YD

# 中华人民共和国通信行业标准

YD/T 1741-2008

# 增值业务网——智能网安全防护检测要求

Security Protection Testing Requirements for
Value Added Service Network(Intelligent 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 1740-2008《增值业务网——智能网安全防护要求》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：张大坤、张 园、李友国、王 宇、严斌峰、赖力为

# 增值业务网——智能网安全防护检测要求

## 1 范围

本标准规定了增值业务网——智能网在安全等级保护、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智能网。

## 2 引用标准

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文件。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

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

**智能网安全等级 Security Classification of Transport Network**

智能网安全重要程度的表征。重要程度可从智能网受到破坏后，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

**智能网安全等级保护 Classified Security Protection of Intelligent Network**

对智能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

**智能网安全风险 Security Risk of Intelligent Network**

人为或自然的威胁可能利用智能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

**智能网安全风险评估 Security Risk Assessment of Intelligent Network**

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

3.6

**智能网资产 Asset of Intelligent Network**

智能网中有价值的资源，是安全防护保护的对象。智能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。如基于某个智能网系统的预付费业务、SCP设备、智能网机房管理规定等。

3.7

**智能网资产价值 Asset Value of Intelligent Network**

智能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

**智能网威胁 Threat of Intelligent Network**

可能导致对智能网产生危害的不希望事件的潜在起因，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。如常见的设备节点失效、火灾、水灾等。

3.9

**智能网脆弱性 Vulnerability of Intelligent Network**

脆弱性是智能网中存在的弱点、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

**智能网灾难 Disaster of Intelligent Network**

由于各种原因，造成智能网故障或瘫痪，使智能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

**智能网灾难备份 Backup for Disaster Recovery of Intelligent Network**

为了智能网灾难恢复而对相关网络要素进行备份的过程。

3.12

**智能网灾难恢复 Disaster Recovery of Intelligent Network**

为了将智能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。

3.14

**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，获取证据以检查智能网安全等级保护、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。

3.15

**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，获取证据以检查智能网安全等级保护、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

**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，获取证据以检查智能网安全等级保护、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。

| | | |
|---|---|---|
| IP | Intelligent Peripheral | 智能外设 |
| SCP | Service Control Point | 业务控制点 |
| SDP | Service Data Point | 业务数据点 |
| SMP | Service Management Point | 业务管理点 |
| SSP | Service Switch Point | 业务交换点 |
| VC | Voucher Center | 充值中心 |

## 5 智能网安全防护检测概述

### 5.1 智能网安全防护检测范围

本标准的安全防护检测范围是智能网。根据YD/T 1740-2008《增值业务网——智能网安全防护要求》，本标准主要对智能网的安全等级保护、安全风险评估、灾难备份及恢复等工作的实施进行检测。

智能网安全等级保护的检测范围确定以后，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 安全防护检测对象

智能网安全防护检测对象是本地智能网、全省智能网和全国智能网。

### 5.3 智能网安全防护检测内容

按照智能网安全防护检测的需要，将智能网安全防护检测分为智能网安全等级保护、智能网安全风险评估和智能网灾难备份及恢复等三个部分。

智能网安全防护检测要求包括以下一些内容：

——智能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、设备安全检测、物理安全检测、管理安全检测等；

——智能网安全风险评估检测

主要包括风险评估范围、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；

——智能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、冗余路由检测、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。

### 5.4 智能网安全防护检测结果判定

智能网安全防护检测包括对智能网的安全等级保护、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）。参照表1将各评测项得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 |
|---|---|
| 25% | 业务安全 |
| 25% | 网络安全 |
| 10% | 设备安全 |
| 10% | 物理环境安全 |
| 30% | 管理安全 |



