ICS 35.040
L 80

中华人民共和国国家标准化指导性技术文件

GB/Z 24364—2009

信息安全技术
信息安全风险管理指南

Information security technology—
Guidelines for information security risk management

2009-09-30 发布　　2009-12-01 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

本指导性技术文件的附录A为资料性附录。

本指导性技术文件由全国信息安全标准化技术委员会提出并归口。

本指导性技术文件起草单位：国家信息中心信息安全研究与服务中心、中国电信股份有限公司北京研究院。

本指导性技术文件主要起草人：吴亚非、张鉴、范红、刘蓓、赵阳。

引　言

一个机构要利用其拥有的资源来完成其使命。在信息时代，信息成为第一战略资源，更是起着至关重要的作用。因此，信息资产的安全是关系到该机构能否完成其使命的大事。资产与风险是天生的一对矛盾，资产价值越高，面临的风险就越大。信息资产有着与传统资产不同的特性，面临着新型风险。信息安全风险管理的目的就是要缓解并平衡这一对矛盾，将风险控制到可接受的程度，保护信息及其相关资产，最终保证机构能够完成其使命。

信息安全风险管理是信息安全保障工作中的一项基础性工作，主要表现在以下几方面：

信息安全风险管理的思想和措施应体现在信息安全保障体系的技术、组织和管理等全方位。由于在信息安全保障体系的技术、组织和管理等方面都存在着相关风险，因此，在信息安全保障体系中，技术、组织、管理中均应引入风险管理的思想，准确地评估风险并合理地处理风险，共同实现信息安全保障的目标。

信息安全风险管理的思想和措施应贯穿于信息系统生命周期的全部过程。信息系统生命周期包括规划、设计、实施、运维和废弃五个阶段。每个阶段都存在着相关风险，同样需要采用信息安全风险管理的思想加以应对，采用风险管理的措施加以控制。

信息安全风险管理的思想和措施是贯彻信息安全等级保护制度的有力支撑。信息安全风险管理依据信息安全等级保护的思想和原则，区分主次，平衡成本与效益，合理部署和利用信息安全的保护机制、信任体系、监控体系和应急处理等重要的基础设施，选择并确定合适的安全控制措施，从而保证机构具有完成其使命所需要的信息安全保障能力。

为落实国家加强信息安全保障工作的要求，为实施信息安全等级保护制度的需要，制定本指导性技术文件。本指导性技术文件可与 GB/T 20984 结合使用，并可作为机构建立信息安全管理体系（ISMS）的参考。

本指导性技术文件参考了 ISO/IEC 27005 等国际信息安全风险管理的相关标准，并经过国家有关行业和地区的试点验证。标准针对信息安全风险管理所涉及的背景建立、风险评估、风险处理、批准监督、监控审查、沟通咨询等不同过程进行了综合性描述，对信息安全风险管理在信息系统生命周期各阶段的应用作了系统阐述。

本指导性技术文件条款中所指的“风险管理”，其含义均为“信息安全风险管理”。

本指导性技术文件中列出的带书名号的文档是示范性的，其格式和详细内容未作规范。

信息安全技术
信息安全风险管理指南

1 范围

本指导性技术文件规定了信息安全风险管理的内容和过程，为信息系统生命周期不同阶段的信息安全风险管理提供指导。

本指导性技术文件适用于指导组织进行信息安全风险管理工作。

2 规范性引用文件

下列文件中的条款通过本指导性技术文件的引用而成为本指导性技术文件的条款。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指导性技术文件，然而，鼓励根据本指导性技术文件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指导性技术文件。

GB 17859—1999 计算机信息系统安全保护等级划分准则

GB/T 18336.2—2008 信息技术 安全技术 信息技术安全性评估准则 第2部分：安全功能要求(ISO/IEC 15408-2:2005，IDT)

GB/T 20984—2007 信息安全技术 信息安全风险评估规范

GB/T 22081—2008 信息技术 安全技术 信息安全管理实用规则(ISO/IEC 27002:2005，IDT)

3 术语和定义

下列术语和定义适用于本指导性技术文件。

3.1

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。

[GB/T 20984]

3.2

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。

[GB/T 20984]

3.3

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。

[GB/T 20984]

3.4

完整性 integrity

保证信息及信息系统不会被非授权更改或破坏的特性。包括数据完整性和系统完整性。

[GB/T 20984]