

NIST 特别出版物 800-59

NIST

**National Institute of
Standards and Technology**

Technology Administration
U.S. Department of Commerce

信息系统风险管理：

机构、任务和信息系统三重视角

转型方案联合任务组

信息安全

国家标准和技术研究所
信息技术实验室
计算机安全处

Gaithersburg, MD 20899-8930

2011年3月



美国商务部
部长：Gary Locke

国家标准和技术研究所
所长：Patrick D. Gallagher

目录

第 1 章 概述

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

第 2 章 基本原理

- 2.1 风险管理的组成部分
- 2.2 多层级风险管理
- 2.3 第 1 层——机构视角
- 2.4 第 2 层——任务/业务流程视角
- 2.5 第 3 层——信息系统视角
- 2.6 信任和可信性
- 2.7 机构文化
- 2.8 关键风险概念之间的关系

第 3 章 流程

- 3.1 框定风险
- 3.2 评价风险
- 3.3 响应风险
- 3.4 监测风险

附录 A 参考文献

附录 B 术语表

附录 C 缩略语

附录 D 角色和责任

附录 E 风险管理流程任务

附录 F 治理模式

附录 G 信任模式

附录 H 风险响应战略