北京中建协认证中心有限公司
BEIJING ZHONG JIAN XIE CERTIFICATION CENTRE CO.,LTD.

认证规则编号	JCC-A05-001		
版本号	2025A		
认证规则名称	信息安全管理体系认证规则		
依据标准	ISO/IEC 27001 《信息安全、网络安全和隐私保护 信息安全管理体系 要求》		
认证标识			
	编写	任志赢	
	审核	郭喜宏	
	审批	郭喜宏	
发布日期	20250813	实施日期	20250813
声明	本认证规则正文、附录 A、附录 B 对外公开； 其余附录为内部文件，不公开。		

目录

1. 适用范围

本规则用于北京中建协认证中心有限公司依据 ISO/IEC 27001《信息安全、网络安全和隐私保护 信息安全管理体系 要求》标准在中国境内开展的信息安全管理体系认证活动。

本规则依据认证认可相关法律法规，结合相关技术标准，对信息安全管理体系（ISMS）认证实施过程作出具体规定。

安全管理体系（ISMS）认证归于分类“A05 信息安全管理体系认证”中。

本规则是北京中建协认证中心有限公司（下称中建协认证中心或 JCC）在信息安全管理体系认证活动中的基本要求，开展认证活动应当遵守本规则。

2. 认证依据

医疗器械质量管理体系应符合 ISO/IEC 27001《信息安全、网络安全和隐私保护 信息安全管理体系 要求》的要求。

3. 初次认证程序

3.1. 受理认证申请

3.1.1. 申请

3.1.1.1. 申请组织至少提交以下资料：

（1）法人资格证明（营业执照、事业单位法人证书或社会团体法人登记证书）；

（2）取得相关法规规定的行政许可文件（适用时）。

（3）从事的业务活动符合中华人民共和国相关法律、法规、信息安全标准和有关规范的要求。

（4）已按认证依据和相关要求建立和实施了文件化的信息安全管理体系。

（5）体系有效运行 3 个月以上，并且已完成内部审核和管理评审。

（6）信息安全风险评估报告及风险处置计划；

（7）适用性声明（SoA）。

（8）保密和敏感信息资产和区域声明。

3.1.1.2. 为确保客户组织符合工信部联协[2010]394 号文《关于加强信息安全管理体系认证安全管理的通知》的要求以及有关主管部门/监管部门对信息安全管理体系认证的管理要求，JCC 采取如下措施：

（1）为确保国家秘密安全，不受理各级政府机关、政府信息系统运营单位、涉密信息系统建设使用单位实施 ISMS 认证。

注 1：政府信息系统运营单位，包括各政府部门、政府投资或控股的科研教育机构与事业单位、政府采购产品和服务的承包商、政府授权的其他社会机构等。

注 2：涉密信息系统建设使用单位，主要有军队和武警、情报与国安系统、核心技术研发机构、重要监管部门与其他关键基础设施等。

（2）为政府部门提供信息技术外包服务的机构申请 ISMS 认证时，若其认证范围涉及“政府信息”，需提供工业和信息化主管部门同意的批文。

（3）通信、金融、铁路、民航、电力等基础信息网络和重要信息系统运营单位申请 ISMS 认证时，需提供行业主管或监管部门同意的批文。

（4）涉及国计民生的国有企业申请 ISMS 认证时，需提供国有资产监管部门同意的批文，涉及国家秘密的还需提供保密行政管理部门同意的批文。

注：国计民生企业指的是与人民生活需求密切相关，为保障人民基本生活、提高人民生活质量和维护社会稳定发挥重要作用的行业，如交通运输、电力、通信、水利、教育、医疗、社会福利等行业。

3.1.2. 申请评审

中建协认证中心申请评审人员应对申请组织提交的申请资料进行评审，根据申请认证的活动范围及场所、员工人数、完成审核所需时间和其他影响认证活动的因素，综合确定是否有能力受理认证申请。

