YD

中华人民共和国通信行业标准

YD/T 1735-2008

移动通信网安全防护检测要求

Security Protection Testing Requirements for
Mobile 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 1735-2008《移动通信网安全防护检测要求》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、中国移动通信集团公司、中国联合通信有限公司、中国电信集团公司

本标准主要起草人：袁　琦、王自亮、刘申建、杨　恒

移动通信网安全防护检测要求

1 范围

本标准规定了移动通信网中的GSM/GPRS/WCDMA/TD-SCDMA网和cdma 2000 1x/HRPD网在安全等级保护、风险评估、灾难备份及恢复等方面的安全防护检测要求，其中WCDMA/TD-SCDMA移动通信网主要对R99版本、R4版本规定了安全防护检测要求。

本标准适用于公用电信移动通信网的安全防护检测。

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 5098-2005	通信局（站）防雷与接地工程设计规范
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 1744-2008	传送网安全防护要求
YD/T 1746-2008	IP 承载网安全防护要求
YD/T 1748-2008	信令网安全防护要求
YD/T 1750-2008	同步网安全防护要求
YD/T 1752-2008	支撑网安全防护要求
YD/T 1754-2008	电信网和互联网物理环境安全等级保护要求
YD/T 1756-2008	电信网和互联网管理安全等级保护要求

3 术语、定义和缩略语

3.1 术语和定义

下列术语和定义适用于本标准。

3.1.1

移动通信网安全等级 Security Classification of Mobile Communication Network

移动通信网安全重要程度的表征。重要程度可从移动通信网受到破坏后，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

移动通信网安全等级保护 Classified Security Protection of Mobile Communication Network

对移动通信网分等级实施安全保护。

3.1.3

组织 Organization

组织是由移动通信网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。

3.1.4

移动通信网安全风险 Security Risk of Mobile Communication Network

人为或自然的威胁利用移动通信网及其管理体系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

移动通信网安全风险评估 Security Risk Assessment of Mobile Communication Network

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

3.1.6

移动通信网资产 Asset of Mobile Communication Network

移动通信网中具有价值的资源是安全防护、保护的对象。移动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，包括频率和码号、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，如移动通信网节点设备、移动通信网的光缆线路、移动通信网的网络布局等。

3.1.7

移动通信网资产价值 Asset Value of Mobile Communication Network

移动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

移动通信网威胁 Threat of Mobile Communication Network

可能导致对移动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。常见的移动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

移动通信网脆弱性 Vulnerability of Mobile Communication Network

脆弱性是移动通信网中存在的弱点、缺陷与不足，不直接对资产造成危害，但可能被威胁利用从而危及资产的安全。

3.1.10

移动通信网灾难 Disaster of Mobile Communication Network

由于各种原因造成移动通信网故障或瘫痪，使移动通信网支持的业务功能停顿或服务水平不可接受、达到特定时间的突发性事件。

3.1.11

移动通信网灾难备份 Backup for Disaster Recovery of Mobile Communication Network

为了移动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

移动通信网灾难恢复 Disaster Recovery of Mobile Communication Network

为了将移动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，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

移动通信网相关系统 Systems of Mobile Communication Network

组成移动通信网的相关系统，包括传送网、IP承载网、信令网、同步网、支撑网等。其中，传送网包括光缆、波分、SDH、微波、卫星等，支撑网则包括业务支撑和网管系统。

3.1.14

访谈 Interview

检测人员通过与移动通信网有关人员（个人/群体）进行交流、讨论等活动，查看移动通信网安全等级保护、移动通信网安全风险评估和移动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。

3.1.15

查看 Examination

检测人员通过对检测对象进行观察、查验和分析等活动，获取证据以证明移动通信网安全等级保护措施、移动通信网风险评估措施和移动通信网灾难备份及恢复措施是否有效。

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，获取证据以证明移动通信网安全等级保护措施、移动通信网风险评估措施和移动通信网灾难备份及恢复措施是否有效。

3.2 缩略语

下列缩略语适用于本标准。

AAA	Authentication, Authorization, and Accounting	认证、授权、计费
AC	Authentication Center	鉴权中心
AUC	Authentication Center	鉴权中心
BG	Border Gateway	边界网关
BSS	Base Station Subsystem	基站子系统
CG	Charging Gateway	计费网关
DNS	Domain Name Server	域名服务器
FA	Foreign Agent	拜访代理
GGSN	Gateway GPRS Support Node	网关 GPRS 支持节点
GSM	Global System for Mobile Communication	全球移动通信系统
GPRS	General Packet Radio Service	通用分组无线业务
HA	Home Agent	归属代理
HRPD	High Rate Packet Data	高速分组数据
IMSI	International Mobile Subscriber Identification	国际移动用户识别码
MSC	Mobile Switch Center	移动交换中心

