信息安全管理体系丛书

北京知识安全工程中心　编著

信息安全管理体系审核指南

中国标准出版社

策划编辑：张　宁　　封面设计：徐东彦　　责任校对：刘宝灵
责任编辑：王　成　　版式设计：李　玲　　责任印制：邓成友

《信息安全管理体系丛书》包括以下7册：

- 信息安全管理体系教程——国家注册ISMS审核员培训教程
- 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——概念、方法和实践
- 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——ISMS内审员培训教程

ISBN 978-7-5066-4532-4
9 787506 645324 >
定价：26.00 元

销售分类建议：信息技术

信息安全管理体系审核指南

Guidelines for Information Security Management Systems Auditing

陈珍成　编著

中国标准出版社
北京

内 容 简 介

本书对ISMS(信息安全管理体系)审核的基础知识、ISMS审核员的能力要求、ISMS总体认证审核过程、ISMS审核活动、ISMS审核的方法和步骤、ISO/IEC 27001:2005要求的符合性审核、控制目标和控制措施的符合性审核、结合审核等内容做了全面而翔实的阐述。

本书适用于希望成为ISMS审核员的人员,ISMS管理人员、ISMS审核员(外部审核员和内部审核员)、ISMS开发和维护人员,以及其他欲了解ISMS标准知识和审核知识的人员。

图书在版编目(CIP)数据

信息安全管理体系审核指南/陈珍成编著. —北京:中国标准出版社,2007
(信息安全管理体系丛书)
ISBN 978-7-5066-4532-4

Ⅰ. 信… Ⅱ. 陈… Ⅲ. 信息系统-安全管理-体系-中国-指南 Ⅳ. TP309-62

中国版本图书馆CIP数据核字(2007)第085125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 9.25 字数 208千字
2007年7月第一版 2007年7月第一次印刷
*
定价 **26.00** 元

信息安全管理体系丛书

Serials of Information Security Management Systems

北京知识安全工程中心 编著

丛书编辑委员会

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

进入21世纪，ISO与IEC先后发布了许多管理体系标准。其中，最新的，并已受到广泛关注的标准是信息安全管理标准(ISO/IEC 27001:2005和ISO/IEC 17799:2005)。

ISO先前发布的质量、环境等管理体系标准早已为人们所熟悉。同时，由于ISO也配套地发布了相关审核指南，例如《质量和(或)环境管理体系审核指南》(即ISO 19011:2002)，因此人们对于基于这些标准的管理体系的审核，也并不感到很困难。

然而，对于基于ISO/IEC 27001:2005的信息安全管理体系(ISMS)的审核，不管是审核员还是管理者都觉得是一种新的挑战。

ISMS审核是一个新项目。为了完成这个项目，审核人员和管理者不仅需要正确地与透彻地理解相关标准，而且也需要有丰富的综合知识、审核技能、沟通能力和组织能力，更需要有公正与忠诚等良好的道德和一丝不苟的认真负责的精神。

随着开发ISMS的组织迅速增多，对ISMS符合性的和高效率的审核显得更加重要，但是目前尚未发现有完全适合ISMS审核的量身度作的指南。基于这些考虑，我们编写本书——基于ISO/IEC 27001:2005标准的ISMS审核指南。

本书旨在帮助ISMS审核员和管理者执行ISMS审核，使ISMS审核既能符合ISO/IEC 27001:2005标准的要求，又能与ISO 19011保持一致，成为帮助受审核的组织完成其目标、改进其工作的一个增值活动。

本书的期望读者是ISMS审核员(包括内部审核员和外部审核员)、ISMS管理人员、ISMS开发人员和维护人员等。本指南也可作为ISMS咨询培训机构的参考教材。审核员可以使用本指南帮助其成功地完成审核任务，也可以使用本指南检查和提高其自己的知识和技能。实际上，与信息安全有关的和对信息安全感兴趣的任何人都可以从本指南获得信息安全审核等相关方面的系统知识。特别是，那些对信息安全标

准仍有疑点或疑问的人，应能从本书找到满意的答案。

本指南对于其他管理体系的审核人员也可提供十分有价值的参考。

本书的正文部分含有7章。

第1章“ISMS审核基础”由浅入深地介绍与信息安全管理体系(ISMS)审核相关的关键的基本概念，目的是提供读者以坚实的、丰富的基础知识，以便其很好地理解和掌握本书后面各章节的内容。

