YD

# 中华人民共和国通信行业标准

YD/T 1730-2008

# 电信网和互联网安全风险评估实施指南

Implementation Guide for Security Risk Assessment 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和附录B是规范性附录。

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、中国电信集团公司、中国移动通信集团公司、中国网络通信集团公司、中国联合通信有限公司、中国铁通集团有限公司

本标准主要起草人：魏　薇、赵　阳、周　智、殷　琪、杜之亭、张云勇、冯　铭

# 电信网和互联网安全风险评估实施指南

## 1 范围

本标准规定了对电信网和互联网安全进行风险评估的要素及要素之间的关系、实施流程、工作形式、遵循的原则，在电信网和互联网生命周期不同阶段的不同要求和实施要点。

本标准适用于电信网和互联网的风险评估工作。

本标准可作为电信网和互联网安全风险评估的总体指导性文件，针对具体网络的安全风险评估可参见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 |
| GB/T 9361-2000 | 计算机场地安全要求 |
| GB/T 19716-2005 | 信息技术信息安全管理实用规则 |
| YD/T 754-95 | 通信机房静电防护通则 |
| YD/T 5026-2005 | 电信机房铁架安装设计标准 |
| YD 5002-94 | 邮电建筑防火设计标准 |
| YD 5098-2005 | 通信局（站）防雷与接地工程设计规范 |
| YDN 126-2005 | 增值电信业务网络信息安全保障基本要求 |
| YDN 127-2005 | 电信设备的安全准则 |
| ISO/IEC 13335.1-2004 | 信息技术—安全技术—IT安全管理指南 第1部分:IT安全管理概念和模型 |
| ISO/IEC 17799-2005 | 信息技术—安全技术—信息安全管理实施准则 |

## 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

**资产 Asset**

电信网和互联网及相关系统中具有价值的资源，是安全防护体系保护的对象。电信网和互联网及相关系统中的资产可能以多种形式存在，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IP承载网中的路由器、支撑网中的用户数据、传送网的网络布局。

3.5

资产价值 Asset Value

电信网和互联网及相关系统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。

3.6

**威胁 Threat**

可能导致对电信网和互联网及相关系统产生危害的不希望事件的潜在起因，它可能是人为的，也可能是非人为的，可能是无意失误，也可能是恶意攻击。常见的网络威胁有偷窃、冒名顶替、病毒、特洛伊木马、错误路由、火灾、水灾等。

3.7

**脆弱性 Vulnerability**

脆弱性是电信网和互联网及相关系统资产中存在的弱点、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。

3.8

**组织 Organization**

组织是由电信网和互联网及相关系统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。

3.9

**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。

3.10

**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，并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。

3.11

**残余风险 Residual Risk**

采取了安全措施后，电信网和互联网及相关系统中仍然可能存在的风险。

3.12

**可用性 Availability**

电信网和互联网及相关系统可正常提供服务。

3.13

**业务战略 Business Strategy**

电信网和互联网及相关系统的组织为实现其发展目标而制定的一组规则或要求。

3.14

安全事件 Security Event

威胁利用脆弱性产生的对电信网和互联网及相关系统的危害情况。

3.15

**安全需求 Security Requirement**

为保证电信网和互联网及相关系统的组织业务战略的正常运作而在安全措施方面提出的要求。

3.16

**安全措施 Security Measure**

电信网和互联网及相关系统中保护资产、抵御威胁、减少脆弱性、降低风险、控制安全事件的影响以及因打击犯罪而实施的各种实践、规程和机制的总称。安全措施主要体现在检测、阻止、防护、限制、修正、恢复和监视等多方面。完整的安全保护体系应协调建立于物理环境、技术环境、人员和管理等 4 个领域。

3.17

**自评估 Self Assessment**

由网络和业务运营商发起的，依据通信行业标准对电信网和互联网及相关系统进行的风险评估活动。

3.18

**检查评估 Inspection Assessment**

由主管部门发起的，依据通信行业标准对电信网和互联网及相关系统进行的具有强制性的检查活动。

## 4 风险评估框架及流程

### 4.1 风险要素关系

风险评估中各要素的关系如图 1 所示。

图 1 中方框部分的内容为风险评估的基本要素，椭圆部分的内容是与这些要素相关的属性。风险评估围绕其基本要素展开，在对这些要素的评估过程中需要充分考虑基本要素相关的各类属性。

风险要素及属性之间存在着以下关系。

a） 业务战略依赖资产去实现。

b） 资产是有价值的，组织的业务战略对资产的依赖度越高，资产价值就越大。

c） 资产价值越大则其面临的风险越大。

d） 风险是由威胁引发的，资产面临的威胁越多则风险越大，并可能演变成安全事件。

e） 脆弱性越多，威胁利用脆弱性导致安全事件的可能性越大。

f） 脆弱性是未被满足的安全需求，威胁要利用脆弱性来危害资产，从而形成风险。

g） 风险的存在及对风险的认识导出安全需求。

h） 安全需求可通过安全措施得以满足，需要结合资产价值考虑实施成本。

i） 安全措施可抵御威胁，降低安全事件发生的可能性，并减少影响。

j） 风险不可能也没有必要降为零，在实施了安全措施后还会有残留下来的风险。有些残余风险来自于安全措施的不当或无效，需要进一步控制，而有些残余风险则是在综合考虑了安全成本与效益后未控制的风险，是可以被接受的。

