YD

中华人民共和国通信行业标准

YD/T 1737-2008

互联网安全防护检测要求

Security Protection Test Requirements for 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 1736-2008《互联网安全防护要求》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

本标准主要起草人：杨　洋、田慧蓉、冀　晖、刘　楠、白海龙

互联网安全防护检测要求

1 范围

本标准规定了互联网业务及应用系统在安全等级保护、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。

本标准适用于互联网业务及应用系统。

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指导性技术文件的条款。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 5271.8-2001　信息技术 词汇 第8部分：安全

YD/T 1736-2008　互联网安全防护要求

YD/T 1743-2008　接入网安全防护检测要求

YD/T 1745-2008　传送网安全防护检测要求

YD/T 1747-2008　IP 承载网安全防护检测要求

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

YD/T 1757-2008　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

GB/T 5271.8-2001确立的术语和定义，以及下列术语和定义适用于本标准。

3.1

互联网相关系统　Systems of Internet

组成互联网的相关系统包括接入网、传送网、IP承载网等。其中，接入网包括各种有线、无线和卫星接入网等，传送网包括光缆、波分、SDH、卫星等。

3.2

互联网安全等级　Security Classification of Internet

互联网及相关系统重要程度的表征。重要程度从互联网及相关系统受到破坏后，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。

3.3

互联网安全等级保护　Classified Security Protection of Internet

对互联网及相关系统分等级实施安全保护。

3.4

互联网安全检测　Security Testing of Internet

对互联网及相关系统的安全保护能力是否达到相应保护要求进行衡量。

3.5

组织 Organization

组织是由互联网及相关系统中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。

3.6

互联网安全风险 Security Risk of Internet

人为或自然的威胁可能利用互联网及相关系统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。

3.7

互联网安全风险评估 Security Risk Assessment of Internet

指运用科学的方法和手段，系统地分析互联网及相关系统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，防范和化解互联网及相关系统安全风险，将风险控制在可接受的水平，为最大限度地保障互联网及相关系统的安全提供科学依据。

3.8

互联网资产 Asset of Internet

互联网及相关系统中具有价值的资源，是安全防护体系保护的对象。互联网及相关系统中的资产可能以多种形式存在，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 IP 承载网中的路由器、传送网的网络布局。

3.9

互联网资产价值 Asset Value of Internet

互联网及相关系统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。

3.10

互联网威胁 Threat of Internet

可能导致对互联网及相关系统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。

3.11

互联网脆弱性 Vulnerability of Internet

互联网及相关系统资产中存在的弱点、缺陷与不足，不直接对互联网资产造成危害，但可能被互联网威胁所利用从而危及互联网资产的安全。

3.12

互联网灾难 Disaster of Internet

由于各种原因，造成互联网及相关系统故障或瘫痪，使互联网及相关系统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。

3.13

互联网灾难备份 Backup for Disaster Recovery of Internet

为了互联网及相关系统灾难恢复而对相关网络要素进行备份的过程。

3.14

互联网灾难恢复 Disaster Recovery of Internet

为了将互联网及相关系统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。

3.15

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，获取证据以检查安全等级保护、安全风险评估、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。

3.16

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，获取证据以检查安全等级保护、安全风险评估、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。

3.17

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，获取证据以检查安全等级保护、安全风险评估、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
CGI	Common Gateway Interface	公共网关接口
CHAP	Challenge Handshake Authentication Protocol	质询握手认证协议
DoS	Denial of Service	拒绝服务
DNS	Domain Name System	域名系统
FTP	File Transfer Protocol	文件传输协议
MTBF	Mean Time Between Failures	平均故障间隔时间
MTTR	Mean Time To Repair	平均维修时间
RPC	Remote Rrocedure Call	远程过程调用
TCP	Transfer Control Protocol	传输控制协议
SMTP	Simple Mail Transfer Protocol	简单邮件传输协议
VPN	Virtual Private Network	虚拟专用网

5 互联网安全防护检测概述

5.1 互联网安全防护检测范围

互联网安全防护检测范围是我国具有管辖权的互联网业务及应用系统以及互联网相关系统。根据YD/T 1736-2008《互联网安全防护要求》，本标准主要对互联网业务及应用系统的安全等级保护、安全

风险评估、灾难备份及恢复等工作的实施进行检测。接入网安全防护检测的具体要求参见YD/T 1743-2008《接入网安全防护检测要求》，传送网安全防护检测的具体要求参见YD/T 1745-2008《传送网安全防护检测要求》，IP承载网安全防护检测的具体要求参见YD/T 1747-2008《IP承载网安全防护检测要求》。

互联网安全等级保护的检测范围确定以后，安全风险评估的检测范围、灾难备份及恢复的检测范围应与安全等级保护的检测范围相一致。

5.2 互联网安全防护检测对象

互联网业务及应用系统的安全防护检测对象是各个互联网业务及应用系统。

应按照检测对象拥有者的不同，分别对其所拥有的相应检测对象进行安全防护检测。

5.3 互联网安全防护检测内容

与互联网安全防护要求相对应，互联网安全防护检测内容主要包括以下3个部分：

——互联网安全等级保护检测

主要包括业务及应用安全检测、设备安全检测、物理环境安全检测、管理安全检测等。

——互联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、安全风险评估赋值检测、安全风险评估计算检测、安全风险评估文件类型检测、安全风险评估文件记录检测等。

——互联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、灾难恢复预案检测等。

5.4 互联网安全防护检测结果判定

互联网安全防护检测包括对互联网的安全等级保护、安全风险评估、灾难备份及恢复3个部分的检测，应对3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。

