

ICS 33.040.01

M 10

YD

中华人民共和国通信行业标准

YD/T 2244-2011

电信网和互联网信息服务业务系统 安全防护检测要求

Security protection test requirements for information service system of
telecom network and internet

2011-06-01 发布

2011-06-01 实施

中华人民共和国工业和信息化部 发布

目 次

前 言	II
1 范围	1
2 规范性引用文件	1
3 术语、定义和缩略语	1
3.1 术语和定义	1
3.2 缩略语	3
4 信息服务业务系统安全防护检测概述	3
4.1 信息服务业务系统安全防护检测范围	3
4.2 信息服务业务系统安全防护检测对象	3
4.3 信息服务业务系统安全防护检测内容	4
4.4 信息服务业务系统安全防护检测结果判定	4
5 信息服务业务系统安全等级保护检测要求	5
5.1 概述	5
5.2 第1级要求	5
5.3 第2级要求	6
5.4 第 3.1 级要求	15
5.5 第 3.2 级要求	21
5.6 第 4 级要求	21
5.7 第 5 级要求	21
6 信息服务业务系统安全风险评估检测要求	21
6.1 安全风险评估范围	21
6.2 安全风险评估内容	22
6.3 安全风险评估要素	22
6.4 安全风险评估赋值原则	23
6.5 安全风险评估赋值计算方法	24
6.6 安全风险评估文件类型	24
6.7 安全风险评估文件记录	25
7 信息服务业务系统灾难备份及恢复检测要求	25
7.1 第 1 级要求	25
7.2 第 2 级要求	25
7.3 第 3.1 级要求	27
7.4 第 3.2 级要求	29
7.5 第 4 级要求	29
7.6 第 5 级要求	29
参考文献	30

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。该系列标准预计结构及名称如下：

1. 《电信网和互联网安全防护管理指南》
2. 《电信网和互联网安全等级保护实施指南》
3. 《电信网和互联网安全风险评估实施指南》
4. 《电信网和互联网灾难备份及恢复实施指南》
5. 《互联网安全防护要求》
6. 《移动通信网安全防护要求》
7. 《互联网安全防护要求》
8. 《增值业务网—消息网安全防护要求》
9. 《增值业务网—智能网安全防护要求》
10. 《接入网安全防护要求》
11. 《传送网安全防护要求》
12. 《IP承载网安全防护要求》
13. 《信令网安全防护要求》
14. 《同步网安全防护要求》
15. 《支撑网安全防护要求》
16. 《非核心生产单元安全防护要求》
17. 《电信网和互联网物理环境安全等级保护要求》
18. 《电信网和互联网管理安全等级保护要求》
19. 《固定网安全防护检测要求》
20. 《移动通信网安全防护检测要求》
21. 《互联网安全防护检测要求》
22. 《增值业务网—消息网安全防护检测要求》
23. 《增值业务网—智能网安全防护检测要求》
24. 《接入网安全防护检测要求》
25. 《传送网安全防护检测要求》
26. 《IP承载网安全防护检测要求》
27. 《信令网安全防护检测要求》
28. 《同步网安全防护检测要求》
29. 《支撑网安全防护检测要求》
30. 《非核心生产单元安全防护检测要求》
31. 《电信网和互联网物理环境安全防护检测要求》
32. 《电信网和互联网管理安全检测要求》

- 33. 《域名系统安全防护要求》
- 34. 《域名系统安全防护检测要求》
- 35. 《网上营业厅安全防护要求》
- 36. 《网上营业厅安全防护检测要求》
- 37. 《WAP网关系统安全防护要求》
- 38. 《WAP网关系统安全防护检测要求》
- 39. 《电信网和互联网信息服务业务系统安全防护要求》
- 40. 《电信网和互联网信息服务业务系统安全防护检测要求》(本标准)
- 41. 《增值业务网 即时消息业务系统安全防护要求》
- 42. 《增值业务网 即时消息业务系统安全防护检测要求》
- 43. 《域名注册系统安全防护要求》
- 44. 《域名注册系统安全防护检测要求》

本标准与YD/T 2243-2011《电信网和互联网信息服务业务系统安全防护要求》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:工业和信息化部电信研究院。

本标准主要起草人:田慧蓉、魏 亮。

电信网和互联网信息服务业务系统安全防护检测要求

1 范围

本标准规定了电信网和互联网信息服务业务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。

本标准适用于电信网和互联网信息服务业务系统。

本标准中信息服务业务系统均特指电信网和互联网信息服务业务系统。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 5271.8-2001	信息技术 词汇 第8部分：安全
YD/T 2243-2011	电信网和互联网信息服务业务系统安全防护要求
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
YD/T 2240-2011	增值业务网 即时消息业务系统安全防护检测要求
YDN 126-2009	增值电信业务网络信息安全保障基本要求

3 术语、定义和缩略语

3.1 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。

3.1.1

信息服务业务系统安全等级 security classification of Information Service System

信息服务业务系统重要程度的表征。重要程度从信息服务系统受到破坏后，对国家安全、社会秩序、经济运行、公共利益、业务运营商造成的损害来衡量。

3.1.2

信息服务业务系统安全等级保护 classified security protection of Information Service System

对信息服务业务系统分等级实施安全保护。

3.1.3

信息服务业务系统安全检测 security testing of Information Service System

对信息服务业务系统的安全保护能力是否达到相应保护要求进行衡量。

3.1.4

组织 organization

由信息服务业务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。

3.1.5

信息服务业务系统安全风险 security risk of Information Service System

人为或自然的威胁可能利用信息服务业务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。

3.1.6

信息服务业务系统安全风险评估 security risk assessment of Information Service System

运用科学的方法和手段，系统地分析信息服务业务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，防范和化解信息服务业务系统安全风险，将风险控制在可接受的水平，为最大限度地保障信息服务业务系统的安全提供科学依据。

3.1.7

信息服务业务系统资产 asset of Information Service System

信息服务业务系统中具有价值的资源，是安全防护体系保护的对象。信息服务业务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，如局域网中的路由器。

3.1.8

信息服务业务系统资产价值 asset value of Information Service System

信息服务业务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。

3.1.9

信息服务业务系统威胁 threat of Information Service System

可能导致对信息服务业务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。

3.1.10

信息服务业务系统脆弱性 vulnerability of Information Service System

信息服务业务系统资产中存在的弱点、缺陷与不足，不直接对信息服务业务系统资产造成危害，但可能被信息服务业务系统威胁所利用从而危及信息服务业务系统资产的安全。

3.1.11

信息服务业务系统灾难 disaster of Information Service System

由于各种原因，造成信息服务业务系统故障或瘫痪，使信息服务业务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。

3.1.12

信息服务业务系统灾难备份 backup for disaster recovery of Information Service System

为了信息服务业务系统灾难恢复而对相关网络要素进行备份的过程。

3.1.13

信息服务业务系统灾难恢复 disaster recovery of Information Service System

为了将信息服务业务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。

3.1.14

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。

3.1.15

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。

3.1.16

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，检查、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。

3.2 缩略语

下列缩略语适用于本标准。

DDoS	Distributed Denial of Service	分布式拒绝服务
DoS	Denial of Service	拒绝服务
FTP	File Transfer Protocol	文件传输协议
HTTP	HyperText Transfer Protocol	超文本传输协议
IP	Internet Protocol	网际协议
POP3	Post Office Protocol v3	邮政代理协议第3版
SIP	Session Initiation Protocol	会话初始化协议
SMTP	Simple Mail Transfer Protocol	简单邮件传输协议

4 信息服务业务系统安全防护检测概述

4.1 信息服务业务系统安全防护检测范围

信息服务业务系统安全防护检测范围是我国具有管辖权的提供信息服务业务的平台或系统。YD/T 2244-2011《电信网和互联网信息服务业务系统安全防护检测要求》。主要对信息服务业务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。

信息服务业务系统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。

基础电信运营企业提供的即时消息业务的安全防护检测依据 YD/T 2240-2011《增值业务网 即时消息业务系统安全防护检测要求》进行。

4.2 信息服务业务系统安全防护检测对象

信息服务业务系统的安全防护检测对象是面向公众用户提供信息服务的各业务系统。

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。

4.3 信息服务业务系统安全防护检测内容

与信息服务业务系统安全防护要求相对应,信息服务业务系统安全防护检测内容主要包括以下3个部分:

——信息服务业务系统安全等级保护检测

主要包括业务及应用安全检测、系统安全检测、主机安全检测、物理环境安全检测、管理安全检测等;

