信息安全管理体系认证规则

文件编号：CCQC-ISMS-001

版本号：A/2

发布日期：2025 年 12 月 3 日　　实施日期：2025 年 12 月 3 日

目录

一、适用范围

1.1 本规则用于规范深圳市中鑫认证检测有限公司（以下简称“CCQC”）对申请认证的各类组织按照 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》建立信息安全管理体系认证的认证活动。

1.2 本规则依据认证认可相关法律法规及认证规范，对信息安全管理体系认证认证活动作出具体规定，明确本机构对认证过程的管理责任，开展信息安全管理体系认证认证活动时应当遵守本规则。

1.3 该规则可以通过本公司官方客服电话（0755-86568634）获取。

二、认证依据

2.1 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》

三、管理要求

3.1 本机构为规范信息安全管理体系（以下简称：ISMS）认证工作,根据《中华人民共和国认证认可条例》、《认证机构管理办法》、《国家认监委关于加强认证规则管理的公告》(2025 年第 9 号)以及 GB/T 27021.1/ISO/IEC 17021-1《合格评定 管理体系审核认证机构要求 第 1 部分:要求》等法律法规及相关认证认可规范文件的要求，结合相关技术标准制定本规则。

3.2 建立内部制约、监督和责任机制，实现培训、认证和认证决定等工作环节相互分开，以符合公正性要求。

3.3 提供的管理体系认证可结合其他管理体系认证活动进行。

四、对认证人员的要求

4.1 对从事信息安全管理体系认证业务的人员（包括：认证规则和认证方案制定人员、认证申请评审人员、认证审核/评价方案管理人员、现场认证审核人

员（组长/组员）、认证决定或复核人员、认证人员能力的评价人员），根据其所承担的任务和公司对认证业务范围特点的分析和风险评估，确定其能力资格，以确保各类认证人员具备适宜的知识和技能。认证审核人员必须取得信息安全管理体系认证注册资格。

4.2 具有本机构信息安全管理体系相应专业类别的人员。

4.3 认证人员应当遵守与从业相关的法律法规，对认证审核活动及相关认证审核记录和认证审核报告的真实性承担相应的法律责任。

五、初次认证程序

5.1 申请认证的组织应提交以下申请资料：

（1）认证申请书，申请书应包括申请认证的生产、经营或服务活动范围及活动情况的说明；

（2）法律地位的证明性文件：营业执照：法定许可文件、备案证明扫描件(适用时)，如资质证书、许可证等：对管理体系覆盖多个法律实体时，应提供每个场所的法律地位证明性文件：

（3）信息安全管理体系文件，包括 1)体系范围；2)方针；3)目标；4)信息安全风险评估准则及报告；5)信息安全风险处置计划；6)残余风险评估报告（适用时）；7)适用的信息安全法律法规要求清单；8)网络拓扑结构图（适用时）；9)组织机构图或职责说明；10)盖申请范围的 1 个或多个适用性声明(SOA)

注：以上文件若包含在手册、程序文件中可不单独提供。

（4）工信部安全审查备案（适用时）。

（5）说明适用的关于认证机构的资质、信息安全守法记录或认证人员身份背景的要求，以及适用的与保守国家秘密或维护国家安全有关的法律法规要求，并即时更新该说明，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（适用时）。

（6）其他需要的文件。

5.2 合同评审

5.2.1 合同评审人员对申请组织提交的申请资料进行审查，并确认：

（1）申请资料齐全。

（2）申请组织从事的活动符合相关法律法规的规定。

（3）申请组织为达到目标而建立了文件化的信息安全管理体系认证。

（4）申请认证的业务范围是否在本公司认证的业务范围之内。

5.2.2 根据申请组织申请的认证范围、生产经营场所、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 CCQC 是否有能力受理认证申请。

5.2.3 对符合 5.2.1 和 5.2.2 要求的，CCQC 将受理认证申请；对不符合 5.2.1 和 5.2.2 要求的，将通知申请组织补充和完善，或者不受理申请并告知理由。

