信息安全管理体系认证规则

编号：CTS/CHTC 0052-2025

信息安全管理体系认证规则

五洲恒通

2025 年 07 月 01 日发布　　2025 年 07 月 01 日实施

北京五洲恒通认证有限公司发布

V0.00　　2025.07

目　录

前　言 1

1 适用范围 1
2 认证模式 1
3 认证的基本过程 1
4 认证依据 1
5 对认证人员的基本要求 1
6 认证实施的基本要求 2
7 监督审核程序 11
8 再认证程序 13
9 认证证书及认证标志 14
10 与其他管理体系的结合审核 18
11 信息报告 18
12 受理组织的申诉 19
13 认证记录的管理 19
14 受理转换认证证书 19
15 记录的管理 19
16 其他 20
17 收费 20
附件 1 22

前　言

本实施规则根据《中华人民共和国认证认可条例》、《认证机构管理办法》，以及《国家认监委关于加强认证规则管理的公告》（2025 年第 9 号）制定。

本由北京五洲恒通认证有限公司制定、发布，版权归北京五洲恒通认证有限公司所有，任何组织及个人未经北京五洲恒通认证有限公司许可，不得以任何形式使用。

本规则由北京五洲恒通认证有限公司技术委员会提出并归口。

本规则主要起草人：滕宇龙　　刘益君　　马尧

本规则由北京五洲恒通认证有限公司 2025 年 07 月 01 日发布。

本规则自 2025 年 07 月 01 日起实施。

本规则由北京五洲恒通认证有限公司解释。

五洲恒通

五洲恒通

V0.00 2025.07

1 适用范围

本规则依据认证认可相关法律法规，对规范北京五洲恒通认证有限公司（以下简称“CHTC”）信息安全管理体系认证过程作出具体规定，明确了信息安全管理体系认证过程的相关责任，保证信息安全管理体系认证活动的规范有效。

本规则是本机构在开展信息安全管理体系认证活动中的基本要求，本规则同时适用于开展信息安全管理体系认证活动。

2 认证模式

文件审核+现场审核+获证后的监督

3 认证的基本过程

信息安全管理体系认证的主要过程包括：认证申请及受理+文件审核+现场审核+复核及认证评定+获证后监督。

4 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》

5 对认证人员的基本要求

5.1 认证审核员应当取得国家认监委确定的认证人员注册机构颁发的信息安全管理体系审核员注册资格。

5.2 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。

5.3 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。

5.4 认证人员不得是国家法律法规和国家政策禁止或者限制从事活动的人员。

6 认证实施的基本要求

6.1 初次认证程序

6.1.1 认证申请

6.1.1.1 CHTC 向申请组织至少公开以下信息：

（1）可开展认证业务的范围，以及获得认可的情况；
（2）本规则的完整内容；
（3）认证证书样式；
（4）对认证过程的申投诉规定。

申请组织可以通过 CHTC 网站或联系电话，下载或索取公开文件，了解信息安全管理体系认证的基本要求及相关信息。

6.1.1.2 认证申请组织应具备以下条件：

（1）取得国家市场监督管理部门或有关机构注册登记的法人资格（或其组成部分），新改扩建设项目符合法规规定的环境评价要求；
（2）适用时，取得相关法规规定的行政许可文件，其申请认证范围应在法律地位文件和资质规定的范围内；
（3）未列入国家信用信息严重失信主体相关名录；
（4）申请组织应按现行有效的认证依据标准建立和实施了文件化的信息安全管理体系，且有

效运行 3 个月以上；
（5）未在被执法监管部门责令停业整顿期间；
（6）近两年内未发生重大、特大环境事故（事件）。

6.1.1.3 认证申请组织应提交的文件和资料：

（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）法律地位的证明文件的复印件；
（3）信息安全管理体系覆盖的活动所涉及法律法规要求的行政许可证明、资质证书、强制性认证证书等的复印件；
(4)认证文件应包括适用性声明的版本；
(5)信息安全管理体系成文信息(适用时)。

6.1.2 认证受理评审

根据认证依据、程序等要求，及时对申请方提交的申请文件和资料进行审核并保存审核记录，以确保：

（1）认证要求规定明确、形成文件并得到理解；
（2）认证机构和申请方之间在理解上的差异得到解决；
（3）对于申请的认证范围、工作场所、员工人数、完成审核所需时间和其他影响认证活动的因素，认证机构均有能力开展认证服务。

