信息安全保障人员认证培训教材

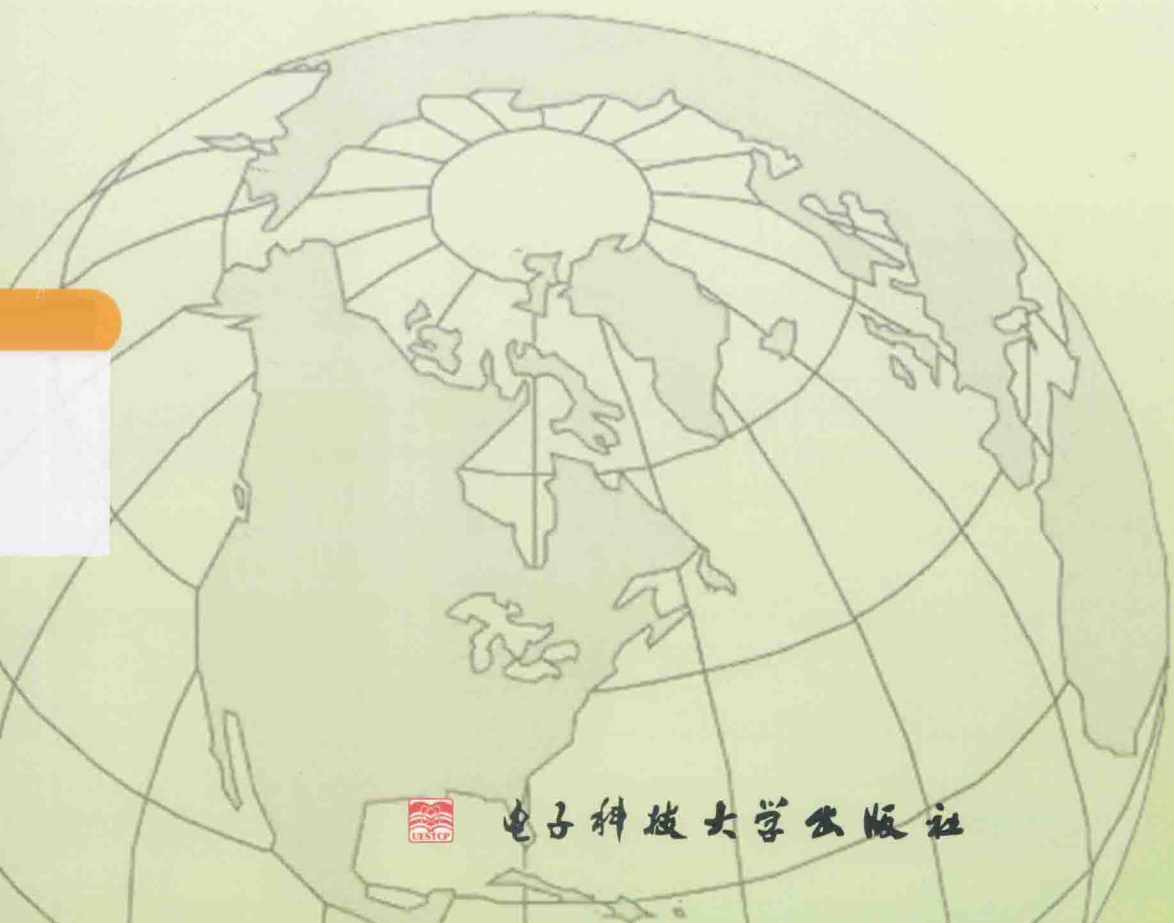
信息安全风险管理

XIN XI AN QUAN FENG XIAN GUAN LI

中国信息安全认证中心

◎主 编 张 剑 ◎副主编 廖国平 林 利 汤 亮

CISAW



电子科技大学出版社

信息安全保障人员认证培训教材

信息安全风险管理

XIN XI AN QUAN FENG XIAN GUAN LI

中国信息安全认证中心

◎主 编 张 剑 ◎副主编 廖国平 林 利 汤 亮

★★★ CISAW ★★★

图书在版编目（CIP）数据

信息安全风险管理 / 张剑主编. -- 成都：电子科技大学出版社，2015.2

ISBN 978-7-5647-2833-5

Ⅰ. ①信… Ⅱ. ①张… Ⅲ. ①信息安全-风险管理-研究-中国 Ⅳ. ①TP309

中国版本图书馆 CIP 数据核字（2015）第 033359 号

内 容 提 要

本书从CISAW信息安全风险管理模型出发，以信息安全风险管理为重点，全面介绍信息安全风险管理的基本概念、信息安全风险管理相关国际以及国家标准、信息安全风险评估技术、信息安全风险处置以及信息安全风险管理实例。书中内容以信息安全风险管理为主线，内容结构合理，层次分明，重点明确，注重信息安全风险管理实践应用。

