国家“十二五”重点规划图书
信息安全管理体系丛书

信息安全管理体系审核指南

- 丛书顾问：蔡吉人　周仲义
- 丛书主编：吕述望　赵战生　陈华平
- 执行主编：谢宗晓　吕茂强

中国信息安全认证中心　组编
魏军　谢宗晓　编著
魏昊　审定

中国质检出版社
中国标准出版社

信息安全管理体系审核指南

中国信息安全认证中心 ◉ 组编
魏 军 谢宗晓 ◉ 编著
魏 昊 ◉ 审定

中国质检出版社
中国标准出版社
北 京

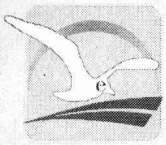
图书在版编目（CIP）数据

信息安全管理体系审核指南/魏军，谢宗晓编著．
—北京：中国标准出版社，2012.10
（信息安全管理体系丛书）
ISBN 978-7-5066-7010-4

Ⅰ.①信… Ⅱ.①魏…②谢… Ⅲ.①信息安全—安全管理体系—中国—指南 Ⅳ.①G203-62

中国版本图书馆 CIP 数据核字（2012）第 230944 号

中国质检出版社
中国标准出版社 出版发行
北京市朝阳区和平里西街甲 2 号（100013）
北京市西城区三里河北街 16 号（100045）
网址：www.spc.net.cn
总编室：（010）64275323 发行中心：（010）51780235
读者服务部：（010）68523946
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 787×960 1/16 印张 8.5 字数 171 千字
2012 年 10 月第一版 2012 年 10 月第一次印刷
*
定价 25.00 元



国家“十二五”重点规划图书
信息安全管理体系丛书

序言

prologue

中国工程院院士 蔡吉人 推荐序

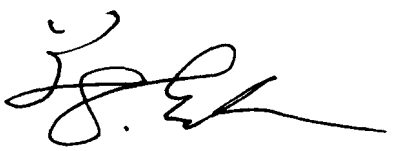
党中央、国务院高度重视信息安全工作。在中办发〔2006〕11号《2006—2020年国家信息化发展战略》中明确指出："坚持积极防御、综合防范，探索和把握信息化与信息安全的内在规律，主动应对信息安全挑战，实现信息化与信息安全协调发展"，"积极跟踪、研究和掌握国际信息安全领域的先进理论、前沿技术和发展动态"。

虽然信息安全技术和信息安全管理得到了前所未有的重视，但是信息安全事件却一直处于有增无减的状态。只有信息安全技术和管理并重，在宏观层次上实施了良好的信息安全管理，才能使微观层次上的安全，如物理措施等，实现其恰当的作用。采用信息安全管理体系并得到认证无疑是组织应该考虑的方案之一。事实上，也只有这样才能真正站在组织的高度上来对待信息安全问题。

信息安全管理体系（ISMS）是基于组织业务风险方法来建立、实施、运行、监视、评审、保持和改进信息安全，它跳出了"为安全信息而信息安全"的传统概念，强调站在组织业务的角度来管理信息安全活动。ISMS相关标准不仅为一个组织提供从框架到细节的全面指导，而且为ISMS的整个产业链提供指南。

基于此，中国质检出版社组织了国内的信息安全专家及标准的起草

者编写了《信息安全管理体系丛书》。本丛书是我国第一套全面系统的信息安全管理体系丛书，它从ISMS的基础信息安全风险管理开始讨论，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，包括ISMS的审核指南、应用方法、业务连续性管理以及在重点行业的应用实例，很有特色，可谓既专又广，是一套充分展示ISMS领域当前成果并将其推广的优秀图书，一定会为我国ISMS专业人才的培养起到重要的推动作用。



2012年9月

序言

prologue

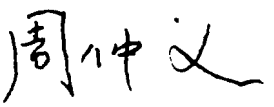
中国工程院院士 周仲义 推荐序

当前，国际上围绕信息的获取、分析、利用和控制的竞争越来越激烈，信息安全已成为维护国家安全、保持社会稳定、关系长远利益的关键组成部分，备受各国政府的关注和重视。如何确保信息安全已是各国政府及各种组织改进其竞争能力的一个新的具有挑战性的任务。