——信息服务业务系统安全风险评估检测

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;

——信息服务业务系统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。

4.4 信息服务业务系统安全防护检测结果判定

信息服务业务系统安全防护检测包括对信息服务系统的安全等级保护、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信息服务业务系统的安全等级保护、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给出了信息服务业务系统安全等级保护各检测子类所占的比重。信息服务业务系统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
$4.5 \leq x \leq 5$	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
$1 \leq x < 1.5$	很差

表3 信息服务业务系统安全等级保护检测子类所占比重

比重（%）	子 类
25	业务及应用安全
15	系统安全
5	主机安全
15	物理环境安全
40	管理安全

5 信息服务业务系统安全等级保护检测要求

5.1 概述

本标准主要对信息服务业务系统提出安全防护检测要求。

对信息服务业务系统进行检测时，可根据检测对象提供的业务及应用进行相应检测，未提供的应用不做检测要求。

5.2 第 1 级要求

5.2.1 业务及应用安全

5.2.1.1 通用要求

5.2.1.1.1 身份鉴别

5.2.1.1.1.1 检测方式

访谈，检查，测试。

5.2.1.1.1.2 检测对象

信息服务业务设计/验收文档，相关服务和应用管理流程文档，业务管理和配置文档。

5.2.1.1.1.3 检测实施

a) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略，识别哪些业务保留了用户个人信息或用户服务信息，并针对这些业务检查是否对用户进行身份标识和鉴别的设计，测试验证是否有用户身份标识和鉴别的实现；

b) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，判断针对提供登录功能的业务系统，是否有用户登录失败处理等功能，检查有关技术手段和措施的启用、实施情况，测试验证是否根据安全策略对登录失败采取了结束会话、限制非法登录次数和自动退出等措施；

c) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，针对提供登录功能的业务系统，检查是否有用户身份标识唯一性检查手段及有关措施启用、实施情况，检查或测试验证是否能保证系统中不存在重复用户身份标识。

5.2.1.1.2 访问控制

5.2.1.1.2.1 检测方式

访谈，检查，测试。

5.2.1.1.2.2 检测对象

信息服务业务设计/验收文档，相关服务和应用管理流程文档，业务管理和配置文档。

5.2.1.1.2.3 检测实施

应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查或验证是否只有授权用户可配置访问控制策略，检查或测试验证业务控制与管理是否严格限制默认帐号的权限。

5.2.1.2 特定业务相关安全

不作要求。

5.2.2 系统安全

不作要求。

5.2.3 主机安全

不作要求。

5.2.4 物理环境安全

应按照YD/T 1755-2008中的4.1节要求（第1级要求）进行检测。

5.2.5 管理安全

应按照YD/T 1757-2008中的4.1节要求（第1级要求）进行检测。

5.3 第2级要求

5.3.1 业务及应用安全检测要求

5.3.1.1 通用要求

5.3.1.1.1 身份鉴别

5.3.1.1.1.1 检测方式

访谈，检查，测试。

5.3.1.1.1.2 检测对象

信息服务业务设计/验收文档，相关服务和应用管理流程文档，业务管理和配置文档。

5.3.1.1.1.3 检测实施

a) 应按照5.2.1.1.1节的要求进行检测；

b) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查用户身份鉴别信息复杂度检查功能、技术手段及有关措施启用、实施情况，检查或测试验证是否能保证系统中身份鉴别信息不易被冒用；

c) 应访谈相关技术和管理人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查是否采用加密方式存储系统业务用户的账号和口令。

5.3.1.1.2 访问控制

5.3.1.1.2.1 检测方式

访谈，检查，测试。

5.3.1.1.2.2 检测对象

信息服务业务设计/验收文档，相关服务和应用管理流程文档，业务管理和配置文档，业务运营商提供的其他文档，相关日志记录等。

5.3.1.1.2.3 检测实施

a) 应按照5.2.1.1.2节的要求进行检测；

b) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查或测试验证是否严格限制各用户的访问权限，按安全策略要求控制用户对业务、数据、网络资源等的访问。

5.3.1.1.3 安全审计

5.3.1.1.3.1 检测方式

访谈, 检查, 测试。

5.3.1.1.3.2 检测对象

信息服务业务设计/验收文档, 相关服务和应用管理流程文档, 业务管理和配置文档, 业务运营商提供的其他文档, 相关日志及审计记录等。

5.3.1.1.3.3 检测实施

a) 应访谈相关技术人员, 检查业务设计/验收文档、业务安全策略、业务管理和配置文档、审计记录, 检查是否提供覆盖到每个用户关键操作的安全审计功能;

b) 应访谈相关技术人员, 检查业务设计/验收文档、业务安全策略、业务管理和配置文档、审计记录, 访谈审计相关工作流程、工作要求, 检查是否对业务用户的重要行为、业务资源使用情况等进行审计分析;

c) 应访谈相关技术人员, 检查业务设计/验收文档、业务安全策略、业务管理和配置文档, 对审计功能和审计记录进行测试, 验证是否保证无法删除、修改或覆盖审计记录;

d) 应访谈相关技术人员, 检查业务设计/验收文档、业务安全策略、业务管理和配置文档、相关审计记录, 访谈审计相关工作流程、审计文件及结果记录要求, 检查验证业务相关审计记录的内容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。

5.3.1.1.4 资源控制

5.3.1.1.4.1 检测方式

访谈, 检查, 测试。

5.3.1.1.4.2 检测对象

信息服务业务设计/验收文档, 相关服务和应用管理流程文档, 业务管理文档, 系统和设备管理配置记录, 故障告警记录, 业务运营商提供的其他文档, 相关设备及日志记录等。

5.3.1.1.4.3 检测实施

应访谈相关技术人员, 检查系统设计/验收文档、系统安全策略、系统及设备管理和配置文档, 检查或测试验证系统能否在用户和业务系统通信双方中的一方在一段时间内未作任何响应时, 自动结束会话。

5.3.1.1.5 信息保护

5.3.1.1.5.1 检测方式

访谈, 检查, 测试。

5.3.1.1.5.2 检测对象

信息服务业务设计/验收文档, 相关服务和应用管理流程文档, 业务安全策略、业务管理和配置文档, 系统和设备管理配置记录, 业务运营商提供的其他文档, 相关设备及日志记录等。

5.3.1.1.5.3 检测实施

a) 应访谈相关技术和管理人员, 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, 检查验证业务提供、控制与管理过程是否能保护用户隐私, 不泄漏用户相关敏感信息, 例如对用户隐私相关的手机号码、通信地址等是否有保护和控制措施;

b) 应访谈相关技术人员, 检查信息服务业务设计/验收文档、业务安全策略、业务管理和配置文档、相关设备及日志记录, 检查核对系统相关日志记录是否出现过相关数据和页面被篡改和破坏的情况, 检查或测试验证保护业务相关信息的安全手段是否能够有效保护和避免相关数据和页面被篡改和破坏;

c) 应访谈相关技术人员, 检查信息服务业务设计/验收文档、业务安全策略、业务管理和配置文档, 检查验证业务是否禁止了不必要的内嵌网络服务, 测试验证是否禁止在用户端自动安装恶意软件;

d) 应访谈相关技术人员, 检查信息服务业务设计/验收文档、业务安全策略、业务管理和配置文档, 检查验证是否对通信过程中的敏感信息字段进行加密;

e) 应访谈相关技术人员, 检查信息服务业务设计/验收文档、业务安全策略、业务管理和配置文档, 检查验证在发现诈骗、虚假广告等信息后, 能否进行处理以防止信息的扩散。

5.3.1.2 特定业务安全相关要求

5.3.1.2.1 检测方式

访谈, 检查, 测试。

5.3.1.2.2 检测对象

信息服务业务设计/验收文档, 相关服务和应用管理流程文档, 业务管理和配置文档, 系统和设备管理配置记录, 故障告警记录, 业务运营商提供的其他文档, 相关设备及日志记录等。