5.3 签订认证合同

公司根据评审结论与认证申请方签署《认证合同书》，信息安全管理体系相应内容应完整、清晰、准确无误。在实施认证审核前，公司应与每个申请组织订立具有法律效力的认证合同或等效文件，以明确双方的责任，合同应至少包含的内容同其他管理体系。

5.4 审核方案和审核策划

5.4.1 审核方案

5.4.1.1 初次认证的审核方案应包括两阶段初次审核、获证后的监督审核和认证到期前进行的再认证审核。

注：一个认证周期通常为 3 年，从初次认证（或再认证）决定算起， 至认证的有效期截止。

5.4.1.2 初次认证审核和再认证审核是对认证委托人完整体系的审核，应覆盖 ISO/IEC 27001:2022 所有要求，以及认证范围内的典型产品和服务。认证证书有效期内的监督审核应覆盖 ISO/IEC 27001:2022 所有要求。

5.4.1.3 初次认证及再认证后的第一次监督审核应在证书签发起 12 个月内进

行。此后，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，且两次监督审核的时间间隔不得超过 15 个月。

5.4.2 审核时间

5.4.2.1 审核时间是指策划并完成一次完整且有效的管理体系审核所需的时间。为确保认证审核的完整有效，CCQC 应根据申请组织信息安全管理体系覆盖的活动范围、特性、复杂程度、风险程度、认证要求和体系覆盖范围内的有效人数等情况，计算审核时间。机构在项目方案制定过程中可以在人日基数上（见附录 A）进行增减。

5.4.2.2 审核时间计算，包括增减人日的考虑因素应满足 GB/T 27021.1《合格评定 管理体系审核认证机构的要求》、CNAS-CC170《信息安全管理体系认证机构要求》等认证认可准则要求。

5.4.2.3 CCQC 应当为每次审核计算管理体系认证审核时间（适用时，含多场所组织的抽样等），并留有记录。

5.4.2.4 如果企业申请管理体系多领域一体化审核，一体化审核时间计算应基于组织的管理体系的一体化程度来确定的审核时间，可在一阶段和后续的审核中，根据所确认的组织管理体系的一体化程度来做出调整。可能会导致审核时间的增加，但在减少审核时间的情况下，其减少量不应超过 20%。

