



中华人民共和国国家标准

GB/T 31509—2015

信息安全技术 信息安全风险评估 实施指南

Information security technology—Guide of implementation for
information security risk assessment

2015-05-15 发布

2016-01-01 实施

中华人民共和国国家质量监督检验检疫总局 发布
中国国家标准化管理委员会

目 次

前言	III
引言	IV
1 范围	1
2 规范性引用文件	1
3 术语、定义和缩略语	1
4 风险评估实施概述	2
4.1 实施的基本原则	2
4.2 实施的基本流程	3
4.3 风险评估的工作形式	3
4.4 信息系统生命周期内的风险评估	4
5 风险评估实施的阶段性工作	4
5.1 准备阶段	4
5.2 识别阶段	10
5.3 风险分析阶段	21
5.4 风险处理建议	24
附录 A (资料性附录) 调查表	28
附录 B (资料性附录) 安全技术脆弱性核查表	35
附录 C (资料性附录) 安全管理脆弱性核查表	45
附录 D (资料性附录) 风险分析案例	52

前 言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:国家信息中心、国家保密技术研究所、北京信息安全测评中心、上海市信息安全测评认证中心、沈阳东软系统集成工程有限公司、国和信诚(北京)信息安全有限公司。

本标准主要起草人:吴亚非、禄凯、张志军、陈永刚、赵章界、席斐、应力、马朝斌、倪志强。