注册信息安全专业人员
资质认证培训教材

信息安全工程与管理

中国信息安全产品测评认证中心 编著

- 由信息安全专家精心编写与认真审校
- 全面覆盖了信息安全学科的知识要点
- 信息安全人员资质权威认证专业教材

人民邮电出版社
POSTS & TELECOM PRESS

注册信息安全专业人员
资质认证培训教材

信息安全工程与管理

中国信息安全产品测评认证中心 编著

人民邮电出版社

图书在版编目（CIP）数据

信息安全工程与管理/中国信息安全产品测评认证中心编. —北京：人民邮电出版社，2003.9
注册信息安全专业人员资质认证培训教材

ISBN 7-115-11514-1

I. 信… II. 中… III. 信息系统—安全技术—技术培训—教材 IV. TP309

中国版本图书馆 CIP 数据核字（2003）第 067025 号

注册信息安全专业人员资质认证培训教材

信息安全工程与管理

◆ 编　　著　中国信息安全产品测评认证中心
责任编辑　杨　璐

◆ 人民邮电出版社出版发行　北京市崇文区夕照寺街 14 号
邮编　100061　电子函件　315@ptpress.com.cn
网址　http://www. ptpress.com.cn
读者热线　010-67132692
北京汉魂图文设计有限公司制作
北京鸿佳印刷厂印刷
新华书店总店北京发行所经销

◆ 开本：787×1092　1/16
印张：18.75
字数：446 千字　　2003 年 9 月第 1 版
印数：1-4 000 册　　2003 年 9 月北京第 1 次印刷

ISBN7-115-11514-1/TP・3554

定价：32.00 元

内容提要

本书主要针对“注册信息安全专业人员”培训，以注册信息安全专业人员所应具备的知识体系为大纲进行编写。全书主要介绍了风险评估、安全策略、安全工程以及信息安全管理的基本知识，并详细列述了对环境、人员、软件、应用系统、操作和文档的安全管理，应急响应和灾难恢复，国家信息安全组织结构等与信息安全管理有关的内容。通过对本书的学习，信息安全及相关行业的从业人员可对风险、安全策略及安全工程的概念有所了解，并明确信息安全管理所应包含的内容。

本书适合作为信息安全专业人员培训班的培训教材，也可供从事相关工作的技术人员和对信息安全感兴趣的读者阅读参考。

注册信息安全专业人员资质认证培训教材

编委会

丛书序

随着我国社会信息化进程发展，计算机网络及信息系统在政府机构、企事业单位及社会团体的运作中发挥着越来越重要的作用。信息化水平的提高在带来巨大发展机遇的同时也带来了严峻的挑战。由于信息系统本身的脆弱性和日益呈现出的复杂性，信息安全问题不断暴露。信息安全既关系着个人的隐私，也关系着国计民生，乃至整个国家的安全与利益。信息安全问题已经倍受政府和社会的广泛关注和重视。在这样的大背景下，社会对信息安全专业人员的需求逐年增加。据统计，国内从事信息安全方面的专业人员仅有 3000 余人，社会需求与人才供给间还存在着很大差距；怎样培养信息安全的专门人才，并确保现有信息安全从业人员的职业素质等，将成为信息安全产业发展中需要迫切解决的重要问题。

人员认证概述

中国信息安全产品测评认证中心是经中央批准成立，代表国家开展信息安全测评认证的职能机构，“中华人民共和国国家信息安全认证”是目前国家对信息安全技术、产品、信息系统安全质量以及信息安全服务资质、人员资质的最高认可，由中国信息安全产品测评认证中心及其授权测评机构进行评估，由中国信息安全产品测评认证中心进行认证。本从书是针对“注册信息安全专业人员认证”部分的培训教材。

“注册信息安全专业人员”（Certified Information Security Professional，简称 CISP）是指机构组织中负责信息系统（网络）建设、运行和应用管理的必备的专业性人才，其基本职能是为信息系统的安全提供技术和管理保障。对信息安全专业人员的认证和注册，是提高信息安全从业人员职业道德和技术水平、提升信息安全产业的竞争能力和强化国家信息安全管理的有效手段。

从书内容特色

本套丛书充分考虑“注册信息安全专业人员”培训学习的需要，以注册信息安全专业人员所应具备的知识体系为大纲，从信息安全的理论基础出发，兼顾理论学习与实践应用，较好地反映了信息安全学科的主要内容和基本特点，较为全面地覆盖了学科的知识要点。

为了使广大信息安全技术人员对信息安全有比较系统和全面的了解，本套丛书共分为以下 3 册：

《信息安全理论与技术》

《信息安全工程与管理》

《信息安全标准与法律法规》

内容涉及安全体系、密码技术、网络安全、系统安全、风险评估、安全策略、安全工程、信息安全管理、应急响应、国内外相关标准及法律等诸多方面，使相关从业人员对信息安全学科有一个较为全面的了解。

适用对象

本丛书适合作为培养信息安全专业人员的培训班教材，也适合从事信息安全工作的技术人员和广大对信息安全感兴趣的读者阅读参考。

关于作者

本丛书由中国信息安全产品测评认证中心组织编写，丛书的编写得到了何德全、周仲义、沈昌祥、蔡吉人几位院士的悉心指点，曲成义、方关宝、宁家骏、黄德根等专家更是为本书细心审校，业内相关人士尤其是首批 CISP 也给予了大力支持，在此一并表示感谢！

