YD

中华人民共和国通信行业标准

YD/T 1729-2008

电信网和互联网安全等级保护实施指南

Implementation Guide for Classified Security Protection of Telecom Network and Internet

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。

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。

本标准的附录A是规范性附录，附录B是资料性附录。

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、中国电信集团公司、中国网络通信集团公司、中国铁通集团有限公司

本标准主要起草人：魏　薇、杨　永、赵　阳、殷　琪、严　萍

电信网和互联网安全等级保护实施指南

1 范围

本标准规定了电信网和互联网安全等级保护的概念、对象、目标，安全等级划分和定级方法，安全等级保护实施过程中的基本原则，并结合电信网和互联网的生命周期定义了电信网和互联网安全等级保护工作的主要阶段及主要活动。

本标准适用于电信网和互联网的安全等级保护工作。

本标准是电信网和互联网安全等级保护的总体指导性文件，针对具体网络的安全等级保护可参考具体网络的安全防护要求和安全防护检测要求。

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 1730-2008　电信网和互联网安全风险评估实施指南

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

电信网 Telecom Network

利用有线和/或无线的电磁、光电系统，进行文字、声音、数据、图像或其他任何媒体的信息传递的网络，包括固定通信网、移动通信网等。

3.2

电信网和互联网安全防护体系 Security Protection Architecture of Telecom Network and Internet

电信网和互联网的安全等级保护、安全风险评估、灾难备份及恢复三项工作互为依托、互为补充、相互配合，共同构成了电信网和互联网安全防护体系。

3.3

电信网和互联网相关系统 System of Telecom Network and Internet

组成电信网和互联网的相关系统，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，而支撑网包括业务支撑和网管系统。

3.4

电信网和互联网安全等级 Security Classification of Telecom Network and Internet

电信网和互联网及相关系统安全重要程度的表征。重要程度可从电信网和互联网及相关系统受到破坏后，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。

3.5

电信网和互联网安全等级保护 Classified Security Protection of Telecom Network and Internet

指对电信网和互联网及相关系统分等级实施安全保护。

3.6

电信网和互联网基本保护要求 Basic Protection Requirements of Telecom Network and Internet

为确保电信网和互联网及相关系统具有与其安全等级相对应的安全保护能力应该满足的最低要求。

3.7

电信网和互联网安全检测 Security Testing of Telecom Network and Internet

对电信网和互联网及相关系统的安全保护能力是否达到相应保护要求进行衡量。

3.8

电信网和互联网安全风险 Security Risk of Telecom Network and Internet

人为或自然的威胁可能利用电信网和互联网及相关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。

3.9

电信网和互联网安全风险评估 Security Risk Assessment of Telecom Network and Internet

指运用科学的方法和手段，系统地分析电信网和互联网及相关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，防范和化解电信网和互联网及相关系统安全风险，将风险控制在可接受的水平，为最大限度地保障电信网和互联网及相关系统的安全提供科学依据。

3.10

电信网和互联网灾难 Disaster of Telecom Network and Internet

由于各种原因，造成电信网和互联网及相关系统故障或瘫痪，使电信网和互联网及相关系统支持的业务功能停顿或服务水平不可接受以及达到特定时间的突发性事件。

3.11

电信网和互联网灾难备份 Backup for Disaster Recovery of Telecom Network and Internet

为了电信网和互联网及相关系统灾难恢复而对相关网络要素进行备份的过程。

3.12

电信网和互联网灾难恢复 Disaster Recovery of Telecom Network and Internet

为了将电信网和互联网及相关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。

4 安全等级保护概述

4.1 安全等级保护对象

电信网和互联网安全防护工作的范围包括网络和业务运营商运营的传输、承载各类电信业务的公众电信网（含公众互联网）及其组成部分，支撑和管理公众电信网及电信业务的业务单元和控制单元以及企业办公系统（含文件管理系统、员工邮件系统、决策支持系统、人事管理系统等）、客服呼叫中心、企业门户网站等非核心生产单元。此外，电信网和互联网安全防护工作的范围还包括经营性互联网信息服务单位、移动信息服务单位、互联网接入服务单位、互联网数据中心、互联网域名服务机构等单位运营的网络或信息系统。

根据电信网和互联网安全防护标准体系，安全等级保护对象包括固定通信网、移动通信网、互联网、增值业务网等业务网，接入网、传送网、IP 承载网、信令网、同步网、支撑网等电信网和互联网相关系统以及非核心生产单元。其中，互联网包括经营性互联网信息服务单位、互联网接入服务单位、互联网数据中心、互联网域名服务机构等单位运营的网络或信息系统，增值业务网目前包括消息网、智能网等业务平台以及业务管理平台。随着安全防护标准体系进一步完善，标准体系还将包括针对增值业务提供商提供的其他增值业务系统的相关标准。

4.2 安全等级保护目标

安全等级保护的目标是通过对电信网和互联网及相关系统进行安全等级划分，按照本系列标准中的安全等级保护要求进行规划、设计、建设、运维等工作，加强电信网和互联网及相关系统的安全防护能力，确保其安全性和可靠性。

本系列标准对不同安全等级的电信网和互联网及相关系统提出不同的基本保护要求，这些基本保护要求是保障各等级电信网和互联网及相关系统安全的最基本要求。电信网和互联网及相关系统应能够满足其所属安全等级的基本保护要求。