信息安全风险管理

主　编　张　剑

副主编　廖国平　林　利　汤　亮

出　　版：电子科技大学出版社（成都市一环路东一段 159 号电子信息产业大厦　邮编：610051）

策划编辑：徐守铭

责任编辑：李　毅

主　　页：www.uestcp.com.cn

电子邮箱：uestcp@uestcp.com.cn

发　　行：新华书店经销

印　　刷：成都市川侨印务有限公司

成品尺寸：185 mm × 260 mm　　**印张** 11.75　　**字数** 242 千字

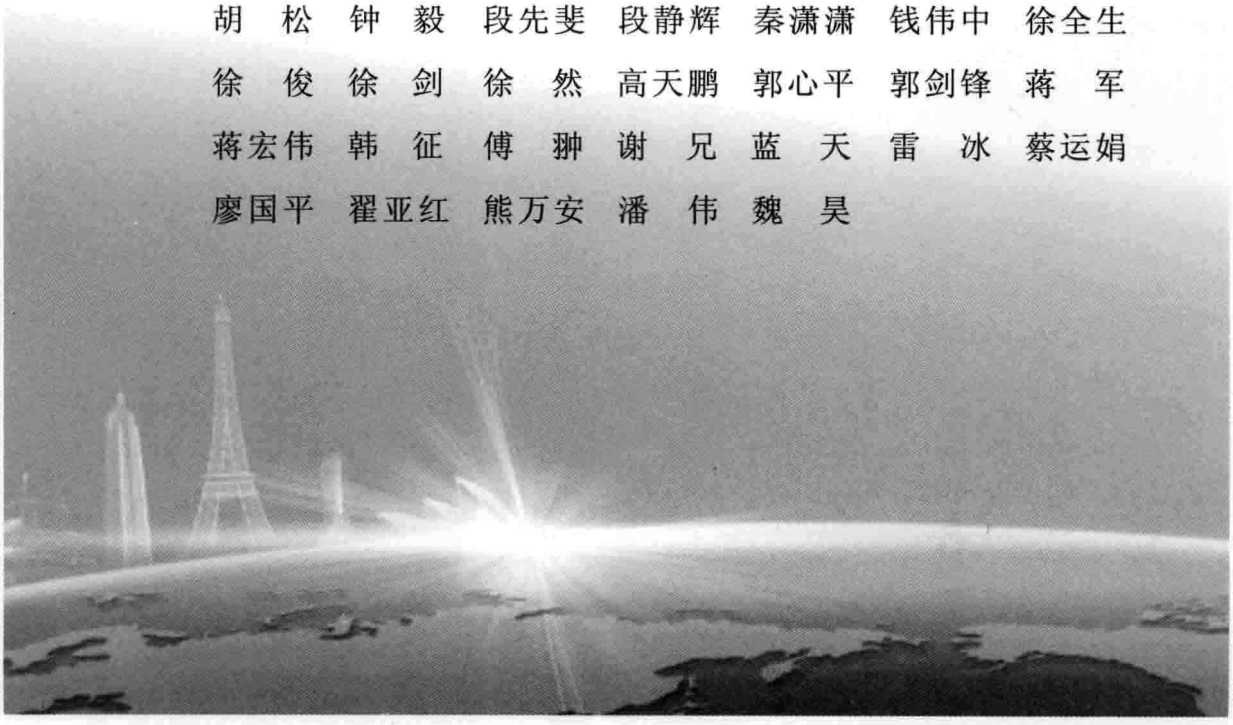
版　　次：2015 年 2 月第一版

印　　次：2015 年 2 月第一次印刷

书　　号：ISBN 978-7-5647-2833-5

定　　价：45.00 元

丛书编委会



编 写 组

主　编　张　剑

副主编　廖国平　林　利　汤　亮

编　委　成林芳　王　刚　李　源　吴芳琼　尹远飞　雷　冰　段先斐
朱灿庭

序

2014年，我国提出了建设网络强国战略与目标。实现网络强国，培养和造就网络与信息安全人才队伍是关键。据调查，截至2014年年底，国内网络与信息安全人才缺口高达50万人，并呈现持续增长的趋势。加快人才培养是我国经济社会发展和信息安全体系建设中的一项长期性、全局性和战略性的任务。

作为我国专业信息安全认证机构和培训机构，中国信息安全认证中心以保障国家网络与信息安全为己任，于2011年推出了信息安全保障人员认证（CISAW）。CISAW认证是面向IT从业人员、在校学生，特别是与网络与信息安全密切相关的高级管理人员、专业技术人员推出的人员资格认证和专业水平认证。CISAW认证的推出和实施，为培养和造就我国网络与信息安全人才探索了一条有效途径，得到了业内专家和社会各界的好评。