对每一部分中的每一个检测项，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）。参照表1将各检测项的评价等级换算成评分，各检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3个部分的总分数，根据总分数可分别对互联网的安全等级保护、安全风险评估、灾难备份及恢复3个部分的检测结果进行等级化评定，总分数和评定等级的关系如表2所示。在计算总分数的过程中，应充分考虑到各检测项在安全防护检测要求中所占的比重，例如表3给出了互联网业务及应用系统安全等级保护各检测子类所占的比重。互联网安全防护检测的结果还应充分考虑到各相关系统的检测结果。

表1 测试项评分方法

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
$4.5 \leqslant x \leqslant 5$	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

表3 互联网业务及应用系统安全等级保护检测子类所占比重

比重（%）	子 类
40	业务及应用安全
5	设备安全
15	物理环境安全
40	管理安全

6 互联网安全等级保护检测要求

6.1 概述

本标准主要对互联网业务及应用系统提出安全防护检测要求。目前运营的互联网业务包括互联网域名服务、互联网数据中心、互联网接入服务、互联网信息服务、在线数据处理与交易处理、移动互联网信息服务等，主流的互联网信息服务包括Web浏览、电子邮件、FTP、公众信息发布等，主流的移动互联网信息服务包括信息浏览、电子邮件、下载业务等。随着互联网业务及应用的发展，本标准将不断补充完善。

对互联网业务及应用安全进行检测时，可根据检测对象提供的业务及应用进行相应检测，未提供的应用不作检测要求。

6.2 第1级要求

不作要求。

6.3 第2级要求

6.3.1 互联网业务及应用安全检测要求

6.3.1.1 通用安全检测要求

6.3.1.1.1 检测方式

访谈，检查，测试。

6.3.1.1.2 检测对象

互联网业务及应用系统的相关服务器和用户端网络，相关服务器检测报告，相关服务器日志记录，相关服务器安全状况检查记录，现场。

6.3.1.1.3 检测实施

a）应访谈相关技术支持人员和管理人员，询问在保护用户隐私、不泄露用户相关信息方面是否存在相应机制；

b）应检查相关服务器是否均安装并启用了防火墙和防病毒软件，相关软件是否进行了合理配置，并检查相关服务器的病毒感染情况，确认相关服务器是否具备防病毒能力；

c）在允许的情况下，可对相关服务器进行模拟攻击测试，确认相关服务器是否具有一定的防DoS攻击、防黑客攻击及防范其他来自内部和外部各种攻击的能力；

d）应检查相关服务器的操作系统、防火墙、防病毒软件、应用软件等，确认是否均已进行了适当更新；

e）应访谈相关技术支持人员和管理人员，确认对相关服务器安全状况进行定期检查的情况，检查是否留有相关服务器安全状况检查记录；

f）应测试是否可通过IP地址、用户名、子网域名等方式限制对相关服务器的管理、配置和相关操作；

g）应检查相关服务器操作日志是否有相应操作记录，应在现场测试相关服务器操作日志的记录情况；

h）应检查相关服务器的读写权限和访问控制策略设置，检查所有用户名是否均有口令，口令是否足够复杂，口令是否经常更换，是否有不必要的开放端口；

i）应访谈相关技术支持人员和管理人员，确认互联网在向用户提供应用时是否可保证相关系统之间传送信息的真实性和完整性，相关系统之间的认证、授权、安全协议及安全算法是否满足相应标准的要求；

j）互联网业务及应用系统的用户端网络安全具体检测要求参见YD/T 1747-2008《IP承载网安全防护检测要求》第2级要求。

6.3.1.2 互联网域名服务安全检测要求

6.3.1.2.1 检测方式

访谈，检查，测试。

6.3.1.2.2 检测对象

DNS服务器、互联网域名注册、互联网域名交易等相关服务器，系统设计/验收文档，相关服务器安全状况检查记录、日志记录。

6.3.1.2.3 检测实施

a）应访谈相关技术支持及管理人员，询问是否有相应机制和制度对要注册的域名进行审查，防止不良域名的出现。

b）应访谈相关技术支持及管理人员，询问是否有防止重要数据被篡改和破坏的相应机制。

c）针对互联网域名解析服务，应访谈相关技术人员，查看系统设计/验收文档,判断是否从设计上保证在排除外力因素（非本企业可控制的因素）的情况下，DNS服务器组的可用性≥99.99%；查看DNS服务器安全状况检查记录，在排除外力因素（非本企业可控制的因素）的情况下，判断DNS服务器组的可用性是否≥99.99%。

d）针对不同的服务，应检查相关服务器的日志记录，检查是否有相应的服务记录，例如域名解析请求的记录，并保留一定期限，检查是否出现过相关日志数据和信息被篡改和破坏的情况，并保留了历史记录。

6.3.1.3 互联网数据中心安全检测要求

6.3.1.3.1 检测方式

访谈，检查，测试。

6.3.1.3.2 检测对象

客户托管、代维或租用的等与互联网数据中心服务相关的服务器，相关服务器日志记录。

6.3.1.3.3 检测实施

a）应访谈相关管理人员，询问是否有进出数据中心的管理制度，确保只有授权的人才能进入相关机房；

b）应访谈相关技术及管理人员，询问是否有硬件、软件、数据以及应用的授权访问控制机制，确保只有授权的人才能对相关服务器进行访问、管理、配置等操作；

c）针对托管/代维的服务器，应访谈相关技术及管理人员，询问按照托管/代维的要求对网络带宽、电力系统、环境等进行管理的机制，并判断是否满足相关要求；

d）针对代维的服务器，应访谈相关技术及管理人员，询问按照代维的要求对服务器进行维护管理所采取的机制和措施，并判断是否满足相关要求；

e）根据客户的要求，如果需要对相关服务器的操作访问等进行记录，则检查相关服务器的日志记录，判断是否有客户所要求的日志记录，并保留了一定的期限，检查是否出现过相关日志数据和信息被篡改和破坏的情况，并保留了历史记录。

