CNAS-CC170:202X《信息安全管理体系认证机构要求》

等认可规范文件修订说明

一、 任务来源和背景

国际标准化组织（ISO）于2024年3月发布了ISO/IEC 27006-1:2024《信息安全、网络安全和隐私保护 信息安全管理体系审核和认证机构要求 第1部分：通用》，该标准代替了ISO/IEC 27006:2015及其相应的修改单。

国际认可论坛（IAF）在2024年5月发布了IAF MD29:2024《ISO/IEC 27006-1:2024转换要求》（第1版）。该文件识别了ISO/IEC 27006-1:2024的主要变化及影响，提出了本次转换周期，并规定了认可机构和认证机构实施转换过程的具体要求。该标准过渡期为2年，即自2024年即3月31日起至2026年3月31日止。

为落实IAF-MD29的相关要求，CNAS按照等同采用ISO/IEC 27006-1:2024的原则，修订了CNAS-CC170:202X《信息安全管理体系认证机构要求》，以取代现行的CNAS-CC170:2015。此外，CNAS根据CNAS-CC170:202X相关要求以及ISMS认可经验总结，将发布CNAS-SC170:202X《信息安全管理体系认证机构认可方案》，以取代CNAS-SC170:2017。考虑信息技术服务管理体系与信息安全管理体系两个认可制度的关联性，本次协调修改了CNAS-SC175:202X《基于ISO-IEC 2000-1的服务管理体系认证机构认可方案》，以取代CNAS-SC175:2017

二、 文件修订的主要内容

1、 CNAS-CC170:202X《信息安全管理体系认证机构要求》

——在规范性引用文件中删除 ISO/IEC 27000；

——增加“控制”、“外部环境”、“信息安全”等术语；

——调整审核员工作经历、培训经历和审核经历要求；

——修改远程审核的相关要求；

——新增认证文件中引用其他标准的要求；

——修改审核时间计算的相关要求；

——依据 CNAS-CC170:2024 附录 A 中的信息安全控制，更新附录 E；

2、 CNAS-SC170:202X《信息安全管理体系认证机构认可方案》

——对认证业务范围的认可描述进行调整；

——明确见证评审要求；

——对于现有认可规范文件中已进行明确规定的内容予以删除，保持相关文件的协调统一，如认可申请、预访问、风险评估和责任安排的内容、ISMS 认证证书等内容；

——基于认证业务的发展，删除 ISMS 认证机构能力分析和评价系统指南；删除资料性附录 通用信息安全技术领域和通用信息技术领域参考分类、知识点及应用；

——调整部分业务范围的等级，调整 02.05 为一级、02.07 为二级、03.05 为二级；

3、 CNAS-SC175:202X《基于 ISO-IEC 2000-1 的服务管理体系认证机构认可方案》

——对认证业务范围的认可描述进行调整；

——明确见证评审要求；

——对于现有认可规范文件中已进行明确规定的内容予以删除，保持相关文件的协调统一，如预访问、信息通报等内容；

——调整部分表述，保持与 CNAS-SC170 协调统一。

三、文件实施建议

本次修订为文件换版修订，三个认可规范文件均拟于 2024 年 9 月 30 日发布，2025 年 9 月 30 日实施。

其中 CNAS-CC170 过渡期为 2024 年即 9 月 30 日起至 2026 年 3 月 31 日止，旧版文件于 2026 年 3 月 31 日失效。

CNAS-SC170、CNAS-SC175 不设置过渡期，自文件发布之日，旧版文件失效。