MS	Mobile Station	移动台
MGW	Media Gateway	媒体网关
MSC	Mobile Switching Center	移动交换中心
PDSN	Packet Data Serving Node	分组数据业务节点
PCF	Packet Control Function	分组控制功能
RNC	Radio Network Controller	无线网络控制器
SGSN	Serving GPRS Support Node	服务 GPRS 支持节点
TD-SCDMA	Time Division Synchronous Code Division Multiple Access	时分同步码分多址
VLR	Visitor Location Register	拜访位置寄存器
WCDMA	Wideband Code Division Multiple Access	宽带码分多址

4 移动通信网安全防护检测概述

4.1 安全防护检测范围

移动通信网是通过无线接入技术为公众用户提供移动通信业务的网络。移动通信网的安全防护检测范畴包括GSM/GPRS/WCDMA/TD-SCDMA网、cdma 2000 1x/HRPD网以及与这些网络运行和业务提供相关的传送网、IP承载网、信令网、同步网、支撑网等，如图1所示。

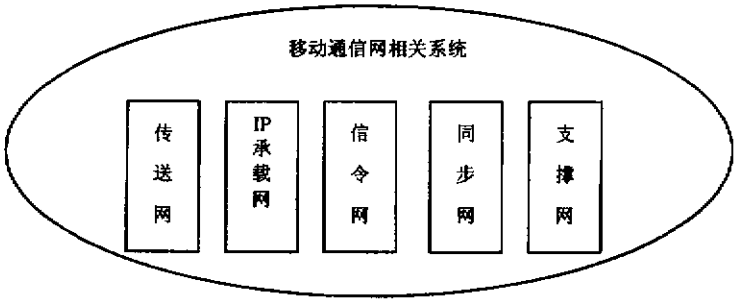

图 1 移动通信网安全防护涉及的相关系统

本标准仅对移动通信网中的GSM/GPRS/WCDMA/TD-SCDMA网和cdma 2000 1x/HRPD网提出安全防护检测要求，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

对GSM/GPRS/WCDMA/TD-SCDMA网进行安全检测时，GSM网检测对象可为本地网、省内长途网、省际长途网（国际部分）。GPRS网检测对象可为省网、国际部分。WCDMA/TD-SCDMA网检测对象分为电路域和分组域。电路域检测对象可为本地网、省内长途网、省际长途网（国际部分）。分组域检测对象可为省网、国际部分。

对cdma 2000 1x/HRPD网进行安全检测时，cdma 2000 1x网检测对象可分为电路域和分组域。电路域检测对象可为本地网、省内长途网、省际长途网（国际部分）。分组域检测对象可为省网、国际部分。HRPD网检测对象可为省网、国际部分。

安全等级保护的检测对象确定以后，风险评估的检测对象、灾难备份及恢复检的测对象应与安全定级保护的检测对象相一致。

4.3 安全防护检测内容

按照移动通信网安全防护检测的需要，将移动通信网安全防护检测分为移动通信网安全等级保护、移动通信网风险评估实施和移动通信网灾难备份及恢复3个部分。

— 移动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、物理安全检测、管理安全检测等。

— 移动通信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。

— 移动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、技术支持能力检测、运行维护管理检测和灾难恢复预案检测等。

4.4 安全防护检测结果判定

移动通信网安全防护检测包括对移动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测试项，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将各测试项的评价等级换算成评分，各测试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，应充分考虑到各测试项在安全防护检测要求中所占的比重，表3给出了安全等级保护子类所占的比重。移动通信网安全防护检测的结果还应充分考虑到支持移动通信网运行的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
$x \geq 4.5$	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
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 移动通信网安全等级保护检测要求

5.1 第1级检测要求

不作要求。

5.2 第2级检测要求

5.2.1 业务安全

5.2.1.1 检测方式

访谈，查看。

5.2.1.2 检测对象

设备运行日志、网络管理系统日志、用户投诉及处理记录、故障记录、入网测试报告、网络设备。

5.2.1.3 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，询问是否接到用户未授权接入业务的投诉，查看对用户在业务接入时是否实现认证机制。

b） 应访谈网络管理员，查看网络设备入网测试报告中的性能检测部分，查看实际的网络设备运行日志、故障记录、用户投诉及处理记录，查看当网络拥塞时移动通信网能对业务连续性予以保证的情况，查看网络设备是否具有当单点故障时业务连续性保证能力。

c） 应访谈网络管理员，查看实际的网络设备运行日志、网络管理系统日志，查看操作维护人员对网络进行的现场操作，是否能够纪录操作维护人员对网络进行的操作，对发布、修改、删除等操作行为是否进行记录，并且是否可以按时间、操作方式、操作人员来查询。