k） 残余风险应受到密切监视，它可能会在将来诱发新的安全事件。

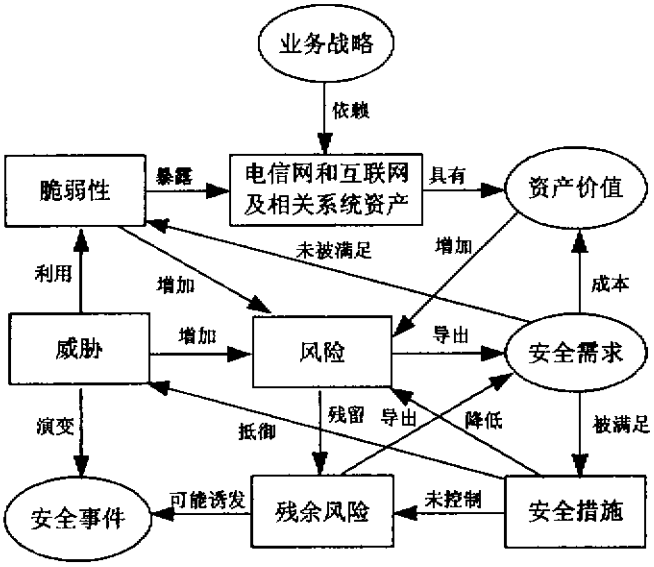


**图 1 电信网和互联网及相关系统风险要素的关系**

## 4.2 实施流程

图 2 给出了风险评估的实施流程，第 5 章将围绕风险评估流程阐述风险评估的具体实施步骤。

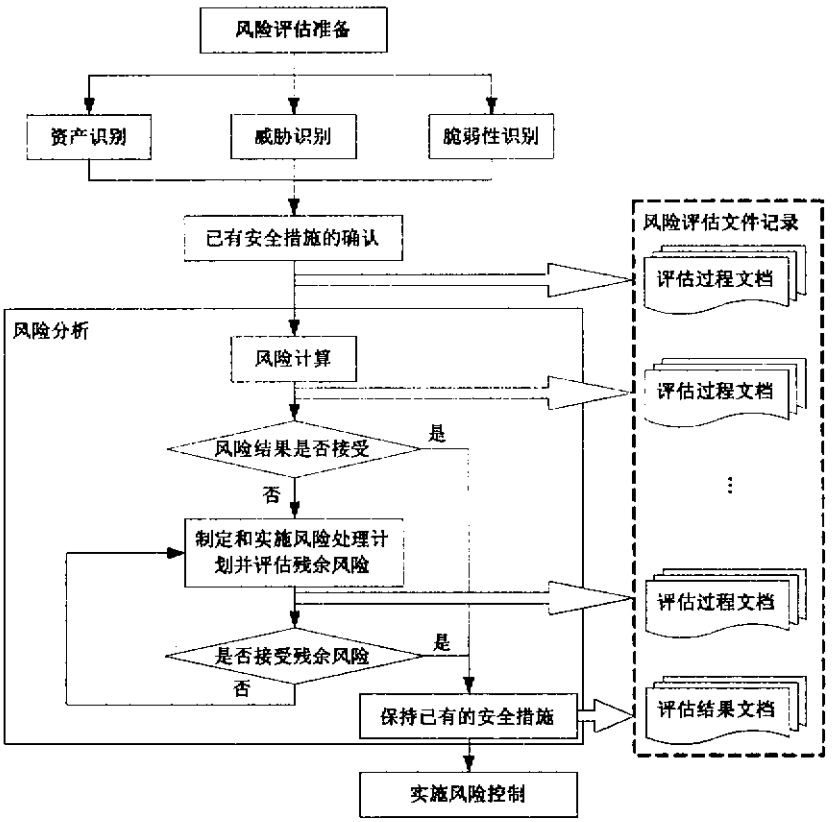


**图 2 风险评估实施的流程**

### 4.3 工作形式

根据评估发起者的不同，可以将风险评估的工作形式分为自评估和检查评估。风险评估应以自评估为主，自评估和检查评估相互结合、互为补充。

#### 4.3.1 自评估

自评估是由网络和业务运营商发起，依据通信行业标准，对其所运营的电信网和互联网及相关系统进行的风险评估。通过自评估，网络和业务运营商可以更好地了解自己运营的电信网和互联网及相关系统的安全状况以及存在的风险，从而进一步选择合适的安全措施，降低被评估的电信网和互联网及相关系统的安全风险。

#### 4.3.2 检查评估

检查评估是由上级主管部门发起、通过行政手段加强电信网和互联网及相关系统安全的重要措施。

检查评估旨在检查网络和业务运营商的风险评估工作的开展情况，电信网和互联网及相关系统的关键点的安全风险是否在可接受的范围内，实施自评估后采取的风险控制措施取得的效果等。

### 4.4 遵循的原则

为顺利完成风险评估，应遵循如下原则。

#### 4.4.1 标准性原则

风险评估工作的指导性原则，指遵循通信行业相关标准开展电信网和互联网及相关系统的安全风险评估工作。

#### 4.4.2 可控性原则

在评估过程中，应保证参与评估的人员、使用的技术和工具、评估过程都是可控的。

#### 4.4.3 完备性原则

严格按照被评估方提供的评估范围进行全面的评估。

#### 4.4.4 最小影响原则

从项目管理层面和工具技术层面，将评估工作对电信网和互联网及相关系统正常运行的可能影响降低到最低限度，不会对被评估网络上的业务运行产生显著影响。

#### 4.4.5 保密原则

评估方应与被评估的网络和业务运营商签署相关的保密协议和非侵害性协议，以保障被评估方的利益。

## 5 风险评估实施

### 5.1 风险评估的准备

风险评估的准备是整个风险评估过程有效性的保证。实施风险评估是一种战略性的考虑，其结果将受到组织的业务战略、业务流程、安全需求、系统规模和结构等方面的影响，因此，在风险评估实施前，应做以下准备：

a） 获得支持和配合；

b） 确定风险评估的目标；

c） 确定风险评估的内容；

d） 组建风险评估团队；

e） 对被评估对象进行调研；

f） 确定评估依据和方法。

#### 5.1.1 获得支持和配合

自评估应该获得本单位负责相关工作的管理者的认可，明确风险评估工作中相关的管理和技术人员的任务。对于检查评估，被评估的网络和业务运营商有支持和配合的责任和义务，以确保检查评估的顺利进行。

#### 5.1.2 确定目标

风险评估的准备阶段应明确风险评估的目标，为风险评估的过程提供导向。

电信网和互联网及相关系统风险评估的目标是，通过识别电信网和互联网及相关系统的技术和管理上的脆弱性、面临的威胁以及可能造成的风险大小，认清客观风险并有重点、有针对地提出和落实相适应的安全保护措施，从而减少安全事件的发生，满足组织业务持续发展在安全方面的需要，维持并提高组织的竞争优势、获利能力和企业形象，满足国家、行业对电信网和互联网及相关系统的要求。

#### 5.1.3 确定内容

基于风险评估目标确定风险评估内容是完成风险评估的前提。电信网和互联网及相关系统安全风险评估内容可以是整个电信网和互联网及相关系统中全部资产、管理机构，也可以是电信网和互联网及相关系统中的某个部分的独立资产、相关的部门等。风险评估的内容包括管理安全的风险和技术安全的风险。管理安全的风险评估内容包括安全管理机构、安全管理制度、人员安全管理、系统建设管理、系统运维管理等，技术安全的风险评估内容包括业务/应用安全、网络安全、设备安全、物理环境安全等内容。

#### 5.1.4 组建团队

应组建适当的风险评估管理与实施团队，以支持整个风险评估过程的推进。自评估可由网络和业务运营商内部开发、维护和管理的相关业务骨干、技术人员和管理人员组成风险评估团队。检查评估可由主管机构、评估机构组成风险评估团队。评估团队应能够保证风险评估工作的有效开展。

#### 5.1.5 评估对象调研

风险评估团队应对电信网和互联网及相关系统中的评估对象进行充分的调研。调研内容应包括网络结构与网络环境，主要的硬件、软件及其包含的数据和信息，管理、维护和使用的人员等。重点调研评估对象的资产价值、存在的脆弱性以及面临的威胁，从而为风险评估的依据和方法的选择，评估的实施奠定基础。

评估对象调研可以采取问卷调查、现场面谈相结合的方式进行。调查问卷是提供一套关于管理或操作控制的问题表格，供技术或管理人员填写；现场面谈则是由评估人员到现场观察并收集被评估方在物理环境和操作等方面的信息。

