关于信息安全管理体系认证依据变更的通知

国际标准化组织（ISO）于 2022 年 10 月发布 ISO/IEC 27001:2022《信息安全、网络安全和隐私保护 信息安全管理体系 要求》（以下简称新版标准），代替了 ISO/IEC 27001:2013（以下简称旧版标准）。针对新版标准换版，国际认可论坛（IAF）于 2022 年 8 月发布 IAF MD26:2022《ISO/IEC 27001:2022 转换要求》（第 1 版），中国合格评定国家认可委员会（CNAS）于 2022 年 11 月 15 日发布并实施认可转换说明文件 CNAS-EC-066:2022《关于 ISO/IEC 27001:2022 认证标准换版的认可转换说明》。2023 年 2 月 15 日，IAF 根据新版标准的发布稿修订了 IAF MD26:2023（第 2 版）；2023 年 2 月 24 日，CNAS 根据 IAF MD26:2023（第 2 版）修订了 CNAS-EC-066:2022。为确保获证组织顺利完成信息安全管理体系认证证书的转换工作，本中心对转换工作做出如下安排：

一、认证证书转换期限

2022年10月31日起至2025年10月31日为过渡期。本中心自2023年8月1日起，开始受理依据新版标准的初次认证和再认证申请，同时停止旧版标准的初次认证和再认证申请受理；对按旧版标准认证的获证组织，本中心将结合最近一次审核活动（包括监督审核、再认证、专项审核）进行认证证书转换工作。自2023年11月1日起，本中心将停止安排旧版标准的所有认证审核活动。为确保获证组织认证证书得到及时有效的转换，本中心鼓励获证组织尽早按照新版标准的要求启动转换工作。

二、实施新版标准认证的安排

1、自 2023 年 8 月 1 日起，本中心开始受理依据新版标准的认证（包括再认证）申请，并同时开始实施获证组织的认证证书新版标准转换工作，在完成所有认证程序后本中心将颁发或换发依据新版标准的认证证书。本中心将在 CNAS 认可范围内，颁发或换发带有 CNAS 认可标识的新版标准认证证书。

2、在新版国家标准发布前，本中心的新版标准认证证书的依据为 ISO/IEC 27001:2022。在新版国家标准发布后，本中心将负责安排对依据 ISO/IEC 27001:2022 标准的认证证书进行更换。

三、过渡期内新颁发旧版标准认证证书的安排

过渡期内新颁发旧版标准认证证书的获证组织，可自 2023 年 8 月 1 日起结合最近一

次审核活动（包括监督审核、再认证、专项审核）进行新版标准认证证书转换。自 2023 年 11 月 1 日起，本中心将停止安排旧版标准的所有认证审核活动，已获本中心颁发的旧版标准认证证书的获证组织应结合最近一次审核活动（包括监督审核、再认证、专项审核）进行认证证书转换工作。对于不能按期结合监督审核、再认证或专项审核进行认证证书转换的获证组织，本中心将按暂停或撤销处理。根据本中心《认证认可标识（牌）使用及认证证书管理规定》的要求，在接到暂停、撤销认证证书的通知后，获证组织应立即停止使用旧版标准相关认证资格（包括认证证书、标识、审核报告等）的声明、文件及广告。

四、已颁发旧版标准认证证书转换的安排

1、自 2023 年 8 月 1 日起，本中心对已颁发的旧版标准认证证书，将结合最近一次审核活动（包括监督审核、再认证、专项审核）完成获证组织的认证证书转换工作。

2、对于结合再认证审核转换的获证组织，经验证符合新版标准要求后重新颁发新版标准认证证书，证书有效期为颁证日期起三年。对于结合监督审核、专项审核进行认证转换的获证组织，经验证符合新版标准要求后换发新版标准认证证书，新版标准认证证书的有效期截止日期与原颁证日期所对应的三年周期的截止日期一致。

3、获证组织由于自身原因，不能结合监督审核、再认证进行认证证书转换时，可以申请专项审核进行认证证书转换。

4、对于不能按期结合监督审核、再认证或专项审核进行认证证书转换的获证组织，本中心将按暂停或撤销处理。根据本中心《认证认可标识（牌）使用及认证证书管理规定》的要求，在接到暂停、撤销认证证书的通知后，获证组织应立即停止涉及认证内容的广告及相关宣传活动。

五、认证证书转换的其他注意事项

1、对于结合监督审核进行认证证书转换的获证组织，本中心仍按原认证周期的监督审核时间进行，审核人日需在原监督审核人日的基础上增加 1.0 个人日（对于复杂程度高、规模大的获证组织，在此基础上可能适当增加人日）以覆盖新版标准的所有要求。结合监督审核转换时，本中心除收取正常监督审核费用外，不再收取额外的转换费用。

2、对于通过专项审核进行认证证书转换的获证组织，本中心将与获证组织签订专项审核协议，专项审核覆盖所有新版标准要求，审核人日按该获证组织的监督转换人日数进

行安排，并按照专项审核协议的约定收取费用。

3、对于结合再认证进行认证证书转换的获证组织，本中心将按照再认证程序与获证组织签订再认证合同，结合再认证实施转换时，审核人日需在原再认证审核人日的基础上增加 0.5 个人日（对于复杂程度高、规模大的获证组织，在此基础上可适当增加人日）。审核期间覆盖所有新版标准要求，并按照再认证合同的约定收取费用。

4、自 2023 年 8 月 1 日起，中心将通过现场审核的方式对获证组织实施转换审核。转换审核的内容应包括但不限于：ISO/IEC 27001:2022 的差距分析及获证组织 ISMS 的变更需求；符合性声明（SoA）的更新；适用时，风险处置计划的更新；获证组织所选的、新的或变化的信息安全控制的实施情况及其有效性。

5、实施新版标准转换的认证人员须经中心专业能力评定委员会确认，其中审核人员适用时应通过 CCAA 相应新版标准转换培训并考试合格。

6、获证组织和申请组织应遵守本中心《认证认可标识（牌）使用及认证证书管理规定》的要求，在获得新版标准认证证书前，不得声明组织的信息安全管理体系通过了新版标准认证，也不得以任何误导方式使用认证证书和标识，以暗示组织的信息安全管理体系通过了新版标准认证。

7、在新版标准认证证书转换过程中，获证组织应及时与本中心联系，尽早商定认证证书转换的各项工作安排，并进一步沟通新版标准转换的相关信息。