ICS 35.040
L 80

中华人民共和国国家标准

GB/T 20984—2007

信息安全技术
信息安全风险评估规范

Information security technology—

Risk assessment specification for information security

2007-06-14 发布　　2007-11-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前言

（略）

引言

随着政府部门、金融机构、企事业单位、商业组织等对信息系统依赖程度的日益增强，信息安全问题受到普遍关注。运用风险评估去识别安全风险，解决信息安全问题得到了广泛的认识和应用。

信息安全分析评估就是从风险管理角度，运用科学的方法和手段，系统地分析信息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整改措施，为防范和化解信息安全风险，将风险控制在可接受的水平，最大限度地保障信息安全提供科学依据。

信息安全风险评估作为信息安全保障工作的基础性工作和重要环节，要贯穿于信息系统的规划、设计、实施、运行维护以及废弃各个阶段，是信息安全等级保护制度建设的重要科学方法之一。

本标准条款中所指的“风险评估”，其含义均为“信息安全风险评估”。

信息安全技术
信息安全风险评估指南

1 范围

本标准提出了风险评估的基本概念、要素关系、分析原理、实施流程和评估方法，以及风险评估在信息系统生命周期不同阶段的实施要点和工作形式。

本标准适用于规范组织开展的风险评估工作。

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。凡是注明日期的引用文件，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 9361 计算站场地安全要求

GB 17859-1999 计算机信息系统安全保护等级划分准则

GB/T 18336-2001 信息技术 安全技术 信息技术安全性评估准则（idt ISO/IEC 15408:1999）

GB/T 19716-2005 信息技术 信息安全管理实用规则(ISO/IEC 17799:2000,MOD)

3 术语和定义

下列术语和定义适用于本标准。

3.1

资产 asset

对组织具有价值的信息或资源，是安全策略保护的对象。

3.2

资产价值 asset value

资产的重要程度或敏感程度的表征。资产价值是资产的属性，也是进行资产识别的主要内容。

3.3

可用性 availability

数据或资源的特性，被授权实体按要求能访问和使用数据或资源。

3.4

业务战略 business strategy

组织为实现其发展目标而制定的一组规则或要求。

3.5

机密性 confidentiality

数据所具有的特性，即表示数据所达到的未提供或未泄露给非授权的个人、过程或其他实体的程度。

3.6

信息安全风险 information security risk

人为或自然的威胁利用信息系统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。

3.7

（信息安全）风险评估　（information security）risk assessment

依据有关信息安全技术与管理标准，对信息系统及由其处理、传输和存储的信息的保密性、完整性和可用性等安全属性进行评价的过程。它要评估资产面临的威胁以及威胁利用脆弱性导致安全事件的可能性，并结合安全事件所涉及的资产价值来判断安全事件一旦发生对组织造成的影响。

3.8

信息系统　information　system

由计算机及其相关的和配套的设备、设施(含网络)构成的，按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统。

典型的信息系统由三部分组成：硬件系统（计算机硬件系统和网络硬件系统）；系统软件（计算机系统软件和网络系统软件）；应用软件（包括由其处理、存储的信息）。

3.9

检查评估　inspection assessment

由被评估组织的上级主管机关或业务主管机关发起的，依据国家有关法规与标准，对信息系统及其管理进行的具有强制性的检查活动。

3.10

完整性 integrity

保证信息及信息系统不会被非授权更改或破坏的特性。包括数据完整性和系统完整性。

3.11

组织　organization

由作用不同的个体为实施共同的业务目标而建立的结构。一个单位是一个组织，某个业务部门也可以是一个组织。

3.12

残余风险　residual risk

采取了安全措施后，信息系统仍然可能存在的风险。

3.13

自评估　self-assessment

由组织自身发起，依据国家有关法规与标准，对信息系统及其管理进行的风险评估活动。

3.14

安全事件　security incident

指系统、服务或网络的一种可识别状态的发生，它可能是对信息安全策略的违反或防护措施的失效，或未预知的不安全状况。

3.15

安全措施　security measure

保护资产、抵御威胁、减少脆弱性、降低安全事件的影响，以及打击信息犯罪而实施的各种实践、规程和机制。

3.16

安全需求 security requirement

为保证组织业务战略的正常运作而在安全措施方面提出的要求。

3.17

威胁 threat

可能导致对系统或组织危害的不希望事故潜在起因。

3.18

脆弱性 vulnerability

可能被威胁所利用的资产或若干资产的薄弱环节。

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：

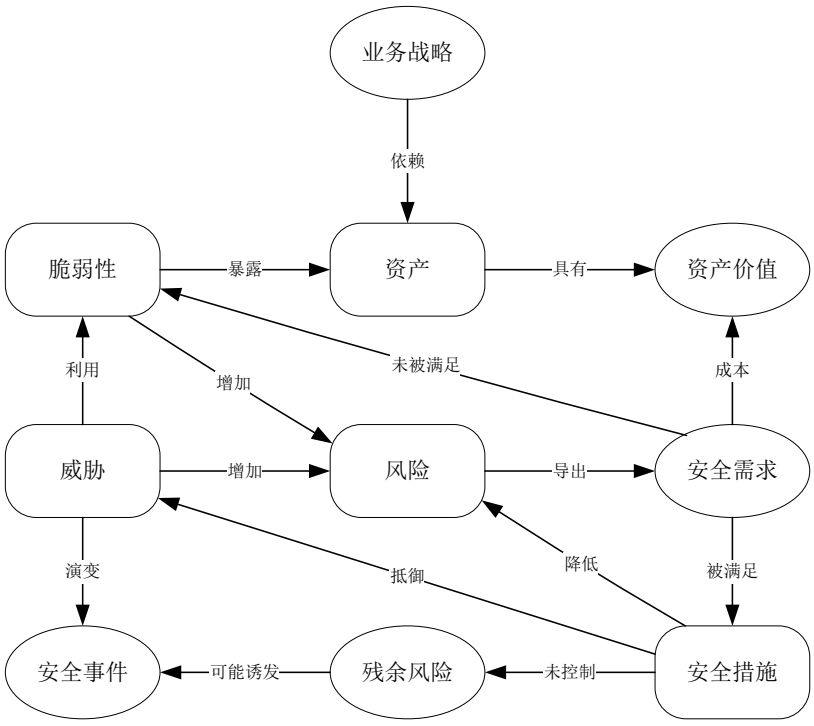

图 1 风险评估要素关系图

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。风险评估围绕着资产、威胁、脆弱性和安全措施这些基本要素展开，在对基本要素的评估过程中，需要充分考虑业务战略、资产价值、安全需求、安全事件、残余风险等与这些基本要素相关的各类属性。

图 1 中的风险要素及属性之间存在着以下关系：

a）业务战略的实现对资产具有依赖性，依赖程度越高，要求其风险越小；

b）资产是有价值的，组织的业务战略对资产的依赖程度越高，资产价值就越大；

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

d）资产的脆弱性可能暴露资产的价值，资产具有的弱点越多则风险越大；

e）脆弱性是未被满足的安全需求，威胁利用脆弱性危害资产；

f）风险的存在及对风险的认识导出安全需求；

g）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；

h）安全措施可抵御威胁，降低风险；

i）残余风险有些是安全措施不当或无效,需要加强才可控制的风险；而有些则是在综合考虑了安全成本与效益后不去控制的风险；

j）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。

4.2 风险分析原理

风险分析原理如图 2 所示：

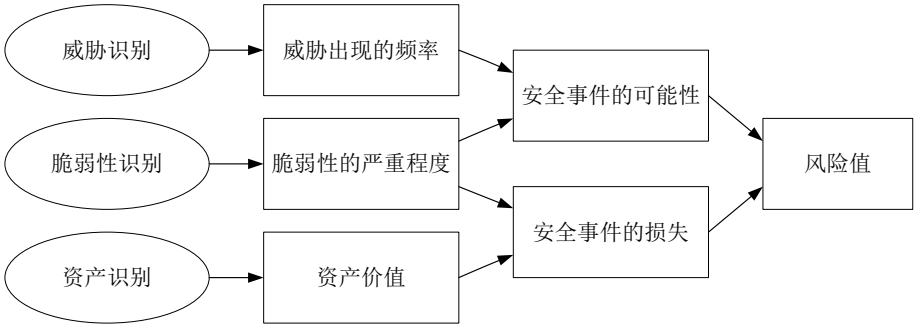

图 2 风险分析原理图

风险分析中要涉及资产、威胁、脆弱性三个基本要素。每个要素有各自的属性，资产的属性是资产价值；威胁的属性可以是威胁主体、影响对象、出现频率、动机等；脆弱性的属性是资产弱点的严重程度。风险分析的主要内容为：