推行CISAW认证，编写高质量的教材尤为重要。鉴于此，中国信息安全认证中心组织国内信息安全保障的专业技术和应用领域的专家，依据《信息安全保障人员认证考试大纲》要求，结合信息安全保障工作的各岗位知识和应用能力要求，共同编著了信息安全保障人员认证系列教材。本系列教材包括《信息安全技术》《信息安全技术应用》和《信息安全实验》3种基础教材；《软件安全开发》《信息系统安全集成》《信息安全管理》《信息安全咨询手册》《信息系统安全运维》《信息系统安全审计》《信息安全风险管理》《网络攻防技术》《业务连续性管理》《云计算安全》《物联网安全》和《工业控制安全》12种专业技术应用教材；《电子政务安全》《电子商务安全》《交通服务信息安全》《能源服务信息安全》《医疗卫生信息安

全》《教育服务信息安全》《金融服务信息安全》《通信服务信息安全》《宾馆服务信息安全》和《物流服务信息安全》10种应用领域教材。

本系列教材以实用为首要原则，从统一的信息安全保障模型出发，构建了包括信息安全技术基础知识、信息安全专业技术知识和应用领域安全保障管理知识的完整信息安全保障知识体系。既是广大CISAW认证申请者的考试指导用书，同时也是广大信息安全保障工作者的工作指南和参考用书。

希望本系列教材的出版，能为广大信息安全保障从业者学习、工作和申请认证提供指导和帮助。

是为序。

中国信息安全认证中心主任　魏　昊

2014年12月28日

前　言

本书力求从实践需要出发，讨论当前信息安全保障工作中的风险管理技术。全书共分为5章，第1章从信息安全风险管理基本模型出发，阐述风险的起源、特性、要素及其关系和风险管理的基本概念；第2章从信息安全风险管理标准出发，阐述ISO/IEC31000、ISO/IEC13335、ISO/IEC27005、卡内基梅隆、GB/T20984等相关标准的内容；第3章关注的是风险管理中的风险评估这一核心要素，详细阐述了信息安全风险评估内容，主要按照风险识别、风险分析、风险评价这样一条主线展开论述，同时辅以部分实例进行说明；第4章从风险处置的角度出发，详细阐述风险处置的过程框架，并讨论了几种典型的风险处置措施及其应用。第5章则是从整体的角度出发，依照本书中第1章提出的风险管理基本模型，以一个实际项目作为案例，对整个风险管理的实施过程进行论述。

