凯新认证（北京）有限公司

Kaixin Certification (Beijing) Co., Ltd.

信息安全管理体系认证实施规则

受控状态：受控

文件编号：**KCB-QPXX05**

发布日期：**2020-01-01**

实施日期：**2020-01-01**

修改日期：**2025-08-26**

版　　次：**G/9**

批准发布：胡娜娜

信息安全管理体系认证实施规则				
文件编号	发布日期	实施日期	修改日期	版　次
KCB-QPXX05	2020-01-01	2020-01-01	2025-08-26	G/9

1.　目的和适用范围

本程序规定了 KCB 对申请认证的组织进行信息安全（ISMS）管理体系审核的要求，确保符合 ISO/IEC17021:2015/CC01:2015《管理体系认证机构要求》和 CNAS 有关认可规范的规定，满足各 ISMS 认证审核的要求。

2. 认证依据及引用文件

认证依据：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》

引用文件：ISO/IEC17021:2015—CNAS-CC01:2015《管理体系认证机构要求》

GB/T19011《管理体系审核指南》

IAF MD1—CNAS-CC11《基于抽样的多场所认证》

IAF MD2—CNAS-CC12《已认可的管理体系认证的转换》

CNAS-CC170《信息安全管理体系认证机构要求》

CNAS-SC170 《信息安全管理体系认证机构认可方案》

3. 定义

采用 ISO 9000 和 CNAS-TRC-007 中的术语和定义。

3.1 “场所”：场所是指组织实施活动或提供服务的常设地点。除了有形场所（如工厂）外，“现场”还可以包括远程访问包含管理体系审核相关信息的电子化场所。

3.2 “临时场所”：临时场所是组织为在有限的时期内进行特定工作或服务而设立的，且不会成为常设场所的场所（例如施工现场）。

3.3 “多场所组织”：多场所组织是指组织有一个确定的中心职能机构（以下称作中心办公室，但不一定是组织的总部）来策划、控制或管理某些活动，并且有一个由地方办公室或分支（即场所）组成的网络来实施（或部分实施）这些活动；

3.4 “审核方案”： 针对特定时间段所策划，并具有特定目的的一组（一次或多次）审核。 就 ISMS 认证而言，审核方案即是在认证机构与认证客户之间、合同规定的时间周期内，为确定认证客户的管理体系满足所选定的管理体系标准而策划的一组(一次或多次)审核，包括为初次认证、监督和再认证活动所策划的一组审核。

4.　申请评审

4.1 申请方应具备的基本条件

1) 有明确的法律地位；

2) 遵守国家信息安全相关的法律、法规、标准及其他要求；

3) 按信息安全管理标准建立了文件化的管理体系，且运行不少于 3 个月。

4）申请方不属于工信部联协[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》、工信部 2011 年第 21 号《政府部门信息技术外包服务机构申请信息安全管理体系认证安全审查程序》要求中的组织，不涉及“国家秘密安全的涉密活动”的信息安全管理，不属于“政府部门信息技术外包服务机构”。

4.2 申请资料的提供：

申请“信息安全管理体系认证”的组织应提交以下基本申请资料：

1.申请方法律地位证明文件（如：有效期内的三证合一的营业执照）；

2.法律法规规定的有效期内的行政许可证明、资质证书、强制性认证证书等；

3.有效的管理体系文件，包括：

a. 管理体系方针、目标、范围、适用性声明，以及标准要求的相关管理体系文件化的信息；

b. SLA 数量；

c. 多场所层级关系说明；

d. 信息系统列表（支撑 IT 服务管理的信息系统）；

e. 适用时，申请方应指明其再申请认证的 SMS 范围内与其他方共同服务的情况。

4.产品/服务提供过程的工艺流程图；

5. 组织适用的与信息安全有关的标准/法律法规清单，与覆盖产品、活动有关的法律/法规/标准；

6.认证范围如涉及多场所（由总部和若干个分部组成的组织），应提供多场所清单；

7.认证范围如涉及临时场所（非固定场所），如：计算机系统集成、硬件维护等，应提供“临时场所清单”。

8. 应在申请书中填写接受与管理体系有关的咨询的情况。

9. 保密协议。

4.3 申请评审的流程内容及要求

4.3.1 确认申请方的基本信息：

1) 依据企业申请认证的领域，核对申请书填写的完整性，申请材料的齐全性；

2) 依据申请书及申请资料，核对客户信息的准确性，包括：企业名称、注册资本、机构代码证号、地址场所信息、法人代表、联系方式等全部内容。

4.3.2 确认 CCAA 相关法规的符合性及证书转换的要求：

4.3.2.1 受理信息安全管理体系认证，应在 CNCA/CNAS/CCAA 网站输入企业名称，核实申请组织是否获得过其他认证机构的体系认证。

4.3.2.2 根据 CCAA 发布的“认证机构公平竞争规范-与认证证书有关的有违公平竞争行为约束” “认证证书转换备案办法” 等相关文件识别是否能够受理，涉及需报 CCAA 备案的项目，需报 CCAA 备案通过后受理。

4.3.2.3 对已认可认证证书转换的项目，“信息安全管理体系”需报 CCAA 备案批准，如备案未得到批准，则不得受理改申请，对申请转换的客户做出不受理的答复。

4.3.2.4 查询“全国企业信用信息公示系统”：

1）被列入了“严重违法企业名单”的申请方，不应受理其认证申请。

2）被列入“经营异常名录信息” 的申请方，应在确认该信息已被移出后受理，确认的方法按照公示系统 “移出经营异常名录的原因”、“移出日期”、“作出决定机关”三项已作出结论为依据。

3）被列入“行政处罚信息”的申请方，应在确认该处罚已被有效处理及整改后方可受理，必要时可以由企业提供相关接受处罚及已实施整改的证据。

4.3.2.5 确认信息安全管理体系申请方是否属于涉及执行“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，是否涉及政府信息，如果涉及，需要到工信部备案；以及有关主管部门/监管部门对信息安全管理体系的管理要求，如工信部 2011 年第 21 号公告《工业和信息化部加强政府信息部门信息技术外包服务安全管理》等要求。

4.3.3 确认法律地位文件：

4.3.3.1 核对申请方是否具有合法的法人地位，营业执照需在有效期内；

4.3.3.2 营业执照即将过期的，要求提供原营业执照复印件和正在办理换证的有效证明或说明，在评审表的资料齐全性中予以记录，供审核部及技术部后续关注。

4.3.3.3 无法人地位的组织，应提供相关证明材料，如社会团体等级证书、非企业法人登记证书的复印件；

4.3.4 确认前置许可资质：

4.3.4.1 依据申请认证的范围，确认是否属于需要前置许可资质的范围，属于需提供前置许可资质的范围应提交相关资质，具体可参考评审部前置许可资质法律法规清单；

4.3.4.2 核对前置许可资质的有效期，资质的许可范围是否覆盖了申请认证的范围，资质的名称、地址信息与申请资料的一致性。

4.3.4.3 评审人员应识别申请方提交的“ISMS 保密协议“附表内容，应确定在缺少这些信息的情况下得到充分审核，如确认的结果是若不核查已识别的保密性或敏感性信息就不能对 ISMS 进行充分审核，应在评审阶段告知客户，并达成访问许可，否则不应受理客户申请。

4.3.4.4 评审人员应识别客户提交的申请书中对于认证机构是否有特殊资质、诚信守法记录或认证人员身份背景的要求等，以便判断公司是否具备对该客户实施认证活动的资格或条件。

4.3.5 确认管理体系文件化的信息

4.3.5.1 核对申请书企业填写的相关信息与申请方提交的文件化的资料中相关信息的一致性，对于不一致的情况，要予以核实。

4.3.5.2 依据申请书填写的体系运行时间以及相关管理体系文件化的信息，确认管理体系满足已运行三个月的要求，以保证实施现场审核时，企业体系已运行满三个月。

4.3.5.3 确认管理体系过程是否存在外包，以及特殊/关键过程、职能分配图等关键内容。

4.3.5.4 当组织申请多体系认证时，确认受审核方管理体系的整合程度；

4.3.5.5 确认在审核实施前策划实施了内审、管评；

4.3.5.6 确认信息安全管理体系的适用性声明的版本；

4.3.5.7“前置许可资质的批准范围”及“营业执照的经营范围”均应覆盖申请认证范围，如未覆盖或有遗漏项，需关注前置许可资质或营业执照是否发生变更，并收集最新有效的前置许可资质或营业执照；

4.3.6 对公正性的评审

4.3.6.1 申请组织是否已经获得 KCB 公正性声明的信息（公开文件）；

4.3.6.2 认证申请方是否对 KCB 的公正性构成威胁；

4.3.6.3 向认证申请方提供认证咨询的组织或个人是否对 KCB 的公正性构成威胁；

4.3.6.4 当确认认证的公正性受到威胁时，KCB 不受理该组织的认证申请，对申请的客户做出不受理的答复。

4.3.6.5 确认申请认证的项目在合同评审的专业技术支持、审核派组、认证决定人员有充足的人力资源，以保证在审核和作出认证决定环节能够相互分开，如相关技术领域的人员配备不能满足该条款要求，对申请的客户做出不受理的答复。

4.3.6.6 以下工作不构成公正性威胁，不会被视为是在做咨询或具有潜在的利益冲突

a） 安排培训课程并作为讲师参与讲授。如果这些课程涉及服务管理、相关的管理体系或审核，我机构向客户提供的培训内容，应仅限于提供可公开获取的通用信息和建议，例如：认证机构不应为某个公司提供专门的建议；

b） 根据请求，提供或发布认证机构对认证审核标准要求的解释性信息；

c） 仅以确定认证审核是否就绪为目的的审核前活动，但是这些活动不应导致提供违反本条款的建议和意见。认证机构应能够证实这些活动不违反本条款的要求，且没有把这些活动作为减少最终认证审核时间的理由；

d） 根据没有包含在认可范围内的标准或法规，实施第二方或第三方审核；

e） 在认证审核和监督访问过程中的增值活动，例如，在审核过程中，当改进机会明显时，识别改进机会但不推荐具体的解决方案。

4.3.6.7 不应为向 KCB 申请认证的客户提供服务管理的内部评审。认证机构应独立于提供 SMS 内部审核的机构（包括任何个人）。

4.3.7 对认证范围的评审

4.3.7.1 对组织申请的管理体系认证范围，应准确表述，应符合国家相关法律法规、行业和产品标准的要求，以降低认证的风险，不得超出营业执照的范围，涉及前置许可的情况，不得超出前置许可的范围；

4.3.7.2 根据组织申请的体系认证范围，通过对组织的产品/服务、过程、活动、地域、管理范围分析，同时考虑其营业执照和资质许可范围来确定受理范围；

4.3.8 审核人日的确定

4.3.8.1 管理体系审核时间（审核总人日数）=在组织控制下工作的人员对应的基准审核人日数 + 增减人日数

当客户由于信息安全的原因在申请评审阶段不能提供足够的信息时，应通过第一阶段审核在客户的现

场补充对上述信息的确认，并完成申请评审任务。这种情况下，应增加第一阶段现场审核时间。

4.3.8.2 确定相应管理体系所覆盖的认证范围内的在组织控制下工作的人员的数量。

4.3.8.3 根据确定的在组织控制下工作的人员数量、认证标准、风险分级在附录 A 人日数表中确定审核所需的基准审核人日数。

4.3.8.4 根据受审核方可能存在的增减人日数因素在基准人日数的基础上加以调整，增加的因素可和减少的因素相抵消。但对某个组织初审审核人日数总量的调整，减少量不能大于基准审核人日数的 30%