对被执法监管部门责令停业整顿或在全国企业信用信息公示系统中被列入“严重违法企业名单”的申请组织，中建协认证中心不受理其认证申请。

3.1.3. 受理

对符合 3.1.1、3.1.2 要求的，中建协认证中心可决定受理认证申请；对不符合上述要求的，中建协认证中心将通知申请组织补充和完善，或者不受理认证申请。

3.1.4. 签订认证合同

在实施认证审核前，中建协认证中心将与申请组织订立具有法律效力的书面认证合同，合同应至少包含以下内容：

（1）申请组织获得认证后持续有效运行管理体系的承诺。

（2）申请组织对遵守认证认可相关法律法规，协助认证监管部门的监督检查，对有关事项的询问和调查如实提供相关材料和信息的承诺。

（3）申请组织承诺获得认证后发生以下情况时，应及时向中建协认证中心通报：

①客户及相关方有重大投诉。

②产品或服务出现信息安全事故。

③相关情况发生变更，包括：法律地位、生产经营状况、组织状态或所有权变更；取得的行政许可资格、强制性认证或其他资质证书变更；法定代表人、最高管理者变更；生产经营或服务的工作场所变更；信息安全管理体系覆盖的活动范围变更；所确定的控制及其引起的适用性声明的重大变更等。

④出现影响管理体系运行的其他重要情况。

（4）申请组织承诺获得认证后正确使用认证证书、认证标志和有关信息，不利用管理体系认证证书和相关文字、符号误导公众认为其产品或服务通过认证。

（5）拟认证的管理体系覆盖的生产或服务的活动范围。

（6）在认证审核实施过程及认证证书有效期内，中建协认证中心和申请组织各自承担的责任、权利和义务。

（7）认证服务的费用、付费方式及违约条款。

3.2. 审核策划

3.2.1. 抽样原则

3.2.1.1. 认证抽样方法

每次抽取的场所数量，一般宜为场所数量的平方根与抽样系数的乘积，即：

$$y = (\sqrt{x})$$

3.2.1.2. 多场所样本量

在进行项目策划时发现有涉及下列因素的特殊情况时，JCC 将适当增加抽样的数量或频率：

（1）场所的规模和员工的数量；

（2）活动和管理体系的复杂程度和风险水平；

（3）工作方式的差异（例如进行倒班）；

（4）所从事活动的差异；

（5）投诉记录，以及纠正措施和预防措施的其他相关方面；

（6）与跨国经营有关的任何方面；

（7）内部审核和管理评审的结果；

（8）其他（对应认证规则内规定的其他情况）。

3.2.2. 审核时间

3.2.2.1. 中建协认证中心申请评审人员以附录 A 所规定的审核时间为基础，根据申请组织管理体系覆盖的业务范围、技术复杂程度、所应用的技术的水平和多样性、认证要求和体系覆盖范围内的有效人数等情况，核算并拟定完成审核工作需要的时间。

3.2.2.2. 在特殊情况下，适当减少审核时间，单独审核减少的时间不得超过附录 A 所规定的审核时间的 30%。

3.2.2.3. 整个审核时间中，现场审核时间不应少于总审核时间的 80%。

3.2.3. 审核组

3.2.3.1. 中建协认证中心根据管理体系覆盖的活动的专业技术领域选择具备相关能力确定审核员组成审核组，必要时可以选择技术专家参加审核组。审核组中的审核员承担审核任务和责任。

3.2.3.2. 技术专家主要负责提供认证审核的技术支持，不作为审核员实施审核，不计入审核时间，其在审核过程中的活动由审核组中的审核员承担责任。

3.2.3.3. 审核组可以有实习审核员，其要在审核员的指导下参与审核，不计入审核时间，不单独出具记录等审核文件，其在审核过程中的活动由审核组中的审核员承担责任。

3.2.4. 审核计划

3.2.4.1. 中建协认证中心方案策划岗向审核组发放审核任务书，负责实施的审核组组长制定书面的审核计划。审核计划至少包括以下内容：审核目的，审核准则，审核范围，现场审核的日期和场所，现场审核持续时间，审核组成员（其中：审核员应标明认证人员注册号;技术专家应标明专业代码、工作单位及专业技术职称）。

