信息安全的体系化管理

—ISMS在电子政务中的应用

主　编　于　军
副主编　傅首清　丁志明　张泽根　詹榜华

国防工业出版社
National Defense Industry Press

信息安全的体系化管理

——ISMS在电子政务中的应用

主　编　于　军

副主编　傅首清　丁志明

张泽根　詹榜华

国防工业出版社

·北京·

图书在版编目(CIP)数据

信息安全的体系化管理:ISMS在电子政务中的应用/于军主编.
—北京:国防工业出版社,2008.6
ISBN 978-7-118-05682-2

Ⅰ.信… Ⅱ.于… Ⅲ.电子政务—安全技术 Ⅳ.D035.1-39

中国版本图书馆CIP数据核字(2008)第053602号

※

国防工业出版社出版发行

(北京市海淀区紫竹院南路23号 邮政编码100044)

国防工业出版社印刷厂印刷

新华书店经售

*

开本 850×1168 1/32 **印张** 7¼ **字数** 150千字

2008年6月第1版第1次印刷 **印数** 1—4000册 **定价** 24.00元

(本书如有印装错误,我社负责调换)

国防书店:(010)68428422 发行邮购:(010)68414474

发行传真:(010)68411535 发行业务:(010)68472764

编委会名单

主　　编　于　军

副 主 编　傅首清　丁志明　张泽根

　　詹榜华

编写组成员　王　晖　梁爱民　付海涛

　　王　西　田春可　尚小鹏

专家顾问组　崔书昆　赵战生　毛东军

　　孙志宜　吴志刚　刘海峰

　　徐国爱　周喜东　李德全

序1

信息安全的复杂性、综合性决定了信息安全既是高技术的对抗，也是科学管理的对抗，建设信息安全保障体系必须采用科学规范的方法和手段。《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)明确提出，信息安全保障要坚持积极防御、综合防范的方针，要坚持管理与技术并重的原则。为此，国务院信息办在税务、证券等重要信息系统和北京市、上海市、武汉钢铁集团公司等开展信息安全管理标准应用的试点工作，探索利用在国际上被称为最佳实践的信息安全管理标准来建立信息安全管理体系的可行性；检验信息安全管理标准的适用性、合理性；了解和掌握构建信息安全管理体系的程序、步骤和方法；探索信息安全管理体系与风险评估和等级保护等工作的关系。

此次试点历时十个月，各单位精心部署、周密

此为试读，需要完整PDF请访问：www.ertongbook.com

计划、认真实施，通过与各自的技术支撑单位密切合作，完成了组织动员、宣传培训、起草工作方案、配合专家组调研、参加中期交流会、编写并颁布体系文档、实施管理体系、运行管理体系等一系列工作。北京市海淀区作为试点中取得优异成绩的单位，紧密把握面向业务需求、面向风险控制的原则，在精心梳理业务流程和全面分析安全风险的基础上，完成了信息安全管理体制、机制和相关制度的建设，初步形成了一套完整的安全管理体系。需要特别指出的是，海淀区在体系建立过程中十分注意与等级保护相结合，注意与已建立的ISO9001质量管理体系相结合，保证了体系具有很强的实用性。通过此次试点，海淀区不仅提高了信息安全保障水平，而且总结出了在政府部门建立科学规范、全面精细的信息安全管理体系的方法和经验。因此这本以此试点经验为基础，充满了实践智慧的书，对有志于通过信息安全管理体系建设来提高信息安全保障水平的地区、部门和单位，都具有很好的参考价值和借鉴意义。

建立和实施ISMS是一项复杂、庞大的系统工程，涉及的知识领域广，覆盖的部门和人员多。要搞好此项工作，需要我们总结并推广好此次试点的经

验，加快相关国家标准的制订，完善相关认证管理工作，积极推动相关工具的研发，希望更多的有识之士参与到此项工作中来。

国务院信息化工作办公室

副司长　熊四皓

2007 年 10 月

序2

随着信息化的普及和深入，北京正在步入信息社会。对于政府来说，网络和信息系统已成为提高政府工作效率、监管能力和服务水平不可或缺的重要手段，不少电子政务系统成为保障城市健康、有序运转的基础设施，搞好信息安全保障已不仅仅关系到信息系统的安全可靠运行，而且关系到城市安全、社会稳定，对于即将举办奥运会的北京市来说，保障信息安全具有十分重要的意义。

