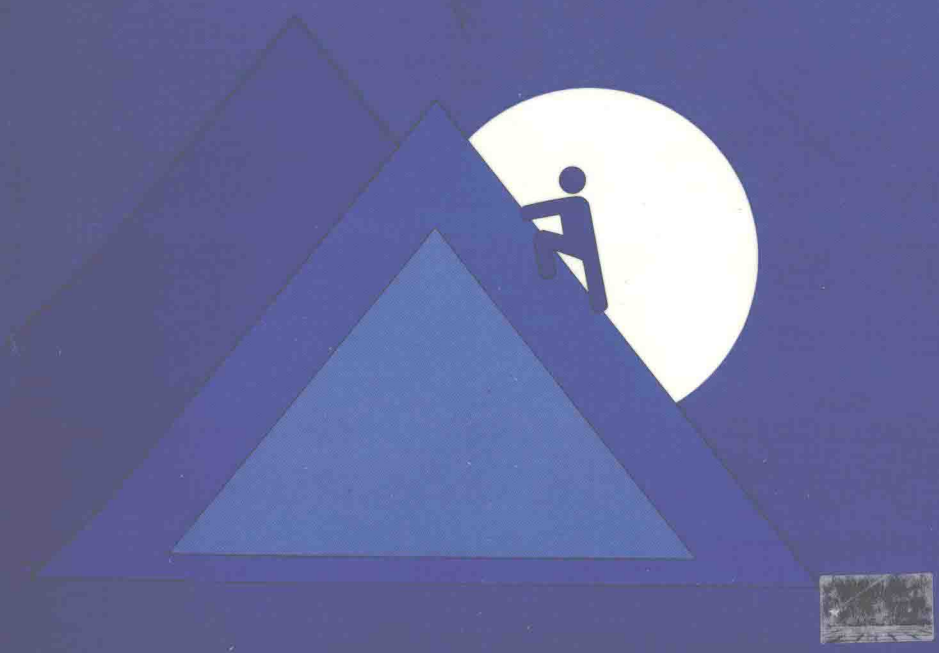
卡内基·梅隆大学软件工程丛书

PEARSON
Addison Wesley

信息安全管理（影印版）

Managing Information Security Risks: The OCTAVE℠ Approach

[美] 克里斯多夫·阿尔伯兹（Christopher Alberts）
奥黛莉·多诺菲（Audrey Dorofee）著



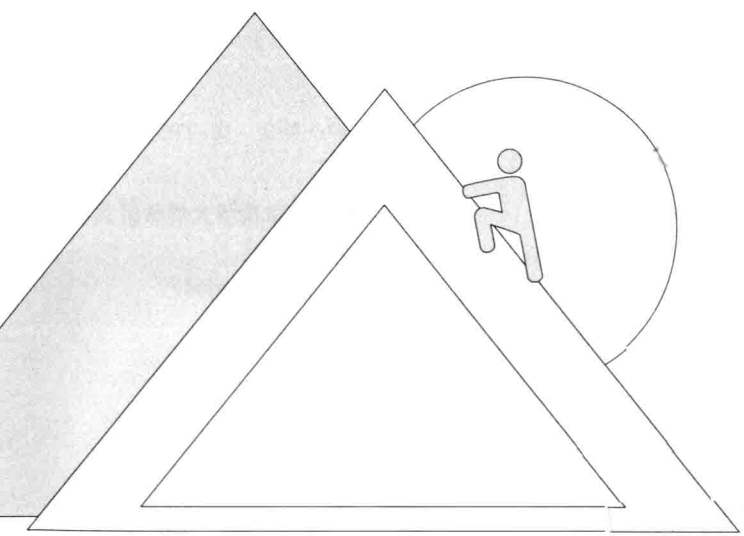
清华大学出版社

卡内基·梅隆大学软件工程丛书

信息安全管理（影印版）

Managing Information Security Risks: The OCTAVE℠ Approach

[美] 克里斯多夫·阿尔伯兹（Christopher Alberts）
奥黛莉·多诺菲（Audrey Dorofee）著



清华大学出版社
北京

图书在版编目（CIP）数据

信息安全管理＝Managing Information Security Risks: The OCTAVE[SM] Approach / （美）阿尔伯兹，（美）多诺菲著. —影印本. —北京：清华大学出版社，2003
（卡内基·梅隆大学软件工程丛书）
ISBN 7-302-07045-8
Ⅰ. 信… Ⅱ. ①阿… ②多… Ⅲ. 信息系统－安全技术－英文 Ⅳ. TP309
中国版本图书馆 CIP 数据核字（2003）第 070071 号

出 版 者：清华大学出版社　　**地　　址**：北京清华大学学研大厦
http://www.tup.com.cn　　**邮　　编**：100084
社 总 机：010-62770175　　**客户服务**：010-62776969

文稿编辑：李　强
封面设计：立日新设计公司
印 刷 者：世界知识印刷厂
发 行 者：新华书店总店北京发行所
开　　本：148×210　**印张**：16.5　**插页**：1
版　　次：2003 年 8 月第 1 版　2003 年 8 月第 1 次印刷
书　　号：ISBN 7-302-07045-8/TP·5179
印　　数：1～3000
定　　价：39.00 元

出 版 说 明