5.2.2 网络安全

5.2.2.1 通用网络安全

5.2.2.1.1 网络拓扑安全

5.2.2.1.1.1 检测方式

访谈，查看。

5.2.2.1.1.2 检测对象

网络拓扑结构，网络拓扑图，网络设计/验收文档，设备运行日志，网络设备。

5.2.2.1.1.3 检测实施

a） 应访谈网络管理人员，查看网络设计/验收文档和历史记录，查看网络设备处理能力是否具备冗余空间，不能由于设备配置不够而导致网络全部或者局部瘫痪，负荷设计的水平是否满足流量高负荷时需求，是否形成单点故障，节假日突发话务量是否会影响网络。

b） 应访谈网络管理人员，查看网络拓扑图，了解目前移动通信网的网络组织情况，查看其与当前运行情况是否一致。

5.2.2.2 GSM网络安全

5.2.2.2.1 检测方式

访谈，查看。

5.2.2.2.2 检测对象

网络设计/验收文档、设备运行日志、入网测试报告、网络设备。

5.2.2.2.3 检测实施

a） 应访谈网络管理人员，查看网络设计/验收文档和入网测试报告，查看设备运行日志，查看网络是否能对接入的用户身份发起鉴权认证，保证授权用户能够接入网络。

b） 应访谈网络管理人员，查看网络设计/验收文档和入网测试报告，查看设备运行日志，查看网络是否提供用户身份的保密措施。在用户初次接入网络的时候 IMSI 才被发送，仅在无线信道上发送移动用户相应的 TMSI。

c） 应访谈网络管理人员，查看网络设计/验收文档和入网测试报告，查看设备运行日志，查看是否在 MS 和 BTS 之间提供数据的加密机制（在国家未对算法作出具体规定之前，对此功能不做要求）。

5.2.2.3 GPRS 网络安全

5.2.2.3.1 检测方式

访谈，查看。

5.2.2.3.2 检测对象

网络设计/验收文档、设备运行日志、入网测试报告、网络设备。

5.2.2.3.3 检测实施

a） 应访谈网络管理人员，查看网络设计/验收文档和入网测试报告，查看设备运行日志，查看对接入的用户身份发起鉴权认证，保证授权用户能够接入网络。

b） 应访谈网络管理人员，查看网络设计/验收文档和入网测试报告，查看设备运行日志，查看是否提供用户身份的保密措施。在用户初次接入网络的时候 IMSI 才被发送，仅在无线信道上发送移动用户相应的 TMSI。

c） 应访谈网络管理人员，查看网络设计/验收文档和入网测试报告，查看设备运行日志，查看是否在 MS 和 SGSN 之间提供数据的加密机制（在国家未对算法作出具体规定之前，对此功能不做要求）。

5.2.2.4 WCDMA/TD-SCDMA 网络安全

5.2.2.4.1 检测方式

访谈，查看。

5.2.2.4.2 检测对象

网络设计/验收文档、设备运行日志、入网测试报告、网络设备。

5.2.2.4.3 检测实施

a） 应访谈网络管理人员，查看网络设计/验收文档和入网测试报告，查看设备运行日志，查看对接入的用户身份发起双向鉴权认证，保证授权用户能够接入网络。

b） 应访谈网络管理人员，查看网络设计/验收文档和入网测试报告，查看设备运行日志，查看是否提供用户身份的保密措施。在用户初次接入网络的时候 IMSI 才被发送，仅在无线信道上发送移动用户相应的 TMSI。

c） 应访谈网络管理人员，查看网络设计/验收文档和入网测试报告，查看设备运行日志，查看是否支持用户和网络之间的密钥协商机制。

d） 应访谈网络管理人员，查看网络设计/验收文档和入网测试报告，查看设备运行日志，查看是否在 MS 和 RNC 之间提供数据的加密机制（在国家未对算法作出具体规定之前，对此功能不做要求）。

e） 应访谈网络管理人员，查看网络设计/验收文档和入网测试报告，查看设备运行日志，查看是否支持对层三 RRC 消息的完整性保护，用于维护信令的完整性。

5.2.2.5 cdma 2000 1x 网络安全

5.2.2.5.1 检测方式

访谈，查看。

5.2.2.5.2 检测对象

网络设计/验收文档、设备运行日志、入网测试报告、网络设备。

5.2.2.5.3 检测实施

a） 应访谈网络管理人员，查看网络设计/验收文档和入网测试报告，查看设备运行日志，并查看是否对接入的用户身份发起鉴权认证，保证授权用户能够接入网络。

b） 应访谈网络管理人员，查看网络设计/验收文档和入网测试报告，查看设备运行日志，查看是否在空中接口的层三提供鉴权和加密的服务。

c） 应访谈网络管理人员，查看网络设计/验收文档和入网测试报告，查看设备运行日志，查看是否在应在 MS 和基站系统之间之间提供数据的加密机制（在国家未对算法作出具体规定之前，对此功能不做要求）。