6.3.1.4 互联网接入服务安全检测要求

6.3.1.4.1 检测方式

访谈，检查，测试。

6.3.1.4.2 检测对象

宽带网络接入服务器或网络接入服务器，宽带网络接入服务器或网络接入服务器检测报告，互联网接入服务系统设计/验收文档，宽带网络接入服务器或网络接入服务器日志记录，宽带网络接入服务器或网络接入服务器安全状况检查记录、互联网接入服务安全检查记录、安全事件处理记录，现场。

6.3.1.4.3 检测实施

a）应访谈相关技术人员，查看系统设计/验收文档，判断是否从设计上保证在排除外力因素（非本企业可控制的因素）的情况下，互联网接入服务的可用性≥99.99%；查看互联网接入服务安全检查记录，判断在排除外力因素（非本企业可控制的因素）的情况下，互联网接入服务可用性是否≥99.99%。

b）应查看相关安全事件处理记录，判断互联网接入服务是否具有一定的可恢复性，在业务中断后，是否能够在可接受时间范围内（业务恢复时间间隔平均≤4h，最长为8h）恢复业务。

c）应检查宽带网络接入服务器或网络接入服务器的日志记录，检查是否对用户接入互联网的情况（至少包括上网用户的上网事件、用户账号、因特网地址或者域名、主叫电话号码等信息）进行了记录，检查是否保留了一定期限（至少60天），检查是否出现过相关数据和信息被篡改和破坏的情况，并保存了相应历史记录。

6.3.1.5 互联网信息服务安全检测要求

6.3.1.5.1 Web 浏览安全检测要求

6.3.1.5.1.1 检测方式

访谈，检查，测试。

6.3.1.5.1.2 检测对象

DNS服务器，Web服务器，数据库服务器，相关服务器日志记录。

6.3.1.5.1.3 检测实施

a）应检查相关服务器日志记录，判断是否出现过相关数据和页面被篡改和破坏的情况，并保存了相应的历史记录；

b）应测试Web服务器是否存在物理路径泄露、CGI源代码泄露、目录遍历、执行任意命令、缓冲区溢出等常见安全隐患；

c）应检查Web服务器是否打开了不必要的内嵌网络服务；

d）应测试Web服务器是否在用户浏览过程中在用户端自动安装恶意软件；

e）应测试Web服务器是否具有监控用户下载软件病毒携带情况的功能，测试相应的自动处理措施；

f）应访谈相关技术人员，询问对外提供Web浏览服务的平台是否有相应的机制确保不向公众发布有害信息；

g）应检查相关服务器的日志记录，检查是否记录了向公众发布的信息内容及其发布时间、互联网地址或者域名等，并保存60日，检查是否出现过相关数据和信息被篡改和破坏的情况，并保存了相应历史记录；

h）应检查Web服务器日志记录，检查是否有对用户访问Web服务器等操作的记录，检查是否出现过相关数据和信息被篡改和破坏的情况，并保留了历史记录。

6.3.1.5.2 电子邮件安全检测要求

6.3.1.5.2.1 检测方式

访谈，检查，测试。

6.3.1.5.2.2 检测对象

DNS服务器，电子邮件服务器，相关服务器日志记录。

6.3.1.5.2.3 检测实施

a）应通过模拟攻击的手段测试电子邮件服务器是否具有监控用户收发电子邮件病毒携带情况的功能，测试所采取的相应处理措施；

b）应询问相关技术人员，检查是否有防范垃圾邮件的机制，判断该机制是否能有效确保正常用户邮件业务的使用；

c）应检查电子邮件服务器日志记录，检查是否有对用户收发邮件等操作的记录，检查是否出现过相关数据和信息被篡改和破坏的情况，并保留了历史记录。

6.3.1.5.3 FTP 安全检测要求

6.3.1.5.3.1 检测方式

访谈，检查，测试。

6.3.1.5.3.2 检测对象

DNS服务器，FTP服务器，相关服务器日志记录。

6.3.1.5.3.3 检测实施

a）应通过模拟攻击的手段测试FTP服务器是否有监控用户上传文件病毒携带情况的功能，测试所采取的相应处理措施；

b）应测试FTP服务器是否有禁止单个IP地址、IP地址段、用户名、子网域进行登陆、浏览、创建目录、删除目录或文件、上传、下载等FTP相关操作的功能；

c）在单个IP地址、IP地址段、用户名、子网域的连接数量或连接频率超过预定上限的条件下，应测试FTP服务器是否能够拒绝其连接请求；

d）应检查FTP服务器日志记录，检查是否有对用户上传下载等操作的记录情况，检查是否出现过相关数据和信息被篡改和破坏的情况，并保留了历史记录。

6.3.1.5.4 公众信息发布安全检测要求

6.3.1.5.4.1 检测方式

访谈，检查，测试。

6.3.1.5.4.2 检测对象

DNS服务器，公众信息发布服务器，相关服务器日志记录。

6.3.1.5.4.3 检测实施

a）应通过模拟攻击的手段测试对公众提供信息发布服务的平台是否具有实时监控用户发布和评论的文字、图片、音频、视频文件的病毒携带情况的功能，测试所采取的相应处理措施；