## 6　智能网安全等级保护检测要求

### 6.1　第1级

不做要求。

### 6.2　第2级

#### 6.2.1　智能网业务安全

##### 6.2.1.1　检测方式

访谈，检查，测试。

##### 6.2.1.2　检测对象

网络设计/验收文档，历史记录。

##### 6.2.1.3　检测实施

a）应访谈智能网管理员，并查看智能网设计/验收文档，历史记录，了解目前智能网的业务提供安全情况；

b）应访谈网络管理员，查看网络设计/验收文档、历史记录，并抽查操作员密码，检查 SCP、SMP 等设备的系统及操作员密码是否进行加密处理；

c）应访谈网络管理员，查看网络设计/验收文档、用户投诉记录等，并进行测试，检查计费信息是否正确、不丢失、不重复，检查计费信息是否能被修改，检查原始话单是否能被增加。

#### 6.2.2 智能网网络安全

##### 6.2.2.1 检测方式

访谈，检查。

##### 6.2.2.2 检测对象

网络设计/验收文档，网络拓扑结构。

##### 6.2.2.3 检测实施

a）应访谈智能网管理人员，并查看网络设计/验收文档，了解目前智能网的实际部署情况；

b）应访谈智能网管理人员，并查看网络设计/验收文档，检查智能网网络中（如SCP和SMP、SMP与账务系统之间）是否采用专网。

#### 6.2.3 智能网设备安全

##### 6.2.3.1 检测方式

访谈，检查。

##### 6.2.3.2 检测对象

设备入网检测报告，设备入网证。

##### 6.2.3.3 检测实施

应访谈相关技术支持人员和管理人员，检查设备是否有入网检测报告、设备入网证、安全检测报告等。



#### 6.2.4 智能网物理环境安全

应满足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》中第2级的安全要求。

#### 6.2.5 智能网管理安全

应满足YD/T 1756-2008《电信网和互联网管理安全等级保护检测要求》中第2级的安全要求。

### 6.3 第 3.1 级

#### 6.3.1 智能网业务安全

##### 6.3.1.1 检测方式

访谈，检查，测试。

##### 6.3.1.2 检测对象

网络设计/验收文档，历史记录。

##### 6.3.1.3 检测实施

除按照第2级的要求进行检测之外，还应按照以下内容进行检测：

a）应访谈网络管理员，查看网络设计/验收文档，历史记录，并进行测试，检查智能网对涉及到用户卡号密码等敏感信息如何传输，并判断传输方式是否有效；

b）应访谈网络管理员，查看网络设计/验收文档，历史记录，检查智能网卡号信息如何生成、传输和管理，并判断以上方式是否满足保密要求。

#### 6.3.2 智能网网络安全

##### 6.3.2.1 检测方式

访谈，检查。

##### 6.3.2.2 检测对象

网络设计/验收文档，网络拓扑结构。

##### 6.3.2.3 检测实施

除按照第 2 级的要求进行检测之外，还应按照以下内容进行检测：

a）应访谈智能网管理人员，并查看网络设计/验收文档，了解目前智能网的实际部署情况；

b）应访谈智能网管理人员，并查看网络设计/验收文档，并到现场检查，检查智能网的网络配置（如节点和链路的处理能力或负荷等）是否合理。

#### 6.3.3 智能网物理环境安全

应满足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》中第3.1级的安全要求。

#### 6.3.4 智能网管理安全

应满足YD/T 1756-2008《电信网和互联网管理安全等级保护检测要求》中第3.1级的安全要求。

### 6.4 第 3.2 级

#### 6.4.1 智能网业务安全

##### 6.4.1.1 检测方式

访谈，检查，测试。

##### 6.4.1.2 检测对象

网络设计/验收文档，历史记录。

##### 6.4.1.3 检测实施

除按照第 3.1 级的要求进行检测之外，还应按照以下内容进行检测。

a）应访谈网络管理员，并查看网络设计/验收文档、历史升级方案及记录，检查设备是否能够保证在运行的智能网系统上引入新业务、升级业务或者升级系统时不会引起智能网所提供业务的中断或系统瘫痪；

