YD

中华人民共和国通信行业标准

YD/T 1733-2008

固定通信网安全防护检测要求

Security Protection Testing Requirements for Fixed Communication 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 1732-2008《固定通信网安全防护要求》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、中国网络通信集团公司、中国电信集团公司、中国联合通信有限公司

本标准主要起草人：魏　薇、黄　颖、魏梦瑜、刘洪声、王新峰、顾旻霞

固定通信网安全防护检测要求

1 范围

本标准规定了固定通信网在安全等级保护、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。本标准仅规定了固定通信网中交换网的安全防护检测要求。

本标准适用于公众电信网中固定通信网的交换网。

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。

GB/T 5271.8-2001 信息技术 词汇 第8部分：安全

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 1748-2008 信令网安全防护检测要求

YD/T 1751-2008 同步网安全防护检测要求

YD/T 1753-2008 支撑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、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

固定通信网安全等级 Security Classification of Fixed Telecommunication Network

固定通信网安全重要程度的表征。重要程度可从固定通信网受到破坏后，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。

3.1.2

固定通信网安全等级保护 Classified Security Protection of Fixed Telecommunication Network

对固定通信网分等级实施安全保护。

3.1.3

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。

3.1.4

固定通信网安全风险 Security Risk of Fixed Telecommunication Network

人为或自然的威胁可能利用固定通信网中存在的脆弱性，导致安全事件的发生及其对组织造成的影响。

3.1.5

固定通信网安全风险评估 Security Risk Assessment of Fixed Telecommunication Network

指运用科学的方法和手段，系统地分析固定通信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，防范和化解固定通信网安全风险，将风险控制在可接受的水平，为最大限度地保障固定通信网的安全提供科学依据。

3.1.6

固定通信网资产 Asset of Fixed Telecommunication Network

固定通信网中具有价值的资源，是安全防护保护的对象。固定通信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，如固定通信网的交换机设备、网络布局等。

3.1.7

固定通信网资产价值 Asset value of Fixed Telecommunication Network

固定通信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。

3.1.8

固定通信网威胁 Threat of Fixed Telecommunication Network

可能导致对固定通信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。常见的固定通信网络威胁有光缆中断、设备节点失效、火灾、水灾等。

3.1.9

固定通信网脆弱性 Vulnerability of Fixed Telecommunication Network

脆弱性是固定通信网中存在的弱点、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。

3.1.10

固定通信网灾难 Disaster of Fixed Telecommunication Network

各种原因造成的固定通信网故障或瘫痪，使固定通信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。

3.1.11

固定通信网灾难备份 Backup for Disaster Recovery of Fixed Telecommunication Network

为了固定通信网灾难恢复而对相关网络要素进行备份的过程。

3.1.12

固定通信网灾难恢复 Disaster Recovery of Fixed Telecommunication Network

为了将固定通信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。

3.1.13

固定通信网相关系统 Systems of Fixed Telecommunication Network

组成固定通信网的相关系统，包括接入网、传送网、IP承载网、信令网、同步网、支撑网等。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，而支撑网则包括业务支撑和网管系统。

3.1.14

访谈 Interview

检测人员通过与固定通信网有关人员（个人/群体）进行交流、讨论等活动，检查固定通信网安全等级保护、固定通信网安全风险评估和固定通信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。

3.1.15

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，检查固定通信网安全等级保护、固定通信网安全风险评估和固定通信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。

3.1.16

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，查看、分析输出结果，检查固定通信网安全等级保护、固定通信网安全风险评估和固定通信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。

3.2 缩略语

下列缩略语适用于本标准。

IP	Internet Protocol	网际协议
IPSec	Internet Protocol Security	IP 安全
PSTN	Public Switched Telephone Network	公众电话交换网
TCP	Transmission Control Protocol	传输控制协议