5 安全等级划分及定级方法

5.1 安全等级划分

在电信网和互联网及相关系统中进行安全等级划分的总体原则是：定级对象受到破坏后对国家安全、社会秩序、经济运行、公共利益以及网络和业务运营商的合法权益的损害程度。

电信网和互联网及相关系统的安全等级划分如下。

第 1 级

定级对象受到破坏后，会对其网络和业务运营商的合法权益造成轻微损害，但不损害国家安全、社会秩序、经济运行和公共利益。

本级由网络和业务运营商依据国家和通信行业有关标准进行保护。

第 2 级

定级对象受到破坏后，会对网络和业务运营商的合法权益产生严重损害，或者对社会秩序、经济运行和公共利益造成轻微损害，但不损害国家安全。

本级由网络和业务运营商依据国家和通信行业有关标准进行保护，主管部门对其安全等级保护工作进行指导。

第 3 级

进一步划分为两个等级。

第 3.1 级

定级对象受到破坏后，会对网络和业务运营商的合法权益产生很严重的损害，或者对社会秩序、经济运行和公共利益造成较大损害，或者对国家安全造成轻微损害。

本级由网络和业务运营商依据国家和通信行业有关标准进行保护，主管部门对其安全等级保护工作进行监督、检查。

第 3.2 级

定级对象受到破坏后，会对网络和业务运营商的合法权益产生特别严重的损害，或者对社会秩序、经济运行和公共利益造成严重的损害，或者对国家安全造成较大损害。

本级由网络和业务运营商依据国家和通信行业有关标准进行保护，主管部门对其安全等级保护工作进行重点监督、检查。

第4级

定级对象受到破坏后，会对社会秩序、经济运行和公共利益造成特别严重的损害，或者对国家安全造成严重的损害。

本级由网络和业务运营商依据国家和通信行业有关标准以及业务的特殊安全要求进行保护，主管部门对其安全等级保护工作进行强制监督、检查。

第5级

定级对象受到破坏后，会对国家安全造成特别严重的损害。

本级由网络和业务运营商依据国家和通信行业有关标准以及业务的特殊安全需求进行保护，主管部门对其安全等级保护工作进行专门监督、检查。

5.2 定级方法

确定定级对象的安全等级应根据以下3个相互独立的定级要素。

a）社会影响力

定级对象的社会影响力表示其受到破坏后对国家安全、社会秩序、经济运行和公共利益的损害程度，定级对象的社会影响力赋值原则见表1。

表1 定级对象的社会影响力赋值原则

社会影响力定义	赋 值
定级对象受到破坏后不损害国家安全、社会秩序、经济运行和公共利益	1
定级对象受到破坏后不损害国家安全，对社会秩序、经济运行和公共利益造成轻微损害	2
定级对象受到破坏后对国家安全造成较大损害，或者对社会秩序、经济运行和公共利益造成较为严重的损害	3
定级对象受到破坏后对国家安全造成严重损害，或者对社会秩序、经济运行和公共利益造成特别严重损害	4
定级对象受到破坏后对国家安全造成特别严重损害	5

损害国家安全的事项包括（不限于）以下几个方面：

- 影响国家政权稳固和国防实力；
- 影响国家统一、民族团结和社会安定；
- 影响国家对外活动中的政治、经济利益；
- 影响国家重要的安全保卫工作；
- 影响国家经济竞争力和科技实力等。

损害社会秩序的事项包括（不限于）以下几个方面：

- 影响国家机关社会管理和公共服务的工作秩序；
- 影响各种类型的经济活动秩序；
- 影响各行业的科研、生产秩序；
- 影响公众在法律约束和道德规范下的正常生活秩序等。

损害经济运行的事项包括（不限于）以下方面：

- 直接或间接导致国家经济活动主体的经济损失等。

损害公共利益的事项包括（不限于）以下几个方面：

- 影响社会成员使用公共设施；

◆ 影响社会成员获取公开信息资源；

◆ 影响社会成员接受公共服务等。

对此定级要素进行赋值时，应先确定对国家安全的损害程度，再确定对社会秩序、经济运行和公共利益的损害程度。定级对象的社会影响力赋值应是对国家安全、社会秩序、经济运行和公共利益的损害程度最严重者。

b）规模和服务范围

定级对象的规模表示其服务的用户数多少，服务范围表示其服务的地区范围大小，定级对象的规模和服务范围赋值如表2所示。

表2 电信网和互联网及相关系统的规模和服务范围赋值

规模和服务范围定义	赋 值
定级对象被破坏后对较少的用户造成影响，或者对较小的地区造成影响	1
定级对象被破坏后对较多的用户造成影响，或者对较大的地区造成影响	2
定级对象被破坏后对很多的用户造成影响，或者对很大的地区造成影响	3
定级对象被破坏后对非常多的用户造成影响，或者对非常大的地区造成影响	4
定级对象被破坏后对特别多的用户造成影响，或者对特别大的地区造成影响	5

c）所提供服务的重要性

定级对象所提供服务的重要性表示其提供的服务被破坏后，对网络和业务运营商的合法权益的影响程度，其重要性赋值如表3所示。

表3 定级对象所提供服务的重要性赋值

所提供服务的重要性定义	赋 值
定级对象所提供服务的重要性较低，被破坏后对网络和业务运营商的合法权益造成轻微损害	1
定级对象所提供服务的重要性一般，被破坏后对网络和业务运营商的合法权益造成较大损害	2
定级对象所提供服务的重要性很高，被破坏后对网络和业务运营商的合法权益造成很大损害	3
定级对象所提供服务的重要性非常高，被破坏后对网络和业务运营商的合法权益造成非常大的损害	4
定级对象所提供服务的重要性特别高，被破坏后对网络和业务运营商的合法权益造成特别严重的损害	5

此定级要素可通过定级对象所提供的服务本身的重要性来衡量，如业务的经济价值、业务的重要性、对企业自身形象的影响等方面。

在确定好定级对象的社会影响力、规模、服务范围和所提供服务的重要性三个定级要素的赋值后，可采用附录A中安全等级的计算方法确定定级对象的安全等级。在确定某一个定级要素的赋值时，无需考虑其他两个定级要素。

安全等级的确定可能不是一个过程就可以完成的，而是需要经过定级要素赋值、定级、定级结果调整的循环过程，最终才能确定出较为科学、准确的安全等级。

6 安全等级保护的实施过程

6.1 基本原则

电信网和互联网安全等级保护工作应首先满足电信网和互联网安全防护工作提出的适度安全原则、标准性原则、可控性原则、完备性原则、最小影响原则以及保密性原则。在此基础上，电信网和互联网安全等级保护工作在实施过程中还应重点遵循以下原则。

a）自主保护原则

各网络和业务运营商应遵照本标准的定级方法确定其运营的电信网和互联网及相关系统的安全等级，并依据国家和通信行业相关标准对电信网和互联网及相关系统自主实施安全保护。

b）同步建设原则

各网络和业务运营商在对电信网和互联网及相关系统进行新建、改建、扩建时，应当同步规划和设计其安全方案，投入一定比例的资金实施安全方案，保障电信网和互联网及相关系统与其所属安全等级的要求相适应。

c）重点保护原则

各网络和业务运营商通过对电信网和互联网及相关系统划分不同的安全等级，根据基本保护要求实现不同程度的安全保护，集中资源优先保护关键的电信网和互联网及相关系统。

d）适当调整原则

各网络和业务运营商跟踪电信网和互联网及相关系统的变化情况调整其安全等级，并根据安全等级的调整情况及时调整相应的安全保护措施。

6.2 基本过程

虽然安全等级保护是一个不断循环和不断提高的过程，但是实施安全等级保护的一次完整过程是可以区分清楚的，包括5个主要阶段：安全等级确定、安全总体规划、安全设计与实施、安全运维、安全资产终止，如图1所示。