3.2.4.2. 对于多场所组织，审核组还应关注以下事项：

（1）只有对 ISMS 中每个重大风险的场所都进行了审核，方可授予认证；

（2）多场所抽样策划时，应确保在三年内覆盖 ISMS 认证范围内的代表性样本，同时考虑随机因素；

（3）客户为确保单一的 ISMS 适用于所有场所并在运行层面实施统一管理所进行的活动。

3.2.4.3. 现场审核安排在认证范围覆盖生产或服务活动正常运行时进行。

3.2.4.4. 在审核活动开始前，审核组应将审核计划交申请组织确认，遇特殊情况临时变更计划时，应及时将变更情况通知申请组织，并协商一致。

3.3. 实施审核

3.3.1. 一般要求

3.3.1.1. 审核组必须按照审核计划的安排完成审核工作。

3.3.1.2. 审核组必须会同申请组织按照程序顺序召开首、末次会议，申请组织的最高管理者及与质量管理体系相关的职能部门负责人员应参加会议。参会人员应签到，审核组必须保留首、末次会议签到表。申请组织要求时，审核组成员应向申请组织出示身份证明文件。

3.3.2. 审核过程及环节

3.3.2.1. 初次认证审核，分为第一、二阶段实施审核。

3.3.2.2. 第一阶段审核至少覆盖以下内容：

（1）结合现场情况，确认申请组织实际情况与管理体系成文信息描述的一致性，特别是体系成文信息中描述产品或服务、部门设置和职责与权限、服务过程等是否与申请组织的实际情况相一致。

（2）结合现场情况，审核申请组织理解和实施 ISO/IEC27001 标准要求的情况，评价管理体系运行过程中是否实施了内部审核与管理评审，确认管理体系是否已运行并且超过 3 个月。

（3）确认申请组织建立的管理体系覆盖的活动内容和范围、体系覆盖范围内有效人数、过程和场所，遵守适用的法律法规及强制性标准的情况。

（4）在组织设置、风险评估与风险处置（包括所确定的控制）、信息安全方针和信息安全目标的背景下充分了解 ISMS 设计；

（5）结合管理体系覆盖产品和服务的特点识别对目标的实现具有重要影响的关键点，并结合其他因素，科学确定重要审核点。

（6）与申请组织讨论确定第二阶段审核安排。对管理体系成文信息不符合现场实际、相关体系运行尚未超过 3 个月或者无法证明超过 3 个月的，以及其他不具备二阶段审核条件的，不应实施二阶段审核。

注：审核组应及时向方案策划人员反馈一阶段审核情况，由方案策划人员确认二阶段是否实施并发送二阶段任务书。

3.3.2.3. 审核组应将第一阶段审核情况形成书面文件告知申请组织。在决定进行第二阶段之前，JCC 将审查第一阶段的审核报告，以便为第二阶段选择具备所需能力的审核组成员。如果第一阶段的审核组长具备能力且适宜时，可由其来实施该审查。让客户知晓在第二阶段可以要求对其他类型的信息和记录进行详细检查。

3.3.2.4. 第二阶段审核应当在申请组织现场进行。审核重点包括：

（1）最高管理层对信息安全目标的领导和承诺；

（2）信息安全风险评估，包括确保在重复实施风险评估时能产生一致的、有效的和可比较的结果；

（3）根据信息安全风险评估和风险处置过程所确定的控制；

（4）信息安全绩效和 ISMS 有效性，包括根据信息安全目标对其实施评价；

（5）所确定的控制、适用性声明、信息安全风险评估结果、风险处置过程与信息安全方针和信息安全目标之间的对应关系；

（6）控制的实现。如了解外部环境、内部环境、相关风险以及组织对信息安全过程和控制的监视、测量与分析过程，并确定控制是否已经实施且在整体上有效的；

（7）方案、过程、规程、记录、内部审核和对 ISMS 有效性的评审，且这些都能追溯到最高管理层的决定、信息安全方针和信息安全目标。

3.3.3. 发生以下情况时，审核组应向中建协认证中心报告，经中建协认证中心技术委员会同意后终止审核。

（1）受审核方对审核活动不予配合，审核活动无法进行。

（2）受审核方实际情况与申请材料有重大不一致。

（3）其他导致审核程序无法完成的情况。

3.4. 审核报告

3.4.1. 审核组应对审核活动形成书面审核报告，由审核组组长签字。审核报告应准确、简明和清晰地描述审核活动的主要内容，至少包括以下内容：

（1）申请组织的名称和地址。

（2）申请组织活动范围和场所。

（3）审核的类型、准则和目的。

（4）审核组组长、审核组成员及其个人注册信息。

（5）审核活动的实施日期和地点，包括固定现场和临时现场；对偏离审核计划情况的说明，包括对审核风险及影响审核结论的不确定性的客观陈述。

（6）叙述从 3.3 条列明的程序及各项要求的审核工作情况，其中：对 3.3.2.4 条的各项审核要求应逐项描述或引用审核证据、审核发现和审核结论；对目标和过程及绩效实现情况进行评价。