5.4.3 多场所抽样方案

5.4.3.1 多场所抽样条件

（1）CCQC 应当逐一到各场所进行审核，不适用场所抽样可能有多种原因，例如：

a） 所有场所实施的过程、活动与管理体系的范围有关且存在显著差别；

b） 客户要求对每个场所审核；

c） 有专门的方案或法规要求规定了系统性地对每个场所审核等。

（2）当客户拥有满足以下 a)至 c)的多个场所时，CCQC 可以考虑使用

基于抽样的方法进行多场所认证审核：

a) 所有的场所在同一个 ISMS 下运行且该 ISMS 实行集中统一的管理、审核和管理评审；

b) 所有的场所都包含在客户的 ISMS 内部审核方案中；

c) 所有的场所都包含在客户的 ISMS 管理评审方案中。

5.4.3.2 多场所抽样规则

（1）在使用基于抽样的方法时应确保：

a) 在初次的合同评审时，最大程度地识别场所之间的差异，以便确定适当的抽样水平；

b) 结合以下因素，认证机构抽取具有代表性的场所：

1)总部(适宜时)及各场所的内部审核结果；

2)管理评审的结果；

3)场所规模的差异；

4)场所业务范围的差异；

5)不同场所信息系统的复杂程度；

6)工作实践的差异；

7)所开展活动的差异；

8)控制的设计与运行的差异；

9)与关键信息系统或处理敏感信息的信息系统之间的潜在交互；

10)任何不同的法律要求；

11)地域因素和文化因素；

12)场所的风险状况；

13)特定场所发生的信息安全事件。

c) 从客户 ISMS 范围内的所有场所中选择具有代表性的样本，该选择应基于一个可体现上述 b)中所列因素的判定，同时也考虑随

机因素；

d） 在授予认证之前，应审核了 ISMS 中每个具有重大风险的场所；

e） 根据上述要求设计审核方案，且审核方案要在三年内覆盖 ISMS 认证范围内的代表性样本；

f） 在单个场所发现不符合时，纠正措施程序的实施适用于证书所覆盖的所有场所。

（2）抽样数量应不少于按以下方法计算的结果：

a）初次认证审核：Y=$\sqrt{X}$

b）监督审核：Y=$0.6\sqrt{X}$

c）再认证审核：Y=$0.8\sqrt{X}$

注：其中 Y 为抽样的数量，结果向上取整；X 为相似场所的总体数量。

（3）除非特定认证方案另有规定，单个被抽样场所审核时间的减少量不应超过 50%。

5.4.3.3 审核应关注客户为确保单一的 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。

5.4.3.4 其他多场所抽样要求将依据 CNAS-CC11《多场所组织的管理体系审核与认证》文件要求。

5.4.4 审核组

5.4.4.1 公司应当根据信息安全管理体系覆盖的活动的专业技术领域选择具备相关能力的审核员组成审核组，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。

5.4.4.2 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。

5.4.4.3 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，在审核过程中的活动由审核组中的审核员承担责任。

5.5 审核计划

5.5.1 审核组长根据 CCQC 委派的审核任务通知书，制定书面审核计划并组织实施。

5.5.2 审核计划至少包括以下内容：审核目的、审核范围、审核过程、审核涉及的部门和场所、审核时间、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）。

5.5.3 初次认证审核、监督、再认证审核应在申请组织申请认证的范围涉及到的各个场所现场进行。

5.5.4 如果信息安全管理体系认证包含在多个场所进行相同或相近的活动，且这些场所都处于该申请组织授权和控制下，认证机构可以在审核中对这些场所进行抽样，但应制定合理的抽样方案以确保对各场所信息安全管理体系认证的正确审核。如果不同场所的活动存在根本不同、或不同场所存在可能对信息安全管理产生显著影响的区域性因素，则不能采用抽样审核的方法，应当逐一到各现场进行审核。

5.5.5 为使现场审核活动能够观察到产品生产或服务活动情况，现场审核应安排在认证范围覆盖的产品生产或服务活动正常运行时进行。

5.5.6 在审核活动开始前，审核组应将书面审核计划交申请组织确认。遇特殊情况临时变更计划时，应及时将变更情况书面通知受审核的申请组织，并协商一致。

5.6 实施审核

审核组应当按照审核计划的安排完成审核工作。除不可预见的特殊情况外，审核过程中不得更换审核计划确定的审核员。

审核组应当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管理体系相关的职能部门负责人员应该参加会议。参会人员应签到，审核组应当保留首、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。

初次认证审核，分为第一、二阶段实施审核。

5.6.1 文件审核

组长或组织相关审核员对受审核方的信息安全管理体系文件及必要的其它文件进行符合性评审，以确定审核的可行性，并确信能够实现审核目标。对评审中发现问题和评审结论应形成《文件评审报告》并提出明确的整改要求和时限。

5.6.2 第一阶段审核

5.6.2.1 第一阶段审核应至少覆盖以下内容：

（1）审核受审核方形成文件的信息安全管理体系信息的真实、准确、完整、有效性；

（2）获取有关 ISMS 设计的文件，包括 ISO27001 所要求的文件。至少应包括：

--ISMS 和其所覆盖活动的一般信息；

--ISO 27001 要求的 ISMS 文件的副本，以及需要时，其他相关文件。

（3）应在客户的组织设置、风险评估与风险处置（包括所确定的控制）、信总安全方针和信息安全目标、适用性声明的背景下充分了解 ISMS 设计，特别是应充分了解客户的审核准备情况。

