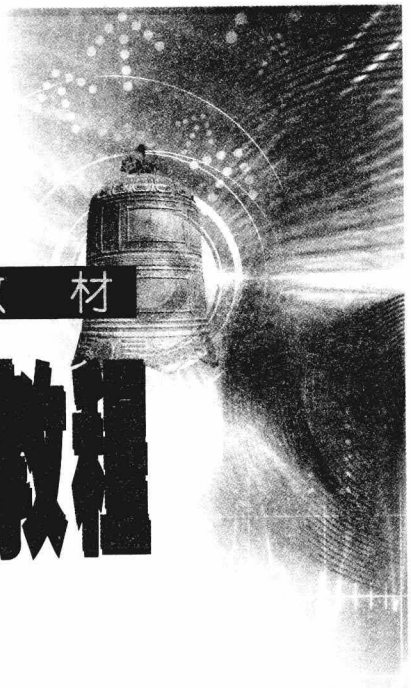
信息安全系列教材

信息安全风险评估教程

吴晓平　付钰　编著

WUHAN UNIVERSITY PRESS
武汉大学出版社



信息安全系列教材

信息安全风险评估教程

吴晓平 付 钰 编著

WUHAN UNIVERSITY PRESS
武汉大学出版社

图书在版编目(CIP)数据

信息安全风险评估教程/吴晓平,付钰编著.—武汉:武汉大学出版社,2011.7
信息安全系列教材
ISBN 978-7-307-08773-6

Ⅰ.信… Ⅱ.①吴… ②付… Ⅲ.信息系统—安全技术—风险分析—教材 Ⅳ.TP309

中国版本图书馆CIP数据核字(2011)第096971号

责任编辑:刘 阳 责任校对:刘 欣 版式设计:支 笛

出版发行:武汉大学出版社 (430072 武昌 珞珈山)
(电子邮件:cbs22@whu.edu.cn 网址:www.wdp.com.cn)
印刷:湖北睿智印务有限公司
开本:787×1092 1/16 印张:11.5 字数:280千字
版次:2011年7月第1版 2011年7月第1次印刷
ISBN 978-7-307-08773-6/TP·397 定价:25.00元

信息安全系列教材

编　委　会

何明星，西华大学数学与计算机学院副院长，教授
代春艳，重庆工商大学计算机科学与信息工程学院
陈　龙，重庆邮电大学计算机科学与技术学院，副教授
杨德刚，重庆师范大学数学与计算机科学学院
黄同愿，重庆工学院计算机学院
郑智捷，云南大学软件学院信息安全系主任，教授
谢晓尧，贵州师范大学副校长，教授

华　东

徐炜民，上海大学计算机工程与科学学院，教授
楚丹琪，上海大学教务处，副教授
孙　莉，东华大学计算机科学与技术学院，副教授
李继国，河海大学计算机及信息工程学院，副教授
张福泰，南京师范大学数学与计算机科学学院，教授
王　箭，南京航空航天大学信息科学技术学院，副教授
张书奎，苏州大学计算机科学与技术学院，副教授
殷新春，扬州大学信息工程学院副院长，教授
林柏钢，福州大学数学与计算机科学学院，教授
唐向宏，杭州电子科技大学通信工程学院，教授
侯整风，合肥工业大学计算机学院计算机系主任，教授
贾小珠，青岛大学信息工程学院，教授
郑汉垣，福建龙岩学院数学与计算机科学学院副院长，高级实验师

中　南

钟　珞，武汉理工大学计算机学院院长，教授
赵俊阁，海军工程大学信息安全系，副教授
王江晴，中南民族大学计算机学院院长，教授
宋　军，中国地质大学（武汉）计算机学院
麦永浩，湖北警官学院信息技术系副主任，教授
亢保元，中南大学数学科学与计算技术学院，副教授
李章兵，湖南科技大学计算机学院信息安全系主任，副教授
唐韶华，华南理工大学计算机科学与工程学院，教授
杨　波，华南农业大学信息学院，教授

内容提要

本书较系统地介绍了信息安全风险评估的基本概念、风险要素与分布、评估准则与流程、风险评估工具与基本方法，构建了信息安全风险系统综合评估模型和计算机网络空间下的风险评估模型，讨论了信息安全风险管理的原则与风险控制策略，给出了信息安全风险评估的案例和信息安全风险评估的相关标准。内容丰富、结构严谨、概念清晰、语言流畅、深入浅出、特色鲜明、启发性好，注重理论联系实际和学生应用能力培养，全书内容完整，系统性强，便于教学。

