YD

中华人民共和国通信行业标准

YD/T 1759-2008

非核心生产单元安全防护检测要求

Security Protection Testing Requirements
for the Support Unit of Core Production 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 1758-2008《非核心生产单元安全防护要求》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、中国移动通信集团公司、中国联合通信有限公司、中国铁通集团有限公司

本标准主要起草人：杨剑锋、刘险峰、赵　阳、陈　欣、顾旻霞、王君珂、刘立松

非核心生产单元安全防护检测要求

1 范围

本标准规定了公众电信网和互联网相关非核心生产单元在安全等级保护、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和互联网相关非核心生产单元。

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/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 定义和缩略语

3.1 定义

下列定义适用于本标准。

3.1.1

非核心生产单元安全等级 Security Classification of the Support Unit of Core Production Network

非核心生产单元安全重要程度的表征。重要程度可从非核心生产单元受到破坏后，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

非核心生产单元安全等级保护 Classified Security Protection of the Support Unit of Core Production Network

对非核心生产单元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

非核心生产单元安全风险 Security Risk of the Support Unit of Core Production Network

人为或自然的威胁可能利用非核心生产单元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

非核心生产单元安全风险评估 Security Risk Assessment of the Support Unit of Core Production Network

指运用科学的方法和手段，系统地分析非核心生产单元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。防范和化解非核心生产单元安全风险，或者将风险控制在可接受的水平，为最大限度地为保障非核心生产单元的安全提供科学依据。

3.1.6

非核心生产单元资产 Asset of the Support Unit of Core Production Network

非核心生产单元中具有价值的资源，是安全防护保护的对象。非核心生产单元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，如非核心生产单元的设备、线路、数据信息等。

3.1.7

非核心生产单元资产价值 Asset Value of the Support Unit of Core Production Network

非核心生产单元中资产的重要程度或敏感程度。非核心生产单元资产价值是非核心生产单元资产的属性，也是进行非核心生产单元资产识别的主要内容。

3.1.8

非核心生产单元威胁 Threat of the Support Unit of Core Production Network

可能导致对非核心生产单元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。常见的非核心生产单元威胁有攻击、故障、灾害等等。

3.1.9

非核心生产单元脆弱性 Vulnerability of the Support Unit of Core Production Network

脆弱性是非核心生产单元中存在的弱点、缺陷与不足，不直接对非核心生产单元资产造成危害，但可能被非核心生产单元威胁所利用从而危及非核心生产单元资产的安全。

3.1.10

非核心生产单元灾难 Disaster of the Support Unit of Core Production Network

由于各种原因，造成非核心生产单元故障或瘫痪，使非核心生产单元提供的服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

非核心生产单元灾难备份 Backup for Disaster Recovery of the Support Unit of Core Production Network

为了非核心生产单元灾难恢复而对相关的要素进行备份的过程。

3.1.12

非核心生产单元灾难恢复 Disaster Recovery of the Support Unit of Core Production Network

为了将非核心生产单元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，并将其提供的服务功能、服务水平等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

访谈 Interview

检测人员通过与非核心生产单元有关人员（个人/群体）进行交流、讨论等活动，检查非核心生产单元安全等级保护、非核心生产单元风险评估和非核心生产单元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。

3.1.14

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，检查非核心生产单元安全等级保护、非核心生产单元风险评估和非核心生产单元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

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，检查非核心生产单元安全等级保护、非核心生产单元风险评估和非核心生产单元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。

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	Hyper Text 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
SMTP	Simple Mail Transfer Protocol	简单邮件传送协议

4 非核心生产单元安全防护检测概述

4.1 安全防护检测范围

本标准的检测范围包括公众电信网和互联网相关企业的企业办公系统、客服呼叫系统、企业门户网站等非核心生产单元。

4.2 安全防护检测对象

非核心生产单元安全防护检测对象为企业办公系统、客服呼叫中心、企业门户网站等系统。

非核心生产单元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

根据非核心生产单元安全防护检测的需要，将非核心生产单元安全防护检测分为非核心生产单元安全等级保护检测、非核心生产单元安全风险评估检测和非核心生产单元灾难备份及恢复检测三个部分。

非核心生产单元安全防护检测要求包括以下内容：

——非核心生产单元安全等级保护检测

主要包括应用安全检测、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。

——非核心生产单元安全风险评估检测

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；

——非核心生产单元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

非核心生产单元安全防护检测包括对非核心生产单元的安全等级保护、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3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见表2。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。例如，表3给出了安全等级保护子类所占的比重。

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 总评分和评定等级的关系

总评分 x	评定等级
$4.5 \leqslant x \leqslant 5$	很好
$3.5 \leqslant x < 4.5$	较好
$2.5 \leqslant x < 3.5$	一般
$1.5 \leqslant x < 2.5$	较差
$1 \leqslant x < 1.5$	很差

表3 安全等级保护子类所占的比重

比重（%）	安全等级保护子类
30	应用安全
20	网络安全
10	设备安全
10	物理环境安全
30	管理安全

5 非核心生产单元安全等级保护检测要求

5.1 第1级要求

本标准对安全等级为第1级的非核心生产单元暂不作要求。

5.2 第2级要求

5.2.1 应用安全

5.2.1.1 身份鉴别

5.2.1.1.1 检测方式

访谈、检查。

5.2.1.1.2 检测对象

系统设计/验收文档，相关服务和应用管理流程文档，系统管理文档，设备管理配置记录，故障告警记录，网络和业务运营商提供的其他文档、系统及相关设备等。

5.2.1.1.3 检测实施

a）应访谈系统管理员，并查看系统设计/验收文档、相关服务和应用管理流程、网络和业务运营商提供的其他文档，检查和验证是否提供专用的登录控制模块对登录用户进行身份标识和鉴别；

b）应访谈系统管理员，并查看系统设计/验收文档、相关服务和应用管理流程、网络和业务运营商提供的其他文档，检查和验证是否提供用户身份标识惟一和鉴别信息复杂度检查功能，验证是否能保证应用系统中不存在重复用户身份标识，身份鉴别信息是否不易被冒用；

c）应访谈系统管理员，并查看系统设计/验收文档、相关服务和应用管理流程、网络和业务运营商提供的其他文档，检查和验证是否提供登录失败处理功能，是否采取结束会话、限制非法登录次数和自动退出等措施；

d）应访谈系统管理员，并查看系统设计/验收文档、相关服务和应用管理流程、网络和业务运营商提供的其他文档，检查和验证是否启用身份鉴别、用户身份标识惟一性检查、用户身份鉴别信息复杂度检查以及登录失败处理功能，并根据安全策略配置相关参数。