5.3.1.2.3 检测实施

a) 对于提供信息服务的平台, 应访谈相关技术人员, 检查信息服务业务设计/验收文档、业务安全策略、业务管理和配置文档, 检查验证是否有相应的自动程序过滤和人工检查相结合的手段, 对相关信息在向公众发布前进行有害信息检查、屏蔽和删除, 检查或测试验证有关技术手段阻止有害信息通过业务网络向公众传播的效果;

b) 对于提供电子邮件服务的平台, 应访谈相关技术人员, 检查信息服务业务设计/验收文档、业务安全策略、业务管理和配置文档, 检查验证业务平台是否按照相关规定要求, 提供相应的安全措施(如, 垃圾邮件防范和过滤等)保证用户邮件业务的正常, 检查或测试验证有关垃圾邮件防范和过滤的技术手段的效果;

c) 对支持用户上传、下载信息的业务平台, 应访谈相关技术人员, 检查信息服务业务设计/验收文档、业务安全策略、业务管理和配置文档, 检查业务平台是否启用相关安全手段和措施, 检查或测试验证是否对用户上传、下载等操作行为进行监控, 防止用户的非授权的读写操作;

d) 对提供信息下载服务的平台, 应访谈相关技术人员, 检查信息服务业务设计/验收文档、业务安全策略、业务管理和配置文档, 检查或测试验证是否能拒绝来自未被允许的地址、用户名、子网域的操作请求, 检查或测试验证对核心服务器的相关资源是否能有效保护或隔离;

e) 对提供信息下载务的平台, 应访谈相关技术人员, 检查信息服务业务设计/验收文档、业务安全策略、业务管理和配置文档, 检查或测试验证是否能对单个地址(地址段)、用户名、子网域的连接数量和连接频率进行限制, 防止资源被过度使用;

f) 对提供信息递送服务的平台, 应访谈相关技术人员, 检查信息服务业务设计/验收文档、业务安全策略、业务管理和配置文档, 检查或验证是否只根据用户需求递送相关信息内容, 是否支持用户对信息的退订;

g) 对提供即时交互服务的平台（如，即时消息服务、基于互联网的音视频通话服务等），应访谈相关技术人员，检查信息服务业务设计/验收文档、业务安全策略、业务管理和配置文档，检查验证是否提供必要的保护措施（如，加密机制）保护用户间通信数据的机密性和完整性；

h) 对于提供群发即时消息的平台，应访谈相关技术人员，检查信息服务业务设计/验收文档、业务安全策略、业务管理和配置文档，检查并通过技术手段测试验证是否能够防范、清除以群发方式发送伪造、隐匿信息发送者真实标记的即时信息；

i) 应访谈相关技术人员，检查信息服务业务设计/验收文档、业务安全策略、业务管理和配置文档、系统日志，检查验证是否记录并留存业务控制和管理相关的日志信息，检查或测试验证是否记录用户发布信息、评论、邮件收发、文件上传和下载等相关日志信息（如，操作内容、操作时间、使用的网络地址或者域名等），检查验证相关日志记录信息保留一定期限（至少60天）；

j) 应访谈相关技术和管理人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档、业务运营商提供的其他文档，检查验证业务实现是否国家、行业和企业相关标准的业务安全要求。

5.3.2 系统安全

5.3.2.1 结构安全

5.3.2.1.1 检测方式

访谈，检查，测试。

5.3.2.1.2 检测对象

信息服务业务系统相关设备，系统设计/验收文档，系统相关管理文档，设备管理配置记录，故障告警记录，业务运营商提供的其他文档。

5.3.2.1.3 检测实施

a) 应访谈相关技术人员，检查系统设计/验收文档、业务运营商提供的其他文档，检查验证是否绘制与当前运行情况相符的系统拓扑结构图；

b) 应访谈相关技术人员，检查系统设计/验收文档、系统管理和配置文档，检查是否根据应用和服务的特点，在满足高峰期流量需求的基础上，合理设计系统带宽，检查或测试验证系统是否能满足高峰期流量的冲击；

c) 应访谈相关技术人员，检查系统设计/验收文档、系统安全策略、系统管理和配置文档、业务运营商提供的其他文档，检查验证是否根据系统内部网络结构特点，按照统一的管理和控制原则划分不同的子网或网段，检查验证相关设备是否依照功能划分及其重要性等因素分区部署；

d) 应访谈相关技术和管理人员，检查系统设计/验收文档、系统告警即故障记录、系统相关日志记录，检查核对在不考虑主动宕机维护的情况下，系统累计宕机时间是否不超过8.76小时/年，验证系统可靠性是否达到99.9%以上。

5.3.2.2 身份鉴别

5.3.2.2.1 检测方式

访谈，检查，测试。

5.3.2.2.2 检测对象

信息服务业务系统相关设备，系统设计/验收文档，系统相关管理文档，设备管理配置记录，故障告警记录，业务运营商提供的其他文档。

5.3.2.2.3 检测实施

a) 应访谈相关技术和管理人员, 检查系统设计/验收文档、系统安全策略、系统管理和配置文档、审计记录/报告, 访谈对系统管理用户是否有身份标识和鉴别措施, 检查或测试验证相关措施的实施情况和有效性;

b) 应访谈相关技术和管理人员, 检查系统设计/验收文档、系统安全策略、系统管理和配置文档, 访谈对系统管理用户的口令设置要求, 检查验证相关用户口令长度(是否均不小于8字节)、口令复杂度(是否使用大写字母、小写字母、数字、标点符号及特殊字符四种字符中至少二种的组合且与用户名或ID无相关性)、口令更新频率(更新周期是否不大于90天)等相关要求, 检查验证是否部署和应用相关技术保障手段(如, 口令统一管理相关技术措施), 并测试相关口令策略和安全要求落实和执行情况, 测试验证口令安全相关技术保障手段的效果;

c) 应访谈相关技术和管理人员, 检查系统设计/验收文档、系统安全策略、系统管理和配置文档, 检查是否有用户登录失败处理等功能, 检查有关技术手段和措施的启用、实施情况, 测试验证是否根据安全策略对登录失败采取了结束会话、限制非法登录次数和自动退出等措施;

d) 应访谈相关技术和管理人员, 检查系统设计/验收文档、系统安全策略、系统管理和配置文档, 检查是否采用加密存储的机制保护系统管理用户账号和口令的安全。

5.3.2.3 访问控制

5.3.2.3.1 检测方式

访谈, 检查, 测试。

5.3.2.3.2 检测对象

信息服务业务系统相关设备, 系统设计/验收文档, 系统相关管理文档, 设备管理配置记录, 故障告警记录, 业务运营商提供的其他文档。

5.3.2.3.3 检测实施

a) 应访谈相关技术人员, 检查系统设计/验收文档、系统安全策略、系统及设备管理和配置文档, 检查验证是否在系统边界部署访问控制设备, 并启用访问控制功能;

b) 应访谈相关技术人员, 检查系统设计/验收文档、系统安全策略、系统及设备管理和配置文档, 检查或通过技术手段测试验证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;

c) 应访谈相关技术人员, 检查业务设计/验收文档、业务安全策略、业务管理和配置文档, 检查或测试验证各帐号是否依据最小授权原则授权, 按安全策略要求控制对文件、数据库表等内容的访问;

d) 应访谈相关技术人员, 检查系统设计/验收文档、系统安全策略、系统管理和配置文档、业务运营商提供的其他文档, 检查验证是否按系统管理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资源访问, 检查或通过技术手段测试验证系统访问控制粒度是否为单个用户;

e) 应访谈相关技术人员, 检查系统设计/验收文档、系统安全策略、系统管理和配置文档、业务运营商提供的其他文档, 检查验证系统是否限制了具有拨号访问权限的管理用户的数量。

5.3.2.4 安全审计

5.3.2.4.1 检测方式

访谈, 检查, 测试。

5.3.2.4.2 检测对象

信息服务业务系统相关设备, 系统设计/验收文档, 系统相关管理文档, 设备管理配置记录, 故障告警记录, 业务运营商提供的其他文档。

5.3.2.4.3 检测实施

a) 应访谈相关技术和管理人员, 检查系统设计/验收文档、系统安全策略、系统管理和配置文档、系统日志, 检查验证是否对系统中的重要设备运行状况、网络流量、系统管理及维护等进行日志记录, 检查验证系统相关日志记录是否保留一定期限(至少180天);

b) 应访谈相关技术和管理人员, 检查系统设计/验收文档、系统安全策略、系统管理和配置文档、审计记录/报告, 检查或测试验证审计记录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。