需要指出的是，由于丛书涉及内容较广，限于水平和经验，难免会有疏漏之处，敬请专家和广大读者指正。

有关本丛书内容的更新更正以及参考资料信息，可查询：http://www.cisp.org.cn。

中国信息安全产品测评认证中心

2003 年 9 月

目 录

第 1 章　风险评估

安全管理是信息安全中非常重要的一环，要实现较完善的安全管理，必须分析、评估安全需求，建立满足需求的计划，实施这些计划，并进行日常维护和管理。由此可见，安全管理过程的第一步就是要建立一个全局安全目标，然后将其整合到机构的安全政策中去。实现这一要求的关键是对风险的评估，将风险减小到可以接受的水平。

在系统工程学中，风险用于度量在技术性能、成本及进度方面达到某种目的的不确定性。对于信息安全这一特定领域来说，风险就是在一定的条件下某些安全威胁利用机构的相关资产对机构、组织或部门造成某种损害的潜在可能性。

安全需求是制定和实施安全政策的依据。安全风险与安全政策是对立统一的矛盾体。安全政策的制定及实施是为了将安全风险减小到可以令人接受的水平。由于风险具有不确定性，因此要完全消除风险是不切实际的。对信息安全管理的设计及维护人员来说，要从信息风险的一般规律提出安全需求，建立具有自适应能力的信息安全模型，从而将风险减小到可以接受的水平。一个信息系统是否安全要看它的风险是否已经减小到最小程度，是否在可控范围内，而不是绝对的无风险。

1.1　安全威胁

安全威胁指信息系统中存在的对机构、组织或部门造成某种损害的潜在可能。计算机系统很容易受到可造成不同程度损失的各种安全威胁。这些损失可能是由病毒造成的文件损坏和由火灾造成的整个计算机中心系统毁坏，也可能是来自内部雇员的欺诈行为、无意过失或是来自外部黑客的非法入侵造成的损失。由于很多损失是难以被发现的或出于各种原因被有意隐瞒了的，因此要想精确地估计与计算机相关的损失是不太可能的。

1.1.1　安全威胁的分类

按照安全威胁是出于自然的还是人为的，是无意的还是有意的，是直接的还是间接的，可以把各种安全威胁加以分类。无论是哪一类安全威胁，都可以根据其发生的概率、造成的损失大小来评估鉴定。

1．自然威胁

自然威胁是不以人的意志为转移的不可抗拒的自然事件，如地震、雷击、洪灾和火灾等。这些自然威胁发生的概率是比较低的，而且与一个机构、组织或部门所处的自然环境密切相关，如有些地方是雷击易发区，几乎每次有雷电产生时，都会损坏一些相关设施，

包括通信器材、网络设备等。对于这类威胁，必须根据实际情况进行具体分析，根据其发生的可能性大小，造成的损失大小，以及为了抵御这类威胁而要采取的措施的代价与产生的损失相比是否合算等因素进行综合考虑，采取相应的解决措施。

2. 人为威胁

一般来说，在现实中人为造成的损失的概率是远远大于自然威胁造成的损失的。

（1）意外的人为威胁

这类安全威胁是各种不确定因素（不正确的操作、配置、设计或人员的疏忽大意）综合在一起时偶然发生的，并不是有人故意造成的。这类安全威胁在人为威胁中是经常发生的，其发生的概率甚至比有意而为的安全威胁发生的概率还要大，产生的损失也可能是非常巨大的、无法挽回的。曾经有计算机安全专家做过长期调查，得出的结论是：无论是私人机构还是公共机构，大约65%的损失都出自于无意的错误或疏忽，错误或疏忽在一个信息系统的整个生存周期中都是存在的。

错误和疏忽对于数据和信息系统完整性的威胁是很大的，它们可能是工作人员每天处理的成百上千的事务中的数据项出错，也可能是所有类型的用户创建及编辑的数据出错。许多应用程序，特别是那些用户为了特定目的而编写的并安装在自己的个人计算机上的程序，由于软件开发过程中缺乏足够的软件质量控制手段，软件没有经过严格的测试，因此在利用这样的软件处理数据的过程中就可能产生各种错误。从另一方面讲，就是非常成熟的软件也不可能检测出所有的输入数据错误。

用户、数据处理人员、系统管理员以及程序员都会经常地、无意地犯一些错误，造成了直接或间接的后果。在某些情况下，这些错误就会成为一种威胁，如某一数据项的错误导致了系统的崩溃；而在另一些情况下，这些错误或疏忽就有可能使信息系统的某一部门成为这个系统中的薄弱环节，从而有可能被各种威胁所利用而造成各种损失。程序设计开发中的错误通常被叫做“BUG”，这些BUG可能是很微小的，也可能是灾难性的。由于现在计算机被应用在包括军事、金融、航天等许多领域中，因此一旦因这些BUG而产生事故，后果可能是非常严重的，如金融动荡、重大事故甚至人身伤害。正是由于这些原因，现在的软件开发者一般都比较重视对软件质量的控制。有关统计说明，现在软件中平均每一千行代码中就有一行是有问题的。由于现在的软件大小增长很快，因此大大抵消了引入软件质量控制技术带来BUG减少的好处。

系统在配置及维护中也可能发生错误及疏忽。如现在的网站中很多系统配置有多处漏洞，有的是由于采用默认配置，有的是身份验证不严格，而有的是未及时为系统安装补丁升级程序。另一些问题发生在路由器、防火墙的配置错误，而形成各种漏洞或薄弱环节。这些都为黑客的非法侵入或病毒的感染打开了方便之门。

要解决这类问题，减少这类错误及疏忽的发生概率，就必须对工作人员及软件编写人员进行培训。

（2）有意的人为威胁

有意的人为威胁包括欺诈或偷窃、内部员工的有意破坏、怀有恶意的黑客行为、侵犯他人个人隐私、恶意代码、工业间谍以及外国间谍等行为。

① 欺诈或偷窃。通过计算机系统进行欺诈或偷窃不但可以用一些“传统”的方法，