基于以下几个方面的因素考虑增减审核天数，几个方面的可能影响审核时间的因素为：

—与 ISMS 范围的规模有关因素（如信息系统数量，处理的信息量，用户数量，网络数量及其规模等）

—与 ISMS 的复杂程度有关因素（如开发项目的数量和规模，远程工作的范围，ISMS 的风险状况等）

—在 ISMS 范围内开展的业务类型

—在 ISMS 各部分所应用的技术的水平和多样性[例如，不同 IT 平台的数量、隔离网络的数量]；

—在 ISMS 范围内的场所的数量

—经证实的以往 ISMS 的绩效

—信息系统开发的程度；

—场所的数量和灾难恢复场所的数量；

—第一阶段之后，认证机构将考虑控制的数量和复杂性；

—在 ISMS 范围内所使用的外包和第三方安排的程度以及对这些服务的依赖程度；

—对于监督或再认证审核：符合 CNAS-CC01 8.5.3 条款的、与 ISMS 相关的变更的数量和程度。

—适用于认证的标准、法规以及任何可能适用的行业特定要求（如等级保护）

注：减少审核时间的因素对每个客户组织的每次计算仅可以使用一次。

4.3.8.5 管理体系认证审核时间安排：在审核方案策划时，依据评审阶段给出的管理体系审核时间（审核总人日数），策划现场审核时间安排。通常情况，管理体系现场审核时间≥管理体系审核时间（审核总人日数）*70%。

4.3.8.6 监督审核时间的确定

ISMS 年度监督审核时间应与初次认证审核（第 1 阶段+第 2 阶段）的时间成比例，约为初审时间的 1/3。在策划每次监督审核时，应获得与客户管理体系有关的更新信息。所策划的监督审核时间应考虑到客户的体系成熟度等变化情况，对策划的监督审核时间进行确认审查，审查的结果（包括对审核时间的调整）应在审核方案策划中予以记录。

4.3.8.7 再认证审核时间的确定

再认证审核时间的确定应考虑客户管理体系的变化和体系成熟度的变化情况和绩效评价结果等因素，而不是简单按初次认证审核时确定的结果计算，依据客户更新的信息（再认证申请及资料）确认组织实施初次认证审核（第 1 阶段+第 2 阶段）的审核时间。ISMS 年度再认证时间应与初次认证审核

（第 1 阶段+第 2 阶段）的时间成比例，再认证审核时间不低于初次审核时间的 2/3 。

4.3.8.8 多场所审核的人天数多场所的审核人日数应不低于相同类型单一场所的审核人日数，适用时，根据申请方多场所的具体情况，考虑增加人日。

4.3.9 认证合同的签订

4.3.9.1通过合同评审后，实施认证审核前，申请评审人员应与认证申请方签署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信息安全管理体系的承诺。

（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，应及时向认证机构通报：

①客户及相关方有重大投诉。

②生产、销售的产品或提供的服务被质量或市场监管部门认定不合格。

③发生产品和服务的质量或信息安全事故。

④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；信息安全管理体系和重要过程的重大变更等。

⑤出现影响信息安全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，不利用信息安全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）在认证审核实施过程及认证证书有效期内，认证机构和申请组织各自应当承担的责任、权利和义务。

（6）认证服务的费用、付费方式及违约条款。

4.3.9.2 认证合同应一式两份，公司和认证申请方各执一份。认证合同内容填写应完整、清晰、准确无误。

5. 审核程序

5.1 审核方案策划

5.1.1 评审部实施合同评审与客户签署认证合同后，由审核项目管理人员负责策划执行该认证审核项目。

5.1.2 审核项目管理人员根据评审部评的评审结果策划审核方案。

5.1.3 审核方案的策划应覆盖一个完整的认证周期，至少包括两个阶段的初次审核、第一年与第二年的监督审核和第三年在认证到期前进行的再认证审核。认证周期的审核方案应覆盖全部管理体系要求。依据认证客户的不同需求，可有特定审核方案，如扩大认证范围的审核方案。对审核方案的任何调

整，应保留合理性的记录。

5.1.4 ISMS认证的初次审核应分两个阶段实施。ISMS一阶段需实施现场审核。现场审核应安排在审核范围覆盖产品和服务的生产期，审核组应在现场观察该产品和服务的生产活动。必要时，为了解受审核方是否已具备实施认证审核的条件，可安排进行预访问。

5.1.5 审核方案的策划

5.1.5.1 应考虑受审核方的组织规模、管理体系的领域、审核的类型、产品及生产和服务过程/环境因素及环境影响/危险源及产品的安全风险程度等因素、组织多场所的情况（固定场所、临时场所等）、季节性生产、轮班情况、KCB 对组织了解的程度、受审核方体系运行的成熟程度及结合审核的方式、法律法规及其行业性的强制要求、以往的审核结论或以往的审核方案的评审结果、认证客户组织或其运作的重大变化、认证客户所处的地域、文化、语言等。

5.1.5.2 应考虑客户是否曾获得其他经认可的认证机构颁发相应管理体系的认证证书，并按照要求对审核方案做出合理的调整，并予以记录，应确保对每个管理体系的审核均符合规定的要求。

5.1.5.3 在确定审核范围和编制审核计划时可能也需要考虑这些事项：

a) 认证机构收到的对客户的投诉
b) 结合、一体化或联合审核；
c) 认证要求的变化；
d) 法律要求的变化；
e) 认可要求的变化；
f) 组织的绩效数据（例如缺陷水平、关键绩效指标（KPI）数据等）
g) 利益相关方的关注；
h) 轮班情况。

5.1.5.4 如果考虑客户已获的认证或由另一认证机构实施的审核，则应获取并保留充足的证据，例如报告和对不符合采取的纠正措施的文件。所获取的文件应为满足本文件要求提供支持。认证机构应根据获取的信息证明对审核方案的任何调整的合理性，并予以记录，并对以前不符合的纠正措施的实施进行跟踪。

5.1.5.5 如果申请信息中提示客户采用轮班作业，申请评审时需根据轮班情况计算客户有效人数，审核方案策划时需关注客户的倒班说明，考虑客户在轮班工作中发生的活动，并将以上信息记录在审核方案策划里，传递给审核组，要求审核组在编制审核计划时关注审核方案策划中企业是否有轮班作业，如有，审核需覆盖。

5.1.5.6 对多场所的项目进行审核方案策划时，需关注不同场所对应不同认证范围时，其对应的技术领域也不同，审核方案策划时需将不同场所对应的认证范围及技术领域分别明示出来，以指导审核组长在日程安排时关注委派专业审核员实施专业过程的审核。

5.1.5.7 如果组织外包其部分职能或过程，组织应提供如下证据：组织已经有效地确定了其采用的控制方式和控制范围，以确保外部提供的职能或过程不会对管理体系有效性（包括组织向其顾客稳定提供合格产品和服务的能力，并承诺满足法规要求方面）产生负面影响。

5.1.5.8 审核过程中审核组发现与审核策划和审核计划不一致的信息（如审核范围、审核地址、企业资质、专业类别、人数、外包情况、倒班等内容）时，审核组应及时将变更的信息填写信息沟通（变更）记录，反馈至评审部，由评审部实施变更评审，确认专业、人日等信息是否有变化，审核方案管理人员依据变更评审结果调整审核方案，并将调整的任何信息记录在审核方案策划表中。审核组根据审核部要求，确认是否继续实施审核，并获取相关审核要求。

认证决定过程中，技术部如有需有传递下次审核组关注的问题，需将传递给审核组的信息传递给审核方案管理人员，审核方案管理人员依据技术部的反馈信息调整审核方案，并将传递给审核组的信息记录在审核方案策划表(二）的审核关注点中。

5.1.5.9 信息安全的审核方案策划还应考虑所确定的信息安全控制。

5.1.6 审核方案策划的内容包括：确定审核类型、审核目的、审核频次、审核时机、审核范围、审核依据、审核时间（拟定时间）、人日数需求、选择审核组长、配置审核人员（必要时，配备技术专家）等。

在审核方案实施过程中应根据审核中收集的变更信息对方案进行必要的调整，并保留记录。

5.1.6.1 确定审核目的

1） 审核目的应由认证机构确定。审核范围和准则，包括任何更改，应由认证机构在与客户商讨后确定。

2） 审核目的应说明审核要完成什么，并应包括下列内容：

a）确定客户管理体系或其部分与审核准则的符合性；

b）确定管理体系确保客户组织满足适用的法律、法规及合同要求的能力；

c）确定管理体系在确保客户可以合理预期实现其规定目标方面的有效性；

d）适用时，识别管理体系的潜在改进区域。

e) 对于信息安全管理体系还应包括确定管理体系的有效性，以确保客户已根据风险评估实施了适用的控制并实现了所设立的信息安全目标。

5.1.6.2 审核范围的确定

审核范围应说明审核的内容和界限，通常，审核的范围应涵盖拟申请或已认证范围内的所有产品/服务、过程和活动、组织单元及其实际位置，以及组织权限所辖的区域等。审核范围不应超出认证客户的营业执照和涉及的法律法规所规定的范围。

5.1.6.3 审核准则应被用作确定符合性的依据，并应包括：

1）所确定的管理体系规范性文件的要求

2）所确定的由客户制定的管理体系的过程和文件

3）相关法律法规要求

5.1.6.4 审核频次

审核部应根据与每个认证客户签订的认证协议和/或认证客户变化的信息来确定并调整其审核频次。通常，一个认证周期的审核频次包括初次认证审核、两次监督审核和认证到期前的再认证审核。当认证客户与认证机构签订的认证协议规定一个认证周期为四次或以上审核频次时，可按照认证协议

的要求确定审核频次。当出现下列情况时，宜考虑调整相应的审核频次：

a）认证客户出现重大信息安全服务事故等；

b）认证客户发生影响认证基础的重大变更，如所有权、规模、产品/服务、人员、设备变化等；

c）国家行政主管部门的要求或抽查的结果。

调整后的审核方案可包括缩短审核周期、增加审核频次或是增加提前较短时间通知的审核。

5.1.6.5 审核时机

审核部宜针对认证客户生产/服务活动的连续性、季节性、周期性、阶段性等特点来选择审核时机。在确定审核时机时，宜尽可能考虑选择能够全面反映认证客户实际管理能力的关键时期，该关键时期宜考虑：

a）审核时认证客户具有正在实施生产/服务活动的场所；

b）生产/服务活动宜具有代表性；

认证机构在建立审核方案时宜基于上述因素的考虑，为每次审核确定适宜的审核时机。

5.1.6.6 选择和指派审核组

5.1.6.6.1 由审核方案管理人员负责选择和任命审核组（包括审核组长及必要的技术专家），审核组的每位审核员不必具有相同的能力，审核组应整体上具备评审部确定的审核能力，及实现审核目的所需的能力，且符合公司公正性要求。如果仅有一名审核员，该审核员即为审核组长，履行审核组长职责。审核方案管理人员在决定审核组的规模和组成时，应考虑以下因素：

a）审核目的、范围、准则和预计的审核时间；

b）是否是结合、联合或一体化审核；

c）实现审核目的所需的审核组整体能力；

d）认证要求（包括任何适用的法律、法规或合同要求）；

e）语言和文化。

5.1.6.6.2 审核组还应符合下列要求：

a）审核组长、审核员的条件和职责应满足 ISO19011 标准的要求，审核组长还应符合公司对审核组长资格的要求，当任命的组长为级别审核员时(见习组长)，组内必须配备一名符合组长条件的审核员，以指导见习组长的工作；

b) 审核组的专业能力应覆盖审核计划涉及的全部技术领域（至小类）；

c）审核组可由一名审核员组成，但必须承担审核组长全部适用的职责；

d）当实习审核员参与审核时，要指派一名审核员作为评价人员，评价人员应由能力接管实习审核员的任务，并对实习审核员的活动和审核发现最终负责。实习审核员人数不能超过组内注册审核员人数；实习审核员不单独出具记录等审核文件；

