BS 7799信息安全管理体系认证指南

王英梅　屈　微　卢大航　编著

中国计量出版社

BS 7799 信息安全管理体系认证指南

王英梅　屈　溦　卢大航　编著

中国计量出版社

图书在版编目（CIP）数据

BS 7799 信息安全管理体系认证指南/王英梅，屈微，卢大航编著 .—北京：中国计量出版社，2004.8

ISBN 7-5026-2031-1

Ⅰ. B… Ⅱ. ①王… ②屈… ③卢… Ⅲ. 信息系统—安全管理—国家标准，BS 7799—英国—指南 Ⅳ. TP309-65

中国版本图书馆 CIP 数据核字（2004）第 084819 号

内 容 提 要

本书全面系统地讲解了 BS 7799 信息安全管理体系标准的基础知识，包括 BS 7799-1（ISO 17799）和BS 7799-2：2002的理解和应用，对各条款做了详细而深入的剖析；介绍了信息安全管理体系建立和运行的全过程，尤其对风险评估和文件编制两个环节做了重点阐述，并给出详细的文件案例；论述了认证审核的概念、过程和规定；以信息安全管理体系与质量管理体系，即 BS 7799 标准与 ISO 9000 族标准结合为例，阐述了信息安全管理体系与其他管理体系整合的要点。

本书适合于信息安全管理人员和技术人员及管理体系的咨询和培训人员使用，也可供大专院校相关专业的师生阅读。

中国计量出版社出版

北京和平里西街甲 2 号

邮政编码 100013

电话（010）64275360

E-mail jlfxb@263.net.cn

北京市迪鑫印刷厂印刷

新华书店北京发行所发行

*

787 mm×1092 mm 16 开本 印张 18.5 字数 409 千字

2004 年 12 月第 1 版 2004 年 12 月第 1 次印刷

*

印数 1—3 000 **定价：38.00 元**

前　言

本书是北京凝瑞资讯有限公司与信息安全相关学科的专家联合编写的一本信息安全管理体系建设、实施和认证的系统理论和实践书籍，可用作审核人员培训教材，也可供有关人员理论研究参考。本书重点介绍信息安全管理体系标准（BS 7799 标准）的知识以及在实施标准和进行认证中有关问题的解决方案；从信息安全管理标准的理解切入，依照理解——实施——认证——与其他管理体系整合的逻辑顺序，对信息安全管理体系的准备、实施和过程监控及对系统认证进行系统描述。就本书所涉及的范围和知识广度而言，对于从事信息安全管理理论研究、信息安全管理体系的管理人员和相关技术人员、信息安全管理体系审核和认证人员都会有重要的参考价值。

本书包括四个部分。其中，第一部分共 3 章，介绍了信息安全管理标准的基本知识，包括 BS 7799 的两个部分的理解及应用，是建立信息安全管理体系的依据，也是本书的讨论框架和范围；第二部分由 4，5，6 章构成，介绍了信息安全管理体系建立的概念，以及体系运行和实施过程中风险评估和文件编写；第三部分包括 7，8，9，10 章，是按照前几章介绍的方法建立组织的信息安全管理体系后，指导组织如何申请、通过和持续认证；最后部分是一个开放性和研究性的课题，我们提出了有关信息安全管理体系与其他管理体系整合和一体化认证的观点，这在国际和国内，都是一个新颖的论题，虽然观点和理论还不成熟，但此方向上的探讨还是很有价值的。

全书取材于实践和理论，涉及的内容十分广泛。读者可根据需要在内容和深度方面自行选择阅读和使用。

由于本书涉及 BS 7799 标准和信息安全管理体系这个应时代发展而新兴的课题，其内容和理论中有许多值得研究和探讨之处，尽管作者已尽了最大努力，但因水平所限，书中难免有错误和不妥之处，望读者不吝赐教斧正，以利于今后相关系列书籍的编写和不断完善，推动我国信息安全管理体系建设和认证工作的开展。