a）对资产进行识别，并对资产的价值进行赋值；

b）对威胁进行识别，描述威胁的属性，并对威胁出现的频率赋值；

c）对脆弱性进行识别，并对具体资产的脆弱性的严重程度赋值；

d）根据威胁及威胁利用脆弱性的难易程度判断安全事件发生的可能性；

e）根据脆弱性的严重程度及安全事件所作用的资产的价值计算安全事件的损失；

f）根据安全事件发生的可能性以及安全事件出现后的损失,计算安全事件一旦发生对组织的影响，即风险值。

4.3 实施流程

风险评估的实施流程如图 3 所示：

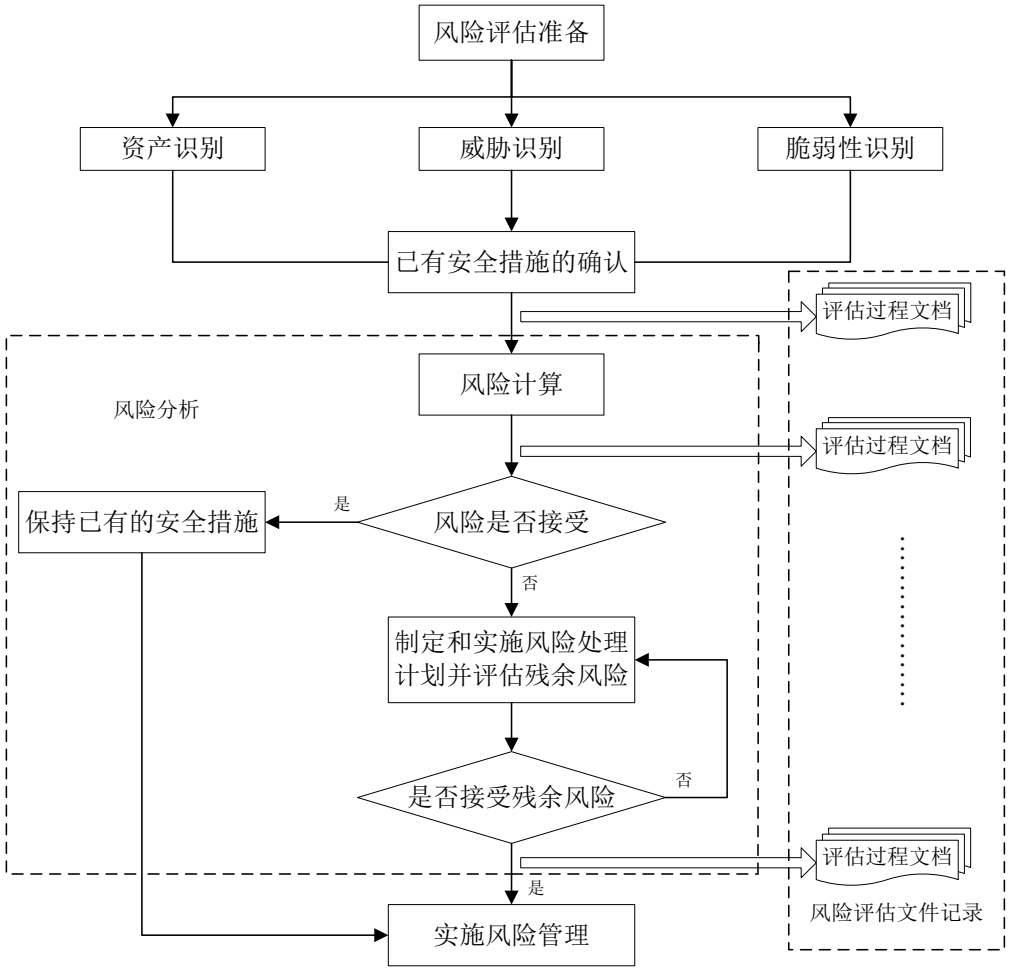

图 3　风险评估实施流程图

风险评估实施流程的详细说明见第5章。

5　风险评估实施

5.1　风险评估准备

5.1.1　概述

风险评估的准备是整个风险评估过程有效性的保证。组织实施风险评估是一种战略性的考虑，其结果将受到组织业务战略、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：

a）确定风险评估的目标；

b）确定风险评估的范围；

c）组建适当的评估管理与实施团队；

d）进行系统调研；

e）确定评估依据和方法；

f）获得最高管理者对风险评估工作的支持。

5.1.2　确定目标

根据满足组织业务持续发展在安全方面的需要、法律法规的规定等内容，识别现有信息系统及管理上的不足，以及可能造成的风险大小。

5.1.3 确定范围

风险评估范围可能是组织全部的信息及与信息处理相关的各类资产、管理机构，也可能是某个独立的信息系统、关键业务流程、与客户知识产权相关的系统或部门等。

5.1.4 组建团队

风险评估实施团队，由管理层、相关业务骨干、信息技术等人员组成的风险评估小组。必要时，可组建由评估方、被评估方领导和相关部门负责人参加的风险评估领导小组，聘请相关专业的技术专家和技术骨干组成专家小组。

评估实施团队应做好评估前的表格、文档、检测工具等各项准备工作，进行风险评估技术培训和保密教育，制定风险评估过程管理相关规定。可根据被评估方要求，双方签署保密合同，必要时签署个人保密协议。

5.1.5 系统调研

系统调研是确定被评估对象的过程，风险评估小组应进行充分的系统调研，为风险评估依据和方法的选择、评估内容的实施奠定基础。调研内容至少应包括：

a）业务战略及管理制度

b）主要的业务功能和要求

c）网络结构与网络环境，包括内部连接和外部连接；

d）系统边界；

e）主要的硬件、软件；

f）数据和信息；

g）系统和数据的敏感性；

h）支持和使用系统的人员；

i）其他。

系统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，供系统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系统在物理、环境和操作方面的信息。

5.1.6 确定依据

根据系统调研结果，确定评估依据和评估方法。评估依据包括（但不限于）：

a）现行国际标准、国家标准、行业标准；

b）行业主管机关的业务系统的要求和制度；

c）系统安全保护等级要求；

d）系统互联单位的安全要求；

e）系统本身的实时性或性能要求等。

根据评估依据，应考虑评估的目的、范围、时间、效果、人员素质等因素来选择具体的风险计算方法，并依据业务实施对系统安全运行的需求，确定相关的判断依据，使之能够与组织环境和安全要求相适应。

5.1.7 制定方案

风险评估方案的目的是为了后面的风险评估实施活动提供一个总体计划,用于指导实施方开展后续工作。风险评估方案的内容一般包括（但不仅限于）：

a）团队组织：包括评估团队成员、组织结构、角色、责任等内容；

b）工作计划：风险评估各阶段的工作计划，包括工作内容、工作形式、工作成果等内容；

c）时间进度安排：项目实施的时间进度安排。

5.1.8 获得支持

上述所有内容确定后，应形成较为完整的风险评估实施方案，得到组织最高管理者的支持、批准；对管理层和技术人员进行传达，在组织范围就风险评估相关内容进行培训，以明确有关人员在风险评估

中的任务。

5.2 资产识别

5.2.1 资产分类

机密性、完整性和可用性是评价资产的三个安全属性。风险评估中资产的价值不是以资产的经济价值来衡量，而是由资产在这三个安全属性上的达成程度或者其安全属性未达成时所造成的影响程度来决定的。安全属性达成程度的不同将使资产具有不同的价值，而资产面临的威胁、存在的脆弱性、以及已采用的安全措施都将对资产安全属性的达成程度产生影响。为此，有必要对组织中的资产进行识别。