5.3.2.5 入侵防范

5.3.2.5.1 检测方式

访谈, 检查, 测试。

5.3.2.5.2 检测对象

信息服务业务系统相关设备, 系统设计/验收文档, 系统相关管理文档, 设备管理配置记录, 故障告警记录, 业务运营商提供的其他文档。

5.3.2.5.3 检测实施

a) 应访谈相关技术人员, 检查系统设计/验收文档、系统安全策略、系统管理和配置文档, 检查验证是否部署攻击、入侵监测的相关技术措施和手段, 检查或通过技术手段验证相关系统能否发现在边界处发生的端口扫描、强力攻击、木马后门攻击、DoS/DDoS攻击、缓冲区溢出攻击、IP碎片攻击和网络蠕虫等攻击;

b) 应访谈相关技术人员, 检查系统设计/验收文档、系统安全策略、系统管理和配置文档, 检查验证是否部署攻击、入侵防护的相关设备或技术措施, 检查或通过技术手段验证相关系统能否对在边界处发生的各类攻击和入侵是否能有效的抵御和防范。

5.3.2.6 软件容错

5.3.2.6.1 检测方式

访谈, 检查, 测试。

5.3.2.6.2 检测对象

信息服务业务系统设计/验收文档, 系统相关管理文档, 业务运营商提供的其他文档。

5.3.2.6.3 检测实施

应访谈相关技术人员, 检查系统设计/验收文档、系统相关管理文档, 检查或验证系统是否能进行数据有效性检验, 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。

5.3.2.7 网络及安全设备防护

5.3.2.7.1 检测方式

访谈, 检查, 测试。

5.3.2.7.2 检测对象

信息服务业务系统相关设备, 设备安全检测报告, 网络设备检测报告、入网证, 业务运营商提供的其他文档。

5.3.2.7.3 检测实施

a) 应访谈相关技术人员和管理人员, 检查网络设备入网检测报告、设备入网证、安全检测报告、业务运营商提供的其他文档, 检查系统相关网络设备是否进行有效的入网检测, 验证是否符合设备入网管理相关要求的规定;

b) 应访谈相关技术人员和管理人员, 询问是否对登录网络设备以及安全设备的用户进行身份鉴别, 检查或测试验证相关措施的实施情况;

c) 应访谈相关技术人员和管理人员, 询问是否对网络设备用户以及安全设备用户做唯一标识, 检查相关设备的用户列表;

d) 应访谈相关技术人员和管理人员, 检查网络管理相关制度, 询问口令管理要求, 检查和验证用户口令是否不小于6字节, 且应有一定的复杂度, 并定期更换(更新周期不大于90天), 检查验证是否部署和应用相关技术保障手段(如, 口令统一管理相关技术措施), 并测试相关口令策略和安全要求落实和执行情况, 测试验证口令安全相关技术保障手段的效果;

e) 应访谈相关技术人员和管理人员, 检查网络设备以及安全设备的管理和配置文档, 检查是否有用户登录失败处理等功能, 检查有关技术手段和措施的启用、实施情况, 测试验证是否根据安全策略对登录失败采取了结束会话、限制非法登录次数和自动退出等措施;

f) 应访谈相关技术人员和管理人员, 检查网络设备以及安全设备的管理和配置文档, 检查是否对管理终端的接入方式、网络地址范围等进行限制, 测试验证相关措施的实施效果;

g) 应访谈相关技术人员和管理人员, 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。

5.3.3 主机安全

5.3.3.1 身份鉴别

5.3.3.1.1 检测方式

访谈, 检查, 测试。

5.3.3.1.2 检测对象

信息服务业务系统相关设备, 主机安全检测报告, 业务运营商提供的其他文档。

5.3.3.1.3 检测实施

a) 应访谈相关技术人员和管理人员, 检查主机安全检测报告、安全策略、主机管理和配置文档, 检查验证对登录操作系统和数据库系统的用户是否进行身份标识和鉴别;

b) 应访谈相关技术人员和管理人员, 检查主机安全检测报告、安全策略、主机管理和配置文档, 检查验证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, 确保用户名具有唯一性;

c) 应访谈相关技术人员和管理人员, 检查主机安全检测报告、安全策略、主机管理和配置文档, 检查验证主机相关用户标识(用户名)是否具有唯一性且不易被冒用, 检查或验证相关用户口令长度(是否均不小于6字节)、口令复杂度(是否使用大写字母、小写字母、数字、标点符号及特殊字符四种字符中至少二种的组合且与用户名或ID无相关性)、口令更新频率(更新周期是否不大于90天)等相关要求, 检查是否部署和应用相关技术保障手段(如, 口令统一管理相关技术措施), 检查或测试验证相关口令策略和安全要求是否有效落实和执行;

d) 应访谈相关技术和管理人员,检查主机的管理和配置文档,检查是否有用户登录失败处理等功能,检查有关技术手段和措施的启用、实施情况,测试验证是否根据安全策略对登录失败采取了结束会话、限制非法登录次数和自动退出等措施;

e) 应访谈相关技术和管理人员,检查主机安全策略要求、业务运营商提供的其他文档,检查验证当对各类主机进行远程管理时,是否采取必要措施,防止鉴别信息在传输过程中被窃听。

5.3.3.2 访问控制

5.3.3.2.1 检测方式

访谈,检查,测试。

5.3.3.2.2 检测对象

信息服务业务系统相关设备,主机安全检测报告,业务运营商提供的其他文档。

5.3.3.2.3 检测实施

a) 应访谈相关技术人员和管理人员,检查主机安全检测报告、安全策略要求、业务运营商提供的其他文档,检查验证是否启用访问控制功能,检查或测试验证是否依据安全策略控制用户对资源的访问;

b) 应访谈相关技术人员和管理人员,检查主机安全检测报告、安全策略要求、业务运营商提供的其他文档,检查验证是否及时删除多余的、过期的账户,避免共享账户的存在;

c) 应访谈相关技术人员,检查主机安全检测报告、安全策略要求、业务运营商提供的其他文档,检查验证是否实现操作系统和数据库系统特权用户的权限分离;

d) 应访谈相关技术人员,检查主机安全检测报告、安全策略要求、业务运营商提供的其他文档,检查或测试验证是否限制默认账户的访问权限,修改这些账户的默认口令,在条件允许的情况下,是否对默认账户进行重命名。

5.3.3.3 安全审计

5.3.3.3.1 检测方式

访谈,检查,测试。

5.3.3.3.2 检测对象

信息服务业务系统相关设备,主机安全检测报告,审计记录/报告,业务运营商提供的其他文档。

5.3.3.3.3 检测实施

a) 应访谈相关技术人员和管理人员,检查主机安全检测报告、安全策略要求、审计记录/报告、业务运营商提供的其他文档,检查或测试验证审计范围是否覆盖到主机/服务器上的每个操作系统用户和数据库用户;

b) 应访谈相关技术人员和管理人员,检查主机安全检测报告、安全策略要求、审计记录/报告、业务运营商提供的其他文档,检查或测试验证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) 应访谈相关技术人员和管理人员,检查主机安全检测报告、安全策略要求、审计记录/报告、业务运营商提供的其他文档,检查验证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) 应访谈相关技术人员和管理人员, 检查主机安全检测报告、安全策略要求、审计记录/报告、业务运营商提供的其他文档, 检查或测试验证是否保护审计记录, 检查或测试验证审计记录是否能避免受到未预期的删除、修改或覆盖等, 检查验证相关审计记录是否保留一定期限(至少180天)。

5.3.3.4 入侵防范

5.3.3.4.1 检测方式

访谈, 检查, 测试。

5.3.3.4.2 检测对象

信息服务业务系统相关设备, 主机安全检测报告, 业务运营商提供的其他文档。

5.3.3.4.3 检测实施

应访谈相关技术人员, 检查主机安全检测报告、安全策略要求、业务运营商提供的其他文档, 检查验证通用主机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, 检查或测试验证相关主机是否均通过安全的方式(如, 设置升级服务器)保持系统补丁及时得到更新。

5.3.3.5 恶意代码防范

5.3.3.5.1 检测方式

访谈, 检查, 测试。

5.3.3.5.2 检测对象

信息服务业务系统相关设备, 主机安全检测报告, 业务运营商提供的其他文档。

5.3.3.5.3 检测实施

a) 应访谈相关技术人员, 检查主机安全检测报告、安全策略要求、业务运营商提供的其他文档, 检查验证通用主机(特别是使用Windows操作系统的主机)是否安装防恶意代码软件, 并及时更新防恶意代码软件版本和恶意代码库;

b) 应访谈系统管理员, 询问是否支持防恶意代码软件的统一管理。

5.3.3.6 资源控制

5.3.3.6.1 检测方式

访谈, 检查, 测试。

5.3.3.6.2 检测对象

信息服务业务系统相关设备, 主机安全检测报告, 业务运营商提供的其他文档。

5.3.3.6.3 检测实施

a) 应访谈相关技术人员, 检查主机安全检测报告、安全策略要求、业务运营商提供的其他文档, 检查或测试验证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) 应访谈相关技术人员, 检查主机安全检测报告、安全策略要求、业务运营商提供的其他文档, 检查或测试验证是否根据安全策略设置登录终端的操作超时锁定。