本书可作为高等院校信息安全、计算机科学与技术、通信与信息工程等专业高年级学生的教材，也可供信息安全科研院所、大型企事业单位与政府部门中从事信息安全管理工作者和工程技术人员学习参考。

序 言

21 世纪是信息的时代，信息成为一种重要的战略资源，信息的安全保障能力成为一个国家综合国力的重要组成部分。一方面，信息科学和技术正处于空前繁荣的阶段，信息产业成为世界第一大产业。另一方面，危害信息安全的事件不断发生，信息安全的形势是严峻的。

信息安全事关国家安全，事关社会稳定，必须采取措施确保我国的信息安全。

我国政府高度重视信息安全技术与产业的发展，先后在成都、上海和武汉建立了信息安全产业基地。

发展信息安全技术和产业，人才是关键。人才培养，教育是根本。2001 年经教育部批准，武汉大学创建了全国第一个信息安全本科专业。2003 年经国务院学位办批准，武汉大学又建立了信息安全的硕士点、博士点和企业博士后产业基地。自此以后，我国的信息安全专业得到迅速的发展。到目前为止，全国设立信息安全专业的高等院校已达 50 多所。我国的信息安全人才培养进入蓬勃发展阶段。

为了给信息安全专业的大学生提供一套适用的教材，武汉大学出版社组织全国 40 多所高校，联合编写出版了这套《信息安全系列教材》。该套教材涵盖了信息安全的主要专业领域，既有基础课教材，又有专业课教材，既有理论课教材，又有实验课教材。

这套书的特点是内容全面，技术新颖，理论联系实际。教材结构合理，内容翔实，通俗易懂，重点突出，便于讲解和学习。它的出版发行，一定会推动我国信息安全人才培养事业的发展。

诚恳希望读者对本系列教材的缺点和不足提出宝贵的意见。

编委会

2008 年 8 月 8 日

前 言

随着国家信息化建设的不断深入，信息已渗透到人类社会的每个缝隙，融入人们生活的每个瞬间，人们在充分享受信息社会带来的快捷、便利、高效的同时，也时刻承受着信息安全隐患带来的工作、生活及生存透明化的威胁。社会信息化水平越高，信息安全问题就越突出。信息安全已与政治安全、经济安全、国防安全等一起成为国家安全的重大战略问题。因此在信息社会中，对信息安全风险进行系统、科学、合理的评估，有着十分重要的现实意义与应用价值。只有开展有效的信息安全风险评估，才能确切地把握各类信息系统及计算机网络系统等所面临的风险，进而提出相应的安全风险控制策略，使信息安全风险处于可控范围之内。信息安全风险评估就是从风险管理角度，运用科学的方法和手段，系统地分析评估对象所面临的威胁及其存在的脆弱性，探究评估对象的风险规律，综合评估安全事件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，以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，从而为最大限度地保障网络和信息安全提供科学依据。

本书是一部介绍信息安全风险评估理论、方法与应用的教材，也是作者长期从事信息安全教学、科研及研究生教育工作的总结。本书旨在面向信息系统安全风险评估的全过程，运用系统工程中整体性、综合性、相关性、满意性等基本观点，提出一整套指导思想明确、方法体系完整、过程科学合理的系统安全风险评估理论与方法。本书涉及信息安全工程、系统工程、管理科学与工程等交叉学科的前沿研究与应用领域，给出面向信息系统与计算机网络系统的安全风险评估理论与方法，促使信息安全风险评估工作更为系统规范也更加科学合理。

本书共分为9章。在全面总结国内外先进信息系统安全风险评估理论方法的基础上，首先介绍了信息安全风险评估的基本概念、风险要素与分布、评估准则与流程、评估工具与基本方法，其次构建了信息系统风险综合评估和计算机网络空间下的风险评估模型，讨论了信息安全风险管理的原则与风险控制策略，最后给出了信息安全风险评估的案例与信息安全风险评估的相关标准。全书编写注重理论联系实际和学生实践能力的培养，力求读者能对信息安全风险评估理论与方法有全面的了解。本书写作注重思想性、系统性与科学性，在内容取舍、概念表述、方法提炼、实例选择、习题配用等方面注意反映大学课堂教学的特点与要求，便于教学组织与实施。

