ICS 35.030
CCS L 80

# 中华人民共和国国家标准

GB/T 31722—2025/ISO/IEC 27005:2022
代替 GB/T 31722—2015

# 网络安全技术　信息安全风险管理指导

**Cybersecurity technology—Guidance on managing information security risks**

（ISO/IEC 27005:2022，Information security，cybersecurity and privacy protection—Guidance on managing information security risks，IDT）

2025-08-01 发布　　2026-02-01 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 31722—2015《信息技术　安全技术　信息安全风险管理》,与GB/T 31722—2015相比,除结构调整和编辑性改动外,主要技术变化如下:

a) 删除了“影响”“信息安全风险”“风险规避”“风险估算”等术语及其定义(见2015年版的第3章);

b) 增加了“风险场景”“控制”等术语及其定义(见第3章);

c) 删除了“背景”(见2015年版的第5章);

d) 增加了“信息安全风险管理循环”(见5.2);

e) 更改了“信息安全风险评估过程”,增加了“基于事态的方法”“基于资产的方法”(见第7章,2015年版的第8章);

f) 增加了“运行”(见第9章);

g) 增加了“利用ISMS相关过程”(见第10章)。

本文件等同采用ISO/IEC 27005:2022《信息安全　网络安全和隐私保护　信息安全风险管理指导》。

本文件做了下列最小限度的编辑性改动:

——为与我国技术标准体系协调,将标准名称改为《网络安全技术　信息安全风险管理指导》。

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。

本文件由全国网络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:中国电子技术标准化研究院、北京安信天行科技有限公司、中国网络安全审查认证和市场监管大数据中心、中国合格评定国家认可中心、中国信息安全测评中心、黑龙江省网络空间研究中心、中电长城网际系统应用有限公司、山东省标准化研究院、北京天融信网络安全技术有限公司、广州民航信息技术有限公司、陕西省网络与信息安全测评中心、亚信科技(成都)有限公司、南方电网数字电网集团信息通信科技有限公司、新华三技术有限公司、国网网安(北京)科技有限公司、国家计算机网络应急技术处理协调中心、中国联合网络通信集团有限公司、启明星辰信息技术集团股份有限公司、北京神州绿盟科技有限公司、中科信息安全共性技术国家工程研究中心有限公司、杭州安恒信息技术股份有限公司、公安部第一研究所、北京山石网科信息技术有限公司、民航成都电子信息技术有限责任公司、北京中金云网科技有限公司、北京赛西认证有限责任公司、上海观安信息技术股份有限公司、上海三零卫士信息安全有限公司、北京时代新威信息技术有限公司、西北工业大学、国家能源集团新能源技术研究院有限公司。

本文件主要起草人:许玉娜、陈青民、林阳荟晨、王秉政、付志高、尤其、范科峰、李琳、王琰、方舟、曲家兴、白瑞、闵京华、公伟、雷晓锋、白旭东、杨婧婧、陆丽、王姣、朱雪峰、郑耀宗、李俊、廖双晓、王健、万晓兰、李祉岐、崔牧凡、靳蒲、胡月、郝少硕、胡建勋、陈星、吕由、李秋香、何伊圣、马勇、程燕、赵丽华、谢江、刘彪、王连强、王震、高超、张秋生、李京、吕方超。

本文件及其所代替文件的历次版本发布情况为:

——2015年首次发布为GB/T 31722—2015;

——本次为第一次修订。

# 引　言

本文件就以下方面提供指导：

——实现 GB/T 22080—2025 中规定的信息安全风险管理要求；应对信息安全相关风险的措施（见 GB/T 22080—2025 中 6.1 和第 8 章）；

——在信息安全环境下实现 GB/T 24353—2022 中的风险管理指导。

本文件包含风险管理的具体指导，并对 GB/T 31496—2023 进行了补充。

# 网络安全技术　信息安全风险管理指导

## 1　范围

本文件提供了指导，以帮助组织：

——满足 GB/T 22080—2025 有关应对信息安全风险活动的要求；

——实施信息安全风险管理活动，特别是信息安全风险评估和处置。

本文件适用于所有组织，无论其类型、规模或领域。

## 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。

ISO/IEC 27000　信息安全技术　信息安全管理体系　概述和词汇（Information security management systems—Overview and vocabulary）

注：GB/T 29246—2023　信息安全技术　信息安全管理体系　概述和词汇（ISO/IEC 27000:2018，IDT）

## 3　术语和定义

ISO/IEC 27000 界定的以及下列术语和定义适用于本文件。

ISO 和 IEC 维护用于标准化的术语数据库，地址如下：

——ISO 在线浏览平台：http://www.iso.org/obp；

——IEC 电子百科平台：http://www.electropedia.org。

### 3.1　信息安全风险相关术语

3.1.1

**外部环境　external context**

组织寻求其目标实现所处的外部状况。

注：外部环境包括以下内容：

——国际、国内、区域或地方的社会、文化、政治、法律、监管、金融、技术、经济、地质环境；

——对组织目标有影响的关键驱动因素和趋势；

——与外部相关方的关系、看法、价值观、需求和期望；

——合同关系和承诺；

——网络的复杂性和依赖性。

［来源：GB/T 23694—2024，3.3.4，有修改］

3.1.2

**内部环境　internal context**

组织寻求其目标实现所处的内部状况。

注：内部环境包括以下内容：

——愿景、使命和价值观；