5.3.3.7 其他

5.3.3.7.1 检测方式

访谈, 检查, 测试。

5.3.3.7.2 检测对象

互联网业务及应用系统相关设备, 主机安全检测报告, 业务运营商提供的其他文档。

5.3.3.7.3 检测实施

应访谈相关技术人员和管理人员，检查主机安全检测报告、业务运营商提供的其他文档，检查验证各类计算机、服务器设备是否符合并满足相关行业标准及业务运营商相关主机设备的要求。

5.3.4 物理环境安全检测要求

5.3.4.1 检测方式

访谈，检查，测试。

5.3.4.2 检测对象

机房，机房及场地相关设计/规划/验收文档。

5.3.4.3 检测实施

a) 应按照YD/T 1755-2008的4.2节的要求（第2级要求）进行检测；

b) 应访谈相关管理和技术人员，询问互联网相关业务及应用系统所处机房是否采取防虫防鼠等保护措施，检查验证相关手段措施是否能有效防范鼠虫蚁害。

5.3.5 管理安全检测要求

应按照YD/T 1757-2008的4.2节要求（第2级要求）进行检测。

5.4 第3.1级要求

5.4.1 业务及应用安全

5.4.1.1 通用安全

5.4.1.1.1 检测方式

访谈，检查，测试。

5.4.1.1.2 检测对象

信息服务业务设计/验收文档，相关服务和应用管理流程文档，业务管理文档，系统和设备管理配置记录，故障告警记录，业务运营商提供的其他文档，相关设备及日志记录等。

5.4.1.1.3 检测实施

a) 应按照5.3.1.1节的要求进行检测；

b) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查验证是否能根据需要对业务及应用相关通信过程中的全部报文或整个会话过程提供必要的保护（如，进行通信数据加密），检查或测试验证是否能提供业务及应用相关访问、通信等数据的防抵赖功能；

c) 应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查是否对业务水平阈值进行定义，验证是否能够对业务及应用服务水平进行检测，检查或测试验证是否具有当服务水平降低到预先规定的阈值时进行告警的功能；

d) 对需要登录访问的信息服务业务平台（或模块），应访谈相关技术人员，检查平台（或模块）设计文档、业务安全策略、业务管理和配置文档，检查或测试验证对公众用户访问和操作的有关环节（如，注册、登录、操作、管理、浏览等）是否提供有效的保护措施，检查或测试验证相关安全保护措施（如，用户注册口令进行强度检查、用户ID检测和帐号保护、以图形验证码保护各类提交信息、对用户重要操作进行确认和验证、授权访问页面使用安全连接等）的效果；

e) 应访谈相关技术人员，检查信息服务业务设计/验收文档、业务安全策略、业务管理和配置文档，检查验证是否提供有效的恶意代码检测和过滤技术手段，检查或测试验证业务平台对相关业务及应用中

用户发布、传送的各类文件（如，用户发布和上传的文件、资源站点可供下载的文件、即时通信用户间传送的文件、电子邮件附件）是否进行必要的安全检查和过滤。

5.4.1.2 特定业务相关安全

5.4.1.2.1 检测方式

访谈，检查，测试。

5.4.1.2.2 检测对象

信息服务业务设计/验收文档，相关服务和应用管理流程文档，业务管理文档，系统和设备管理配置记录，故障告警记录，业务运营商提供的其他文档，相关设备及日志记录等。

5.4.1.2.3 检测实施

a) 应按照5.3.1.2节的要求进行检测；

b) 对于提供信息浏览和发布服务的平台，应访谈相关技术人员，检查信息服务业务设计/验收文档、业务安全策略、业务管理和配置文档，检查或测试验证是否能拒绝由未被允许的地址、子网域发起的请求（如，浏览、发布、评论等），验证是否能拒绝以未经授权的方式访问服务器上有限公开的相关内容和资源；

c) 对于提供电子邮件服务的平台，应访谈相关技术人员，检查信息服务业务设计/验收文档、业务安全策略、业务管理和配置文档，检查或测试验证是否对邮件发送者进行身份认证，检查或测试验证是否支持限制和禁止自动转发电子邮件的功能；

d) 对于提供电子邮件服务的平台，应访谈相关技术人员，检查信息服务业务设计/验收文档、业务安全策略、业务管理和配置文档，检查业务安全相关技术手段功能及配置，检查或测试验证是否能拒绝由未被允许的地址、用户名、子网域发起的电子邮件服务连接请求，是否能拒绝电子邮件转发次数超过预定上限的电子邮件的继续转发操作，是否能拒绝收信人数量超过预定上限的电子邮件的发送操作，是否能拒绝附件数量超过预定上限的电子邮件的发送操作，是否能拒绝邮件大小超过预定上限的电子邮件的发送操作，是否对单个IP地址或用户名的连接数量和连接频率进行限制；

e) 对于提供电子邮件服务的平台，应访谈相关技术人员，检查信息服务业务设计/验收文档、业务安全策略、业务管理和配置文档，检查或测试验证是否能对进入电子邮件服务器的电子邮件相关的关键信息（如，发送地址、接收地址、标题等）进行必要的检测，是否能按一定的规则和方式（如，黑名单、白名单）对匹配的电子邮件进行过滤和拦截，是否向用户通知有关处理结果；

f) 对于提供信息递送服务的平台，应访谈相关技术人员，检查业务设计/验收文档、业务安全策略、业务管理和配置文档，检查是否能为承载内容（如，静态信息、流媒体等）的特点提供差异化的业务质量控制和管理策略，检查或测试验证根据平台内、外部性能监测的状况，实时智能的平衡和优化网络流量。

5.4.2 系统安全

5.4.2.1 结构安全

5.4.2.1.1 检测方式

访谈，检查，测试。

5.4.2.1.2 检测对象

信息服务业务系统及相关设备,系统设计/验收文档,系统相关管理文档,设备管理配置记录,故障告警记录,业务运营商提供的其他文档。

5.4.2.1.3 检测实施

a) 应按照5.3.2.1节要求进行检测;

b) 应访谈相关技术人员,检查系统设计/验收文档、系统安全策略、系统及设备管理和配置文档,检查验证是否有效避免将重要设备部署在网络边界处且直接连接外部网络/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;

c) 应访谈相关技术人员,检查系统设计/验收文档、系统安全策略、系统及设备管理和配置文档,检查验证是否有过负荷保护功能,确保系统在过负荷时,重要业务仍能正常运行;

d) 应访谈相关技术和管理人员,检查系统设计/验收文档、系统告警即故障记录、系统相关日志记录,检查核对在不考虑主动宕机维护的情况下,系统累计宕机时间是否不超过4.38小时/年,验证系统可靠性是否达到99.95%以上。

5.4.2.2 身份鉴别

应按照5.3.2.2节进行检测。

5.4.2.3 访问控制

5.4.2.3.1 检测方式

访谈,检查,测试。

5.4.2.3.2 检测对象

信息服务业务系统及相关设备,系统设计/验收文档,系统相关管理文档,设备管理配置记录,故障告警记录,业务运营商提供的其他文档。

5.4.2.3.3 检测实施

a) 应按照5.3.2.3节的要求进行检测;

b) 应访谈相关技术人员,检查系统设计/验收文档、系统安全策略、系统及设备管理和配置文档,检查验证是否对进出系统的信息内容进行过滤,检查或测试验证是否能支持并有效实施对相关协议(如,HTTP、FTP、Telnet、SMTP、POP3、SIP等)命令级的控制;

c) 应访谈相关技术人员,检查系统设计/验收文档、系统安全策略、系统及设备管理和配置文档,检查或通过技术手段测试验证对系统重要资源是否进行了有效管理和保护(如,限制系统访问/连接数上限、限制系统出口带宽使用率等);

d) 应访谈相关技术人员,检查系统设计/验收文档、系统安全策略、系统及设备管理和配置文档,检查或通过技术手段测试验证是否能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) 应访谈相关技术人员,检查系统设计/验收文档、系统安全策略、系统及设备管理和配置文档,检查或测试验证系统对允许的最大并发会话连接数是否进行限制,测试验证是否可对特定用户帐号的并发会话数进行限制;

f) 应访谈相关技术人员,检查系统设计/验收文档、系统安全策略、系统及设备管理和配置文档,检查或测试验证重要网段内是否采取技术手段防止地址欺骗(IP地址和MAC地址)。