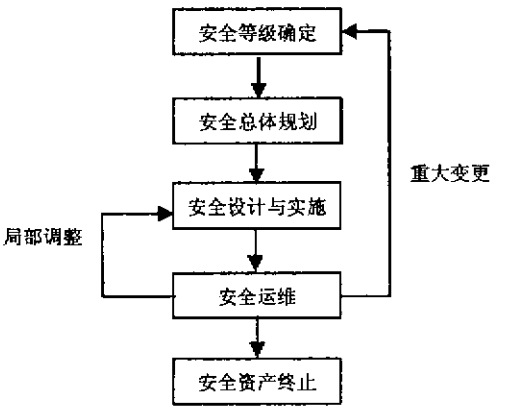

图1 安全等级保护实施的基本过程

安全等级保护的5个主要阶段及其主要活动如下。

a）安全等级确定阶段

安全等级确定阶段主要包括对电信网和互联网的识别和描述，定级对象的划分以及安全等级确定、评审和备案等几个主要安全活动。通过对电信网和互联网的识别和描述，划分并确定定级对象。根据本标准中的定级方法，科学准确地确定各定级对象的安全等级，并对定级结果进行评审和备案。

b）安全总体规划阶段

安全总体规划阶段主要包括安全需求分析、安全总体设计、安全建设规划等几个主要活动。网络和业务运营商通过安全需求分析判断网络安全保护现状与安全要求之间的差距，确定初步的安全需求，通过风险评估确定额外的安全需求；然后根据网络的实际情况，设计出合理的、满足安全等级保护要求的安全总体方案，并制定出安全建设的方案，以指导后续的网络安全建设工程实施。

c）安全设计与实施阶段

安全设计与实施阶段主要包括安全方案详细设计、安全详细设计方案的实施、安全检测等几个主要

活动。网络和业务运营商通过安全方案详细设计，将安全总体规划阶段的安全总体方案和安全建设方案具体落实到网络中，最终提交满足安全需求的网络以及配套的安全技术和管理体系。网络和业务运营商应在网络实际运行之前对其安全等级保护工作的实施情况进行安全检测，确保其达到安全防护要求。

d）安全运维阶段

安全运维阶段需要进行的安全控制活动很多，本标准描述一些重要的安全控制活动。网络和业务运营商通过运行管理和控制、变更管理和控制、安全状态监控，对发生的安全事件及时响应，确保电信网和互联网及相关系统正常运行。通过安全检查和持续改进不断跟踪电信网和互联网及相关系统的变化，并依据变化调整其安全等级和安全措施。通过安全检测，确保电信网和互联网及相关系统满足相应安全等级的要求。

e）安全资产终止阶段

安全资产终止阶段主要包括对电信网和互联网及相关系统中的信息转移、暂存或清除，设备迁移或废弃，存储介质的清除或销毁，安全检测等主要活动。核心关注点是对电信网和互联网及相关系统中过时或无用部分进行报废处理的过程，防止敏感信息泄漏。

在安全运维阶段，当电信网和互联网及相关系统发生局部调整时，如果不影响其安全等级，应从安全运维阶段进入安全设计与实施阶段，重新调整和实施安全措施，确保满足安全等级保护的要求。当电信网和互联网及相关系统发生重大变更影响其安全等级时，应从安全运维阶段进入安全等级确定阶段，重新开始一次安全等级保护的实施过程。

6.3 安全等级保护工作与电信网和互联网及相关系统生命周期的关系

电信网和互联网及相关系统的生命周期包括5个阶段：启动阶段、设计阶段、实施阶段、运维阶段和废弃阶段。电信网和互联网及相关系统的安全等级保护工作将贯穿其生命周期的各个阶段。安全等级保护工作可分为：对新建电信网和互联网及相关系统的安全等级保护和对已建电信网和互联网及相关系统的安全等级保护，两者在电信网和互联网及相关系统生命周期中的切入点是不同的，但是安全等级保护工作的主要活动基本相同，其安全等级保护过程与电信网和互联网及相关系统生命周期的关系如图2所示。

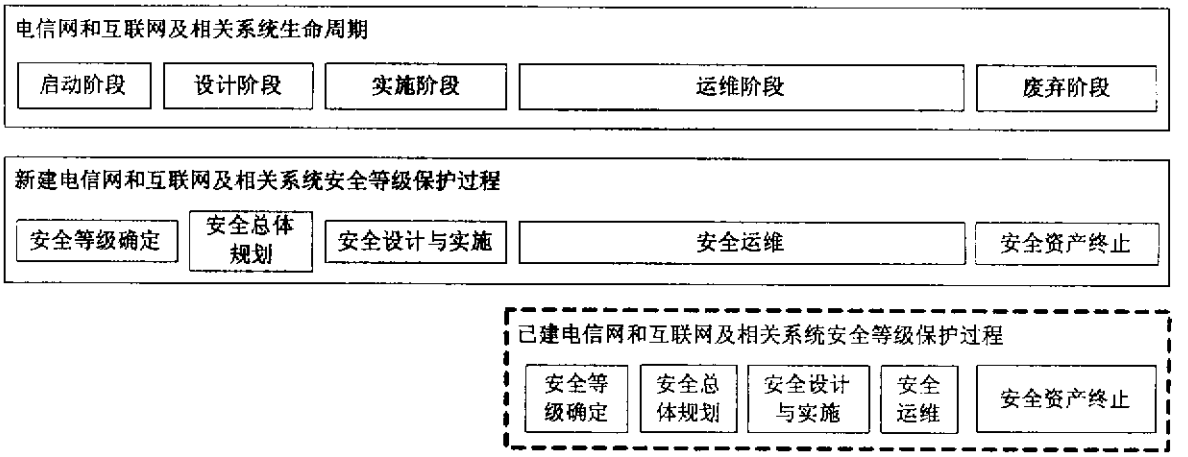

图2 安全等级保护过程与电信网和互联网及相关系统生命周期的关系

新建的电信网和互联网及相关系统在生命周期中的各个阶段应同步考虑安全等级保护的主要活动。在启动阶段，应该仔细分析和合理划分各个电信网和互联网，确定各个定级对象的安全等级，定级过程也可能在设计阶段；在设计阶段，应根据各个定级对象的安全等级，进行安全总体规划；在实施阶段，

应在网络建设的同时，同步进行安全措施的设计与实施；在运维阶段，应按照本系列标准中安全等级保护的要求进行安全运维；在废弃阶段，应对废弃的信息、设备或存储介质等资产进行有效的安全管理。

已建的电信网和互联网及相关系统通常处于运维阶段，由于在启动阶段、设计阶段和实施阶段可能没有同步考虑安全等级保护的要求或者对安全等级保护的要求考虑不足，因此应在运维阶段启动安全等级保护工作，安全等级保护过程中的安全等级确定、安全总体规划、安全设计与实施的主要活动都将在生命周期的运维阶段完成。由于是已经存在的电信网和互联网及相关系统，工作的重点是在现有网络的基础上，根据安全等级保护要求，在安全总体规划阶段如何制定满足要求的、补充的安全建设方案，在安全设计与实施阶段，如何保证在不影响现有业务/应用的情况下，分步骤、分阶段、分目标地使各类安全补救措施可以顺利落实。