e） 现场应满足审核策划确定的人日数要求，实习审核员、技术专家和翻译人员不计算审核人日；

f） 当审核组中安排人员的初始见证、定期见证或专业见证时，需适当增加审核人日（一般情况下，宜增加 0.5 人日）；已保证见证人与被见证人有同时实施审核的时间；

g） 审核组成员应确保公正。在现场审核前，审核组成员应将自己或其所在的组织与拟受审核方现

在、过去或将来可能的联系，告知 KCB，以保证认证活动的公正性，同时在审核报告中签署公正性承诺；该认证项目的市场开发人不得参与该项目的审核活动。

h） 如受审核方建立了远程访问相关信息的电子站点时，还需考虑审核组成员中应具备计算机辅助审核技术的能力；

i）审核组长和审核员所需的知识和技能可以通过技术专家和翻译人员补充。技术专家和翻译人员应在审核员的指导下工作。使用翻译人员时，翻译人员的选择要考虑到他们与拟受审核方的利益关系，不能对审核产生不正当影响。技术专家的选择准则根据每次审核的审核组和审核范围的需要为基础确定。

j）结合审核或一体化审核的审核组长宜至少对一个标准有深入的知识，并了解该审核所使用的其他标准。

5.1.6.6.3 审核方案管理人员在配置审核组的专业能力时，应考虑以下因素：

a） 指派审核组时应安排专业审核人员的能力满足能力评价人员评定的结果；

b） 当审核现场较多时，应确保审核组的整体专业能力满足要求。保证每个现场均有专业审核员参加审核，或有技术专家提供专业支持；

c） 对两个以上管理体系的结合审核时，应特别关注审核组的整体审核能力满足对每一个管理体系实施完整审核的能力要求；

5.1.6.6.4 观察员

审核部与客户应在实施审核前就审核活动中观察员的到场及理由达成一致。审核组应确保观察员不影响或不干预审核过程或审核结果。观察员可以是客户组织的成员、咨询人员、实施见证的认可机构人员、监管人员或其他有合理理由的人员。

5.1.6.6.5 向导

每个审核员应由一名向导陪同，除非审核组长与客户另行达成一致。为审核组配备向导是为了方便审核。审核组应确保向导不影响或不干预审核过程或审核结果。向导的职责包括：

a) 为面谈建立联系或安排时间；

b) 安排对现场或组织的特定部分的访问；

c) 确保审核组成员知道并遵守关于现场安全和安保程序的规则；

d) 代表客户观察审核；

e) 应审核员请求提供澄清或信息。

5.1.6.6.6 技术专家

认证机构应在实施审核前与客户就技术专家在审核活动中的作用达成一致。技术专家不应担任审核组中的审核员。技术专家应由审核员陪同。

5.1.6.6.7多场所的抽样

5.1.6.6.7.1抽样的条件

当客户组织拥有满足以下条件的多个场所时，适用CNAS-CC11，基于抽样的方法进行多场所抽样审核，依据附录B要求并结合以下要求进行抽样：

（1） 所有的场所在同一ISMS 下运行，并接受统一的管理、内部审核和管理评审；

（2）　所有的场所都包含在客户组织的 ISMS 内部审核方案中；

（3）　所有的场所都包含在客户组织的 ISMS 管理评审方案中。

5.1.6.6.7.2抽样的考虑因素

（1）申请评审管理人员在使用基于抽样的方法时，应确保抽样审核的结果应可以满足证明其ISMS 的适宜性、充分性和有效性，如果抽样无法满足以下要求时应进行相应的调整；

（2）在初次的合同评审中，最大程度地识别场所之间的差异，以便确定适宜的抽样水平并结合以下因素抽取具有代表性的场所，以体现抽样样本的代表性和随机性：

a)　总部及其他场所的内部审核的结果；

b)　管理评审的结果；

c)　场所规模的差异；

d)　场所业务目的的差异；

e)　ISMS的复杂程度；

f)　不同场所的信息系统的复杂程度；

g)　工作实践的差异；

h)　所实施的活动的差异

i)　控制的设计与运行的差异；；

j)　与关键的信息系统或处理敏感信息的信息系统之间的潜在相互作用；

k)　任何不同的法律要求；

l)　地域和文化因素；

m)　场所的风险状况；

n)　发生在特定场所的信息安全事件；

（3）从客户组织的 ISMS范围内所有场所中选择具有代表性的样本，这种选择应基于一个可体现上述（2）中所列因素，同时也考虑随机因素；

（4）在授予认证前，KCB的审核组已审核了ISMS中每个具有重大风险的场所；

（5）根据上述要求，设计审核方案，并在三年的时间内覆盖 ISMS认证范围内的代表性样本；

（6）无论是在总部还是在单个场所发现不符合，纠正措施规程的实施适用于包括认证范围内的总部和所有场所。

5.1.6.7 审核计划

5.1.6.7.1 审核项目管理人员根据下列信息安排审核项目：

1）受审核组织认证范围所属的技术领域；

2）合同评审所确定的审核人日数；

3）受审核组织的认证领域和管理体系的类型（单一体系、多体系整合及整合的程度）；

4）受审核组织所提供的管理体系的相关信息（包括体系形成文件的信息等）；

5）计算机辅助审核技术应用的需求；

6）认证人员管理部对审核人员专业能力的评定结果；

7）其他来自外部的信息（如政府监管、顾客申投诉等）。

5.1.6.7.2 审核部应按照审核方案提前与受审核方沟通审核安排事宜，确定审核时间并告知拟定审核组。选择审核时间时，与拟审核的组织就选择一个能最有效地证实其全部范围的审核时间达成一致。适当时，可考虑季度、月份、日期和班次。如受审核方接受对以上安排，审核部将制定管理体系审核计划（通知）书，并于现场审核前将管理体系审核计划（通知）书发送至受审核方，经受审核方确认。如受审核方提出合理更换审核组的要求时，审核部需立即重组审核组，或调整审核时间，应保证受审核方有足够时间对审核组成员的任命表示同意。

5.1.6.7.3 审核部正式任命审核组长和选择审核组成员，向审核组下发管理体系审核计划（通知）书、审核作业指导书（必要时）。

5.1.6.7.4 管理体系审核计划（通知）书应体现以下内容：审核目的、审核准则、审核范围（包括识别拟审核的组织和职能单元或过程）、拟实施现场审核活动（适用时，包括对临时场所的访问和远程审核活动）的日期和场所、预计的现场审核活动持续时间、审核组成员（其中：审核员应标明注册证书号及专业代码；技术专家应标明专业代码、技术职称或职务，如果在职应注明其服务的单位）及与审核组同行的人员（例如观察员或翻译）的角色和职责。

5.1.6.7.5 编制审核计划

审核组长应按照审核方案和管理体系审核计划（通知）书的要求编制管理体系审核计划。在现场审核活动开始前，审核组应至少提前一天将书面审核计划交申请组织确认。如存在特殊情况下导致的计划临时变更，审核组应及时将变更情况书面通知受审核的申请组织，并协商一致。 ISMS 审核计划应考虑所确定的信息安全控制。如适宜，审核计划应识别审核中将使用的网络支持审核技术。

网络支持审核技术可包括：例如，电话会议、网络会议、基于网络的交互式通信和远程电子访问 ISMS 文件和（或）ISMS 过程。对这些技术的关注重点，宜是提高审核的有效性和效率，并支持审核过程的完整性。

对存在多场所的组织可按照 5.1.6.6.7 的要求进行抽样，应确保抽样的合理性。审核计划的编制应满足审核方案的所有要求，应与审核目的和范围相适应，确保其完整性。审核组长在与审核组商议后，应向每个审核组成员分配对特定过程、职能、场所、区域或活动实施审核的职责，应根据审核组成员的能力进行合理分工，有效利用审核资源，确保审核人日利用的充分性以及对审核过程专业能力管理的有效性。在审核进程中，为确保实现审核目的，可以改变工作分配。审核时间必须按照审核计划执行，不得通过增加每个工作日的工作小时数来减少审核人日数。审核计划编制完成后，由审核组长在审核活动开始前提交受审核方确认（如受审核方不是审核委托方，审核计划还应同时提交审核委托方）。审核计划遇特殊情况临时变更计划时，应及时将变更情况通知受审核企业，同时按规定方式向国家认监委报送相关信息。

5.1.6.8 审核方法

KCB 的程序不预先假定 ISMS 实施的特殊方式或文件和记录的特殊格式，将重点放在确定客户的 ISMS 满足 ISO/IEC 27001:2022 的要求和客户的策略与目标。

注：ISO/IEC 27007 给出了有关审核的进一步指南。

5.2 初次审核

5.2.1 总体要求

受审核方需要为审核组调阅内部审核报告和信息安全独立评审报告做出所有的必要安排。在认证审核的第一阶段，客户应至少提供以下信息：

a) ISMS 和其所覆盖活动的一般信息；

b) ISO/IEC 27001 要求的 ISMS 文件的副本，以及需要时，其他相关文件。

5.2.2 认证范围

审核组应根据所有适用的认证要求，对包含在确定范围内的客户 ISMS 进行审核。审核组应确认客户在其 ISMS 范围内满足了 ISO/IEC 27001:2022 中 4.3 的要求。

5.2.3 现场审核时审核组应确认：客户的信息安全风险评估和风险处置是否准确地体现了其活动，并延伸到认证范围内所界定的、其活动的边界。确认这在客户的 ISMS 范围和适用性声明中得到了体现。现场审核时应验证每个认证范围至少有一个适用性声明。

现场审核时确认：与不完全包含在 ISMS 范围内的服务或活动的接口，已在寻求认证的 ISMS 中得到说明，并已包括在客户的信息安全风险评估中。与其他机构共享设施（例如，IT 系统、数据库、通信系统或外包一项业务职能），是这类情形的一个示例。

5.2.4 文件审核

5.2.4.1 文件审核一般应由审核组长实施，或由审核组长指定的具备能力的审核员实施。当文审人员不具备专业能力时，由具备专业能力的人员（或专家）提供专业支持。应由审核组长做出文审的结论意见，并对文审负责。

5.2.4.2 文件审核一般审查申请方提供的形成文件的信息。

5.2.4.3 当申请方提交的形成文件的信息不符合管理体系标准的要求时，文审人员应做好记录，形成文审报告。由审核组长就发现的问题提出纠正的要求，通知申请方。文审发现的问题至少应在第二阶段现场审核前验证关闭。应保留验证关闭的证据。

5.2.4.4 特殊情况下，当文件审核工作不能由审核组长或本审核组成员实施时，审核部可安排其他具备能力的审核员实施，最终由审核组长复审确认。审核组长应对文审的结果负责。

5.2.5 第一阶段审核

第一阶段审核策划应确保第一阶段的目的能够实现，应告知第一阶段需实施的任何现场活动。

5.2.5.1 实施第一阶段审核条件

a）受审核方的管理体系已运行，且不少于 3 个月；

b）受审核方已向 KCB 提交了评审需要的形成文件的信息；

c) 受审核方已实施了内审和管理评审。

ISMS 初次认证审核的第一阶段审核应包括在客户现场实施的审核活动，ISMS 一阶段需实施现场审核。

当客户由于信息安全的原因在申请评审阶段不能提供足够的信息时，应通过第一阶段审核在客户

的现场补充对上述信息的确认，并完成申请评审任务。这种情况下，应增加第一阶段现场审核时间。

5.2.5.2 第一阶段审核的目的是收集相关信息，了解受审核方管理体系建立、运行的情况；确定组织的第二阶段审核准备情况及资源配置情况，识别第二阶段审核的关注点。

第一阶段的审核内容应覆盖的内容及审核关注的问题：

5.2.5.2.1 审核客户的文件化的管理体系信息

关注受审核方管理体系文件与认证准则标准的符合性，现场进一步了解受审核方组织机构、职能、产品/服务、活动和过程等方面的特点，特别是管理体系过程的总体策划和实施情况，确认其适宜性、充分性；需确定受审核方管理体系文件是否符合一体化管理体系要求。