4 固定通信网安全防护检测概述

4.1 安全防护检测范围

固定通信网的安全防护范畴包括交换网（PSTN和软交换网络）以及与交换网运行和业务提供相关的接入网、传送网、IP承载网、信令网、同步网、支撑网等相关系统。本标准仅对固定通信网中的交换网提出安全防护检测要求，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》，信令网安全防护检测的具体要求参见YD/T 1749-2008《信令网安全防护检测要求》，同步网安全防护检测的具体要求参见YD/T 1751-2008《同步网安全防护检测要求》，支撑网安全防护检测的具体要求参见YD/T 1753-2008《支撑网安全防护检测要求》。

4.2 安全防护检测对象

固定通信网安全防护检测对象是各个本地网或者本地网的端局、汇接局、关口局，省内长途网，省际长途网（含国际长途网）。安全等级保护的检测对象确定后，安全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 安全防护检测内容

按照固定通信网安全防护检测的需要，将固定通信网安全防护检测分为固定通信网安全等级保护检测、固定通信网安全风险评估检测和固定通信网灾难备份及恢复检测三个部分。

固定通信网安全防护检测要求包括以下内容。

a）固定通信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、物理环境安全检测、管理安全检测等。

b）固定通信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。

c）固定通信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。

4.4 安全防护检测结果判定

固定通信网安全防护检测包括对固定通信网的安全等级保护、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给出了安全等级保护子类所占的比重。固定通信网安全防护检测的结果还应充分考虑到支持固定通信网运行的各相关系统的检测结果。

表1 检测项评分方法

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
$4.5 \leqslant x \leqslant 5$	很好
$3.5 \leqslant x < 4.5$	较好

表 2（续）

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

表3 安全等级保护子类所占的比重

比重（%）	安全等级保护子类
20	业务安全
20	网络安全
10	设备安全
10	物理环境安全
40	管理安全

5 固定通信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 业务提供安全

5.2.1.1.1 检测方式

访谈，检查。

5.2.1.1.2 检测对象

设备运行日志，用户投诉及处理记录，故障记录，入网测试报告，网络设备。

5.2.1.1.3 检测实施

a）应访谈网络管理员，查看设备运行日志、用户投诉及处理记录，检查交换网是否发生因为过负荷或者突发业务量而影响网络安全的情况；如果发生过安全事件，通过查看故障记录检查事件的处理情况。

b）应访谈网络管理员，查看交换网设备入网测试报告中的性能检测部分，检查当网络拥塞时交换网能对特定的通信予以保证的情况，例如对维护操作呼叫予以优先保证；通过查看实际的网络设备和设备运行日志，检查网络设备是否具有当网络拥塞对特定通信予以优先保证的功能。

c）应访谈网络管理员，查看设备运行日志、故障记录、用户投诉及处理记录，检查后台计费系统毁坏是否影响交换网的业务提供。

5.2.1.2 业务数据安全

5.2.1.2.1 检测方式

访谈，检查，测试。

5.2.1.2.2 检测对象

网络设计/验收文档，备份数据，相关数据库，操作维护人员的使用手册，网络和业务运营商提供的其他文档。

5.2.1.2.3 检测实施

a） 应访谈网络管理员，查看实际的备份数据，检查交换网对重要的业务数据进行备份（包括不同物理位置、不同存储格式、不同存储介质等）的情况，以及必要时对数据进行恢复的情况；检查数据的备份及恢复情况是否符合设计要求。

b） 应访谈网络管理员，对实际网络进行检查和测试，检查用于操作维护的系统密码等重要数据在数据库中是否以明文显示；检测交换网是否能对重要数据的访问权限采用身份认证与授权的方式进行限制；检查重要数据的加密和访问权限管理的设计文档，现场检查这些功能是否符合设计要求。