1984 年，美国国防部出资在卡内基·梅隆大学设立软件工程研究所(Software Engineering Institute，简称 SEI)。SEI 于 1986 年开始研究软件过程能力成熟度模型（Capability Maturity Model，CMM)，1991 年正式推出了 CMM 1.0 版，1993 年推出 CMM 1.1 版。此后，SEI 还完成了能力成熟度模型集成（Capability Maturity Model Integration，简称 CMMI)。目前，CMM 2.0 版已经推出。

CMM 自问世以来备受关注，在一些发达国家和地区得到了广泛应用，成为衡量软件公司软件开发管理水平的重要参考因素，并成为软件过程改进的事实标准。CMM 目前代表着软件发展的一种思路，一种提高软件过程能力的途径。它为软件行业的发展提供了一个良好的框架，是软件过程能力提高的有用工具。

SEI 十几年的研究过程和成果，都浓缩在由 SEI 参与研究工作的资深专家亲自撰写的卡内基·梅隆大学软件工程丛书（SEI Series In Software Engineering）中。

为增强我国软件企业的竞争力，提高国产软件的水平，清华大学出版社全面引进了这套丛书，分批影印和翻译出版，这套丛书采取开放式出版。不断改进，不断出版，旨在满足国内软件界人士学习原版软件工程高级教程的愿望。

清华大学出版社

卡内基·梅隆大学软件工程丛书

编 委 会 名 单

总　序

周伯生

美国卡内基•梅隆大学软件工程研究所（CMU/SEI）是美国联邦政府资助构建的研究单位，由美国国防部主管。他们确认，为了保证软件开发工作的成功，由软件开发人员、软件采办人员和软件用户组成的集成化团队必须具有必要的软件工程知识和技能，以保证能按时向用户交付正确的软件。所谓“正确的”就是指在功能、性能和成本几个方面都能满足用户要求且无缺陷；所谓“无缺陷”就是指在编码后对软件系统进行了彻底的穷举测试修复了所有的缺陷，或保证所编写的代码本身不存在缺陷。

CMU/SEI 为了达到这个目的，提出了创造、应用和推广的战略。这里的“创造”是指与软件工程研究社团一起，共同创造新的实践或改进原有的实践，而不墨守成规。这里的“应用”是指与一线开发人员共同工作，以应用、改进和确认这些新的或改进的实践，强调理论联系实际。这里的“推广”是指与整个社团一起，共同鼓励和支持这些经过验证和确认的、新的或改进的实践在世界范围内的应用，通过实践进行进一步的检验和提高。如此循环，往复无穷。