5.2.2.6 HRPD 网络安全

5.2.2.6.1 检测方式

访谈，查看。

5.2.2.6.2 检测对象

网络设计/验收文档、设备运行日志、入网测试报告、网络设备。

5.2.2.6.3 检测实施

a） 应访谈网络管理人员，查看网络设计/验收文档和入网测试报告，查看设备运行日志，查看是否 AN AAA 对移动台进行无线接入网的认证和授权。

b） 应访谈网络管理人员，查看网络设计/验收文档和入网测试报告，查看设备运行日志，查看是否对接入的用户身份发起鉴权认证，保证授权用户能够接入网络。

c） 应访谈网络管理人员，查看网络设计/验收文档和入网测试报告，查看设备运行日志，查看是否支持空中接口安全层的密钥交换、鉴权和加密服务，安全层使用密钥交换协议、鉴权协议、加密协议和安全协议提供这些功能。

d） 应访谈网络管理人员，查看网络设计/验收文档和入网测试报告，查看设备运行日志，查看是否在应在 MS 和基站系统之间提供数据加密机制(在国家未对算法作出具体规定之前，对此功能不做要求)。

5.2.3 设备安全

5.2.3.1 检测方式

访谈，查看。

5.2.3.2 检测对象

设备入网检测报告、设备入网证、安全检测报告。

5.2.3.3 检测实施

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

5.2.4 物理环境安全

5.2.4.1 机房、办公场地物理环境安全

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。

5.2.4.2 室外无线接入设备场地物理环境安全

5.2.4.2.1 物理位置的选择

5.2.4.2.1.1 检测方式

访谈，检查。

5.2.4.2.1.2 检测对象

室外无线接入设备场地、场地设计/验收文档

5.2.4.2.1.3 检测实施

a） 应访谈物理安全负责人，询问现有室外无线接入设备场地是否具有基本的防震、防风和防雨等能力，是否出现过由于防震、防风、防雨能力不足造成的安全事件，有没有及时采取补救措施；检查场地的设计/验收文档，查看是否有场地所在地建筑能够具有防震、防风和防雨等能力的说明；检查场地是否在具有防震、防风和防雨等能力的建筑内。

b） 应查看场地设计文档，检查场地承重是否满足承重要求。

5.2.4.2.2 防盗窃和防破坏

5.2.4.2.2.1 检测方式

访谈，检查。

5.2.4.2.2.2 检测对象

场地设施、设备管理制度文档、通信线路布线文档、防盗报警系统和监控报警系统的安装测试/验收报告。

5.2.4.2.2.3 检测实施

a） 应访谈维护人员，询问主要设备放置位置是否做到安全可控，设备或主要部件是否进行了固定和标记，通信线缆是否铺设在隐蔽处。

b） 应检查主要设备是否放置在机房内或其他不易被盗窃和破坏的可控范围内；检查主要设备或设备的主要部件的固定情况，是否不易被移动或被搬走，是否设置明显的无法除去的标记。

c） 应检查通信线缆铺设是否在隐蔽处（如铺设在地下或管道中等）。

d） 应检查是否有设备管理制度文档、通信线路布线文档；查看文档中的条文是否与设备放置位置、设备或主要部件保护、通信线缆铺设等实际情况一致。

5.2.4.2.3 防雷击

5.2.4.2.3.1 检测方式

访谈，检查。

5.2.4.2.3.2 检测对象

场地设施，建筑防雷设计/验收文档。

5.2.4.2.3.3 检测实施

a） 应访谈物理安全负责人，询问为防止雷击事件导致重要设备被破坏采取了哪些防护措施，场地建筑是否设置了避雷装置，是否通过验收或国家有关部门的技术检测。

b） 应访谈维护人员，询问建筑避雷装置是否有人定期进行检查和维护。

c） 应检查场地是否设置了接地线排。

d） 应检查场地是否有建筑防雷设计/验收文档、场地接地设计/验收文档，查看是否有地线连接要求的描述，与实际情况是否一致。

5.2.4.2.4 防火

5.2.4.2.4.1 检测方式

访谈，检查

5.2.4.2.4.2 检测对象

场地设施、场地安全管理制度、场地防火设计/验收文档。

5.2.4.2.4.3 检测实施

a） 应访谈物理安全负责人，询问场地是否设置了灭火设备，是否制订了有关场地消防的管理制度和消防预案，是否进行了消防培训。

b） 应访谈物理安全负责人，询问对场地出现的消防安全隐患是否能够及时报告并得到排除，是否参加过场地灭火设备的使用培训，是否能够正确使用灭火设备。

c） 应检查是否有场地消防方面的管理制度文档；检查是否有场地防火设计/验收文档，检查是否有场地及相关房间的建筑材料、区域隔离防火措施的验收文档或消防检查验收文档。