在已建的电信网和互联网及相关系统基础上进行扩容的安全等级保护工作，扩容部分应与新建的电信网和互联网及相关系统的安全等级保护过程一致。

7 安全等级确定阶段

7.1 安全等级确定阶段的主要活动

安全等级确定阶段的主要活动如图3所示。

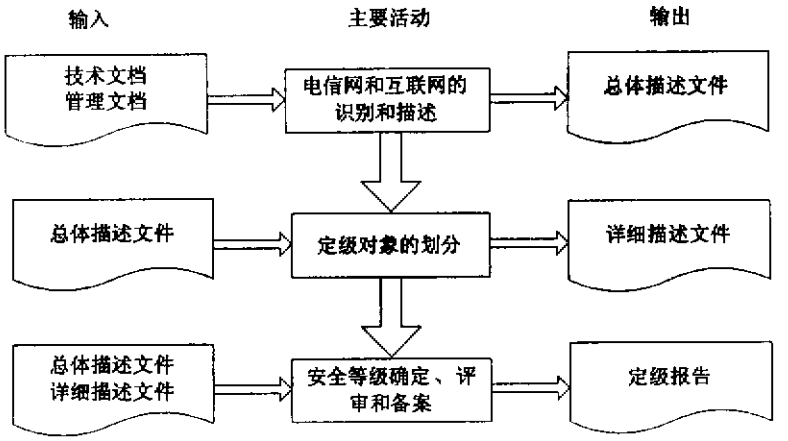

图3 安全等级确定阶段的主要活动

7.2 电信网和互联网的识别和描述

活动输入：电信网和互联网的技术文档、管理文档。

活动输出：电信网和互联网的总体描述文件。

活动描述

网络和业务运营商对电信网和互联网的识别和描述过程主要包括以下活动内容。

a）识别电信网和互联网的基本信息

调查了解电信网和互联网的企业特征、业务范围、地理位置以及其他基本情况。

b）识别电信网和互联网的管理信息

了解电信网和互联网的组织管理结构及其主要职能、岗位职责等内容，获得支持网络运营的管理特征和管理框架方面的信息。

c）识别电信网和互联网的技术信息

了解电信网和互联网的物理环境、网络拓扑结构、硬件设备的部署情况、业务/应用范围、网络处理和传送的信息资产、服务范围和用户类型等信息，明确网络边界。

d）描述电信网和互联网

对收集的电信网和互联网的基本信息、管理信息和技术信息等方面的内容进行整理、分析，形成对电信网和互联网进行总体描述的文件。

7.3 定级对象的划分

活动输入：电信网和互联网的总体描述文件。

活动输出：定级对象的详细描述文件。

活动描述

定级对象的划分包括以下主要的活动。

a）划分和确定定级对象

电信网和互联网根据所提供的业务划分为固定通信网、移动通信网、互联网、增值业务网—消息网、增值业务网—智能网等类型的业务网。业务网的底层支撑网络划分为接入网、传送网、IP承载网、信令网、同步网、支撑网等各类电信网和互联网相关系统。将电信网和互联网按照上述网络类型进行划分，并结合服务地域、责任主体等因素，进一步划分成各个定级对象。将非核心生产单元按照企业办公系统、客服呼叫中心、企业门户网站等类型进行划分，并根据管理级别进一步划分成各个定级对象。划分后的每个定级对象应属于同一种类型的网络/系统，并由单一的责任主体负责。

定级对象的划分情况如表4所示。B类定级对象是在A类定级对象的基础上进一步划分出的定级对象，网络和业务运营商可以根据具体网络情况选择A类定级对象或B类定级对象进行定级。

表4 电信网和互联网安全防护体系的定级对象划分

网络/系统类型	子网络/子系统类型	划分的定级对象	
		A类定级对象	B类定级对象
固定通信网	—	本地网	端局
			汇接局
			关口局
		省内长途网	
		省际长途网（含国际长途网）	
移动通信网	电路域	本地网	无线接入子系统
			核心交换网
			关口局
		省内长途网	
		省际长途网（含国际长途网）	
	分组域	省网部分	无线接入子系统
			核心交换网
		国际部分	
	—	电信智能卡	
互联网	—	业务及应用系统	

表4（续）

网络/系统类型		子网络/子系统类型	划分的定级对象	
			A类定级对象	B类定级对象
增值业务网—消息网		—	短消息网	
			多媒体消息网	
			消息网相关的信息服务单位系统	
增值业务网—智能网		—	本地智能网	
			省内智能网	
			全国智能网	
电信网和互联网相关系统	接入网	—	本地网下不同区域（如区、县等）	
	传送网	光传送网	本地传送网（含城域传送网）	核心层
				汇聚层
				接入层
			省内骨干传送网	
			省际骨干传送网	
			国际传送网	
		微波接力传送网	省内传送网	
			省际传送网	
		卫星传送网	国内卫星传送网	
			国际卫星传送网	
	IP承载网	—	IP城域网	汇聚层
				核心层
			IP骨干网	
	信令网	—	省内信令网	
			省际信令网（含国际信令网）	
	同步网	—	省内同步网	
			省际骨干同步网	
	支撑网	业务运营支撑系统	省业务运营支撑系统	
			全国业务运营支撑系统	
		网管系统	省网管系统	
			全国网管系统	
非核心生产单元		企业办公系统	省公司办公系统	
			集团公司办公系统	
		客服呼叫中心	地市客服呼叫中心	
			省客服呼叫中心	
			集团客服呼叫中心	
		企业门户网站	省公司门户网站	
			集团公司门户网站	

b）详细描述定级对象

划分并确定定级对象后，网络和业务运营商应准确描述划分出的定级对象，包括划分后的定级对象的个数，每个定级对象的涵盖范围、架构、边界、设备部署、业务/应用范围、处理或传送的信息资产类型、服务范围和用户类型等方面的内容，形成对定级对象的详细描述文件。

7.4 安全等级确定、评审和备案

活动输入：电信网和互联网的总体描述文件、定级对象的详细描述文件。

活动输出：定级报告。

活动描述

安全等级确定、评审和备案包括以下主要活动内容。

a）初步确定定级对象的安全等级

网络和业务运营商应根据本标准的定级方法，初步确定各个定级对象的安全等级。

可采取两种方法确定某一定级对象的安全等级：一种方法是通过本标准的定级方法直接确定其安全等级，另一种方法是在构成此定级对象的B类定级对象的安全等级基础上，通过一定的算法（如取最高安全等级）得到此定级对象的安全等级。

b）形成定级报告

网络和业务运营商对电信网和互联网的总体描述、定级对象的详细描述、安全等级确定结果等内容进行整理，针对各定级对象形成定级报告，若定级对象包含两个或两个以上的安全等级，需针对每一个安全等级分别形成定级报告。