5.2.2 网络安全

5.2.2.1 PSTN 安全

5.2.2.1.1 检测方式

访谈，检查。

5.2.2.1.2 检测对象

网络设计/验收文档，网络拓扑图，设备运行日志，网络设备。

5.2.2.1.3 检测实施

a） 应访谈网络管理员，并查看 PSTN 拓扑图，检查是否与 PSTN 当前运行情况相符合。

b） 应访谈网络管理员，查看网络设计/验收文档，并现场检查 PSTN 的端局到同一长途局是否具备了双路由，是否与设计相符合。

c） 应访谈网络管理员，查看网络设计/验收文档，并现场检查 PSTN 中设备的关键部件（包括中央处理机结构、交换矩阵、铃流源、二次电源、时钟板必须采用冗余设计）是否采用主备热备份的结构，是否与设计相符合。

d） 应访谈网络管理员，查看对设备进行配置、监控等操作的界面，检查 PSTN 中的设备是否均是网络和业务运营商可控和可管理的，是否能够确保合法且通过认证的交换机设备和管理终端才能够进入交换网。

e） 应访谈网络管理员，检查交换机与操作维护接口是否采用了专线的方式，是否能保证数据通信的安全；对于未采用专线的情况，检查当交换机与操作维护接口采用 TCP/IP 传输时，是否提供必要的安全机制，例如可以对传输的数据采用 IPSec 等安全技术进一步处理。

5.2.2.2 软交换网络

5.2.2.2.1 软交换网络拓扑安全

5.2.2.2.1.1 检测方式

访谈，检查。

5.2.2.2.1.2 检测对象

网络设计/验收文档，软交换网络拓扑图，入网检测报告，故障记录，软交换网络中的设备。

5.2.2.2.1.3 检测实施

a） 应访谈网络管理人员，查看软交换网络拓扑图，检查是否与软交换网络当前运行情况相符合。

b） 应访谈网络管理人员，查看网络设计/验收文档，并现场查看软交换的网络配置情况，检查网络配置是否合理，各节点和链路的位置、数量、负荷分担分配比例的实际配置是否与设计相符合；查看故障记录，检查是否发生过因网络配置不合理而导致的网络全部或者局部瘫痪事件。

c） 应访谈网络管理员，并现场检查软交换网络与互联网间的边界关口是否采取了安全措施（例如防火墙配置，常用端口屏蔽等），安全措施是否与设计相符合。

5.2.2.2.2 软交换网络通信安全

5.2.2.2.2.1 检测方式

访谈，检查。

5.2.2.2.2.2 检测对象

网络设计/验收文档，投诉记录，故障记录，软交换网络中的设备。

5.2.2.2.2.3 检测实施

a） 应访谈网络管理员，查看投诉记录，并现场检查软交换网络采取了哪些措施对传送的管理信息进行保护，是否能够防止信息被非法或恶意地窃听、篡改。

b） 应访谈网络管理员，询问软交换网络采取了哪些保护信令流通信安全的措施；现场检查软交换网络是否落实了这些安全措施，并保证会话建立过程中信令流的通信安全，安全措施是否与设计相符合。

c） 应访谈网络管理员，查看网络设计/验收文档，检查软交换网络采取了哪些保证媒体流传输过程中的保密性、完整性的措施，保护措施是否有效；通过查看故障记录，检查是否存在通信数据保密性、完整性缺失的情况。

5.2.2.2.3 软交换网络攻击防范

5.2.2.2.3.1 检测方式

访谈，检查，测试。

5.2.2.2.3.2 检测对象

网络设计/验收文档，用户投诉及处理记录，故障记录，软交换网络中的设备。

5.2.2.2.3.3 检测实施

a） 应访谈网络管理员，通过对软交换网络中的设备进行配置，检查软交换网络中的设备是否均是网络和业务运营商可控、可管理的，是否能够确保合法且通过认证的设备（软交换设备、媒体网关、信令网关、媒体服务器、应用服务器、软交换业务接入控制设备、接入网关、软交换网络管理终端等）才能够进入软交换网络，是否有不明设备接入软交换网络的情况。

b） 应访谈网络管理员，并现场检查网络或设备发生故障或故障消失时是否能及时产生告警信息并发送至网元管理系统，是否与设计相符合。

5.2.3 设备安全

5.2.3.1.1 检测方式

访谈，检查。

5.2.3.1.2 检测对象

设备入网检测报告，设备入网证，设备安全检测报告。

5.2.3.1.3 检测实施

应访谈相关技术支持人员和管理人员，检查设备（PSTN 主要包括交换机设备，软交换网络包括软交换设备、媒体网关、信令网关、媒体服务器、应用服务器、软交换业务接入控制设备、接入网关等）是否有入网检测报告、入网证。