5.2.4.2.5 防水和防潮

5.2.4.2.5.1 检测方式

访谈，检查。

5.2.4.2.5.2 检测对象

场地设施、建筑防水和防潮设计/验收文档、场地湿度记录、除湿装置运行记录。

5.2.4.2.5.3 检测实施

a） 应访谈物理安全负责人，询问场地建设是否有防水防潮措施，在湿度较高地区或季节是否有人负责场地防水防潮事宜，配备除湿装置。

b） 应访谈场地维护人员，询问场地是否出现过漏水和返潮事件；如果出现场地水蒸气结露和地下积水的转移与渗透现象是否采取防范措施。

c） 应检查场地是否有建筑防水和防潮设计/验收文档，是否与场地防水防潮的实际情况一致。

d） 应检查场地是否不存在屋顶和墙壁等出现过漏水、渗透和返潮现象，场地及其环境是否存在明显的漏水和返潮的威胁，如果出现漏水、渗透和返潮现象是否能够及时修复解决。

e） 如果在湿度较高地区或季节，应检查场地是否有湿度记录，是否有除湿装置并能够正常运行，是否有防止出现场地地下积水的转移与渗透的措施，是否有防水防潮处理记录和除湿装置运行记录，与场地湿度记录情况是否一致。

5.2.4.2.6 温湿度控制

5.2.4.2.6.1 检测方式

访谈，检查。

5.2.4.2.6.2 检测对象

场地设施、温湿度控制设计/验收文档、温湿度记录、运行记录和维护记录。

5.2.4.2.6.3 检测实施

a） 应访谈物理安全负责人，询问场地是否配备了恒温恒湿系统，保证温湿度能够满足计算机设备运行的要求，是否在场地管理制度中规定了温湿度控制的要求，是否有人负责此项工作。

b） 应访谈维护人员，询问是否定期检查和维护场地的温湿度自动调节设施，询问是否出现过温湿度影响系统运行的事件。

c） 应检查场地是否有温湿度控制设计/验收文档，是否能够满足系统运行需要，是否与当前实际情况相符合。

d） 应检查恒温恒湿系统是否能够正常运行，查看是否有温湿度记录、运行记录和维护记录，查看机房温、湿度是否满足 GF014-95的要求。

5.2.4.2.7 防尘

5.2.4.2.7.1 检测方式

访谈，检查。

5.2.4.2.7.2 检测对象

机房设施，防尘设计/验收文档，运行记录和维护记录。

5.2.4.2.7.3 检测实施

a） 应访谈物理安全负责人，询问机房采取了哪些防尘措施。

b） 应检查出入场地是否使用鞋套，是否有专人定期对场地进行除尘工作。

c） 应检查是否有防尘记录、运行记录和维护记录。

5.2.4.2.8 电力供应

5.2.4.2.8.1 检测方式

访谈，检查。

5.2.4.2.8.2 检测对象

场地设施、电力供应安全设计/验收文档、检查和维护记录。

5.2.4.2.8.3 检测实施

a） 应访谈物理安全负责人，询问场地供电线路是否与其他供电分开；询问场地供电线路上是否设置了稳压器和过电压防护设备；是否设置了短期备用电源设备（如UPS），供电时间是否满足系统最低电力供应需求。

b） 应访谈场地维护人员，询问是对在场地供电线路上的稳压器、过电压防护设备、短期备用电源设备等进行定期检查和维护；是否能够控制电源稳压范围满足机房系统运行正常。

c） 应检查场地是否有电力供应安全设计/验收文档，查看文档中是否标明场地供电与其他供电分开，是否配备稳压器、过电压防护设备、备用电源设备与场地电力供应实际情况是否一致。