#### 5.1.6 确定依据和方法

应根据被评估对象的调研结果，确定风险评估的评估依据和评估方法。评估依据包括通信行业安全防护的标准、其他相关的通信行业标准和技术规范等。应综合考虑对电信网和互联网及相关系统进行风险评估的目的、范围、时间、效果、人员素质等因素来选择具体的评估方法，包括访谈、检查和测试等，使之能够与组织环境和安全要求相适应。

### 5.2 资产识别

#### 5.2.1 资产分类

电信网和互联网及相关系统资产是具有价值的资源，是安全策略保护的对象。它能够以多种形式存

在，有无形的、有形的，有硬件、软件，有文档、代码，也有服务、形象等。电信网和互联网及相关系统的风险评估中，首先需要将电信网和互联网及相关系统资产进行恰当的分类，以此为基础进行下一步的风险评估。在实际工作中，具体的资产分类方法可以根据具体的评估对象和要求，由评估者来灵活把握。根据资产的表现形式，可将资产分为数据、软件、硬件、文档、服务、人员等类型。表 1 列出了一种资产分类方法。

表 1　一种基于表现形式的资产分类方法

| 分　类 | 示　例 |
|---|---|
| 数据 | 保存在设备上的各种数据资料，包括源代码、数据库数据、系统文档、运行管理规程、计划、报告、用户手册等 |
| 软件 | 系统软件：操作系统、协议包、工具软件、各种数据库软件等；<br>应用软件：外部购买的应用软件，外包开发的应用软件，各种共享、自行或合作开发的各种软件等 |
| 硬件 | 网络设备：路由器、网关、交换机等；<br>计算机设备：大型机、小型机、服务器、工作站、台式计算机、移动计算机等；<br>存储设备：磁带机、磁盘阵列等；<br>传输线路：光纤、双绞线等；<br>保障设备：动力保障设备（如 UPS、变电设备等）、消防设施等 |
| 服务 | 网络服务：各种网络设备、设施提供的网络连接服务等；<br>业务提供服务：依赖电信网和互联网及相关系统开展的各类业务等 |
| 文档 | 纸质的各种文件，如设计文档、管理规定和技术要求等 |
| 人员 | 掌握重要技术的人员，如网络维护人员、网络或业务的研发人员等 |
| 其他 | 企业形象，客户关系等 |

电信网和互联网及相关系统中具体网络的资产可参见具体网络的安全防护要求。

### 5.2.2　资产赋值

资产的赋值过程体现出资产的安全状况对于组织的重要性。资产赋值可综合考虑资产的社会影响力、业务价值和可用性三个安全属性，并在此基础上得出一个综合的结果。为确保资产赋值时的一致性和准确性，组织应建立一个资产价值评价尺度，以指导资产赋值。

#### 5.2.2.1　社会影响力

根据资产在社会影响力上的不同，将其分为 5 个不同的等级，表示资产在被破坏后对社会的影响。表 2 提供了一种资产社会影响力赋值的参考。

表 2　资产社会影响力赋值表

| 赋　值 | 标　识 | 定　义 |
|---|---|---|
| 5 | 很高 | 资产的社会影响力价值非常高，资产被破坏会对社会造成灾难性的损害和致命性的潜在影响 |
| 4 | 高 | 资产的社会影响力价值较高，资产被破坏会对社会造成严重损害 |
| 3 | 中等 | 资产的社会影响力价值中等，资产被破坏会对社会造成一定损害 |
| 2 | 低 | 资产的社会影响力价值较低，资产被破坏会对社会造成轻微损害，但影响较小 |
| 1 | 很低 | 资产的社会影响力价值非常低，资产被破坏对社会造成的危害可以忽略 |

#### 5.2.2.2　业务价值

根据资产所提供业务的价值的不同，将其分为 5 个不同的等级，分别对应资产在业务价值缺失时对整个组织的影响。表 3 提供了一种业务价值赋值的参考。

表3 资产业务价值赋值表

| 赋 值 | 标 识 | 定 义 |
|---|---|---|
| 5 | 很高 | 资产所提供业务的价值非常关键，资产被破坏，导致业务无法正常运行，会对组织造成严重的或无法接受的影响 |
| 4 | 高 | 资产所提供业务的价值较高，资产被破坏，导致业务无法正常运行，会对组织造成重大影响 |
| 3 | 中等 | 资产所提供业务的价值中等，资产被破坏，导致业务无法正常运行，会对组织造成明显的影响 |
| 2 | 低 | 资产所提供业务的价值较低，资产被破坏，导致业务无法正常运行，会对组织造成轻微影响 |
| 1 | 很低 | 资产所提供业务的价值非常低，资产被破坏，导致业务无法正常运行，对组织造成的影响可以忽略 |

#### 5.2.2.3 可用性

根据资产在可用性上的不同要求，将其分为 5 个不同的等级，分别对应资产在可用性上的满足的不同程度。表 4 提供了一种可用性赋值的参考。

表4 资产可用性赋值表

| 赋 值 | 标 识 | 定 义 |
|---|---|---|
| 5 | 很高 | 可用性价值非常关键，可用性应在正常工作时间达到年度 99.999%以上 |
| 4 | 高 | 可用性价值较高，可用性应在正常工作时间达到年度 99.99%以上 |
| 3 | 中等 | 可用性价值中等，可用性应在正常工作时间达到年度 99.9%以上 |
| 2 | 低 | 可用性价值较低，可用性应在正常工作时间达到年度 99%以上 |
| 1 | 很低 | 可用性价值非常低，可用性在正常工作时间低于年度 99% |

#### 5.2.2.4 资产价值

资产价值应依据资产在社会影响力、业务价值和可用性上的赋值等级，经过综合评定得出。综合评定方法可以根据组织自身的特点，选择对资产社会影响力、业务价值和可用性最为重要的一个属性的赋值等级作为资产价值的最终赋值结果，也可以根据资产社会影响力、业务价值和可用性的不同重要程度对其赋值进行加权计算而得到资产价值的最终赋值。

附录A中列举的几种资产价值计算方法可做参考。评估者可根据实际情况灵活选择合适的计算方法，也可以采用其他计算方法。

根据最终得到的资产价值将资产划分为 5 级，级别越高表示资产越重要。表 5 中提供了一种资产价值等级划分参考。评估者可根据资产赋值结果，确定重要资产的范围，并主要围绕重要资产进行下一步的风险评估。

表5 资产价值等级及含义描述

| 等 级 | 标 识 | 定 义 |
|---|---|---|
| 5 | 很高 | 非常重要，其安全属性被破坏后可能对组织造成非常严重的损失 |
| 4 | 高 | 重要，其安全属性被破坏后可能对组织造成比较严重的损失 |
| 3 | 中等 | 比较重要，其安全属性被破坏后可能对组织造成中等程度的损失 |
| 2 | 低 | 不太重要，其安全属性被破坏后可能对组织造成较低的损失 |
| 1 | 很低 | 不重要，其安全属性被破坏后对组织造成非常低的损失，甚至忽略不计 |

### 5.3 威胁识别

#### 5.3.1 威胁分类

威胁是一种对资产构成潜在破坏的可能性因素，是客观存在的。威胁可以通过威胁主体、动机、途径等多种属性来描述。造成威胁的因素包括技术因素、环境因素和人为因素等。环境因素包括自然界不