5.4.2.4 安全审计

5.4.2.4.1 检测方式

访谈，检查，测试。

5.4.2.4.2 检测对象

信息服务业务系统及相关设备，系统设计/验收文档，系统相关管理文档，设备管理配置记录，故障告警记录，业务运营商提供的其他文档。

5.4.2.4.3 检测实施

- a) 应按照5.3.2.4节要求进行安全检测。
- b) 访谈系统管理员，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；
- c) 访谈系统管理员，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。

5.4.2.5 入侵防范

5.4.2.5.1 检测方式

访谈，检查，测试。

5.4.2.5.2 检测对象

信息服务业务系统及相关设备，系统设计/验收文档，系统相关管理文档，设备管理配置记录，故障告警记录，业务运营商提供的其他文档。

5.4.2.5.3 检测实施

- a) 应按照5.3.2.5节要求进行检测；
- b) 应访谈相关技术人员，检查系统设计/验收文档、系统安全策略、系统及设备管理和配置文档、系统日志，检查或测试验证当检测到入侵行为时，是否能记录攻击源IP、攻击类型、攻击目的地址、攻击时间，测试验证在发生严重入侵事件时是否提供报警。

5.4.2.6 软件容错

5.4.2.6.1 检测方式

访谈，检查，测试。

5.4.2.6.2 检测对象

信息服务业务系统设计/验收文档，系统相关管理文档，故障处理文档，业务运营商提供的其他文档。

5.4.2.6.3 检测实施

- a) 应按照5.3.2.6节的要求进行检测；
- b) 应访谈相关技术人员，检查系统设计/验收文档、系统安全策略、系统及设备管理和配置文档、系统日志，故障处理文档等，检查或测试验证系统能够在发生故障时，自动保护当前所有状态，保证系统能够进行恢复。

5.4.2.7 恶意代码防范

5.4.2.7.1 检测方式

访谈，检查，测试。

5.4.2.7.2 检测对象

信息服务业务系统及相关设备，系统设计/验收文档，系统相关管理文档，设备管理配置记录，故障告警记录，业务运营商提供的其他文档。

5.4.2.7.3 检测实施

a) 应访谈相关技术人员, 检查系统设计/验收文档、系统安全策略、系统及设备管理和配置文档、系统日志, 检查或测试验证在系统边界处是否能对恶意代码进行有效检测和清除;

b) 应访谈相关技术人员, 检查系统设计/验收文档、系统安全策略、系统及设备管理和配置文档、系统日志, 检查是否定期和有效维护恶意代码库的升级和检测系统的更新。

5.4.2.8 网络及安全设备防护

应按照5.3.2.7节要求进行安全检测。

5.4.3 主机安全

5.4.3.1 身份鉴别

5.4.3.1.1 检测方式

访谈, 检查, 测试。

5.4.3.1.2 检测对象

信息服务业务系统及相关设备, 系统设计/验收文档, 系统相关管理文档, 设备管理配置记录, 故障告警记录, 业务运营商提供的其他文档。

5.4.3.1.3 检测实施

a) 应按照5.3.3.1节的要求进行安全检测;

b) 应访谈相关技术人员和管理人员, 检查主机安全检测报告、安全策略要求、业务运营商提供的其他文档, 检查或测试验证是否采用两种或两种以上组合的鉴别技术对相关设备的管理用户进行身份鉴别;

c) 应访谈相关技术人员和管理人员, 检查主机安全检测报告、安全策略要求、主机配置和管理记录, 检查验证重要主机、数据库是否使用安全性较高的身份鉴别措施(如, 数字证书)对用户进行身份鉴别。

5.4.3.2 访问控制

5.4.3.2.1 检测方式

访谈, 检查, 测试。

5.4.3.2.2 检测对象

信息服务业务系统及相关设备, 系统设计/验收文档, 系统相关管理文档, 设备管理配置记录, 故障告警记录, 业务运营商提供的其他文档。

5.4.3.2.3 检测实施

a) 应按照5.3.3.2节的要求进行安全检测;

b) 应访谈相关技术人员和管理人员, 检查主机安全检测报告、安全策略要求、业务运营商提供的其他文档, 检查验证是否根据最小权限分配原则, 按设备相关各类管理、维护帐号的角色分配权限, 检查或测试验证是否实现管理帐号与操作、维护帐号的权限分离;

c) 访谈系统管理员, 询问是否对重要信息资源设置敏感标记, 检查具体标记;

d) 访谈系统管理员, 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。

5.4.3.3 安全审计

5.4.3.3.1 检测方式

访谈, 检查, 测试。

5.4.3.3.2 检测对象

信息服务业务系统及相关设备,系统设计/验收文档,系统相关管理文档,设备管理配置记录,故障告警记录,业务运营商提供的其他文档。

5.4.3.3.3 检测实施

a) 应按照5.3.3.3节的要求进行安全检测;

b) 应访谈相关技术人员和管理人员,检查主机安全检测报告、主机安全策略要求、审计记录/报告、业务运营商提供的其他文档,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;

c) 应访谈相关技术人员和管理人员,检查主机安全检测报告、安全策略要求、审计记录/报告、业务运营商提供的其他文档,检查或测试验证是否对审计进程进行保护,避免受到未预期的中断。

5.4.3.4 入侵防范

5.4.3.4.1 检测方式

访谈,检查,测试。

5.4.3.4.2 检测对象

信息服务业务系统及相关设备,系统设计/验收文档,系统相关管理文档,设备管理配置记录,故障告警记录,业务运营商提供的其他文档。

5.4.3.4.3 检测实施

a) 应按照5.3.3.4节的要求进行安全检测;

b) 应访谈相关技术人员,检查主机安全检测报告、安全策略要求、相关日志、业务运营商提供的其他文档,检查或测试验证对重要主机是否进行入侵行为的监测,测试验证是否能够记录入侵的源IP、攻击的类型、攻击的目的地址、攻击的时间,并在发生严重入侵事件时提供报警;

c) 应访谈相关技术人员,检查主机安全检测报告、安全策略要求、相关日志、业务运营商提供的其他文档,检查验证重要的主机是否能够对重要程序的完整性进行检测,检查或测试验证在检测到程序完整性受到破坏后是否能进行可靠的恢复。

5.4.3.5 恶意代码防范

5.4.3.5.1 检测方式

访谈,检查,测试。

5.4.3.5.2 检测对象

信息服务业务系统相关设备,设备安全检测报告,网络设备检测报告,业务运营商提供的其他文档。

5.4.3.5.3 检测实施

a) 应按照5.3.3.5节的要求进行安全检测。

b) 应访谈相关技术人员和管理人员,检查主机安全检测报告、安全策略要求、业务运营商提供的其他文档,检查验证主机使用的防恶意代码产品相关恶意代码库是否与网络/系统防恶意代码产品使用的恶意代码库不同。

5.4.3.6 资源控制

5.4.3.6.1 检测方式

访谈,检查,测试。

5.4.3.6.2 检测对象

信息服务业务系统及相关设备，系统设计/验收文档，系统相关管理文档，设备管理配置记录，故障告警记录，业务运营商提供的其他文档。

5.4.3.6.3 检测实施

a) 应按照5.3.3.6节的要求进行安全检测；

b) 应访谈相关技术人员和管理人员，检查主机安全检测报告、安全策略要求、主机监测日志/记录业务运营商提供的其他文档，检查或测试验证是否对重要服务器进行性能监测，监测内容是否包括服务器的CPU、硬盘、内存、网络等资源的使用情况；

c) 应访谈相关技术人员，检查主机安全检测报告、安全策略要求、主机日志/告警记录、业务运营商提供的其他文档，检查验证是否能够对服务器、数据库等系统的服务水平设定报警阈值，检查或测试验证当监测到服务水平降低到阈值时验证是否能进行报警。