编著者

2004 年 8 月

目　录

第一章　信息安全管理概论

第二章　BS 7799 标准控制措施理解及选取

第三章 BS 7799 标准规范理解及实施

第四章 信息安全管理体系概述

第五章 信息安全风险评估

第六章 信息安全管理体系文件编写

第七章　信息安全管理体系认证

第八章 认证中组织应了解的有关问题

第九章 认证后组织深入贯彻的有关问题

第十章 认证和咨询机构的选择

第十一章 信息安全管理体系与其他管理体系的整合

第一章

信息安全管理概论

1 信息安全管理相关概念

(1) 信息

● 从任何来源得到的知识。

——一般词典

● 信息是一种物质，在某种关系中对于它的接受者有意义。一些信息可以转换成数据和传递给其他接受者。

——计算机词典

● 信息是一种资产，向组织的其他重要的业务资产一样，对组织具有价值，因此需要妥善保护。

不管信息以何种形式出现，以何种方式被分享，存储于何种介质中，它都应该被妥善保护。

——ISO/IEC 17799：2000

(2) 信息资产的表现形式

● 纸面上；

● 电子存储设备中；

● 传递（通过邮政或电子手段）中；

● 以其他方式展示出来；

● 交谈中流露出来。

(3) 信息安全

信息安全是对所说、所写及计算机中的信息的保密性、完整性和可用性进行保护，使信息免受来自方方面面的威胁，以保证组织业务的连续性，最大程度地减少业务损失，并使投资回报和商务机会最大化。

信息安全的三个基本成分：

a) 保密性——保证信息只被有授权的人访问；

b) 完整性——保护信息和处理方法的准确性和完整性；

c) 可用性——保证有授权的使用者在需要时能够访问信息及其相关资产。

(4) 信息安全管理

信息安全不仅是技术过程，更是一个管理过程。

(5) 信息安全管理体系

信息安全管理体系（Information Security Management System，ISMS）是指通过计划、组织、领导、控制等措施以实现组织信息安全目标的相互关联或相互作用的一组要素。

2 社会发展对信息的依赖给信息安全提出新的挑战

人类社会进入信息时代，信息不只意味着财富和实力，同时成为衡量国家实力、安全、主权的实质依据和基本参照。信息的开发、控制和利用是目前各国研究的焦点，甚至成为事关国家兴衰强弱的核心。信息空间已成为继陆、海、空、天之后，引发又一轮国际竞争的新的第五维战略空间。近几年来，面对日益激烈的信息争夺战和不断蔓延的网络犯罪现象，世界各国政府普遍意识到信息安全对其国家利益的重要性，从技术、管理、法律等角度构筑自己的信息安全防线。美国是最早也是最重视建构信息安全体系的国家。它通过安全的信息技术和产业使自己的经济和科技站在世界前沿。与此同时，它也试图利用互联网将自己的价值观影响全球，以期维护其政治、经济、军事和信息的霸权地位。因此，美国提出了全民防御的“国家信息安全保障”政策。信息是组织的血液，存在方式各异：可以是打印、手写，也可以是电子、演示和口述的。当今商业竞争日趋激烈，来源于不同渠道的信息，威胁着信息的一致性。它们来自内部、外部、意外的，还可能是恶意的。随着信息储存、发送新技术的广泛使用，我们面临的各种风险也在增高。信息科技进步，因特网兴起，电子商务深入企业，新的犯罪也跟随科技发展而产生，所以信息安全管理成为今日各企业的重要课题。

