；

d） 应检查培训记录，查看数据备份人员是否定期得到灾难备份及恢复方面的技能培训。

8.2.3 接入网运行维护管理能力

8.2.3.1 检测方式

访谈，检查。

8.2.3.2 检测对象

管理制度。

8.2.3.3 检测实施

a） 应访谈安全管理人员，询问是否有相应的介质存取、验证和转储管理制度；

b） 应检查接入网相关管理制度，查看其是否具有介质存取、验证和转储管理制度。

8.2.4 接入网灾难恢复预案

8.2.4.1 检测方式

访谈，检查。

8.2.4.2 检测对象

灾难恢复预案，设计/验收文档，管理制度。

8.2.4.3 检测实施

a） 应访谈安全管理人员，询问重要用户的接入网是否具有灾难恢复预案；

b） 应检查重要用户的接入网灾难恢复预案设计/验收文档，查看其是否具备完整的接入网灾难恢复预案；

c） 应检查重要用户的接入网灾难恢复预案，查看其与设计是否一致。

8.3 第 3.1 级要求

应满足8.2的检测要求。

8.4 第 3.2 级要求

应满足8.2的检测要求。

8.5 第 4 级要求

同第3.2级要求。

8.6 第 5 级要求

待补充。