国家863高技术研究发展计划资助项目(2004AA147070)

# 信息安全风险评估实施教程

范红　冯登国　编著

清华大学出版社

国家863高技术研究发展计划资助项目(2004AA147070)

# 信息安全风险评估
# 实施教程

范红　冯登国　编著

清华大学出版社
北京

## 内 容 简 介

本书是《信息安全风险评估方法与应用》的配套教材，主要介绍了信息安全风险评估的基本概念、原理、流程和方法，给出了依据国家标准《信息安全风险评估规范》进行的两个评估案例。为方便读者熟悉与掌握风险评估的流程，本书提供了操作演示光盘。同时，在附录部分为《信息安全风险评估方法与应用》(已由清华大学出版社出版)的各章节配了一套练习题并提供了答案。

本书可作为信息安全风险评估专业的培训教程，也可供从事相关专业的教学或工程技术人员参考。



**图书在版编目(CIP)数据**

信息安全风险评估实施教程/范红，冯登国编著. —北京：清华大学出版社，2007.4
ISBN 978-7-302-14145-7

Ⅰ.信…　Ⅱ.①范…②冯…　Ⅲ.信息系统－安全管理－风险分析－教材　Ⅳ.TP309

中国版本图书馆 CIP 数据核字(2006)第 137592 号

**责任编辑**：张　民　顾　冰
**责任校对**：梁　毅
**责任印制**：李红英

**出版发行**：清华大学出版社　　**地　　址**：北京清华大学学研大厦 A 座
http://www.tup.com.cn　　**邮　　编**：100084
c-service@tup.tsinghua.edu.cn
**社 总 机**：010-62770175　　**邮购热线**：010-62786544
**投稿咨询**：010-62772015　　**客户服务**：010-62776969

**印 刷 者**：北京市清华园胶印厂
**装 订 者**：三河市金元印装有限公司
**经　　销**：全国新华书店
**开　　本**：170×230　**印　张**：8.75　**字　数**：164 千字
(附光盘 1 张)
**版　　次**：2007 年 4 月第 1 版　**印　次**：2007 年 4 月第 1 次印刷
**印　　数**：1～3000
**定　　价**：25.00 元

# 前言

Preface

信息安全风险评估是依据国家信息安全风险评估有关管理要求和技术标准，对信息系统及由其存储、处理和传输的信息的机密性、完整性和可用性等安全属性进行科学、公正的综合评价的过程。通过对信息及信息系统的重要性、面临的威胁、其自身的脆弱性以及已采取安全措施有效性的分析，判断脆弱性被威胁源利用后可能发生的安全事件以及其所造成的负面影响程度来识别信息安全风险。

信息安全风险评估是信息安全保障体系建立过程中的重要的评价方法和决策机制。没有准确及时的风险评估，将使得各个机构无法对其信息安全的状况做出准确的判断。因为任何信息系统都会有安全风险，信息安全建设的宗旨之一，就是在综合考虑成本与效益的前提下，通过安全措施来控制风险，并使残余风险降低到可接受的范围内。所以，所谓安全的信息系统，实际是指信息系统在实施了风险评估并做出风险控制后，仍然存在可被接受的残余风险的信息系统。

信息安全风险评估工作是信息安全的新领域，无论在评估理论研究，还是在评估具体实践上，都对信息安全风险评估的组织者和实施者提出了新的要求。为确保风险评估工作的有效实施，提高风险评估人员的业务能力，本书将信息安全风险评估领域的最新研究成果及其在实践中的具体做法整理成册，并以习题形式帮助读者掌握风险评估的基本内容。希望通过有关知识的推广与普及，规范和指导信息安全风险评估的实践。

本书分为信息安全风险评估流程和信息安全风险评估案例两大部分。第1章介绍了信息安全风险评估的实施流程，并在该章后

附有练习题。为便于读者对风险评估实施流程有一个更加直观的理解，随书附上信息安全风险评估实施流程演示系统的光盘，结合第 1 章的内容，详细阐述了评估实施各阶段的工作目标、内容和方式等。在第 2、3 章分别介绍了两个具体的风险评估实施案例，便于读者理解在实践工作中如何运用风险评估的原理、方法和规范。第 4 章给出演示系统的操作说明。在附录 A 部分为《信息安全风险评估方法与应用》(已由清华大学出版社出版)一书的各章节配了一套练习题并附有答案。

作　者

2006.9

# 目 录

Contents

# 第1章 信息安全风险评估实施流程

信息安全风险评估是从风险管理角度，运用科学的方法和手段，系统地分析网络与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，为防范和化解信息安全风险，或者将风险控制在可接受的水平，制定有针对性的抵御威胁的防护对策和整改措施以最大限度地保障网络和信息安全提供科学依据。

在信息化建设中，各类应用系统及其赖以运行的基础网络、处理的数据和信息是业务实现的保障，由于其可能存在软硬件设备缺陷、系统集成缺陷等，以及信息安全管理中潜在的薄弱环节，都将导致不同程度的安全风险。