在本书付梓之际，要感谢海军工程大学信息安全系赵俊阁副教授，他不吝光阴审阅了全书，并提出了具体的修改建议。还要感谢信息安全系的陈泽茂博士、叶清博士、王甲生博士和朱婷婷老师在编写过程中给予的帮助。要特别感谢武汉大学出版社林莉老师在本书成稿过程中给予的支持与鼓励。限于作者的学识，书中定有不当之处，诚望读者批评指正。

作 者

2011年1月13日

目 录

第 1 章 信息安全风险评估概述 …… 1
1.1 引言 …… 1
1.2 信息安全风险评估的基本概念 …… 1
1.3 信息安全风险评估的发展与现状 …… 3
1.3.1 信息安全评估标准的发展 …… 3
1.3.2 信息安全风险评估的现状 …… 4
1.3.3 信息安全风险评估的研究热点 …… 7
1.4 教材主要内容与章节安排 …… 8
习题 1 …… 9

第 2 章 信息安全风险评估原理 …… 10
2.1 信息安全风险及其分布 …… 10
2.1.1 风险的定义 …… 10
2.1.2 信息安全风险要素 …… 10
2.1.3 信息系统安全风险分布 …… 18
2.2 信息安全风险评估准则 …… 20
2.2.1 信息安全风险评估的基本特点 …… 20
2.2.2 基于 BS 7799 标准的信息安全风险评估准则 …… 21
2.2.3 基于 BS 7799 标准的分析 …… 21
2.2.4 风险接受准则 …… 22
2.3 信息安全风险评估流程 …… 25
2.3.1 评估准备 …… 25
2.3.2 风险识别 …… 26
2.3.3 风险确定 …… 26
2.3.4 风险控制 …… 26
习题 2 …… 26

第 3 章 信息安全风险评估工具 …… 28
3.1 选择信息安全风险评估工具的基本原则 …… 28
3.2 管理型信息安全风险评估工具 …… 30
3.2.1 概述 …… 30
3.2.2 COBRA 风险评估系统 …… 30
3.2.3 CRAMM 风险评估系统 …… 31

3.2.4 ASSET 风险评估系统 …… 33
3.2.5 RiskWatch 风险评估系统 …… 33
3.2.6 其他工具 …… 34
3.2.7 常用风险评估与管理工具对比 …… 35
3.3 技术型信息安全风险评估工具 …… 35
3.3.1 漏洞扫描工具 …… 37
3.3.2 渗透测试工具 …… 38
3.4 风险评估辅助工具 …… 41
习题 3 …… 41

第 4 章 信息安全风险评估基本方法 …… 42
4.1 风险评估方法概述 …… 42
4.1.1 技术评估与整体评估 …… 42
4.1.2 定性评估和定量评估 …… 43
4.1.3 基于知识的评估和基于模型的评估 …… 43
4.1.4 动态分析与评估 …… 44
4.2 典型的风险评估方法分析 …… 45
4.2.1 风险评估方法介绍 …… 45
4.2.2 方法比较 …… 51
习题 4 …… 53

第 5 章 信息安全风险系统综合评估 …… 54
5.1 信息安全风险系统综合评估思想 …… 54
5.2 信息安全风险评估指标体系构建 …… 55
5.2.1 评估指标体系的层次结构模型 …… 55
5.2.2 信息安全风险评估指标体系建立 …… 55
5.2.3 信息系统安全风险因素的系统分析 …… 58
5.3 信息安全风险评估指标处理方法 …… 62
5.3.1 定性指标的量化处理方法 …… 62
5.3.2 定量指标的标准化处理方法 …… 66
5.4 信息安全风险评估指标权重确定方法 …… 71
5.4.1 指标权重的作用 …… 71
5.4.2 指标权重确定的基本原则 …… 72
5.4.3 指标权重的确定方法 …… 72
习题 5 …… 83

第 6 章 计算机网络下的信息安全风险评估 …… 84
6.1 相关依据 …… 84
6.1.1 NSA IAM …… 84
6.1.2 CESG CHECK …… 84
6.2 评估过程 …… 85

