信息安全管理体系丛书

信息安全管理体系教程

——国家注册ISMS审核员培训教程

北京知识安全工程中心　编著

中国标准出版社

信息安全管理体系教程

信息安全管理体系教程

—— 国家注册ISMS审核员培训教程

Tutorial for Information Security Management Systems

— Training Tutorial for National Register of Certificated ISMS Auditors

王新杰　陈珍成　王连强　谢宗晓　编著

中国标准出版社

内 容 简 介

ISO/IEC 27001 所提出的 ISMS(信息安全管理体系)正在成为信息安全和管理体系两个领域中的政策部门、企业、认证机构所关注的热点。作为“国家注册 ISMS 审核员”的培训教程,本书从信息安全、风险评估、ISO/IEC 27000 标准族、管理体系和 ISMS 审核等不同领域、多个侧面,详细阐述了 ISMS 及 ISMS 审核的基本概念、ISO/IEC 27001 的理解与实施、ISMS 过程要求和控制要求审核的方法和流程,以及 ISMS 与其他管理体系的结合审核等。

如果你想了解 ISMS 国际标准,学习 ISMS 知识,或者想成为 ISMS 审核员,如果你是政府或企事业单位的信息安全工作者,ISMS 实施人员或者信息安全风险评估工作者,这本教程将带给你最好的参考和帮助。

图书在版编目(CIP)数据

信息安全管理体系教程:国家注册 ISMS 审核员培训教程/王新杰等编著. —北京:中国标准出版社,2007
(信息安全管理体系丛书)
ISBN 978-7-5066-4431-0

Ⅰ. 信… Ⅱ. 王… Ⅲ. 信息系统-安全管理-体系-中国-技术培训-教材 Ⅳ. TP309

中国版本图书馆 CIP 数据核字(2007)第 021958 号

中国标准出版社出版发行
北京复兴门外三里河北街 16 号
邮政编码:100045
网址 www.spc.net.cn
电话:68523946 68517548
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 787×1092 1/16 印张 12 字数 290 千字
2007 年 3 月第一版 2007 年 3 月第一次印刷
*
定价 **35.00** 元

丛书序

看到由北京知识安全工程中心编写的ISMS丛书，我很高兴，并十分乐意向广大读者推荐这套将信息安全知识和管理体系知识融合在一起的丛书！丛书的出版为中国读者了解ISMS知识打开了一扇窗户，必将促进ISMS在中国的推广和有效实施，为保障我国信息安全带来积极的作用！

ISMS(Information Security Management System，信息安全管理体系)是继质量管理体系、环境管理体系、职业健康安全管理体系、食品安全管理体系之后发展起来的一个新兴的管理体系，是管理体系家族中的一个新“成员”。通过建立和实施ISMS并取得ISMS认证，已经成为各种类型和规模的组织保障信息安全的一个科学、有效的方法。伴随着ISO/IEC 27001:2005和ISO/IEC 17799:2005等ISMS系列国际标准的发布，ISMS开始被全球越来越多的组织认识并接受。

近年来，我国高度重视信息安全保障工作。为指导信息安全保障工作的有效开展，党中央在总结以往信息安全保障经验的基础上，在《国家信息化领导小组关于加强信息安全保障工作的意见》(中办发[2003]27号)中明确提出了“立足国情，以我为主，坚持管理与技术并重”的信息安全保障原则。同时还要求“各级党委和政府要充分认识加强信息安全保障工作的重要性和紧迫性，要抓紧建立健全信息安全管理体制”。信息安全涉及国家安全，因此要“以我为主”，管理和技术都是实现信息安全目标的重要手段，因此要“坚持管理与技

术并重”。建立和实施ISMS符合中央提出的信息安全保障原则，是落实中央精神、保障国家信息安全的要求。

我国认证认可、信息安全、标准化等有关部门对ISMS标准和认证的发展也进行了积极、深入的跟踪、探索和研究。2002年以来，全国信息安全标准化技术委员会就开始着手制定ISMS相关国家标准，并于2005年发布了国家标准GB/T 19716—2005《信息安全管理实用规则》。国家认证认可监督管理委员会开始研究建立ISMS认证认可制度，相继批准了一批ISMS试点认证机构和认证培训机构，中国认证认可协会和中国合格评定国家认可委员会也分别开展了ISMS人员培训注册和机构认可等相关工作。2006年11月国家成立了“中国信息安全认证中心”，专门负责在信息安全领域开展产品和管理体系认证等相关工作。这些探索和实践为ISMS在我国的推广和有效实施奠定了基础。

尽管我们对ISMS进行了一定的探索和实践，但是对于大部分读者来说，ISMS仍然是一个新领域、新事物，它涉及信息安全、管理体系、标准、认证等多个知识领域，是一门典型的交叉学科。北京知识安全工程中心组织力量编写的这套丛书，从不同领域、多个侧面，对ISMS相关知识进行了细致的介绍和阐述，有理论，更有实践。丛书中的每一本既相对独立，又相互联系，既可以单独使用，也可组合起来作为一套教材系统地学习。丛书可谓既专又广，是一套ISMS领域不可多得的优秀教科书，一定会为我国ISMS专业人才的培养起到积极的推动作用。