（7）识别出的不符合项。

（8）审核组对是否通过认证的意见建议。

3.4.2. 中建协认证中心保留用于证实审核报告中相关信息的证据。

3.4.3. 中建协认证中心在作出认证决定后 30 个工作日内，由中建协认证中心对接客户的项目管理人员将审核报告提交申请组织，并保留签收或提交的证据。

3.4.4. 对终止审核的项目，审核组应将已开展的工作情况形成报告，中建协认证中心将此报告及终止审核的原因提交给申请组织，并保留签收或提交的证据。

3.5. 不符合项的纠正和纠正措施及其结果的验证

3.5.1. 对审核中发现的不符合项，要求申请组织分析原因，并提出纠正和纠正措施。对于严重不符合，要求申请组织在 6 个月期限内采取纠正和纠正措施。

3.5.2. 中建协认证中心对申请组织所采取的纠正和纠正措施及其结果的有效性进行验证。

3.5.3. 如果未能在第二阶段结束后 6 个月内验证对严重不符合实施的纠正和纠正措施，则应按 3.6.5 条处理，或者按照 3.3.2.4 条重新实施第二阶段审核。

3.6. 认证决定

3.6.1. 中建协认证中心认证评定人员在对审核报告、不符合项的纠正和纠正措施及其结果进行综合评价基础上，进行复核；技术委员会，作出认证决定；总经理，批准认证决定。

3.6.2. 认证决定人员为中建协认证中心管理控制下的人员，审核组成员不参与对审核项目的认证决定。

3.6.3. 在作出认证决定前应确认如下情形：

（1）审核报告符合本规则第 3.4 条要求，审核组提供的审核报告及其他信息能够满足作出认证决定所需要的信息。

（2）反映以下问题的不符合项，中建协认证中心已派遣审核员评审、接受并验证了纠正和纠正措施的有效性。

①在持续改进管理体系的有效性方面存在缺陷，实现质量目标有重大疑问。

②制定的目标不可测量、或测量方法不明确。

③对实现目标具有重要影响的关键点的监视和测量未有效运行，或者对这些关键点的报告或评审记录不完整或无效。

④其他严重不符合项。

（3）中建协认证中心对其他一般不符合项已派遣审核员评审，并接受了申请组织计划采取的纠正和纠正措施。

3.6.4. 在满足 3.6.3 条要求的基础上，当中建协认证中心有充分的客观证据证明申请组织满足下列要求的，将评定该申请组织符合认证要求，向其颁发认证证书。

（1）申请组织的管理体系符合标准要求且运行有效。

（2）认证范围覆盖产品和服务符合相关法律法规要求。

（3）申请组织按照认证合同规定履行了相关义务。

3.6.5. 申请组织不能满足上述要求或者存在以下情况的，评定该申请组织不符合认证要求，以书面形式告知申请组织并说明其未通过认证的原因。

（1）受审核方的管理体系有重大缺陷，不符合 ISO/IEC 27001 标准的要求。

（2）发现受审核方存在重大信息安全问题或有其他与产品或服务相关的信息安全严重违法违规行为。

3.6.6. 中建协认证中心在颁发认证证书后，中建协认证中心证书管理人员在 30 个工作日内按照规定的要求将认证结果相关信息报送国家认监委。

4. 监督审核程序

4.1. 一般规定

4.1.1. 中建协认证中心对持有其颁发的信息安全管理体系认证证书的组织（以下称获证组织）进行有效跟踪，监督获证组织持续运行管理体系并符合认证要求。

4.1.2. 为确保达到 4.1.1 条要求，中建协认证中心根据获证组织服务的质量风险程度或其他特性，确定对获证组织的监督审核的频次。初次认证后的第一次监督审核应在认证证书签发日起 12 个月内进行。此后，监督审核少每年进行一次，监督审核的最长时间间隔不超过 12 个月。