在这扑面而来的信息时代，我国也面临着同样的挑战。信息成为重要的战略资源，信息对抗是当代全球开放网络中的普遍现象，是未来信息战的主要内容。网络中的信息截获与反截获、破译与反破译、入侵与反入侵等都是信息对抗所涉及的问题。主动攻击（包括各种侦听、病毒制造与释放等）和被动防御（包括审计、追踪、防病毒等）是目前网络环境下信息对抗的使用手段，而网络环境下的安全体系结构研究是保证信息安全的关键，包括计算机安全操作系统、各种安全协议、安全机制（数字签名、信息认证、数据加密等），直至安全系统，其中任何一个安全漏洞都可以威胁全局安全。面对信息安全面临的大量问题，很多学者从技术和管理的角度进行了不同程度的研究，希望通过某种方式能够保证信息的安全。在人们的不断实践中发现，信息安全“三分技术，七分管理”的特点很突出。再先进的技术手段，离开科学合理的管理也不能发挥全部的作用。因此，管理体系的建立在保证信息安全过程中发挥重要的作用。

目前国内的企业基本上已全面运用了信息系统来对企业的各种资源进行管理，以降低运

营成本、提高生产力并快速响应顾客的需求，从而获得最大的商业利润。随着信息系统的广泛应用，信息安全问题也就越来越受到人们的关注。现在人们的安全意识已经普遍增强，在新构建的信息系统中，已经没有人不考虑安全问题了。然而就普遍的情况来看，人们对安全问题的认识还只是停留在技术层面上，很少有人从管理的角度去看问题，更不要说从系统管理的角度去解决问题。由此就产生了这样的现象：企业花了很多的钱去购买信息安全产品，但却不知道本企业的信息安全状况到底如何，还有哪些问题需要注意。这种状况是很令人担忧的。为使信息系统能够为组织的业务运作提供强有力的支持，必须要有一套管理体系来了解信息系统与资源运作的现状，进而采取必要的改善措施，以防患未然。

3 信息安全管理标准

BS 7799 是目前世界上应用最广泛、最典型的信息安全管理标准。它涵盖了安全管理所应涉及的方方面面，全面而不失可操作性，提供了一个可持续提高的信息安全管理环境。BS 7799 可以解决信息安全管理中的众多问题，它是一套最完整的建立信息安全管理体系的参考方法与依据，用来指导组织构建自己的信息安全管理体系，确保信息系统与资源的安全，确保信息系统与资源能持续运作且发挥最大效益。企业可以参照信息安全管理模型，建立组织完整的信息安全管理体系并实施与保持，达到动态、系统、全员参与、制度化、以预防为主的信息安全管理要求，用最低的成本达到可接受的信息安全水平，从根本上保证业务的连续性。

BS 7799 把信息定义为一种资产，并从资产管理的角度去考虑信息安全的管理问题。它不仅说明了如何去构建一个信息安全管理体系，而且还指出了如何对该体系进行评价以及如何运作、维护与改进，因而是一个操作性很强的、具有很大实际意义的标准。

3.1 BS 7799 的历史发展

英国标准 BS 7799 是目前世界上应用最广泛与最典型的安全管理标准，它是在 BSI/DISC的 BDD/2 信息安全管理委员会指导下制定完成的。BS 7799 标准于 1993 年由英国贸易工业部立项。1995 年于英国首次出版了 BS 7799－1：1995《信息安全管理实施细则》，它提供了一套综合的、由信息安全最佳惯例组成的实施规则，其目的是作为确定各类信息系统通用控制范围的惟一参考基准，并使其适用于大中小组织。在第一部分编写的过程中，不同行业的大公司和企业都为标准的编写提供了经验的支持。如在金融服务业中，英国保险协会、英格兰和威尔士渣打会计协会、内部审核员协会、劳埃德检测、全国建筑协会、汇丰银行，通信业中大英电讯公司和 Racal Network Services 等都提供了自己在信息安全管理方面的心得和容易存在的问题。包括大型零售行业 Marks and Spencer plc 以及壳牌、联合利华、毕马威等国际公司，都为第一部分的组织和内容提供了建议和验证。可见《信息安全管理实施细则》是在实践中不断积累的产物，它积累和凝炼了不同行业的特点和不同的关注点，因此具有一定的普适性。1998 年英国公布了该标准的第二部分 BS 7799－2《信息安全管理体系规范》，它规定信息安全管理体系要求与信息安全控制要求，是一个组织全面或部分的信