ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 20984—2022
代替 GB/T 20984—2007

信息安全技术　信息安全风险评估方法

Information security technology—Risk assessment method for information security

2022-04-15 发布　　2022-11-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件代替GB/T 20984—2007《信息安全技术　信息安全风险评估规范》，与GB/T 20984—2007相比，除结构调整和编辑性改动外，主要技术变化如下：

a) 增加了“业务”和“信息系统生命周期”（见3.4和3.7）；

b) 删除了“业务战略”的术语和定义（见2007年版的3.4）；

c) 删除了“资产”“资产价值”“可用性”“保密性”“信息系统”“完整性”“残余风险”“安全事件”“威胁”和“脆弱性”的术语和定义（见2007年版的3.1、3.2、3.3、3.5、3.8、3.10、3.12、3.14、3.17和3.18）；

d) 更改了风险评估框架及流程中的风险要素关系、风险分析原理和评估实施流程（见第4章，2007年版的第4章）；

e) 更改了风险评估实施过程中风险要素识别和关联分析内容（见5.2和5.3，2007年版的5.2、5.3、5.4、5.5和5.6）；

f) 将原标准中评估对象生命周期各阶段的风险评估和风险评估的工作形式调整到规范性附录A和资料性附录B中（见附录A和附录B，2007年版的第6章和第7章）。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由全国信息安全标准化技术委员会（SAC/TC 260）提出并归口。

本文件起草单位：国家信息中心、北京安信天行科技有限公司、信息产业信息安全测评中心、北京信息安全测评中心、中国信息安全测评中心、中国网络安全审查技术与认证中心、中国电子技术标准化研究院、公安部信息安全等级保护评估中心、公安部第一研究所、上海观安信息技术股份有限公司、成都民航电子技术有限责任公司、河南金盾信安检测评估中心有限公司、深圳市南山区政务服务数据管理局、云南公路联网收费管理有限公司、国网宁夏电力有限公司、国网新疆电力有限公司。

本文件主要起草人：禄凯、詹榜华、陈永刚、刘丰、陈青民、赵增振、张益、高亚楠、任金强、刘龙涛、刘德林、刘凯俊、孙明亮、杜宇鸽、翟亚红、王惠莅、任卫红、彭海龙、李秋香、安佳伟、马勇、张军、汤志强、段明磊、杨童、肖强、张宏杰、刘育辰、陈涛、李峰。

本文件及其所代替文件的历次版本发布情况为：

——2007年首次发布为GB/T 20984—2007；

——本次为第一次修订。

信息安全技术　信息安全风险评估方法

1　范围

本文件描述了信息安全风险评估的基本概念、风险要素关系、风险分析原理、风险评估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。

本文件适用于各类组织开展信息安全风险评估工作。

2　规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改版）适用于本文件。

GB/T 25069　信息安全技术　术语

GB/T 33132—2016　信息安全技术　信息安全风险处理实施指南

3　术语和定义、缩略语

3.1　术语和定义

GB/T 25069 界定的以及下列术语和定义适用于本文件。

3.1.1

信息安全风险　information security risk

特定威胁利用单个或一组资产脆弱性的可能性以及由此可能给组织带来的损害。

注：它以事态的可能性及其后果的组合来度量。

[来源：GB/T 31722—2015，3.2]

3.1.2

风险评估　risk assessment

风险识别、风险分析和风险评价的整个过程。

[来源：GB/T 29246—2017，2.71]

注：本文件专指信息安全风险评估。

3.1.3

组织　organization

具有自身的职责、权威和关系以实现其目标的个人或集体。

注：组织的概念包括但不限于个体经营者、公司、法人、商行、企业、机关、合伙关系、慈善机构或院校，或者其部分或组合，无论注册成立与否、是公共的还是私营的。

[来源：GB/T 29246—2017，2.57，有修改]

3.1.4

业务　business

组织为实现某项发展规划而开展的运营活动。

注：该活动具有明确的目标，并延续一段时间。