在一个组织中，资产有多种表现形式；同样的两个资产也因属于不同的信息系统而重要性不同，而且对于提供多种业务的组织，其支持业务持续运行的系统数量可能更多。这时首先需要将信息系统及相关的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、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	保存在信息媒介上的各种数据资料，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、各类纸质的文档等
软件	系统软件：操作系统、数据库管理系统、语句包、开发系统等 应用软件：办公软件、数据库软件、各类工具软件等 源程序：各种共享源代码、自行或合作开发的各种代码等
硬件	网络设备：路由器、网关、交换机等 计算机设备：大型机、小型机、服务器、工作站、台式计算机、便携计算机等 存储设备：磁带机、磁盘阵列、磁带、光盘、软盘、移动硬盘等 传输线路：光纤、双绞线等 保障设备： UPS、变电设备等、空调、保险柜、文件柜、门禁、消防设施等 安全保障设备：防火墙、入侵检测系统、身份鉴别等 其他：打印机、复印机、扫描仪、传真机等
服务	信息服务：对外依赖该系统开展的各类服务 网络服务：各种网络设备、设施提供的网络连接服务 办公服务：为提高效率而开发的管理信息系统，包括各种内部配置管理、文件流转管理等服务
人员	掌握重要信息和核心业务的人员，如主机维护主管、网络维护主管及应用项目经理等
其它	企业形象、客户关系等

分类	示例
服务	信息服务：对外依赖该系统开展的各类服务 网络服务：各种网络设备、设施提供的网络连接服务 办公服务：为提高效率而开发的管理信息系统，包括各种内部配置管理、文件流转管理等服务
人员	掌握重要信息和核心业务的人员，如主机维护主管、网络维护主管及应用项目经理等
其它	企业形象、客户关系等

5.2.2 资产赋值

5.2.2.1 保密性赋值

根据资产在保密性上的不同要求，将其分为五个不同的等级，分别对应资产在保密性上应达成的不同程度或者保密性缺失时对整个组织的影响。表 2 提供了一种保密性赋值的参考。

表 2 资产保密性赋值表

赋值	标识	定义
5	很高	包含组织最重要的秘密，关系未来发展的前途命运，对组织根本利益有着决定性的影响，如果泄露会造成灾难性的损害
4	高	包含组织的重要秘密，其泄露会使组织的安全和利益遭受严重损害
3	中等	组织的一般性秘密，其泄露会使组织的安全和利益受到损害
2	低	仅能在组织内部或在组织某一部门内部公开的信息，向外扩散有可能对组织的利益造成轻微损害
1	很低	可对社会公开的信息，公用的信息处理设备和系统资源等

5.2.2.2 完整性赋值

根据资产在完整性上的不同要求，将其分为五个不同的等级，分别对应资产在完整性上缺失时对整个组织的影响。表 3 提供了一种完整性赋值的参考。

表 3 资产完整性赋值表

赋值	标识	定义
5	很高	完整性价值非常关键，未经授权的修改或破坏会对组织造成重大的或无法接受的影响，对业务冲击重大，并可能造成严重的业务中断，难以弥补
4	高	完整性价值较高，未经授权的修改或破坏会对组织造成重大影响，对业务冲击严重，较难弥补
3	中等	完整性价值中等，未经授权的修改或破坏会对组织造成影响，对业务冲击明显，但可以弥补
2	低	完整性价值较低，未经授权的修改或破坏会对组织造成轻微影响，对业务冲击轻微，容易弥补
1	很低	完整性价值非常低，未经授权的修改或破坏对组织造成的影响可以忽略，对业务冲击可以忽略

5.2.2.3 可用性赋值

根据资产在可用性上的不同要求，将其分为五个不同的等级，分别对应资产在可用性上应达成的不同程度。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	可用性价值非常高，合法使用者对信息及信息系统的可用度达到年度 99.9%以上，或系统不允许中断
4	高	可用性价值较高，合法使用者对信息及信息系统的可用度达到每天 90%以上，或系统允许中断时间小于 10 min
3	中等	可用性价值中等，合法使用者对信息及信息系统的可用度在正常工作时间达到 70%以上，或系统允许中断时间小于 30 min
2	低	可用性价值较低，合法使用者对信息及信息系统的可用度在正常工作时间达到 25%以上，或系统允许中断时间小于 60 min

1	很低	可用性价值可以忽略，合法使用者对信息及信息系统的可用度在正常工作时间低于 25%

5.2.2.4 资产重要性等级

资产价值应依据资产在机密性、完整性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自身的特点，选择对资产机密性、完整性和可用性最为重要的一个属性的赋值等级作为资产的最终赋值结果；也可以根据资产机密性、完整性和可用性的不同等级对其赋值进行加权计算得到资产的最终赋值结果。加权方法可根据组织的业务特点确定。

本标准中，为与上述安全属性的赋值相对应，根据最终赋值将资产划分为五级，级别越高表示资产越重要，也可以根据组织的实际情况确定资产识别中的赋值依据和等级。表 5 中的资产等级划分表明了不同等级的重要性的综合描述。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 资产等级及含义描述

等级	标识	描述
5	很高	非常重要，其安全属性破坏后可能对组织造成非常严重的损失
4	高	重要，其安全属性破坏后可能对组织造成比较严重的损失
3	中	比较重要，其安全属性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，其安全属性破坏后对组织造成导很小的损失，甚至忽略不计

5.3 威胁识别

5.3.1 威胁分类

威胁可以通过威胁主体、资源、动机、途径等多种属性来描述。造成威胁的因素可分为人为因素和环境因素。根据威胁的动机，人为因素又可分为恶意和非恶意两种。环境因素包括自然界不可抗的因素和其它物理因素。威胁作用形式可以是对信息系统直接或间接的攻击，在机密性、完整性或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，应考虑威胁的来源。表 6 提供了一种威胁来源的分类方法。

表 6 威胁来源列表

来源		描述
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、意外事故等环境危害或自然灾害，以及软件、硬件、数据、通讯线路等方面的故障
人为因素	恶意人员	不满的或有预谋的内部人员对信息系统进行恶意破坏；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 外部人员利用信息系统的脆弱性，对网络或系统的机密性、完整性和可用性进行破坏，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信息系统故障或被攻击。

对威胁进行分类的方式有多种，针对上表的威胁来源，可以根据其表现形式将威胁分为以下几类。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	威胁子类

种类	描述	威胁子类
软硬件故障	对业务实施或系统运行产生影响的设备硬件故障、通讯链路中断、系统本身或软件缺陷造等问题	设备硬件故障、传输设备故障、存储媒体故障、系统软件故障、应用软件故障、数据库软件故障、开发环境故障
物理环境影响	对信息系统正常运行造成影响的物理环境问题和自然灾害	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
无作为或操作失误	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	维护错误、操作失误等
管理不到位	安全管理无法落实或不到位，从而破坏信息系统正常有序运行	管理制度和策略不完善、管理规程缺失、职责不明确、监督控管机制不健全等
恶意代码	故意在计算机系统上执行恶意任务的程序代码	病毒、特洛伊木马、蠕虫、陷门、间谍软件、窃听软件等
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，或者滥用自己的职权，做出破坏信息系统的行为	非授权访问网络资源、非授权访问系统资源、滥用权限非正常修改系统配置或数据、滥用权限泄露秘密信息等
网络攻击	利用工具和技术通过网络对信息系统进行攻击和入侵	网络探测和信息采集、漏洞探测、嗅探（账户、口令、权限等）、用户身份伪造和欺骗、用户或业务数据的窃取和破坏、系统运行的控制和破坏等
物理攻击	通过物理的接触造成对软件、硬件、数据的破坏	物理接触、物理破坏、盗窃等
泄密	信息泄露给不应了解的他人	内部信息泄露、外部信息泄露等
篡改	非法修改信息，破坏信息的完整性使系统的安全性降低或信息不可用	篡改网络配置信息、篡改系统配置信息、篡改安全配置信息、篡改用户身份信息或业务数据信息等
抵赖	不承认收到的信息和所作的操作和交易	原发抵赖、接收抵赖、第三方抵赖等

5.3.2 威胁赋值

判断威胁出现的频率是威胁赋值的重要内容，评估者应根据经验和（或）有关的统计数据来进行判断。在评估中，需要综合考虑以下三个方面，以形成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频率的统计；

c）近一两年来国际组织发布的对于整个社会或特定行业的威胁及其频率统计，以及发布的威胁预警。

可以对威胁出现的频率进行等级化处理，不同等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。

表 8 提供了威胁出现频率的一种赋值方法。在实际的评估中，威胁频率的判断依据应在评估准备阶段根据历史统计或行业判断予以确定，并得到被评估方的认可。

表 8　威胁赋值表

等级	标识	定义
5	很高	出现的频率很高（或≥1 次/周）；或在大多数情况下几乎不可避免；或可以证实经常发生过
4	高	出现的频率较高（或≥ 1 次/月）；或在大多数情况下很有可能会发生；或可以证实多次发生过
3	中	出现的频率中等（或〉1 次/半年）；或在某种情况下可能会发生；或被证实曾经发生过
2	低	出现的频率较小；或一般不太可能发生；或没有被证实发生过
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