入选国家“十二五”重点图书规划的出版项目《信息安全管理体系丛书》，融入了作者多年来在信息安全、信息安全管理体系领域的研究和实践成果，包括多项具有自主知识产权的创新成果，是面向现代信息安全从业人员普及国家信息安全政策和信息安全知识，强化组织信息安全意识和信息安全保障能力建设，展示信息安全领域最新成果和信息安全管理体系建设、实施、运行、审核成就的高水平通俗读物。

该套丛书共有13个分册，主要内容涉及信息安全风险管理和风险评估、信息安全管理体系实施、信息安全管理体系审核、业务连续性管理、信息安全管理体系与ISO/IEC 20000的整合、信息安全管理体系与信息系统安全等级保护的整合以及信息安全管理体系在重点行业和领域的应用。书中各种典型的案例，针对各种网络安全问题的应对措施，为组织提供了一个完整的业务不间断计划，能为组织业务的正常运行起到保驾护航的作用。

该套丛书主要作者长期从事信息安全领域的科学研究与实践，曾参与多项信息安全国家标准的制修订，经验丰富，成果丰硕。他们编著的这套《信息安全管理体系丛书》，可代表现阶段我国信息安全管理体系领域最高研究水平，在服务于国家或组织，提升国家安全战略方面将起到非常重要的作用，必将产生显著的社会效益。该套丛书的出版，在我国工程技术领域是具有重要意义的大事，将为我国信息安全保障能力建设提供有力的支撑，让信息安全管理体系真正成为对抗信息霸权主义、抵御信息侵略的重要保障。



2012 年 9 月

丛书前言

Series introduction

信息通信技术（ICT）的快速发展和广泛应用，为人类开拓出继陆、海、空、天之外的第五维生存空间——赛博空间（Cyberspace）。ICT 的潜能不但使赛博空间展现出前所未有的美好前景，也为人类在陆、海、空、天的生产活动、科学研究以及知识学习、文化传承与交流和社会管理带来了高效率、高效益。信息化成为当今社会发展的巨大推动力。

但是，在新技术的应用中，风险和机遇并存。技术的不成熟，使得社会犯罪分子利用这些技术的漏洞谋取利益；霸权国家为其核心利益展现的把赛博空间作为新的战争空间的国策，使赛博空间显现出不和谐、不安宁的不良态势。

探究当代各国的信息安全战略和实践可知，提升信息安全保障能力是应对危机的对策，技术与管理并重是保障能力提升的出路，风险管理是指导保障能力形成的思想。

保障能力体现于预警能力、保护能力、检测能力、响应能力、恢复能力和反制能力。

技管并重要求，信息安全保障能力建设不但需要运用技术手段，还要运用管理手段，并且要运用技术手段支持管理手段，运用管理手段提升技术手段应有作用的有效发挥。

风险管理的思想使我们清醒地认识到，面对信息系统的应用，我们实际上是面对一个人机结合的、智能化的、非线性的时变复杂大系统。我们所做的防护努力，只能减少信息安全事件发生的可能性和发生事件

的损失及影响。绝对杜绝事件的发生是不可能的，我们必须积极应对处置可能发生的事件，保障依赖信息系统要完成的使命。

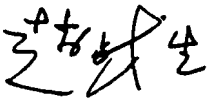
信息安全已经从关注技术平台发展到关注业务使命和组织治理。信息安全保障也提升到了依赖信息化手段的使命保障。我们需要跟上这个提升，研究思考和部署更高层次的安全保障。

信息安全管理的理论和实践，已经从依据长官意志的人治型管理，经由制度化建设的规章型管理，发展到了根据管理理论和成功实践经验加以规范化、标准化的体系化管理。ISO/IEC SC 27 的 27000 系列标准将不断丰富和完善的信息安全管理体系（ISMS）展现在我们面前。发达国家结合国情，也各自拥有与 27000 系列指导思想相一致的相关标准（例如美国国家技术标准研究所开发颁布的风险管理框架 NIST 特别出版物 SP 800 的相关系列标准）。我国信息安全标准化技术委员会已经把 27000 系列定为国家标准，同时结合国情颁布了若干为等级保护所需要的信息安全管理标准和风险评估、风险管理、事件分级分类、处置、灾难备份恢复等国家标准。

本系列丛书的目的在于跟踪国际和国家标准的发展，分析解析标准的内涵要义，试图帮助读者加深理解标准，也试图以总结作者的实践案例来宣贯标准，帮助读者正确地实施标准，执行标准。