5.2.4 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。

5.2.5 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。

5.3 第 3.1 级要求

5.3.1 业务安全

5.3.1.1 业务提供安全

5.3.1.1.1 检测方式

访谈，检查。

5.3.1.1.2 检测对象

设备运行日志，用户投诉及处理记录，故障记录，入网测试报告，网络设备。

5.3.1.1.3 检测实施

除按照5.2.1.1的要求进行检测之外，还应按照本节内容进行检测。

a） 应访谈网络管理员，查看软交换设备的入网测试报告，检查软交换设备发生故障或与媒体网关连接中断时，是否影响正在通话的呼叫；查看设备运行日志、故障记录、用户投诉及处理记录，检查是否发生过软交换设备发生故障或与媒体网关连接中断而影响正在进行的通话的情况。

b） 应访谈网络管理员，询问交换设备提供的业务是否受系统引入其他新业务、系统补丁加载的影响；查看交换设备运行日志、用户投诉及处理记录，检查交换设备提供的业务是否存在因为系统引入其他新业务、系统补丁加载而中断的情况。

5.3.1.2 业务数据安全

5.3.1.2.1 检测方式

访谈，检查，测试。

5.3.1.2.2 检测对象

网络设计/验收文档，备份数据，相关数据库，操作维护人员的使用手册，网络和业务运营商提供的其他文档。

5.3.1.2.3 检测实施

除按照5.2.1.2的要求进行检测之外，还应按照本节内容进行检测。

a） 应访谈网络管理员，查看交换设备的计费功能、计费相关数据库，检查计费信息在交换设备中的存储情况是否满足相关要求，包括存储时间、存储方式等；存储时间是否不少于 24h，未被采集前是否不被删除。

b） 应访谈网络管理员，查看操作维护人员的使用手册，检查重要数据（如计费数据）所占存储空间达到阈值时，系统是否能产生相应的告警信息。

c） 应访谈网络管理员，对操作维护人员口令进行实际配置，并以不同级别的操作维护人员登录和操作，检查对操作维护人员账户权限分级管理的情况以及对操作维护人员身份进行认证的情况；检查是否能够及时删除临时账户；通过查看日志，检查是否能够记录操作维护人员对业务所进行的任何操作，通过实际查询操作，检查对操作维护信息进行查询的情况；查看网络设备的相关配置及操作手册，检查操作维护信息保存时间是否符合相关设计要求。

5.3.2 网络安全

5.3.2.1 PSTN 安全

5.3.2.1.1 检测方式

访谈，检查。

5.3.2.1.2 检测对象

网络设计/验收文档，网络拓扑图，设备运行日志，网络设备。

5.3.2.1.3 检测实施

除按照 5.2.2.1 的要求进行检测之外，还应按照本节内容进行检测：应访谈网络管理员，查看网络设计/验收文档，并现场检查 PSTN 的汇接局是否采用了双局设置，端局到汇接局应具备双归属能力，是否与设计相符合。

5.3.2.2 软交换网络安全

5.3.2.2.1 软交换网络拓扑安全

5.3.2.2.1.1 检测方式

访谈，检查。

5.3.2.2.1.2 检测对象

网络设计/验收文档，软交换网络拓扑图，入网检测报告，故障记录，软交换网络中的设备。

5.3.2.2.1.3 检测实施

除按照5.2.2.2.1的要求进行检测之外，还应按照本节内容进行检测。

a） 应访谈网络管理人员，现场检查软交换网络的软交换设备是否采用多节点工作的方式，是否与设计相符合；查看入网检测报告、故障记录，检查一个节点的损害是否影响业务提供，是否具有对拥塞进行话务控制的功能。

b） 应访谈网络管理员，现场检查软交换网络的关键设备热冗余备份的情况，是否与设计相符合，例如，软交换设备的主处理板、电源和通信板等主要部件是否支持热冗余备份；媒体网关的系统控制模块、外部时钟源、电源、信令链路、数据链路等主要部件是否进行了热冗余备份；信令网关的主处理机部件、数据库部件、管理中心接口、操作维护工作站接口、时钟源输入接口、时钟系统等重要部件是否支持热备份方式。