c）定级结果评审和备案

网络和业务运营商应根据要求，将定级结果上报评审并办理备案，填写备案信息登记表，并提交最终的定级报告。

8 安全总体规划阶段

8.1 主要活动

网络和业务运营商在安全总体规划阶段的主要活动内容如图4所示。

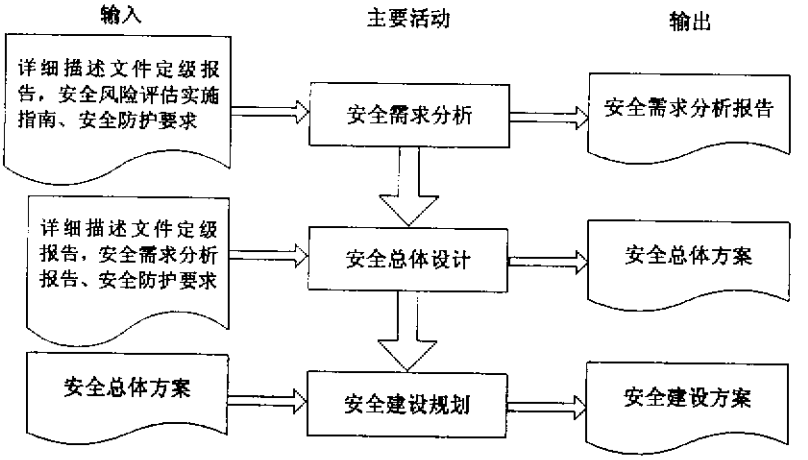

图4 安全总体规划阶段的主要活动

8.2 安全需求分析

活动输入：详细描述文件、定级报告、电信网和互联网安全风险评估实施指南、安全防护要求。

活动输出：电信网和互联网及相关系统的安全需求分析报告。

活动描述

安全需求分析包括以下主要活动内容。

a）确定初步的安全需求

网络和业务运营商首先应确定具体进行安全等级保护工作的对象，包括整体对象（如机房、办公环境、网络等）和具体对象（如边界设备、网关设备、服务器设备、工作站、应用系统等）；获得其技术和管理方面的信息。技术方面包括业务/应用、网络、设备、物理环境等信息；管理方面包括安全管理机构、安全管理制度、人员管理、网络建设和运维管理等信息。

在此基础上，将安全等级保护对象对应的安全防护要求中，安全等级保护管理和技术方面的安全指标作为依据，将安全等级保护对象的安全现状与指标进行逐一对比，通过观察现场、询问人员、查询资料、检查记录等方式进行安全管理方面的比较。通过观察现场、询问人员、查询资料、检查记录、检查配置、技术测试、渗透攻击等方式进行安全技术方面的比较，判断安全管理和技术的各个方面与等级保护要求中的基本安全要求之间的差距，给出初步的安全需求。

b）制定额外的安全需求

在确定初步安全需求的基础上，参照YD/T 1730-2008《电信网和互联网安全风险评估实施指南》对安全等级保护对象进行安全风险评估，即通过分析安全等级保护对象中的重要资产的资产价值、存在的脆弱性、面临的威胁以及已经采取的安全措施，判断安全等级保护对象可能存在的安全风险，在初步安全需求的基础上，制定出额外的安全需求。

对于安全等级保护对象中的关键系统和数据，为确保在灾难发生后网络能够尽快恢复和继续运行，应制定出有效的灾难备份及恢复的额外需求。

在制定额外安全需求时，应明确国家及企业的安全目标，借鉴以往建设的类似或相关的电信网和互联网及相关系统的安全需求，并且确保安全需求与其他相关标准或规范对其安全需求不发生冲突。

c）输出安全需求分析报告

总结安全指标对比结果和风险评估的结果，获得安全等级保护对象安全现状的汇总与安全防护要求中安全等级保护要求的差距汇总和额外的安全需求的汇总，最终形成安全需求分析报告，报告中应包括安全管理状况和安全技术状况。

8.3 安全总体设计

活动输入：详细描述文件、定级报告、安全需求分析报告、安全防护要求。

活动输出：电信网和互联网及相关系统的安全总体方案。

活动描述

安全总体设计包括以下主要活动内容。

a）设计各电信网和互联网及相关系统的安全措施

对一个大型、复杂电信网和互联网及相关系统的构成内容进行抽象处理，提取共性形成模型和要素，如服务器设备、构成网络的网络设备等。根据安全防护要求中的等级保护相关要求和安全需求分析报告，针对模型要素提出需要实现的安全措施，包括安全技术方面的措施和安全管理方面的措施，以指导安全等级保护工作的具体实现。

b）设计结果文档化

最终将安全总体设计工作的结果文档化，形成满足其所属的安全等级要求的安全总体方案。安全总

体方案中包括总体安全策略、技术措施和管理措施等。

8.4 安全建设规划

活动输入：电信网和互联网及相关系统的安全总体方案。

活动输出：电信网和互联网及相关系统的安全建设方案。

活动描述

安全建设规划包括以下主要活动内容。

a）确定分阶段的安全建设目标、内容、方案

安全建设规划是依据电信网和互联网及相关系统安全总体方案，网络和业务运营商当前面临的机遇和挑战以及安全建设时间和经费投入状况，结合安全需求的分析结果，同时考虑到网络和业务运营商的中长期发展规划，提出分阶段的安全建设目标、设计建设内容，并形成安全建设方案，重点是形成近期可行的安全建设方案。安全建设方案中包括安全技术建设规划和安全管理建设规划。

b）规划结果文档化

最终将安全建设规划的结果文档化，形成分阶段的安全建设方案，安全建设方案中包括总体安全建设规划、技术体系建设规划和管理体系建设规划等。

9 安全设计与实施阶段

9.1 主要活动

网络和业务运营商按照安全总体方案的要求，结合安全建设方案，分期、分步骤地对其运营的电信网和互联网及相关系统落实安全措施。安全设计与实施阶段的主要活动如图5所示。

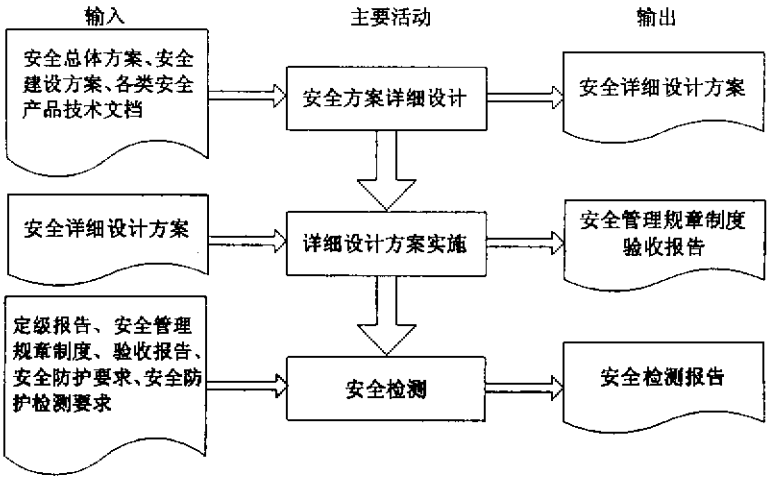

图5 安全设计与实施阶段的主要活动

9.2 安全方案详细设计

活动输入：电信网和互联网及相关系统的安全总体方案、安全建设方案、各类安全产品技术文档。

活动输出：电信网和互联网及相关系统的安全详细设计方案。

活动描述

安全方案详细设计包括以下主要活动内容。

a）安全等级保护实施内容设计

安全等级保护技术实施内容的设计是网络和业务运营商根据本期建设目标和建设内容，将安全总体方案和安全建设方案在本阶段中的要求落实到产品功能或物理形态上，提出指定的产品或组件及其具体