信息安全风险评估可以不断地、深入地发现信息系统建设、运行、管理中的安全隐患，并为增强安全性提供有效建议，以便采取更加经济、更加有力的安全保障措施，提高信息安全的科学管理水平，进而全面提升网络与信息系统的安全保障能力。

信息安全风险评估在具体实施中一般包括风险评估的准备活动，对信息系统资产、面临威胁、存在脆弱性的识别，对已采取安全措施的确认，对可能存在的信息安全风险的识别等环节。下面对各具体步骤进行详细描述。

## 1.1 风险评估的准备

风险评估的准备是实施风险评估的前提，只有有效地进行了信息安全风险评估准备，才能更好地开展信息安全风险评估。由于实施信息安全风险评估，

涉及组织的业务流程、信息安全需求、信息系统规模、信息系统结构等各方面内容，因此开展信息安全风险评估的准备活动，通过确定目标、进行调研、获得组织高层管理者对评估的支持等，对有效实施风险评估是十分必要的。

风险评估的准备活动包括：

(1) 确定风险评估的目标；

(2) 确定风险评估的范围；

(3) 组建评估管理团队和评估实施团队；

(4) 进行系统调研；

(5) 确定评估依据和方法；

(6) 获得最高管理者对风险评估工作的支持。

### 1.1.1 确定风险评估的目标

首先需要确定风险评估的目标。信息安全需求是一个组织为保证其业务正常、有效运转而必须达到的信息安全要求，通过分析组织必须符合的相关法律法规、组织在业务流程中对信息安全等的机密性、可用性、完整性等方面的需求，来确定风险评估的目标。

### 1.1.2 确定风险评估的范围

在实施风险评估前，需要确定风险评估的范围。风险评估的范围，包括组织内部与信息处理相关的各类软硬件资产、相关的管理机构和人员、所处理的信息等各方面。实施一次风险评估的范围可大可小，需要根据具体评估需求确定，可以对组织全部的信息系统进行评估，也可以仅对关键业务流程进行评估，也可以对组织的关键部门的信息系统进行评估等。

### 1.1.3 组建评估管理团队和评估实施团队

在确定风险评估的目标、范围后，需要组建风险评估实施团队，具体执行组织的风险评估。由于风险评估涉及组织管理、业务、信息资产等各个方面，因此风险评估团队中除了信息安全风险评估专业人员外，还需要组织管理层、相关业务骨干、信息安全运营管理人员等参与，以便更好地了解组织信息安全状况，以利于风险评估的实施。

### 1.1.4　进行系统调研

在确定了风险评估的目标、范围、团队后，要进行系统调研，并根据系统调研的结果决定评估将采取的评估方法等技术手段。系统调研内容包括：

(1) 组织业务战略；

(2) 组织管理制度；

(3) 组织主要业务功能和要求；

(4) 网络结构、网络环境(包括内部连接和外部连接)；

(5) 网络系统边界；

(6) 主要的硬件、软件；

(7) 数据和信息；

(8) 系统和数据的敏感性；

(9) 系统使用人员；

(10) 其他。

系统调研可以采取问卷调查、现场访谈等方法进行。

### 1.1.5　确定评估依据和方法

以系统调研结果为依据，根据被评估信息系统的具体情况，确定风险评估依据和方法。

评估依据包括(但不限于)现有国际或国家有关信息安全标准、组织的行业主管机关的业务系统的要求和制度、组织的信息系统互联单位的安全要求、组织的信息系统本身的实时性或性能要求等。

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

### 1.1.6　获得支持

就上述内容形成较为完整的风险评估实施方案，并报组织最高管理者批准，以获得其对风险评估方案的支持，同时在组织范围就风险评估相关内容对管理者和技术人员进行培训，以明确有关人员在风险评估中的任务。

## 1.2 资产识别

### 1.2.1 资产分类

风险评估需要对资产的价值进行识别，因为价值不同将导致风险值不同。而风险评估中资产的价值不是以资产的经济价值来衡量，而是以资产的机密性、完整性和可用性三个安全属性为基础进行衡量。资产在机密性、完整性和可用性三个属性上的要求不同，则资产的最终价值也不同。

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。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、文档、服务、人员等类型。表 1-1 列出了一种资产分类方法。

表 1-1 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、用户手册等 |
| 软件 | 系统软件：操作系统、语句包、工具软件、各种库等<br>应用软件：外部购买的应用软件，外包开发的应用软件等<br>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<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、磁带、光盘、软盘、硬盘等<br>传输线路：光纤、双绞线等<br>保障设备：动力保障设备(UPS、变电设备等)、空调、保险柜、文件柜、门禁、消防设施等<br>安全保障设备：防火墙、入侵检测系统、身份验证等<br>其他：打印机、复印机、扫描仪、传真机等 |
| 服务 | 办公服务：为提高效率而开发的管理信息系统(MIS)，包括各种内部配置管理、文件流转管理等服务<br>网络服务：各种网络设备、设施提供的网络连接服务<br>信息服务：对外依赖该系统开展的各类服务 |