6.3 计算机网络空间下的风险因素 …… 86
6.3.1 计算机网络空间的构成 …… 86
6.3.2 漏洞分析 …… 86
6.3.3 攻击者分类与攻击方式分析 …… 88
6.4 计算机网络空间下的风险评估模型 …… 90
6.4.1 基本风险 …… 91
6.4.2 提升的风险 …… 92
6.4.3 整体风险 …… 93
6.4.4 风险控制 …… 94
6.5 一种面向多对象的网络化信息安全风险评估算法 …… 94
6.5.1 网络化信息安全风险分析 …… 94
6.5.2 基于广义权距离的信息安全风险评估方法 …… 95
6.5.3 算例 …… 97
习题 6 …… 98

第 7 章 信息安全风险管理 …… 99
7.1 风险管理概述 …… 99
7.1.1 风险管理的意义和基本概念 …… 99
7.1.2 风险管理的对象、角色与责任 …… 100
7.1.3 风险管理的内容和过程 …… 101
7.2 生命周期各阶段的风险管理 …… 102
7.2.1 与信息系统生命周期和信息系统安全目标的关系 …… 102
7.2.2 规划阶段的信息安全风险管理 …… 103
7.2.3 设计阶段的信息安全风险管理 …… 105
7.2.4 实施阶段的信息安全风险管理 …… 106
7.2.5 运维阶段的信息安全风险管理 …… 108
7.2.6 废弃阶段的信息安全风险管理 …… 109
7.3 信息安全风险控制策略 …… 110
7.3.1 物理安全策略 …… 110
7.3.2 软件安全策略 …… 111
7.3.3 管理安全策略 …… 112
7.3.4 数据安全策略 …… 112
习题 7 …… 113

第 8 章 信息安全风险评估案例 …… 114
8.1 信息安全保密系统介绍 …… 114
8.2 信息安全风险的模糊综合评价 …… 115
8.2.1 一级系统模糊综合评价 …… 115
8.2.2 二级系统模糊综合评价 …… 117
8.2.3 带置信因子的系统模糊综合评价 …… 118
8.2.4 基于改进模糊综合评价方法的信息系统安全风险评估 …… 120

8.2.5 案例分析 …… 124
8.3 信息安全风险评估系统设计 …… 126
8.3.1 需求分析与系统工具选择 …… 126
8.3.2 信息安全风险评估系统的结构设计 …… 126
8.3.3 信息安全风险评估系统的详细设计 …… 128
8.4 信息安全风险评估系统实现 …… 131
8.4.1 系统登录 …… 131
8.4.2 系统管理 …… 132
8.4.3 风险评估准备 …… 133
8.4.4 风险要素识别 …… 134
8.4.5 评估指标体系 …… 135
8.4.6 总体评估 …… 135

第 9 章 信息安全风险评估标准 …… 138
9.1 引言 …… 138
9.2 国际上主要的标准化组织 …… 138
9.2.1 国际标准化组织 …… 138
9.2.2 Internet 工程任务组 …… 138
9.2.3 美国标准化组织 …… 139
9.2.4 欧洲标准化组织 …… 139
9.3 BS 7799 信息安全管理实施细则 …… 139
9.3.1 BS 7799 历史 …… 139
9.3.2 BS 7799 架构 …… 141
9.3.3 BS 7799 认证 …… 144
9.4 ISO/IEC 17799 信息安全管理实施细则 …… 144
9.4.1 ISO/IEC 17799：2000 …… 144
9.4.2 ISO/IEC 17799：2005 …… 145
9.4.3 两个版本的比较 …… 145
9.5 ISO 27001：2005 信息安全管理体系要求 …… 146
9.6 CC 通用标准 …… 148
9.6.1 CC 是若干标准的综合 …… 148
9.6.2 主要内容 …… 148
9.6.3 安全要求 …… 148
9.7 ISO 13335 信息和通信技术安全管理指南 …… 149
9.8 系统安全工程能力成熟度模型 …… 150
9.8.1 安全工程过程域 …… 150
9.8.2 基于过程的信息安全模型 …… 151
9.9 NIST 相关标准 …… 154