5.4 脆弱性识别

5.4.1 脆弱性识别内容

脆弱性是资产本身存在的，如果没有被相应的威胁利用，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，严重的威胁也不会导致安全事件发生，并造成损失。即，威胁总是要利用资产的脆弱性才可能造成危害。

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。

脆弱性识别是风险评估中最重要的一个环节。脆弱性识别可以以资产为核心，针对每一项需要保护的资产,识别可能被威胁利用的弱点，并对脆弱性的严重程度进行评估；也可以从物理、网络、系统、应用等层次进行识别，然后与资产、威胁对应起来。脆弱性识别的依据可以是国际或国家安全标准，也可以是行业规范、应用流程的安全要求。对应用在不同环境中的相同的弱点，其脆弱性严重程度是不同的，评估者应从组织安全策略的角度考虑、判断资产的脆弱性及其严重程度。信息系统所采用的协议、应用流程的完备与否、与其他网络的互联等也应考虑在内。

脆弱性识别时的数据应来自于资产的所有者、使用者，以及相关业务领域和软硬件方面的专业人员等。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。

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层、网络层、系统层、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应按 GB/T 9361 中的技术指标实施；对操作系统、数据库应按 GB 17859-1999 中的技术指标实施。对管理脆弱性识别方面应按 GB/T 19716-2005 的要求对安全管理制度及其执行情况进行检查，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 脆弱性识别内容表

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
	网络结构	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、网络设备安全配置等方面进行识别
	系统软件	从补丁安装、物理保护、用户账号、口令策略、资源共享、事件审计、访问控制、新系统配置、注册表加固、网络安全、系统管理等方面进行识别
	应用中间件	从协议安全、交易完整性、数据完整性等方面进行识别。
	应用系统	从审计机制、审计存储、访问控制策略、数据完整性、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、符合性等方面进行识别

5.4.2 脆弱性赋值

可以根据对资产的损害程度、技术实现的难易程度、弱点的流行程度，采用等级方式对已识别的脆弱性的严重程度进行赋值。由于很多弱点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弱点，以确定这一方面脆弱性的严重程度。

对某个资产，其技术脆弱性的严重程度还受到组织管理脆弱性的影响。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表

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，将对资产造成的损害可以忽略。

5.5 已有安全措施确认

在识别脆弱性的同时，评估人员应对已采取的安全措施的有效性进行确认。安全措施的确认应评估其有效性，即是否真正地降低了系统的脆弱性，抵御了威胁。对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。对确认为不适当的安全措施应核实是否应被取消或对其进行修正，或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后对组织或系统造成的影响。

已有安全措施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系统技术或管理上的脆弱性，但安全措施确认并不需要和脆弱性识别过程那样具体到每个资产、组件的脆弱性，而是一类具体措施的集合，为风险处理计划的制定提供依据和参考。

5.6 风险分析

5.6.1 风险计算原理

在完成了资产识别、威胁识别、脆弱性识别，以及对已有安全措施确认后，将采用适当的方法与工具确定威胁利用脆弱性导致安全事件发生的可能性。综合安全事件所作用的资产价值及脆弱性的严重程度，判断安全事件造成的损失对组织的影响，即安全风险。本标准给出了风险计算原理，以下面的范式形式化加以说明：

风险值=R（A，T，V）= R(L(T，V)，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； 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；L 表示威胁利用资产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弱点的状况，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(T，V)

在具体评估中，应综合攻击者技术能力（专业技术程度、攻击设备等）、脆弱性被利用的难易程度（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）计算安全事件发生后的损失

根据资产价值及脆弱性严重程度，计算安全事件一旦发生后的损失，即：

安全事件的损失=F(资产价值，脆弱性严重程度)＝F(Ia，Va)

部分安全事件的发生造成的损失不仅仅是针对该资产本身，还可能影响业务的连续性；不同安全事件的发生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。

部分安全事件损失的判断还应参照安全事件发生可能性的结果，对发生可能性极小的安全事件（如处于非地震带的地震威胁、在采取完备供电措施状况下的电力故障威胁等）可以不计算其损失。

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，安全事件造成的损失)＝R(L(T，V)，F(Ia，Va))

评估者可根据自身情况选择相应的风险计算方法计算风险值，如矩阵法或相乘法。矩阵法通过构造一个二维矩阵，形成安全事件发生的可能性与安全事件的损失之间的二维关系；相乘法通过构造经验函数，将安全事件发生的可能性与安全事件的损失进行运算得到风险值。

附录A中列举了矩阵法和相乘法的风险计算示例。

5.6.2 风险结果判定

为实现对风险的控制与管理，可以对风险评估的结果进行等级化处理。可以将风险划分为五级，等级越高，风险越高。

评估者应根据所采用的风险计算方法，计算每种资产面临的风险值，根据风险值的分布状况，为每个等级设定风险值范围，并对所有风险计算结果进行等级处理。每个等级代表了相应风险的严重程度。

表 11 提供了一种风险等级划分方法。

表 11　风险等级划分表

等　级	标　识	描　述
5	很高	一旦发生将产生非常严重的经济或社会影响，如组织信誉严重破坏、严重影响组织的正常经营，经济损失重大、社会影响恶劣
4	高	一旦发生将产生较大的经济或社会影响，在一定范围内给组织的经营和组织信誉造成损害
3	中等	一旦发生会造成一定的经济、社会或生产经营影响，但影响面和影响程度不大
2	低	一旦发生造成的影响程度较低，一般仅限于组织内部，通过一定手段很快能解决
1	很低	一旦发生造成的影响几乎不存在，通过简单的措施就能弥补

风险等级处理的目的是为风险管理过程中对不同风险的直观比较，以确定组织安全策略。组织应当综合考虑风险控制成本与风险造成的影响，提出一个可接受的风险范围。对某些资产的风险，如果风险计算值在可接受的范围内，则该风险是可接受的风险，应保持已有的安全措施；如果风险评估值在可接受的范围外，即风险计算值高于可接受范围的上限值，是不可接受的风险，需要采取安全措施以降低、控制风险。另一种确定不可接受的风险的办法是根据等级化处理的结果，不设定可接受风险值的基准，达到相应等级的风险都进行处理。

5.6.3 风险处理计划

对不可接受的风险应根据导致该风险的脆弱性制定风险处理计划。风险处理计划中明确应采取的弥补弱点的安全措施、预期效果、实施条件、进度安排、责任部门等。安全措施的选择应从管理与技术两个方面考虑。安全措施的选择与实施应参照信息安全的相关标准进行。

5.6.4残余风险评估

在对于不可接受的风险选择适当安全措施后，为确保安全措施的有效性，可进行再评估，以判断实施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提出的风险评估流程实施，也可做适当裁减。一般来说，安全措施的实施是以减少脆弱性或降低安全事件发生可能性为目标的，因此，残余风险的评估可以从脆弱性评估开始，在对照安全措施实施前后的脆弱性状况后，再次计算风险值的大小。

某些风险可能在选择了适当的安全措施后，残余风险的结果仍处于不可接受的风险范围内，应考虑是否接受此风险或进一步增加相应的安全措施。

5.7 风险评估文档记录

5.7.1 风险评估文档记录的要求

记录风险评估过程的相关文档，应符合以下要求（但不仅限于此）：

a）确保文档发布前是得到批准的；

b）确保文档的更改和现行修订状态是可识别的；

c）确保文档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档；

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

对于风险评估过程中形成的相关文档，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。

相关文档是否需要以及详略程度由组织的管理者来决定。

5.7.2 风险评估文档

风险评估文档是指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，包括（但不仅限于此）：

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：明确评估的目的、职责、过程、相关的文档要求，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；

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，包括具体弱点的名称、描述、类型及严重程度等；

g）已有安全措施确认表：根据对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：根据风险评估程序，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。

6 信息系统生命周期各阶段的风险评估

6.1 信息系统生命周期概述

风险评估应贯穿于信息系统生命周期的各阶段中。信息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、要求等各方面也有所不同。具体而言，在规划设计阶段，通过风险评估以确定系统的安全目标；在建设验收阶段，通过风险评估以确定系统的安全目标达成与否；在运行维护阶段，要不断地实施风险评估以识别系统面临的不断变化的风险和脆弱性，从而确定安全措施的有效性，确保安全目标得以实现。因此，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。有条件时，应采用风险评估工具开展风险评估活动。