注：超过期限而未能实施监督审核的，按 6.1 或 6.2 条处理。

4.1.3. 监督审核的时间，不少于按 3.2.1 条计算审核时间人日数的 1/3。

4.1.4. 监督审核的审核组，符合 3.2.2 条和 3.3.1 条的要求。

4.1.5. 监督审核应在获证组织现场进行，且满足第 3.2.3.3 条确定的条件。由于市场、季节性等原因，

在每次监督审核时难以覆盖所有服务或过程的，在认证证书有效期内的监督审核需覆盖认证范围内的所有产品、服务或过程。

4.2. 审核规定

4.2.1. 监督审核时至少审核但不局限于以下内容：

（1） ISMS 维护要素，如信息安全风险评估与控制的维护、ISMS 内部审核、管理评审和纠正措施；

（2） ISO/IEC 27001 要求的与外部各方的沟通；

（3） ISMS 在实现客户信息安全方针的目标方面的有效性；

（4） 相关信息安全法律法规合规性的定期评价和审查规程的运行情况；

（5） 所确定的控制的变更，及其引起的适用性声明变更；

（6） 客户提供的申诉和投诉记录；

（7） 在发现任何不符合或不满足认证要求时，应检查客户是否对其自身的 ISMS 和规程进行了调查并采取了适当的纠正措施；

（8） 认证所需的其他文件。

4.2.2. 在监督审核中发现的不符合项，获证组织必须分析原因，在最多 6 个月内完成纠正和纠正措施并提供纠正和纠正措施有效性的证据。

4.2.3. 中建协认证中心采用适宜的方式及时验证获证组织对不符合项进行处置的效果。

4.2.4. 监督审核的审核报告，应按 4.2.1 条列明的审核要求逐项描述或引用审核证据、审核发现和审核结论。

4.2.5. 中建协认证中心认证评定人员和技术委员会根据监督审核报告及其他相关信息，作出继续保持或暂停、撤销认证证书的决定。

5. 再认证程序

5.1. 一般规定

5.1.1. 认证证书期满前，若获证组织申请继续持有认证证书，申请组织应在证书期满前 3 个月提出再认证申请，中建协认证中心依照程序进行申请评审，通过申请评审并完成再认证合同的签订后，安排实施再认证审核，并决定是否延续认证证书。

5.1.2. 北京中建协认证中心按本规则 3.2.2 条和 3.3.1 条要求组成审核组。按照 3.2.3 条要求并结合历次监督审核情况，制定再认证审核计划交审核组实施。

5.1.3. 在管理体系及获证组织的内部和外部环境无重大变更时，再认证审核可省略第一阶段的现场审核，且审核时间应不少于按 3.2.1 条计算人日数的 2/3，现场审核人日不少于总审核人日数的 80%。

5.2. 审核规定

针对不符合实施纠正措施的时限，应与不符合的严重程度和相关的信息安全风险相一致。

对再认证审核中发现的严重不符合项，获证组织必须实施纠正与纠正措施，中建协认证中心将在原认证证书到

期前完成对纠正与纠正措施的验证。

5.3. 其他规定

5.3.1. 中建协认证中心按照 3.6 条要求作出再认证决定。获证组织继续满足认证要求并履行认证合同义务的，向其换发认证证书。

5.3.2. 如果在当前认证证书的终止日期前完成了再认证活动并决定换发证证书，新认证证书的终止日期可以基于当前认证证书的终止日期。新认证证书上的颁证日期应不早于再认证决定日期。

5.3.3. 如果在当前认证证书终止日期前，JCC 未能完成再认证审核或对严重不符合项实施的纠正和纠正措施未能进行验证，则不应予以再认证，也不应延长原认证证书的有效期。

5.3.4. 在当前认证证书到期后，如果 JCC 能够在 6 个月内完成未尽的再认证活动，则可以恢复认证，否则应至少进行一次第二阶段审核才能恢复认证。认证证书的生效日期应不早于再认证决定日期，终止日期应基于上一个认证周期。。

6. 暂停或撤销认证证书

6.1. 暂停证书

6.1.1. 获证组织有以下情形之一的，中建协认证中心将在调查核实后的 5 个工作日内暂停其认证证书。

（1）信息安全管理体系持续或严重不满足认证要求，包括对信息安全管理体系运行有效性要求的。

（2）不承担、履行认证合同约定的责任和义务的。

（3）被有关执法监管部门责令停业整顿的。

（4）不接受或不配合认证认可监督管理部门的监督管理；

（5）主动请求暂停的。

（6）其他应当暂停认证证书的。

6.1.2. 认证证书暂停期不得超过 6 个月。

6.1.3. 中建协认证中心将在中建协认证中心官网公开暂停认证证书的信息，明确暂停的起始日期和暂停期限，并声明在暂停期间获证组织不得以任何方式使用认证证书、认证标识或引用认证信息。