规范，明确安全产品的功能和性能要求设计，网络或设备的部署方案。

安全等级保护管理实施内容的设计是网络和业务运营商根据当前安全管理和技术需要提出与安全总体方案中管理部分相适应的本期安全实施内容，以保证在安全技术建设的同时，安全管理的同步建设。安全管理设计的内容主要考虑安全管理机构和人员的配套、安全管理制度的配套、人员安全管理技能的配套等。

b）设计结果文档化

将安全等级保护技术实施内容和安全等级保护管理实施内容的设计汇总，同时考虑工时和经费，最后形成安全详细设计方案，指导具体的安全实施。

9.3 安全详细设计方案实施

活动输入：电信网和互联网及相关系统的安全详细设计方案。

活动输出：电信网和互联网及相关系统的安全管理规章制度、验收报告。

活动描述

安全详细设计方案的具体实施包括以下主要活动内容。

a）实施安全详细设计方案

在本期安全详细设计方案的指导下，进行安全等级保护管理实施和安全等级保护技术实施。

安全等级保护管理实施主要是建立与电信网和互联网及相关系统安全技术和安全运行相适应的安全管理机制，包括建立配套的安全管理机构和人员，建立配套的安全管理制度和操作规程，进行人员的安全技能培训等，并且在安全实施过程中，对工程的质量、进度、文档和变更等方面的工作进行监管。

安全等级保护技术实施主要是保证按照安全详细设计方案实现各项安全技术措施，包括安全产品采购、安全控制开发、安全控制集成、测试与验收等主要活动环节。安全产品采购是按照安全详细设计方案中对于产品的具体指标要求进行产品采购，根据产品或产品组合实现的功能和满足安全设计要求的情况来选购所需的安全产品；安全控制开发是对于一些不能通过采购现有安全产品来实现的安全措施和安全功能，通过专门的设计、开发来实现；安全控制集成依据安全详细设计方案，将安全产品、软件平台和开发的安全控制模块与各种应用综合、整合成为一个系统；最后通过测试与验收检验网络/系统是否严格按照安全详细设计方案进行建设，是否实现了设计的功能和性能，从而确保安全技术措施的有效性。

b）实施结果文档化

在本期安全实施完成后，建成满足安全需求并通过测试验收的电信网和互联网及相关系统，提交验收报告，内容包括安全产品清单、验收过程及结果等；提交配套的安全管理规章制度。

9.4 安全检测

活动输入：定级报告、安全管理规章制度、验收报告、安全防护要求、安全防护检测要求。

活动输出：电信网和互联网及相关系统的安全检测报告。

活动描述

安全检测是依据本系列标准中的安全防护要求和安全防护检测要求，对电信网和互联网及相关系统的安全保护管理制度和技术措施的落实情况以及安全现状的达标情况进行检查，判断其安全保护措施是否符合相应安全等级的基本保护要求。

安全检测完成后，检测方应根据实际检测情况形成检测报告。

10 安全运维阶段

10.1 主要活动

安全运维是确保电信网和互联网及相关系统正常运行的必要环节。安全运维阶段涉及的内容较多，本标准关注网络和业务运营商在安全运维阶段进行的运行管理和控制、变更管理和控制、安全状态监控、安全事件处置、应急预案、安全检查和持续改进等活动。重点描述各个活动的主要活动内容，网络和业务运营商可根据自身网络实际情况考虑对其他安全运维阶段的活动内容进行添加或删减。安全运维阶段的工作还包括对安全等级保护工作落实情况进行的安全检测。

安全运维阶段的主要活动内容如图 6 所示。

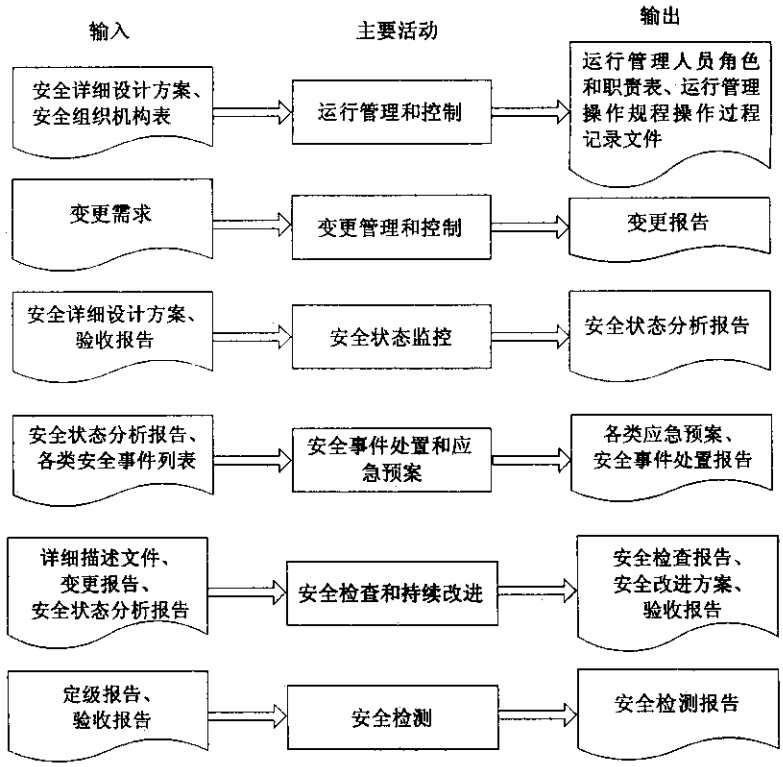

图6 安全运维阶段的主要活动

10.2 运行管理和控制

活动输入：电信网和互联网及相关系统的安全详细设计方案、安全组织机构表。

活动输出：电信网和互联网及相关系统的运行管理人员角色和职责表、运行管理操作规程、操作过程记录文件。

活动描述

运行管理和控制的目标是确保电信网和互联网及相关系统的安全运行，操作人员应实行正确和安全的操作，并且保证不断变化和种类繁多的运行管理活动得到控制。本标准中，安全运行管理和控制关注的方面主要是运行管理职责确定和运行管理过程控制。

