科飞管理咨询公司　编著

信息安全管理丛书

BS 7799和ISO/IEC 17799信息安全管理体系及其认证认可相关知识问答

中国标准出版社

信息安全管理丛书

BS7799和ISO/IEC17799
信息安全管理体系及其认证认可
相关知识问答

科飞管理咨询公司 编著

中国标准出版社

内 容 简 介

本书涉及到 BS 7799 和 ISO /IEC 17799 几乎全部的要点，也包括两个标准在发展中的一些问题。全书共分为五章，其中包括：BS 7799 的术语和定义，BS 7799-2 标准的适用范围、PDCA 过程模式、信息安全管理体系文件编写，风险评估方面的问题，在应用 ISO /IEC 17799 过程中可能遇到的问题及认证、认可相关的疑问等。

本书适合企事业单位信息化管理者、电子政务管理者、信息安全管理者、信息安全服务提供者以及信息安全管理研究人员、爱好者参考使用。

图书在版编目(CIP)数据

BS 7799 和 ISO/IEC 17799 信息安全管理体系及其认证认可相关知识问答/科飞管理咨询公司编著．—北京：中国标准出版社，2003

ISBN 7-5066-3249-7

Ⅰ．B… Ⅱ．科… Ⅲ．①信息系统－安全管理－国家标准，BS 7799－英国－问答②信息系统－安全管理－国际标准，ISO/IEC 17799－问答 Ⅳ．TP309-65

中国版本图书馆 CIP 数据核字(2003)第 071448 号

中国标准出版社出版(北京复兴门外三里河北街 16 号) 邮政编码：100045 电 话：68523946 68517548

中国标准出版社秦皇岛印刷厂印刷 新华书店北京发行所发行 各地新华书店经售

网址 www. bzcbs. com

开本 880×1230 1/32 印张 8¾ 字数 205 千字

2003 年 9 月第一版 2003 年 9 月第一次印刷

印数 1—4 000 定价：25.00 元

本书编写组名单

组长　门洪利

主编　于海霞　吴昌伦

编委　俎全胜　孙洪涛　王毅刚

前　言

当今世界，信息对企业生存和发展的作用越来越大，已经成为关系企业核心竞争力的重要资源，如何保障信息安全这个课题也备受瞩目。近几年，在众多的信息安全标准中，信息安全管理标准 BS 7799 脱颖而出，从管理和技术的角度，通过建立、实施、保持并持续改进信息安全管理体系来保障组织的信息安全。BS 7799 已在全球范围内得到广泛的应用，被翻译成多种语言版本，甚至还被许多国家转化为国家标准。

组织在进行信息化建设，尤其是在进行信息安全规划、安全建设和验收的时候，或者在按照 BS 7799 标准建立信息安全管理体系的时候，经常对一些问题存在理解上的差异。为了减少理解分歧，帮助组织更好地把信息安全工作做好，我们编写了本书。

本书涉及到 BS 7799 和 ISO/IEC 17799 几乎全部的要点，也包括两个标准在发展中的一些问题。问题主要来源包括：ISMS 国际用户组织（IUG）注册用户普遍关注的问题、科飞公司与国际知名认证机构在信息安全管理领域广泛探讨的问题、读者对《信息安全管理概论——BS 7799 理解与实施》的反馈信息、我们在进行信息安全管理咨询过程中遇到的典型问题等。

全书共分为五章。第一章：BS 7799 和 ISO/IEC 17799 概括性问题，主要涵盖了 BS 7799 的术语和定义、组成、发展、相关的信息安全管理标准，BS 7799-1 国际

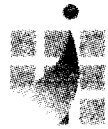
化进程以及 ISO/IEC 17799 相关的问题；第二章：BS 7799-2 涉及的问题，主要涵盖了 BS 7799-2 标准的适用范围、PDCA 过程模式、信息安全管理体系文件编写，以及 BS 7799-2 修订的相关内容；第三章：风险评估涉及的问题，主要解答了风险评估相关的术语和定义、风险评估方法的分类和定义，以及评估方法的选择等方面的问题；第四章：ISO/IEC 17799（BS 7799-1）涉及的问题，主要解答了在应用 ISO/IEC 17799 过程中可能遇到的问题，按照标准的结构，分节予以解释；第五章：有关认证、认可的问题，主要解答了认证、认可相关的疑问和信息安全管理体系认证认可的发展状况，以及与信息安全管理体系审核员相关的问题。

本书面向的读者群包括企事业单位的信息化管理者、电子政务管理者、信息安全管理者、信息安全服务提供者以及信息安全管理研究人员、爱好者。随着人们对信息安全管理重视程度的提高，将会有越来越多的人想对 BS 7799 有更深层、更全面、更准确的理解，我们希望本书能够加强您对 BS 7799 和 ISO/IEC 17799 标准的理解，推动企业的信息安全管理工作更好地开展。

由于信息安全管理是一个新兴的行业，也是一门新兴的学问，在我国的应用还刚刚起步，加之编者对信息安全的了解和认识毕竟有限，书中难免有不当之处，敬请广大读者批评指正。

编　　者

2003 年 7 月



目　录

第一章　BS 7799 和 ISO/IEC 17799 概括性问题

第二章 BS 7799-2 涉及的问题

第三章 风险评估涉及的问题