他们把所获得的成就归纳为两个主要领域。一个是倡导软件工程管理的实践，使软件组织在采办、构建和改进软件系统时，具有预测的能力与控制质量、进度、成本、开发周期和生产效率的能力。另一个是改进软件工程技术的实践，使软件工程师具有分析、预测和控制软件系统属性的能力，其中包括在采办、构建和改进软件系统时，能进行恰当的权衡，作出正确的判断和决策。CMU/SEI 通过出版软件工程丛书，总结他们的研究成果和实践经

验，是推广这两个领域经验的重大举措。

卡内基·梅隆大学软件工程丛书由 CMU/SEI 和 Addison-Wesley 公司共同组织出版，共分 4 个部分：计算机和网络安全（已出版了 2 本著作），工程实践（已出版了 8 本著作），过程改进和过程管理（已出版了 11 本著作），团队软件过程和个体软件过程（已出版了 3 本著作）。前两者属于软件工程技术实践，后两者属于软件工程管理实践。目前这 4 个部分共出版了 24 本著作，以向软件工程实践人员和学生方便地提供最新的软件工程信息。这些著作凝聚了全世界软件工程界上百位开拓者和成千上万实践者的创造性劳动，蕴含了大量的宝贵经验和沉痛教训，很值得我们学习。

清华大学出版社邀请我和郑人杰教授共同组织卡内基·梅隆大学软件工程译丛编委会。清华社计划首先影印 6 本著作，翻译出版 15 本著作。据我所知，在 Addison-Wesley 公司出版的 SEI 软件工程丛书中，人民邮电出版社已经翻译出版了《个体软件过程》和《团队软件过程》，还拟影印出版《个体软件过程》和《软件工程规范》；电子工业出版社已经翻译出版了《净室软件工程的技术与过程》、《能力成熟度模型 CMM 1.1 指南》、《能力成熟度模型集成 CMMI》和《软件项目管理》；北京航空航天大学出版社已经翻译出版了《统计过程控制》。这些出版社共计影印 2 本著作，翻译出版 7 本著作。这样，可以预期我国在今年年底共可影印 8 本著作，翻译出版 22 本著作。各个出版社的有远见的辛勤劳动，为我们创造了“引进、消化、吸收、创新”的机遇。我们应该结合各自的实践，认真学习国外的先进经验，以大大提高我国软件工程的理论和实践水平。

在这套丛书中，特别值得一提的是，在过程工程领域被誉为软件过程之父的 Humphrey 先生所撰写的《软件过程管理》、《技术人员管理》、《软件工程规范》、《个体软件过程》、《团队软件过程》和《软件制胜之道》等 6 本著作，将于今年年内全部翻译出

版，其中《软件过程管理》、《技术人员管理》、《软件工程规范》、《个体软件过程》和《软件制胜之道》等 5 本著作亦已经或将于今年年内影印出版。

《软件过程管理》是软件过程领域的开创性著作，是为软件公司经理和软件项目经理撰写的。用这本书提出的原理来指导软件开发，可以有效地按照预定进度得到高质量的软件，同时还可了解如何持续进行过程改进。美国 CMU/SEI 按照这本书提出的原理开发了能力成熟度模型，在国际上得到绝大多数国家的认可和广泛采用，是改进软件过程能力的有力武器。在信息技术迅速发展和企业激烈竞争的今天，能否持续改进过程往往决定企业的命运。

作为一个软件经理，在改进组织的能力之前，首先必须明确绝大多数软件问题是由管理不善所引起的。因此，要改进组织的性能，首先需要改进自己的管理模式。同时还要认识到软件开发是一项智力劳动，需要拥有掌握高技能和忘我工作的技术人员。因此，有效的软件管理需要充分注意技术人员的管理。