b）应访谈相关技术人员，并检查对公众提供信息发布服务的平台是否有实时机制（例如利用软件进行关键字过滤，人工实时检查等）过滤向公众发布的各种文本信息内容，是否采用技术或人工手段有效防止其他类型（图像、音频、视频等）有害信息通过业务网络向公众传播；

c）应访谈相关技术和管理支持人员，询问是否有有害信息检查机制和投诉处理制度；

d）应检查公众信息发布服务器的日志记录，检查是否记录了向公众发布的信息内容及其发布时间、互联网地址或者域名等，并保存60日，检查是否出现过相关数据和信息被篡改和破坏的情况，并保存了相应历史记录；

e）应检查公众信息发布服务器日志记录，检查是否有对用户发布信息、浏览信息、评论、下载等操作的记录，检查是否出现过相关数据和信息被篡改和破坏的情况，并保留了历史记录。

6.3.1.6 在线数据处理与交易处理安全检测要求

6.3.1.6.1 检测方式

访谈，检查，测试。

6.3.1.6.2 检测对象

DNS服务器，在线数据处理与交易处理服务器，在线数据处理与交易处理系统设计/验收文档，相关服务器安全状况检查记录、安全事件处理记录、日志记录，在线数据处理与交易处理业务安全检查记录。

6.3.1.6.3 检测实施

a）应访谈相关技术人员，查看系统设计/验收文档，判断是否从设计上保证在排除外力因素（非本企业可控制的因素）的情况下，业务的可用性≥99.99%；查看在线数据处理与交易处理安全检查记录，在排除外力因素（非本企业可控制的因素）的情况下，判断业务的可用性是否≥99.99%。

b）应访谈相关技术支持人员，询问采用何种加密和验证技术机制保证业务数据传输和存储的安全性，保证业务资源的保密性和完整性。

c）应访谈相关技术支持人员，询问是否有相应的机制例如数字签名机制，确保业务信息真实不可抵赖。

d）应访谈相关技术支持人员，询问是否有所有业务数据的可靠备份，以及在业务中断后，是否能够利用备份数据在可接受时间范围内（业务恢复时间间隔平均≤4h，最长为8h）恢复业务，且业务数据不丢失；应查看相关安全事件处理记录，判断所提供业务是否具有一定的可恢复性，在业务中断后，是否能够在可接受时间范围内（业务恢复时间间隔平均≤4h，最长为8h）恢复业务。

e）应访谈相关技术支持人员，询问是否采用有效的接入认证与授权机制（例如数字签名机制）来保证业务的用户的合法性以及业务本身的安全性。

f）应检查在线数据处理与交易处理服务器日志记录，检查是否有用户业务日志（包括详细的交易事件信息、操作步骤、时间等），并且做永久或一定期限（至少3个月）的保存，并检查是否出现过相关数据和信息被篡改和破坏的情况，并保留了历史记录。

6.3.1.7 移动互联网信息服务安全检测要求

应根据服务类型，按照6.3.1.5节互联网信息服务的安全要求进行检测。

6.3.2 互联网设备安全检测要求

6.3.2.1 检测方式

访谈，检查。

6.3.2.2 检测对象

互联网业务及应用系统的相关服务器、用户端网络设备入网检测报告。

6.3.2.3 检测实施

应检查互联网业务及应用系统的相关服务器（包括DNS服务器、域名注册/交易服务器、宽带网络接入服务器、网络接入服务器、Web服务器、电子邮件服务器、FTP服务器、公众信息发布服务器、在线数据处理与交易处理服务器、数据库服务器等）、用户端网络设备（包括路由器、交换机、网管系统设备等）是否具有相应的入网检测报告和入网许可证。

6.3.3 互联网物理环境安全检测要求

应按照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》第2级的要求进行检测。

6.3.4 互联网管理安全检测要求

应按照YD/T 1757-2008《电信网和互联网管理安全等级保护检测要求》第2级的要求进行检测。

6.4 第3.1级要求

6.4.1 互联网业务及应用安全检测要求

6.4.1.1 通用安全检测要求

6.4.1.1.1 检测方式

访谈，检查，测试。

6.4.1.1.2 检测对象

互联网业务及应用系统的相关服务器和用户端网络，相关服务器检测报告，相关服务器安全日志，相关服务器安全状况检查记录，现场。

6.4.1.1.3 检测实施

除按照6.3.1.1节的要求进行检测之外，还应按照本节内容进行检测：

a）应检查相关服务器的检测报告，确认MTBF是否均大于10 000h；

b）应检查相关服务器的检测报告，确认MTTR是否均小于1h；

c）应检查相关服务器的处理器、主存、板卡、电源等重要部件是否有冗余配置；

d）应测试相关服务器的操作系统是否存在非法文件访问、系统后门、RPC漏洞、Unicode漏洞、缓冲区溢出漏洞、文件名错误解码漏洞等常见缺陷和隐患；

e）应测试DNS服务器是否存在名字欺骗、信息隐藏、缓冲区溢出等常见安全隐患；

f）应检查是否配备有多台相关服务器；

g）应检查相关服务器的是否具有相应的数据备份机制；

h）针对某项互联网业务及应用，应在个别服务器中止运行时测试该业务及应用的提供情况和系统的运行情况，判断相应的备份机制是否能保证个别服务器中止运行不会引起互联网业务及应用的终端或系统瘫痪；