可抗的因素和其他物理因素。根据威胁的动机，人为因素又可分为恶意和非恶意两种。威胁作用形式可以是对电信网和互联网及相关系统直接或间接的攻击。在社会影响力、业务价值和可用性等方面造成损害，也可能是偶发的或蓄意的事件。

在对威胁进行分类前，首先要考虑威胁的来源。表 6 提供了一种根据威胁来源的威胁分类方法。

**表 6　威胁来源列表**

| 来　源 | | 描　述 |
|---|---|---|
| 技术因素 | | 由于设备自身的软硬件故障、系统本身设计缺陷或软件缺陷等 |
| 环境因素 | | 断电、静电、灰尘、潮湿、温度、鼠蚁虫害、电磁干扰、洪灾、火灾、地震等环境条件和自然灾害，意外事故或软件、硬件、数据、通信线路方面的故障 |
| 人为因素 | 恶意人员 | 不满的或有预谋的内部人员对电信网和互联网及相关系统进行恶意破坏；采用自主或内外勾结的方式盗窃机密信息或进行篡改，获取利益；外部人员利用电信网和互联网及相关系统的脆弱性，对网络或系统进行破坏，以获取利益或炫耀能力 |
| | 非恶意人员 | 内部人员由于缺乏责任心或者由于不关心和不专注，或者没有遵循规章制度和操作流程而导致故障或信息损坏；内部人员由于缺乏培训，专业技能不足，不具备岗位技能要求而导致电信网和互联网及相关系统故障或被攻击 |

对威胁进行分类的方式有多种多样，表 7 提供了一种基于表现形式的威胁分类方法。

**表 7　一种基于表现形式的威胁分类表**

| 种　类 | 描　述 |
|---|---|
| 软硬件故障 | 由于设备硬件故障、通信链路中断、系统本身设计或软件缺陷导致对业务高效稳定运行的影响 |
| 物理环境威胁 | 断电、静电、灰尘、潮湿、温度、鼠蚁虫害、电磁干扰、洪灾、火灾、地震等环境问题和自然灾害 |
| 无作为或操作失误 | 由于应该执行而没有执行相应的操作或无意地执行了错误的操作，对电信网和互联网及相关系统造成影响 |
| 管理不到位 | 安全管理无法落实、不到位，造成安全管理不规范或者管理混乱，从而破坏电信网和互联网及相关系统正常有序运行 |
| 恶意代码和病毒 | 具有自我复制、自我传播能力，对电信网和互联网及相关系统构成破坏的程序代码 |
| 越权或滥用 | 通过采用一些措施，超越自己的权限访问了本来无权访问的资源，或者滥用职权，做出破坏电信网和互联网及相关系统的行为 |
| 黑客攻击技术 | 利用黑客工具和技术，例如侦察、密码猜测攻击、缓冲区溢出攻击、安装后门、嗅探、伪造和欺骗、拒绝服务攻击等手段对电信网和互联网及相关系统进行攻击和入侵 |
| 物理攻击 | 物理接触、物理破坏、盗窃 |
| 泄密 | 机密信息泄漏给他人 |
| 篡改 | 非法修改信息 |
| 抵赖 | 不承认收到的信息和所做的操作或交易 |

### 5.3.2　威胁赋值

判断威胁出现的频率是威胁识别的重要工作。威胁频率等级划分为 5 级，分别代表威胁出现的频率的高低，等级数值越大，威胁出现的频率越高，对资产的影响越大。表 8 提供了威胁出现频率的一种赋值方法。

表 8 威胁出现频率的赋值

| 等 级 | 标 识 | 定 义 |
|---|---|---|
| 5 | 很高 | 威胁出现的频率很高，在大多数情况下几乎不可避免或者可以证实经常发生过 |
| 4 | 高 | 威胁出现的频率较高，在大多数情况下很有可能会发生或者可以证实多次发生过 |
| 3 | 中等 | 威胁出现的频率中等，在某种情况下可能会发生或被证实曾经发生过 |
| 2 | 低 | 威胁出现的频率较低，一般不太可能发生，也没有被证实发生过 |
| 1 | 很低 | 威胁几乎不可能发生，仅可能在非常罕见和例外的情况下发生 |

威胁出现的频率非常难以度量，评估者应根据经验和（或）有关的统计数据来进行判断。在风险评估过程中，需要综合考虑以下三个方面，以得出在某种评估环境中各种威胁出现的频率：

a） 以往安全事件报告中出现过的威胁及其发生频率的统计；

b） 实际环境中通过检测工具以及各种日志发现的威胁及其发生频率的统计；

c） 近一两年来国际组织发布的对于通信行业的威胁及其发生频率统计以及发布的威胁预警。

针对电信网和互联网及相关系统中具体网络的威胁可参见具体网络的安全防护要求。

### 5.4 脆弱性识别

#### 5.4.1 脆弱性识别内容

脆弱性是对一个或多个资产弱点的总称。脆弱性识别也称为弱点识别，脆弱性是资产本身存在的，威胁总是要利用资产的脆弱性才可能造成危害。如果没有相应的威胁发生，单纯的脆弱性本身不会对资产造成损害，而且如果系统足够强健，再严重的威胁也不会导致安全事件的发生并造成损失。资产的脆弱性具有隐蔽性，有些脆弱性只有在一定条件和环境下才能显现，这是脆弱性识别中最为困难的部分。不正确的、起不到应有作用的或没有正确实施的安全措施本身就可能是一个脆弱性。

脆弱性识别所采用的方法主要有：问卷调查、工具检测、人工核查、文档查阅、渗透性测试等。需要注意的是，在识别已经运行的电信网和互联网及相关系统资产脆弱性时，应尽量避免影响电信网和互联网及相关系统的正常运行，尽可能在等同条件的实验环境中完成。

脆弱性识别以资产为核心，针对每个资产分别识别其可能被威胁利用的脆弱性，并对脆弱性的严重程度进行评估。也可以从物理环境、设备和系统、网络、业务/应用等层次进行识别，然后与资产、威胁结合起来。脆弱性识别时的数据应来自于资产的所有者、使用者以及电信网和互联网及相关系统业务领域的专家和软硬件方面的专业等人员等。

脆弱性识别主要从技术和管理两个方面进行，技术脆弱性涉及物理环境层、设备和系统层、网络层、业务/应用层等各个层面的安全问题；管理脆弱性又可分为技术管理脆弱性和组织管理脆弱性两方面，前者与具体技术活动相关，后者与管理环境相关。

对不同的识别对象，其脆弱性识别的具体要求应参照相应的技术或管理标准实施。例如，对物理环境的脆弱性识别可以参照 GB/T 9361-2000、YD/T 5026-2005、YD 5098-2005、YD 5002-94、YD/T 754-95 等标准中的技术指标实施；对设备、网络等的脆弱性识别可以参照 YDN 126-2005、YDN 127-2005 等标准中的技术指标实施；对管理脆弱性的识别可以参照 GB/T 19716-2005、ISO/IEC 17799-2005 和 ISO/IEC 13335.1-2004 等标准中的要求对安全管理制度及其执行情况进行检查，以发现管理漏洞和不足。