第2章“ISMS审核员的能力需要”描述审核员是成功审核的关键因素。本章从多方面论述审核的“能力”，包括个人素质、知识和技能等；同时还论述审核员如何获得和提高所需要的能力，特别强调教育、培训、研究和实践的重要性。

第3章“总体认证审核过程”阐述认证机构(即第三方)以证书的颁发与维护为主要目的，而应开展的一系列的审核(外部审核)，包括预审核、初次审核、监督审核和重新评估审核等。本章的目的是提供ISMS审核员和相关人员以ISMS认证的总体审核过程。

第4章“ISMS审核活动”详细地描述可应用于各类审核(包括内部审核和外部审核等)具有共同性的审核活动。本章与第3章“认证审核过程”有一定的必要的重叠，可互为补充和参照。

第5章“ISO/IEC 27001要求的符合性审核”提供了审核人员以如何确保“ISMS符合ISO/IEC 27001:2005标准要求”的详细指导：透彻地分析和清晰地列出ISO/IEC 27001:2005标准的每一条强制性要求；提出这些要求是否获得满足的具体检查表；详细地解释其中的关键点和疑难点；强调审核人员应确实地把好“确保ISMS符合ISO/IEC 27001:2005标准要求”的质量关。

第6章“控制目标和控制措施的符合性审核”为ISMS审核人员和信息安全管理人员，对ISO/IEC 27001:2005附录A的符合性审核提供足够详细的指南。本章描述了11个信息安全领域下的39个控制目标和133个控制措施，以及为如何满足这些控制措施提出相应的检查表。同时，本章注意到ISO/IEC 27006，并把其审核方法作为附录A的符合性审核的补充。

第7章“结合审核”对正在成为一个新的、对审核员具有挑战性的、越来越重要的竞争论题——多个管理体系的“结合审核”，提供了应有的概要性的指导。

由于编者水平有限，书中谬误之处在所难免，敬请读者提出宝贵意见。

2007年5月17日

目 录

第1章 ISMS审核基础

为了使读者能很好地理解和掌握本书后面各章节的内容。本章由浅入深地介绍某些关键的基本概念。

1.1 信息

1.1.1 什么是信息

在信息时代的今天，信息(Information)已成为企业赖以生存和发展的最有价值的资产之一，犹如维持生命所必须的血液。从不同的角度，信息可有多个并不矛盾的定义。以下是一些可供参考的定义。

(1) 信息是一种类似其他重要业务资产，任何组织的业务所必要的、因而需要加以适当保护的资产。而资产是指对组织具有价值的任何事物。(来自 ISO/IEC 17799:2005)

(2) 信息是经过组织并变得有意义、可理解的数据。(来自"A Glossary of Computer and Communications Jargon" http://www.christlinks.com/glossary2.html)

(3) 信息是可以进行沟通的事实、概念，或指示；任何类型的知识或假定。(来自"Engineering Data Management Glossary" http://cedar.web.cern.ch/CEDAR/glossary.html#Information)

(4) 信息是经过加工处理的、以适合人类理解的方式表示的、常常具有启迪作用的数据。(来自"Glossary"http://www.cbu.edu/~lschmitt/I351/glossary.htm)

(5) 信息是将数据以增添接收者知识的方式，进行加工处理和组织的结果。(来自"Glossary of Terms "www.orafaq.com/glossary/faqglosi.htm 25-Nov-2006)

1.1.2 信息的类型

信息可保存于多种不同的存储介质，包括纸介质、电磁光介质(如硬盘、软盘、磁带、U盘和光盘等)和物理环境(如办公室、文件柜和抽屉等)等。特别值得注意的是，信息还可以保存于人的大脑。

(1) 按信息的存储介质划分，信息主要类型应包括(但不限于)：

- 纸文件 (包括印刷品和手写笔记等)；
- 电子文件(包括计算机文件、e-mail 文件、录像带和录音带等)；
- 交谈信息(包括电话和面对面谈话等)。

在实际工作中，为了简化管理，某些组织常常把一个系统（如信息系统和服务器系统等）作为一类信息。如果一个系统含有多于一个以上机密级别的信息或文件，那么这个系统必须按照其最机密的信息保护需要进行分类[见下面(2)]。