i）应检查在向用户提供业务及应用之前，用户认证信息的传输是否采用加密机制；

j）互联网业务及应用系统的用户端网络安全具体检测要求参见YD/T 1747-2008《IP承载网安全防护检测要求》第3.1级要求。

6.4.1.2 互联网域名服务安全检测要求

6.4.1.2.1 检测方式

访谈，检查，测试。

6.4.1.2.2 检测对象

DNS服务器、互联网域名注册、互联网域名交易等相关服务器，相关服务器安全状况检查记录、安全事件处理记录、日志记录。

6.4.1.2.3 检测实施

除按照6.3.1.2节的要求进行检测之外，还应按照本节内容进行检测：

a）针对域名解析服务，应查看相关安全事件处理记录，判断在服务中断后，能否在满足6.3.1.2节的c）的检测要求的情况下，尽快恢复域名解析服务。

b）应访谈相关技术支持人员，是否有重要数据例如域名信息的备份机制。

c）应访谈相关技术支持人员，询问是否能根据相关服务器日志信息进行入侵检测和入侵分析，询问是否在发生严重入侵事件时有相应的报警机制；查看相应的日志记录，判断在检测到入侵行为时，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，是否有在发生严重入侵事件时的报警记录。

6.4.1.3 互联网数据中心安全检测要求

6.4.1.3.1 检测方式

访谈，检查，测试。

6.4.1.3.2 检测对象

客户托管或租用的服务器，相关服务器安全状况检查记录、安全事件处理记录、日志记录。

6.4.1.3.3 检测实施

除按照6.3.1.3节的要求进行检测之外，还应按照本节内容进行检测：

a）应检查是否有相关的机制确保数据中心某个客户的服务异常不会导致为其他客户提供服务的异常，例如针对多个客户使用同一个虚拟主机的情况，某个客户的业务出现故障或异常，不应影响其他客户的业务。

b）如果按照客户要求记录了相关服务器的操作访问日志，应访谈相关技术支持人员，询问是否能根据相关服务器日志信息进行入侵检测和入侵分析，询问是否在发生严重入侵事件时有相应的报警机制；查看相应的日志记录，判断在检测到入侵行为时，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，是否有在发生严重入侵事件时的报警记录。

6.4.1.4 互联网接入服务安全检测要求

6.4.1.4.1 检测方式

访谈，检查，测试。

6.4.1.4.2 检测对象

宽带网络接入服务器或网络接入服务器，宽带网络接入服务器或网络接入服务器检测报告，现场。

6.4.1.4.3 检测实施

除按照6.3.1.4节的要求进行检测之外，还应按照本节内容进行检测：

a）应查看宽带网络接入服务器或网络接入服务器检测报告、或通过测试判断是否具有通过用户名等方式识别并确认用户身份的功能；

b）应查看宽带网络接入服务器或网络接入服务器检测报告、或通过测试判断是否支持CHAP、802.1x等不同的认证协议对用户进行身份验证的功能；

c）应查看宽带网络接入服务器或网络接入服务器检测报告、或通过测试判断是否支持队列调度机制、接入带宽控制机制等不同策略来控制用户接入和对资源访问的功能；

d）应查看宽带网络接入服务器或网络接入服务器检测报告、或通过测试判断是否具有控制同一用户建立TCP会话的数量的功能，是否具有根据用户类型对能够建立的TCP会话数量进行配置的功能；

e）应查看宽带网络接入服务器或网络接入服务器检测报告、或通过测试判断是否具有通过ACL等机制实现对资源的控制、监控的功能；

f）应查看宽带网络接入服务器检测报告、或通过测试判断是否支持VPN的相关功能。

6.4.1.5 互联网信息服务安全检测要求

6.4.1.5.1 Web浏览安全检测要求

6.4.1.5.1.1 检测方式

访谈，检查，测试。

6.4.1.5.1.2 检测对象

DNS服务器，Web服务器，数据库服务器，相关服务器日志记录。

6.4.1.5.1.3 检测实施

除按照6.3.1.5.1节的要求进行检测之外，还应按照本节内容进行检测：

a）应测试Web服务器是否具有禁止部分IP地址、子网域进行Web浏览的功能。

b）应访谈相关技术支持人员和管理人员，检查Web服务器是否有对各种执行程序的访问进行控制的相应机制。

c）应访谈相关技术支持人员，询问是否能根据Web服务器的日志信息进行入侵检测和入侵分析，询问是否在发生严重入侵事件时有相应的报警机制；查看相应的日志记录，判断在检测到入侵行为时，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，是否有在发生严重入侵事件时的报警记录。

6.4.1.5.2 电子邮件安全检测要求

6.4.1.5.2.1 检测方式

访谈，检查，测试。

6.4.1.5.2.2 检测对象

DNS服务器，电子邮件服务器，相关服务器日志记录。

6.4.1.5.2.3 检测实施

除按照6.3.1.5.2节的要求进行检测之外，还应按照本节内容进行检测：

a）应测试电子邮件服务器是否支持强制SMTP认证；

b）应测试电子邮件服务器是否支持关闭自动转发邮件的功能；

c）应测试电子邮件服务器是否支持禁止部分IP地址、用户名、子网域进行收发邮件等操作的功能；

d）应测试电子邮件服务器支持创建、修改、保存、删除黑名单和白名单等功能，是否可据此阻止或放行相关电子邮件；

e）在特定电子邮件的转发次数超过预定上限的条件下，应测试电子邮件服务器是否可拒绝其继续转发的操作请求；

f）在特定电子邮件的收信人数量超过预定上限的条件下，应测试电子邮件服务器是否可拒绝其发送的操作请求；

g）在特定电子邮件的附件数量超过预定上限的条件下，应测试电子邮件服务器是否可拒绝其发送的操作请求；

h）在特定电子邮件的大小超过预定上限的条件下，应测试电子邮件服务器是否可拒绝其发送的操作请求；

i）在单个IP地址或用户名的连接数量或连接频率超过预定上限的条件下，应测试电子邮件服务器是否可拒绝其连接请求；

j）应通过隐藏发信人地址、隐藏消息来源、含有虚假的发件人、含有虚假的中继消息、特定关键字等方式对电子邮件服务器进行模拟攻击，测试电子邮件服务器对电子邮件地址、标题等关键信息进行扫描、检测、过滤、拦截的功能；