5.2.5.2.2 评价客户的运作场所和现场的具体情况，并与客户的人员进行讨论，以确定第二阶段审核的准备情况；

5.2.5.2.3 审查客户理解和实施标准要求的情况，特别是对管理体系的关键绩效或重要的因素、过程、目标和运作的识别情况；

5.2.5.2.4 收集关于客户的管理体系范围的必要信息，包括客户的场所、使用的过程和设备、所建立的控制的水平（特别是客户为多场所时）、适用的法律法规要求；

（1）确认受审核方的管理体系范围、过程和场所的必要信息是否充分，确认受审核方成文信息描述的ISMS认证范围与现场运行的产品、服务和活动范围情况的一致性，对申请评审确定的认证范围予以确认。

（2）与相关法律法规有关的内容

a、相关的法律法规要求和企业的遵守情况，有无违法及投诉内容 ，企业相关法律许可文件的有效性（营业执照、组织机构代码证，当行业、法规有要求时应提供企业资质证书、生产许可证、安全生产许可证、3C 等专业认证证书；环评或安评等证据；）

b、受审核方对适用法律法规的识别及在管理体系中的运用情况，方针、目标、指标、管理方案与法律法规要求的一致性；

c、适用的生产标准的符合性（企标必须备案）；

5.2.5.2.5 审查第二阶段审核所需资源的配置情况，并与客户商定第二阶段审核的细节；

现场观察客户运作场所及现场的分布、距离及周边环境，了解生产/服务状况、流程、班次安排；确认第二阶段审核的时间、路线安排细节；

5.2.5.2.6 结合可能的重要因素充分了解客户的管理体系和现场运作，以便为策划第二阶段审核提供关注点；

5.2.5.2.7 评价客户是否策划和实施了内部审核与管理评审，以及管理体系的实施程度能否证明客户已为第二阶段审核做好准备。

a) 内审、管理评审是否覆盖了管理体系范围内的活动及管理体系标准的要求；

b) 内审、管理评审的可信度；

c) 内审的不符合项是否已经验证关闭。

在收集遵守法规的信息时，应对相关资质证明的有效性进行检查。

5.2.5.3 审核组长应将第一阶段目的是否达到及第二阶段是否准备就绪的书面结论告知客户，包括识别任何引起关注的、在第二阶段可能被判定为不符合的问题。审核组长根据第一阶段审核发现编制第一阶段审核报告和第一阶段审核问题清单，并告知受审核方第一阶段的结果可能导致推迟或取消第二阶段审核。对影响第二阶段审核的问题要求客户整改后方能进行第二阶段审核，对不影响进入第二阶段审核的一般问题可在第二阶段审核现场跟踪验证。一阶段审核结束后，审核组长将第一阶段审核报告、问题清单和整改跟踪报告提交至公司信息系统，由审核部进行审核确认符合后安排实施第二阶段审核，如果发生任何影响管理体系的重要变更（如文件、审核范围增加、地址变更等），应考虑重复整个或部分第一阶段。第一阶段审核和第二阶段审核应安排适宜的间隔时间，使申请组织有充分的时间解决第一阶段中发现的问题。信息安全服务管理体系初次认证第一阶段和第二阶段审核的间隔应不超过 6 个月。如果超过 6 个月，应重新实施第一阶段审核。

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，确认申请组织评价管理体系运行中是否实施内部审核与管理评审，确认管理体系是否已有效运行并且超过 3 个月。对管理体系形成文件的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，不应实施二阶段审核。

在该审核阶段，审核组应获取有关 ISMS 设计的文件，其中包括 ISO/IEC 27001 所要求的文件。审核组应充分了解在组织环境下所进行的 ISMS 设计、风险评估和处置（包括所确定的控制）、信息安全方针和目标，以及特别是客户的审核准备情况。审核组将上述信息填写至审核报告，并传递至该项目管理员。

审核组应让客户知晓第二阶段可能需要详细检查的、更多类型的信息和记录。

5.2.5.4 发生以下情况时，审核组应向认证机构报告，经认证机构同意后终止审核。

（1）申请组织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。

5.2.6 第二阶段审核

5.2.6.1 审核的目的：是对认证准则所有要求的完整审核，评价客户管理体系的实施情况及其有效性，确认客户遵守自身的方针、目标和规程情况，确定能否推荐认证注册。第二阶段审核必须在客户现场进行。

5.2.6.2 第二阶段审核关注的内容

a）对体系要求进行全面审核以获取与体系标准及规范性文件所有要求的符合性及证据；

b）依据关键绩效目标和指标（与适用的管理体系标准或其他规范性文件的期望一致），对绩效进行的监视、测量、报告和评审；

c）客户管理体系的能力以及在符合适用法律法规要求和合同要求方面的绩效；；

d）客户体系过程（含产品/服务实现过程）运作的符合性、有效性，及对过程控制的能力；

e）内审、管理评审、纠正/预防措施等自我完善机制的有效性；

f）针对客户方针管理职责的适宜性。方针、目标、指标制定的适宜性、可测量性及得到沟通、监视；

g）规范性要求、方针、绩效目标和指标（与适用的管理体系标准或其他规范性文件的期望一致）、适用的法律法规要求、职责、人员能力、运作、程序、绩效数据和内部审核发现及结论之间的关系；

h）申请组织实际工作记录是否真实，对于审核发现的真实性存疑的证据应予以记录并在做出审核结论及认证决定时予以考虑。

信息安全管理体系审核还应关注：

最高管理层对信息安全方针和信息安全目标的领导和承诺；

对与信息安全有关的风险的评估，以及在重复评估时可产生一致的、有效的和可比较的结果；

基于风险评估和风险处置过程所确定的控制目标和控制；

根据信息安全目标对其实施了评价的信息安全绩效和 ISMS 有效性；

a） 所确定的控制、适用性声明和风险评估与风险处置过程的结果，与信息安全方针和目标之间的一致性；

b） 控制的实现，考虑了外部环境、内部环境、相关的风险，以及组织为确定控制是否得以实现、有效且达到其所规定的信息安全目标而对信息安全过程和控制进行的监视、测量与分析；

c） 方案、过程、规程、记录、内部审核和对 ISMS 有效性的评审，以确保其可被追溯至管理决定、信息安全方针和信息安全目标。

5.2.7 初次认证的审核结论

5.2.7.1 审核组应对在第一阶段和第二阶段审核中收集的所有信息和证据进行分析，以评审审核发现并就审核结论达成一致。

5.2.7.2 为使认证机构做出认证决定，审核组至少应向认证机构提供以下信息：

a) 审核报告：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；

b) 对不符合的意见，适用时，还包括对客户采取的纠正和纠正措施的意见；

c) 对提供给认证机构用于申请评审的信息的确认；

d) 对是否授予认证的推荐性意见及附带的任何条件或评论。

5.3 实施审核

当审核的任何部分以电子手段实施时，或拟审核的场所为虚拟场所时，认证机构应确保由具备适宜能力的人员实施此类活动。在此类审核活动中获取的证据应足以让审核员对相关要求的符合性做出有根据的决定。

注：“现场”审核可以包括对包含管理体系审核相关信息的电子化场所的远程访问。也可以考虑使用电子手段实施审核。

审核组现场审核时应：

a) 要求客户证实对信息安全相关风险的评估与 ISMS 范围内的 ISMS 运行是相关的和充分的；确定客户识别、检查和评价信息安全相关风险的规程及其实施结果是否与客户的方针、目标和指标相一致。

b) 审核组还应确定客户用于风险评估的规程是否健全并得到正确实施。

5.3.1 审核组准备

5.3.1.1 审核组宜提前进驻受审核方，了解受审核方概况。审核组在现场如发现受审核方实际有效雇员数量与其申请的人数不符、实际认证范围与企业申请的认证范围不符、生产或服务过程覆盖的区域与其申请信息不一致时，应立即通知审核部，并将变更的信息传递至审核部。审核部将根据实际情况，调整审核方案。组长对审核计划进行必要的调整，并保留记录。

5.3.1.2 现场审核前，审核组长组织召开审核组预备会，明确审核组成员的分工和审核要求，与并由专业审核员或技术专家对非专业审核员进行专业培训，以保证审核组成员能有效识别和判断受审核方的产品和服务过程、管理业务和相关的规定要求。一般情况，审核组的任务分工与组长提前交至受审核方的审核计划一致，如需调整，应及时告知受审核方，也可在首次会议中对审核计划的调整情况进行沟通。

5.3.1.3 每一位审核组成员应按照审核组的分工及审核程序、认证标准要求、企业体系过程和活动的特点编制审核检查表及抽样计划。审核员要根据审核进展情况灵活地运用检查表，以达到审核目的的要求，并记录审核发现。

由审核组长主持召开首次会议，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该参加会议，会议目的是简要解释将如何进行审核活动，并应包括下列要素，首次会议的详略程度可与客户对审核过程的熟悉程度相一致：

a) 介绍参会人员，包括简要介绍其角色，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；

b) 确认认证范围；

c) 确认审核计划（包括审核的类型、范围、目的和准则）及其任何变化，以及与客户的其他相关安排，例如末次会议的日期和时间，审核期间审核组与客户管理层的会议的日期和时间；

d) 确认审核组与客户之间的正式沟通渠道；

e) 确认审核组可获得所需的资源和设施；

f) 确认与保密有关的事宜；

g) 确认适用于审核组的相关的工作安全、应急和安保程序；

h) 确认可得到向导和观察员及其角色和身份；

i) 报告的方法，包括审核发现的任何分级；

j) 说明可能提前终止审核的条件；

k) 确认审核组长和审核组代表认证机构对审核负责，并应控制审核计划（包括审核活动和审核路径）的执行；

l) 适用时，确认以往评审或审核的发现的状态；

m) 基于抽样实施审核的方法和程序；

n) 确认审核中使用的语言；

o) 确认在审核中将告知客户审核进程及任何关注点；

p) 让客户提问的机会。

5.3.2 获取和验证信息

审核员在审核中应通过适当的抽样来收集与审核目的、范围和准则相关的信息（包括与职能、活动和过程之间的接口有关的信息），并对这些信息进行验证，使之成为审核证据。审核员应保证审核抽样的合理、代表性。审核时的抽样应覆盖审核范围内的所有产品及服务过程，监督审核时如因市场原因不能全部覆盖范围，应传递下次审核，确保周期内监督审核全部覆盖。如审核时发现抽取的样本不能支持认证范围，应根据审核情况与企业沟通调整认证范围，并反馈审核部。

审核员可以通过面谈、审查文件和记录、对过程和活动进行观察等方法收集审核证据，并应保留审核记录。应保证收集的审核证据可追溯。

如果发现受审核组织不允许接触信息资产或无法满足受审核组织关于接触信息资产的相关要求时，KCB 对审核和认证所受到的影响进行评估并采取相应措施（例如终止审核、缩小审核和认证的范围等）；

如果受审核组织事先没有禁止 KCB 接触某一信息资产或未和告知 KCB 关于接触信息资产的相关要求，而 KCB 在认证过程中发现自己不具备接触该信息资产的资格和条件时，应立即向受审核组织提出。审核组成员不宜在审核过程中以任何方式记录客户的保密或敏感信息。审核组在离开客户前，宜请客户检查和确认审核组携带的文件、资料和设备中未夹带客户的任何保密或敏感信息。