信息安全保障能力是信息化条件下的综合国力的体现，能力低下必定吃亏挨打。我们不能满足我国信息化的发展速度和规模。我们必须依靠自己和世界上平等待我的朋友一起共建赛博家园，保障赛博家园的安康。

中国科学院信息安全国家重点实验室



2012 年 8 月

前言

preface

随着信息化的发展，信息安全已经成为关系国家安全、经济发展和社会稳定的重大战略问题，受到各国政府的高度关注。美国将网络和计算机视为国家战略资产，将其安全列为国家安全的优先事项。2009 年以来，各国纷纷出台或调整信息安全战略，维护和扩大自身在网络空间的地位与利益，对信息安全的重视达到了空前的高度。

信息安全认证认可在保障信息安全中发挥着基础性的作用，也是各国的通行做法。原国信办在 2006 年曾启动试点专项，研究 ISO/IEC 27001 在我国的适用性以及在提升企业信息安全水平中发挥的作用，商务部随即出台“千百十工程”等相关鼓励政策，自此拉开了各类组织纷纷按照国际标准实施信息安全体系化管理并积极申请认证的序幕。据不完全统计，截至今年上半年，我国已有超过 1200 家企业获得信息安全管理体系认证证书，企业的人员意识、信息安全管理水平得到了一定的提高。

国家对于信息安全管理体系工作非常重视。2010 年，工信部、质检总局、人民银行、国资委等六部委出台了《关于加强信息安全管理体系认证的安全管理的通知》。文件明确提出：“开展信息安全管理体系认证，有利于各单位规范信息安全管理，有利于企业特别是服务外包企业开拓国际市场”。南方电网、银监会、保监会等行业主管部门和地方政府也出台了相关鼓励政策，支持企业通过信息安全管理体系方面的工作降低安全风险、提升信息安全管理水平。2011 年我国《国民经济和社会发展第十二个五年规划纲要》在“加强网络与信息安全保障”章节中更是提出

“健全网络与信息安全法律法规，完善信息安全标准体系和认证认可体系”，以期进一步发挥信息安全认证认可在信息安全保障中的作用。

中国信息安全认证中心作为我国专注于信息安全认证的国家机构，开展了信息安全产品认证、信息安全服务资质认证、ISO 27001 与 ISO 20000 认证、人员认证及相关培训业务，也是截至目前我国唯一一个可以开展 ISO 20000 认证的认证机构。我们的 ISO 27001 认证客户群体涵盖银行、期货、证券、电力、能源、航空、政府、教育及上市企业等重点领域，我们在对 ISMS 标准的理解和体系认证方面积累了许多大型案例和丰富的实践经验。相对于传统的质量管理体系，信息安全管理体系是一个较新的领域，我们在审核工作中发现，无论是企业、咨询公司还是业界的审核人员，对 ISO 27001 的作用都充满了期待，但部分从业人员由于技术背景的限制只会注重标准条款的字面意思，知其然不知其所以然，对标准吃不准，理解不透，从而使得企业的体系咨询、运行水平不高，风险评估和控制措施脱节。部分业界审核员按照传统 ISO 9000 的惯性思路去审，不但不能有效地对体系情况开展客观的合格评定活动，帮助客户持续改进，反而会助推企业产生一个庞大臃肿且与业务并不切合的高风险体系。正因为此，我们感到肩上有一个责任，推动我们去寻找一个适宜的平台将我们积累的经验与大家进行交流和分享，以期共同提高，为企业输出高水准的认证服务。中国质检出版社约稿编纂新版的《信息安全管理体系审核指南》恰好提供了这样一个机会。

本书分为七章，从审核基础、标准族介绍、认证流程介绍到审核实施等逐步展开。其中，第 2 章“ISMS 标准族介绍”，将 ISMS 标准族所有标准的进展情况更新到今年 3 月份；第 6 章“信息安全控制措施审核”借鉴了 ISO/IEC 27008 的最新进展，较详细地介绍了控制恶意代码的技术检查，审计日志控制措施的技术检查，特殊权限管理控制措施的技术检查，备份控制措施的技术检查，网络安全管理控制措施的技术检查，

用户职责管理控制措施技术检查的检查内涵、检查方法和相关证据要求，为从业人员理解控制措施的有效性检查和审核点起到抛砖引玉的作用。第7章“ISMS结合审核”的内容也借鉴了ISO/IEC 27013的部分思想，从风险管理、有效性测量、信息安全事件管理、变更管理、容量管理、相关方管理和业务连续性管理7个方面，分析了两个标准的针对性要求和结合审核方法。