k）应访谈相关技术支持人员，询问是否能根据电子邮件服务器的日志信息进行入侵检测和入侵分析，询问是否在发生严重入侵事件时有相应的报警机制；查看相应的日志记录，判断在检测到入侵行为时，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，是否有在发生严重入侵事件时的报警记录。

6.4.1.5.3 FTP 安全检测要求

6.4.1.5.3.1 检测方式

访谈，检查，测试。

6.4.1.5.3.2 检测对象

DNS服务器，FTP服务器，相关服务器日志记录。

6.4.1.5.3.3 检测实施

除按照6.3.1.5.3节的要求进行检测之外，还应按照本节内容进行检测：

a）应测试FTP服务器是否能对一个访问账户或一个请求进程占用的资源进行限制。

b）应访谈相关技术支持人员，询问是否能根据FTP服务器的日志信息进行入侵检测和入侵分析，询问是否在发生严重入侵事件时有相应的报警机制；查看相应的日志记录，判断在检测到入侵行为时，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，是否有在发生严重入侵事件时的报警记录。

6.4.1.5.4 公众信息发布安全检测要求

6.4.1.5.4.1 检测方式

访谈，检查，测试。

6.4.1.5.4.2 检测对象

DNS服务器，公众信息发布服务器，相关服务器日志记录。

6.4.1.5.4.3 检测实施

除按照6.3.1.5.4节的要求进行检测之外，还应按照本节内容进行检测：

a）应测试公众信息发布服务器是否具有禁止部分IP地址、用户名、子网域发布信息、浏览信息、评论和下载的功能。

b）应访谈相关技术支持人员，询问是否能根据公众信息发布服务器的日志信息进行入侵检测和入侵分析，询问是否在发生严重入侵事件时有相应的报警机制；查看相应的日志记录，判断在检测到入侵行为时，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，是否有在发生严重入侵事件时的报警记录。

6.4.1.6 在线数据处理与交易处理安全检测要求

应按照6.3.1.6节的要求进行检测。

6.4.1.7 移动互联网信息服务安全检测要求

应根据服务类型，按照6.3.1.7节互联网信息服务的安全要求进行检测。

6.4.2 互联网设备安全检测要求

应按照6.3.2节的要求进行检测。

6.4.3 互联网物理环境安全检测要求

应按照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》第3.1级的要求进行检测。

6.4.4 互联网管理安全检测要求

应按照YD/T 1757-2008《电信网和互联网管理安全等级保护检测要求》第3.1级的要求进行检测。

6.5 第3.2级要求

与第3.1级要求相同。

6.6 第4级要求

同第3.2级要求。

6.7 第5级要求

待补充。

7 互联网安全风险评估检测要求

7.1 互联网安全风险评估范围

7.1.1 检测方式

访谈，检查。

7.1.2 检测对象

安全风险评估报告。

7.1.3 检测实施

a）应访谈互联网安全风险评估负责人，询问进行互联网安全风险评估时，选择的安全风险评估范围是什么，并检查互联网安全风险评估报告，查看其安全风险评估范围是否与要求相一致。

b）应访谈互联网安全风险评估负责人，询问进行互联网安全风险评估时，安全风险评估范围中各个组成部分的评估权重因子如何分配；并检查互联网安全风险评估报告，查看安全风险评估范围中各个组成部分的综合计算方法的合理性。

7.2 互联网安全风险评估内容

7.2.1 检测方式

访谈，检查。

7.2.2 检测对象

安全风险评估报告。

7.2.3 检测实施

a）应访谈互联网安全风险评估负责人，并检查互联网安全风险评估报告，判断安全风险评估相关内容是否覆盖了技术安全和管理安全；

b）应访谈互联网安全风险评估负责人，并检查互联网安全风险评估报告，查看技术安全中是否覆盖了应用安全、网络安全、设备安全和物理环境安全；

c）应访谈互联网安全风险评估负责人，并检查互联网安全风险评估报告，查看管理安全中是否覆盖了安全管理机构、安全管理制度、人员安全管理、系统建设管理、系统运维管理等方面。

7.3 互联网安全风险评估要素

7.3.1 检测方式

访谈，检查。

7.3.2 检测对象

安全风险评估报告，历史记录。

7.3.3 检测实施

a）应访谈互联网安全风险评估负责人，询问进行风险评估时采用了哪些风险评估要素；查看互联网安全风险评估报告，检查安全风险评估要素是否包含了资产、威胁、脆弱性、安全措施、风险和残余风险等要素。

b）应访谈互联网安全风险评估负责人，询问进行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，检查互联网安全风险评估报告是否包含了与评估要素密切相关的属性的业务战略、资产价值、安全需求和安全事件等属性。

c）应访谈互联网安全风险评估负责人，询问进行风险评估时评估了哪些资产；查看互联网安全风险评估报告，检查资产是否包括互联网业务及应用系统的相关服务器（如DNS服务器、Web服务器、电子邮件服务器、FTP服务器、公众信息发布服务器、在线数据处理与交易处理服务器、数据库服务器、宽带网络接入服务器、网络接入服务器等）、和各种互联网业务及应用正常提供相关的用户端网络设备（如路由器、交换机、网管系统设备等）、和各种互联网业务及应用正常提供相关的用户端网络链路、相关