有关风险评估工具的说明参见附录B。

6.2 规划阶段的风险评估

规划阶段风险评估的目的是识别系统的业务战略，以支撑系统安全需求及安全战略等。规划阶段的评估应能够描述信息系统建成后对现有业务模式的作用，包括技术、管理等方面，并根据其作用确定系统建设应达到的安全目标。

本阶段评估中，资产、脆弱性不需要识别；威胁应根据未来系统的应用对象、应用环境、业务状况、操作要求等方面进行分析。评估着重在以下几方面：

a）是否依据相关规则，建立了与业务战略相一致的信息系统安全规划，并得到最高管理者的认可；

b）系统规划中是否明确信息系统开发的组织、业务变更的管理、开发优先级；

c）系统规划中是否考虑信息系统的威胁、环境，并制定总体的安全方针；

d）系统规划中是否描述信息系统预期使用的信息，包括预期的应用、信息资产的重要性、潜在的价值、可能的使用限制、对业务的支持程度等；

e）系统规划中是否描述所有与信息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、组织安全策略、习惯、专门技术和知识等。

规划阶段的评估结果应体现在信息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规划阶段所明确的系统运行环境、资产重要性，提出安全功能需求。设计阶段的风险评估结果应对设计方案中所提供的安全功能符合性进行判断，作为采购过程风险控制的依据。

本阶段评估中，应详细评估设计方案中对系统面临威胁的描述，将使用的具体设备、软件等资产及其安全功能需求列表。对设计方案的评估着重在以下几方面：

a）设计方案是否符合系统建设规划，并得到最高管理者的认可；

b）设计方案是否对系统建设后面临的威胁进行了分析，重点分析来自物理环境和自然的威胁，以及由于内、外部入侵等造成的威胁；

c）设计方案中的安全需求是否符合规划阶段的安全目标，并基于威胁的分析，制定信息系统的总体安全策略；

d）设计方案是否采取了一定的手段来应对系统可能的故障；

e）设计方案是否对设计原型中的技术实现以及人员、组织管理等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。

f）设计方案是否考虑可能随着其他系统接入而产生的风险；

g）系统性能是否满足用户需求，并考虑到峰值的影响，是否在技术上考虑了满足系统性能要求的方法；

h）应用系统（含数据库）是否根据业务需要进行了安全设计；

i）设计方案是否根据开发的规模、时间及系统的特点选择开发方法，并根据设计开发计划及用户需求，对系统涉及的软件、硬件与网络进行分析和选型；

j）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。

设计阶段的评估可以以安全建设方案评审的方式进行，判定方案所提供的安全功能与信息技术安全技术标准的符合性。评估结果应体现在信息系统需求分析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系统安全需求和运行环境对系统开发、实施过程进行风险识别，并对系统建成后的安全功能进行验证。根据设计阶段分析的威胁和制定的安全措施，在实施及验收时进行质量控制。

基于设计阶段的资产列表、安全措施，实施阶段应对规划阶段的安全威胁进行进一步细分，同时评估安全措施的实现程度，从而确定安全措施能否抵御现有威胁、脆弱性的影响。实施阶段风险评估主要对系统的开发与技术/产品获取、系统交付实施两个过程进行评估。

开发与技术/产品获取过程的评估要点包括：

a）法律、政策、适用标准和指导方针：直接或间接影响信息系统安全需求的特定法律；影响信息系统安全需求、产品选择的政府政策、国际或国家标准；

b）信息系统的功能需要：安全需求是否有效地支持系统的功能；

c）成本效益风险 ：是否根据信息系统的资产、威胁和脆弱性的分析结果，确定在符合相关法律、政策、标准和功能需要的前提下选择最合适的安全措施。

d）评估保证级别：是否明确系统建设后应进行怎样的测试和检查，从而确定是否满足项目建设、实施规范的要求。

系统交付实施过程的评估要点包括：

a）根据实际建设的系统，详细分析资产、面临的威胁和脆弱性；

b）根据系统建设目标和安全需求，对系统的安全功能进行验收测试；评价安全措施能否抵御安全威胁；

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）对系统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，应重新进行信息系统安全策略的设计与调整。

本阶段风险评估可以采取对照实施方案和标准要求的方式，对实际建设结果进行测试、分析。

6.5 运行维护阶段的风险评估

运行维护阶段风险评估的目的是了解和控制运行过程中的安全风险，是一种较为全面的风险评估。评估内容包括对真实运行的信息系统、资产、威胁、脆弱性等各方面。

a）资产评估：在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、系统运行过程中生成的信息资产、相关的人员与服务等，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：应全面地分析威胁的可能性和影响程度。对非故意威胁导致安全事件的评估可以参照安全事件的发生频率；对故意威胁导致安全事件的评估主要就威胁的各个影响因素做出专业判断；

c）脆弱性评估：是全面的脆弱性评估。包括运行环境中物理、网络、系统、应用、安全保障设备、管理等各方面的脆弱性。技术脆弱性评估可以采取核查、扫描、案例验证、渗透性测试的方式实施；安全保障设备的脆弱性评估，应考虑安全功能的实现情况和安全保障设备本身的脆弱性；管理脆弱性评估可以采取文档、记录核查等方式进行验证；

d）风险计算：根据本标准的相关方法，对重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。

运行维护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更时，也应进行风

险评估。重大变更包括以下情况（但不限于）：

a）增加新的应用或应用发生较大变更；

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；

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了影响。

6.6 废弃阶段的风险评估

当信息系统不能满足现有要求时，信息系统进入废弃阶段。根据废弃的程度，又分为部分废弃和全部废弃两种。

废弃阶段风险评估着重在以下几方面：

a） 确保硬件和软件等资产及残留信息得到了适当的处置，并确保系统组件被合理地丢弃或更换；

b）如果被废弃的系统是某个系统的一部分，或与其他系统存在物理或逻辑上的连接，还应考虑系统废弃后与其他系统的连接是否被关闭；

c）如果在系统变更中废弃，除对废弃部分外，还应对变更的部分进行评估，以确定是否会增加风险或引入新的风险；

d）是否建立了流程，确保更新过程在一个安全、系统化的状态下完成。

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。对由于系统废弃可能带来的新的威胁进行分析，并改进新系统或管理模式。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。

信息系统的维护技术人员和管理人员均应该参与此阶段的评估。

7 风险评估的工作形式

7.1 概述

信息安全风险评估分为自评估和检查评估两种形式。信息安全风险评估应以自评估为主，自评估和检查评估相结合、互为补充。

7.2 自评估

自评估是指信息系统拥有、运营或使用单位发起的对本单位信息系统进行的风险评估。自评估应在本标准的指导下，结合系统特定的安全要求进行实施。周期性进行的自评估可以在评估流程上适当简化，重点考察自上次评估后系统发生变化后引入的新威胁，以及系统脆弱性的完整识别，以便于两次评估结果的对比。但系统发生本标准6.5节中所列的重大变更时，应依据本标准进行完整的评估。

自评估可由发起方实施或委托风险评估服务技术支持方实施。由发起方实施的评估可以降低实施的费用、提高强信息系统相关人员的安全意识，但可能由于缺乏风险评估的专业技能，其结果不够深入准确；同时，受到组织内部各种因素的影响，其评估结果的客观性易受影响。委托风险评估服务技术支持方实施的评估，过程比较规范、评估结果的客观性比较好，可信程度较高；但由于受到行业知识技能及业务了解的限制，对被评估系统的了解，尤其是在业务方面的特殊要求存在一定的局限。但由于引入第三方本身就是一个风险因素，因此，对其背景与资质、评估过程与结果的保密要求等方面应进行控制。

此外，为保证风险评估的实施，与系统相连的相关方也应配合，以防止给其他方的使用带来困难或引入新的风险。

7.3 检查评估

检查评估是指信息系统上级管理部门组织或国家有关职能部门依法开展的风险评估。

检查评估可依据本标准的要求，实施完整的风险评估过程。

检查评估也可在自评估实施的基础上，对关键环节或重点内容实施抽样评估，包括以下内容（但不仅限于）：

a）自评估队伍及技术人员审查；

b）自评估方法的检查；

c）自评估过程控制与文档记录检查；

d）自评估资产列表审查；

e）自评估威胁列表审查；

f）自评估脆弱性列表审查；

g）现有安全措施有效性检查；

h）自评估结果审查与采取相应措施的跟踪检查；

i）自评估技术技能限制未完成项目的检查评估；

j）上级关注或要求的关键环节和重点内容的检查评估；

k）软硬件维护制度及实施管理的检查；

l）突发事件应对措施的检查；

检查评估也可委托风险评估服务技术支持方实施，但评估结果仅对检查评估的发起单位负责。由于检查评估代表了主管机关，涉及评估对象也往往较多，因此，要对实施检查评估机构的资质进行严格管理。