(2) 从信息的重要性和需要保护的等级角度，许多组织常把信息分为以下类型：

- 公开信息——非保密信息。
- 保密信息，从低到高依次又分为3个不同的级别：

——内部信息；

——机密信息；

——绝密信息。

内部、机密和绝密信息属于密级信息，是受保护的资产，只能为已被授权者访问。不同密级的信息有不同的保密要求。信息的分类级别决定了该信息受控制和安全保护的程度，也表示其在业务上的价值。特别是绝密信息，是一类高度敏感的、安全级别最高的信息。这类信息对组织的发展至关重要。对其破坏，或未授权访问，不管是来自外部的，还是内部的，组织都会受到极其严重的危害。

在信息安全体系建设中，一个十分重要的活动就是识别要保护的信息资产。而审核的一个重要任务之一也是检查这些要保护的信息资产是否获得识别和受到与其类别（或价值）相当的保护。

1.1.3 信息的生命周期

信息要经历创建、存储、处理、传输、使用、老化和消亡等阶段。从信息的创建到消亡所经历的时间称为信息的生命周期。信息在创建、存储、处理、传输和使用中，如果不加以适当保护，就会出现安全问题。

1.2 信息安全

1.2.1 什么是信息安全

信息安全(Information security)是指确保对组织具有重要意义的信息的机密性、完整性和可用性，以及真实性、责任性、不可否认性和可靠性等。

信息的机密性、完整性和可用性对维持组织的竞争优势、盈利性、合法性和商业形象至关重要。信息的机密性、完整性和可用性中的一个或多个的损失都可以威胁组织的继续存在。

(1) 机密性(Confidentiality)：信息不能被未授权的个人、实体或者过程利用或泄漏的特性。

(2) 完整性(Integrity)：保护信息的完整性是指保护信息和信息处理方法的准确性和完全性。这里，最重要的是要防范未授权者篡改信息。

(3) 可用性(Availability)：资产可被已授权的实体根据其需要进行访问和利用的特性。如果一个已授权的实体（包括个人和过程）在其需要某个资产时，能够访问和利用该资产，那么这个资产达到可用性。从信息安全标准看，资产应包括信息、系统、设施、网络和计算机系统等。所有这些资产必须为已授权的实体，在其需要时能够得到使用。

1.2.2　信息安全的威胁源

信息可能受到多方面的威胁。威胁可能来自内部，也可能来自外部，可能是无意的，也可能是恶意的。此外，信息安全的威胁还可能来自自然灾害。据国外调查和报道，威胁信息安全的人（包括无意的和恶意的），80％以上来自组织内部的员工。在一个组织内，每一个人（包括上至最高领导下至普通员工）在信息安全的管理上都扮演一个角色。其工作、活动和行为对信息安全都有一定的影响。表 1-1 示出某些威胁信息安全的例子。

表 1-1　威胁信息安全的例子

(1)	缺乏信息安全意识的员工（包括当前的员工和以前的员工），滥用或误用机密信息，更改数据和未授权访问等
(2)	内外人员的意外行为，包括意外地把错误数据输入到系统，造成系统含有不正确的信息等
(3)	系统发生故障，包括硬件缺陷、软件缺陷、相关系统不可用和其他问题等
(4)	竞争对手，盗窃和破坏商业机密等
(5)	恶意代码（包括病毒和特洛伊木马等），造成数据损坏、服务中断和系统损害等
(6)	电脑黑客（或解密高手）入侵系统、盗窃和破坏信息等
(7)	自然灾害（包括洪水、地震和火灾等），造成数据损失、服务中断、系统损害和员工受伤（或麻烦）等
(8)	其他

1.2.3　如何实现信息安全

信息安全的成功解决方法，是正确地建立、实施和维护一个如 ISO/IEC 27001:2005 标准所描述的信息安全管理体系。

1.3　信息安全管理体系

1.3.1　什么是信息安全管理体系

1.3.1.1　“体系”的含义

“信息安全管理体系”（Information Security Management System，简称 ISMS）中的“体系”来自英文“System”。“System”当然可翻译为“体系”，但通常也翻译为“系统”。同样，“Management System”当然可翻译为“管理体系”，但通常也翻译为“管理系统”。例如在计算机领域中，一个十分常见的术语“Database Management System”，被普遍公认地翻译为“数据库管理系统”（简称 DBMS），而几乎没有人将其翻译为“数据库管理体系”。很显然，如果把“Information Security Management System”翻译为“信息安全管理系统”，也未尝不可。