d） 应检查供电线路，查看系统供电是否与其他供电分开。

e） 应查看场地供电线路上的稳压器、过电压防护设备和短期备用电源设备是否正常运行，查看供电电压是否正常。

f） 应检查是否有稳压器、过电压防护设备以及短期备用电源设备等电源设备的检查和维护记录，以及上述供电的运行记录，是否能够符合系统正常运行的要求。

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级检测要求

5.3.1 业务安全

应满足6.2.1的要求。

5.3.2 网络安全

5.3.2.1 通用网络安全

5.3.2.1.1 网络拓扑安全

5.3.2.1.1.1 检测方式

访谈，查看。

5.3.2.1.1.2 检测对象

网络拓扑结构、网络拓扑图、网络设计/验收文档、设备运行日志、网络设备。

5.3.2.1.1.3 检测实施

除满足 6.2.2.1.1 要求外，还需满足下列要求。

a） 应访谈网络管理人员，查看网络拓扑图、网络设计/验收文档，查看对重要设备是否实行双归属配置、1+1 互为主备或 *N*+1 冗余备份等方案。

b） 应访谈网络管理人员，查看网络拓扑图，核心网络重要的节点设备之间是否采用负荷分担方式选择路由，是否设置迂回路由或备用路由。

5.3.2.1.2 用户数据存储

5.3.2.1.2.1 检测方式

访谈，查看。

5.3.2.1.2.2 检测对象

网络设计/验收文档、设备运行日志、网络设备。

5.3.2.1.2.3 检测实施

a） 应访谈网络管理人员，查看网络设计/验收文档和设备运行日志，查看重要设备中用户数据和参数存储的安全性，查看在线接入是否依操作者的等级不同控制接入。

b） 应访谈网络管理人员，查看网络设计/验收文档和设备运行日志，查看重要设备存储的用户数据和参数应保证有可靠的备份功能。

5.3.2.1.3 计费信息安全

5.3.2.1.3.1 检测方式

访谈，查看。

5.3.2.1.3.2 检测对象

网络设计/验收文档、设备运行日志、网络设备。

5.3.2.1.3.3 检测实施

应访谈网络管理人员，查看网络设计/验收文档和设备运行日志，查看是否保证计费信息的安全，是否提供可靠的话单备份、转储手段，以进行话单数据的可靠备份。

5.3.2.2 GSM 网络安全

应满足 6.2.2.2 的要求。

5.3.2.3 GPRS 网络安全

5.3.2.3.1 检测方式

访谈，查看。

5.3.2.3.2 检测对象

网络设计/验收文档、设备运行日志、入网测试报告、网络设备。

5.3.2.3.3 检测实施

除了满足6.2.2.3要求外，还需满足下列要求：

a） 应访谈网络管理人员，查看网络设计/验收文档，在 GGSN 与外部 IP 网络之间应设置防火墙进行隔离是否与设计相符。

b） 应访谈网络管理人员，查看网络设计/验收文档，不同 GPRS 网之间互连时，在 BG 处设置必要的安全机制是否与设计相符。

5.3.2.4 WCDMA/TD-SCDMA 网络安全

5.3.2.4.1 检测方式

访谈，查看。

5.3.2.4.2 检测对象

网络设计/验收文档、设备运行日志、入网测试报告、网络设备。

5.3.2.4.3 检测实施

除满足 6.2.2.4 要求外，还需满足下列要求。

a） 应访谈网络管理人员，查看网络设计/验收文档，在 WCDMA/TD-SCDMA 分组域与外部 IP 网络之间设置防火墙进行隔离是否与设计相符。

b） 应访谈网络管理人员，查看网络设计/验收文档，不同 WCDMA/TD-SCDMA 分组域之间互连时，在 BG 处设置必要的安全机制是否与设计相符。

5.3.2.5 cdma 2000 1x 网络安全

5.3.2.5.1 检测方式

访谈，查看。

5.3.2.5.2 检测对象

网络设计/验收文档、设备运行日志、入网测试报告、网络设备。

5.3.2.5.3 检测实施

除满足6.2.2.5要求外，还需：

应访谈网络管理人员，查看网络设计/验收文档，在cdma 2000 1x分组域与外部IP网络之间设置防火墙进行隔离是否与设计相符。

5.3.2.6 HRPD 网络安全

5.3.2.6.1 检测方式

访谈，查看。

5.3.2.6.2 检测对象

网络设计/验收文档、设备运行日志、入网测试报告、网络设备。

5.3.2.6.3 检测实施

除满足6.2.2.6要求外，还需访谈网络管理人员，查看网络设计/验收文档，查看在HRPD分组域与外部IP网络之间设置防火墙进行隔离是否与设计相符。

5.3.3 设备安全

应满足6.2.3的要求。

5.3.4 物理环境安全

5.3.4.1 机房、办公场地物理环境安全

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。

5.3.4.2 室外无线接入设备场地物理环境

5.3.4.2.1 物理位置的选择

5.3.4.2.1.1 检测方式

访谈，检查。

5.3.4.2.1.2 检测对象

机房，办公场地，机房场地设计/验收文档

5.3.4.2.1.3 检测实施

除满足6.2.4.2.1的要求外，还需满足下列要求。

a） 应访谈物理安全负责人，询问现有场地的环境条件不在强电场、强磁场、强震动源、强噪声源、重度环境污染、易发生火灾、水灾、易遭受雷击的地区等。

b） 应检查设计/验收文档，查看场地接地方式、接地线布放、接地电阻是否满足相关要求，并现场检查场地的接地方式、接地线布放、接地电阻是否与设计文档相符。

5.3.4.2.2 防盗窃和防破坏

5.3.4.2.2.1 检测方式

访谈，检查。

5.3.4.2.2.2 检测对象

机房设施、设备管理制度文档、通信线路布线文档、防盗报警系统和监控报警系统的安装测试/验收报告。

5.3.4.2.2.3 检测实施

应满足6.2.4.2.2的要求。

a） 应访谈维护人员是否对场地安装的防盗报警系统和监控报警系统进行定期维护检查。

b） 应检查场地防盗报警设施是否正常运行，并查看运行和报警记录；检查、传感等监控报警系统是否正常运行，并查看运行记录、监控记录和报警记录。

5.3.4.2.3 防雷击

应满足6.2.4.2.3的要求。

5.3.4.2.4 防火

应满足6.2.4.2.4的要求。

5.3.4.2.5 防水和防潮

应满足6.2.4.2.5的要求。

5.3.4.2.6 温湿度控制

应满足6.2.4.2.6的要求。

5.3.4.2.7 防尘

应满足6.2.4.2.7的要求。

5.3.4.2.8 电力供应

5.3.4.2.8.1 检测方式

访谈，检查。

5.3.4.2.8.2 检测对象

机房设施、电力供应安全设计/验收文档、检查和维护记录。

5.3.4.2.8.3 检测实施

除满足6.2.4.2.8的要求，还需满足下列要求：