6.1.4. 在暂停认证期间，获证组织的信息安全管理体系认证证书暂时无效。

6.1.5. 如果获证组织未能在认证机构规定的时限内解决造成暂停认证的问题，JCC 将撤消其信息安全服务管理体系认证证书或缩小其相应的认证范围。

6.2. 暂停恢复

如果在当前认证证书暂停终止日期前，获证组织消除了导致证书暂停的原因措施并完成了验证，则恢复证书有效。

6.3. 撤销证书

6.3.1. 获证组织有以下情形之一的，中建协认证中心将在获得相关信息并调查核实后 5 个工作日内撤

销其认证证书。

（1）被注销或撤销法律地位证明文件的。

（2）被国家市场监督管理总局列入信用严重失信企业名单。

（3）拒绝配合认证监管部门实施的监督检查，情节严重的，或者对有关事项的询问和调查提供了虚假材料或信息的。

（4）出现重大信息安全事故，经执法监管部门确认是获证组织违规造成的。

（5）有其他严重违反法律法规行为的。

（6）暂停认证证书的期限已满但导致暂停的问题未得到解决或纠正的。

（7）没有运行管理体系或者已不具备运行条件的。

（8）不按相关规定正确引用和宣传获得的认证信息，造成严重影响或后果，或者北京中建协认证中心已要求其纠正但超过 2 个月仍未纠正的。

（9）其他应当撤销认证证书的。

6.3.2. 撤销认证证书后，获证组织必须寄回撤销的认证证书。中建协认证中心也将在中建协认证中心官方网站上公布或声明撤销决定。

6.4. 其他规定

6.4.1. 暂停或撤销认证证书会在中建协认证中心官方网站上公布相关信息，同时报国家认监委。

7. 缩小、扩大或其他变更认证范围

7.1. 缩小认证范围

7.1.1. 申请单位提出缩小认证范围的申请提交给市场专员，市场专员将申请传递给技术委员会进行评定审批，评定通过后，市场专员向企业发送缩小认证范围的审批通过通知书和新证书。

7.1.2. 评定审批应在收到缩小认证范围申请后一周内完成，发送缩小认证范围审批通过通知书和新证书应在评定审批通过内一周完成。

7.2. 扩大或其他变更认证范围

7.2.1. 在认证证书有效期内，扩大或其他变更范围的程序：

（1）申请到合同签订（或补充协议）的过程按初认证处理；

（2）方案策划，应说明扩大或其他变更认证范围实施方案：

①扩大或其他变更审核；

②结合监督/再认证进行扩大或其他变更。

（3）应说明审核时间确认方法：

①扩大或其他变更审核，按监督审核时间确定；

②结合监督/再认证进行扩大或其他变更，依据不同认证产品，增加 1~3 人日。

7.2.2. 各实施阶段的时机和时限，同初认证。

8. 认证证书及认证标识

8.1. 认证证书

8.1.1. 证书内容

（1）获证组织名称、地址和统一社会信用代码（或组织机构代码）。该信息应与其法律地位证明文件的信息一致。

（2）管理体系覆盖的生产经营或服务的地址和业务范围。若认证的管理体系覆盖多场所，表述覆盖的相关场所的名称和地址信息。

（3）管理体系符合 GB/T 42061-2022/ISO 13485:2016 标准的表述。

（4）证书编号；

（5）认证机构名称及注册地址。（北京中建协认证中心有限公司；地址：北京市朝阳区南湖东园 122 号博泰国际大厦 A 座 20 层）

（6）有效期的起止年月日。

（7）“获证组织必须定期接受监督审核、经审核合格并且获得《监督审核保持认证注册资格通知书》后，此证书方继续有效”的提示信息。

（8）相关的认可标识及认可注册号（适用时）。

（9）证书查询方式。“本证书有效性信息可扫描下方二维码、登陆我公司网站 www.jccchina.org，或国家认证认可监督管理委员会网站 www.cnca.gov.cn 查询。”接受社会监督。