5.3.3 审核发现及审核结论

a）审核发现应简述符合性，详细描述不符合以及为其提供支持的审核证据，并予以分级和报告，以便为认证决定或保持认证提供充分的信息。审核组应在末次会前的内部会议中评审审核发现及审核中收集的其他信息。

b）对不符合的审核发现应对照审核准则的具体要求记录支持的审核证据，包含对不符合的清晰陈述，并详细标识不符合所基于的客观证据。应与客户讨论不符合，以确保证据准确且不符合得到理解。但是，审核员应避免提示不符合的原因或解决方法。

c）审核组应确定不符合项的等级。不符合分为轻微不符合及严重不符合。影响管理体系实现预期结果的能力的不符合判定为严重不符合；其他不影响管理体系实现预期结果的能力的不符合，判定为轻微不符合。

d）审核组应在与受审核方领导层的交流会上沟通不符合，以确认审核证据的准确性，使受审核方理解不符合，解决对审核发现和（或）审核证据的意见分歧，如果有未解决的分歧点应予以记录，提交认证机构裁决。注：如发现不符合有关法规要求时，这类不符合应立即通知受审核方。

e）审核组就审核结论达成一致，由审核组长负责编写审核报告。

5.3.4 准备审核结论

在末次会议前，由审核组长负责，审核组应：

a) 对照审核目的和审核准则，审查审核发现和审核中收集的任何其他适用的信息，并对不符合分级；

b) 考虑审核过程中内在的不确定性，就审核结论达成一致；

c) 确定任何必要的跟踪活动；

d) 确认审核方案的适宜性，或识别任何为将来的审核所需要的修改（例如范围、审核时间或日

期、监督频次、审核组能力等）。

5.3.5 末次会议

末次会议由审核组长主持，出席人员同首次会议。

会议目的是报告审核情况，宣布审核发现和审核结论，包括关于认证的推荐性意见。并应包括下列要素，末次会议的详略程度可与客户对审核过程的熟悉程度相一致：

a）向客户说明所收集的审核证据基于对信息的抽样，因而会有一定的不确定性；

b）介绍 KCB 有关本阶段审核的相关规定（如审核发现和审核结论类型及判定的原则等）；

c）认证机构处理不符合（包括与客户认证状态有关的任何结果）的过程；

d）与受审核方确定审核中发现的任何不符合的纠正和纠正措施完成时间或完成计划；

e）认证机构在审核后的活动；

f）说明投诉处理过程和申诉过程，代表审核组重申保密承诺；

g）请受审核方提出需要澄清的问题；

受审核方应有机会提出问题。审核组与客户之间关于审核发现或结论的任何分歧意见应得到讨论并尽可能获得解决。任何未解决的分歧意见应予以记录并提交技术部。

5.3.6 审核报告

5.3.6.1 审核组长编制审核报告，审核报告应足够详细，以支持认证决定。审核报告应包含认证范围的界定，提及范围的任何变更，并描述所遵循的重要审核路线和所使用的审核方法。

报告应包括审核组对客户认证的推荐意见，以及证实该推荐意见的信息。这种证实应包括对与的实施和有效性相关的不符合和改进机会的总结。

其内容至少包括：

a）注明认证机构；

b）客户的名称和地址及客户的代表；

c）审核的类型（例如初次、监督、再认证或特殊审核）；

d）审核准则；

e）审核目的；

f）审核范围，特别是标识出所审核的组织或职能单元或过程，以及审核时间；

g）任何偏离审核计划的情况及其理由，包括对审核风险及影响审核结论的不确定性的客观陈述；

h）任何影响审核方案的重要事项；

i）注明审核组长、审核组成员及任何与审核组同行的人员；

j）审核活动（现场或非现场，永久或临时场所）的实施日期和地点；

k）与审核类型的要求一致的审核发现（见 9.4.5）、对审核证据的引用以及审核结论；

l）如有时，在上次审核后发生的影响客户管理体系的重要变更；

m）已识别出的任何未解决的问题；

n）适用时，是否为结合、联合或一体化审核；

o）说明审核基于对可获得信息的抽样过程的免责声明；

p）审核组的推荐意见；

q）适用时，接受审核的客户对认证文件和标志的使用进行着有效的控制；

r）适用时，对以前不符合采取的纠正措施有效性的验证情况。

信息安全管理体系审核报告应提供以下信息或对这些信息的引用：

a）对客户信息安全风险分析进行认证审核的说明；

b）客户在实施 ISO/IEC 27001:2022 6.1.3 c) 所要求的比较时，所使用的任何信息安全控制集。

c) 所采用的主要审核路线和所使用的审核方法

d）所引用的适用性声明的版本，以及适用时，与客户以往认证审核结果的任何有用的对照。

完成的问卷、检查清单、观察结果、日志或审核员笔记可以构成完整的审核报告的一部分。如果使用这些方法，这些文件应作为支持认证决定的证据提供给审议人员。

报告应考虑客户所采用的内部组织和规程的充分性，以便对其 ISMS 建立信心。

e）关于 ISMS 要求和信息安全控制的实现与有效性的、最重要的观察（正面的和负面的）的摘要；

f）审核组关于客户的 ISMS 是否获得认证的建议，以及支持该建议的信息。

g）如果使用了远程审核方法，报告应说明远程审核方法在审核中的使用程度及其实现审核目标的有效性。

h）当组织的活动不是在明确的物理位置实施的，而是其所有活动都是远程实施的时，审核报告应说明组织所有活动都是远程实施的。

5.3.6.2 审核综述及对体系的评价应包含的基本内容；

a）关于管理体系符合性与有效性的声明以及对下列方面相关证据的总结：

-- 管理体系满足适用要求和实现预期结果的能力；

-- 内部审核和管理评审的过程；

b）对认证范围适宜性的结论；

c）确认是否达到审核目的。

5.3.7 组长在末次会议上口头宣布审核结论，审核组可以识别改进机会，但不应提出具体解决办法的建议。形成的书面报告即审核报告由审核组长组织编制，于审核结束后提交给受审核方，并保留签收或提交的证据。KCB 享有对审核报告的所有权。

5.3.8 纠正和纠正措施验证

5.3.8.1 审核组长负责对受审核方的不符合所采取的纠正和纠正措施实施情况进行验证。验证时要求：

a）分析不符合产生的原因；

b）举一反三对产生的不符合进行纠正；

c）针对原因，制定防止不符合再发生的纠正措施或预防措施。

5.3.8.2 受审核方应在规定的期限内对不符合采取纠正和纠正措施，对不符合的原因分析，纠正及纠正措施的实施证据均应予以记录，并将纠正措施验证报告及必要的证明文件提交审核组长，由审核组长

或具备能力的组员验证所采取的纠正和纠正措施的有效性。对不符合的验证关闭的证据审核组长或具备能力的组员应予以记录，并将审查和验证的结果告知客户。

对于严重不符合，应要求申请组织在最多不超过 6 个月期限内采取纠正和纠正措施。审核组应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。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 5.3.8.3 条处理，或按照 5.2.3.2 条重新实施第二阶段审核。

如果为了验证纠正和纠正措施的有效性，将需要补充一次全面的或有限的审核，或者需要文件化的证据（需要在未来的审核中确认），则应告知客户。 可以通过审查客户提供的文件化信息，或在必要时实施现场验证来验证纠正和纠正措施的有效性。验证活动通常由审核组成员完成。

5.3.8.3 受审核方如未能在规定期限内完成纠正措施，审核组将改变原审核结论，不予以推荐认证。

5.3.9 在审核结束后，审核组长将完整档案提交技术部，提交的信息足以确定认证要求的满足情况和认证范围。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，审核组长应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。技术部组织认证决定人员在评价审核发现和结论及任何其他相关信息（如公共信息、客户对审核报告的意见）的基础上提出认证决定的结论。

5.3.10 经公司总经理批准后，向认证申请方颁发认证证书。

5.4 监督审核

5.4.1 监督审核的策划

审核部负责针对每一个获证客户策划年度监督审核方案，以便定期对管理体系范围内有代表性的区域和职能进行监视，监督审核时间不宜少于1天。监督审核应至少每个日历年（应进行再认证的年份除外）进行一次。初次认证后的第一次监督审核应在认证决定日期起12个月内进行。对未能按照监督审核方案及时接受现场审核的客户，应提前告知未按期实施监督审核将导致的结果，并保留联系记录。在策划方案时并应考虑获证客户多场所或临时现场的审核、结合或联合审核以及认证合同签订的特殊要求（如证书转换等）的审核、以往的审核结果或以往的审核方案的评审结果及其管理体系的变更情况等。策划的结果通过月度计划告知审核组。监督活动应包括对获证客户管理体系满足认证标准规定要求的情况进行评价的现场审核，但不一定是对整个体系的审核，并应与其他监督活动一起策划，以使认证机构能对获证管理体系在认证周期内持续满足要求保持信任。季节性产品应在生产季节进行监督。每次跟踪监督审核应尽可能覆盖ISMS认证范围内的所有产品和服务。由于市场及产品的季节性原因，在每次跟踪监督审核时难以覆盖所有产品和服务的，在认证证书有效期内的跟踪监督审核必须覆盖ISMS认证范围内的所有产品和服务。

除定期监督审核外，当获证方质量体系出现下列情况时，应增加一次监督审核：

a) 获证方管理体系发生重大变化或其他影响认证基础的变更；

b) 获证方因不满足认证要求，导致认证资格被暂停（因欠费暂停除外）；

c) 获证方发生重大信息安全服务事故，严重影响管理体系的有效性；

d) 发生重大顾客申诉、投诉，或被媒体曝光；

e) 国家或上级有要求时；

f) 获证企业的产品在产品质量国家监督抽查中被查出不合格时，自国家质检总局发出通报起 30 日内，认证机构应对该企业实施监督审核。

5.4.2 监督审核准备

审核部提前两个月与应实施监督审核与企业确认监督审核事宜，同时向企业下发获证方情况调查表，以确认已获证组织与体系相关的信息有无变更。对获证方情况的调查结果如有变更需要提交评审部重新评审，审核部依据评审的结果及时调整审核方案。

5.4.2.1 审核部按照审核方案策划的能力要求任命监督审核组组长和审核员。

5.4.2.2 审核部应提前与获证方确认审核时间及审核组成员信息，应保证受审核方有足够时间对某一审核员或技术专家的任命表示反对，并在反对有效时能够重组审核组。审核部向受审核方及审核组长下达管理体系审核计划（通知）书、相关工作文件 及上一次审核的不符合报告等。如果获证方体系文件换版，审核部安排审核组长或具备能力的审核员进行文审。

5.4.2.3 审核组长按要求编制审核计划。对多场所可采用抽样审核，抽样结果填写在核信息传递及周期评价表相应栏目中。

5.4.2.4 审核组长编制审核计划，并与现场审核实施前提交至受审核方确认。

5.4.2.5 审核组应提前进驻审核现场。如发现受审核方实际员工数量、认证范围等与审核策划提供的信息不符时，审核组长应立即通知审核部，并填写“信息沟通（变更）记录”传递至审核部。审核部将根据实际情况，调整审核计划、更新系统记录。