附录 A （资料性附录）风险的计算方法

对风险进行计算，需要确定影响风险要素、要素之间的组合方式以及具体的计算方法，将风险要素按照组合方式使用具体的计算方法进行计算，得到风险值。

目前通用的风险评估中风险值计算涉及的风险要素一般为资产、威胁、和脆弱性（其关系如正文图 1 所示）；这些要素的组合方式如正文 5.6.1 节风险计算原理中指出，由威胁和脆弱性确定安全事件发生可能性，由资产和脆弱性确定安全事件的损失，以及由安全事件发生的可能性和安全事件的损失确定风险值。目前，常用的计算方法是矩阵法和相乘法。

本附录首先说明矩阵法和相乘法的原理，然后基于 5.6.1 风险计算原理中指出的风险要素和要素组合方式，以示例的形式说明采用矩阵法和相乘法计算风险值的过程。

在实际应用中，可以将矩阵法和相乘法结合使用。

A.1 使用矩阵法计算风险

A.1.1 矩阵法原理

矩阵法主要适用于由两个要素值确定一个要素值的情形。首先需要确定二维计算矩阵，矩阵内各个要素的值根据具体情况和函数递增情况采用数学方法确定，然后将两个元素的值在矩阵中进行比对，行列交叉处即为所确定的计算结果。

即 $z = f(x, y)$，函数 f 可以采用矩阵法。

矩阵法的原理是：

$x = \{x_1, x_2, \cdots, x_i, \cdots, x_m\}, 1 \le i \le m$， x_i 为正整数，

$y = \{y_1, y_2, \cdots, y_j, \cdots, y_n\}, 1 \le y \le n$， y_j 为正整数，

以要素 x 和要素 y 的取值构建一个二维矩阵，如表 A.1 所示。矩阵行值为要素 y 的所有取值，矩阵列值为要素 x 的所有取值。矩阵内 $m \times n$ 个值即为要素 z 的取值，$z = \{z_{11}, z_{12}, \cdots, z_{ij}, \cdots, z_{mn}\}, 1 \le i \le m, 1 \le j \le n$， z_{ij} 为正整数。

表 A.1 矩阵构造

	y	y_1	y_2	…	y_j	…	y_n
x	x_1	z_{11}	z_{12}	…	z_{1j}	…	z_{1n}
	x_2	z_{21}	z_{22}	…	z_{2j}	…	z_{2n}
	…	…	…	…	…	…	…
	x_i	z_{i1}	z_{i2}	…	z_{ij}	…	z_{in}
	…	…	…	…	…	…	…
	x_m	z_{m1}	z_{m1}	…	z_{mj}	…	z_{mn}

对于 z_{ij} 的计算，可以采取以下计算公式，

$z_{ij} = x_i + y_j$，或 $z_{ij} = x_i \times y_j$，

或 $z_{ij} = \alpha \times x_i + \beta \times y_j$，其中 α 和 β 为正常数。

z_{ij}的计算需要根据实际情况确定，矩阵内z_{ij}值的计算不一定遵循统一的计算公式，但必须具有统一的增减趋势，即如果f是递增函数，z_{ij}值应随着x_i与y_j的值递增，反之亦然。

矩阵法的特点在于通过构造两两要素计算矩阵，可以清晰罗列要素的变化趋势，具备良好灵活性。

在风险值计算中，通常需要对两个要素确定的另一个要素值进行计算，例如由威胁和脆弱性确定安全事件发生可能性值、由资产和脆弱性确定安全事件的损失值等，同时需要整体掌握风险值的确定，因此矩阵法在风险分析中得到广泛采用。

A.1.2 计算示例

本节中，基于本标准 5.6.1 节风险计算原理，具体说明使用矩阵法计算风险的过程。

A.1.2.1 条件

共有三个重要资产，资产 A1、资产 A2 和资产 A3；

资产 A1 面临两个主要威胁，威胁 T1 和威胁 T2；

资产 A2 面临一个主要威胁，威胁 T3；

资产 A3 面临两个主要威胁，威胁 T4 和 T5；

威胁 T1 可以利用的资产 A1 存在的两个脆弱性，脆弱性 V1 和脆弱性 V2；

威胁 T2 可以利用的资产 A1 存在的三个脆弱性，脆弱性 V3、脆弱性 V4 和脆弱性 V5；

威胁 T3 可以利用的资产 A2 存在的两个脆弱性，脆弱性 V6 和脆弱性 V7；

威胁 T4 可以利用的资产 A3 存在的一个脆弱性，脆弱性 V8；

威胁 T5 可以利用的资产 A3 存在的一个脆弱性，脆弱性 V9。

资产价值分别是：资产 A1=2，资产 A2=3，资产 A3=5；

威胁发生频率分别是：威胁 T1=2，威胁 T2=1，威胁 T3=2，威胁 T4=5，威胁 T5=4；

脆弱性严重程度分别是：脆弱性 V1=2，脆弱性 V2=3，脆弱性 V3=1，脆弱性 V4=4，脆弱性 V5=2，脆弱性 V6=4，脆弱性 V7=2，脆弱性 V8=3，脆弱性 V9=5。

A.1.2.2 计算重要资产的风险值

三个资产的风险值计算过程类似，下面以资产 A1 为例使用矩阵法计算风险值。

资产 A1 面临的主要威胁包括威胁 T1 和威胁 T2，威胁 T1 可以利用的资产 A1 存在的脆弱性包括两个，威胁 T2 可以利用的资产 A1 存在的脆弱性包括三个，则资产 A1 存在的风险值包括五个。五个风险值的计算过程类似，下面以资产 A1 面临的威胁 T1 可以利用的脆弱性 V1 为例，计算安全风险值。

a）计算安全事件发生可能性

威胁发生频率：威胁 T1=2；

脆弱性严重程度：脆弱性 V1=2。

首先构建安全事件发生可能性矩阵，如表 A.2 所示。

表 A.2 安全事件可能性矩阵

	脆弱性严重程度	1	2	3	4	5
威胁发生频率	1	2	4	7	11	14
	2	3	6	10	13	17
	3	5	9	12	16	20
	4	7	11	14	18	22
	5	8	12	17	20	25

然后根据威胁发生频率值和脆弱性严重程度值在矩阵中进行对照，确定安全事件发生可能性值=6。

由于安全事件发生可能性将参与风险事件值的计算，为了构建风险矩阵，对上述计算得到的安全风险事件发生可能性进行等级划分，如表 A.3 所示，安全事件发生可能性值=2。

表 A.3 安全事件可能性等级划分

安全事件发生可能性值	1-5	6-11	12-16	17-21	22-25
发生可能性等级	1	2	3	4	5

b）计算安全事件的损失

资产价值：资产 A1=2；

脆弱性严重程度：脆弱性 V1=2。

首先构建安全事件损失矩阵，如表 A.4 所示。

表 A.4 安全事件损失矩阵

	脆弱性严重程度	1	2	3	4	5
资产价值	1	2	4	6	10	13
	2	3	5	9	12	16
	3	4	7	11	15	20
	4	5	8	14	19	22
	5	6	10	16	21	25

然后根据资产价值和脆弱性严重程度值在矩阵中进行对照，确定安全事件损失值=5。

由于安全事件损失将参与风险事件值的计算，为了构建风险矩阵，对上述计算得到的安全事件损失进行等级划分，如表 A.5 所示，安全事件发生可能性值=1。

表 A.5 安全事件损失等级划分

安全事件损失值	1-5	6-10	11-15	16-20	21-25
安全事件损失等级	1	2	3	4	5

c）计算风险值

安全事件发生可能性=2；安全事件损失=1。

首先构建风险矩阵，如表 A.6 所示。

表 A.6 风险矩阵

	可能性	1	2	3	4	5
损失	1	3	6	9	12	16
	2	5	8	11	15	18
	3	6	9	13	17	21
	4	7	11	16	20	23
	5	9	14	20	23	25