运行管理和控制包括以下主要活动内容。

a）运行管理职责确定

运行管理职责确定是通过对运行管理活动相关的角色划分，并授予相应的管理权限，来确定安全运行管理的具体人员和职责。

b）运行管理过程控制

运行管理过程控制是通过制定运行管理操作规程，确定运行管理人员的操作目的、操作内容、操作时间和地点、操作方法和流程等，并进行操作过程记录，确保对操作过程进行控制。安全等级越高的电信网和互联网及相关系统，需要控制的运行活动就越多。

c）输出结果文档

通过运行管理的职责确定形成运行管理人员角色和职责表；通过对运行管理过程进行控制，形成运行管理操作规程以及操作过程记录文件。

10.3 变更管理和控制

活动输入：电信网和互联网及相关系统的变更需求。

活动输出：电信网和互联网及相关系统的变更报告。

活动描述

变更管理和控制的目标是确保在电信网和互联网及相关系统发生变化的时候，使用标准的方法和步骤尽快地实施变更。

运行管理和控制包括以下主要活动内容。

a）变更需求和影响分析

通过对变更需求和变更影响的分析，制定变更方案。

b）变更过程控制

确保变更实施过程受到控制，审核变更内容，对各项变化内容进行记录，保证变更对正在运行的电信网和互联网及相关系统的影响最小。

c）输出结果文档

根据变更方案和变更实施过程的各项活动，形成变更报告。

10.4 安全状态监控

活动输入：电信网和互联网及相关系统的安全详细设计方案、验收报告。

活动输出：电信网和互联网及相关系统的安全状态分析报告。

活动描述

安全状态监控包括以下主要活动内容。

a）确定监控对象和工具

不同安全等级的电信网和互联网及相关系统在安全状态监控方面要求采用的手段和监控的内容不同，所以应根据监控的必要性和可行性、监控的开销和成本等因素确定监控对象，形成监控对象列表。根据监控对象的特点、监控管理的具体要求、监控工具的功能、性能特点等，选择合适的监控工具。

b）监控对象状态

通过监控工具对监控对象的安全状态进行监控，收集来自监控对象的各类状态信息，可能包括网络流量、日志信息、安全报警和性能状况等，或者是来自外部环境的安全标准和法律法规的变更信息。

c）监控状态分析和报告

对安全状态信息进行分析，及时发现安全事件或安全变更需求，并对其影响程度和范围进行分析，形成安全状态分析报告。

10.5 安全事件处置和应急预案

活动输入：电信网和互联网及相关系统的安全状态分析报告、各类安全事件列表。

活动输出：电信网和互联网及相关系统的各类应急预案、安全事件处置报告。

活动描述

安全事件处置和应急预案包括以下主要活动内容。

a）安全事件分级

安全事件采取分级响应与处置的机制。网络和业务运营商应根据安全事件相关标准中规定的安全事件分级原则和划分结果，结合自身具体的实际情况，通过预测、评估和分析事件对电信网和互联网及相关系统的破坏程度以及所造成后果的严重程度，将安全事件进行等级划分。

b）应急预案制定

针对安全事件等级，确定需制定应急预案的安全事件对象。针对不同等级、不同优先级的安全事件，制定相应的应急预案程序，说明应急预案启动的条件，发生安全事件后要采取的流程和措施等，充分体现自主保护的原则，保障电信网和互联网及相关系统的持续运行。

c）安全事件处置

根据安全状态分析报告分析可能的安全事件，如果明确为安全事件的，则需采取适当的方法进行处置，对安全事件的等级和影响程度等进行分析，确定是否启动应急预案。

d）输出结果文档

对安全事件处置过程进行总结，形成安全事件处置报告，报告中包括安全事件的类型、等级和采取的措施等，并输出制定的应急预案。

10.6 安全检查和持续改进

活动输入：电信网和互联网及相关系统的详细描述文件、变更报告，安全状态分析报告。

活动输出：电信网和互联网及相关系统的安全检查报告、安全改进方案、验收报告。

安全检查和持续改进包括以下主要活动内容。

a）安全状态检查

在电信网和互联网及相关系统安全运维过程中，会发生电信网和互联网及相关系统变更、安全状态改变等情况，因此必须定期对电信网和互联网及相关系统进行安全检查。网络和业务运营商通过安全状态检查，为电信网和互联网及相关系统的持续改进过程提供依据和建议，确保电信网和互联网及相关系统的安全保护能力满足其相应等级的基本安全要求和自身特殊的安全需求。

安全检查可以采用定期的安全检测、自我检查等手段实现，本节描述自我检查过程。风险评估可以作为安全检查的一种手段。网络和业务运营商可通过询问、检查和测试等多种手段进行安全状况检查，记录各种检查活动的结果数据，分析安全措施的有效性、安全事件产生的可能性，并可根据检查结果提出对电信网和互联网及相关系统的改进需求和建议等。

关于安全检测参见10.7节。

b）改进方案制定和实施

根据安全检查结果对电信网和互联网及相关系统进行持续改进，确定安全改进的策略，分为以下几种情况。

1） 如果涉及安全等级的变化，则应进入安全等级保护的一个新的循环过程。

2） 如果安全等级不变，有以下两种情况。

i 如果调整内容较多、涉及范围较大，则应对安全改进项目进行立项，重新开始安全设计与实施过程。

ii 如果调整内容较小，则制定安全改进方案进行局部补充或局部调整，确定安全改进的工作方法、工作内容、人员分工、时间计划、管理内容的调整和技术内容的调整等。然后进行安全改进方案的实施，并对改进后的电信网和互联网及相关系统进行验收。

通过对电信网和互联网及相关系统进行持续改进，确保电信网和互联网及相关系统的安全保护能力满足相应等级安全要求和自身特殊的安全需求，确保安全等级保护工作的有效性。

c）输出结果文档

对安全状态检查后，形成安全检查报告，制定安全改进方案，并根据验收结果形成验收报告。

10.7 安全检测

活动输入：电信网和互联网及相关系统的定级报告、验收报告。

活动输出：电信网和互联网及相关系统的安全检测报告。

活动描述

遵照安全等级保护相关标准，对已经完成安全等级保护建设，并投入运行的电信网和互联网及相关系统进行安全检测，判断其安全保护措施是否符合相应安全等级的基本保护要求。

具体活动过程参见9.4节。

11 安全资产终止阶段

11.1 主要活动

安全资产终止是指电信网和互联网及相关系统中部分设备或者信息，由于技术改进或业务升级等原因需要转移、终止或废弃，此时应将网络/系统中的重要信息转移到新的网络/系统中，并且进行相关的设备迁移或介质销毁等工作，从而确保网络和业务运营商的网络、重要信息，为用户提供服务的安全。

本标准在安全资产终止阶段关注网络和业务运营商对信息转移、暂存和清除、设备迁移或废弃、存储介质的清除或销毁等活动，重点描述各个活动的主要内容，网络和业务运营商可根据网络的实际情况考虑对安全资产终止阶段具体活动内容进行添加或删减。安全资产终止阶段的工作还包括对安全等级保护工作落实情况进行的安全检测。