《技术人员管理》这本著作就是为达到这个目的而撰写的。高质量的技术工作要求没有差错，这就要求人们高度专心和高度献身。因此要求人们对他所从事的工作不仅具有高度的责任感，而且具有浓厚的兴趣和高度的热忱。在当前知识经济群龙相争的今天，一个能激励人们进行创造性工作的领导群体，是众多竞争因素中最重要的因素。本书提供了大量的实用指南，可用来有效地改进工程人员、经理和组织的性能。

Humphrey 先生还认为这本书特别适合于在我国工作的软件经理。我国是一个人口大国，拥有大量能干的知识分子，而且信息领域的劳动力价格比国际市场的价格要低，因此吸引了许多国家到我国来投资。但若不提高人员的素质，不在产品质量和进度方面也狠下功夫，就不能在这方面持续保持优势。

《软件工程规范》是为编程人员撰写的。它精辟地阐述了个体软件过程（PSP）的基本原理，详尽地描述了人们如何来控制自己的工作，如何与管理方协商各项安排。在软件工程界，这本著作被誉为是软件工程由定性进入定量的标志。目前在世界范围内，有成千上万的软件工程技术人员正在接受有关 PSP 的培训，以便正确地遵循 PSP 的实践、开发和管理工作计划，在他们承诺的进度范围内，交付高质量的产品。

《软件制胜之道》这本著作描述了团队软件过程的基本原理，详尽地阐述了在软件组织中如何应用 PSP 和 TSP 的原理以及它所能带来的效益。此外，虽然 CMM 同样适用于小型组织，但在其他著作中都没有描述如何应用 CMM 于个体或小型团队，这本书填补了这个空白。应该指出，如果一个组织正在按照 CMM 改进过程，则 PSP 和 TSP 是和 CMM 完全相容的。如果一个组织还没有按照 CMM 改进过程，则有关 PSP 和 TSP 的训练，可以为未来的 CMM 实践奠定坚实的基础。

在软件工程技术实践方面目前共出版了 10 本著作，其中《用商业组件构建系统》、《软件构架实践》和《软件构架评估——方法和案例研究》等 3 本著作详尽地阐述了软件构架的构建、实践和评估。鉴于是否有一个稳定的软件构架，对软件的质量和成本影响很大，因此如何获得一个良好的构架就成为当今软件界研究的重点。我相信这几本著作的出版，将对我国软件构架领域的研究与实践有重要的参考价值。此外，众所周知，计算机与网络的安全问题对信息系统的可靠使用关系极大，《CERT 安全指南——系统与网络安全实践》的出版将会对我国在这一领域的研究和实践起积极的促进作用。《风险管理——软件系统开发方法》、《软件采办管理——开放系统和 COTS 产品》、《项目管理原理》、《软件产品线——实践和模式》和《系统工程：基于信息的设计方法》等 5 本著作，分别从风险管理、软件采办、项目管理、软件产品线以及信息系统设计方法等几个方面阐述了大型、复杂软件系统

的开发问题，是有关发展软件产业的重要领域，很值得我国软件产业界借鉴。

目前我们所处的时代是信息化时代，是人类进入能够综合利用物质、能量和信息三种资源的时代。千百年来以传统的物质产品的生产、流通、消费为基本特征的物质型经济，将逐步进入以信息产品的生产、流通、利用和消费为基本特征的知识型经济。在这个历史任务中，建造和广泛应用各类计算机应用系统是其公共特征。计算机软件是计算机应用系统的灵魂，没有先进的软件产业，不可能有先进的信息产业，从而也不可能建成现代化的知识型经济。

我们应该看到，在软件领域中我国在总体上离世界先进水平还有相当大的差距。但是，我们不能跟随他国的脚印，走他人的老路。我们应该抓住机遇，直接针对未来的目标，在软件工程技术和软件工程管理两个方面，注意研究卡内基·梅隆大学软件工程丛书中倡导的原理和方法，联系实际，认真实践，并充分利用我国丰富优秀的人力资源和尊重教育的优良传统，大力培养各个层次的高质量的软件工程人员，使其具有开发各类大型、复杂软件系统的能力。我衷心地预祝清华大学出版社影印和翻译出版这套丛书，在把我国建设成为一个真正现代化的软件产业大国的历史任务中起到推波助澜的作用，并请读者在阅读这些译著时，对这套丛书的选题、译文和编排等方面都提出批评和建议。