5.2.1.2 访问控制

5.2.1.2.1 检测方式

访谈、检查。

5.2.1.2.2 检测对象

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，故障告警记录，网络和业务运营商提供的其他文档、系统及相关设备等。

5.2.1.2.3 检测实施

a）应访谈系统管理员，并查看系统设计/验收文档、相关服务管理流程、系统安全策略、网络和业务运营商提供的其他文档，检查和验证是否提供访问控制功能，依据安全策略控制用户对文件、数据库表等客体的访问；

b）应访谈系统管理员，并查看系统设计/验收文档、相关服务和应用管理流程、系统安全策略、网络和业务运营商提供的其他文档，检查和验证访问控制的覆盖范围是否包括与资源访问相关的主体、客体及它们之间的操作；

c）应访谈系统管理员，并查看系统设计/验收文档、相关服务和应用管理流程、系统安全策略、网络和业务运营商提供的其他文档，检查和验证由授权主体配置访问控制策略，验证是否严格限制默认账户的访问权限；

d）应访谈系统管理员，并查看系统设计/验收文档、相关服务和应用管理流程、系统安全策略、网络和业务运营商提供的其他文档，检查和验证是否授予不同账户为完成各自承担任务所需的最小权限，验证不同账户间是否存在相互制约的关系。

5.2.1.3 安全审计

5.2.1.3.1 检测方式

访谈、检查。

5.2.1.3.2 检测对象

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，故障告警记录，审计记录及报告，网络和业务运营商提供的其他文档、系统及相关设备等。

5.2.1.3.3 检测实施

a）应访谈系统管理员，并查看系统设计/验收文档、相关服务管理流程、系统安全策略、审计记录及报告、网络和业务运营商提供的其他文档，检查和验证是否提供覆盖到每个用户的安全审计功能，是否对应用系统重要安全事件进行审计；

b）应访谈系统管理员，并查看系统设计/验收文档、相关服务管理流程、系统安全策略、审计记录及报告、网络和业务运营商提供的其他文档，检查和验证是否能保证无法删除、修改或覆盖审计记录；

c）应访谈系统管理员，并查看系统设计/验收文档、相关服务管理流程、系统安全策略、审计记录及报告、网络和业务运营商提供的其他文档，检查和验证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。

5.2.1.4 通信数据安全

5.2.1.4.1 检测方式

访谈、检查。

5.2.1.4.2 检测对象

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，网络和业务运营商提供的其他文档、系统及相关设备等。

5.2.1.4.3 检测实施

a）应访谈系统管理员，并查看系统设计/验收文档、相关系统管理流程、系统安全策略、网络和业务运营商提供的其他文档，检查和验证是否采用校验码技术保证通信过程中数据的完整性；

b）应访谈系统管理员，并查看系统设计/验收文档、相关系统管理流程、系统安全策略、网络和业务运营商提供的其他文档，检查和验证是否能够检测到鉴别信息和重要业务数据在传输过程中完整性受到破坏的情况。

c）应访谈系统管理员，并查看系统设计/验收文档、相关系统管理流程、系统安全策略、网络和业务运营商提供的其他文档，检查和验证是否采用加密或其他保护措施实现鉴别信息的存储保密性；

d）应访谈系统管理员，并查看系统设计/验收文档、相关系统管理流程、系统安全策略、网络和业务运营商提供的其他文档，检查和验证在通信双方建立连接之前，应用系统是否利用密码技术进行会话初始化验证；

e）应访谈系统管理员，并查看系统设计/验收文档、相关系统管理流程、系统安全策略、网络和业务运营商提供的其他文档，检查和验证对通信过程中的敏感信息是否进行加密，验证加密的强度。

5.2.1.5 资源控制

5.2.1.5.1 检测方式

访谈、检查。

5.2.1.5.2 检测对象

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，网络和业务运营商提供的其他文档、系统及相关设备等。

5.2.1.5.3 检测实施

a）应访谈系统管理员，并查看系统设计/验收文档、相关服务管理流程、系统安全策略、网络和业务运营商提供的其他文档，检查和验证当应用系统的通信双方中的一方在一段时间内未作任何响应时，另一方是否能够自动结束会话。

b）应访谈系统管理员，并查看系统设计/验收文档、相关服务管理流程、系统安全策略、网络和业务运营商提供的其他文档，检查和验证是否能够对应用系统的最大并发会话连接数进行限制。

c）应访谈系统管理员，并查看系统设计/验收文档、相关服务管理流程、系统安全策略、网络和业务运营商提供的其他文档，检查和验证是否能够对单个账户的多重并发会话进行限制。