续表

| 分类 | 示　　例 |
| --- | --- |
| 文档 | 纸质的各种文件，如传真、电报、财务报告、发展计划等 |
| 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 |
| 其他 | 企业形象、客户关系等 |

## 1.2.2　资产赋值

对资产的赋值不仅要考虑资产的经济价值，更重要的是要考虑资产的安全状况，即资产的机密性、完整性和可用性，对组织信息安全性的影响程度。资产赋值的过程也就是对资产在机密性、完整性和可用性上的要求进行分析，并在此基础上得出综合结果的过程。资产对机密性、完整性和可用性上的要求可由安全属性缺失时造成的影响来表示，这种影响可能造成某些资产的损害以至危及信息系统，还可能导致经济效益、市场份额、组织形象的损失。

### 1. 机密性赋值

根据资产在机密性上的不同要求，将其分为 5 个不同的等级，分别对应资产在机密性缺失时对整个组织的影响。表 1-2 提供了一种机密性赋值的参考。

**表 1-2　资产机密性赋值表**

| 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 |

### 2. 完整性赋值

根据资产在完整性上的不同要求，将其分为 5 个不同的等级，分别对应资

产在完整性上缺失时对整个组织的影响。表 1-3 提供了一种完整性赋值的参考。

表 1-3 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，损失难以弥补 |
| 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，损失较难弥补 |
| 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，但损失可以弥补 |
| 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，损失容易弥补 |
| 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 |

### 3. 可用性赋值

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缺失时对整个组织的影响。表 1-4 提供了一种可用性赋值的参考。

表 1-4 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 分钟 |
| 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 分钟 |
| 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 分钟 |
| 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% |

#### 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。

这里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 5 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 1-5 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，并围绕重要资产进行下一步的风险评估。

**表 1-5　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很小的损失，甚至忽略不计 |

## 1.3　威胁识别

### 1.3.1　威胁分类

信息安全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力的因素和其他物理因素。

威胁作用形式可以是对信息系统直接或间接的攻击，也可能是偶发的或蓄意的安全事件，都会在信息的机密性、完整性或可用性等方面造成损害。

在对威胁进行分类前，应考虑威胁的来源。表 1-6 提供了一种威胁来源的分类方法。

表 1-6 威胁来源列表

| 来源 | | 描述 |
|---|---|---|
| 环境因素 | | 由于断电、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、自然灾害、意外事故以及软件、硬件、数据、通信线路等方面的故障所带来的威胁 |
| 人为因素 | 恶意人员 | 因某种原因，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<br>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，针对表 1-6 的威胁来源，可以根据其表现形式将威胁进行分类。表 1-7 提供了一种基于表现形式的威胁分类方法。

表 1-7 一种基于表现形式的威胁分类表

| 种类 | 描述 | 威胁子类 |
|---|---|---|
| 软硬件故障 | 由于设备硬件故障、通信链路中断、系统本身或软件缺陷造成对业务实施、系统稳定运行的影响 | 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 | 由于断电、静电、灰尘、潮湿、温度、鼠蚁虫害、电磁干扰、洪灾、火灾、地震等环境问题或自然灾害对系统造成影响 | |
| 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，对系统造成的影响 | 维护错误、操作失误 |
| 管理不到位 | 安全管理措施没有落实，造成安全管理不规范，或者管理混乱，从而破坏信息系统正常有序运行 | |
| 恶意代码 | 故意在计算机系统上执行恶意任务的程序代码 | 网络病毒、间谍软件、窃听软件、蠕虫、陷门等 |
| 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 |

续表

| 种　类 | 描　　述 | 威 胁 子 类 |
| --- | --- | --- |
| 网络攻击 | 利用工具和技术，如侦察、密码破译、嗅探、伪造和欺骗、拒绝服务等手段，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 |
| 物理攻击 | 通过物理接触造成对软件、硬件、数据的破坏 | 物理接触、物理破坏、盗窃 |
| 泄密 | 信息泄露给不应了解的人员 | 内部信息泄露、外部信息泄露 |
| 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、系统配置信息、安全配置信息、用户身份信息或业务数据信息 |
| 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 |

### 1.3.2　威胁赋值

威胁出现的频率是衡量威胁严重程度的重要要素，因此威胁识别后需要对威胁频率进行赋值，已带入最后的风险计算中。

评估者应根据经验和(或)有关的统计数据来对威胁频率进行赋值，威胁赋值中需要综合考虑以下三个方面因素：

(1) 以往安全事件报告中出现过的威胁及其频率的统计；

(2) 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；

(3) 近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 1-8 提供了威胁出现频率的一种赋值方法。在实际的评估中，威胁频率的判断应根据历史统计或行业判断，在评估准备阶段确定，并得到被评估方的认可。

表 1-8 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 |

## 1.4 脆弱性识别

### 1.4.1 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进而带来损失。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存在脆弱性。

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