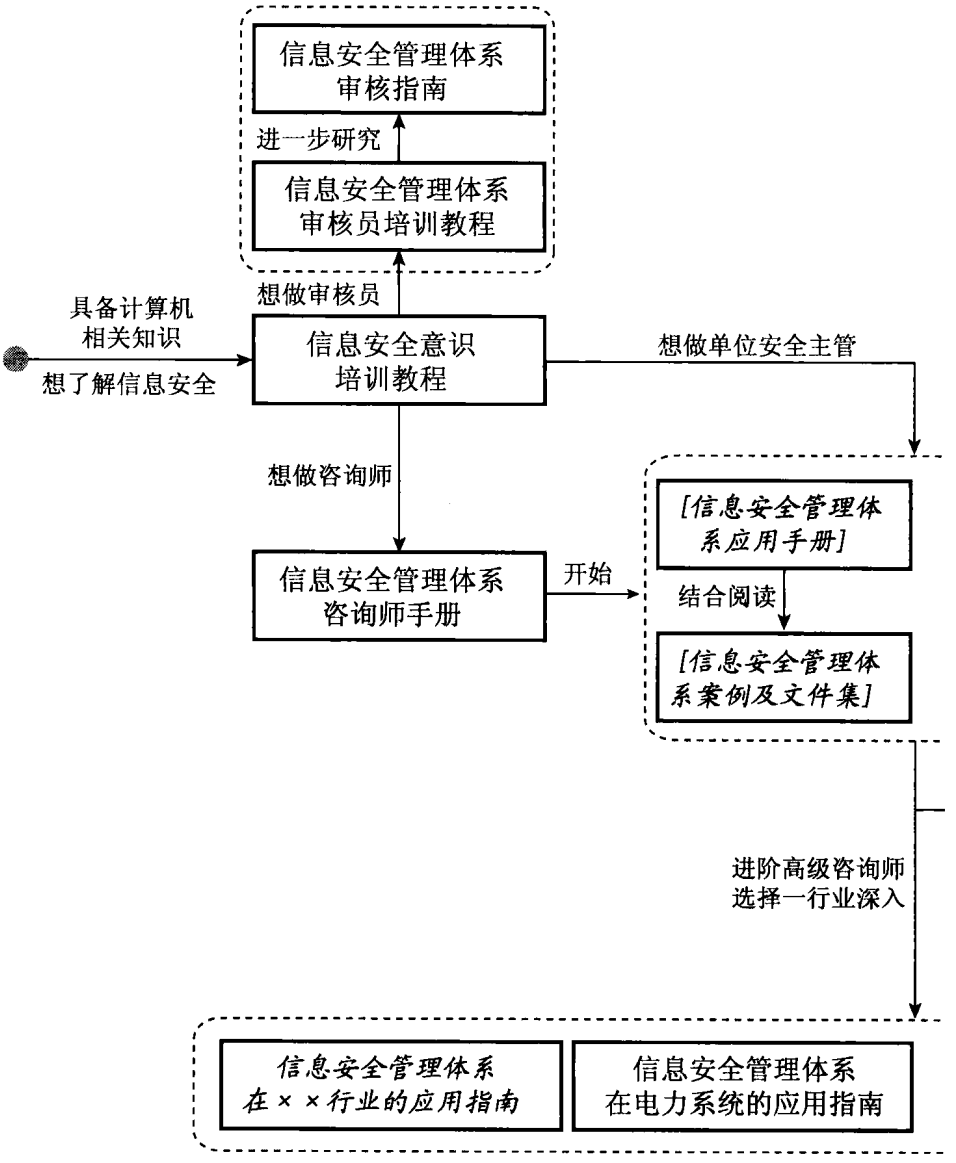
本书第2、3、4、6、7章的编写人员主要包括尤其、王明、朱博、李旭、李智、程瑜琦、亓明和、赵杰、陈鑫和左晓栋。他们的辛勤付出为本书尽快付梓提供了保障。本书成稿过程中，更是得到了崔书昆、赵战生、吕述望、戴英侠、李爱东、骆絮飞、温红子、庞翔、刘晓红、董德山等老师的指导，缴远、张庆元（信达资产）、杨文艳、韩建国（人民银行）、孙洋、马兰（东方资产）、范原辉、谢以清、蒋勇青、侯凯涛（农行）、顾俊（工行）、卢士达（上海电力）、刘树吉、赵永彬（辽宁电力）、唐云海、穆银芳（中信银行）、王啸（广发行）、罗玲（招商银行）、金典、张建华（上海电信）、杨威（中金所）、黄昌来（上期所）等专家也提出了宝贵经验，在此表示感谢。

