ICS 03.060
CCS A 11

中华人民共和国国家标准

GB/T 42926—2023

金融信息系统网络安全风险评估规范

Specification of financial information system cybersecurity risk assessment

2023-08-06 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。

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。

本文件由全国金融标准化技术委员会(SAC/TC 180)归口。

本文件起草单位：中国金融电子化集团有限公司、北京国家金融科技认证中心有限公司、北京天融信网络安全技术有限公司、中国工商银行股份有限公司、亚信科技(成都)有限公司。

本文件主要起草人：张海燕、唐辉、高强裔、潘丽扬、张璐、张澍、杨剑、孟宪哲、李吉、金红月、李者龙。

引　言

随着金融与科技融合成为新趋势，云计算、大数据、物联网、移动互联、人工智能等新型金融科技应用场景呈爆发式增长，金融信息系统面临复杂多变的网络安全威胁和日趋严峻的网络安全形势，开展金融信息系统网络安全风险评估有助于全面分析金融信息系统面临的威胁、存在的脆弱性以及风险等级，并基于风险评估结果开展风险处理工作。为了更好地适应金融科技变革，金融信息系统网络安全风险评估体系也需进一步完善。

本文件在成熟的风险评估方法论基础上，结合金融信息系统特点以及信息系统安全建设需求，提出面向金融业务和金融信息系统共性的网络安全风险评估模型、流程和风险分析方法，为金融信息系统网络安全风险评估提供指导。

金融信息系统网络安全风险评估规范

1 范围

本文件确立了风险评估工作的要点、原则、要素和原理，规定了风险评估准备阶段、识别阶段、风险计算及处理阶段工作的要求。

本文件适用于金融管理部门、金融业机构和网络安全风险评估服务机构开展金融信息系统网络安全风险评估工作。

注：本文件条款中的“风险评估”均指“金融信息系统网络安全风险评估”。

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 20269—2006 信息安全技术 信息系统安全管理要求

GB/T 20984—2022 信息安全技术 信息安全风险评估方法

GB/T 22240—2020 信息安全技术 网络安全等级保护定级指南

GB/T 25069—2022 信息安全技术 术语

GB/T 31509—2015 信息安全技术 信息安全风险评估实施指南

3 术语和定义

GB/T 20269—2006、GB/T 25069—2022 和 GB/T 20984—2022 界定的以及下列术语和定义适用于本文件。

3.1

资产价值 asset value

资产的重要程度或敏感程度的表征。

注：资产价值是资产的属性，也是进行资产识别的主要内容。

4 缩略语

下列缩略语适用于本文件。

CNNVD：中国国家信息安全漏洞库（China National Vulnerability Database of Information Security）

CNVD：国家信息安全漏洞共享平台（China National Vulnerability Database）

CPU：中央处理器（Central Processing Unit）

CVE：通用漏洞披露（Common Vulnerabilities and Exposures）