5.4.2.6 审核组长召开审核前预备会，明确审核任务，编制检查清单，培训非专业审核员。

5.4.2.7 监督审核应考虑：

a） 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；

b） 根据 ISO/IEC 27001:2022 要求的与外部各方的沟通，以及认证所需的其他文件。

5.4.3 现场审核

监督审核主要审查受审核方的如下（但不限于以下）内容：

a）内部审核和管理评审；

b）以往审核的结果，特别是对上次审核中确定的不符合采取的措施；

c）对体系有影响的有关投诉的处理，并且在发现任何不符合或不满足认证要求时，还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；

d）管理体系在实现获证客户目标和管理体系的预期结果方面的有效性；

e）为持续改进而策划的活动的进展；

f）持续的运作控制；

g）客户及其管理体系的任何变化；

h）外部环境的变化（如法规的变化）

i）法律法规的遵守情况；

j）证书/标志的使用和（或）任何其他对认证资格的引用；

k）质量监督或行业主管部门抽查的结果；

l）ISMS在实现客户信息安全方针的目标方面的有效性；

m）对与相关信息安全法律法规的符合性进行定期评价与评审的规程的运行情况；

n）所确定的控制的变更，及其引起的适用性声明的变更；

o）控制的实现和有效性（根据审核方案来审查）。

p）有关消除以往出现的不符合、适用性声明的版本和从上次审核之后发生的重大变更的信息。

5.4.3.1 审核组长将现场抽样的结果（部门、过程、场所）填写在审核信息传递及周期评价表中并随审核资料一同交审核部，由审核部转交下次监督的组长做为监督审核策划的输入。

5.4.3.2 现场审核结束后，审核组召开内部会议，对受审核方的管理体系运行状况做出判断，得出审核结论，程序同初次认证审核程序。

5.4.3.3 审核组长在末次会议上宣布监督审核结论，审核结论有以下四种：

1) 推荐保持认证注册资格；

2) 在商定的时间内完成对不符合项的整改，并经审核组验证有效后，推荐保持认证注册；

3) 建议暂停/撤销认证注册资格；

4) 暂停证书的原因已经消除，推荐恢复认证注册。

注：现场审核时如发现客户的获证管理体系持续或严重地不满足认证要求，包括对管理体系有效性的要求，比如管理体系存在严重的系统性问题，不能满足相关管理体系标准要求，审核组长需提出暂停获证客户的认证资格的审核结论。

5.4.4 不符合关闭

5.4.4.1 在监督审核中发现的不符合项，审核组长应要求获证方分析原因，在规定时限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。审核组长应采用适宜的方式及时验证获证方对不符合项进行处置的效果。审核组长将不符合及纠正措施验证关闭后，应在规定期限内将审核资料报技术部。如果获证方未能在规定期限内提交纠正措施资料，并被有效验证关闭，将影响其认证资格的保持。

5.4.4.2 如因获证方超期未提交纠正措施导致被暂停，由审核组长负责提供书面说明后报审核部。审核部负责及时向技术部报送暂停的信息。审核组长继续负责跟踪获证方的后续情况，直至获证方纠正措施验证有效或未能满足要求导致撤销认证资格，审核组长整理齐全审核资料，移交技术部。

5.4.4.3 如果审核结论为暂停或撤销认证资格，则按照 KCB 有关暂停、撤销的控制程序执行。

5.5 再认证审核

5.5.1 再认证审核的策划

5.5.1.1 策划和实施再认证审核，以评价获证客户是否持续满足相关管理体系标准或其他规范性文件的所有要求。再认证审核的目的是确认管理体系作为一个整体的持续符合性与有效性，以及与认证范围的持续相关性和适宜性，以便决定是否更新认证，换发认证证书。

5.5.1.2 再认证活动应考虑管理体系在最近一个周期内的绩效，包括调阅以前的监督审核报告。

5.5.1.3 评审部于第二次监督审核认证决定日期后 10 个月或认证证书有效期满前三个月，收集每一获证组织的体系变更信息，对确认申请再认证的获证组织实施申请评审，并签订合同。由审核部策划和安排再认证审核。再认证审核应在认证证书到期前完成。

5.5.1.4 一般情况下，再认证审核不需第一个阶段审核。但当获证组织管理体系、组织或管理体系的运作环境发生重大变更时（如区域、法律法规等的变更、食品安全标准的变更、发生重大有效性问题等），合同评审人员应评审确认是否需安排第一阶段审核。

注：此类变更可能在认证周期中的任何时间发生，可能需要实施特殊审核（见 5.6），该特殊审核可能需要或不需要两阶段审核，审核部需重新策划审核方案。

5.5.1.5 审核部对再认证审核按照 5.1.5 条要求进行审核策划，对于多场所认证和多体系认证的组织，再认证审核策划要确保现场审核要有足够的覆盖范围。

5.5.2 再认证审核

5.5.2.1 审核部按照初审要求制定管理体系审核计划（通知）书，传达至受审核方、并任命审核组。审核组组成的要求同初次审核。再认证审核时间约为更新后初次认证审核时间的 2/3。审核部向审核组提供相关文件、记录表格，包括：上一周期历次的审核报告（初审、监督和特殊审核）和“不符合报告”。

5.5.2.2 审核组长应对实施再认证的进行文件审查，并提交文审报告，确认受审核方管理体系文件是否持续满足确定的管理体系标准的要求。

5.5.2.3 在现场审核前，审核组长应根据审核部提供历次的审核报告和不符合报告对受审核方管理体系在上一个认证周期的绩效进行评价，以识别再认证审核的关注重点，作为审核计划策划的输入。此后，按照 5.1.6.7.4 条要求并结合历次监督审核情况，制定再认证计划并于审核实施前提交申请方确认。

5.5.3 再认证审核的关注点

a) 管理体系的变更及有效性，认证范围的持续相关性和适宜性；

b) 过去的认证有效期内管理体系运行情况、组织自我完善机制，改进管理体系提高绩效承诺的实现情况。

c) 现行管理体系运行是否促进了组织方针及目标和管理体系预期结果的实现。

d) 认证证书及标志使用情况等。

5.5.4 再认证现场审核的实施与初次认证第二阶段审核的相关程序一致。

5.5.5 再认证审核中发现的严重不符合，纠正措施计划应在 15 天内提交，且这些措施应在认证到期前得到实施和验证。允许采取纠正措施的时间，应与不符合的严重程度和相关的信息安全风险相一致。

5.5.6 如果在认证终止日期前，未能完成再认证审核或不能验证对严重不符合实施的纠正和纠正措施，则不推荐再认证，也不延长认证的效力。告知客户并解释后果。

5.5.7 在认证到期后，若能够在 6 个月内完成未尽的再认证活动（如轻微不符合的验证、认证决定过程等）则可以恢复认证，否则应至少进行一次第二阶段才能恢复认证。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。

5.5.8 由技术部根据再认证审核的结果，以及认证周期内的体系评价结果和认证使用方的投诉等信息组织认证决定人员进行审议，做出是否更新认证的决定的结论，报总经理批准，更新认证证书。

5.6 特殊审核

5.6.1 特殊审核包括扩大认证范围的审核和提前较短时间通知或不通知的审核。特殊审核可以和监督审核一起策划和实施。

5.6.2 扩大认证范围

ISMS扩大范围审核应覆盖标准所有条款，并按照本文件申请评审相关要求提交申请文件，实施申请评审、审核策划。

5.6.3 提前较短时间通知或不通知的审核包括：

a）组织的管理体系出现严重影响其活动和运作的变更(如所有权、人员、设备变动)时；

b）出现对组织的重大投诉，并经 KCB 确认可能导致其管理体系不满足认证准则的要求时；

c）组织出现重大的质量/环境/职业健康安全事故或主管部门抽查发现其产品服务质量不合格或出现违规行为时；

d）认证要求发生变更时（如认证准则发生变更等）；

e）组织被暂停认证资格时对其体系持续符合性的跟踪；

f）KCB管委会或技术委员会提出要求时。

5.6.4 特殊审核由审核部根据收集的信息进行策划。策划时考虑到组织对审核组成员的任命缺乏表示反对的机会，应确保审核组成员的公正性地位满足规定的要求。

5.6.5 当结合监督审核实施特殊审核时，在审核策划和审核实施中应关注完整覆盖监督审核和特殊审核的所有要求。

5.6.6 当结合监督实施恢复认证资格的审核时，应首先通过现场审核确认暂停的原因是否已有效消除。在确定已满足恢复认证条件的前提下，审核组可继续按照监督方案实施监督审核。当确定不满足恢复认证条件时，现场审核将终止，审核组长反馈至策划人员。

5.7 不通知现场审核

如采用不通知现场审核的方式对获证组织实施跟踪调查， 可以在审核前 48 小时向获证组织提供审核计划，获证组织无正当理由不得拒绝审核。

第一次不接受审核将收到书面告诫，第二次不接受审核将导致证书的暂停。

5.7.3 不通知检查结果处理

当不通知检查结果表明获证组织已不再符合认证要求时，应收集详细的信息资料并说明原因，向技术部提出暂停或撤销其认证证书资格的申请。

5.8 审核资料收集及转挡

5.8.1 审核组长负责审核档案的完整性，至少包括（但不限于）：

1）管理体系审核通知（计划）书；

2）文审报告（必要时）；适用性声明文件（IS 适用）；

3）审核记录；

4）第一阶段问题清单、不符合报告及验证关闭的证实材料；

5）审核报告；

6）首、末次会议签到表；

7）不符合报告及纠正措施证据；

8）管理体系证书内容确认表；

9）其他有关记录表等（如：审核现场实施的照片；交通票据；与受审核方交接清单等）。

审核组长负责收集、整理全部审核资料，核查资料的完整性和真实性，现场审核收集的申请认证组织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。一般情况下在30 天内交技术部，遇特殊情况需一定整改时间的，提交资料周期最长不超过审核计划结束日期后三个月；再认证项目审核组长应关注证书到期时间。

5.8 审核信息的上报

根据中国认监委建立的自愿性认证活动执法监管信息动态上报制度的要求（参照国认法[2010]60 号文件）的要求，审核部应将已安排好的审核计划信息上报至认证认可业务信息统一上报平台。上报信息包括审核开始/结束时间、审核场所及审核地址、审核组人员信息、以及受审核方联系人及联系方式等。上报信息应及时、准确，至少在审核开始实施之日起的前 4 天完成上。如审核计划有任何变更，审核部应根据审核组或受审核组织反馈的信息，及时调整审核方案及审核计划，确认后将调整后的审核计划信息更新至认证认可业务信息统一上报平台，修改时间截止到认证活动开始前一天的 18：00 点。如因特殊情况，审核活动现场终止，应与审核组了解并记录详细情况，并立即在上报平台中对该项目进行终止审核。