5.2.2 网络安全

5.2.2.1 结构安全

5.2.2.1.1 检测方式

访谈、检查。

5.2.2.1.2 检测对象

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，网络和业务运营商提供的其他文档、系统及相关设备等。

5.2.2.1.3 检测实施

a）应访谈系统管理员，并查看系统设计/验收文档、系统拓扑图、网络和业务运营商提供的其他文档，检查和验证是否绘制与当前运行情况相符的系统拓扑结构图；

b）应访谈系统管理员，并查看系统设计/验收文档、相关服务管理流程、系统安全策略、网络和业务运营商提供的其他文档，检查和验证是否根据服务的特点，系统的带宽和处理能力是否满足高峰期流量需求，检查系统设计是否合理；

c）应访谈系统管理员，并查看系统设计/验收文档、相关服务管理流程、系统安全策略、网络和业务运营商提供的其他文档，检查和验证是否根据各部门的工作职能、重要性和所涉及信息的重要程度等因素划分子网和网段，网段规划是否按照统一的管理和控制原则进行。

5.2.2.2 访问控制

5.2.2.2.1 检测方式

访谈、检查。

5.2.2.2.2 检测对象

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，故障告警记录，网络和业务运营商提供的其他文档、系统及相关设备等。

5.2.2.2.3 检测实施

a）应访谈系统管理员，并查看系统设计/验收文档、相关服务管理流程、系统安全策略、网络和业务运营商提供的其他文档，检查和验证在网络边界是否部署访问控制设备，启用访问控制功能。

b）应访谈系统管理员，并查看系统设计/验收文档、相关服务管理流程、系统安全策略、网络和业务运营商提供的其他文档，检查和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，验证控制粒度是否达到网段级别。

c）应访谈系统管理员，并查看系统设计/验收文档、相关服务管理流程、系统安全策略、网络和业务运营商提供的其他文档，检查和验证按照用户和系统之间的允许访问规则，是否能进行允许或拒绝用户对受控系统进行资源访问，控制粒度是否达到单个用户。

d）应访谈系统管理员，并查看系统设计/验收文档、相关服务管理流程、系统安全策略、网络和业务运营商提供的其他文档，检查和验证是否限制具有拨号访问权限的用户数量。

5.2.2.3 安全审计

5.2.2.3.1 检测方式

访谈、检查。

5.2.2.3.2 检测对象

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，安全审计记录，设备管理配置记录，故障告警记录，网络和业务运营商提供的其他文档、系统及相关设备等。

5.2.2.3.3 检测实施

a）应访谈系统管理员，并查看系统设计/验收文档、相关服务管理流程、系统安全策略、网络和业务运营商提供的其他文档，检查和验证对网络系统中的网络设备运行状况、网络流量、用户行为等是否进行日志记录；

b）应访谈系统管理员，并查看系统设计/验收文档、相关服务管理流程、系统安全策略、网络和业务运营商提供的其他文档，检查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。

5.2.2.4 入侵防范

5.2.2.4.1 检测方式

访谈、检查。

5.2.2.4.2 检测对象

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，故障告警记录，网络和业务运营商提供的其他文档、系统及相关设备等。

5.2.2.4.3 检测实施

a）应访谈系统管理员，并查看系统设计/验收文档、相关服务管理流程、系统安全策略、网络和业务运营商提供的其他文档，检查和验证是否在网络边界处对发生的端口扫描、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攻击等攻击和入侵事件进行检测，验证是否具有有效的抵御攻击和入侵防范能力；

b）应访谈系统管理员，并查看系统设计/验收文档、相关服务管理流程、系统安全策略、网络和业务运营商提供的其他文档，检查和验证是否能够对内部网络中出现的内部用户未通过授权，私自联到外部网络的行为进行检查。

5.2.3 设备安全

5.2.3.1 安全检测

5.2.3.1.1 检测方法

访谈、检查。

5.2.3.1.2 检测对象

设备安全检测报告，网络设备检测报告、入网证，网络和业务运营商提供的其他文档、相关设备。

5.2.3.1.3 检测实施

a）应访谈相关技术支持人员和管理人员，查看网络设备入网检测报告、设备入网证、安全检测报告、网络和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、安全检测，验证安全检测是否符合网络和业务运营商相关设备的要求；

b）应访谈相关技术支持人员和管理人员，查看通用计算机、服务器等设备安全检测报告、网络和业务运营商提供的其他文档，检查系统相关通用服务器、计算机等设备是否有进行有效的安全检测，检查设备的安全检测是否符合网络和业务运营商相关通用设备的要求。

5.2.3.2 身份鉴别

5.2.3.2.1 检测方法

访谈、检查。

5.2.3.2.2 检测对象

设备安全检测报告，设备配置、管理记录文档，系统安全策略，故障告警记录，网络和业务运营商提供的其他文档、系统及相关设备等。

5.2.3.2.3 检测实施

a）应访谈相关技术支持人员和管理人员，查看设备相关配置及管理记录、系统安全策略、安全检测报告、网络和业务运营商提供的其他文档，检查和验证是否对登录操作系统和数据库系统的用户进行身份标识和鉴别；

b）应访谈相关技术支持人员和管理人员，查看设备相关配置及管理记录、系统安全策略、安全检测报告、网络和业务运营商提供的其他文档，检查和验证计算机、服务器等通用主机操作系统和数据库系统管理用户身份标识是否具有不易被冒用的特点，口令应有复杂度要求并定期更换；

c）应访谈相关技术支持人员和管理人员，查看设备相关配置及管理记录、系统安全策略、安全检测报告、网络和业务运营商提供的其他文档，检查和验证是否启用登录失败处理功能，可采取的安全措施是否包括结束会话、限制非法登录次数和自动退出等；

d）应访谈相关技术支持人员和管理人员，查看设备相关配置及管理记录、系统安全策略、安全检测报告、网络和业务运营商提供的其他文档，检查当对主机进行远程管理时，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；

e）应访谈相关技术支持人员和管理人员，查看设备相关配置及管理记录、系统安全策略、安全检测报告、网络和业务运营商提供的其他文档，检查和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，确保用户名具有惟一性。