表 9 提供了一种脆弱性识别内容的参考。

表 9 脆弱性识别内容

| 类 型 | 识别对象 | 识别内容 |
|---|---|---|
| 技术脆弱性 | 物理环境 | 从机房场地、机房防火、机房供配电、机房防静电、机房接地与防雷、电磁防护、通信线路的保护、机房区域防护、机房设备管理等方面进行识别 |
| | 设备（含操作系统） | 从物理保护、用户账号、口令策略、资源共享、访问控制、新系统配置（初始化）等方面进行识别 |
| | 网络 | 从网络结构设计、边界保护、外部访问控制策略、内部访问控制策略、网络安全配置等方面进行识别 |
| | 数据库 | 从补丁安装、鉴别机制、口令机制、访问控制、网络和服务设置、备份及恢复机制等方面进行识别 |
| | 业务/应用 | 从访问控制策略、业务连续性、通信、鉴别机制、密码保护等方面进行识别 |
| 管理脆弱性 | 技术管理 | 从物理和环境安全、通信与操作管理、访问控制、系统开发与维护、业务连续性等方面进行识别 |
| | 组织管理 | 从安全策略、组织安全、资产分类与控制、人员安全等方面进行识别 |

### 5.4.2 脆弱性赋值

可以根据对资产损害程度、技术实现的难易程度、脆弱性流行程度，采用等级方式对已识别的脆弱性的严重程度进行赋值。由于很多脆弱性反映的是同一方面的问题，或可能造成相似的后果，赋值时应综合考虑这些脆弱性，最终确定某一方面的脆弱性的严重程度。

对某个资产，其技术脆弱性的严重程度还受到该资产所属电信网和互联网及相关系统的管理脆弱性的影响，因此，资产的脆弱性赋值还应参考技术管理和组织管理脆弱性的严重程度。

脆弱性严重程度可以进行等级化处理，不同的等级分别代表资产脆弱性严重程度的高低。等级数值越大，脆弱性严重程度越高。表 10 提供了脆弱性严重程度的一种赋值方法。

表 10 脆弱性严重程度赋值

| 等 级 | 标 识 | 定 义 |
|---|---|---|
| 5 | 很高 | 如果被威胁利用，将对资产造成完全损害 |
| 4 | 高 | 如果被威胁利用，将对资产造成重大损害 |
| 3 | 中等 | 如果被威胁利用，将对资产造成一般损害 |
| 2 | 低 | 如果被威胁利用，将对资产造成较小损害 |
| 1 | 很低 | 如果被威胁利用，对资产造成的损害可以忽略 |

针对电信网和互联网及相关系统中具体网络的脆弱性可参见具体网络的安全防护要求。

## 5.5 威胁利用脆弱性的关联关系

表 11 从环境因素类的威胁、人为因素类的威胁出发，列举出部分威胁与可利用的脆弱性的关联关系。这种关联关系因具体的网络状态和环境而不同，可根据具体的专业、地域、网络状态及环境的不同进一步制定具体的威胁利用脆弱性的关联关系。

表 11　威胁利用脆弱性的关联关系举例

| 威　胁 | 威胁子类 | | 威胁可利用的脆弱性 |
|---|---|---|---|
| 环境威胁 | 物理环境 | 静电、电磁干扰、灰尘、潮湿、湿度等不达标 | 防静电、防电磁干扰、场地环境措施 |
| | | | 机房故障应急机制有效性 |
| | | 电源/断电威胁 | 市电引入、油机、蓄电池 |
| | | | 电源类应急机制的有效性 |
| | 自然灾害 | 鼠蚁虫害 | 防鼠蚁虫害措施 |
| | | | 应急机制有效性 |
| | | 洪灾、水灾、泥石流、山体滑坡等 | 抗洪防汛措施 |
| | | | 洪水灾害应急机制有效性 |
| | | 台风、雷电 | 防台风、雷电措施 |
| | | | 台风、雷电灾害应急机制有效性 |
| 人为威胁 | 非恶意 | 无作为、误操作威胁 | 核心盘有无保护 |
| | | | 备品备件配置是否充足 |
| | | | 设备老化问题 |
| | | | 网管服务器及数据的备份 |
| | | | 厂家支持力度 |
| | | | 人员素质及管理 |
| | | | 故障应急机制有效性 |
| | | 外力施工 | 光缆铺设合理性 |
| | | | 承载系统保护机制 |
| | | | 光纤老化问题 |
| | | | 法律法规宣传 |
| | | | 巡纤周期密度是否足够 |
| | | | 故障应急机制有效性 |
| | 恶意 | 恶意代码和病毒 | 防恶意代码及病毒措施 |
| | | | 网络及系统漏洞 |
| | | 网络攻击 | 防网络攻击措施 |
| | | | 针对网络攻击的网络脆弱性 |
| | | 泄密、篡改、抵赖 | 防泄密、篡改、抵赖措施 |
| | | | 保密管理的脆弱性 |

### 5.6　已有安全措施的确认

组织应对已采取的安全措施的有效性进行确认，对于有效的安全措施继续保持，以避免不必要的工作和费用，防止安全措施的重复实施。对于确认为不适当的安全措施应核实是否应被取消，或者用更合适的安全措施替代。

安全措施可以分为预防性安全措施和保护性安全措施两种，预防性安全措施可以降低威胁利用脆弱性导致安全事件发生的可能性，如入侵检测系统；保护性安全措施可以减少因安全事件发生对资产造成的影响，如业务持续性计划。

已有安全措施的确认与脆弱性识别存在一定的联系。一般来说，安全措施的使用将减少脆弱性，但

安全措施的确认并不需要与脆弱性识别过程那样具体到每个资产的脆弱性，而是一类具体措施的集合。比较明显的例子是防火墙的访问控制策略，不必要描述具体的端口控制策略、用户控制策略，只需要表明采用的访问控制措施。

### 5.7 风险分析

#### 5.7.1 风险计算原理

在完成了资产识别、威胁识别、脆弱性识别后，将采用适当的方法确定威胁利用脆弱性导致安全事件发生的可能性，综合资产价值及脆弱性的严重程度判断安全事件一旦发生造成的损失，最终得到风险值。