本书按照信息安全保障人员认证考试大纲的要求进行编写，适合广大申请认证考试的人员使用；同时，也适合所有从事信息安全风险管理相关的工作人员以及期望了解信息安全风险管理相关知识的人员使用。本书配套教程《信息安全技术》详细介绍了相关安全技术的基本概念和技术原理，可供相关人员参考。

本书由张剑、廖国平、林利、汤亮、成林芳、王刚、李源、吴芳琼、尹远飞、雷冰、段先斐、朱灿庭等共同编写完成，在此，对各位的辛勤付出表示感谢。

本书在成书过程中得到了《信息安全保障人员认证考试用书》编委会的指导，同时得到了中国信息安全认证中心、湖南省网络与信息安全测评

中心、四川省中认信安技术服务有限公司和四川亚和企业咨询服务有限公司的大力支持，在此表示衷心感谢。

本书在编写过程中参考或引用了国内外同行的大量文献资料，在此向这些文献资料的作者表示衷心感谢。

本书力图通过较小的篇幅比较完整地、正确地介绍信息安全相关的基本技术应用。同时，为了能够扩大读者面，尽量使用简单、实用和易于理解的方式进行阐述。但书中仍难免存在疏漏和错误，在此，恳请广大读者和同行批评指正，以便我们再版修订时加以改正和完善。

张　剑

2014 年 12 月 16 日

目　录

第1章 概 述

1.1 风险起源

1.1.1 风险的发展历程

“风险”一词由来已久，最普通的说法是：以打鱼捕捞为生的渔民们，每次出海前都要祈祷，祈求神灵保佑自己能够平安归来，其中祈求的主要内容就是让神灵保佑自己在出海时能够风平浪静、满载而归；他们在长期的捕捞实践中，深深的体会到“风”给他们带来的无法预测无法确定的危险，他们认识到，在出海捕捞打鱼的过程中，“风”即意味着“险”，“风险”一词也因此而得来。

另一种经由多个研究者论证的“源出说”称，风险（Risk）一词是舶来品，一部分人认为其来源于阿拉伯语，也有一部分人认为其来自于西班牙语或者是拉丁语，但公认度较高的一种说法是“风险”一词来源于意大利语的“Risque”。在最初的运用中，风险也是被理解为客观存在的危险，例如在航海过程中遇到的礁石、风暴等事件或者其他一些非正常的自然现象。

然而人们对于风险的理解和定义总是随着人类文明的进步而不断发展和变化的。大约到了19世纪，经过两个多世纪的发展，风险的概念与人类的决策和行为后果有着更为紧密的联系，并且逐渐被视为影响个人和群体的事件的特定方式。“风险”一词的使用也从早期的航海贸易行业和保险业渐渐衍生到其他各行各业之中。

现代意义上的风险，已经大大超越了“遇到危险”的狭义含义，而是“遇到破坏或损失的机会或危险”，到了近现代社会，风险一词越来越被概念化，并随着人类活动的复杂性和深刻性而逐步深化，且被赋予了更广泛更深层次的含义。从风险的概念出现到目前，近现代人们关于风险的理解一直在不断地发展和演进：1987年，威森（Wison）在《科学》杂志上发表了风险相关的文章，并将风险的本质阐述为“不确定性，定义为期望值”；1989年，马斯克里（Maskrey）定义风险是“某种自然灾害发生的可