（4）确认受审核方的 ISMS 范围和边界的界定是否清晰和充分。

（5）通过现场观察，了解组织的基本概况，包括组织机构及职能，信息安全服务的流程和特点、活动的现场分布情况，提供过程中对资产的保密性、完整性及可用性要求，重要资产清单中所列资产的物理位置。应关注在服务和活动过程中和 ISMS 直接相关的重要场所:信息安全管理体系推进部门；核心信息处理设施的放置场所，如核心机房等；IT 部门，如信息系统的设计、开发及维护部门；与重要信息资产有关的现场。

（6）审查第二阶段审核所需资源的配置情况，并与申请组织商定第二阶

段审核的细节。

（7）评价组织对外包方的识别管理情况。

（8）以上所了解的信息应用于策划第二阶段。并使客户知晓在二阶段审核中可以要求对更进一步的或其他类型的信息、文件、记录进行详细检查。

5.6.2.2 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。对在第二阶段审核中可能被判定为不符合项的重要关键点，要及时提醒申请组织特别关注。

5.6.3 第二阶段审核

5.6.3.1 第二阶段审核应当在申请组织现场进行。重点是审核信息安全管理体系认证符合 ISO/IEC 27001:2022 标准要求和有效运行情况，应至少覆盖以下内容：

（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来确定控制

（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：审核应考虑外部环境、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，并确定待实现的控制是否已经实现且在整体上是有效的

（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。

5.6.3.2 发生以下情况时，审核组应向公司报告，经公司同意后终止审核：

（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。

5.6.4 审核报告

审核组长应对审核活动形成书面审核报告。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）ISMS 管理体系范围、过程、场所的必要信息。

（2）所采用的主要审核路线和所使用的审核方法。

（3）客户信息安全风险分析的审核情况说明。

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

（5）所引用的适用性声明版本，以及适用时，与客户以往认证审核结果的何有用的比较。

注:完成的问卷、检查清单、评论意见、日志或审核员笔记可以构成审核报告的组成部分。如果使用了这些方法，这些文件应作为支持认证决定的证据提供给公司。有关审核中所评价的样本的信息，应包含在审核报告或其他认证资料中。

（6）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。

（7）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。

（8）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。受审核方的 ISMS 管理体系符合标准的情况，如方针、目标指标和管理要求的实施完成情况，重要信息安全风险是否都得到控制，各种程序文件和作业指导书的执行情况等。

（9）受审核方 ISMS 管理体系实施的适宜性和有效性，包括改进机会等:应概述关于 ISMS 要求和信息安全控制的实现与有效性的最重要评论意见(正面的和负面的)。

（10）审核发现的不符合项概述，以及实施完成纠正措施的要求:不符合项纠正措施有效性验证情况。

（11）是否偏离审核计划的情况。

5.6.5 不符合项的纠正和纠正措施及其结果的验证

5.6.5.1 审核组应当根据审核发现形成严重或轻微不符合，要求受审核方在规定的时限内对不符合进行原因分析、采取相应的纠正和纠正措施(轻微不符合可以是纠正措施计划)。公司应审查受审核方提交的纠正和纠正措施，以确定其是否可被接受。

5.6.5.2 对于严重不符合，要求受审核方在规定时间内完成整改；公司应当督促受审核方及时进行整改，并对其纠正和纠正措施的有效性进行验证。

5.6.5.3 对于组织未能在规定的时限完成对不符合所采取措施的情况，审核组不应当给予该受审核方推荐认证、保持认证或再认证。

5.6.6 认证决定

5.6.6.1 认证决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)进行复核，审核过程中对认证范围、关键过程的实施等方面重点关注，不符合项已评审、接受并验证了纠正和纠正措施及其结果的有效性。

5.6.6.2 对于符合认证要求的申请人，应颁发认证证书。对于不符合认证要求的申请人，应以书面的形式明示其不能通过认证的原因。

5.6.6.3 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。对经审定不合格的申请组织，公司应做出不予以认证注册的决定，并将不能注册的原因书面通知申请组织。