周伯生

于北京

2002 年 8 月 18 日

前　言

在谈到信息安全问题时，很多人似乎都在寻求一种犀利的工具。他们通常希望通过购买最新的工具或技术解决所面临的问题。几乎没有一个组织在选择方案之前，会从组织的角度去评估他们实际上试图保护什么（以及原因）。在从事信息安全领域的工作中，我们已经发现安全问题变得越来越复杂，并且很少能够仅用一种技术就解决这些问题。大多数安全问题深深地植根于一个或者多个组织和业务问题中。在实施安全方案之前，应当通过在业务环境中评估安全需求和风险，刻画出基本问题的真实本质。

想想当前使用的各种各样的安全评估方法及其局限性，在试图选择一种合适的方法来评估信息安全风险时，极易产生困惑。当前所用的大多数方法都是“自下而上”的方法：它们都从计算基础结构开始，强调技术弱点，不考虑组织的任务和业务目标的风险。一种更好的方法是着眼于组织本身识别出需要保护的东西、确定它为什么存在风险，并开发出技术和实践相结合的解决方案。

一种综合的信息安全风险评估方法应满足如下条件：

- 结合资产、威胁和弱点。
- 使得决策者能够根据对组织重要的内容制定相对的优先级。
- 结合与员工如何使用计算基础结构来实现组织的业务目标相关的组织问题。
- 结合与计算基础结构的配置相关的技术问题。

- 应该是一种能够根据每个组织的需要进行惟一剪裁的灵活方法。

建立一种上下文敏感的评估方法的方式是，为评估定义一个基本的需求集，然后开发一系列满足那些需求的方法，即一个方法族。方法族中的每种方法可以针对一种惟一的业务环境或者情况。我们构想了可操作的关键性威胁、资产和弱点评估（Operationally Critical Threat,Asset,and Vulnerability Evaluation[SM]，简称 OCTAVE[SM]）项目[①]，以定义一种系统的、组织范围内的评估信息安全风险的方法，它包括多种与方法族一致的方法。我们还将这种方法设计成自主型，以使人们能够学习安全问题和改善其组织的安全状况，而无须不必要地依赖于外部专家和厂商。

评估本身仅提供了组织信息安全活动的方向。除非组织实现了评估结果并管理其信息安全风险，否则不会实现实质性的改进。OCTAVE 是进行信息安全风险管理的重要的第一步。

OCTAVE 的历史

在开发 OCTAVE 之前，我们在专家的领导下对组织进执行了信息安全评估（Information Security Evaluation，简称 ISE）。一组安全专家将访问一个站点、与选定的信息技术人员和关键系统的用户进行会谈，并检查选用的计算基础结构的技术弱点。评估人

---

① [SM]Operationally Critical Threat, Asset, and Vulnerability Evaluation 和 OCTAVE 都是卡内基·梅隆大学的服务标记。OCTAVE 由 CERT 协调中心（CERT Coordination Center，简称 CERT/CC）开发。OCTAVE 建立于 1988 年，是现有的最老的计算机安全反应小组。该中心既警告安全性受到威胁的 Internet 站点，又提供工具和技术，以使典型的用户的管理员能够有效地保护系统不受侵入者的破坏。CERT/CC 的总部是软件工程研究所（Software Engineering Institute，简称 SEI），这是一个由联邦政府提供基金并由卡内基·梅隆大学运作的研发中心，有着改进软件工程实践的广泛授权。

