

NIST 特别出版物 800-30

第 1 修订版

**NIST**

**National Institute of  
Standards and Technology**

Technology Administration  
U.S. Department of Commerce

# 风险评估

# 实施指南

转型方案联合任务组

内部资料 翻译：高卓

## 信息安全

计算机安全部  
信息技术实验室  
国家标准和技术研究所

Gaithersburg, MD 20899-8930

2012 年 9 月



美国商务部

代理部长：Rebecca M. Blank

国家标准和技术研究所

负责标准和技术的商务部副部长

兼NIST所长：Patrick D. Gallagher

北京江南天安科技有限公司



# 目录

## 第1章 概述

- 1.1 目的和适用性
- 1.2 适用对象
- 1.3 相关出版物
- 1.4 篇章结构

## 第2章 基本信息

- 2.1 风险管理流程
- 2.2 风险评价
- 2.3 关键风险概念
- 2.4 风险评价应用

## 第3章 流程

- 3.1 准备风险评价
- 3.2 实施风险评价
- 3.3 沟通交流和共享风险评价信息
- 3.4 保持风险评价

## 附录 A 参考文献

## 附录 B 术语表

## 附录 C 缩略语

## 附录 D 威胁源

## 附录 E 威胁事件

## 附录 F 脆弱性和诱发条件

## 附录 G 发生可能性

## 附录 H 影响

## 附录 I 风险确定

## 附录 J 为风险响应提供依据

## 附录 K 风险评价报告

## 附录 L 任务汇总

