ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 28450—2026/ISO/IEC 27007:2020
代替 GB/T 28450—2020

网络安全技术
信息安全管理体系审核指南

Cybersecurity technology—Guidelines for information security management systems auditing

（ISO/IEC 27007:2020，Information security，cybersecurity and privacy protection—Guidelines for information security management systems auditing，IDT）

2026-05-25 发布　　2026-12-01 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/T 28450—2020《信息技术　安全技术　信息安全管理体系审核指南》,与GB/T 28450—2020相比,除结构调整和编辑性改动外,主要技术变化如下:

——删除了“审核方案的管理”一章中“总则”“建立审核方案”及“识别和评估审核方案风险”的所有内容(见2020年版的5.1、5.3.4);

——删除了“审核方案的管理”一章中“规划ISMS时所确定的风险和机会”[见2020年版的5.2.1d)];

——删除了“审核方案的管理”一章中“实施审核方案”中的“IS 5.4.2规定每次审核的目标、范围和准则”的“评价维护和有效改进ISMS的过程”[见2020年版的5.4、5.4.2.1b)];

——删除了“实施审核”一章中“审核报告的分发”中“在分发审核报告时,宜采取适当措施确保报告的保密性”(见2020年版的6.5、6.5.2.1)。

本文件等同采用ISO/IEC 27007:2020《信息安全　网络安全和隐私保护　信息安全管理体系审核指南》。

本文件做了下列最小限度的编辑性改动:

——将标准名称改为《网络安全技术　信息安全管理体系审核指南》;

——增加了附录A中针对变更的规划(见A.3.3);

——更改了附录A持续改进和不符合纠正措施顺序。

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:北京时代新威信息技术有限公司、中国网络安全审查认证和市场监管大数据中心、中国电子技术标准化研究院、中国合格评定国家认可中心、全国组织机构统一社会信用代码数据服务中心、广州赛宝认证中心服务有限公司、国家计算机网络应急技术处理协调中心、中国网络空间研究院、国家计算机病毒应急处理中心、北京赛西认证有限责任公司、北京神州绿盟科技有限公司、启明星辰信息技术集团股份有限公司、三六零数字安全科技集团有限公司、瀚高基础软件股份有限公司、长扬科技(北京)股份有限公司、岚图汽车科技股份有限公司、天翼安全科技有限公司、北京源堡科技有限公司、罗克佳华科技集团股份有限公司、中标华信(北京)认证中心有限公司、浪潮软件集团有限公司、中国民航信息网络股份有限公司、陕西省网络与信息安全测评中心、浙江省发展信息安全测评技术有限公司、杭州高新区(滨江)区块链与数据安全研究院、中移动信息技术有限公司、中检集团天帷网络安全技术(合肥)有限公司。

本文件主要起草人:王新杰、王连强、杨玉忠、付志高、程瑜琦、王姣、王寒生、翟亚红、魏立茹、孙镇、赵捷、陈艳、鲁立、潘文博、崔牧凡、宋首友、刘盈颖、赵丽华、叶晓虎、张睿、杨天识、张靖琦、冯明冉、张亚京、徐晓琳、方宇、梁露露、李玮、薛学琴、刘伯钊、孟建、李恩哲、马卓元、陈恩惠、魏遵博、高运霞、胡兴元、孙苏炜、陈明辉、毕建发、张巍巍、石巍。

本文件及其所代替文件的历次版本发布情况为:

——2012年首次发布为GB/T 28450—2012,2020年第一次修订;

——本次为第二次修订。

网络安全技术
信息安全管理体系审核指南

1 范围

本文件在GB/T 19011—2021的基础上,提供了对信息安全管理体系(ISMS)审核方案管理、审核实施,以及ISMS审核员能力等方面的指南。

本文件适用于需要理解或实施ISMS的内部或外部审核,或需要管理ISMS审核方案的所有组织。

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 19011—2021 管理体系审核指南(ISO 19011:2018,IDT)

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

GB/T 19011—2021和GB/T 29246—2023界定的术语和定义适用于本文件。

4 审核原则

GB/T 19011—2021中第4章的原则适用。

5 审核方案的管理

5.1 总则

GB/T 19011—2021中5.1的指南适用。

5.2 确立审核方案的目标

5.2.1 GB/T 19011—2021中5.2的指南适用。增加了5.2.2的内容。

5.2.2 确立ISMS审核方案目标时,可能包括以下内容:

a) 识别的信息安全要求;

b) GB/T 22080—2025的要求;

c) 发生信息安全事态和事件时所反映出的受审核方的绩效水平,以及ISMS的有效性;

注:关于绩效监视、测量、分析和评价的更多信息,见ISO/IEC 27004。

d) 相关方的信息安全风险,即受审核方和审核委托方。