参考文献 …… 161

第1章 信息安全风险评估概述

1.1 引言

随着信息化建设的高速发展，信息系统的应用也逐步深入社会、经济、军事发展的方方面面，已经成为政府和军队信息化建设的重要基础设施。但是各类信息系统在设计、开发及应用管理上，常存在这样与那样的不足。特别在现阶段，信息系统的核心器件与软硬件关键技术主要依赖进口，使得信息系统存在多种安全隐患与漏洞，比如通信安全隐患、物理安全隐患、软件安全隐患以及电磁泄漏等；信息系统的应用环境也易遭受黑客攻击、病毒侵袭，时常会有泄密现象发生，因此信息系统安全面临着严峻的挑战与考验。在高度网络化的条件下，制约信息系统作用发挥的关键因素已经不完全是技术问题，而是信息系统的安全及其管理问题。

近年来，信息安全风险评估的研究已经发展成为一门融合了信息安全、运筹学、管理学、社会学等综合知识的新学科。信息安全风险评估的总体目标是为了服务国家和军队信息化建设的高速发展，促进信息系统安全保障体系的建设，有效提高信息系统的安全防护能力。信息安全风险评估也成为衡量信息系统安全性的一种重要手段，进而为信息系统建设以及管理决策等提供了非常重要的依据。

本教材着重介绍信息安全风险评估原理、技术手段、基本方法、系统综合评估方法、计算机网络下的信息安全风险评估以及风险控制策略的制定、信息安全风险评估软件系统的设计与实现等方面的理论与方法。期望读者通过对本书的学习，能正确认识信息系统面临的各种安全风险，准确把握其系统安全状况，提高信息安全保障能力。

1.2 信息安全风险评估的基本概念

1. 信息安全

信息安全是指信息的保密性（Confidentiality）、完整性（Integrity）和可用性（Availability）的保持。其最早产生于军事通信需求，而后逐渐发展成一门学科，由最初的通信安全（COMSEC）、计算机安全（COMPSEC）、信息安全（INFOSEC），发展到了信息保障（IA）阶段。在信息保障的概念下，安全已经作为一个过程来看待，不但有保护、检测、响应、恢复等环节，还包括信息系统安全工程（ISSE）、应急响应、安全管理、教育培训、法律法规等支撑部分。信息安全的一切研究和实践都希望能以可度量的准则或可信度作为结果的评价指标，从而直接导致信息安全评估、认证和信息安全标准的产生。

2. 信息系统

信息系统是指用于采集、处理、存储、传输、分发和部署信息的整个基础设施、组织结

构、人员及组件的总和。根据《中华人民共和国计算机信息系统安全保护条例》中的定义，信息系统是指由计算机及其相关和配套的设备、设施（含网络）构成，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。

3. 信息系统安全

信息系统安全是指确保信息系统结构安全、与信息系统相关的元素安全以及与此相关的各项安全技术、安全服务和安全管理的总和。从系统工程的角度看，信息系统安全就是信息在存储、处理、集散和传输过程中，保持其机密性、完整性、可用性、可追溯性和抗抵赖性等能力与作用的发挥的系统辨识及控制策略实施过程。

随着 Internet 技术的普及，其组网技术的开放互连性给人类带来信息资源充分共享潜在能力的同时，也为外部世界非授权进入局域网信息系统、非授权获取与窃取相关信息资源等提供了机会。在当今大规模开放互连网络环境下，即使采取相对完善的安全保护措施，信息系统的安全风险依然存在。信息系统组件本身固有的脆弱性和设计上的缺陷等是系统不安全的客观因素；在信息系统运行过程中，内部的操作不当、管理不严等所造成的系统漏洞则是导致信息系统不安全的主观原因。因而，信息系统的安全风险是由人为或自然的威胁与攻击，直接或间接地利用系统脆弱性和漏洞等所造成的不确定性事件及其后果。随着信息系统的逐渐普及，一旦风险事件发生，对信息系统的管理者、使用者、社会和国家等都将造成损失，甚至产生重大影响。如何有效预防和控制风险事件的发生，从安全角度保障信息系统正常、有序和持续性运行，合理地利用现有资源获取最大的社会和经济效益，是信息系统安全领域所面临的重大研究课题。

4. 信息安全风险评估

信息安全风险评估是指依据有关信息安全技术标准和准则，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全面、科学的分析和评价的过程。信息安全风险评估将对信息系统的脆弱性、信息系统面临的威胁以及脆弱性被威胁源利用后所产生的实际负面影响进行分析、评价，并将根据信息安全事件发生的可能性及负面影响的程度来识别信息系统的安全风险。