5.9 认证决定要求

公司授权认证决定人员实施认证决定，认证决定人员对认证决定的结果进行批准，认证评定人员根据对审核过程中收集的信息以及审核过程之外获取的任何可作为认证决定依据的信息（如来自行政监管部门、顾客、行业协会的信息等）进行认证决定。 为确保公正性，所有参与认证决定的人员不能是实施审核的人员。对于信息安全管理体系还应满足下面要求：

a)认证决定应基于审核报告中审核组对客户的 ISMS 是否通过认证的建议。

b)通常情况下，审议人员不宜推翻审核组的负面建议。如果发生这种情况，应记录其做出推翻建议的决定的依据，并说明其合理性。

c)只有具备充分的证据证实管理评审和 ISMS 内部审核的安排已经实施，且是有效的并将得到保持，才可向客户授予认证。

6. 授予、拒绝、保持认证、扩大或缩小认证范围、更新、暂停或恢复或者撤销认证资格

6.1 授予认证资格

当受审核组织满足以下条件时，相关管理体系将获得授予：

a) 认证客户的申请材料真实、准确、有效；

b) 认证客户建立和实施的相关管理体系符合认证标准/规范性文件要求，审核组提出推荐认证的结论意见；

c) 认证客户申请认证范围在法律地位文件和资质规定的范围内；

d) 国家或地方或行业有要求时，认证客户申请认证范围内的组织单元、服务及其过程和活动已满足适用的法律法规的要求；

e) 审核证据表明管理评审和内部审核的安排已实施、有效且得到保持，并已进行了一次覆盖管理体系所有要求的完整内部审核；

f) 审核中发现的不合格在规定期限内已经采取纠正/纠正措施，经 KCB 验证有效。

g) 至少近一年来，认证客户申请认证范围内未发生信息安全泄露事故或国家检查不合格；

h) 按认证合同规定履行了相关义务（如缴纳认证费用）。

6.2 拒绝认证注册的程序

a) 不满足满足批准认证资格的条件，经 KCB 评审为不予受理认证或认证客户的管理体系不满足批准认证资格条件；

b) KCB 向认证客户发出不予认证注册通知。

6.3 保持认证资格的程序

当受审核组织满足以下条件时，相关管理体系将获得保持其认证注册资格：

a) 获证组织接受 KCB 监督审核的结果，将作为 KCB 做出保持、扩大、缩小、暂停、恢复、撤销决定的依据。

b) 获证组织接受监督审核后，KCB 评定确认符合认证标准要求，符合保持条件，将做出保持认证证书决定后，将向其发放保持认证注册资格通知书。

6.4 扩大认证范围程序

当获证组织的活动、产品发生变化时，获证组织可以申请变更认证范围。

a) 获证方欲扩大认证范围时，应向 KCB 提出书面申请，明确扩大的认证范围，补充必要的信息。

b) 获证方扩大认证范围时，应将有关体系文件随同申请一起提交。

c) KCB 对获证方拟扩大认证范围的申请进行评审，签订扩大认证范围的认证合同。

d) KCB 对获证方的管理体系文件实施审核后，实施对扩大认证范围的现场审核。扩大认证范围的补充审核可单独进行，也可结合获证组织的监督审核或者再认证审核进行。

e) 扩大认证范围的审核结论由 KCB 审议批准后，予以换发认证证书。

6.5 缩小认证范围的程序

a) 获证方欲缩小认证范围时，应及时向公司提交书面报告，说明缩小范围的原因。公司接到获证方报告后，报公司技术部批准。

b) 在监督审核时发现下列情况，审核组可建议缩小认证范围，并在审核报告中说明，报 KCB。

——如果客户未能在认证机构规定的时限内解决造成暂停的问题，认证机构应缩小或撤销其认证范围。

——如果客户在认证范围的某些部分持续地或严重地不满足认证要求，KCB 将缩小其认证范围，以排除不满足要求的部分。认证范围的缩小应与认证标准的要求一致。

c) 经 KCB 审查作出决定后，予以更换认证证书。

6.6 变更认证证书的程序

有下列情况之一时，获证组织应提出书面申请，必要时应提供有关书面证实材料，KCB 将根据情况对获证组织进行审核和/或验证书面材料，确认达到授予条件者，予以换发认证证书：

——获证组织申请认证依据标准和/或体系覆盖范围扩大或者缩小时；

——认证活动依据认证标准和/或 KCB 认证要求发生修改时；

——引起认证证书内容变更的其它情况（如：组织名称、地址变更）。

以上变更，组织需填写认证证书内容确认单并签字和加盖公章。技术部将对获证组织提交的资料进行评审，确认后为获证组织换发新的认证证书。

6.7 暂停认证资格的程序

a) 发生以下情况（但不限于）时，KCB 应暂停获证客户的认证证书和标志的使用资格：

——管理体系持续或严重不满足认证要求，包括对管理体系运行有效性要求的；

——组织不承担、履行认证合同约定的责任和义务的；

——获证组织在证书有效期内受到相关执法监管部门处罚；

——被地方认证监管部门发现体系运行存在问题，需要暂停证书的；

——持有的行政许可证明、资质证书、强制性认证证书等过期失效，重新提交的申请已被受理但尚未换证的；

——组织主动请求暂停，提交申请后经公司批准的；

——组织发生信息安全泄露相关的重大事故，反映出组织的体系建立及运行存在重大缺陷的；

——组织存在其它严重影响体系运行的严重不符合，不能在规定的时间内及时采取有效的纠正措施的;

——其他应当暂停认证证书的。

b) 在暂停期间，客户的管理体系认证暂时无效，应停止使用带有认证标志的认证证书、其它对外宣传材料。KCB 暂停获证组织认证注册资格后，将向该获证组织发出暂停认证注册资格通知书，同时在 KCB 网站上公告。

c) 如果客户未能在 KCB 规定的时限内解决造成暂停的问题，将撤销或缩小其认证范围。多数情况下，暂停期限为 6 个月。

6.8 恢复认证资格的程序

a) 获证组织已针对暂停认证资格的原因采取了有效的纠正措施，产生原因已经消除，认证资格的恢复符合相关的认证要求，同时已证实在暂停期间内没有使用、引用认证资格（如广告宣传）和使用认证标志；

b)经 KCB 审定，确认获证客户在暂停认证资格的认证范围内已恢复符合相关的认证要求，作出同意恢复认证资格的结论，颁发恢复通知书并公告。

6.9 撤销认证资格的程序

在认证证书有效期内，发生下列情况之一时，经 KCB 确认，将撤销获证组织认证注册资格：

a) 审核未通过；

b) 被注销或撤销法律地位证明文件的；

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

d) 出现重大的信息安全泄露事故，经执法监管部门确认是获证组织违规造成的；

e)　获证组织在证书有效期内有其他严重违反法律法规行为的；

f)　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（包括持有的行政许可证明、资质证书、强制性认证证书等已经过期失效但申请未获批准）；

g)　没有运行管理体系或者已不具备运行条件的；

h)　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，或者认证机构已要求其纠正但超过 2 个月仍未纠正的；

i)　获证组织发生了与信息安全泄露有关的重大事故，反映出组织的体系建立及运行存在重大缺陷的；

j)　获证组织不承担、履行认证合同约定的责任和义务；

k)　获证组织主动放弃认证；

l)　获证组织存在其它严重影响体系运行的严重不符合、不能在规定期限内及时采取有效纠正措施的；

m)　被国家质量监督检验检疫总局列入信用严重失信企业名单；

n)　拒绝接受国家产品质量监督抽查的；

o)　其他应当撤销认证证书的。

KCB 撤销获证组织认证注册资格后，将向该获证组织发出撤销认证注册资格通知书， 同时在 KCB 网站上公告。

获证组织须按国家认监委（CNCA）、认可委规定，从接到撤销通知书之日起立即停止使用带有认证标志的认证证书、对外宣传资料和/或产品包装。

对撤销认证资格的获证组织的违规活动，一切后果由该获证组织自行承担。

7.　认证证书和认证标志

7.1 认证证书

KCB 对受审核组织管理体系符合认证要求所颁发的证明文件，有效期三年。

管理体系认证证书的内容包括：

a)　证书名称；

b)　认证注册号（即证书编号）；

c)　获证客户的名称、地址（多场所认证包括总部和所有场所的地址信息）、统一社会信用代码。该信息应与其法律地位证明文件的信息一致；

d)　管理体系认证所覆盖的范围，适用时，包括每个场所相应的认证范围，且没有误导或歧义；

e)　授予认证、扩大或缩小认证范围、更新认证的生效日期，生效日期不应早于相关认证决定的日期；

f)　认证有效期 ；

g)　审核获证客户时所用的管理体系标准和（或）其他规范性文件，包括发布状态的标示（例如修订的时间或编号）；

h)　认证用标准和（或）其他规范性文件所要求的任何其他信息；

i)　公司的名称、地址和认证标识；

j)　公司的印章和公司法人的签字；

k)　相关的认可标识及认可注册号（适用时）；

l)　为便于社会监督，在证书上应注明："本证书信息可在国家认证认可监督管理委员会官方网站（www.cnca.gov.cn）上查询"。

7.2 认证标志：KCB 对受审核组织管理体系是否符合认证要求给予的认证标志

ISO/IEC27001
KCB Certification

7.3 认证证书和标志的使用原则和要求

7.3.1 认证证书和标志只能由获证方在获准认证范围内使用，不准以任何方式转让、出售或借用、冒用。使用时必须与获证方单位名称和产品名称放在一起。

7.3.2 认证证书有效期三年，在有效期内，经公司年度监督审核通过后，颁发保持认证注册资格通知书，与主证书一并使用，证书才能继续有效，获证方方可继续使用管理体系认证证书和认证标志。

7.3.3 认证标志可以用于组织有关文件、文具、邮政信件和出版物等组织介绍宣传材料上，但不得用于获证组织的产品上或以其他可能误导的方式，暗示其产品、过程或服务已通过我公司认证。如果用于运输的包装箱上使用该标志，必须声明箱子中产品的生产商已通过管理体系认证并符合具体的认证标准。

7.3.4 对于检验和校准实验室的管理体系的认证，由于检验报告或实验室报告被视作产品，因此认证标志不能使用在这些报告上。

7.3.5 获证方在标志使用方案报公司批准后方可正式使用。获证组织应当在认证范围内使用认证证书和认证标志，不得利用管理体系认证证书、认证标志和相关文字、符号，误导公众认为其产品、服务已通过认证。

7.3.6 使用标志图案时，必须根据公司提供的图样按比例放大或缩小，不得变形使用；

7.3.7 获证方不得进行被公司认为误导顾客的错误宣传，一经发现不正确宣传证书和标志的误导使用，公司将采取监管措施直至撤销认证资格，必要时采取法律手段。

7.3.8 获证方认证证书缩小范围时，应修改所有的广告宣传材料；

7.3.9 获证客户如要在产品包装上或附带信息中声明通过管理体系认证，需包含以下内容：

—— 获证客户的标识（例如品牌或名称）；

—— 管理体系的类型和适用标准；

—— 颁发证书的认证机构。

使用认证标识时，应同时附有明确的声明以避免导致对该产品、过程或服务通过认证。产品包装的判

别标准是其可从产品上移除且不会导致产品分解、碎裂或损坏。附带信息的判别标准是其可分开获得或易于分离。型号标签或铭牌被视为产品的一部分。

7.4 认证证书和标志的暂停使用和恢复

7.4.1 当获证方被公司暂停认证注册资格时，获证方应暂停证书和标志的使用。

7.4.2 当获证方被公司批准恢复认证资格时，公司应及时通知其恢复使用认证证书和标志。

附录 A 信息安全管理体系 员工有效人数与审核时间的关系（仅适用于初次审核）

组织员工数	初审总审核人日 （标准基础人日）
1-10	5
11-15	6
16-25	7
26-45	8.5
46-65	10
66-85	11
86-125	12
126-175	13
176-275	14
276-425	15
426-625	16.5
626-875	17.5
876-1175	18.5
1176-1550	19.5
1551-2025	21
2026-2675	22
2676-3450	23
3451-4350	24
4351-5450	25
5451-6800	26
6801-8500	27

注 1：表中的人数宜视为连续变化的，而不是阶梯式变化的；当人数超过 8500 人时，审核时间遵循上表中的递进规律，与该表保持一致。

附录 B 适用抽样审核的多场所组织的抽样要求

1 确认抽样数量

1.1 每次审核最少审核的场所数量是：

初次认证审核：样本的数量应为场所数量的平方根（y= √x ），计算结果向上取整为最接近的整数，其中 y 为将抽取场所的数量、x 为场所总数。

监督审核：每年的抽样数量应为场所数量的平方根乘以 0.6 即（y=0.6 √x ），计算结果向上取整为最接近的整数。

再认证审核：样本的数量应与初次审核相同。然而，如果证明管理体系在认证周期中是有效的，样本的数量可以减少至乘以系数 0.8 即（y=0.8√ x ），计算结果向上取整为最接近的整数。