5.2.3.3 访问控制

5.2.3.3.1 检测方法

访谈、检查。

5.2.3.3.2 检测对象

设备安全检测报告，设备配置、管理记录文档，系统安全策略，故障告警记录，网络和业务运营商提供的其他文档、系统及相关设备等。

5.2.3.3.3 检测实施

a）应访谈相关技术支持人员和管理人员，查看设备相关配置及管理记录、系统安全策略、安全检测报告、网络和业务运营商提供的其他文档，检查是否启用访问控制功能，验证是否能依据安全策略控制用户对资源的访问；

b）应访谈相关技术支持人员和管理人员，查看设备相关配置及管理记录、系统安全策略、安全检测报告、网络和业务运营商提供的其他文档，检查是否实现操作系统和数据库系统特权用户的权限分离；

c）应访谈相关技术支持人员和管理人员，查看设备相关配置及管理记录、系统安全策略、安全检测报告、网络和业务运营商提供的其他文档，检查和验证是否限制默认账户的访问权限，重命名系统默认账户，修改这些账户的默认口令；

d）应访谈相关技术支持人员和管理人员，查看设备相关配置及管理记录、系统安全策略、安全检测报告、网络和业务运营商提供的其他文档，检查是否及时删除多余的、过期的账户，避免共享账户的存在。

5.2.3.4 安全审计

5.2.3.4.1 检测方法

访谈、检查。

5.2.3.4.2 检测对象

设备安全检测报告，设备配置、管理记录文档，系统安全策略，设备日志，审计记录、报告，故障告警记录，网络和业务运营商提供的其他文档、系统及相关设备等。

5.2.3.4.3 检测实施

a）应访谈相关技术支持人员和管理人员，查看设备相关配置及管理记录、系统安全策略、设备日志、审计报告、安全检测报告、网络和业务运营商提供的其他文档，检查审计范围是否覆盖到服务器上的每个操作系统用户和数据库用户；

b）应访谈相关技术支持人员和管理人员，查看设备相关配置及管理记录、系统安全策略、设备日志、审计报告、安全检测报告、网络和业务运营商提供的其他文档，检查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）应访谈相关技术支持人员和管理人员，查看设备相关配置及管理记录、系统安全策略、设备日志、审计记录、安全检测报告、网络和业务运营商提供的其他文档，检查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）应访谈相关技术支持人员和管理人员，查看设备相关配置及管理记录、系统安全策略、设备日志、安全检测报告、网络和业务运营商提供的其他文档，检查和验证是否能保护审计记录，避免受到未预期的删除、修改或覆盖等。

5.2.3.5 恶意代码防范

5.2.3.5.1 检测方法

访谈、检查。

5.2.3.5.2 检测对象

设备安全检测报告，设备配置、管理记录文档，系统安全策略，故障告警记录，网络和业务运营商提供的其他文档、系统及相关设备等。

5.2.3.5.3 检测实施

a）应访谈相关技术支持人员和管理人员，查看设备相关配置及管理记录、系统安全策略、安全检测报告、网络和业务运营商提供的其他文档，检查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，验证是否能通过安全的方式（如设置升级服务器等）保持系统补丁及时得到更新；

b）应访谈相关技术支持人员和管理人员，查看设备相关配置及管理记录、系统安全策略、安全检测报告、网络和业务运营商提供的其他文档，检查计算机、服务器等主机是否安装防恶意代码软件，是否能及时更新防恶意代码软件版本和恶意代码库；

c）应访谈相关技术支持人员和管理人员，查看设备相关配置及管理记录、系统安全策略、安全检测报告、网络和业务运营商提供的其他文档，检查计算机、服务器等主机是否支持防恶意代码软件的统一管理。

5.2.3.6 资源控制

5.2.3.6.1 检测方法

访谈、检查。

5.2.3.6.2 检测对象

设备安全检测报告，设备配置、管理记录文档，系统安全策略，故障告警记录，网络和业务运营商提供的其他文档、系统及相关设备等。

5.2.3.6.3 检测实施

a）应访谈相关技术支持人员和管理人员，查看设备相关配置及管理记录、系统安全策略、安全检测报告、网络和业务运营商提供的其他文档，检查是否能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）应访谈相关技术支持人员和管理人员，查看设备相关配置及管理记录、系统安全策略、安全检测报告、网络和业务运营商提供的其他文档，检查和验证是否根据安全策略设置登录终端的操作超时锁定；

c）应访谈相关技术支持人员和管理人员，查看设备相关配置及管理记录、系统安全策略、安全检测报告、网络和业务运营商提供的其他文档，检查和验证是否限制单个用户对系统资源的最大或最小使用限度。

5.2.4 物理环境安全

应按照YD/T 1755-2008《电信网和互联网物理环境安全等级保护检测要求》中第2级的相关要求进行检测。

5.2.5 管理安全

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

5.3 第3.1级要求

5.3.1 应用安全

5.3.1.1 身份鉴别

5.3.1.1.1 检测方式

访谈、检查。

5.3.1.1.2 检测对象

系统设计/验收文档，相关服务和应用管理流程文档，系统管理文档，设备管理配置记录，故障告警记录，网络和业务运营商提供的其他文档、系统及相关设备等。

5.3.1.1.3 检测实施

除按照第2级的要求进行检测之外，还应按照本节内容进行检测：

应访谈系统管理员，并查看系统设计/验收文档、相关服务和应用管理流程、网络和业务运营商提供的其他文档，检查和验证是否能根据需要对同一用户采用两种或两种以上组合的鉴别技术实现用户身份鉴别。

5.3.1.2 访问控制

5.3.1.2.1 检测方式

访谈、检查。

5.3.1.2.2 检测对象

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，故障告警记录，网络和业务运营商提供的其他文档、系统及相关设备等。