我在向广大读者推荐这套ISMS丛书的同时，也真诚地企盼能有更多的信息安全和管理体系相关工作者投入到ISMS的研究和推广工作中去，为更广大的读者不断提供更丰富、更新鲜的作品，为我国信息安全保障和ISMS认证认可工作做出贡献！

国家认证认可监督管理委员会副主任

2007年1月26日于北京

丛书前言

IT技术的快速发展和广泛应用掀起了全球信息化的大潮，使人类进入了继农业革命、工业革命后的第三次生产力的革命阶段。我国信息化的规模和速度全球瞩目，逐步渗透到各行各业。人们享用着信息化的成果，憧憬着信息化带来的前所未有的美好前景。

由于人们认识真理、实践真理的能力的局限性，IT产品存在安全性问题，信息系统存在着脆弱性。加之存在着意识形态的斗争、经济发展的竞争以及社会犯罪和恐怖主义活动，信息系统的正常功能受到制约，信息化带来的高效率、高效益受到限制，信息资源受到威胁，信息空间的安全形势严峻。

为了强化信息安全保障，各国都在制定方略，加强研究，采取措施，建设信息安全保障体系。人们逐步认识到，依靠信息安全技术产品只是解决信息安全问题的一个方面，大量的问题还需要通过管理来解决，而且技术和管理都需要通过人来使用和操作。为了规范信息安全产品的生产使用和信息安全管理操作，各国都加强了信息安全各类标准的制定工作。ISMS等信息安全管理标准成为当前的热点和重点。

《国家信息化领导小组关于加强信息安全保障工作的意见》(中办发[2003]27号)提出了“立足国情，以我为主，坚持技术管理并重”的要求，并提出了“抓紧制定急需的信息安全管理和技术标准”的任务。国务院信息办常务副主任，全国信息安全标准化技术委员会主任曲维枝同志最近也指出：“没有信息安全的信息化是危险的信息化；没有完善的信息安全标准，信息化建设中的产品、系统、工程就不能实现安全的互联、互通、互操作，就不能形成我国自主的信息安全产业，就不能构造出一个自主可控的信息安全保障体系，就难以保证国家信

息安全和国家利益。”根据以上要求和国务院信息办组织的信息安全管理标准应用试点工作的实践，全国信息安全标准化技术委员会确定了跟踪借鉴ISMS国际标准制定我国信息安全管理体系标准的任务。

北京知识安全工程中心作为我国第一个依据《中华人民共和国认证认可条例》授权进行ISMS认证培训服务的机构，为了规范自己的培训和咨询服务，根据国际和国家标准以及自己长期研究和实践的经验，编写了一套ISMS的丛书。该丛书由《信息安全管理体系教程》、《信息安全管理体系教程习题与案例分析》、《信息安全风险评估》、《信息安全管理体系控制措施实施和测量》、《信息安全管理体系审核指南》、《信息安全管理体系建立和实施》、《信息安全管理体系内部审核》等组成。丛书全面涉及了ISMS的概念，构建ISMS的程序、步骤和方法要求等各个方面，是一套深入浅出、系统介绍ISMS的实用教材，将为我国宣传贯彻ISMS标准，落实ISMS认证工作，加强ISMS人才培养发挥重要的作用。

建立和实施ISMS是一个组织有序提升信息安全管理能力的有效战略举措。不论是否以通过ISMS认证为目的，都具有重要的参考借鉴作用。只要组织存在信息安全问题，就需要根据组织自身的需要和特点，建立起自己的ISMS。ISMS的建立和运行为我国的信息安全等级保护制度的执行提供有力支撑，是在一个组织范围内落实信息安全保障的各项基础性工作的科学指南。ISMS是一个持续的计划(P)、实施(D)、检查(C)、改进(A)的过程。为了加强ISMS的执行力，形成ISMS的常态化，形成体系文件是必要的，但是落实到人和信息系统是更为重要的。通过角色和责任的落实和数字化自动化支撑工具的运用才能把心里想的、纸上写的落实到信息安全工作的过程和活动中。

没有明白人，难办明白事。ISMS的人才培养是成功建立和实施ISMS的重中之重。让我们积极行动起来，加大信息安全专门人才培养的工作力度，不断创造适合我国国情的新经验、新手段，把建设我国信息安全保障体系的艰巨任务不断推进，落到实处。

2007年1月21日

前言

2000年以来，我国政府主管部门和相关企业就开始了信息安全管理体系（ISMS，Information Security Management System）标准和认证认可制度的探索研究。北京知识安全工程中心（PKSEC，Peking Knowledge Security Engineering Center）作为国内较早开展ISMS相关工作的组织，参与了ISMS国家标准的制修订工作，并于2005年被国家认证认可监督管理委员会（CNCA）批准为首家ISMS认证培训机构，开展“国家注册ISMS审核员”培训工作和ISMS认证咨询工作。

PKSEC组织编写了《信息安全管理体系教程》，作为“国家注册ISMS审核员”的培训教材，并于2006年8月获得了中国认证认可协会（CCAA，China Certification & Accreditation Association）的确认。根据CCAA的规定和要求，“国家注册ISMS审核员”课程为40课时，主要内容包括ISMS基础、ISMS标准和ISMS审核等三部分内容。