风险计算原理如图 3 所示。

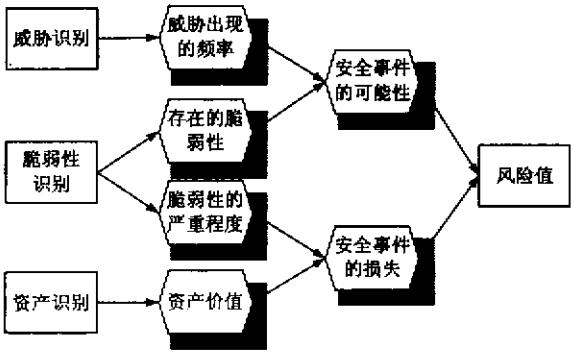


图 3 风险计算原理示意

对风险计算原理可以采用下面的范式形式化加以说明：

风险值 $=R\ (A,\ T,\ V)=R\ (L\ (Ta,\ Vb),\ F\ (Ia,\ Va))$

其中，$R$ 表示安全风险计算函数，$A$ 表示资产，$T$ 表示威胁，$V$ 表示脆弱性，$Ta$ 表示威胁出现的频率，$Ia$ 表示安全事件所作用的资产价值，$Va$ 表示脆弱性严重程度，$Vb$ 表示存在的脆弱性，$L$ 表示威胁利用资产存在的脆弱性导致安全事件发生的可能性，$F$ 表示安全事件发生后产生的损失。有以下三个关键计算环节。

a）计算安全事件发生的可能性

根据威胁出现频率及脆弱性状况，计算威胁利用脆弱性导致安全事件发生的可能性，即：

安全事件发生的可能性 $=L$（威胁出现频率，脆弱性）$=L\ (Ta,\ Vb)$

在具体评估中，应综合攻击者技术能力（如专业技术程度、攻击设备等）、脆弱性被利用的难易程度（如可访问时间、设计和操作知识公开程度等）、资产吸引力等因素来判断安全事件发生的可能性。

b）计算安全事件的损失

根据资产价值及脆弱性严重程度，计算安全事件一旦发生造成的损失，即：

安全事件的损失 $=F$（资产价值，脆弱性严重程度）$=F\ (Ia,\ Va)$

部分安全事件发生造成的损失不仅仅是针对该资产本身，还可能影响其提供业务的连续性。不同安全事件对组织造成的影响也是不一样的，在计算某个安全事件的损失时，应将对组织的影响也考虑在内。

c）计算风险值

根据计算出的安全事件发生的可能性以及安全事件的损失，计算风险值，即：

风险值 $=$R（安全事件发生的可能性，安全事件的损失）$=R[L\ (Ta,\ Vb),\ F\ (Ia,\ Va)]$

附录B中列举的几种风险计算方法可做参考。评估者可根据具体情况选择合适的风险计算方法，也可以采用其他计算方法。

### 5.7.2 风险结果判定

为实现对风险的控制与管理，对风险值进行等级化处理，将风险划分为一定的级别，本标准将风险等级划分为5级，每个等级代表了相应风险的严重程度，等级越高，风险越高。

表12提供了一种风险等级划分方法。

**表 12 风险等级划分方法**

| 等 级 | 标 识 | 描 述 |
|---|---|---|
| 5 | 很高 | 一旦发生将使电信网和互联网及相关系统遭受非常严重破坏，组织利益受到非常严重损失，如严重破坏组织信誉、严重影响组织业务的正常运行、经济损失重大、社会影响恶劣等 |
| 4 | 高 | 如果发生将使电信网和互联网及相关系统遭受比较严重的破坏，组织利益受到很严重损失 |
| 3 | 中等 | 发生后将使电信网和互联网及相关系统受到一定的破坏，组织利益受到中等程度的损失 |
| 2 | 低 | 发生后将使电信网和互联网及相关系统受到的破坏程度和利益损失一般 |
| 1 | 很低 | 即使发生只会使电信网和互联网及相关系统受到较小的破坏 |

在得到资产的风险值之后，需要结合资产已经采取的安全措施判断其风险是否在可以接受的范围内，如果风险结果在可接受的范围内，则该风险是可接受的风险，应保持已有的安全措施；如果风险结果在可接受的范围外，是不可接受的风险，需要制定风险处理计划并采取新的安全措施降低、控制风险。

应综合考虑风险控制成本与风险造成的影响，并结合资产所在网络或系统的安全等级，提出一个可接受的风险阈值。

### 5.7.3 风险处理计划

对于不可接受的风险，应根据导致该风险的脆弱性和威胁制定风险处理计划。风险处理计划中明确应采取的弥补其脆弱性、降低安全事件造成的损失或减少安全事件发生可能性的新的安全措施、预期效果、实施条件、进度安排、责任部门等。安全措施的选择应充分考虑到组织、资金、环境、人员、时间、法律、技术和社会文化等多方面的可能限制因素，从管理与技术两个方面考虑，管理措施可以作为技术措施的补充。安全措施的选择与实施应参照国家和行业的相关标准。

在对不可接受风险选择新的安全措施后，为确保安全措施的有效性，应进行再评估，以判断实施新的安全措施后的残余风险是否已经降低到可接受的水平。残余风险的评估可以依据本标准的风险评估流程实施，也可做适当裁减。

某些风险可能在选择了新的安全措施后，残余风险的风险评估结果仍处于不可接受范围内，应考虑是否接受此风险或进一步增加相应的安全措施。

## 5.8 风险评估文件

### 5.8.1 风险评估文件记录的要求

在对电信网和互联网及相关系统进行风险分析过程中，应记录风险评估过程，作为评估文档保存下来。应该符合（但不仅限于）以下要求：

a） 确保文件发布前是得到批准的；

b） 确保文件的更改和现行修订状态是可识别的；

c） 确保文件的分发得到适当的控制，并确保在使用时可获得有关版本的适用文件；

d） 防止作废文件的非预期使用，若因任何目的需保留作废文件时，应对这些文件进行适当的标识。

对于风险评估过程中形成的相关文件，还应规定其标识、储存、保护、检索、保存期限以及处置所需的控制。

### 5.8.2 风险评估文件

风险评估文件包括在整个风险评估过程中产生的评估过程文档和评估结果文档，风险评估文件包括（但不仅限于）以下几项：

a） 风险评估方案：阐述风险评估的目标、范围、人员、评估方法、评估结果的形式和实施进度等；

b） 风险评估程序：明确风险评估的目的、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；

c） 资产识别清单：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；

d） 重要资产清单：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；

e） 威胁列表：根据威胁识别和赋值的结果，形成威胁列表，包括威胁名称、种类、来源、动机及出现的频率等；

f） 脆弱性列表：根据脆弱性识别和赋值的结果，形成脆弱性列表，包括具体脆弱性的名称、描述、类型及严重程度等；

g） 已有安全措施确认表：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，包括已有安全措施名称、类型、功能描述及实施效果等；

h） 风险评估报告：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） 风险处理计划：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） 风险评估记录：要求风险评估过程中的各种现场记录可复现评估过程，并作为产生歧义后解决问题的依据。

相关文件是否需要以及详略程度可参见具体网络的安全防护检测要求。

## 6 风险评估在电信网和互联网及相关系统生命周期中的不同要求

### 6.1 电信网和互联网及相关系统生命周期概述

风险评估应贯穿于电信网和互联网及相关系统生命周期的各阶段中，电信网和互联网及相关系统生命周期各阶段中涉及的风险评估的原则和方法是一致的，但由于各阶段实施的内容、对象、安全需求不同，使得风险评估的对象、目的、安全要求等各方面也有所不同，每个阶段风险评估的具体实施应根据该阶段的特点有所侧重地进行。