通过系统周密的风险分析与评估，可以导出信息系统风险的安全需求，实现信息系统风险的安全控制，从而建立一个可靠、有效的风险控制体系，保障信息系统的动态安全。因此，信息系统安全风险评估是建立信息安全保障体系的必要前提，目前正越来越受到人们的重视。信息系统安全评估依其应用环境、应用领域以及处理信息敏感度的不同，安全需求上有很大差别。但概括起来，信息安全风险评估具有如下作用：

其一，明确信息系统的安全现状：进行信息系统安全风险评估后，可以准确地了解系统自身的网络、各种应用系统以及管理制度规范的安全现状，从而明晰安全需求。

其二，确定信息系统的主要安全风险：在对信息系统进行安全风险评估后，可以确定信息系统的主要安全风险，并选择合理的风险控制策略，以避免风险或降低风险。

其三，指导信息系统安全技术体系与管理体系的建设：进行信息系统安全风险评估后，可以制定信息系统的安全策略及安全解决方案，从而指导信息系统安全技术体系（如部署防火墙、入侵检测与漏洞扫描系统、防病毒系统、数据备份系统等）与管理体系（如安全管理制度、安全培训机制等）的建设。

1.3 信息安全风险评估的发展与现状

1.3.1 信息安全评估标准的发展

1. 国外信息安全风险评估标准的发展

国内外关于信息系统安全体系结构理论的研究已有二十多年的历史，1985年美国国防部正式公布的DOD5200.28-STD《可信计算机系统评估准则》（TCSEC，从橘皮书到彩虹系列）是公认的第一个计算机信息系统评估准则。受该准则的影响和信息处理技术发展的需要，法国、英国、荷兰、加拿大等IT发达国家纷纷建立了自己的信息系统安全评估准则、认证机构和风险评估认证体系，负责研究并开发相关的评估标准、评估认证方法与评估技术，并进行基于评估标准的信息安全评估和认证（包括信息系统安全风险评估）。随着信息安全的内涵不断延伸，信息系统安全风险评估也从单一的通信保密向网络化信息的完整性、可用性、可控性等方面拓展，取得了大量研究成果。

1985年，《可信计算机系统安全评估准则》由美国国防部为适应军用计算机的保密需要而制定，其后又对网络系统、数据库等方面作出了系列安全解释，形成了信息系统安全体系结构的最早原则。至今美国已研制出满足TCSEC要求的安全系统（包括安全操作系统、安全数据库、安全网络部件）多达百余种，而TCSEC标准把系统的保密性作为讨论的重点，忽略了信息的完整性与可用性等安全属性，因而这些系统有相当大的局限性，同时也没有真正达到形式化描述和证明的可信水平。

20世纪90年代初，法、英、荷、德四国针对TCSEC准则只考虑保密性的局限，联合提出了包括信息的机密性、完整性、可用性等安全属性概念的“信息技术安全评价准则”（ITSEC，欧洲白皮书）。ITSEC把可信计算机的概念提高到可信信息技术的高度上来认识，对国际信息安全的研究、实施产生了深刻的影响。但是该标准也同样没有给出形式化描述的理论证明。

1996年，美、加、英、法、德、荷六国联合提出了信息技术安全评估的通用准则（Common Criteria，CC），并逐渐形成国际标准ISO15408。该标准定义了评价信息技术产品和系统安全性的基本准则，提出了目前国际上公认的表述信息技术（或系统）安全性的结构，也被认为是第一个信息技术安全评价的国际标准，它的发布对信息安全工作的深入开展具有重要意义，是信息技术安全评价标准以及信息安全技术发展的一个重要里程碑。但该标准的风险评估准则是针对产品与系统的安全性能测试和等级评估，事先假定用户知道安全需求，忽略了对信息系统的安全风险分析，缺少综合解决保障信息系统多种安全属性的理论模型依据。

英国1995年提出的本国的信息安全管理体系标准BS7799，是国际上具有代表性的信息安全管理体系标准。它用管理加技术的方式全面保障信息的保密性、完整性和可用性，BS7799主要提供了有效地实施IT安全管理的建议，给出了安全管理的方法和程序。国际标准化组织（ISO）于2000年12月在此基础上制定并通过了ISO/IEC 17799，它主要采用系统工程的方法保护信息安全，即确定信息安全管理的方针和范围，在风险评估的基础上选择适宜的控制目标与控制方式进行控制，制定业务持续性计划，建立并实施信息安全管理体系。

