ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 24364—2023
代替 GB/Z 24364—2009

信息安全技术
信息安全风险管理实施指南

Information security technology—
Implementation guide for information security risk management

2023-05-23 发布　　2023-12-01 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/Z 24364—2009《信息安全技术　信息安全风险管理指南》，与GB/Z 24364—2009相比，除结构调整和编辑性改动外，主要技术变化如下：

a) 标准对象和范围由面向信息系统修改为风险管理对象（见第1章）；

b) 删除了“可用性”“保密性”“完整性”“风险”“风险处理”的术语和定义（见2009年版的3.1、3.2、3.4、3.5、3.7）；

c) 增加了信息安全风险管理框架，增加了风险管理原则、保障机制、保障措施、管理能力等内容（见第4章）；

d) 更改了信息安全风险管理的内容和过程（见9.1，2009年版的4.2）；

e) 更改了语境建立流程，引入基本准则确定内容等（见9.2，2009年版的第5章）；

f) 更改了风险评估相关内容（见9.3，2009年版的第6章）；

g) 将监控审查改为监视与评审，并将相关内容更改（见9.6，2009年版的第9章）；

h) 更改了沟通与咨询相关内容（见9.7，2009年版的第10章）；

i) 删除了各生命周期阶段风险管理内容（见2009年版第11章、第12章、第13章、第14章、第15章）；

j) 更改了风险处置相关内容（见9.2、9.4，2009版的第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、中国电子科技集团公司第十五研究所、北京安信天行科技有限公司、北京天融信网络安全技术有限公司、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、深信服科技股份有限公司、北京信息安全测评中心、公安部第一研究所、公安部第三研究所、北京国信京宁信息安全科技有限公司、上海观安信息技术股份有限公司、郑州轻工业大学、河南农业大学、深圳市信息安全管理中心、广州市信息安全测评中心、深圳市龙华区政务服务数据管理局、深圳华晟九思科技有限公司。

本文件主要起草人：禄凯、陈永刚、赵增振、葛晓囡、陈青民、杨剑、刘润一、杜宇鸽、陈杨国、刘德林、程瑜琦、李媛、马江涛、李秋香、陈盼、陈一博、张益、刘健、刘丰、任金强、王焱、张锐卿、董安波、刘永杰、朱润酥、高杰、汤志强、朱建兴、李尚号。

本文件及其所代替文件的历次版本发布情况为：

——2009年首次发布为GB/Z 24364—2009；

——本次为第一次修订。

引　言

目前，信息安全风险管理标准主要包括：

——GB/T 24364—2023《信息安全技术　信息安全风险管理指南》；

——GB/T 26333—2010《工业控制网络安全风险评估规范》；

——GB/T 31722—2015《信息技术 安全技术　信息安全风险管理》(ISO/IEC 27005:2008,IDT)；

——GB/T 31509—2015《信息安全技术　信息安全风险评估实施指南》；

——GB/T 33132—2016《信息安全技术　信息安全风险处理实施指南》；

——GB/T 36637—2018《信息安全技术　ICT 供应链安全风险管理指南》；

——GB/T 20984—2022《信息安全技术　信息安全风险评估方法》；

——ISO 31000:2018《风险管理　指南》；

——ISO/IEC 27005:2018《信息技术　安全技术　信息安全风险管理》。

本文件作为信息安全风险管理标准之一，在修订过程中依据国家信息安全风险管理相关的政策并参考 GB/T 31722—2015、ISO 31000:2018、ISO/IEC 27005:2018 等标准，为组织的信息安全风险管理实施提供了更加具体的指导，包括信息安全风险管理的目标、原则、保障机制、保障措施、能力和过程等内容，表 1 给出了本文件与 ISO 31000:2018、GB/T 31722—2015、ISO/IEC 27005:2018 标准的风险管理过程的对应关系。

然而，本文件不指定信息安全风险管理的特定实施细节，组织可根据自身风险管理范围、风险管理语境或所处行业来确定其风险管理实施细节。其现有的方法也可在本文件描述的框架下使用，以满足风险管理工作的要求。

表 1　风险管理过程对应关系表

ISO 31000:2018	GB/T 31722—2015	ISO/IEC 27005:2018	本文件
范围、语境、准则	语境建立	环境创建	语境建立
风险评估	风险评估	风险评估	风险评估
风险处置	风险处置	风险处置	风险处置
—	风险接受	—	批准留存
沟通与咨询	风险沟通	沟通与咨询	沟通与咨询
监督与评审	风险监视与评审	监测与评审	监视与评审
记录与报告	—	—	批准留存
注：在本文件的第 9 章，对信息安全风险管理实施过程的概念、工作内容等进行了详细阐述。			

信息安全技术
信息安全风险管理实施指南

1 范围

本文件确立了信息安全风险管理的实施框架，描述了信息安全风险管理的原则、保障机制、保障措施、能力和过程，提供了每个管理过程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管理工作。

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(包括所有的修改单)适用于本文件。

GB/T 20984—2022 信息安全技术 信息安全风险评估方法

GB/T 24363—2009 信息安全技术 信息安全应急响应计划规范

GB/T 25069—2022 信息安全技术 术语

GB/T 29246—2017 信息技术 安全技术 信息安全管理体系 概述和词汇

GB/T 31509 信息安全技术 信息安全风险评估实施指南

GB/T 31722—2015 信息技术 安全技术 信息安全风险管理

GB/T 38645—2020 信息安全技术 网络安全事件应急演练指南

3 术语和定义、缩略语

3.1 术语和定义

GB/T 25069—2022、GB/T 29246—2017、GB/T 31722—2015 和 GB/T 20984—2022 中界定的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：以事态的可能性及其后果的组合来度量。

[来源：GB/T 25069—2022，3.681]

3.1.2

风险管理 risk management

指导和控制组织相关风险的协调活动。

[来源：GB/T 29246—2017，2.76]

3.1.3

业务 business

组织为实现某项发展战略而开展的运营活动。