ISMS是1998年前后从英国发展起来的为解决信息安全问题的一个新的管理体系（MS，Management System）。ISMS同其他MS如质量管理体系（QMS）、环境管理体系（EMS）、职业健康安全管理体系（OHSMS）、食品管理体系（FSMS）等一样，具有许多共同的要素，其原理、方法、过程和体系的结构也基本一致。ISMS是MS思想和方法在解决信息安全问题中的应用。近年来，信息安全问题日益突出，逐渐成为影响企业生存和发展的重要因素，甚至影响国家安全。ISMS认证成为组织向社会及其相关方证明其信息安全水平和能力的一个有效途径。

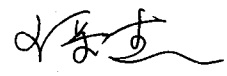
“ISMS 审核员”是 ISMS 认证过程中的最重要的角色，由 ISMS 审核员和技术专家（必要时）组成的审核小组对申请 ISMS 认证的组织进行审核，审核结束后审核小组向认证机构做出推荐注册或不推荐注册的建议，即通过认证还是没有通过认证。根据《中华人民共和国认证认可条例》，提供 ISMS 认证的第三方认证机构必须具备规定数量（不少于 10 名）的 ISMS 审核员，而且申请 ISMS 认证的组织也必须拥有一定数量的 ISMS 内审员。

《信息安全管理体系教程》将帮助那些希望成为 ISMS 审核员的读者迅速了解 ISMS 基础知识，理解 ISMS 标准的要求，掌握 ISMS 审核的方法和步骤，最终成为“国家注册 ISMS 审核员”。同时，《信息安全管理体系教程》也可以为企业的 ISMS 实施人员、ISMS 内审员、信息安全风险评估工作者和希望了解 ISMS 标准知识、审核知识的读者提供帮助和参考。ISMS 是一门交叉学科，它涵盖了信息安全和管理体系两个不同领域的知识。《信息安全管理体系教程》将这两个不同学科的知识有机地结合在一起，希望能为不同的读者学习和使用带来方便。

撰写这本教程是一项艰苦的工作。我特别感谢我的同事，是他们的智慧、勤奋和细心成就了这本教程，他们是谢宗晓，撰写了教程的第一部分 ISMS 基础；王连强，撰写了教程的第二部分 ISMS 标准；陈珍成，撰写了教程的第三部分 ISMS 审核。此外，也感谢陈清和刘江河在本教程的编写过程中提供了大量有价值的资料。

感谢为本教程顺利出版付出辛苦努力的审稿者，是他们的认真审阅和真知灼见大大提高了这本教程的质量。

无论教程的编者怎样地努力，这本教程存在的不足是客观的，希望读者在使用这本教程的过程中，能不吝赐教，多提改进意见，以帮助我们对这本教程持续改进。



2007 年 1 月 21 日

目录

第一部分 基 础

第二部分 标 准

第三部分 审 核

第一部分

Serials of
Information Security Management Systems

基础

第1章 信息安全

2000年12月13日，CNN.COM报道了一名骇客攻击了CREDIT CARD.COM，盗取了其中55 000张信用卡号码，然后试图利用这些信息通过某在线信用卡公司欺骗钱财。欺诈行为虽然最终没有得逞，但这个事件在当时也引起很大的震动。然而，之后的几年，类似于此的信息安全事件变得越来越多，已经谈不上什么“新闻”了。

毫无疑问，这些事件都影响了“信息安全”。我们不禁要问，为什么这些安全事件会不断发生？

在计算机网络出现的最初几十年里，主要被大学的研究人员用于发送电子邮件，以及被公司的员工共享打印机等，在这样的环境下，安全问题并没有得到足够的关注。但从互联网得到广泛应用之后，普通市民都开始利用网络来完成网上购物、银行转账等事务，因此，安全问题的隐患就开始凸显。

1.1 什么是信息安全

1.1.1 信息安全的概念

信息安全是一个很宽泛的概念，很难精确地加以定义。从其发展的历史来看，最初在20世纪40年代，人们在信息安全问题上最关注的是“通信保密(COMSEC)”；到20世纪70年代，转移到计算机的非授权使用问题，这时可以称为“计算机安全(COMPSEC)”；在20世纪90年代之后，人们关注的注意力显然都集中到“网络安全(NETSEC)”上了；最近几年，人们又提出“知识安全”概念。因此，各个发展阶段出现的词汇往往与信息安全概念等同起来，如“计算机安全”、“网络信息安全”、“数据安全”和“知识安全”等。

经过四五十年的发展，人们对信息安全的认识不断深化，现在已经发展成为一个妇孺皆知的概念。那么，如何来给信息安全下一个定义？

目前，国内外对信息安全的定义主要分为两类：从安全内容进行定义和从安全属性进行定义。

从安全内容进行定义强调安全涉及的方面。

一种是在定义中历数信息安全涉及的保护区域。例如：信息安全是与保护相关的概念，其目的是保护组织的资产，至少要包括下面这些方面：管理实践、物理安全、人员安全、