能性”；1991 年联合国赈灾组织定义“风险是在特定的区域以及给定的时间段内，由某种自然灾害而导致的人们生命财产和经济活动的期望损失值”；1997 年，托宾（Tobin）和门茨（Montz）定义“风险是某一个灾害发生的可能性概率和期望损失的乘积”；1998 年，黛尔（Deyle）定义“风险是对某一灾害概率与结果的描述”；2007 年 6 月，ISO（国际标准化组织）技术管理局将风险定义为“对目标的不确定性影响（Effect of Uncertainty on Objectives）”。

1.1.2 风险定义

ISO/IEC 31000 将风险的定义为“对目标的不确定性影响”。

从 ISO 技术管理局对风险的定义可以看出，风险是一种影响，影响可能是正面的，也可能是反面的。正面的影响会给我们带来机会与利益，相反，就会给我们带来威胁与损失。就像我们平常坐飞机存在失事的风险，正常情况下，飞机可以让我们到达目的地的旅行时间大为缩短，然而，一旦飞机失事，我们付出的可能就是生命的代价。

风险是针对某个目标而言的，离开了目标而谈论风险是没有任何意义的。目标是组织的目标或者利益相关方的目标，并且它是具体的，而不是抽象的。

风险往往具有潜在事件与后果或者潜在事件与后果两者相结合的特征。从这一点我们可以看出，事件是风险的一个载体。如果没有安全威胁事件，就谈不上安全威胁事件的可能性及其影响。而没有了可能性与影响，风险也就无从谈起。所以，在我们的风险评估实践中，风险是由可能性与后果的组合来计算的。

当然，能够影响目标的因素有很多种，风险所涉及的只是其中的一种因素，那就是“不确定性”。从 ISO 对风险的定义我们可以看得出来，“不确定性”是风险最本质的特征，它指的是缺乏或者部分缺乏对某个事件及其后果或者该事件发生的可能性的相关信息的了解或者认识的状态。不确定性包含事件发生与否的不确定、发生时间的不确定与影响结果的不确定。

本书重点关注的内容是信息安全风险，对于信息安全风险，本书的定义为“威胁利用脆弱性对风险管理对象所造成的不确定性影响”。

1.1.3 风险管理

根据维基百科定义，风险管理（Risk Management）是一个管理过程，包括对风险的定义、测量、评估和应对风险的策略。风险管理的目的是将能够避免的风险、成本以及损失最小化。理想中的风险管理，在事先就已经排定好优先次序，对于引发最大的损失以及发生概率最高的事件可以优先处理，然后再对风险相对比较低的事件进行处理。实际情况中，由于风险与发生概率往往不一致，很难对处理顺序进行事先排序，因此需要衡量两者的比重，进行最合适的判断。

信息安全风险管理是一个持续的管理过程。整个过程包含建立合适的风险管理框

架，实施风险评估，利用风险处置计划来实施风险建议和决策并处置风险，最后通过对整个管理过程实施评审以达到整个管理过程的持续改进。信息安全风险管理过程适用于整个组织或者其中的任何部分（如部门，物理区域甚至是一个服务），它也适用于任何的信息系统。

1.2 风险管理的模型

伴随着信息科学技术的飞速发展和社会信息化进程的不断加快，国民经济乃至国家安全对信息和信息系统的依赖程度越来越大。因此，信息的安全性已经引起了国家的高度重视。信息安全管理的本质是风险管理，安全与风险是密不可分的，没有绝对的安全也没有彻底的风险。

有效的风险管理一定是建立在一定的模型之上。模型是人们认识和描述客观世界的一种方法。在信息安全保障阶段，通常的模型有：PDR（保护、检测和响应）、PPDR（安全策略、保护、检测和响应）、PDRR（保护、检测、响应和恢复）、MPDRR（管理、保护、检测、响应和恢复）和 WPDRRC（预警、保护、检测、响应、恢复、反击）等动态安全模型。