5.3.1.2.3 检测实施

除按照第2级的要求进行检测之外，还应按照本节内容进行检测：

a）应访谈系统管理员，并查看系统设计/验收文档、相关服务管理流程、系统安全策略、网络和业务运营商提供的其他文档，检查和验证对重要信息资源是否有设置敏感标记的功能；

b）应访谈系统管理员，并查看系统设计/验收文档、相关服务管理流程、系统安全策略、网络和业务运营商提供的其他文档，检查和验证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。

5.3.1.3 安全审计

5.3.1.3.1 检测方式

访谈、检查。

5.3.1.3.2 检测对象

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，故障告警记录，审计记录及报告，网络和业务运营商提供的其他文档、系统及相关设备等。

5.3.1.3.3 检测实施

除按照第2级的要求进行检测之外，还应按照本节内容进行检测：

a）应访谈系统管理员，并查看系统设计/验收文档、相关服务管理流程、系统安全策略、审计记录及报告、网络和业务运营商提供的其他文档，检查和验证是否能保证无法单独中断审计进程；

b）应访谈系统管理员，并查看系统设计/验收文档、相关服务管理流程、系统安全策略、审计记录及报告、网络和业务运营商提供的其他文档，检查和验证是否能提供对审计记录数据进行统计、查询、分析及生成审计报表的功能。

5.3.1.4 通信数据安全

5.3.1.4.1 检测方式

访谈、检查。

5.3.1.4.2 检测对象

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，网络和业务运营商提供的其他文档、系统及相关设备等。

5.3.1.4.3 检测实施

除按照第2级的要求进行检测之外，还应按照本节内容进行检测：

a）应访谈系统管理员，并查看系统设计/验收文档、相关系统管理流程、系统安全策略、网络和业务运营商提供的其他文档，检查和验证是否采用密码技术保证通信过程中数据的完整性；

b）应访谈系统管理员，并查看系统设计/验收文档、相关系统管理流程、系统安全策略、网络和业务运营商提供的其他文档，检查和验证是否对通信过程中的整个报文或会话过程进行加密；

c）应访谈系统管理员，并查看系统设计/验收文档、相关系统管理流程、系统安全策略、网络和业务运营商提供的其他文档，检查和验证是否能根据需要提供必要的通信数据防抵赖的功能。

5.3.1.5 资源控制

5.3.1.5.1 检测方式

访谈、检查。

5.3.1.5.2 检测对象

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，网络和业务运营商提供的其他文档、系统及相关设备等。

5.3.1.5.3 检测实施

除按照第2级的要求进行检测之外，还应按照本节内容进行检测：

a）应访谈系统管理员，并查看系统设计/验收文档、相关服务管理流程、系统安全策略、网络和业务运营商提供的其他文档，检查和验证是否能够对一个时间段内可能的并发会话连接数进行限制；

b）应访谈系统管理员，并查看系统设计/验收文档、相关服务管理流程、系统安全策略、网络和业务运营商提供的其他文档，检查和验证是否能够对一个访问账户或一个请求进程占用的资源分配最大限额和最小限额；

c）应访谈系统管理员，并查看系统设计/验收文档、相关服务管理流程、系统安全策略、网络和业务运营商提供的其他文档，检查和验证是否能够对系统服务水平降低到预先规定的最小值进行检测和报警；

d）应访谈系统管理员，并查看系统设计/验收文档、相关服务管理流程、系统安全策略、网络和业务运营商提供的其他文档，检查是否能提供服务优先级设定功能，检查和验证是否能根据安全策略设定访问账户或请求进程的优先级，是否能根据优先级分配系统资源。

5.3.2 网络安全

5.3.2.1 结构安全

5.3.2.1.1 检测方式

访谈、检查。

5.3.2.1.2 检测对象

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，网络和业务运营商提供的其他文档、系统及相关设备等。

5.3.2.1.3 检测实施

除按照第2级的要求进行检测之外，还应按照本节内容进行检测：

a）应访谈系统管理员，并查看系统设计/验收文档、系统拓扑图、网络和业务运营商提供的其他文档，检查和验证在业务终端与业务服务器之间是否能进行路由控制，建立安全的访问路径；

b）应访谈系统管理员，并查看系统设计/验收文档、系统拓扑图、网络和业务运营商提供的其他文档，检查是否未将重要网段部署在网络边界处，检查重要网段是否不直接连接外部信息系统，检查和验证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）应访谈系统管理员，并查看系统设计/验收文档、系统拓扑图、网络和业务运营商提供的其他文档，检查和验证是否按照对业务服务的重要次序来指定带宽分配优先级别，是否能保证在网络发生拥堵的时候优先保护重要主机。

5.3.2.2 访问控制

5.3.2.2.1 检测方式

访谈、检查。

5.3.2.2.2 检测对象

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，故障告警记录，网络和业务运营商提供的其他文档、系统及相关设备等。

5.3.2.2.3 检测实施

除按照第2级的要求进行检测之外，还应按照本节内容进行检测：

a）应访谈系统管理员，并查看系统设计/验收文档、相关服务管理流程、系统安全策略、网络和业务运营商提供的其他文档，检查和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，控制粒度是否为端口级；

b）应访谈系统管理员，并查看系统设计/验收文档、相关服务管理流程、系统安全策略、网络和业务运营商提供的其他文档，检查和验证对进出网络的信息内容是否进行过滤，实现对应用层HTTP、FTP、Telnet、SMTP、POP3等协议的控制；

c）应访谈系统管理员，并查看系统设计/验收文档、相关服务管理流程、系统安全策略、网络和业务运营商提供的其他文档，检查和验证当会话在一定时间内处于非活跃状态或会话结束后是否能终止网络连接；

d）应访谈系统管理员，并查看系统设计/验收文档、相关服务管理流程、系统安全策略、网络和业务运营商提供的其他文档，检查和验证是否限制网络最大流量数及网络连接数；

e）应访谈系统管理员，并查看系统设计/验收文档、相关服务管理流程、系统安全策略、网络和业务运营商提供的其他文档，检查和验证重要网段是否采取技术手段防止地址欺骗。

5.3.2.3 安全审计

5.3.2.3.1 检测方式

访谈、检查。

5.3.2.3.2 检测对象

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，审计记录，设备管理配置记录，故障告警记录，网络和业务运营商提供的其他文档、系统及相关设备等。