然后根据安全事件发生可能性和安全事件损失在矩阵中进行对照，确定安全事件风险=6。

按照上述方法进行计算，得到资产 A 的其它的风险值，以及资产 A2 和资产 A3 的风险。然后再进行风险结果等级判定。

A.1.2.3 结果判定

确定风险等级划分 如表 A.7 所示。

表 A.7 风险等级划分

风险值	1-6	7-12	13-18	19-23	24-25
风险等级	1	2	3	4	5

根据上述计算方法，以此类推，得到三个重要资产的风险值，并根据风险等级划分表，确定风险等级，结果如表 A.8 所示。

表 A.8 风险结果

资产	威胁	脆弱性	风险值	风险等级
资产 A1	威胁 T1	脆弱性 V1	6	1
	威胁 T1	脆弱性 V2	8	2
	威胁 T2	脆弱性 V3	3	1
	威胁 T2	脆弱性 V4	9	2
	威胁 T2	脆弱性 V5	3	1
资产 A2	威胁 T3	脆弱性 V6	11	2
	威胁 T3	脆弱性 V7	8	2
资产 A3	威胁 T4	脆弱性 V8	20	4
	威胁 T5	脆弱性 V9	25	5

重要资产的风险值等级柱状图如图 A.1 所示。

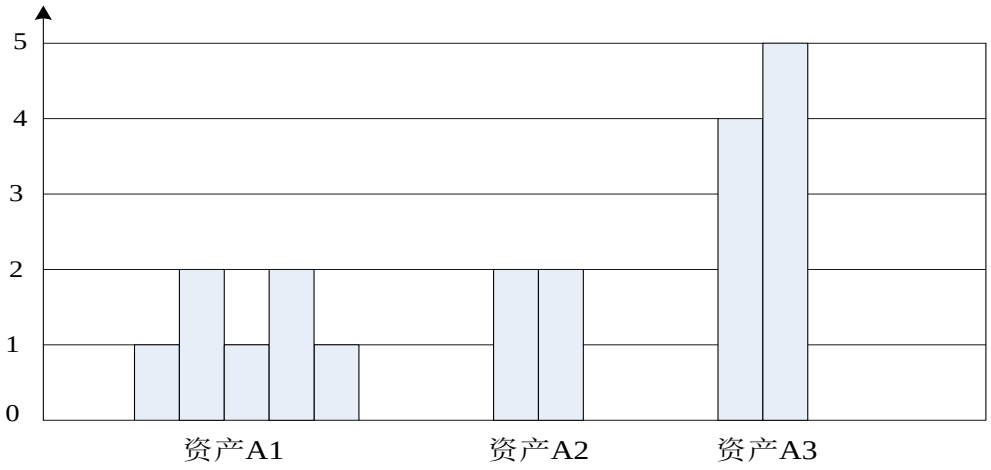

图 A.1 风险等级柱状图

A.2 使用相乘法计算风险

A.2.1 相乘法原理

相乘法主要用于两个或多个要素值确定一个要素值的情形。即 $z = f(x, y)$，函数 f 可以采用相乘

法。

相乘法的原理是：

$z=f(x,y)=x\otimes y$。

当 f 为增量函数时，$\otimes$ 可以为直接相乘，也可以为相乘后取模等，例如：

$z=f(x,y)=x\times y$，

或 $z=f(x,y)=\sqrt{x\times y}$，

或 $z=f(x,y)=\left[\sqrt{x\times y}\right]$，

或 $z=f(x,y)=\left[\dfrac{\sqrt{x\times y}}{x+y}\right]$ 等。

相乘法提供一种定量的计算方法，直接使用两个要素值进行相乘得到另一个要素的值。相乘法的特点是简单明确，直接按照统一公式计算，即可得到所需结果。

在风险值计算中，通常需要对两个要素确定的另一个要素值进行计算，例如由威胁和脆弱性确定安全事件发生可能性值、由资产和脆弱性确定安全事件的损失值，因此相乘法在风险分析中得到广泛采用。

A.2.2 计算示例

本节中，基于本标准 5.6.1 节风险计算原理，具体说明使用相乘法计算风险的过程。

A.2.2.1 条件

共有两个重要资产，资产 A1 和资产 A2；

资产 A1 面临三个主要威胁，威胁 T1、威胁 T2 和威胁 T3；

资产 A2 面临两个主要威胁，威胁 T4 和威胁 T5；

威胁 T1 可以利用的资产 A1 存在的一个脆弱性，脆弱性 V1；

威胁 T2 可以利用的资产 A1 存在的两个脆弱性，脆弱性 V2、脆弱性 V3；

威胁 T3 可以利用的资产 A1 存在的一个脆弱性，脆弱性 V4；

威胁 T4 可以利用的资产 A2 存在的一个脆弱性，脆弱性 V5；

威胁 T5 可以利用的资产 A2 存在的一个脆弱性，脆弱性 V6。

资产价值分别是：资产 A1=4，资产 A2=5；

威胁发生频率分别是：威胁 T1=1，威胁 T2=5，威胁 T3=4，威胁 T4=3，威胁 T5=4；

脆弱性严重程度分别是：脆弱性 V1=3，脆弱性 V2=1，脆弱性 V3=5，脆弱性 V4=4，脆弱性 V5=4，脆弱性 V6=3。

A.2.2.2 计算重要资产的风险值

两个资产的风险值计算过程类似，下面以资产 A 为例使用矩阵法计算风险值。

资产 A1 面临的主要威胁包括威胁 T1、威胁 T2 和威胁 T3，威胁 T1 可以利用的资产 A1 存在的脆弱性有一个，威胁 T2 可以利用的资产 A1 存在的脆弱性有两个，威胁 T3 可以利用的资产 A1 存在的脆弱性有一个，则资产 A1 存在的风险值包括四个。四个风险值的计算过程类似，下面以资产 A1 面临的威胁 T1 可以利用的脆弱性 V1 为例，计算安全风险值。其中计算公式使用：

$z=f(x,y)=\sqrt{x\times y}$，并对 z 的计算值四舍五入取整得到最终结果。

a）计算安全事件发生可能性

威胁发生频率：威胁 T1=1；
脆弱性严重程度：脆弱性 V1=3。

计算安全事件发生可能性，安全事件发生可能性=$\sqrt{1\times 3}=\sqrt{3}$。

b）计算安全事件的损失
资产价值：资产 A1=4；
脆弱性严重程度：脆弱性 V1=3。

计算安全事件的损失，安全事件损失=$\sqrt{4\times 3}=\sqrt{12}$。

c）计算风险值
安全事件发生可能性=2；
安全事件损失=3。

安全事件风险值=$\sqrt{3}\times\sqrt{12}=6$。

按照上述方法进行计算，得到资产 A1 的其它的风险值，以及资产 A2 和资产 A3 风险值。然后再进行风险结果等级判定。

A.2.2.3 结果判定

确定风险等级划分如表 A.9 所示。

表 A.9 风险等级划分

风险值	1-5	6-10	11-15	16-20	21-25
风险等级	1	2	3	4	5

根据上述计算方法，以此类推，得到两个重要资产的风险值，并根据风险等级划分表，确定风险等级，结果如表 A.10 所示。

表 A.10 风险结果

资产	威胁	脆弱性	风险值	风险等级
资产 A1	威胁 T1	脆弱性 V1	6	2
	威胁 T2	脆弱性 V2	4	1
	威胁 T2	脆弱性 V3	22	5
	威胁 T3	脆弱性 V4	16	4
资产 A2	威胁 T4	脆弱性 V5	15	3
	威胁 T5	脆弱性 V6	13	3