员运用他们的专业知识建立一个关于组织和技术弱点（脆弱性）的列表。一个站点的管理人员接到该弱点列表及其对应的建议时，他们通常并不知道如何着手克服这些弱点。他们首先应当处理哪些问题，是组织问题还是技术问题？在资金和人员受到限制的情况下，最重要的 5 个问题是什么？这些问题问得很好。遗憾的是，如果仅检查弱点，就很难确立正确的指导原则。在着手确立重点问题之前，需要在组织试图实现什么的环境下对弱点进行研究。

除了在弱点评估方面的经验外，我们还开发和应用了各种软件开发风险评估和管理技术『Williams 00 和 Dorofee 96』。这些技术重点强调了可能影响项目目标的关键性风险。

借助于这些经验，我们决定重点关注基于风险的方法，而不是基于弱点的方法。基于风险的方法能够帮助人们理解信息安全如何影响其组织的任务和业务目标、确立哪些资产对于组织是重要的以及它们的风险程度。于是，就可以在这种风险信息的环境下执行弱点评估了。因为信息安全风险与组织的任务和业务目标相联系，所以在评估时除了包含技术人员外还必须包含业务人员。

在进行弱点评估期间，我们观察到的另一个重要问题涉及一个给定的站点的参与程度，以及随后对建成后的站点的所有权。因为弱点评估高度依赖于评估人员的专业知识，所以评估过程中涉及的站点人员的参与非常少。当我们能够返回站点时，每次访问都会看到同样的弱点。几乎没有或者根本没有组织学习可言。这些组织中的成员没有感觉到对各种评估结果的“所有权”，因此还没有实施评估结果。我们决定站点需要更深入地参与安全评估，以便了解它们的安全过程并参与制定改进建议。我们已开始开发一种自主的评估方法，这种方法：

- 强调信息资产的风险；
- 强调基于实践的风险缓和措施，采用公认的、良好的安

全实践[①]；

- 包含业务人员和信息技术部门的人员；
- 在评估的所有方面包括一个站点成员；

1999 年 6 月，我们公布了一个描述 OCTAVE 框架『Alberts 99』的报告，这是一种信息安全风险评估规范。它被细化为 OCTAVE Method『Alberts 01a』，这是专为大型组织开发的。此外，我们正在开发一个针对小型组织的方法。在进行这些工作期间，我们得出 OCTAVE 框架不能充分地捕获我们想要的自主型信息安全风险评估的通用方法或需求。我们把该框架细化为 OCTAVE 标准『Alberts 01b』，即一系列定义 OCTAVE 方法的原则、特征和结果。

本书内容

本书主要讨论信息安全风险评估的 4 个主要方面：

定义了一种自主的信息安全风险评估方法（OCTAVE 标准）；

说明了如何在组织中使用 OCTAVE Method 实现评估方法；

说明了如何剪裁 OCTAVE Method 以适应不同类型的组织；

描述了这种方法如何奠定了信息安全风险管理的基础；

为了解决这些关键性问题，我们将本书的内容分成 3 部分：

第Ⅰ部分，引言，概述了 OCTAVE 方法，提出了自主的信息安全风险评估的原则、特征和结果。

第Ⅱ部分，OCTAVE Method，说明了一种能够在组织中实现 OCTAVE 方法的方法。本部分以 OCTAVE Method 的“要点综述”

[①] 实践目录中的实践（附录 C）取自几种安全性实践来源，包括 CERT/CC、英国标准学会（British Standards Institute）、美国国家标准和技术学会（National Institute of Standards and Technology）和政府法规。

开始，然后详细介绍了该方法。

第Ⅲ部分，OCTAVE Approach 的变体，描述为不同的组织类型剪裁 OCTAVE Method 以满足它们的需要的思想。本部分还介绍了与评估后的信息安全风险管理有关的基本概念。