WPDRRC 安全模型是我国 863 信息安全专家组在 PDR 模型、P2DR 模型及 PDRR 模型的基础上提出的适合我国国情的网络动态安全模型。WPDRRC 模型在 PDRR 模型四个环节的基础上增加了预警（Warning）和反击（Counterattack）两个组件，共计六个环节。它们形成了具有动态反馈关系的整体。预警环节根据已掌握的系统脆弱性以及威胁发展趋势，去预测未来可能受到的攻击与危害；反击则是采用一切可能的技术手段，获取有关威胁行为的线索与证据，形成强有力的取证能力和依法打击手段。首先在 WPDRRC 安全模型的基础上结合实际应用与认证体系提出了 CISAW 信息安全保障模型，通过把 CISAW 信息安全保障模型应用到信息安全风险管理领域，得出了一个实践可行的信息安全风险管理模型，如图 1－1 所示。

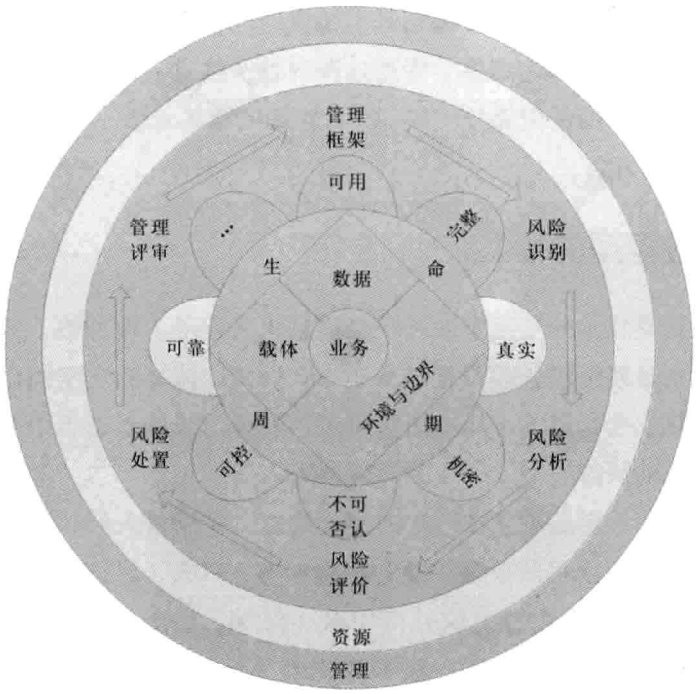


图 1-1　信息安全风险管理模型

1.2.1　风险管理对象

如图 1-1 所示的信息安全风险管理模型中，从核心管理对象——“业务”出发，具体解决数据、载体、环境与边界四个对象全生命周期的信息安全风险管理问题，提供可用性、完整性、真实性、机密性、不可否认性（抗抵赖性）等若干安全属性，并综合协调管理人、技术、财务、信息四类主要资源，在管理框架、风险识别、风险分析、风险评价、风险处置和管理评审的六个环节上，实现信息安全风险的管理与监视评审。

1. 本质对象

信息安全风险管理的本质对象是“业务”，“业务”是一个组织的正常运转的核心活动。业务的连续性直接关系到组织是否能够正常履行其职能。组织业务的保障需要组织投入人力、物力和财力资源，来维持组织业务的开展。随着信息化水平的提高，业务信息资源的依赖性越来越大。与此同时，信息资源所面临的威胁也是越来越多，针对信息资源的攻击手段也越来越多样化。因此，信息资源受到了来自各个方面（主要包括技术与管理两个层次）的风险的威胁。从而使得信息安全风险管理成为信息化组织所必不可少的环节。

例如：某游戏网站业务完全依赖于实时在线的众多游戏玩家，如果该游戏网站遭遇到 DDoS（Distributed Denial of Service）攻击，将使得众多玩家无法正常进入网站进行游戏，这将会使得玩家对该网站失去兴趣。然而，由于该游戏网站在建设初期就已