ICS 35.040
L 80

中华人民共和国国家标准

GB/T 31509—2015

信息安全技术　信息安全风险评估实施指南

Information security technology—Guide of implementation for information security risk assessment

2015-05-15 发布　　2016-01-01 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

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:国家信息中心、国家保密技术研究所、北京信息安全测评中心、上海市信息安全测评认证中心、沈阳东软系统集成工程有限公司、国和信诚(北京)信息安全有限公司。

本标准主要起草人:吴亚非、禄凯、张志军、陈永刚、赵章界、席斐、应力、马朝斌、倪志强。

引　言

信息安全风险评估是信息安全保障工作的重要内容之一，与信息系统等级保护、信息安全检查、信息安全建设等工作紧密相关，并通过风险发现、分析、评价为上述相关工作提供支持。

为指导信息安全风险评估工作的开展，本标准依据《信息安全技术　信息安全风险评估规范》(GB/T 20984—2007)，从风险评估工作开展的组织、管理、流程、文档、审核等几个方面提出了相关要求，是《信息安全技术　信息安全风险评估规范》(GB/T 20984—2007)的操作性指导标准，它也是信息安全风险管理相关标准之一。

信息安全技术　信息安全风险评估实施指南

1　范围

本标准规定了信息安全风险评估实施的过程和方法。

本标准适用于各类安全评估机构或被评估组织对非涉密信息系统的信息安全风险评估项目的管理，指导风险评估项目的组织、实施、验收等工作。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB/T 20984—2007　信息安全技术　信息安全风险评估规范

GB/Z 24364—2009　信息安全技术　信息安全风险管理指南

3　术语、定义和缩略语

GB/T 20984—2007 和 GB/Z 24364—2009 中界定的以及下列术语和定义适用于本文件。

3.1　术语和定义

3.1.1

实施　implementation

将一系列活动付诸实践的过程。

3.1.2

信息系统生命周期　information system lifecycle

信息系统的各个生命阶段，包括规划阶段、设计阶段、实施阶段、运行维护阶段和废弃阶段。

3.1.3

评估目标　assessment target

评估活动所要达到的最终目的。

3.1.4

系统调研　system investigation

对信息系统相关的实际情况进行调查了解与分析研究的活动。

3.1.5

评估要素　assessment factor

风险评估活动中必须要识别、分析的一系列基本因素。

3.1.6

识别　identify

对某一评估要素进行标识与辨别的过程。