本书最后有 3 个附录，它们补充了正文部分提供的材料。

附录 A 提供了 OCTAVE 场景示例的一个样本最终报告。

附录 B 说明了 OCTAVE Method 的工作表和说明书。

附录 C 列出了一个实践目录（一个常用的良好安全实践的结构化集合）。

本书的读者对象

本书适合于各种各样的读者。了解安全问题对阅读本书会有好处，但并非基本要求；我们将在所有的概念和术语出现时对它们进行定义。本书既能满足初次接触安全性的读者的需要，也能满足安全风险管理专家的需要。

信息安全风险评估适用于任何使用联网的计算机进行业务，因此可能会存在关键信息资产风险的人。本书适合那些需要执行信息安全风险评估的人，以及那些对用一种自主的方法解决组织和信息技术问题感兴趣的人。那些关心和负责保护关键信息资产的经理、职员和信息技术人员都会发现本书的价值。

此外，那些为其他组织提供信息安全服务的顾问，也会对研究如何在他们现有的产品和服务中结合进 OCTAVE Method 方法或 OCTAVE Method 感兴趣。信息安全风险评估产品和服务的客户可以运用 OCTAVE 方法的原则、特征和结果来理解是什么构成了评估信息安全风险的综合方法。客户还可以使用这些原则、特征和结果作为选择厂商和顾问提供的产品和服务的基准。

OCTAVE Method 要求一个涵盖各专业的综合分析团队来执行评估，并担当安全改进工作的核心。因此，任何有可能成为分析团队中的一员或与他们合作的人，都是本书的主要读者。本书既提供了进行评估的详细指导信息，也提供了与评估后进行风险管理有关的概念。对于一个风险分析团队，整本书的内容都是适用的。

那些需要理解 OCTAVE 方法的人应当阅读第 I 部分。那些仅仅需要 OCTAVE Method 的综述和大致了解可能会如何使用的人，应当阅读第 1 章和第 3 章。那些已经在执行信息安全风险评估并寻求其他改进思路的人，应当首先阅读第 1 章和第 3 章，然后决定需要深入研究哪个领域。那些准备开始研究如何在其组织中执行自主的信息安全评估的人，应当阅读本书的第 II 部分。最后，那些对自定义 OCTAVE Method 感兴趣或者想了解评估后的工作的人，应当阅读第III部分。

致　谢

著书需要付出艰辛的劳动。在此，谨向为本书写作提供过帮助的每一个人致以衷心的感谢。没有他们的帮助，拙作至今不可能顺利面世。

感谢参与本书审阅并提供极有价值的反馈意见的工作人员：Julia Allen, Rich Caralli, Jeff Collmann, Carol A.Sledge, Andrew Moore, William Wilson 和 Carol Woody。

我们要特别感谢 Rich Pehtia，联网系统生存规划的规划经理，和 William Wilson，生存企业管理组的技术经理，感谢他们对我们工作的鼓励和大力支持。同时，我们还要感谢管理部门的坚定支持和帮助。

感谢为本书技术内容作出贡献的众多人员。需特别提出的是：

Julia Allen 帮我们编排了实践目录；Rich Caralli 提供了使用 OCTAVE 的不足之处；Jeff Collmann 对我们早期的原型作出了富有洞察力的详细评论；Bradford Willke 对 OCTAVE 的技术性的内容作出了重要贡献。

我们也非常感谢那些为本书出版作出贡献的人们。Linda Pesante 协助设计并担任了技术编辑；David Biber 提供了全书使用的多数图表。

书中技术内容是对软件工程研究所以前的研究成果的总结。我们综合了许多项目的技术资料。包括连续性风险管理、软件风险评估、信息安全评估及 OCTAVE 框架的早期工作。许多人对这些项目都付出了辛勤劳动，我们感谢他们本书奠定了坚实的基础。

我们也要感谢所有给“OCTAVE”的研发提供资金和实验机会的组织。

最后，要感谢爱妻 Carol Feola，感谢她不断的支持和鼓励，致使我能够忍受撰书的种种挫折。从开始撰写到本书面世以及最后的审定，她都给予了难以置信的耐心帮助。