a） 应访谈物理安全负责人，询问机房供电线路是否安装了冗余或并行的电力电缆线路（如双路供电方式）；如果没有安装冗余或并行的电力电缆线路，是否建立备用供电系统（如备用发电机），采用其他手段保证不间断供电。

b） 应访谈维护人员，询问冗余或并行的电力电缆线路（如双路供电方式）在双路供电切换时是否能够对机房正常供电；定期检查备用供电系统（如备用发电机），是否能够在规定时间内正常启动和正常供电。

c） 应检查备用供电系统（如备用发电机）定期检测记录。

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 级检测要求

5.4.1 业务安全

应满足6.3.1的要求。

5.4.2 网络安全

应满足6.3.2的要求。

5.4.3 设备安全

应满足6.3.3的要求。

5.4.4 物理环境安全

5.4.4.1 机房、办公场地物理环境安全

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。

5.4.4.2 室外无线接入设备物理场地环境

应满足6.3.4.2的要求。

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级的安全要求。

5.5 第 4 级检测要求

同第3.2级要求。

5.6 第 5 级检测要求

待补充。

6 移动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，询问进行移动通信网风险评估时选择的风险评估范围；检查风险评估报告，查看移动通信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） 应访谈移动通信网风险评估负责人、查看风险评估报告，检查移动通信网风险评估是否覆盖了技术安全和管理安全。

b） 应访谈移动通信网风险评估负责人、查看风险评估报告，检查移动通信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） 应访谈移动通信网风险评估负责人、查看风险评估报告，检查移动通信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，询问进行移动通信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，检查移动通信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，询问进行移动通信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，检查移动通信网风险评估报告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，询问进行移动通信网风险评估时评估了哪些资产；查看风险评估报告，检查移动通信网风险评估时的资产是否包含了频率和码号资源、电信智能卡、网络设备（GSM网络设备包括BTS、BSC、MSC、VLR、HLR、AUC等，GPRS网络设备包括BTS、BSC、PCU、SGSN、GGSN、VLR、HLR、AUC、BG、CG等，基于R99的WCDMA/TD-SCDMA网络设备包括Node B、RNC、MSC、SGSN、GGSN、VLR、HLR、AUC、BG、CG等，基于R4的WCDMA/TD-SCDMA网络设备包括Node B、RNC、MGW、MSC Server、SGSN、GGSN、VLR、HLR、AUC、BG、CG等，cdma 2000 1x网络设备包括BTS、BSC、PCF 、MSC、VLR、HLR、AC、PDSN、AAA、HA、FA等，HRPD网络设备包括BTS、

BSC、PCF、AN AAA、PDSN、AAA、HA、FA等，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，设备中的重要数据，网络提供的各类业务，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，询问计算移动通信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，检查移动通信网风险评估中，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，询问识别了移动通信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，检查移动通信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，询问识别了移动通信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，检查移动通信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，询问对移动通信网存在哪些威胁；查看风险评估报告，检查移动通信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，检查移动通信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，检查移动通信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，检查移动通信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，检查移动通信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，询问移动通信网风险评估时资产的赋值遵循的原则；查看风险评估报告，检查移动通信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，询问移动通信网风险评估时脆弱性的赋值遵循的原则；查看风险评估报告，检查移动通信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，询问移动通信网风险评估时威胁的赋值遵循的原则；查看风险评估报告，检查移动通信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，询问移动通信网风险评估中采用什么样的方法计算资产价值；查看风险评估报告，检查移动通信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，询问移动通信网风险评估中采用什么样的方法计算风险值；查看风险评估报告，检查移动通信网风险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。