服务器和用户端网络设备的操作维护系统、相应的数据存储和备份介质、相关服务器和用户端网络设备的操作系统和应用软件、相关服务器和用户端网络设备的操作维护系统软件、相关服务器和用户端网络设备的重要数据、互联网提供的各种业务及应用、相关服务器和用户端网络设备维护人员、各种管理规定、相关服务器和用户端网络设备文档。

d）应访谈互联网安全风险评估负责人，询问计算互联网各资产的资产价值时考虑了哪些因素；查看互联网安全风险评估报告，检查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）应访谈互联网安全风险评估负责人，询问识别互联网各资产脆弱性时考虑了哪些方面的脆弱性；查看互联网安全风险评估报告，检查互联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；技术脆弱性是否包含了业务及应用脆弱性、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、运维管理方面的脆弱性。

f）应访谈互联网安全风险评估负责人，询问对互联网存在哪些威胁；查看互联网安全风险评估报告，检查威胁是否包含了技术威胁、环境威胁和人为威胁；环境威胁是否包括自然界不可抗的威胁和其他物理威胁，人为威胁是否包括恶意和非恶意等类型。

g）应访谈互联网安全风险评估负责人，询问威胁识别的依据是什么；查看互联网安全风险评估报告，检查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并综合考虑。

h）应访谈互联网安全风险评估负责人，询问风险值的计算方法；查看互联网安全风险评估报告，检查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。

i）应访谈互联网安全风险评估负责人，询问确定风险阈值的方法；查看互联网安全风险评估报告，检查确定的风险阈值是否合理，是否与资产所在业务及应用系统的安全等级相结合。

j）应访谈互联网安全风险评估负责人，并检查互联网安全风险评估报告，查看对于不可接收的互联网安全风险，是否制定了相应的安全风险处理计划以及采用安全风险处理计划以后，互联网风险值是否满足阈值要求。

k）应访谈互联网安全风险评估负责人，并检查互联网安全风险评估报告，查看互联网安全风险评估时发现的主要问题及其解决方案，同时检查历史记录，查看互联网安全风险评估并采取安全措施后，网络的安全性是否提高。

7.4 互联网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

安全风险评估报告。

7.4.3 检测实施

a）应访谈互联网安全风险评估负责人，询问风险评估时对资产的赋值遵循了什么样的原则；查看互联网安全风险评估报告，检查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）应访谈互联网安全风险评估负责人，询问风险评估时对脆弱性的赋值遵循了什么样的原则；查看互联网安全风险评估报告，检查脆弱性的赋值是否综合考虑赋值对象对资产损害程度、技术实现的难易程度、脆弱性流行程度等多个方面因素，同时是否按照5个等级进行赋值。

c）应访谈互联网安全风险评估负责人，询问风险评估时对威胁的赋值遵循了什么样的原则；查看互联网安全风险评估报告，查看威胁的赋值是否依据经验和（或）有关的统计数据来进行分析，同时是否按照5个等级进行赋值。

7.5 互联网安全风险评估赋值计算方法

7.5.1 检测方式

访谈，检查。

7.5.2 检测对象

安全风险评估报告。

7.5.3 检测实施

a）应访谈互联网安全风险评估负责人，询问风险评估中采用了什么样的方法计算资产价值；查看互联网安全风险评估报告，检查资产价值计算方法是否合理，是否具有对于所采用计算方法的理论分析。

b）应访谈互联网安全风险评估负责人，询问风险评估中采用了什么样的方法计算风险值；查看互联网安全风险评估报告，检查安全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 互联网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，风险处理计划，风险评估记录等风险评估文件。

7.6.3 检测实施

a）应访谈互联网安全风险评估负责人，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）应访谈互联网安全风险评估负责人，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涉及的各种资产、威胁、脆弱性识别和判断依据等内容。

c）应访谈互联网安全风险评估负责人，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）应访谈互联网安全风险评估负责人，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。

e）应访谈互联网安全风险评估负责人，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。

f）应访谈互联网安全风险评估负责人，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。

g）应访谈互联网安全风险评估负责人，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。

h）应访谈互联网安全风险评估负责人，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。

i）应访谈互联网安全风险评估负责人，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 互联网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）应访谈互联网安全风险评估负责人，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）应访谈互联网安全风险评估负责人，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）应访谈互联网安全风险评估负责人，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）应访谈互联网安全风险评估负责人，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）应访谈互联网安全风险评估负责人，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 互联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 冗余系统、冗余设备及冗余链路检测要求