b）应访谈智能网管理员，并查看智能网设计/验收文档、历史记录，检查重要业务数据及计费数据是否进行备份（包括不同物理位置、不同存储格式、不同存储介质等）。

#### 6.4.2 智能网网络安全

##### 6.4.2.1 检测方式

访谈，检查。

##### 6.4.2.2 检测对象

网络设计/验收文档，网络拓扑结构。

##### 6.4.2.3 检测实施

除按照第 3.1 级的要求进行检测之外，还应按照以下内容进行检测。

a）应访谈智能网管理人员，并查看网络设计/验收文档，并到现场检查，检查网络拓扑设计是否合理，是否充分考虑连接的冗余设置，是否存在因单点故障而影响其他节点间数据传送的节点；

b）应访谈智能网管理人员，并查看网络设计/验收文档，并到现场检查，检查重要设备是否有异地备份，互为备份的设备是否在两个不同的机房。

#### 6.4.3 智能网物理环境安全

应满足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》中第3.2级的安全要求。

#### 6.4.4 智能网管理安全

应满足YD/T 1756-2008《电信网和互联网管理安全等级保护检测要求》中第3.2级的安全要求。

### 6.5 第 4 级

同第3.2级要求。

### 6.6 第 5 级

待补充。

## 7 智能网安全风险评估检测要求

### 7.1 智能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

风险评估报告。

#### 7.1.3 检测实施

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



### 7.2 智能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

风险评估报告。

#### 7.2.3 检测实施

a）应访谈智能网风险评估负责人，询问风险评估相关内容是否覆盖了技术安全和管理安全两大类，以及技术安全中是否覆盖了业务安全、网络安全、设备安全和物理安全，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；

b）应检查智能网风险评估报告，查看风险评估报告是否覆盖了技术安全和管理安全两大类；

c）应检查智能网风险评估报告，查看风险评估报告中技术安全是否覆盖了业务安全、网络安全、设备安全和物理安全等方面；

d）应检查智能网风险评估报告，查看风险评估报告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、系统建设管理、系统运维管理等方面。

### 7.3 智能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

风险评估报告，历史记录。

#### 7.3.3 检测实施

a）应访谈风险评估负责人，询问进行智能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，检查智能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，询问进行智能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，检查智能网风险评估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）应访谈风险评估负责人，询问进行智能网风险评估时评估了哪些资产；查看风险评估报告，检查智能网风险评估时的资产是否包含了网络设备（智能网包括SCP、SDP、SSP、SMP、IP、VC等设备）；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，网络提供的各类业务，网络拓扑，设备维护人员，各种管理规定和设备文档，码号资源等。

d）应访谈风险评估负责人，询问计算智能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，检查智能网风险评估中，计算各资产的资产价值时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，询问识别智能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，检查智能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，询问识别智能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，检查智能网风险评估中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。

g）应访谈风险评估负责人，询问对智能网存在哪些威胁；查看风险评估报告，检查智能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，检查智能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，检查智能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，检查智能网风险评估中确定的风险阈值是否合理。

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，检查智能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 智能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

风险评估报告。

#### 7.4.3 检测实施

a）应访谈风险评估负责人，询问智能网风险评估时对资产的赋值遵循了什么原则；查看风险评估报告，检查智能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个等级进行的。

b）应访谈风险评估负责人，询问智能网风险评估时对脆弱性的赋值遵循了什么原则；查看风险评估报告，检查智能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，询问智能网风险评估时对威胁的赋值遵循了什么原则；查看风险评估报告，检查智能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 智能网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，询问智能网风险评估中采用了什么方法计算资产价值；查看风险评估报告，检查智能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，询问智能网风险评估中采用了什么方法计算风险值；查看风险评估报告，检查智能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 智能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了处理计划，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 智能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 智能网灾难备份及恢复检测要求