1.2 当对拟认证或获证管理体系涵盖的过程、活动进行风险分析，发现涉及下列因素的特殊情况时，应增加抽样的数量或频率：

——场所的规模和员工的数量；

——过程、活动以及管理体系复杂程度和风险水平；

——工作方式的差异（如：倒班）；

——所从事过程、活动的差异；

——投诉记录，以及纠正措施和预防措施的其他相关方面；

——与跨国经营有关的任何方面；

——内部审核和管理评审的结果。

1.3 如果组织的分支机构分为不同等级（如：总部办公室/中心办公室，全国性办公室，地区办公室，地方分支），上述的初次认证审核抽样模式适用于每个等级的场所。示例：

1 个总部办公室：每个审核周期（初次审核、监督审核或再认证审核）都审核；

4 个全国性办公室：样本数量=2，至少 1 个为随机抽样；

27 个地区办公室：样本数量=6，至少 2 个为随机抽样；

1700 个地方分支：样本数量=42，至少 11 个为随机抽样。

地区办公室的样本中宜至少覆盖到每个全国办公室控制的地区办公室。地方分支的样本中宜至少覆盖到每个地区办公室控制的地区分支。这样可能导致每个等级的场所抽样数量超过计算的最小抽样数量。

1.4 抽样过程应作为审核方案管理的一部分。在任何时候（即：在策划监督审核之前、或组织的任何场所变更其结构时、或将在认证边界之内增加新的场所时），应预先评审审核方案中的抽样安排，以便在为

保持认证对样本审核之前能确定抽样数量调整的需求。

2 确认抽样审核的场所

2.1 在初次认证审核、每次再认证审核以及作为监督的一部分在每个日历年至少一次的审核中，都应对中心职能审核。

2.2 样本中应有一部分根据以下因素选取，一部分随机抽取；并且其结果应选到在有代表性的不同场所，确保认证范围内覆盖的所有过程将被审核到，且使得证书有效期内所选场所之间的差异尽可能大。

2.3 至少 25%的样本应随机抽取。

2.4 场所选取应考虑，但不限于以下方面：

——对场所内部审核、管理评审和/或以前认证审核的结果；

——投诉记录以及纠正和预防措施的其他相关方面；

——各场所在规模上的显著差异；

——在倒班安排和工作程序上的差异；

——管理体系以及在场所实施过程的复杂程度；

——上次认证审核后的变化；

——管理体系的成熟度和组织的理解程度；

——对于环境管理体系，考虑环境问题和环境因素及其关联影响的程度；

——对于职业健康安全管理体系，考虑与其所进行活动相关的 OHS 风险、合同协议、被另一认证机构认证的情况、内部审核制度、事故统计和未遂事件统计，以及每个场所的业务活动（技术、设备、使用和存储的危险材料的数量、工作环境、场所等）之间的差异；

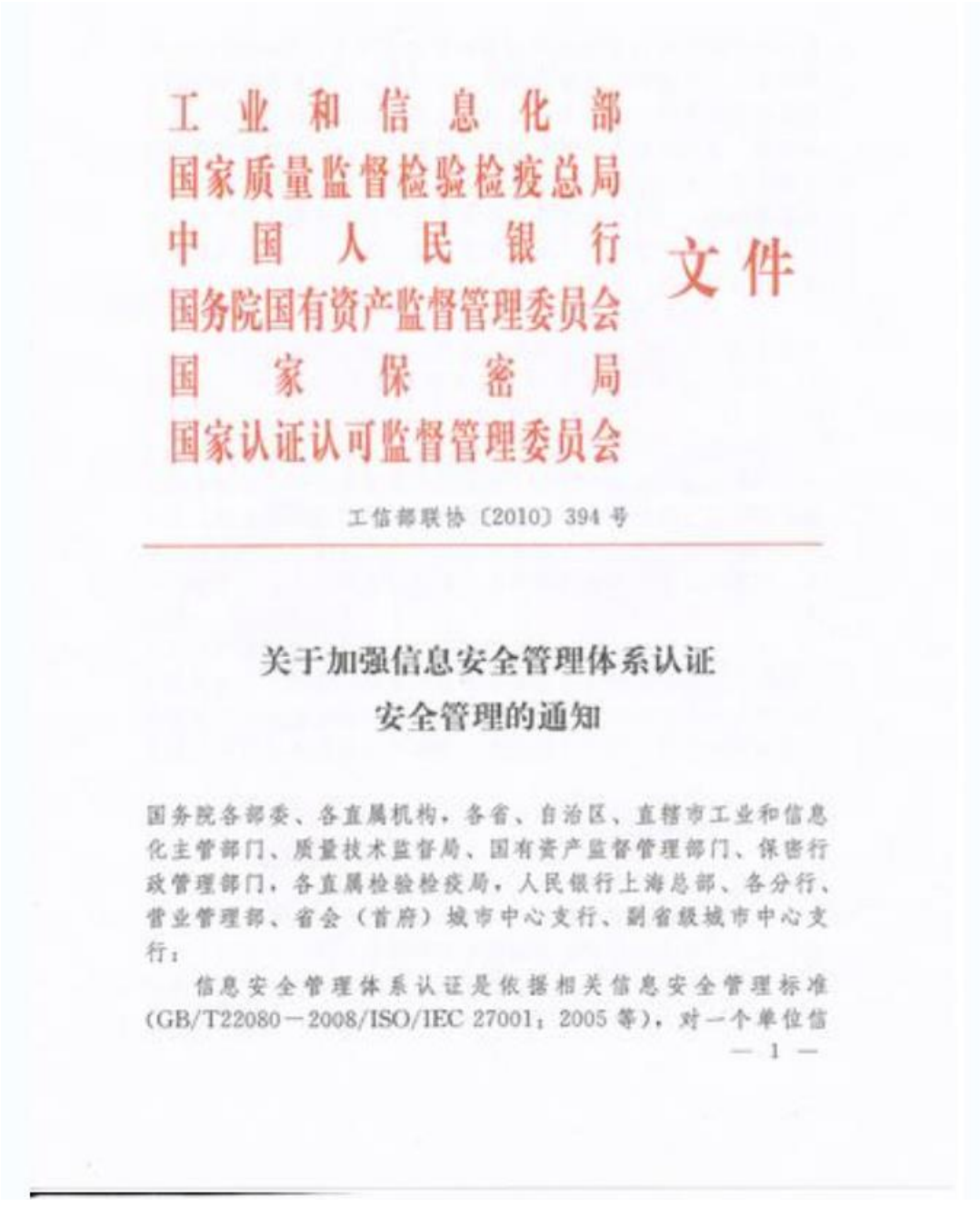
——文化、语言和法律法规方面的差异；

——地理位置的分散程度；

——场所是常设的、临时的或虚拟的。

2.5　并不是必须在审核过程一开始就完成抽样。也可能在完成对中心职能的审核时完成抽样。不论哪种情况，应将样本中所包括的场所通知中心职能。这可能是在相对较短时间内通知，但应给出充分的时间用于审核准备。

附录 C 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》



工 业 和 信 息 化 部
国家质量监督检验检疫总局
中 国 人 民 银 行
国务院国有资产监督管理委员会
国 家 保 密 局
国家认证认可监督管理委员会

文件

工信部联协〔2010〕394 号

关于加强信息安全管理体系认证安全管理的通知

国务院各部委、各直属机构，各省、自治区、直辖市工业和信息化主管部门、质量技术监督局、国有资产监督管理部门、保密行政管理部门，各直属检验检疫局，人民银行上海总部、各分行、营业管理部、省会（首府）城市中心支行、副省级城市中心支行：

信息安全管理体系认证是依据相关信息安全管理标准（GB/T22080－2008/ISO/IEC 27001：2005 等），对一个单位信

— 1 —

息安全管理状况进行评价的过程。开展信息安全管理体系认证，有利于各单位规范信息安全管理，有利于企业特别是服务外包企业开拓国际市场。但由于认证活动涉及被认证单位组织体系、业务流程、网络拓扑、关键信息设备配置、安全防护情况及薄弱环节等敏感信息，如果管理不到位，造成敏感信息泄露，将会使被认证单位面临信息安全风险，甚至危及国家经济安全和利益。为加强信息安全管理体系认证的安全管理，减少信息安全风险，现就有关事项通知如下：

一、各级政府机关和政府信息系统运行单位，不得利用社会第三方认证机构开展信息安全管理体系认证。为确保国家秘密安全，涉密信息系统建设使用单位不得申请信息安全管理体系认证。

二、各级工业和信息化主管部门要了解掌握同级政府部门信息技术外包服务情况，结合实际提出安全管理要求；指导督促为政府部门提供信息技术外包服务的机构加强信息安全管理。为政府部门提供信息技术外包服务的机构申请信息安全管理体系认证时，若其认证范围涉及政府信息，须经工业和信息化主管部门同意。

三、国家认证认可监督管理部门要针对信息安全管理体系认证的特点，进一步完善信息安全管理体系认证管理办法和相关标准，严格信息安全管理体系认证机构的市场准入管理，加强资质审查和日常监管，规范认证行为，依法严肃查处违法违规认证活动。

四、基础信息网络和重要信息系统主管部门及国有资产监督管理部门应加强对行业和国有企业的信息安全管理，对信息安全管理体系认证提出管理要求。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确需申请信息安全管理体系认证，应事先报行业主管或监管部门同意，其他涉及国计民生的国有企业确需申请信息安全管理体系认证，应事先报国有资产监督管理部门同意，涉及国家秘密的应报保密行政管理部门同

意。通过认证后，应加强信息安全风险评估，及时排查安全漏洞和安全隐患。

五、申请认证单位应选择国家认证认可监督管理部门批准从事信息安全管理体系认证的认证机构进行认证，并与认证机构签订安全和保密协议，严格信息安全和保密管理，要求认证机构切实履行不泄露、不扩散、不转让认证信息的义务，保证重要敏感信息不出境。

工业和信息化部　　国家质量监督检验检疫总局

中国人民银行　　国务院国有资产监督管理委员会

国家保密局　　国家认证认可监督管理委员会

二〇一〇年八月十二日

信息安全管理体系认证实施规则				
文件编号	发布日期	实施日期	修改日期	版　次
KCB-QPXX05	2020-01-01	2020-01-01	2025-08-26	G/9

附件：

文件更改记录

更改页	更改状态	更改内容	更改人	日期
封面、页眉、全文	有效	调整 LOGO	付冉	2020.05.07
11	有效	5.2.5.3：审核一、二阶段间隔要求	刘越	2020.12.12
13、20	有效	5.3.2 审核证据需覆盖认证范围 5.6.2 明确扩项条款要求	季倩	2022-9-20
13	有效	5.3.2 增加确认审核范围要求	季倩	2023-09-18
4、21	有效	5.1.6.6.1 增加 ITSMS 认证选择和指派审核组时的特殊要求 5.8.1 增加 ISMS 收集企业适用性声明文件要求	季倩	2023-11-30
10	有效	5.2.5.2.1 增加一体化管理体系确认要求	王文哲	2024-06-03
5、8、11、12、18、20	有效	依据 ISO/IEC 27006-1:2024 修订审核策划及审核实施的要求	李会凤	2025-3-27
	有效	CNAS-CC170 转换，修订 5.3.6.1 审核报告要求	季倩	2025-3-28
全文	有效	第 2 章中增加“认证依据”，增加“6 授予、拒绝、保持认证、扩大或缩小认证范围、更新、暂停或恢复或者撤销认证资格”及“7 认证证书和认证标志”，删除规则中与 ITSMS 相关部分	胡娜娜	2025-05-27
全文	有效	补充申请评审程序、人日要求、抽样要求，修订引用内部文件相关内容	胡娜娜	2025-08-26