8.1.2. 有效期

初次认证证书有效期最长为 3 年。再认证的认证证书有效期不超过最近一次有效认证证书截止期再加 3 年。

8.1.3. 有效期

初次认证证书有效期最长为 3 年。再认证的认证证书有效期不超过最近一次有效认证证书截止期再加 3 年。

8.1.4. 认证标识认证证书的使用

8.1.4.1. 获证组织可在投标、宣传、广告和证实组织具有满足顾客和使用的法规要求能力的场合或其它场合使用认证证书。

8.1.4.2. 认证证书不允许使用在产品上，或其他会被理解为产品符合的情况。

8.1.4.3. 认证证书不允许使用在产品认证证书和管理体系认证证书使用场合。

8.1.4.4. 获证组织使用认证证书时，可以采用原证书的同一色调或其它单一色调的影印件。可按比例放大或缩小，确保字迹清晰，不得有任何涂改、增删。

8.1.4.5. 通过以下方式，使获证组织了解认证证书的正确使用：

8.1.4.6. （1）通过 JCC 的公开文件，明确使用要求。签订合同时，交给申请认证方。

8.1.4.7. （2）由审核组长在现场审核的末次会议上介绍使用要求。

8.1.4.8. 当 JCC 暂停、注销或撤销获证组织认证资格时，该获证组织应立即停止使用并向 JCC 交回认证证书。

8.1.4.9. 当认证范围扩大/缩小时，原获证组织应立即用原证书换领已扩大/缩小认证范围的认证证书。

8.1.4.10. 认证证书的监督管理

8.1.4.11.凡初次违反证书使用规定的提出警告，限期制定和实施纠正措施加以整改，要求立即终止不正确使用或误导使用认证证书的行为，并消除由此引起的影响。

8.1.4.12.如不能按期整改，或两次违反规定，将暂停获证方的认证资格。

8.1.4.13.情节严重者将撤销其认证资格，必要时可采取法律手段。

8.1.4.14.作废证书的处置

（1）超过有效期的认证证书为作废证书，不能继续使用，由使用组织自行销毁。

（2）因认证范围扩大/缩小而回收的原认证证书和因注销/撤销的而收回的认证证书，均由 JCC 负责销毁并做相应记录（如执行人、证明人、销毁时间）。

（3）证书副本的有关规定

证书副本一般根据企业需要制作。

因扩大/缩小审核范围而换发证书的有效期内应与原证书一致，注明换证日期。

8.2. 认证标识

8.2.1. 认证标识

8.2.2. 认证标志使用规定

8.2.2.1. “华表”标志仅可使用在与获证组织的认证有关的场合，且必须完整使用。

8.2.2.2. 获证组织可将标志使用在投标、有关文件、 出版物和所有宣传广告等证实组织具有满足顾客和使用的法规要求能力的场合或其它场合上。

8.2.2.3. 获得服务认证的组织应当在广告等有关宣传中正确使用管理体系认证标志，可以将管理体系认证标志悬挂在其宣传管理体系通过认证的场合，但不得利用管理体系认证标志误导公众认为其产品、服务通过认证。

8.2.3. 认证标志的复制方式

8.2.3.1. 需要时可采用单一色调图样复制。

8.2.3.2. 认证标志图样可按比例放大或缩小，但不得变形使用，图案和字迹必须清晰。

8.2.3.3. 认证标志的管理与监督

8.2.3.4. 获证组织需单独使用 JCC 认证标志时，应向 JCC 审核管理部提出书面申请，经 JCC 总经理批准后由综合管理部备案并通知申请方。

8.2.3.5. 通过以下方式，让获证组织了解认证标志的正确使用。

（1）通过 JCC 的公开文件，明确使用要求。

（2）由审核组长在现场审核的末次会议上介绍使用要求。

8.2.4. 认证标志的终止使用

8.2.4.1. 当 JCC 暂停或撤销获证组织全部或部分认证资格时， 原获证组织应立即停止使用和发放带有认证标志的所有证书、文件和宣传资料或上述有关部分。

9. 与其他管理体系的结合审核

与其他管理体系实施结合审核时，通用或共性要求应满足本规则要求，审核报告中应清晰地体现 3.4 条要求，并易于识别。

10. 受理转换认证证书

（1）JCC 履行社会责任，严禁以牟利为目的受理不符合 ISO/IEC 27001《信息安全、网络安全和隐私保护 信息安全管理体系 要求》标准、不能有效执行信息安全管理体系的组织申请认证证书的转换。