另外，1996年12月15日开始发布的ISO13335标准，给出了关于IT安全的机密性、完整性、可用性、审计性、真实性、可靠性六个方面的含义，并提出了基于风险管理的安全模型。该模型阐述了信息安全评估的思路，对企业的信息安全评估工作具有指导意义，但该标准缺乏对系统资源分布的结构化分析和风险分布与强度的形式化描述，无法给出系统风险的

可信量化评估。2000 年 9 月美国国家安全局为促进美国政府信息系统安全需求的协调，在综合工业界/政府联合信息保障技术框架论坛中的各类合作成果的基础上，推出了《信息保障技术框架（IATF）》3.0 版。该技术框架提出了纵深保卫战略的概念，并围绕该概念对信息系统进行建设和保护，但它仅起到对安全需求的协调和安全解决方案的建议作用，并没有对一个信息系统提供完整的安全解决方案的技术框架和技术路线进行描述。

2. 我国信息安全风险评估标准的发展

我国是国际标准化组织的成员国，国内信息安全标准的制定工作始于 20 世纪 80 年代中期，主要是等同采用国际标准。国内信息安全标准化工作与国际已有的成果相比较，其覆盖面还非常有限，宏观和微观的指导作用也有待于进一步的提高。

1998 年 10 月经国家质量技术监督局授权成立了中国国家信息安全测评认证中心（CNITSEC），它是代表国家对信息技术、信息系统、信息安全产品以及信息安全服务的安全性实施公正评价的技术职能机构。另外，国家标准 GB17895—1999《计算机信息系统安全保护等级划分准则》正式颁布实施。2002 年 4 月 15 日全国信息安全标准化技术委员会（简称信息安全标委会，TC260）在北京正式成立，其工作任务是向国家标准化委员会提出本专业标准化工作的方针、政策和技术措施的建议，同时将协调各有关部门，提出一套系统、全面、分布合理的信息安全标准体系，进而依此开展信息安全标准的制定工作。2002 年 9 月在国家信息中心信息安全处的基础上，组建成立了国家信息中心信息安全研究与服务中心，该中心参与完成了国家标准《信息安全技术评估准则》，参加了《国家电子政务指南——信息安全》编写和公安部相关标准的编写与评审。2006 年，国信办[2006]5 号文件制定了《国家网络与信息安全协调小组关于开展信息安全风险评估工作的意见》，等等。另外，制定了一系列涉及开放系统安全框架的国家标准，如访问控制框架（GB/T18794.3—2003）、抗抵赖框架（GB/T18794.4—2003）、机密性框架（GB/T18794.5—2003）、完整性框架（GB/T18794.6—2003）、安全审计和报警框架（GB/T18794.7—2003），还制定了 GB17859-1999《计算机信息系统安全保护等级划分准则》及 GJB4484—2003《军队计算机网络信息系统安全保密要求》，2007 年 6 月发布了 GB/T20984—2007《信息安全技术——信息安全风险评估规范》、GB/T20988—2007《信息安全技术——信息系统灾难恢复规范》，2008 年发布了 GB/T22240—2008《信息安全技术——信息系统安全等级保护定级指南》，等等。

由上可知，现有的信息安全评估标准虽然都强调了风险评估的必要性，要求以系统的风险分析为核心，通过评估系统的安全属性来判断信息系统的安全等级是否符合要求，但这些标准及其方法，通常采用问卷式调查给出不同风险域在安全管理方面存在的漏洞和安全等级，进而给出策略建议，这将使对于信息系统风险分布规律的认识大多停留在专业人员和专家的个人认识上，缺乏系统性和客观性；且风险评估的量化也缺乏可操作的工程数学方法，评估结果在系统性与准确性方面还存在较大的主观偏好。尽管如此，现有的信息安全评估标准还是为人们进行信息安全风险评估提供了实用的风险分析程序与风险评估准则，即为人们开展信息安全风险评估工作提供了必要的基础。

1.3.2 信息安全风险评估的现状

信息安全风险评估就是要运用系统工程的理论与方法，结合信息系统自身的特点，借助于信息系统安全相关标准开展工作。

信息安全风险评估方法的选择，解决了评估所采集信息和风险评估结果的对应问题。在