5.4.3.7 其他

应按照5.3.3.7节的要求进行安全检测。

5.4.4 物理环境安全检测要求

5.4.4.1 检测方式

访谈，检查，测试。

5.4.4.2 检测对象

机房，机房及场地相关设计/规划/验收文档

5.4.4.3 检测实施

a) 应按照YD/T 1755-2008的4.3节要求（3.1级要求）进行检测；

b) 应访谈相关管理和技术人员，询问互联网相关业务及应用系统所处机房是否采取防虫防鼠等保护措施，检查验证相关手段措施是否能有效防范鼠虫蚁害。

5.4.5 管理安全检测要求

应按照YD/T 1757-2008的4.3节要求（第3.1级要求）进行检测。

5.5 第3.2级要求

与5.4节（第3.1级）检测要求相同。

5.6 第4级要求

与5.5节（第3.2级）检测要求相同。

5.7 第5级要求

待补充。

6 信息服务业务系统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

安全风险评估报告。

6.1.3 检测实施

a) 应访谈信息服务业务系统安全风险评估负责人, 询问进行信息服务业务系统安全风险评估时, 选择的安全风险评估范围是什么; 并检查信息服务业务系统安全风险评估报告, 检查其安全风险评估范围是否与要求相一致;

b) 应访谈信息服务业务系统安全风险评估负责人, 询问进行信息服务业务系统安全风险评估时, 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; 并检查信息服务业务系统安全风险评估报告, 检查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。

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

安全风险评估报告。

6.2.3 检测实施

a) 应访谈信息服务业务系统安全风险评估负责人, 并检查信息服务业务系统安全风险评估报告, 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) 应访谈信息服务业务系统安全风险评估负责人, 并检查信息服务业务系统安全风险评估报告, 检查技术安全中是否覆盖了业务及应用安全、业务及应用系统安全、设备安全和物理环境安全;

c) 应访谈信息服务业务系统安全风险评估负责人, 并检查信息服务业务系统安全风险评估报告, 检查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。

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

安全风险评估报告, 历史记录。

6.3.3 检测实施

a) 应访谈信息服务业务系统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; 检查信息服务业务系统安全风险评估报告, 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) 应访谈信息服务业务系统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; 检查风险评估报告, 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) 应访谈信息服务业务系统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; 检查信息服务业务系统安全风险评估报告, 检查资产是否包括各类业务及应用涉及的主机、服务器和数据库(如, Web服务器、电子邮件服务器等), 各类业务及应用相关辅助设备(如, 安全过滤、入侵检测和防护设备), 系统内部网络设备(如, 系统内部组网路由器、交换机等设备)、系统内部链路, 有必要独立识别的软件(如, 相关应用软件、数据库软件、业务控制和运维管理软件等), 保证信息服务业务系统正常提供的数据和信息(如, 业务数据、系统配置数据、管理员操作维护记录、用户信息等), 信息服务

业务系统可提供的各类业务及应用（如，信息浏览和发布服务、信息递送服务等），纸质以及保存在存储介质中的各种文件资料（如，设计文档、技术要求、管理规定、工作计划、技术或财务报告、用户手册等），相关管理、维护、开发、数据备份人员等，业务及应用系统所处的物理环境，机房、电力、防火、防水、防静电、温湿度控制等相关设施；

d) 应访谈信息服务业务系统安全风险评估负责人，询问计算信息服务业务系统各资产的资产价值时考虑了哪些因素；检查信息服务业务系统安全风险评估报告，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) 应访谈信息服务业务系统安全风险评估负责人，询问识别信息服务业务系统各资产脆弱性时考虑了哪些方面的脆弱性；检查信息服务业务系统安全风险评估报告，检查信息服务业务系统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) 应访谈信息服务业务系统安全风险评估负责人，询问对信息服务业务系统存在哪些威胁；检查信息服务业务系统安全风险评估报告，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) 应访谈信息服务业务系统安全风险评估负责人，询问威胁识别的依据是什么；检查信息服务业务系统安全风险评估报告，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) 应访谈信息服务业务系统安全风险评估负责人，询问风险值的计算方法；检查信息服务业务系统安全风险评估报告，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) 应访谈信息服务业务系统安全风险评估负责人，询问确定风险阈值的方法；检查信息服务业务系统安全风险评估报告，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) 应访谈信息服务业务系统安全风险评估负责人，并检查信息服务业务系统安全风险评估报告，检查对于不可接收的信息服务业务系统安全风险，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，信息服务业务系统风险值是否满足阈值要求；

k) 应访谈信息服务业务系统安全风险评估负责人，并检查信息服务业务系统安全风险评估报告，检查信息服务业务系统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，检查信息服务业务系统安全风险评估并采取安全措施后，网络的安全性是否提高。

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

安全风险评估报告。

6.4.3 检测实施

a) 应访谈信息服务业务系统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;检查信息服务业务系统安全风险评估报告,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) 应访谈信息服务业务系统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;检查信息服务业务系统安全风险评估报告,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) 应访谈信息服务业务系统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;检查信息服务业务系统安全风险评估报告,检查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。

6.5 安全风险评估赋值计算方法

6.5.1 检测方式

访谈,检查。

6.5.2 检测对象

安全风险评估报告。

6.5.3 检测实施

a) 应访谈信息服务业务系统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;检查信息服务业务系统安全风险评估报告,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) 应访谈信息服务业务系统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;检查信息服务业务系统安全风险评估报告,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。

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,风险处理计划,风险评估记录等风险评估文件。

6.6.3 检测实施

a) 应访谈信息服务业务系统安全风险评估负责人,询问是否制定了风险评估方案;检查此文件,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) 应访谈信息服务业务系统安全风险评估负责人,询问是否制定了风险评估程序;检查此文件,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) 应访谈信息服务业务系统安全风险评估负责人,询问是否制定了资产识别清单;检查此文件,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) 应访谈信息服务业务系统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; 检查此文件, 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) 应访谈信息服务业务系统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; 检查此文件, 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) 应访谈信息服务业务系统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; 检查此文件, 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) 应访谈信息服务业务系统安全风险评估负责人, 询问是否有风险评估报告; 检查此文件, 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) 应访谈信息服务业务系统安全风险评估负责人, 询问是否有风险处理计划; 检查此文件, 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) 应访谈信息服务业务系统安全风险评估负责人, 询问是否有风险评估记录; 检查此文件, 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) 应访谈信息服务业务系统安全风险评估负责人, 询问风险评估文件在正式确认以前是否需要批准; 应检查风险评估文件, 检查文件正式确认以前是否得到批准;

b) 应访谈信息服务业务系统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; 应检查风险评估文件, 检查文件的更改和现行修订状态是否是可识别的;

c) 应访谈信息服务业务系统安全风险评估负责人, 询问风险评估文件的版本如何管理; 应检查风险评估文件, 检查是否有版本划分以及相应的版本使用说明;

d) 应访谈信息服务业务系统安全风险评估负责人, 询问作废文件是如何管理的; 应检查风险评估文件, 检查是否对于作废文件作了标识;

e) 应访谈信息服务业务系统安全风险评估负责人, 询问如何对文件进行控制; 应检查风险评估文件, 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 信息服务业务系统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检测要求

7.2.1.1 检测方式

访谈，检查，测试。

7.2.1.2 检测对象

信息服务业务系统设计/验收文档，相关服务管理流程文档，系统管理文档，系统安全策略、系统拓扑图、设备管理配置记录，故障告警记录，业务运营商提供的其他文档，系统及相关设备等。

7.2.1.3 检测实施

a) 应访谈系统管理员，并检查系统设计/验收文档、系统拓扑图、业务运营商提供的其他文档，检查验证业务及应用系统相关设备的处理能力是否具备一定的冗余，检查或测试验证是否满足业务高峰期需要；

b) 应访谈系统管理员，并检查系统设计/验收文档、系统拓扑图、业务运营商提供的其他文档，检查验证系统关键设备的重要部件是否采用冗余的方式提供保护；

c) 应访谈系统管理员，并检查系统设计/验收文档、系统拓扑图、业务运营商提供的其他文档，检查验证系统是否具备一定的灾难备份和恢复的能力，检查验证关键设备、重要线路是否采用冗余的保护方式。

7.2.2 备份数据检测要求

7.2.2.1 检测方式

访谈，检查。

7.2.2.2 检测对象

信息服务业务系统设计/验收文档，相关服务管理流程文档，系统管理文档，系统安全策略、设备管理配置记录，备份数据，业务运营商提供的其他文档，系统及相关设备等。

7.2.2.3 检测实施

a) 应访谈系统管理员，并检查系统设计/验收文档、相关服务管理流程、系统安全策略、业务运营商提供的其他文档，检查验证是否建立对业务及应用关键数据和重要信息进行备份和恢复的管理和控制机制；

b) 应访谈系统管理员，并检查系统设计/验收文档、相关服务管理流程、系统安全策略、业务运营商提供的其他文档，检查验证相关业务及应用的关键数据（如业务数据、计费数据、系统配置数据、管理员操作维护记录、用户信息等）是否有必要的容灾备份；

c) 应访谈系统管理员，并检查系统设计/验收文档、相关服务管理流程、系统安全策略、业务运营商提供的其他文档，检查验证相关业务及应用的数据备份范围和时间间隔、数据恢复能力是否满足行业管理、业务运营商应急预案相关要求。