### 8.1 第1级

不做要求。

### 8.2 第2级

#### 8.2.1 智能网冗余系统、冗余设备及冗余链路

##### 8.2.1.1 检测方式

访谈，检查。

8.2.1.2 检测对象

智能网系统，设计/验收文档，演练文档。

8.2.1.3 检测实施

应检查智能网的冗余设备系统、设备及链路，是否成对配置，在某个模块或链路出现故障时，是否能够由备用系统代替工作。

8.2.2 智能网冗余路由

8.2.2.1 检测方式

访谈，检查。

8.2.2.2 检测对象

设计/验收文档，历史记录，演练记录。

8.2.2.3 检测实施

a）应访谈安全管理人员，询问智能网的物理链路是否采用了冗余路由；

b）应检查智能网物理链路，查看其冗余路由是否与设计一致；

c）应检查演练记录和历史记录，查看智能网是否有流量负荷分担的功能，是否满足要求。

8.2.3 智能网人员和技术支持能力

8.2.3.1 检测方式

访谈，检查。

8.2.3.2 检测对象

历史值班记录，培训记录。

8.2.3.3 检测实施

应访谈安全管理相关人员，询问并查看历史值班记录，检查是否有负责灾难备份及恢复的机房运行管理人员，检查相关人员对灾难备份及恢复的技术支持能力。

8.2.4 智能网运行维护管理能力

8.2.4.1 检测方式

访谈，检查。

8.2.4.2 检测对象

管理制度，安全管理人员。

8.2.4.3 检测实施

a）应访谈安全管理人员，询问并查看机房运行管理制度，检查是否有完善的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，检查是否有完善的针对灾难备份及恢复的介质存取、验证和转储管理制度，检查备份数据的授权访问情况。