5.3.2.3.3 检测实施

除按照第2级的要求进行检测之外，还应按照本节内容进行检测：

a）应访谈系统管理员，并查看系统设计/验收文档、相关服务管理流程、系统安全策略、网络和业务运营商提供的其他文档，检查和验证是否能够根据记录数据进行分析，并生成审计报表

b）应访谈系统管理员，并查看系统设计/验收文档、相关服务管理流程、系统安全策略、网络和业务运营商提供的其他文档，检查和验证审计记录是否受到保护，是否能避免受到未预期的删除、修改或覆盖等。

5.3.2.4 入侵防范

5.3.2.4.1 检测方式

访谈、检查。

5.3.2.4.2 检测对象

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，故障告警记录，网络和业务运营商提供的其他文档、系统及相关设备等。

5.3.2.4.3 检测实施

除按照第2级的要求进行检测之外，还应按照本节内容进行检测：

a）应访谈系统管理员，并查看系统设计/验收文档、相关服务管理流程、系统安全策略、网络和业务运营商提供的其他文档，检查和验证在网络边界处是否能够对恶意代码进行检测和清除；检查和验证是否及时维护恶意代码库的升级和检测系统的更新；

b）应访谈系统管理员，并查看系统设计/验收文档、相关服务管理流程、系统安全策略、网络和业务运营商提供的其他文档，检查和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、攻击时间，在发生严重入侵事件时是否能提供报警；

c）应访谈系统管理员，并查看系统设计/验收文档、相关服务管理流程、系统安全策略、网络和业务运营商提供的其他文档，检查和验证是否能够对非授权设备私自联到内部网络、以及内部网络用户私自联到外部网络等行为进行检查，验证是否能准确定出位置，并对其进行有效阻断。

5.3.3 设备安全

5.3.3.1 安全检测

同第2级的相关检测要求。

5.3.3.2 身份鉴别

5.3.3.2.1 检测方法

访谈、检查。

5.3.3.2.2 检测对象

设备安全检测报告，设备配置、管理记录文档，系统安全策略，故障告警记录，网络和业务运营商提供的其他文档、系统及相关设备等。

5.3.3.2.3 检测实施

除按照第2级的要求进行检测之外，还应按照本节内容进行检测：

应访谈相关技术支持人员和管理人员，查看设备相关配置及管理记录、系统安全策略、安全检测报告、网络和业务运营商提供的其他文档，检查和验证是否采用两种或两种以上组合的鉴别技术对管理用户进行身份鉴别。

5.3.3.3 访问控制

5.3.3.3.1 检测方法

访谈、检查。

5.3.3.3.2 检测对象

设备安全检测报告，设备配置、管理记录文档，系统安全策略，故障告警记录，网络和业务运营商提供的其他文档、系统及相关设备等。

5.3.3.3.3 检测实施

除按照第2级的要求进行检测之外，还应按照本节内容进行检测：

a）应访谈相关技术支持人员和管理人员，查看设备相关配置及管理记录、系统安全策略、安全检测报告、网络和业务运营商提供的其他文档，检查和验证是否能根据管理用户的角色分配权限，实现管理用户的权限分离，检查和验证是否仅授予管理用户所需的最小权限；

b）应访谈相关技术支持人员和管理人员，查看设备相关配置及管理记录、系统安全策略、安全检测报告、网络和业务运营商提供的其他文档，检查和验证对重要信息资源是否设置敏感标记；

c）应访谈相关技术支持人员和管理人员，查看设备相关配置及管理记录、系统安全策略、安全检测报告、网络和业务运营商提供的其他文档，检查和验证是否能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。

5.3.3.4 安全审计

5.3.3.4.1 检测方法

访谈、检查。

5.3.3.4.2 检测对象

设备安全检测报告，设备配置、管理记录文档，系统安全策略，设备日志，审计记录，故障告警记录，网络和业务运营商提供的其他文档、系统及相关设备等。

5.3.3.4.3 检测实施

除按照第2级的要求进行检测之外，还应按照本节内容进行检测：

a）应访谈相关技术支持人员和管理人员，查看设备相关配置及管理记录、系统安全策略、设备日志、审计报告、安全检测报告、网络和业务运营商提供的其他文档，检查审计范围是否覆盖到服务器和重要

客户端上的每个操作系统用户和数据库用户；

b）应访谈相关技术支持人员和管理人员，查看设备相关配置及管理记录、系统安全策略、设备日志、审计报告、安全检测报告、网络和业务运营商提供的其他文档，检查是否能够根据日志记录数据进行分析，并生成审计报表；

c）应访谈相关技术支持人员和管理人员，查看设备相关配置及管理记录、系统安全策略、设备日志、审计报告、安全检测报告、网络和业务运营商提供的其他文档，检查是否能保护审计进程，避免受到未预期的中断。

5.3.3.5 恶意代码防范

5.3.3.5.1 检测方法

访谈、检查。

5.3.3.5.2 检测对象

设备安全检测报告，设备配置、管理记录文档，系统安全策略，故障告警记录，网络和业务运营商提供的其他文档、系统及相关设备等。

5.3.3.5.3 检测实施

除按照第2级的要求进行检测之外，还应按照本节内容进行检测：

a）应访谈相关技术支持人员和管理人员，查看设备相关配置及管理记录、系统安全策略、安全检测报告、网络和业务运营商提供的其他文档，检查和验证对重要主机是否能够进行入侵行为的监测，是否能够记录入侵的源IP、攻击的类型、攻击的目的、攻击的时间，验证是否能在发生严重入侵事件时提供报警；

b）应访谈相关技术支持人员和管理人员，查看设备相关配置及管理记录、系统安全策略、安全检测报告、网络和业务运营商提供的其他文档，检查和验证通用主机是否能够对重要程序的完整性进行检测，是否能在检测到完整性受到破坏后提供恢复的措施；

c）应访谈相关技术支持人员和管理人员，查看设备相关配置及管理记录、系统安全策略、安全检测报告、网络和业务运营商提供的其他文档，检查和验证计算机、服务器等通用主机防恶意代码产品是否使用与网络防恶意代码产品不同的恶意代码库。