六、监督审核程序

6.1 CCQC 对信息安全管理体系获证组织进行有效跟踪，监督获证组织通过认证的信息安全管理体系认证持续符合要求。

6.2 作为最低要求，在初次认证的第二阶段审核后至少 12 个月内应进行一次监督审核。此后，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，且两次监督审核的时间间隔不得超过 15 个月。

6.3 监督审核的时间，应不少于初审审核时间人日数的 1/3。

监督审核应在获证组织现场进行，但不一定是对整个体系的审核，除应满足管理体系认证通用要求外，还应包括下述方面的审核内容：

（1）ISMS 在实现客户信息安全方针的目标方面的有效性。

（2）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。

（3）所确定的控制的变更，及其引起的适用性声明变更。

（4）审核方案中所述控制的实现和有效性。

6.4 审核组应提出是否继续保持认证证书的意见建议。CCQC 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。

6.5 超过期限未能实施监督审核的，按照暂停或撤销程序处理。

七、再认证程序

7.1 在认证证书期满前，若获证组织申请继续持有认证证书，CCQC 将实施再认证审核决定是否延续认证证书。

7.2 CCQC 将根据整个认证周期的策划并结合历次监督审核情况，策划再认证。

7.3 在信息安全管理体系认证及获证组织的内、外部无重大变更时，再认证可省略第一阶段审核，但审核时间不应少于初次审核时间的 2/3。

7.4 再认证审核还应关注以下内容：

a)对获证客户的业绩评价和文件再评审（需安排在现场审核前进行）。

b)审查获证客户针对保持管理体系有效性和改进管理体系提高整体绩效的承诺的证据。

c)再认证应考虑在最近一个认证周期内的绩效情况。

d)客户的管理体系在实现目标和预期结果方面的有效性。

7.5 对于再认证审核中发现的不符合项，应按要求实施纠正和纠正措施并进行验证，验证应在原有效期满前完成，按照 5.6.6 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。

八、认证证书状态管理规定（认证资格的暂停、恢复、撤销、变更、注销）

8.1 获证组织出现以下情形之一的，CCQC 在调查核实后的 5 个工作日内暂停其认证证书：

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

（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）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。

（5）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。

（6）主动请求暂停的。

（7）其他应当暂停认证证书的。

认证证书暂停期不得超过 6 个月。但属于 8.1 第（5）项情形的暂停期可至相关单位作出许可决定之日。明确暂停的起始日期和暂停期限，及时上报认监委，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。

8.2 暂停证书的恢复

暂停期间，如获证组织采取有效的纠正措施，造成暂停的原因已消除的，应恢复其认证资格，并保留相应证据。

8.3 获证组织出现以下情形之一的，CCQC 在调查核实后的 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）拒绝配合认证监管部门实施的监督检查，或者对有关事项的问询和调查提供了虚假材料或信息的。

（3）出现重大的产品或服务等安全事故，经执法监管部门确认是获证组织违规造成的。

（4）有其他严重违反法律法规行为的。

（5）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）

（6）没有运行信息安全管理体系认证或者已不具备运行条件的。

（7）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 6 个月仍未纠正的。

（8）其他应当撤销认证证书的。

撤销认证证书后，CCQC 将及时收回撤销的认证证书。若无法收回，CCQC 将及时在相关媒体和网站上公布或声明撤销决定，并及时上报认监委。

8.4 证书的变更

出现下列情况之一时，重新更换认证证书

（1）在认证证书有效期内，出现下列情况之一的，应按照有关规定重新换证：

a）管理体系认证标准转换；

b）CCQC 名称、认证标志发生变化；

c）组织名称、地址、认证范围和统一信用代码等认证证书信息发生变化。

（2）在信息安全管理体系认证认证标准变更的情况下，要安排进行审核，审核与认证决定通过后，重新换证，审核可结合年度监督或再认证进行。

（3）在获证组织体系认证范围变更时，获证组织应及时通知 CCQC，如变更的发生对体系产生了较严重的影响时，则需要重新进行审核，审核与认

证决定通过后重新换证。

8.5 认证资格的注销

获证组织主动申请不再保持认证资格时，应注销其认证资格，并保留相应证据。

九、认证证书和认证标志

9.1 认证证书至少包括以下信息：

（1）获证组织名称、地址和组织机构代码。该信息与其法律地位证明文件的信息一致。

（2）信息安全管理体系认证覆盖的生产经营地址或服务的地址和业务范围。若认证的信息安全管理体系认证覆盖多场所，表述覆盖的相关场所的名称和地址信息，该信息应与相应的法律地位证明文件信息一致。