8.2.5 智能网灾难恢复预案

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，演练记录，管理制度。

8.2.5.3 检测实施

应访谈安全管理人员，询问并查看灾难恢复预案，检查智能网是否具有完整的灾难恢复预案，是否与设计/验收文档一致。

8.3 第3.1级

8.3.1 智能网冗余系统、设备及链路

8.3.1.1 检测方式

访谈，检查。

8.3.1.2 检测对象

智能网系统，设计/验收文档，演练文档。

8.3.1.3 检测实施

除按照第2级的要求进行检测之外，还应按照以下内容进行检测。

应检查智能网的业务软件是否有备份，当主业务软件出现故障时，是否能够由备用业务软件代替工作。

8.3.2 智能网备份数据

8.3.2.1 检测方式

访谈，检查。

8.3.2.2 检测对象

设计/验收文档，演练历史记录。

8.3.2.3 检测实施

除按照第2级的要求进行检测之外，还应按照以下内容进行检测。

a）访谈智能网安全管理人员，询问知否支持重要数据（如业务数据、网络配置数据、告警数据、加密密钥、用户属性等）的本地定期备份。

b）应检查设计/验收文档，查看智能网是否支持重要数据的本地定期备份。

c）应检查智能网数据备份服务器，查看其与设计文档是否一致。

d）应检查演练历史记录，查看智能网数据备份范围和时间间隔、数据恢复能力是否与设计文档一致。

8.3.3 人员和技术支持能力

8.3.3.1 检测方式

访谈，检查。

8.3.3.2 检测对象

设备管理人员，网络管理人员，技术支持人员，历史值班记录，培训记录。

8.3.3.3 检测实施

除按照第2级的要求进行检测之外，还应按照以下内容进行检测。

a）应访谈安全管理相关人员，询问并查看历史值班记录，检查是否有负责灾难备份及恢复的设备管理人员，检查相关人员对灾难备份及恢复的技术支持能力。

b）应访谈安全管理相关人员，询问并查看历史值班记录，检查是否有负责灾难备份及恢复的网络管理人员，检查相关人员对灾难备份及恢复的技术支持能力。

c）应访谈安全管理相关人员，询问并查看历史值班记录，检查是否有负责灾难备份及恢复的技术支持人员，检查相关人员对灾难备份及恢复的技术支持能力。

d）应访谈安全管理相关人员，询问并查看培训记录，检查对负责灾难备份及恢复的人员定期进行灾难备份及恢复方面技能培训的情况。

#### 8.3.4 运行维护管理能力

##### 8.3.4.1 检测方式

访谈，检查。

##### 8.3.4.2 检测对象

设备和网络运行管理制度，联络和协作的记录，数据异地实时容灾备份管理制度。

##### 8.3.4.3 检测实施

除按照第2级的要求进行检测之外，还应按照以下内容进行检测。

a）应访谈安全管理人员，询问并检查按介质特性对灾难备份及恢复相关数据定期进行有效性验证的情况。

b）应访谈安全管理人员，询问并查看设备和网络运行管理制度，检查是否有完善的针对灾难备份及恢复的设备和网络运行管理制度。

c）应访谈安全管理人员，询问并查看与其他组织进行联络和协作的记录，检查智能网内部是否具有与外部组织保持良好联络和协作的能力。

#### 8.3.5 智能网灾难恢复预案

##### 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、演练、调整记录和管理制度。

##### 8.3.5.3 检测实施

除按照第2级的要求进行检测之外，还应按照以下内容进行检测。

a）应访谈安全管理人员，询问并查看灾难恢复预案的教育和培训记录，检查对灾难恢复预案进行教育和培训的情况，检查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，询问并查看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

#### 8.4.1 智能网冗余系统、冗余设备及冗余链路

##### 8.4.1.1 检测方式

访谈，检查。

##### 8.4.1.2 检测对象

智能网系统，设计/验收文档，演练文档。

8.4.1.3 检测实施

除按照第3.1级的要求进行检测之外，还应按照以下内容进行检测。

应检查智能网的冗余设备系统是否在异地备份，如SCP、VC等设备。

8.4.2 智能网冗余路由

8.4.2.1 检测方式

访谈，检查。

8.4.2.2 检测对象

设计/验收文档、历史记录、演练记录。

8.4.2.3 检测实施

除按照第3.1级的要求进行检测之外，还应按照以下内容进行检测。

应检查设计/验收文档，查看重要地区、骨干智能网的物理链路是否采用了冗余路由，包括SCP和SSP之间、SCP和IP之间、SCP和SDP之间及SSP和IP之间的路由。

8.4.3 智能网备份数据

8.4.3.1 检测方式

访谈，检查。

8.4.3.2 检测对象

设计/验收文档，演练历史记录。

8.4.3.3 检测实施

除按照第3.1级的要求进行检测之外，还应按照以下内容进行检测。

a）访谈智能网安全管理人员，询问知否支持重要数据（如业务数据、网络配置数据、告警数据、加密密钥、用户属性等）的不同的位置定期备份；

b）应检查设计/验收文档，查看智能网是否支持重要数据的异地定期备份。

8.4.4 运行维护管理能力

8.4.4.1 检测方式

访谈，检查。

8.4.4.2 检测对象

设备和网络运行管理制度，联络和协作的记录，数据异地实时容灾备份管理制度。

8.4.4.3 检测实施

除按照第3.1级的要求进行检测之外，还应按照以下内容进行检测：

应访谈安全管理人员，询问并查看数据异地实时容灾备份管理制度，检查是否有完善的针对灾难备份及恢复的数据异地实时容灾备份管理制度。

8.4.5 智能网灾难恢复预案

8.4.5.1 检测方式

访谈，检查。

8.4.5.2 检测对象

灾难恢复预案，设计/验收文档，演练记录，管理制度。

#### 8.4.5.3 检测实施

除按照第 3.1 级的要求进行检测之外，还应按照以下内容进行检测。

应检查智能网管理制度，查看其是否具有灾难恢复预案管理制度。

### 8.5 第 4 级

同第3.2级要求。

### 8.6 第 5 级

待补充。

中 华 人 民 共 和 国
通 信 行 业 标 准
**增值业务网——智能网安全防护检测要求**
YD/T 1741-2008
*
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
北京新瑞铭印刷有限公司印刷

*
开本：880×1230　1/16　　2008 年 1 月第 1 版
印张：1.5　　2008 年 1 月北京第 1 次印刷
字数：38 千字
ISBN 978 - 7 - 115 - 1630/08 - 74
定价：15 元
本书如有印装质量问题，请与本社联系 电话：(010)67114922