ICS 35.040
L 80

中华人民共和国国家标准

GB/T 22080—2008/ISO/IEC 27001:2005

信息技术　安全技术
信息安全管理体系　要求

Information technology—Security techniques—Information security management systems—Requirements

(ISO/IEC 27001:2005, IDT)

2008-06-19 发布　　2008-11-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

GB/T 22080—2008/ISO/IEC 27001:2005

中华人民共和国
国家标准
信息技术　安全技术
信息安全管理体系　要求
GB/T 22080—2008/ISO/IEC 27001:2005
*
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 880×1230　1/16　印张 2　字数 47 千字
2008年9月第一版　2008年9月第一次印刷
*
书号:155066·1-33396　定价 24.00 元

GB/T 22080-2008

参 考 文 献

标准出版物

[1] GB/T 19001—2000 质量管理体系 要求

[2] GB /T 19011—2003 质量和(或)环境管理体系审核指南

[3] GB/T 24001—2004 环境管理体系要求及使用指南

[4] GB/Z 20985—2007 信息技术 安全技术 信息安全事件管理

[5] ISO/IEC 指南 62:1996 从事质量体系的评估和认证/注册的机构的通用要求

[6] ISO/IEC 指南 73:2002 风险管理 术语 标准使用指南

[7] ISO/IEC 13335-1:2004 信息技术 安全技术 信息和通信技术安全管理 第 1 部分:管理和规划 ICT 安全的概念和模型

[8] ISO/IEC TR 13335-3:1998 信息技术 IT 安全管理指南 第 3 部分:IT 安全管理技术

[9] ISO/IEC TR 13335-4:2000 信息技术 IT 安全管理指南 第 4 部分:防护措施的选择

其他出版物

[1] OECD. OECD 信息系统和网络安全指南——面向安全的文化. 巴黎:OECD,2002 年 7 月. www. oecd. org

[2] NIST SP 800-30 信息技术系统的风险管理指南.

[3] Deming W. E. Out of the crisis,剑桥,Mass:MIT,高级工程研究中心,1986.

目 次

附 录 C
（资料性附录）
GB/T 19001—2000，GB/T 24001—2004 和本标准之间的对照

表 C.1 显示了 GB/T 19001—2000、GB/T 24001—2004 和本标准之间的对应关系。

表 C.1 GB/T 19001—2000、GB/T 24001—2004 和本标准之间的对应关系

本标准	GB/T 19001—2000	GB/T 24001—2004
0 引言 0.1 总则 0.2 过程方法 0.3 与其他管理体系的兼容性	0 引言 0.1 总则 0.2 过程方法 0.3 与 GB/T 19004 的关系 0.4 与其他管理体系的相容性	引言
1 范围 1.1 总则 1.2 应用	1 范围 1.1 总则 1.2 应用	1 范围
2 规范性引用文件	2 引用标准	2 规范性引用文件
3 术语和定义	3 术语和定义	3 术语和定义
4 信息安全管理体系 4.1 总要求 4.2 建立和管理 ISMS 4.2.1 建立 ISMS 4.2.2 实施和运行 ISMS 4.2.3 监视和评审 ISMS 4.2.4 保持和改进 ISMS 4.3 文件要求 4.3.1 总则 4.3.2 文件控制 4.3.3 记录控制	4 质量管理体系 4.1 总要求 8.2.3 过程的监视和测量 8.2.4 产品的监视和测量 4.2 文件要求 4.2.1 总则 4.2.2 质量手册 4.2.3 文件控制 4.2.4 记录控制	4 EMS 要求 4.1 总要求 4.4 实施和运行 4.5.1 监视和测量 4.5.2 合规性评价 4.4.5 文件控制 4.5.4 记录控制
5 管理职责 5.1 管理承诺	5 管理职责 5.1 管理承诺 5.2 以顾客为关注焦点 5.3 质量方针 5.4 策划 5.5 职责、权限和沟通	 4.2 环境方针 4.3 策划
5.2 资源管理 5.2.1 资源提供 5.2.2 培训、意识和能力	6 资源管理 6.1 资源提供 6.2 人力资源 6.2.2 能力、意识和培训 6.3 基础设施 6.4 工作环境	 4.4.2 能力、培训和意识
6 ISMS 内部审核	8.2.2 内部审核	4.5.5 内部审核

前 言

本标准等同采用 ISO/IEC 27001:2005《信息技术 安全技术 信息安全管理体系 要求》，仅有编辑性修改。

本标准的附录 A 是规范性附录，附录 B 和附录 C 是资料性附录。

本标准由中华人民共和国信息产业部提出。

本标准由全国信息安全标准化技术委员会归口。

本标准由中国电子技术标准化研究所、上海三零卫士有限公司、北京知识安全工程中心、北京市信息安全测评中心、北京数字认证中心负责起草。

本标准主要起草人：上官晓丽、许玉娜、胡啸、王新杰、赵战生、王连强、曾波、孔一童、刘海峰、汤永利、尚小鹏、闵京华。