5.3.2.2.2 软交换网络通信安全

5.3.2.2.2.1 检测方式

访谈，检查。

5.3.2.2.2.2 检测对象

网络设计/验收文档，投诉记录，故障记录，软交换网络中的设备。

5.3.2.2.2.3 检测实施

除按照 5.2.2.2.2 的要求进行检测之外，还应按照本节内容进行检测：应访谈网络管理员，查看投诉记录，并现场检查软交换网络采取的保护传输的媒体流的措施是否考虑了电信监管需求和对媒体流服务质量的影响，是否与设计相符合。

5.3.2.2.3 软交换网络攻击防范

5.3.2.2.3.1 检测方式

访谈，检查。

5.3.2.2.3.2 检测对象

网络设计/验收文档，用户投诉及处理记录，故障记录，软交换网络中的设备。

5.3.2.2.3.3 检测实施

除按照 5.2.2.2.3 的要求进行检测之外，还应按照本节内容进行检测。

a） 应访谈网络管理员，查看用户投诉及处理记录、故障记录，并现场检查软交换网络采取安全对策应对网络攻击的情况，采取的安全对策是否能够有效地防止非法用户利用各种手段对网络发起的攻击，是否发生过网络攻击造成网络及设备无法正常工作或瘫痪的情况，安全对策是否与网络设计/验收文档相符合，安全对策可以是防病毒软件、系统加固、网络隔离、防火墙、访问控制等。

b） 应访谈网络管理员，并现场检查软交换网络部署基于主机和基于网络的入侵检测系统的情况，是否能及时处理入侵检测系统的报警，入侵检测系统的部署情况是否与设计相符合。

c） 应访谈网络管理员，并现场检查对软交换网络中关键的主机系统和网络定期进行安全检查的情况，是否具有检查出网络弱点和策略配置上的问题的能力；是否使用安全扫描软件进行检查，采取的安全扫描软件是否与设计相符合。

5.3.3 设备安全

应满足5.2.3的检测要求。

5.3.4 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3.1级的检测要求。

5.3.5 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 3.1 级的检测要求。

5.4 第 3.2 级要求

5.4.1 业务安全

应满足5.3.1的检测要求。

5.4.2 网络安全

5.4.2.1 PSTN 安全

5.4.2.1.1 检测方式

访谈，检查。

5.4.2.1.2 检测对象

网络设计/验收文档，网络拓扑图，设备运行日志，网络设备。

5.4.2.1.3 检测实施

除按照 5.3.2.1 的要求进行检测之外，还应按照本节内容进行检测：应访谈交换网管理人员，查看网络设计/验收文档，并现场检查 PSTN 长途交换局是否采用双局设置，两个长途局是否放在不同的机房中，是否与设计相符合。

5.4.2.2 软交换网络安全

应满足5.3.2.2的检测要求。

5.4.3 设备安全

应满足5.3.3的检测要求。

5.4.4 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3.2级的检测要求。

5.4.5 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 3.2 级的检测要求。

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 固定通信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。

6.1.3 检测实施

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

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。

6.2.3 检测实施

a） 应访谈交换网风险评估负责人，查看风险评估报告，检查交换网风险评估是否覆盖了技术安全和管理安全。

b） 应访谈交换网风险评估负责人，查看风险评估报告，检查交换网风险评估中技术安全是否覆盖了业务安全、网络安全、设备安全和物理环境安全等方面。

c） 应访谈交换网风险评估负责人，查看风险评估报告，检查交换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。