5.3.3.6 资源控制

5.3.3.6.1 检测方法

访谈、检查。

5.3.3.6.2 检测对象

设备安全检测报告，设备配置、管理记录文档，系统安全策略，故障告警记录，网络和业务运营商提供的其他文档、系统及相关设备等。

5.3.3.6.3 检测实施

除按照第2级的要求进行检测之外，还应按照本节内容进行检测：

a）应访谈相关技术支持人员和管理人员，查看设备相关配置及管理记录、系统安全策略、安全检测报告、网络和业务运营商提供的其他文档，检查和验证对重要主机是否进行性能监视，包括监视主机的CPU、硬盘、内存、网络等资源的使用情况；

b）应访谈相关技术支持人员和管理人员，查看设备相关配置及管理记录、系统安全策略、安全检测报告、网络和业务运营商提供的其他文档，检查和验证能够对服务器、数据库等系统的服务水平设定报警阈值，验证当监测到服务水平降低到阈值时是否能进行报警。

5.3.4 物理环境安全

应按照YD/T 1755-2008《电信网和互联网物理环境安全等级保护检测要求》中第3.1级的相关要求进行检测。

5.3.5 管理安全

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

5.4 第3.2级要求

同第3.1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

安全等级为第5级的安全检测要求待补充。

6 非核心生产单元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，询问进行非核心生产单元风险评估时，选择的风险评估范围是什么；应检查风险评估报告，查看其风险评估范围是否与要求相一致。

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，应检查风险评估报告，查看风险评估报告是否覆盖了技术安全和管理安全；

b）应访谈风险评估负责人，询问风险评估相关技术安全中是否覆盖了服务安全、系统安全、设备安全和物理安全，应检查风险评估报告，查看风险评估报告中技术安全是否覆盖了服务安全、系统安全、设备安全和物理安全等方面；

c）应访谈风险评估负责人，询问风险评估相关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、安全建设管理、安全运维管理等方面，应检查风险评估报告，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、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，历史记录。

6.3.3 检测实施

a）应访谈风险评估负责人，询问进行风险评估时采用了哪些风险评估的要素和相关属性，应检查风险评估报告，风险评估报告中风险评估要素是否包含了资产、脆弱性、威胁、安全措施、风险和残余风险等要素，同时是否包含了与这些要素密切相关的属性，如服务、资产价值、安全需求和安全事件等；

b）应检查风险评估报告，查看风险评估报告中资产是否包含设备及主机、独立软件、数据信息、服务、人员、环境/设施等；

c）应检查风险评估报告，查看风险评估报告中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；

d）应检查风险评估报告，查看风险评估报告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，其中技术脆弱性是否包含系统脆弱性、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；

e）应检查风险评估报告，查看风险评估报告中威胁是否包含技术威胁、环境威胁和人为威胁，其中环境威胁是否包含物理环境和灾害，人为威胁是否包含恶意人员和非恶意人员；

f）应检查风险评估报告，查看风险评估报告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综合考虑；

g）应访谈风险评估负责人，询问风险评估结果是否满足风险阈值，应检查风险评估报告，查看风险评估报告中风险值的计算是否采用了合理的计算方法，是否制定了合理的风险阈值；

h）应检查风险评估报告，查看对于不可接收的风险，是否制定了相应的风险处理计划，以及采用风险处理计划以后，风险值是否满足阈值要求；

i）应访谈风险评估负责人，对于不可接收的风险，采取了哪些风险处理计划，应检查风险评估报告，查看风险评估时发现的主要问题及其解决方案，同时检查历史记录，查看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

风险评估报告。

6.4.3 检测实施

a）应访谈风险评估负责人，检查风险评估报告，验证风险评估的赋值是否遵循了合理的原则；应检查风险评估报告，查看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）应检查风险评估报告，查看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）应检查风险评估报告，查看威胁的赋值是否依据经验和（或）有关的统计数据来进行分析

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，询问风险评估中资产价值和风险值是否采用了合理的计算方法；应检查风险评估报告，查看资产价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；

b）应检查风险评估报告，查看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

风险评估报告，风险评估文件。

6.7.3 检测实施

a）应访谈风险评估负责人，询问风险评估过程中对于文件记录进行了哪些限制和控制？应检查风险评估报告和风险评估文件，查看文件发布以前是否得到批准；

b）应检查风险评估报告和风险评估文件，查看文件的更改和现行修订状态是否是可识别的；

c）应检查风险评估报告和风险评估文件，查看是否有版本划分以及相应的版本使用说明；

d）应检查风险评估报告和风险评估文件，查看是否对于作废文件作了标识；

e）应检查风险评估报告和风险评估文件，查看是否规定其标识、储存、保护、检索、保存期限以及处置所需的控制。

7 非核心生产单元灾难备份及恢复检测要求

7.1 第1级要求

本标准对安全等级为第1级的非核心生产单元暂不作要求。

7.2 第2级要求

7.2.1 冗余保护要求

7.2.1.1.1 检测方式

访谈、检查。

7.2.1.1.2 检测对象

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，网络和业务运营商提供的其他文档、系统及相关设备等。

7.2.1.1.3 检测实施

a）应访谈系统管理员，并查看系统设计/验收文档、系统拓扑图、网络和业务运营商提供的其他文档，检查和验证设备的处理能力是否具备一定的冗余是否满足业务高峰期需要。

b）应访谈系统管理员，并查看系统设计/验收文档、系统拓扑图、网络和业务运营商提供的其他文档，检查和验证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，并查看系统设计/验收文档、系统拓扑图、网络和业务运营商提供的其他文档，检查和验证系统关键设备、重要线路是否采用设备冗余的保护方式，是否具有提供灾难备份和恢复的能力。