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所确认的结果，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做了标识。

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 移动通信网灾难备份及恢复检测要求

7.1 第1级检测要求

不作要求。

7.2 第2级检测要求

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，查看。

7.2.1.2 检测对象

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，询问并现场查看移动通信网目前有哪些冗余系统、冗余设备、冗余链路的设计和部署，是否与设计/验收文档相符合，查看运行日志、故障记录，查看出现灾难以后采用冗余系统、冗余设备和冗余链路来进行灾难恢复的情况。

b） 应访谈安全管理人员，询问并现场查看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，查看运行日志、故障记录，查看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，安全措施是否与设计/验收文档相符合。

c） 应访谈安全管理人员，查看演练文档以及移动通信网的网络灾难演练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，查看。

7.2.2.2 检测对象

冗余路由、设计/验收文档、演练记录、历史记录。

7.2.2.3 检测实施

应访谈安全管理人员，查看设计/验收文档和历史记录，询问移动通信网络的物理链路是否采用了冗余路由，查看其冗余路由是否与设计一致。

7.2.3 备份数据

7.2.3.1 检测方式

访谈，查看。

7.2.3.2 检测对象

数据备份服务器、设计/验收文档、演练历史记录。

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服务器，查看移动通信网中关键数据（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服务器、演练记录，查看移动通信网关键数据的备份范围和时间间隔、采取的备份方式、数据恢复能力的情况，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，查看。

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，查看是否有负责灾难备份及恢复的机房管理人员。

7.2.5 运行维护管理能力

7.2.5.1 检测方式

访谈，查看。

7.2.5.2 检测对象

机房运行管理制度、介质存取以及验证和转储管理制度、设备和网络运行管理制度，数据容灾备份管理制度、联络和协作的记录。

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，查看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，查看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，查看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，查看。

7.2.6.2 检测对象

灾难恢复预案、设计/验收文档。

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，查看移动通信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级检测要求

除满足8.1中要求外，还需满足下列要求。

7.3.1 冗余系统、冗余设备及冗余链路

应满足8.2.1的要求。

7.3.2 冗余路由

7.3.2.1 检测方式

访谈，查看。

7.3.2.2 检测对象

冗余路由、设计/验收文档、演练记录、历史记录、传送链路。

7.3.2.3 检测实施

除需满足8.2.1的要求外，还需：

应访谈安全管理人员，检查设计/验收文档和历史记录，查看移动通信网是否采用了流量负荷分担方式。

7.3.3 备份数据

7.3.3.1 检测方式

访谈，查看。

7.3.3.2 检测对象

数据备份服务器、设计/验收文档、演练历史记录

7.3.3.3 检测实施

除需满足8.2.2的要求外，还需：

应访谈安全管理人员，询问并查看数据备份服务器，查看移动通信网中关键数据（如计费数据、网络配置数据）在不同的地理位置进行备份的情况。

7.3.4 人员和技术支持能力

7.3.4.1 检测方式

访谈，查看。

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

除需满足8.2.3的要求外，还需满足下列要求。

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，查看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，查看。

7.3.5.2 检测对象

设备和网络运行管理制度、数据异地实时容灾备份管理制度、联络和协作的记录。

7.3.5.3 检测实施

除需满足8.2.4的要求外，还需满足下列要求。

a） 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，查看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。

b） 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，查看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。

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，查看移动通信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，查看。

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

除需满足8.2.5的要求外，还需满足下列要求。

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，查看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，查看相关人员对灾难恢复预案的了解情况，查看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，查看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，查看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级检测要求

7.4.1 冗余系统、冗余设备及冗余链路

应满足8.3.1的要求。

7.4.2 冗余路由

应满足8.3.2的要求。

7.4.3 备份数据

应满足8.3.3的要求。

7.4.4 人员和技术支持能力

应满足8.3.4的要求。

7.4.5 运行维护管理能力

应满足8.3.5的要求。

7.4.6 灾难恢复预案

7.4.6.1 检测方式

访谈，查看。

7.4.6.2 检测对象

灾难恢复预案、设计/验收文档、灾难恢复预案的管理制度。

7.4.6.3 检测实施

除需满足8.3.6的要求外，还需：

应访谈安全管理人员，询问并查看移动通信网管理制度，查看是否有灾难恢复预案的管理制度。

7.5 第4级检测要求

同第3.2级要求。

7.6 第5级检测要求

待补充。