



# 中华人民共和国国家标准

GB/T 20984—2007

## 信息安全技术 信息安全风险评估规范

Information security technology—  
Risk assessment specification for information security

2007-06-14 发布

2007-11-01 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

## 目 次

前言 .....	I
引言 .....	II
1 范围 .....	1
2 规范性引用文件 .....	1
3 术语和定义 .....	1
4 风险评估框架及流程 .....	3
4.1 风险要素关系 .....	3
4.2 风险分析原理 .....	3
4.3 实施流程 .....	4
5 风险评估实施 .....	5
5.1 风险评估准备 .....	5
5.2 资产识别 .....	6
5.3 威胁识别 .....	8
5.4 脆弱性识别 .....	10
5.5 已有安全措施确认 .....	11
5.6 风险分析 .....	12
5.7 风险评估文档记录 .....	13
6 信息系统生命周期各阶段的风险评估 .....	14
6.1 信息系统生命周期概述 .....	14
6.2 规划阶段的风险评估 .....	14
6.3 设计阶段的风险评估 .....	15
6.4 实施阶段的风险评估 .....	15
6.5 运行维护阶段的风险评估 .....	16
6.6 废弃阶段的风险评估 .....	16
7 风险评估的工作形式 .....	17
7.1 概述 .....	17
7.2 自评估 .....	17
7.3 检查评估 .....	17
附录 A (资料性附录) 风险的计算方法 .....	18
A.1 使用矩阵法计算风险 .....	18
A.2 使用相乘法计算风险 .....	21
附录 B (资料性附录) 风险评估的工具 .....	24
B.1 风险评估与管理工具 .....	24
B.2 系统基础平台风险评估工具 .....	25
B.3 风险评估辅助工具 .....	25
参考文献 .....	26

## 前 言

本标准的附录 A 和附录 B 是资料性附录。

本标准由国务院信息化工作办公室提出。

本标准由全国信息安全标准化技术委员会归口。

本标准主要起草单位：国家信息中心、公安部第三研究所、国家保密技术研究所、中国信息安全产品测评认证中心、中国科学院信息安全国家重点实验室、解放军信息技术安全研究中心、中国航天二院七〇六所、北京信息安全测评中心、上海市信息安全测评认证中心。

本标准主要起草人：范红、吴亚非、李京春、马朝斌、李嵩、应力、王宁、江常青、张鉴、赵敬宇。