



中华人民共和国国家标准

GB/T 22080—2016/ISO/IEC 27001:2013
代替 GB/T 22080—2008

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 27001:2013, IDT)

2016-08-29 发布

2017-03-01 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

目 次

前言	III
引言	IV
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 组织环境	1
4.1 理解组织及其环境	1
4.2 理解相关方的需求和期望	1
4.3 确定信息安全管理体系统范围	1
4.4 信息安全管理体系统	2
5 领导	2
5.1 领导和承诺	2
5.2 方针	2
5.3 组织的角色,责任和权限	2
6 规划	2
6.1 应对风险和机会的措施	2
6.2 信息安全目标及其实现规划	4
7 支持	4
7.1 资源	4
7.2 能力	4
7.3 意识	4
7.4 沟通	4
7.5 文件化信息	5
8 运行	5
8.1 运行规划和控制	5
8.2 信息安全风险评估	5
8.3 信息安全风险处置	6
9 绩效评价	6
9.1 监视、测量、分析和评价	6
9.2 内部审核	6
9.3 管理评审	6
10 改进	7
10.1 不符合及纠正措施	7
10.2 持续改进	7
附录 A (规范性附录) 参考控制目标和控制	8

GB/T 22080—2016/ISO/IEC 27001:2013

附录 NA (资料性附录) GB/T 22080—2016 与 GB/T 22080—2008 版对比	18
附录 NB (资料性附录) GB/T 22080—2016 与 GB/T 22080—2008 主要关键词变化	20
参考文献	21