7.2.3 人员和技术支持能力检测要求

7.2.3.1 检测方式

访谈，检查。

7.2.3.2 检测对象

各级安全负责人，各相关管理、技术、运维人员，人员任职信息，责任岗位规章，人员管理制度，值班记录，培训考核记录。

7.2.3.3 检测实施

a) 应访谈安全负责人、其他相关人员，并检查人员任职信息、责任岗位规章、人员管理制度、培训考核记录，检查验证业务及应用系统的运维是否有专职的管理责任人；

b) 应访谈安全负责人、其他相关人员，并检查人员任职信息、责任岗位规章、人员管理制度、培训考核记录，检查验证是否有系统业务管理和控制，以及设备操作、维护、管理等相关技术人员；

c) 应访谈安全负责人、其他相关人员，并检查人员任职信息、责任岗位规章、人员管理制度、培训考核记录，检查验证相关管理和技术人员是否通过技术培训和考核。

7.2.4 运行维护管理能力检测要求

7.2.4.1 检测方式

访谈，检查，测试。

7.2.4.2 检测对象

业务及应用相关运行管理制度。

7.2.4.3 检测实施

a) 应访谈安全管理人员、各相关管理、技术、运维人员，询问是否有机房管理制度，询问机房管理制度覆盖的范围，检查验证是否具有完善运行维护管理制度，管理制度是否涵盖业务管理和控制、系统运行、设备操作和维护等方面；

b) 应访谈安全管理人员、各相关管理、技术、运维人员，询问是否有机房管理制度，询问机房管理制度覆盖的范围，检查验证是否按照统一的运行维护要求，对业务及应用系统进行规范化的维护；

c) 应访谈安全管理人员、各相关管理、技术、运维人员，检查机房管理制度覆盖的范围，验证是否有业务及应用系统相关介质存取、验证和转储的管理制度，检查或测试验证是否能确保有关备份数据、信息的授权访问；

d) 应访谈安全管理人员、各相关管理、技术、运维人员，检查验证是否建立和保持与其他部门、外部单位间良好的联络和协作机制，是否具有正常对外联络和协作能力。

7.2.5 灾难恢复预案检测要求

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，相关管理制度，安全管理人员。

7.2.5.3 检测实施

a) 应访谈安全管理人员，并检查是否有完整的信息服务业务系统灾难恢复预案；

b) 应访谈安全管理人员，询问是否进行灾难恢复预案教育、培训和演练，检查和验证灾难恢复预案教育、培训和演练记录，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；

c) 应访谈安全管理人员，检查和验证信息服务业务系统灾难恢复能力是否满足行业管理、业务运营商应急预案相关要求，相关系统可用性、业务恢复时间是否符合YDN 126-2009有关要求。

7.3 第 3.1 级要求

7.3.1 冗余系统、冗余设备及冗余链路检测要求

7.3.1.1 检测方式

访谈，检查，测试。

7.3.1.2 检测对象

信息服务业务系统设计/验收文档，相关服务管理流程文档，系统管理文档，系统安全策略、系统拓扑图、设备管理配置记录，故障告警记录，业务运营商提供的其他文档，系统及相关设备等。

7.3.1.3 检测实施

应按照8.2.1节和本节的要求进行检测：

a) 应访谈系统管理员，并检查系统设计/验收文档、系统拓扑图、业务运营商提供的其他文档，检查验证重要设备、线路是否采用热备份的保护方式进行保护；

b) 应访谈系统管理员，并检查系统设计/验收文档、系统拓扑图、业务运营商提供的其他文档，检查验证系统是否有必要的流量负荷分担设计，检查或测试验证系统符合分担技术措施的效果；

c) 应访谈系统管理员，并检查系统设计/验收文档、系统拓扑图、业务运营商提供的其他文档，检查验证系统是否具备较好的灾难备份和业务恢复的能力，提供重要服务的业务及应用系统是否进行系统级备份，检查或测试验证系统容灾备份和业务恢复保障措施在是否能在灾难发生时保证相关业务的连续性。

7.3.2 备份数据检测要求

7.3.2.1 检测方式

访谈，检查，测试。

7.3.2.2 检测对象

信息服务业务系统设计/验收文档，相关服务管理流程文档，系统管理文档，系统安全策略、设备管理配置记录，备份数据，业务运营商提供的其他文档，系统及相关设备等。

7.3.2.3 检测实施

应按照8.2.2节和本节的要求进行检测：

a) 应访谈系统管理员，并检查系统设计/验收文档、相关服务管理流程、系统安全策略、业务运营商提供的其他文档，检查验证是否建立对业务及应用全部数据、信息进行备份和恢复的管理和控制机制；

b) 应访谈系统管理员，并检查系统设计/验收文档、相关服务管理流程、系统安全策略、业务运营商提供的其他文档，检查验证系统重要的业务及应用相关数据是否进行异地备份；

c) 应访谈系统管理员，并检查系统设计/验收文档、相关服务管理流程、系统安全策略、业务运营商提供的其他文档，检查或测试验证系统是否提供数据自动保护功能，检查或测试验证当发生故障后系统是否能保证恢复到故障前的业务状态。

7.3.3 人员和技术支持能力检测要求

7.3.3.1 检测方式

访谈，检查。

7.3.3.2 检测对象

各级安全负责人，各相关管理、技术、运维人员，人员任职信息，责任岗位规章，人员管理制度，值班记录，培训考核记录。

7.3.3.3 检测实施

应按照8.2.3节和本节的要求进行检测：

a) 应访谈安全负责人、其他相关人员，并检查人员任职信息、责任岗位规章、人员管理制度、培训考核记录，检查验证是否有专职系统业务管理和控制，以及设备操作、维护、管理等相关技术人员；

b) 应访谈安全负责人、其他相关人员，并检查人员任职信息、责任岗位规章、人员管理制度、培训考核记录，检查验证相关管理和技术人员是否定期组织安全技术培训和考核。

7.3.4 运行维护管理能力检测要求

7.3.4.1 检测方式

访谈，检查。

7.3.4.2 检测对象

业务及应用相关运行管理规章/制度。

7.3.4.3 检测实施

应按照8.2.4节和本节的要求进行检测：

a) 应访谈安全管理人员、各相关管理、技术、运维人员，询问备份数据验证相关管理制度覆盖的范围，检查验证按介质特性对业务及应用、系统、设备相关各类备份数据是否进行定期的有效性验证；

b) 应访谈安全管理人员、各相关管理、技术、运维人员，询问灾难备份和恢复相关管理制度覆盖的范围，检查验证是否制定针对业务及应用恢复、系统灾难备份的应急运行管理制度。

7.3.5 灾难恢复预案检测要求

7.3.5.1 检测方式

访谈，检查。

7.3.5.2 检测对象

灾难恢复预案，设计/验收文档，演练记录，相关管理制度，安全管理人员。

7.3.5.3 检测实施

应按照8.2.5节和本节的要求进行检测：

a) 应访谈安全管理人员，检查互联网业务及应用系统灾难恢复预案教育和培训记录，检查是否对灾难恢复预案的进行定期教育、培训和演练，验证教育和培训是否达到预期目标；

b) 应访谈安全管理人员，询问是否具有灾难恢复预案，应检查灾难恢复预案管理制度，检查是否按照统一的灾难恢复预案管理制度对系统相应的预案进行管理，检查灾难恢复预案管理、修订相关记录。

7.4 第3.2级要求

同第3.1级要求。

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

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

中华人民共和国
通信行业标准
电信网和互联网信息服务业务系统安全防护检测要求
YD/T 2244-2011

*

人民邮电出版社出版发行
北京市崇文区夕照寺街14号A座
邮政编码：100061
宝隆元（北京）印刷技术有限公司印刷
版权所有 不得翻印

*

开本：880×1230 1/16 2012年1月第1版
印张：2.5 2012年1月北京第1次印刷
字数：62千字

ISBN 978-7-115-2409/11-360

定价：25元

本书如有印装质量问题，请与本社联系 电话：(010)67114922