安全资产终止阶段的主要活动如图7所示。

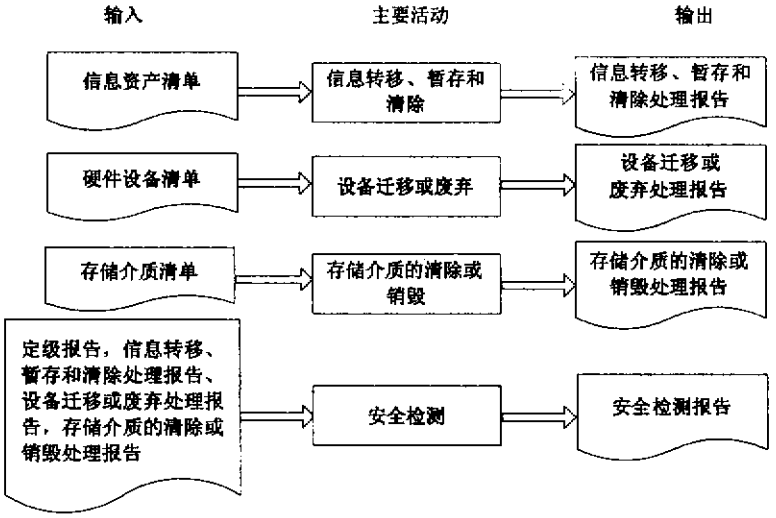

图7 安全资产终止阶段的主要活动

11.2 信息转移、暂存或清除

活动输入：电信网和互联网及相关系统的信息资产清单。

活动输出：电信网和互联网及相关系统的信息转移、暂存和清除处理报告。

活动描述

信息转移、暂存或清除包括以下主要活动内容。

a）识别要转移、暂存和清除的信息资产

在安全资产终止处理过程中，对于可能会在另外的电信网和互联网及相关系统中使用的信息，应采取适当的方法将其安全地转移或暂存到可以恢复的介质中，确保将来可以继续使用，同时采用安全的方法清除要终止的电信网和互联网及相关系统中的信息。

网络和业务运营商应根据要终止的电信网和互联网及相关系统的信息资产清单，对其当前状态进行分析，列出需转移、暂存和清除的信息资产的清单。

b）信息资产转移、暂存和清除

网络和业务运营商应根据信息资产的重要程度制定信息资产的转移、暂存和清除的处理方案，包括处理方法和过程等。处理方案应该经过审查和批准。审批通过后，根据处理方案对信息资产进行转移、暂存和清除。

c）处理过程记录

网络和业务运营商应记录信息转移、暂存和清除的过程，包括参与的人员、转移、暂存和清除的方式以及目前信息所处的位置等，输出信息转移、暂存和清除处理报告。

11.3 设备迁移或废弃

活动输入：电信网和互联网及相关系统的设备清单。

活动输出：电信网和互联网及相关系统的设备迁移或废弃处理报告。

活动描述

设备迁移或废弃包括以下主要活动内容：

a）硬件设备识别

网络和业务运营商应根据要终止的电信网和互联网及相关系统的设备清单，对设备当前状态进行分析，列出需迁移或废弃的设备清单。

b）硬件设备处理

网络和业务运营商应根据规定和实际情况制定设备处理方案，包括重用设备、废弃设备、敏感信息的清除方法等。设备处理方案应该经过审查和批准。审批通过后，根据设备处理方案对设备进行处理，确保迁移或废弃的设备内不包括敏感信息，对设备的处理方式应符合国家和行业相关部门的要求。

a） 设备处理过程记录

网络和业务运营商应记录设备处理过程，包括参与的人员、处理的方式、是否有残余信息的检查结果等，输出设备迁移或废弃处理报告。

11.4 存储介质的清除或销毁

活动输入：电信网和互联网及相关系统的存储介质清单。

活动输出：电信网和互联网及相关系统的存储介质的清除或销毁处理报告。

活动描述

存储介质的清除或销毁包括以下主要活动内容。

a）识别要清除或销毁的介质

网络和业务运营商应根据要终止的电信网和互联网及相关系统的存储介质（包括磁带、磁盘、打印结果和文档）清单，识别载有重要信息的存储介质、所处的位置以及当前状态等，列出需清除或销毁的存储介质清单。

b）存储介质处理

网络和业务运营商应根据存储介质所承载信息的敏感程度确定存储介质处理方案，包括对存储介质的处理方式和处理流程等内容，处理方式包括数据清除和存储介质销毁等。通过采用合理的方式对存储介质进行清除或销毁处理，防止介质内的敏感信息泄露。处理方案应该经过审查和批准。审批通过后，根据存储介质处理方案对存储介质进行处理。

c）存储介质处理过程记录

网络和业务运营商应记录处理过程，包括参与的人员、处理的方式、是否有残余信息的检查结果等，输出存储介质的清除或销毁处理报告。

11.5 安全检测

活动输入：电信网和互联网及相关系统的定级报告，信息转移、暂存和清除处理报告，设备迁移或废弃处理报告，存储介质的清除或销毁处理报告。

活动输出：电信网和互联网及相关系统的安全检测报告。

活动描述

通过对电信网和互联网及相关系统中的废弃资产进行安全检测，判断其安全保护措施是否符合相应安全等级的基本保护要求。

具体活动过程参见9.4节。

附 录 A
（规范性附录）
安全等级的计算方法——对数法

可使用下面的公式来计算定级对象的安全等级值：

$k = \mathrm{Round1}\{\mathrm{Log}_2\{[\alpha\times 2^I+\beta\times 2^R+\gamma\times 2^V]\}\}$

其中，k代表安全等级值，I代表社会影响力赋值、R代表规模和服务范围赋值、V代表所提供服务的重要性赋值，Round1{}表示四舍五入处理，保留1位小数，Log_2[]表示取以2为底的对数，α、β、γ分别表示定级对象的社会影响力、规模和服务范围以及所提供服务的重要性赋值所占的权重，$\alpha\geq 0$、$\beta\geq 0$、$\gamma\geq 0$，且$\alpha+\beta+\gamma=1$。网络和业务运营商可根据具体网络的情况确定α、β、γ的取值。

计算所得定级对象的安全等级值与安全等级的映射关系如表A.1所示。

表A.1 安全等级值与安全等级的映射关系

安全等级值 k	安全等级
$1\leq k < 1.5$	第 1 级
$1.5\leq k < 2.5$	第 2 级
$2.5\leq k < 3.3$	第 3.1 级
$3.3\leq k\leq 4$	第 3.2 级
$4 < k < 4.5$	第 4 级
$4.5\leq k\leq 5$	第 5 级

附 录 B
（资料性附录）
定级实例

本附录以增值业务网—消息网中的短消息网为例，对定级过程进行简要分析，并假定确定的定级对象为短消息网A。

例1 短消息网A

采用对数法确定短消息网A的安全等级，则短消息网A的安全等级分析如下：

1） 短消息网A主要为公众用户提供服务，短消息网A被损害后对国家安全不产生影响，也不会对其他重要行业、企事业单位造成影响，仅对公众用户使用短消息进行通信造成影响，因此社会影响力的赋值为2；

2） 短消息网A为某中等规模省份的短消息网，因此规模和服务范围的赋值为2；

3） 消息类业务与语音业务等基本业务相比重要性较低，但也是近年来网络和业务运营商的重要收入来源，因此短消息网A所提供服务的重要性为2；

4） 采用对数法，取$\alpha=\beta=\gamma=1/3$，计算得短消息网A的安全等级值为2；

5） 通过表A.1可知，短消息网A的安全等级是第2级。

参 考 文 献

1. 国家标准　　信息安全技术 信息系统安全等级保护实施指南
2. 国家标准　　信息安全技术 信息系统安全等级保护定级指南