电信网和互联网及相关系统生命周期包含启动、设计、实施、运维和废弃等 5 个阶段。图 4 列出了生命周期各阶段中的主要安全活动。

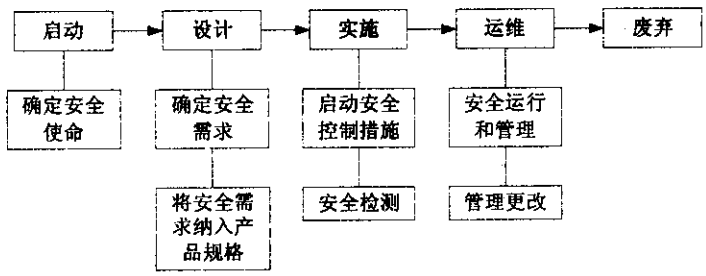


**图 4　电信网和互联网及相关系统生命周期各阶段的主要安全活动**

### 6.2　启动阶段的风险评估

启动阶段风险评估的目的是确定电信网和互联网及相关系统的安全使命，用以支撑电信网和互联网及相关系统的安全需求。启动阶段的风险评估应能够描述电信网和互联网及相关系统建成后的作用，包括技术、管理等方面，并确定电信网和互联网及相关系统建设应达到的安全目标。

本阶段的风险评估着重以下几方面：

a）　整体规划中是否制定总体的安全方针；

b）　整体规划中是否描述电信网和互联网及相关系统的设备、数据、应用等资产的重要性和潜在的价值、可能的使用限制等；

c）　整体规划中是否考虑来自资产的应用对象、应用环境、业务状况、操作要求等方面的威胁；

d）　整体规划中是否描述电信网和互联网及相关系统安全相关的运行环境，包括物理和人员的安全配置以及明确相关的法规、组织安全政策、专门技术和知识等。

启动阶段的评估结果应体现在电信网和互联网及相关系统整体规划或项目建议书中。

### 6.3　设计阶段的风险评估

设计阶段的风险评估需要根据启动阶段所明确的运行环境、资产重要程度等，在建设方案中提出安全功能需求，并对安全功能符合性进行判断，作为采购过程风险控制的依据。

本阶段的评估对象是建设方案，应详细评估其中对威胁的描述、将使用的具体设备、软件等资产的列表以及这些资产的安全功能需求。

本阶段的评估包括以下内容：

a）　是否对电信网和互联网及相关系统建设后面临的物理和自然环境，内外部入侵等威胁进行了分析，制定电信网和互联网及相关系统建设的总体安全策略；

b）　是否采取了一定的手段应对电信网和互联网及相关系统可能的故障，是否考虑可能随着其他网络接入而产生的风险；

c）　是否根据开发的规模、时间及网络的特点选择开发方法，并根据设计开发计划及用户需求，对涉及的软件、硬件与网络进行分析和选型；

d）　对设计或者原型中的技术实现以及人员、组织管理等各方面的脆弱性进行评估，包括设计过程中的管理脆弱性和技术平台固有的脆弱性；

e）　设计活动中所采用的安全控制措施、安全技术保障手段对风险结果的影响，在安全需求变更和设计变更后，也需要重复这项评估。

设计阶段的风险评估应判定建设方案所提供的安全功能与电信网和互联网及相关系统安全防护要求的符合性。评估结果最终应体现在电信网和互联网及相关系统的设计报告或建设实施方案中。

### 6.4 实施阶段的风险评估

实施阶段风险评估的目的是根据电信网和互联网及相关系统的安全需求和运行环境对电信网和互联网及相关系统的开发实施过程进行风险识别，并根据设计阶段分析的威胁和建立的安全控制措施，对电信网和互联网及相关系统实施及验收时进行安全检测和质量控制。

本阶段的评估对象是安全措施的实现程度，确定安全措施能否抵御现有威胁、脆弱性的影响。

实施阶段风险评估包括开发阶段、实施交付阶段两部分评估。

开发阶段的具体评估内容包括：

a） 评估通信行业风险评估相关标准对安全需求的影响；

b） 评估安全需求是否有效地支持电信网和互联网及相关系统的功能；

c） 评估电信网和互联网及相关系统的资产、威胁和脆弱性，分析成本与效益的关系，以确定在符合相关法律、政策、标准和功能需要下最合适的防范措施；

d） 评估开发阶段的安全活动，包括安全开发的内容、开发过程的监视、安全问题的防范、需求更改的响应以及监视外来的威胁。

实施交付阶段的具体评估内容包括：

a） 根据实际建成的电信网和互联网及相关系统，详细分析其面临的威胁；

b） 根据建设目标和安全需求，对电信网和互联网及相关系统的安全功能进行验收测试，评价安全功能能否抵御安全威胁；

c） 评估是否建立了与整体安全策略一致的组织管理制度；

d） 对实现的风险控制效果与预期设计的符合性进行判断，如存在较大的不符合，应重新进行安全策略的设计与调整。

本阶段风险评估可以采取对照建设实施方案和标准要求的方式对实际建设结果进行检测。

### 6.5 运维阶段的风险评估

运维阶段风险评估的目的是了解和控制运行过程中的电信网和互联网及相关系统的安全风险，是一种较为全面的风险评估。

本阶段的评估对象是真实运行的电信网和互联网及相关系统资产、威胁、脆弱性等各方面。

本阶段的具体评估内容包括。

a） 资产评估：对真实环境下较为细致的评估，包括实施阶段采购的软硬件资产、系统运行过程中的人员与服务等。本阶段资产识别是前期资产识别的补充与增加。

b） 威胁评估：真实环境中的威胁分析，应全面地评估威胁的可能性。对非故意威胁产生安全事件的评估可以参照事故发生率；对故意威胁主要由评估人员就威胁的各个影响因素做出专业判断，同时考虑已有控制措施。

c） 脆弱性评估：是全面的脆弱性评估，包括运行环境下物理、网络、系统、应用、安全保障设备、管理等方面的脆弱性。对于技术的脆弱性评估采取核查、扫描、案例验证、渗透性测试的方式验证脆弱性；对于管理脆弱性采取文档、记录核查进行验证。

d） 风险分析：根据本标准的相关方法，对主要资产的风险进行定性或定量的风险分析，描述不同资产的风险高低状况。

运维阶段的风险评估应定期执行，当组织的业务流程、系统状况发生重大变化时，也应进行风险评

估。重大变更包括（但不限于）以下变更：

a） 增加新的业务/应用或业务/应用发生较大变更；

b） 网络结构和连接状况发生较大变更；

c） 技术平台大规模的更新；

d） 系统扩容或改造后进行；

e） 发生重大安全事件后或基于某些运行记录怀疑将发生重大安全事件；

f） 组织结构发生重大变动对系统产生影响。

### 6.6 废弃阶段的风险评估

废弃阶段风险评估的目的是确保硬件和软件等资产及残留信息得到了适当的废弃处置，并确保电信网和互联网及相关系统的更新过程在一个安全的状态下完成。

本阶段应重点对废弃资产对组织的影响进行分析，并根据不同的影响制定不同的处理方式。对由于废弃可能带来的新的威胁进行分析，并改进新的技术或管理模式。对废弃资产的处理过程应在有效的监督之下实施，同时对废弃的执行人员进行安全教育。维护工作的技术人员和管理人员均应该参与此阶段的评估。