（2）JCC 受理组织申请转换为本机构的认证证书，详细了解申请转换的原因，必要时进行现场审核。

（3）转换仅限于现行有效认证证书。被暂停或正在接受暂停、撤销处理的认证证书以及已失效的认证证书，不得接受转换申请。

（4）被发证的认证机构撤销证书的，除非该组织进行彻底整改，导致暂停或撤销认证证书的情形已消除，否则不应受理其认证申请。

11. 受理组织的申诉和投诉

（1）申请组织或获证组织对认证决定有异议时，应按照北京中建协认证中心官网发布的申诉程序进行申诉，中建协认证中心接受申诉并且及时处理，并在 60 日内将处理结果形成书面通知送交申诉人。

（2）申请组织若认为中建协认证中心未遵守认证相关法律法规或本规则并导致自身合法权益受到严重侵害的，可以直接向所在地认证监管部门或国家认监委投诉，也可以向相关认可机构投诉。

12. 认证记录的管理

（1）中建协认证中心根据认证记录保持制度，记录认证活动全过程并妥善保存，此项工作由技术质量部档案管理人员完成。

（2）实体记录资料使用中文，保存时间 3 年。

（3）电子文档，保存时间 3 年。

13. 其他

（1）本规则内容提及 ISO/IEC 27001 标准时均指认证活动发生时该标准的有效版本。认证活动及认证证书中描述该标准号时，应采用当时有效版本的完整标准号。

（2）本规则所提及的各类证明文件的复印件应是在原件上复印的，并经审核员签字确认与原件一致。

（3）北京中建协认证中心开展 ISO/IEC 27001 标准及相关技术标准的宣贯培训，并保存培训及考核记录。

附录 A 认证审核时间要求

信息安全管理体系认证审核时间要求

有效人数	审核时间（天）		
	初审（第一阶段+第二阶段）	监督	再认证
1-10	5	1.5	3.5
11-15	6	2	4
16-25	7	2.5	4.5
26-45	8.5	3	5.5
46-65	10	3.5	6.5
66-85	11	3.5	7.5
86-125	12	4	8
126-175	13	4.5	8.5
176-275	14	4.5	9.5
276-425	15	5	10
426-625	16.5	5.5	11
626-875	17.5	6	11.5
876-1175	18.5	6	12.5
1176-1550	19.5	6.5	13
＞1550	遵守上述递进规律		

注：

1、确定有效人数：

在认证范围内的、处于组织控制下工作的、所有班次的人员的总数，是确定审核时间的起点。当人员中达到 50%从事某些相同的活动时，允许在计算审核时间前进行人员数量的折减。按照对实施每项相同活动的人数开平方根的方式，得到用于计算审核时间的有效人数。该数值是允许折减到的最小值。

从事某项被认定为重复活动/工作的示例包括：

1) 履行职责时对信息只有读取访问权限的人员；

2) 不能使用组织 ISMS 范围内的信息处理设施的人员；

3) 对组织 ISMS 范围内的信息处理设施具有明确且可证实的受限访问权限人员；

4) 在有严格限制以防信息泄露的场所工作的人员，例如采取措施禁止个人物品和设备进入工作区域。

2、组织正常工作期间（如轮班制组织）安排的审核时间可以计入有效的管理体系认证审核时间，但往返多审核场所之间所花费的时间不计入有效的管理体系认证审核时间。

附录 B 认证证书样式

北京中建协认证中心有限公司

信息安全管理体系认证证书

注册号：023**ISMS***

兹　证　明

*******有限公司

(统一社会信用代码：**********)

地址：**********8；

信息安全管理体系符合 ISO/IEC27001:2022 标准的要求

特发此证，并予注册。

本证书覆盖范围：**********

****

生效日期：****年**月**日

有 效 期：****年**月**日至****年**月**日

在适用的法律法规要求的行政许可证明、资质证书、强制性认证证书等有效期内，接受例行年度监督审核并持有《监督审核保持认证注册资格通知书》的情况下本证书方可保持有效。本证书有效性信息可扫描下方二维码、登陆我公司网站 www.jccchina.com，或国家认证认可监督管理委员会网站 www.cnca.gov.cn 查询。

北京中建协认证中心有限公司

(地址：北京市朝阳区南湖东园 122 号博泰国际大厦 A 座 20 层)

董事长