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。

6.3.3 检测实施

a） 应访谈风险评估负责人，询问进行交换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，检查交换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，询问进行交换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，检查交换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，询问进行交换网风险评估时评估了哪些资产；查看风险评估报告，检查交换网风险评估时的资产是否包含了网络设备（PSTN 包括交换机设备；软交换网络包括软交换设备、媒体网关设备、信令网关设备、媒体服务器设备、应用服务器设备、业务接入控制设备、接入网关；PSTN 设备和软交换网络设备相关的链路、操作维护系统）；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、系统控制软件、协议软件、操作维护系统软件，支撑交换网运行的各种重要数据，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，询问计算交换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，检查交换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，询问识别交换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，检查交换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，询问识别交换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，检查交换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，询问交换网存在哪些威胁；查看风险评估报告，检查交换网风险评估时威胁识别是否包含了环境威胁、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，检查交换网风险评估中威胁识别是否依据已有的安全事件报告数据、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，检查交换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，检查交换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，询问对于不可接收的风险，是否制定了相应的风险处理计划；查看风险评估报告，检查交换网风险评估中对于不可接收的风险，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。

6.4.3 检测实施

a） 应访谈风险评估负责人，询问交换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，检查交换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，询问交换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，检查交换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，询问交换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，检查交换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。

6.5.3 检测实施

a） 应访谈风险评估负责人，询问交换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，检查交换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，询问交换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，检查交换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） 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。

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。

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） 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。

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。

7 固定通信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

交换网的冗余系统、冗余设备和冗余链路，运行日志、故障记录，设计/验收文档，演练文档。

7.2.1.3 检测实施

a）应访谈安全管理人员，询问并现场检查采取了哪些措施防止单节点的灾难导致其他节点的业务提供发生异常，安全措施是否与设计/验收文档相符合；查看运行日志、故障记录，检查是否发生过单一地区范围的灾难导致其他地区的业务提供发生异常的情况。

b）应访谈安全管理人员，查看演练文档，检查交换网的网络灾难恢复时间是否能够满足行业管理、网络和业务运营商应急预案的相关要求。

7.2.2 冗余路由

7.2.2.1 检测方式

访谈，检查。

7.2.2.2 检测对象

交换网的路由配置，设计/验收文档，演练记录，故障记录。

7.2.2.3 检测实施

应访谈安全管理人员，询问并查看交换网的路由配置，检查交换网的路由是否支持冗余方式，冗余路由是否都可以传送业务，是否与设计/验收文档相符合，检查 PSTN 端局到同一长途局是否配备了双路由。

7.2.3 备份数据

7.2.3.1 检测方式

访谈，检查。

7.2.3.2 检测对象

交换网的数据备份介质，设计/验收文档，演练记录。

7.2.3.3 检测实施

a） 应访谈安全管理人员，询问并查看数据备份介质，检查交换网中关键数据（如计费数据、用户数据、网络配置数据、管理员操作维护记录）本地备份的情况。

b） 应访谈安全管理人员，询问并查看数据备份介质、演练记录，检查交换网关键数据的备份范围和时间间隔、采取的备份方式、数据恢复能力，是否与设计/验收文档一致。

7.2.4 人员和技术支持能力

7.2.4.1 检测方式

访谈，检查。

7.2.4.2 检测对象

负责灾难备份及恢复的管理人员，历史值班记录。

7.2.4.3 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管理人员，检查相关人员对灾难备份及恢复的支持能力。

7.2.5 运行维护管理能力

7.2.5.1 检测方式

访谈，检查。

7.2.5.2 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。

7.2.5.3 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。

7.2.6 灾难恢复预案

7.2.6.1 检测方式

访谈，检查。

7.2.6.2 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。

7.2.6.3 检测实施

应访谈安全管理人员，询问并查看灾难恢复预案，检查交换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。

7.3 第3.1级要求

7.3.1 冗余系统、冗余设备及冗余链路

7.3.1.1 检测方式

访谈，检查。

7.3.1.2 检测对象

PSTN汇接局，设计/验收文档。

7.3.1.3 检测实施

除按照7.2.1的要求进行检测之外，还应按照本节内容进行检测：应访谈安全管理人员，询问并现场检查PSTN汇接局的双局设置情况，检查是否与设计/验收文档相符合。

7.3.2 冗余路由

应满足7.2.2的检测要求。

7.3.3 备份数据

7.3.3.1 检测方式

访谈，检查。

7.3.3.2 检测对象

交换网的数据备份存储介质，设计/验收文档。

7.3.3.3 检测实施

除按照7.2.3的要求进行检测之外，还应按照本节内容进行检测：应访谈安全管理人员，询问并查看数据备份存储介质，检查交换网中关键数据（如计费数据、网络配置数据）在不同的局址进行备份的情况，是否与设计/验收文档一致。