# 附 录 A
## （规范性附录）
## 资产价值的计算方法

本附录介绍了几种资产价值的计算方法，评估者可根据实际情况灵活选择相应的计算方法，也可以采用其他计算方法。

### A.1 对数法

通常，根据电信网和互联网及相关系统的实际经验，3 个安全属性中最高的一个对最终的资产价值影响最大。换而言之，整体安全属性的赋值并不随着 3 个属性值的增加而线性增加，较高的属性值具有较大的权重，因此可以使用下面的公式计算资产价值：

$$\text{Asset Value} = \text{Round1}\{\text{Log}_2[(\alpha\times 2^I+\beta\times 2^V+\gamma\times 2^A]\}$$

其中，$I$ 代表社会影响力赋值；$V$ 代表业务价值赋值；$A$ 代表可用性赋值；Round1{}表示四舍五入处理，保留 1 位小数；$\text{Log}_2$[]表示取以 2 为底的对数；$\alpha$、$\beta$ 和 $\gamma$ 分别表示社会影响力、业务价值和可用性所占的权重，网络和业务运营商可根据具体网络的情况确定 $\alpha$、$\beta$ 和 $\gamma$ 的取值，$\alpha\geq 0$，$\beta\geq 0$，$\gamma\geq 0$，且 $\alpha+\beta+\gamma=1$。

对计算所得的资产价值采用向上进位的方法确定资产价值的等级。

### A.2 矩阵法

矩阵法的特点是建立资产的社会影响力、业务价值和可用性的对应矩阵，并且预先根据一定的方法确定了资产价值。使用本方法需要首先确定资产的社会影响力、业务价值和可用性的赋值，再查矩阵获得资产价值。

例如，采用对数法提前确定矩阵中的资产价值，并设 $\alpha=\beta=\gamma=1/3$，则可得表 A.1 所示的资产价值判别矩阵。

表 A.1 资产价值判别矩阵

| 资产 | 业务价值 | 1 | | | | | 2 | | | | | 3 | | | | | 4 | | | | | 5 | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 价值 | 可用性 | 1 | 2 | 3 | 4 | 5 | 1 | 2 | 3 | 4 | 5 | 1 | 2 | 3 | 4 | 5 | 1 | 2 | 3 | 4 | 5 | 1 | 2 | 3 | 4 | 5 |
| 社 | 1 | 1 | 2 | 2 | 3 | 4 | 2 | 2 | 3 | 3 | 4 | 2 | 3 | 3 | 4 | 4 | 3 | 3 | 4 | 4 | 5 | 4 | 4 | 4 | 5 | 5 |
| 会 | 2 | 2 | 2 | 3 | 3 | 4 | 2 | 2 | 3 | 3 | 4 | 3 | 3 | 3 | 4 | 4 | 3 | 3 | 4 | 4 | 5 | 4 | 4 | 4 | 5 | 5 |
| 影 | 3 | 2 | 3 | 3 | 4 | 4 | 3 | 3 | 3 | 4 | 4 | 3 | 3 | 3 | 4 | 4 | 4 | 4 | 4 | 4 | 5 | 4 | 4 | 4 | 5 | 5 |
| 响 | 4 | 3 | 3 | 4 | 4 | 5 | 3 | 3 | 4 | 4 | 5 | 4 | 4 | 4 | 4 | 5 | 4 | 4 | 4 | 4 | 5 | 5 | 5 | 5 | 5 | 5 |
| 力 | 5 | 4 | 4 | 4 | 5 | 5 | 4 | 4 | 4 | 5 | 5 | 4 | 4 | 4 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 | 5 |

# 附 录 B
（规范性附录）
风险值的计算方法

本附录介绍了几种资产风险值的计算方法。评估者可以根据具体情况选择合适的风险值计算方法，也可以采用其他计算方法。当一个资产是由若干个子资产构成时，可以先分别计算各子资产的风险值，然后通过一定的计算方法（如相加法）计算总的风险值。

## B.1 相乘法

考虑到影响电信网和互联网及相关系统的资产风险值的因素有资产价值、威胁值以及脆弱性值等，这些因素与风险值都是正相关的，因此，可将这些因素值相乘得到资产对应某项脆弱性的风险值。计算公式如下：

风险值＝资产价值×威胁值×脆弱性值

根据影响风险值的各个因素的取值范围可以知道，采用相乘法计算风险值的取值范围为 1~125。为实现对风险的控制与管理，本标准对风险值进行等级化处理，将风险等级划分为 5 级，如表 12 所示，每个等级代表了相应风险的严重程度，等级越高，风险越高。表 B.1 提供了一种风险等级划分方法，根据表 B.1 可确定风险值对应的风险等级。

表 B.1 风险等级的判定

| 风险值 | 1~10 | 11~30 | 31~60 | 61~90 | 91~125 |
|---|---|---|---|---|---|
| 风险等级 | 1 | 2 | 3 | 4 | 5 |

## B.2 矩阵法

矩阵法的特点是建立资产价值等级、威胁等级和脆弱性等级的对应矩阵，并且预先根据一定的方法确定了风险等级。使用本方法对于每一资产的风险，都需要首先确定资产价值等级、威胁等级和脆弱性等级的赋值，再查矩阵获得风险等级。

例如，采用相乘法提前确定矩阵中的风险等级，则可得表 B.2 所示的资产风险判别矩阵。

表 B.2 资产风险判别矩阵

| 风险等级 | 威胁等级 | 1 | | | | | 2 | | | | | 3 | | | | | 4 | | | | | 5 | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 脆弱性等级 | 1 | 2 | 3 | 4 | 5 | 1 | 2 | 3 | 4 | 5 | 1 | 2 | 3 | 4 | 5 | 1 | 2 | 3 | 4 | 5 | 1 | 2 | 3 | 4 | 5 |
| 资产价值等级 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 2 | 2 | 1 | 1 | 2 | 2 | 2 | 1 | 1 | 2 | 2 | 2 |
| | 2 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 2 | 2 | 2 | 1 | 2 | 2 | 2 | 2 | 1 | 2 | 2 | 3 | 3 | 1 | 2 | 2 | 3 | 3 |
| | 3 | 1 | 1 | 1 | 2 | 2 | 1 | 2 | 2 | 2 | 2 | 1 | 2 | 2 | 3 | 3 | 2 | 2 | 3 | 3 | 3 | 2 | 2 | 3 | 3 | 4 |
| | 4 | 1 | 1 | 2 | 2 | 2 | 1 | 2 | 2 | 3 | 3 | 2 | 2 | 3 | 3 | 3 | 2 | 3 | 3 | 4 | 4 | 2 | 3 | 3 | 4 | 5 |
| | 5 | 1 | 1 | 2 | 2 | 2 | 1 | 2 | 2 | 3 | 3 | 2 | 2 | 3 | 3 | 4 | 2 | 3 | 3 | 4 | 5 | 2 | 3 | 4 | 5 | 5 |

# 参 考 文 献

1. GB/T 20984-2007　　信息安全技术 信息安全风险评估规范