诚然，时间仓促，还有些内容和想法不能在这一版实现，略有遗憾。更由于作者学识有限，谬误之处难免，恳请读者批评指正。对于书中的谬误或讨论，可直接发至我的信箱：weij@isccc.gov.cn或xiezongxiao@vip.163.com。

魏 军

2012年8月6日

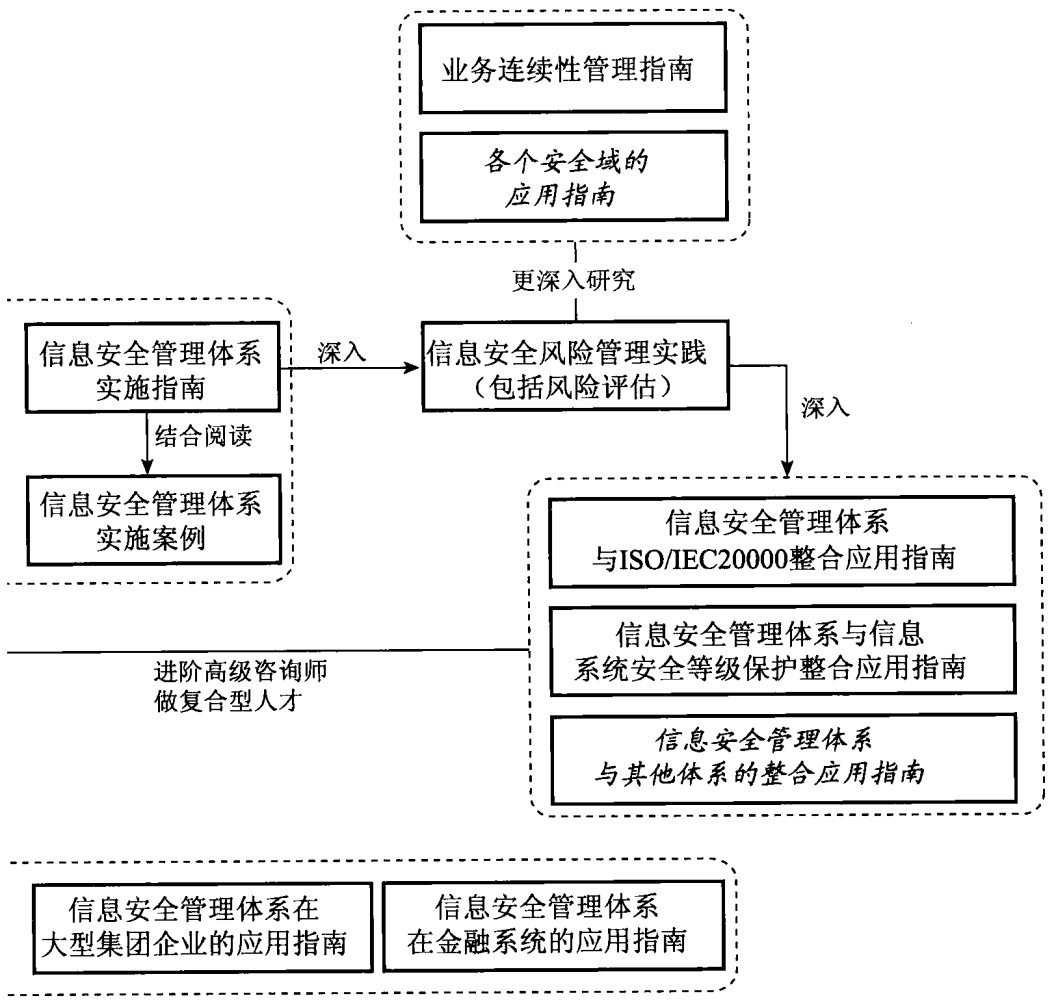
信息安全管理体系丛书阅读指南



备注：

1）*仿宋斜体*，表示限于篇幅，未列入本次出版计划中；

2）*[楷体斜体]*，表示该书已经出版，与本丛书有一定互补。



目录

contents