信息安全管理体系建设是信息安全保障体系建设的重要内容，通过体制、机制和制度建设，形成多层次的完备安全责任体系，将“谁主管谁负责，谁运行谁负责”的要求落到实处，并建立从策略目标到具体安全控制措施、安全管理程序和记录的有效运转体系。得益于国信办组织的信息安全管理标准应用试点，北京市信息安全保障体系的建设，在科学化、规范化、精细化方面得到了有力的推进，大大促进了我市政府信

息安全管理水平的提高。我市信息化发展水平很高的海淀区政府在此次试点中，严格按照信息安全管理标准的要求，紧密结合自身实际，按照 PDCA 模型，围绕明确目标策略、健全安全组织、落实安全责任、确立安全措施、建立工作机制和流程等环节，形成了一套完备的文档化的管理体系，切实解决了以往信息安全管理“头痛医头，脚痛医脚”的凭感觉、“拍脑袋”现象。

本书以海淀区建立信息安全管理体系的具体实践为基础，作者结合实际讲述了如何理解标准、如何按照标准要求在政府部门建立 ISMS、如何与信息安全等级保护相结合、如何与区政府已建立的 ISO9001 质量管理体系相融合的经验，是一本源于实践的创新之作，相信对广大致力于科学建立信息安全管理体系的读者一定会有所启迪，书中的方法和经验对政府部门的实践者将很有参考价值。

北京市信息化工作办公室

副主任　白　新

2007 年 8 月

前　言

2006年3月，国务院信息化工作办公室启动了“信息安全管理体系标准应用试点”工作，试点工作的主要任务和目标是：“检验信息安全管理标准的适用性、合理性；了解和掌握构建信息安全管理体系的程序、步骤和方法；探索信息安全管理体系与风险评估和等级保护等工作的关系”。北京市海淀区政府是这次试点工作的试点单位之一，通过在海淀区电子政务系统建立和实施基于ISO/IEC27001：2005的信息安全管理体系，以实现试点工作的任务和目标。

ISO/IEC27001：2005是由国际标准化组织信息技术委员会安全分技术委员会（ISO/IEC JTC1/SC27）于2005年10月15日正式发布的系列信息安全管理体系国际标准之一，是管理体系标准中的“要求”类标准，是组织建立和实施信息安全管理体系的要求和依据，也是用于认证的依据。

海淀区电子政务的任务是建立起以信息技术为

基础的、系统的政府管理体系、服务体系和监督体系，提高行政效率，降低行政成本。其建设过程历经“数字园区”、“数字政府”和“数字海淀”三个重点建设阶段。从1998年开始进行“数字园区”一期工程建设，2000年7月28日成功开通数字园区电子政务网上审批系统至今，海淀区电子政务办公自动化系统及政府内部事务网上协同处理电子政务已覆盖区内90%的政府机构，90%以上的政府服务业务和60%以上的政府管理业务均实现了网上处理，为海淀区国民经济与社会的发展与进步提供了坚实的基础保障。

网络与信息安全已经成为海淀区电子政务面临的突出问题，传统的网络与信息安全方法和手段以采购和使用安全产品为主，往往是“事件驱动型的”，或者是“产品导向型的”，其结果常常是“头痛医头，脚痛医脚”。海淀区电子政务的发展要求系统化地分析和解决信息安全问题，尤其要预防为主，防患于未然。国信办组织的这次试点工作为体系化解决海淀区电子政务中的信息安全问题提供了契机。

在国信办和市信息办的领导下，海淀区政府信息办圆满完成了这次试点任务。接到试点工作任务后，海淀区政府信息办聘请北京数字认证中心作为此次试点的技术支撑单位，并联合成立了项目工作组。在

此为试读，需要完整PDF请访问：www.ertongbook.com

项目工作组坚苦卓绝的努力下，于2006年12月成功完成了试点工作，在海淀区政府初步建立了符合国际标准ISO/IEC27001：2005的信息安全管理体系。

作为对此次试点工作的总结和探索，我们把试点工作中的点点滴滴汇集成册，希望对我国的信息安全管理体系的发展带来一些帮助。也希望通过这本册子，与国内外同行就信息安全管理体系标准以及信息安全管理体系的建设和实施进行交流。

北京市海淀区区委常委

副区长　于军

2008年1月

目　录

此为试读，需要完整PDF请访问：www.ertongbook.com