7.2.2 数据备份要求

7.2.2.1.1 检测方式

访谈、检查。

7.2.2.1.2 检测对象

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，网络和业务运营商提供的其他文档、系统及相关设备等。

7.2.2.1.3 检测实施

a）应访谈系统管理员，并查看系统设计/验收文档、相关服务管理流程、系统安全策略、网络和业务运营商提供的其他文档，检查和验证是否建立对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，并查看系统设计/验收文档、相关服务管理流程、系统安全策略、网络和业务运营商提供的其他文档，检查和验证对关键数据和重要信息是否定期进行备份，是否具有保证相关数据和信息及时恢复的能力。

7.2.3 相关人员和技术能力要求

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，并查看人员任职信息、责任岗位规章、人员管理制度、培训考核记录，检查验证非核心生产单元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，并查看人员任职信息、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和设备操作、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，并查看人员任职信息、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 运行维护管理能力要求

7.2.4.1 检测方式

访谈、检查。

7.2.4.2 检测对象

相关管理规章/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，管理制度应涵盖系统运行、设备操作等方面。

b）应访谈安全管理人员、各相关管理、技术、运维人员，询问是否有维护管理制度，询问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，询问是否有维护管理制度，询问管理制度覆盖的范围，检查验证是否保持与其他部门、外部单位间良好的联络和协作能力。

7.2.5 灾难恢复预案要求

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，询问是否具有灾难恢复预案，应检查灾难恢复预案设计/验收文档，检查是否建立相应的灾难恢复预案。

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培训记录，检查是否对灾难恢复预案的进行教育、培训和演练。

7.3 第3.1级要求

7.3.1 冗余保护要求

7.3.1.1.1 检测方式

访谈、检查。

7.3.1.1.2 检测对象

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，网络和业务运营商提供的其他文档、系统及相关设备等。

7.3.1.1.3 检测实施

除按照第2级的要求进行检测之外，还应按照本节内容进行检测：

a）应访谈系统管理员，并查看系统设计/验收文档、系统拓扑图、网络和业务运营商提供的其他文档，检查和验证重要设备、线路是否采用冗余热备份的保护方式进行保护。

b）应访谈系统管理员，并查看系统设计/验收文档、系统拓扑图、网络和业务运营商提供的其他文档，检查和验证系统是否有流量负荷分担设计。

c）应访谈系统管理员，并查看系统设计/验收文档、系统拓扑图、网络和业务运营商提供的其他文档，检查和验证提供重要服务的系统是否进行系统级备份。

7.3.2 数据备份要求

7.3.2.1.1 检测方式

访谈、检查。

7.3.2.1.2 检测对象

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，网络和业务运营商提供的其他文档，系统及相关设备等。

7.3.2.1.3 检测实施

除按照第2级的要求进行检测之外，还应按照本节内容进行检测：

a）应访谈系统管理员，并查看系统设计/验收文档、相关服务管理流程、系统安全策略、网络和业务运营商提供的其他文档，检查和验证是否提供数据自动保护功能，当故障发生时自动保护当前所有状态，是否能保证对系统进行恢复。

b）应访谈系统管理员，并查看系统设计/验收文档、相关服务管理流程、系统安全策略、网络和业务运营商提供的其他文档，检查和验证重要的数据信息和应用服务系统是否采用分布式数据结构。

7.3.3 相关人员和技术能力要求

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

除按照第2级的要求进行检测之外，还应按照本节内容进行检测：

a）应访谈安全负责人、其他相关人员，并查看人员任职信息、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和设备操作、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，并查看人员任职信息、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进行技术培训并通过考核。

7.3.4 运行维护管理能力要求

7.3.4.1 检测方式

访谈、检查。

7.3.4.2 检测对象

相关管理规章/制度。

7.3.4.3 检测实施

除按照第2级的要求进行检测之外，还应按照本节内容进行检测：

a）应访谈安全管理人员、各相关管理、技术、运维人员，询问是否有维护管理制度，询问管理制度覆盖的范围，检查验证是否具有介质存取、验证管理制度，确保数据授权访问。

b）应访谈安全管理人员、各相关管理、技术、运维人员，询问是否有维护管理制度，询问管理制度覆盖的范围，检查验证对备份数据是否进行定期的完整性、有效性验证。

7.3.5 灾难恢复预案要求

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

除按照第2级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。

7.4 第3.2级要求

同第3.1级的检测要求。

7.5 第4级要求

同第3.2级要求。

7.6 第5级要求

安全等级为第5级的安全要求待补充。

参 考 文 献

1. GB/T 18336-2000　信息技术 信息技术安全性评估准则
2. GB/T 19716-2005　信息技术 信息安全管理实用规则
3. GB/T 19715.2-2005　信息技术 信息安全管理指南 第2部分
4. GB17859-1999　计算机信息系统安全等级划分准则
5. YD/T 1728-2008　电信网和互联网安全防护管理指南
6. YD/T 1729-20008　电信网和互联网安全等级保护实施指南
7. YD/T 1730-2008　电信网和互联网安全风险评估实施指南
8. YD/T 1731-2008　电信网和互联网灾难备份及恢复实施指南
9. YD/T 1754-2008　电信网和互联网物理环境安全等级保护要求
10. YD/T 1756-2008　电信网和互联网管理安全等级保护要求