7.3.4 人员和技术支持能力

7.3.4.1 检测方式

访谈，检查。

7.3.4.2 检测对象

负责灾难备份及恢复的技术人员，历史值班记录，培训记录。

7.3.4.3 检测实施

除按照7.2.4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人员，检查相关人员对灾难备份及恢复的技术能力。

b） 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的技能培训的情况。

7.3.5 运行维护管理能力

7.3.5.1 检测方式

访谈，检查。

7.3.5.2 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。

7.3.5.3 检测实施

除按照7.2.5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，询问并查看数据容灾备份管理制度，检查是否有完善的针对灾难备份及恢复数据的容灾备份管理制度。

d） 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，检查交换网内部是否具有与外部组织保持良好的联络和协作的能力。

7.3.6 灾难恢复预案

7.3.6.1 检测方式

访谈，检查。

7.3.6.2 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。

7.3.6.3 检测实施

除按照7.2.6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，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。

7.4 第3.2级要求

7.4.1 冗余系统、冗余设备及冗余链路

7.4.1.1 检测方式

访谈，检查。

7.4.1.2 检测对象

PSTN长途交换局，设计/验收文档。

7.4.1.3 检测实施

除按照7.3.1的要求进行检测之外，还应按照本节内容进行检测：应访谈安全管理人员，询问并现场检查PSTN长途交换局是否采用了双局配置，是否在不同的物理位置容灾，是否与设计/验收文档相符合。

7.4.2 冗余路由

7.4.2.1 检测方式

访谈，检查。

7.4.2.2 检测对象

交换网的路由配置，设计/验收文档，演练记录，故障记录。

7.4.2.3 检测实施

除按照7.3.2的要求进行检测之外，还应按照本节内容进行检测：应访谈安全管理人员，询问并查看演练记录、故障记录，检查交换网是否有流量负荷分担的功能，是否与设计/验收文档相符合，是否发生过负荷分担能力不足影响网络业务提供的情况。

7.4.3 备份数据

应满足7.3.3的检测要求。

7.4.4 人员和技术支持能力

应满足7.3.4的检测要求。

7.4.5 运行维护管理能力

应满足7.3.5的检测要求。

7.4.6 灾难恢复预案

7.4.6.1 检测方式

访谈，检查。

7.4.6.2 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。

7.4.6.3 检测实施

除按照7.3.6的要求进行检测之外，还应按照本节内容进行检测：应访谈安全管理人员，询问并查看交换网管理制度，检查是否有完善的灾难恢复预案的管理制度。

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

1. YD/T 751-1995　公用电话网局用数字电话交换设备进网检验方法
2. YD/T 1128-2001　电话交换设备总技术规范（补充件 1）
3. YD/T 1534-2006　数字程控交换机信息安全要求及测试方法
4. YD/T 1434-2006　软交换设备总体技术要求（修订版）
5. YD/T 1385-2005　基于软交换的综合接入设备技术要求
6. YD/T 1386-2005　基于软交换的媒体服务器技术要求
7. YD/T 1203-2002　No.7 信令与 IP 的信令网关设备技术规范
8. YD/T 1243.1-2002　媒体网关设备技术要求——IP 中继媒体网关
9. YD/T 1390-2005　基于软交换的应用服务器设备技术要求
10. YDC 004-2002　固定电话用户选择不同长途网络对交换机的技术要求
11. YDN 088-1998　自动交换电话（数字）网技术体制
12. YDN 065-1997　邮电部电话交换设备总技术规范书
13. YDN 065-1997　邮电部电话交换设备总技术规范书（附录）