ICS 35.040
L 80

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

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。

引　言

随着政府部门、企事业单位以及各行各业对信息系统依赖程度的日益增强，信息安全问题受到普遍关注。运用风险评估去识别安全风险，解决信息安全问题得到了广泛的认识和应用。

信息安全风险评估就是从风险管理角度，运用科学的方法和手段，系统地分析信息系统所面临的威胁及其存在的脆弱性，评估安全事件一旦发生可能造成的危害程度，提出有针对性的抵御威胁的防护对策和整改措施，为防范和化解信息安全风险，将风险控制在可接受的水平，最大限度地保障信息安全提供科学依据。

信息安全风险评估作为信息安全保障工作的基础性工作和重要环节，要贯穿于信息系统的规划、设计、实施、运行维护以及废弃各个阶段，是信息安全等级保护制度建设的重要科学方法之一。

本标准条款中所指的“风险评估”，其含义均为“信息安全风险评估”。

信息安全技术
信息安全风险评估规范

1 范围

本标准提出了风险评估的基本概念、要素关系、分析原理、实施流程和评估方法，以及风险评估在信息系统生命周期不同阶段的实施要点和工作形式。

本标准适用于规范组织开展的风险评估工作。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本标准，然而，鼓励根据本部分达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

GB/T 9361 计算站场地安全要求

GB 17859—1999 计算机信息系统安全保护等级划分准则

GB/T 18336—2001 信息技术 安全技术 信息技术安全性评估准则(idt ISO/IEC 15408:1999)

GB/T 19716—2005 信息技术 信息安全管理实用规则(ISO/IEC 17799:2000,MOD)

3 术语和定义

下列术语和定义适用于本标准。

3.1

资产 asset

对组织具有价值的信息或资源，是安全策略保护的对象。

3.2

资产价值 asset value

资产的重要程度或敏感程度的表征。资产价值是资产的属性，也是进行资产识别的主要内容。

3.3

可用性 availability

数据或资源的特性，被授权实体按要求能访问和使用数据或资源。

3.4

业务战略 business strategy

组织为实现其发展目标而制定的一组规则或要求。

3.5

保密性 confidentiality

数据所具有的特性，即表示数据所达到的未提供或未泄露给非授权的个人、过程或其他实体的程度。

3.6

信息安全风险 information security risk

人为或自然的威胁利用信息系统及其管理体系中存在的脆弱性导致安全事件的发生及其对组织造成的影响。