8.2.1.1 检测方式

访谈，检查。

8.2.1.2 检测对象

互联网业务及应用系统，演练记录，历史记录。

8.2.1.3 检测实施

应检查演练记录和历史记录，查看互联网业务及应用系统的灾难恢复时间是否满足相关要求。

8.2.2 备份数据检测要求

8.2.2.1 检测方式

访谈，检查。

8.2.2.2 检测对象

互联网业务及应用系统，设计/验收文档，数据备份服务器，演练记录，历史记录。

8.2.2.3 检测实施

a）应访谈安全管理和技术人员，询问互联网业务及应用系统是否有关键数据备份机制；

b）应检查互联网业务及应用系统在备份数据方面的灾难备份及恢复能力，查看设计/验收文档，判断互联网业务及应用系统支持关键数据（如系统配置数据、管理员操作维护记录、用户信息等）的数据容灾备份能力是否满足要求；

c）应检查互联网业务及应用系统的数据备份服务器，查看其与设计文档是否一致；

d）应检查演练记录和历史记录，查看互联网业务及应用系统的数据备份范围和时间间隔、数据恢复能力是否满足相关要求。

8.2.3 人员和技术支持能力检测要求

8.2.3.1 检测方式

访谈，检查。

8.2.3.2 检测对象

机房运行管理人员，历史值班记录。

8.2.3.3 检测实施

应访谈安全管理相关人员，查看历史值班记录，检查是否有负责互联网业务及应用灾难备份及恢复的机房管理人员，检查相关人员对灾难备份及恢复的技术支持能力。

8.2.4 运行维护管理能力检测要求

8.2.4.1 检测方式

访谈，检查。

8.2.4.2 检测对象

机房运行管理制度，介质存取、验证和转储管理制度。

8.2.4.3 检测实施

a）应访谈安全管理人员，并查看机房运行管理制度，检查是否有针对灾难备份及恢复的机房运行管理制度；

b）应访谈安全管理人员，询问并查看介质存取、验证和转储管理制度，检查是否有针对灾难备份及恢复的介质存取、验证和转储管理制度，是否可确保相关服务器、用户端网络设备备份数据的授权访问。

8.2.5 灾难恢复预案检测要求

8.2.5.1 检测方式

访谈，检查。

8.2.5.2 检测对象

灾难恢复预案，设计/验收文档。

8.2.5.3 检测实施

应访谈安全管理人员，并查看灾难恢复预案，检查是否有完整的互联网业务及应用系统灾难恢复预案，检查是否与设计/验收文档一致。

8.3 第3.1级要求

8.3.1 冗余系统、冗余设备及冗余链路检测要求

8.3.1.1 检测方式

访谈，检查。

8.3.1.2 检测对象

互联网业务及应用系统，设计/验收文档。

8.3.1.3 检测实施

除按照8.2.1节的要求进行检测之外，还应按照本节内容进行检测：

a）应访谈安全管理人员，询问互联网业务及应用系统目前在冗余系统、冗余设备及冗余链路等方面有哪些相关设计和部署,判断是否满足要求；

b）应检查互联网业务及应用系统的相关服务器、用户端网络设备和链路的主备份情况是否满足要求；

c）应检查互联网业务及应用系统在冗余系统、冗余设备及冗余链路方面的灾难备份及恢复能力，查看设计/验收文档，确认互联网在发生灾难以后是否能够采用其他替代方式支持互联网业务及应用的提供；

d）应检查互联网业务及应用系统的冗余系统、冗余设备及冗余链路部署情况，确认其是否与设计一致。

8.3.2 备份数据检测要求

8.3.2.1 检测方式

访谈，检查。

8.3.2.2 检测对象

互联网业务及应用系统，设计/验收文档，数据备份服务器，演练记录，历史记录。

8.3.2.3 检测实施

应按照8.2.2节的要求进行检测。

8.3.3 人员和技术支持能力检测要求

8.3.3.1 检测方式

访谈，检查。

8.3.3.2 检测对象

负责灾难备份及恢复的技术人员。

8.3.3.3 检测实施

除按照8.2.3节的要求进行检测之外，还应按照本节内容进行检测：

应访谈安全管理相关人员，询问并检查是否有负责互联网业务及应用系统的灾难备份及恢复技术支持人员（例如负责数据库、服务器等的技术支持人员），检查相关人员的技术支持能力是否满足要求。

8.3.4 运行维护管理能力检测要求

8.3.4.1 检测方式

访谈，检查。

8.3.4.2 检测对象

备份数据的有效性验证制度，数据容灾备份管理制度。

8.3.4.3 检测实施

除按照8.2.4节的要求进行检测之外，还应按照本节内容进行检测：

a）应访谈安全管理人员，询问是否有对备份数据的有效性验证制度；应检查互联网业务及应用系统是否按介质特性对相关服务器、用户端网络设备备份数据进行定期的有效性验证。

b）应访谈安全管理人员，询问是否有数据容灾备份管理制度；应检查是否有针对互联网业务及应用系统在相关服务器、用户端网络设备的数据容灾备份管理制度。

8.3.5 灾难恢复预案检测要求

8.3.5.1 检测方式

访谈，检查。

8.3.5.2 检测对象

灾难恢复预案，设计/验收文档，灾难恢复预案的教育和培训记录、演练记录、调整记录、管理制度。

8.3.5.3 检测实施

除按照8.2.5节的要求进行检测之外，还应按照本节内容进行检测：

a）应访谈安全管理人员，并查看互联网业务及应用系统灾难恢复预案教育和培训记录，检查是否有灾难恢复预案的教育和培训，是否达到了教育和培训的预期目标，检查相关人员对灾难恢复预案的了解情况，检查相关人员是否具有对灾难恢复预案进行实际操作的能力。

b）应访谈安全管理人员，并查看互联网业务及应用系统灾难恢复预案演练记录，检查灾难恢复预案的演练情况，灾难恢复预案演练的效果是否达到设计要求；查看灾难恢复预案调整记录，检查根据演练结果对灾难恢复预案进行修正的情况。

8.4 第3.2级要求

同第3.1级要求。

8.5 第4级要求

同第3.2级要求。

8.6 第5级要求

待补充。

参 考 文 献

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
YD/T 1736-2008	互联网安全防护要求
YD/T 126-2005	增值电信业务网络信息安全保障基本要求