（3）信息安全管理体系认证符合 ISO/IEC 27001:2022 标准的表述。

（4）证书编号。

（5）认证机构名称。

（6）证书签发日期及有效期的起止年月日。对初次认证以来未中断过的再认证证书，可表述该获证组织初次获得认证证书的年月日。

（7）相关的认可标识及认可注册号（适用时）。

（8）证书查询方式。除公布认证证书在本机构网站上的查询方式，还在证书上注明“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）和和公司官网（www.szccqc.cn）上查询”，以便于社会监督。

（9）证书有效期最长为 3 年。

（10）其他需要说明的内容。

9.2 认证标志式样和使用、管理要求

9.2.1 CCQC 的通用标志如下图所示：

9.2.2 认证申请组织通过认证并获得认证证书后，可以在认证范围内使用认证标志。但应当遵守以下规定：

（1）不得使用变形、不完整，或规格、色标不符合要求的认证标识；

（2）保证使用认证标志符合认证要求；

（3）在广告、服务项目介绍等宣传材料中正确地使用认证标志、不得利用认证标志误导消费者；

（4）认证标识不得用于产品或产品包装之上，或以任何其他可解释为表示产品符合性的方式使用；

（5）接受国家认证认可监督委员会、各地质检行政部门和机构对认证标志使用情况的监督审查；

（6）当认证证书被暂停、注销或撤消认证时，应停止使用认证标志和发放带有认证标志的所有文件和宣传资料。

9.2.3 公司对获证组织使用认证证书和认证标志的活动进行监督管理，并已在公司网站公开。发现获证组织未正确使用认证证书和认证标志的，要求获证组织立即采取有效纠正措施，并跟踪监督纠正情况。

十、申诉和投诉

10.1 申请组织或获证组织对认证决定有异议时，可在 10 个工作日内向本机构提出申诉，本机构自收到申诉之日起，在一个月内进行处理，并将处理结果书

面通知申诉人。

10.2 若申诉人认为认证机构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，可以直接向认证监管部门投诉。

十一、认证记录的管理

11.1 应当建立文件管理档案室，并妥善保存。

11.2 记录应当真实准确以证实认证活动得到有效实施。记录资料应当使用中文，保存时间至少应当与认证证书有效期一致。

11.3 以电子文档方式保存记录的，应采用不可编辑的电子文档格式。

11.4 所有具有相关人员签字的书面记录，可以制作成电子文档保存使用，但是原件必须妥善保存，保存时间至少应当与认证证书有效期一致。

附录 A 信息安全管理体系审核时间（引用 CNAS CC170《信息安全管理体系认证机构要求》 附录 B）

在组织控制下工作的人员的数量	ISMS 初次审核审核时间（审核人日）	在组织控制下工作的人员的数量	ISMS 初次审核审核时间（审核人日）	在组织控制下工作的人员的数量	ISMS 初次审核审核时间（审核人日）
1 ~ 10	5	176 ~ 275	14	2676 ~ 3450	23
11 ~ 15	6	276 ~ 425	15	3451 ~ 4350	24
16 ~ 25	7	426 ~ 625	16.5	4351 ~ 5450	25
26 ~ 45	8.5	626 ~ 875	17.5	5451 ~ 6800	26
46 ~ 65	10	876 ~ 1175	18.5	6801 ~ 8500	27
66 ~ 85	11	1176 ~ 1550	19.5	8501 ~ 10700	28
86 ~ 125	12	1551 ~ 2025	21	> 10700	沿用以上规律
126 ~ 175	13	2026 ~ 2675	22		