重要资产的风险值等级柱状图如图 A.2 所示。

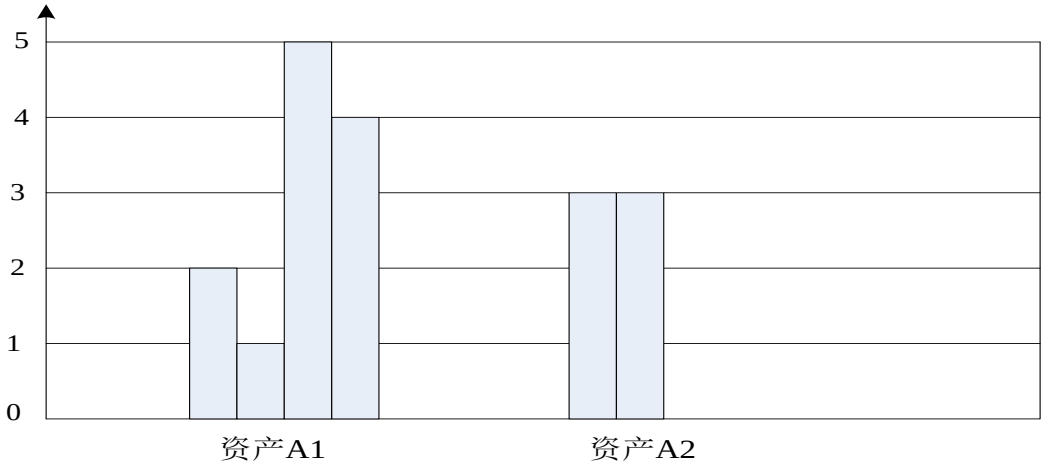

图 A.2 风险等级柱状图

附录 B （资料性附录）风险评估的工具

风险评估工具是风险评估的辅助手段，是保证风险评估结果可信度的一个重要因素。风险评估工具的使用不但在一定程度上解决了手动评估的局限性，最主要的是它能够将专家知识进行集中，使专家的经验知识被广泛的应用。

根据在风险评估过程中的主要任务和作用原理的不同，风险评估的工具可以分成风险评估与管理工具、系统基础平台风险评估工具、风险评估辅助工具三类。风险评估与管理工具是一套集成了风险评估各类知识和判据的管理信息系统，以规范风险评估的过程和操作方法；或者是用于收集评估所需要的数据和资料，基于专家经验，对输入输出进行模型分析。系统基础平台风险评估工具主要用于对信息系统的主要部件（如操作系统、数据库系统、网络设备等）的弱点进行分析，或实施基于弱点的攻击。风险评估辅助工具则实现对数据的采集、现状分析和趋势分析等单项功能，为风险评估各要素的赋值、定级提供依据。

B.1 风险评估与管理工具

风险评估与管理工具大部分是基于某种标准方法或某组织自行开发的评估方法，可以有效地通过输入数据来分析风险，给出对风险的评价并推荐控制风险的安全措施。

风险评估与管理工具通常建立在一定的模型或算法之上，风险由重要资产、所面临的威胁以及威胁所利用的弱点三者来确定；也有的通过建立专家系统，利用专家经验进行分析，给出专家结论。这种评估工具需要不断进行知识库的扩充。

此类工具实现了对风险评估全过程的实施和管理，包括：被评估信息系统基本信息获取、资产信息获取、脆弱性识别与管理、威胁识别、风险计算、评估过程与评估结果管理等功能。评估的方式可以通过问卷的方式，也可以通过结构化的推理过程，建立模型、输入相关信息，得出评估结论。通常这类工具在对风险进行评估后都会有针对性地提出风险控制措施。

根据实现方法的不同，风险评估与管理工具可以分为三类：

a ）基于信息安全标准的风险评估与管理工具

目前，国际上存在多种不同的风险分析标准或指南，不同的风险分析方法侧重点不同，例如 NIST SP 800-30 、BS7799、ISO/IEC 13335 等。以这些标准或指南的内容为基础，分别开发相应的评估工具，完成遵循标准或指南的风险评估过程。

b）基于知识的风险评估与管理工具

基于知识的风险评估与管理工具并不仅仅遵循某个单一的标准或指南，而是将各种风险分析方法进行综合，并结合实践经验，形成风险评估知识库，以此为基础完成综合评估。它还涉及来自类似组织（包括规模、商务目标和市场等）的最佳实践，主要通过多种途径采集相关信息，识别组织的风险和当前的安全措施；与特定的标准或最佳实践进行比较，从中找出不符合的地方；按照标准或最佳实践的推荐选择安全措施以控制风险。

c）基于模型的风险评估与管理工具

基于标准或基于知识的风险评估与管理工具，都使用了定性分析方法或定量分析方法，或者将定性与定量相结合。定性分析方法是目前广泛采用的方法，需要凭借评估者的知识、经验和直觉，或者业界的标准和实践，为风险的各个要素定级。定性分析法操作相对容易，但也可能因为评估者经验和直觉的偏差而使分析结果失准。定量分析则对构成风险的各个要素和潜在损失水平赋予数值或货币金额，通过对度量风险的所有要素进行赋值，建立综合评价的数学模型，从而完成风险的量化计算。定量分析方法准确，但前期建立系统风险模型较困难。定性与定量结合分析方法就是将风险要素的赋值和计算，根据需要分别采取定性和定量的方法完成。

基于模型的风险评估与管理工具是在对系统各组成部分、安全要素充分研究的基础上，对典型系统的资产、威胁、脆弱性建立量化或半量化的模型，根据采集信息的输入，得到评价的结果。

B.2 系统基础平台风险评估工具

系统基础平台风险评估工具包括脆弱性扫描工具和渗透性测试工具。脆弱性扫描工具又称为安全扫描器、漏洞扫描仪等，主要用于识别网络、操作系统、数据库系统的脆弱性。通常情况下，这些工具能够发现软件和硬件中已知的弱点，以决定系统是否易受已知攻击的影响。

脆弱性扫描工具是目前应用最广泛的风险评估工具，主要完成操作系统、数据库系统、网络协议、网络服务等的安全脆弱性检测功能，目前常见的脆弱性扫描工具有以下几种类型：

a）基于网络的扫描器：在网络中运行，能够检测如防火墙错误配置或连接到网络上的易受攻击的网络服务器的关键漏洞。

b）基于主机的扫描器：发现主机的操作系统、特殊服务和配置的细节，发现潜在的用户行为风险，如密码强度不够，也可实施对文件系统的检查。

c）分布式网络扫描器：由远程扫描代理、对这些代理的即插即用更新机制、中心管理点三部分构成，用于企业级网络的脆弱性评估，分布和位于不同的位置、城市甚至不同的国家。

d）数据库脆弱性扫描器：对数据库的授权、认证和完整性进行详细的分析，也可以识别数据库系统中潜在的弱点。

渗透性测试工具是根据脆弱性扫描工具扫描的结果进行模拟攻击测试，判断被非法访问者利用的可能性。这类工具通常包括黑客工具、脚本文件。渗透性测试的目的是检测已发现的脆弱性是否真正会给系统或网络带来影响。通常渗透性工具与脆弱性扫描工具一起使用，并可能会对被评估系统的运行带来一定影响。

B.3 风险评估辅助工具

科学的风险评估需要大量的实践和经验数据的支持，这些数据的积累是风险评估科学性的基础。风险评估过程中，可以利用一些辅助性的工具和方法来采集数据，帮助完成现状分析和趋势判断，如：

a）检查列表：检查列表是基于特定标准或基线建立的，对特定系统进行审查的项目条款。通过检查列表，操作者可以快速定位系统目前的安全状况与基线要求之间的差距。

b）入侵监测系统：入侵监测系统通过部署检测引擎，收集、处理整个网络中的通信信息，以获取可能对网络或主机造成危害的入侵攻击事件；帮助检测各种攻击试探和误操作；同时也可以作为一个警报器，提醒管理员发生的安全状况。

c）安全审计工具：用于记录网络行为，分析系统或网络安全现状；它的审计记录可以作为风险评估中的安全现状数据，并可用于判断被评估对象威胁信息的来源。

d）拓扑发现工具：通过接入点接入被评估网络，完成被评估网络中的资产发现功能，并提供网络资产的相关信息，包括操作系统版本、型号等。拓扑发现工具主要是自动完成网络硬件设备的识别、发现功能。

e）资产信息收集系统：通过提供调查表形式，完成被评估信息系统数据、管理、人员等资产信息的收集功能，了解到组织的主要业务、重要资产、威胁、管理上的缺陷、采用的控制措施和安全策略的执行情况。此类系统主要采取电子调查表形式，需要被评估系统管理人员参与填写，并自动完成资产信息获取。

f）其他：如用于评估过程参考的评估指标库、知识库、漏洞库、算法库、模型库等。

参 考 文 献

[1] GB/T 19715.1-2005 信息技术 信息技术安全管理指南 第 1 部分：信息技术安全概念和模型（ISO/IEC TR 13335-1:1996,IDT）

[2] GB/T 5271.8-2001 信息技术 词汇 第 8 部分：安全（idt ISO/IEC 2382-8:1998）

[3]NIST Special Publication 800-26:Security Self-Assessment Guide for Information Technology Systems

[4]NIST Special Publication 800-30:Risk Management Guide for Information Technology Systems