申请组织应对提供的资料的真实性负责。

CHTC 根据相关要求对申请进行评审，必要时，要求申请组织补充信息。对不能受理的，CHTC 应发出不予受理的通知。

6.1.3 认证协议

对受理认证申请组织，在实施认证审核之前本机构将与认证申请组织签订具有法律效力的书面认证合同，以明确相关方的责任。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 CHTC 通报：

①客户及相关方有重大投诉；

②发生环境污染事故；

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；信息安全管理体系和重要过程的重大变更等；

④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）拟认证的信息安全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，CHTC 和申请组织各自应当承担的责任、权利和义务；

（7）认证服务的费用、付费方式及违约条款。

6.2 审核策划

6.2.1 审核时间

6.2.1.1 为确保认证审核的完整有效，CHTC 依据附件 1 所规定的审核时间为基础，但不应孤立的使用附件中所规定的时间，还应考虑与 ISMS 复杂程度和审核工作量相关的因素，根据申请组织信息安全管理体系覆盖的活动，核算并拟定完成审核工作需要的时间，在特殊情况下，可以减少审核时间，但减少的时间不得超过所规定的审核时间的 30%。

6.2.1.2 整个审核时间中，现场审核时间不应少于总审核时间的 80%。

6.2.2 本机构根据信息安全管理体系认证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，以保证审核组具有足够的技术领域审核能力。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。实习审核员不计入审核时间。

6.2.3 审核组

6.2.3.1 CHTC 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，且至少保证有一名具有专业技术领域的审核人员参加审核组。

6.2.3.2 实习审核员的职责是参加认证审核活动的学习，不作为审核员单独实施审核，不计入审核时间。

6.2.4 审核计划

6.2.4.1 审核组长为每次审核前应制定书面的审核计划。审核计划包括以下内容：

（1）审核目的

（2）审核准则

（3）审核范围

（4）现场审核的日期和场所

（5）审核组成员（其中：审核员应标明认证人员注册号；且应标明专业代码以示其技术领域）。

6.2.4.2 若审核覆盖范围覆盖多个场所，这些场在同一个信息安全管理体系下运行且该信息安全管理体系实行集中统一的管理、审核和管理评审，且这些场所都处于申请组织的授权和控制下，可以根据多现场组织审核抽样的有关要求，在审核中对这些场所进行抽样，抽样方法采用场所数量平方根法。

如果不同场所的管理活动的环境要素存在明显差异，则不能采用抽样审核的方法，应当逐一到各现场进行审核。

6.2.4.3 为使现场审核活动能够观察到相关过程的信息安全管理情况，现场审核将安排在认证范围覆盖的活动正常运行时进行。

6.2.4.4 在审核活动开始前，审核组长应将审核计划提交申请组织确认，遇特殊情况临时变更计划时，将通知申请组织有关变更情况，并协商一致。

6.3 实施审核

6.3.1 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。

6.3.2 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

信息安全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有效的身份证明文件。

6.3.3 审核员根据所分配的审核任务，通过索取/查阅受审核方有关文件和资料、借助通讯工具的沟通、与受审核方代表在其现场外的场所的面谈等方式，收集信息，必要时加以确认。

6.3.4 审核过程及环节

6.3.4.1 初次认证审核，分为第一、二阶段实施审核。

6.3.4.2 第一阶段审核应至少覆盖以下内容：

（1）结合现场情况，确认申请组织实际情况与信息安全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的产品和服务、部门设置和职责与权限、生产或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/IEC 27001:2022 标准要求的情况，评价信息安全管理体系运行过程中是否实施了内部审核与管理评审，确认信息安全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信息安全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）结合信息安全管理体系覆盖产品和服务的特点识别对信息安全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；

（5）与申请组织讨论确定第二阶段审核安排。对信息安全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。

6.3.4.3 在下列情况，第一阶段审核可以不在申请组织现场进行，但应记录未在现场进行的原因：

（1）申请组织已获我机构颁发的其他有效认证证书，我机构已对受审核组织信息安全管理体系有充分了解；

（2）我机构有充足的理由证明申请组织的生产经营或服务的技术特征明显、过程简单，通过对其提交文件化信息的审查可以达到第一阶段审核的目的和要求；

五洲恒通

（3）申请组织获得了其他经认可机构认可的认证机构颁发的有效的信息安全管理体系认证证书，通过对其文件和资料的审查可以达到第一阶段审核的目的和要求。

除以上情况之外，第一阶段审核应在受审核组织的生产经营或服务场所进行现场实施。

6.3.4.4 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。

6.3.4.5 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符合 ISO/IEC 27001:2022 和有效运行情况，应至少覆盖以下内容：

（1）申请组织信息安全管理体系与认证依据标准要求的符合情况及其证据；

（2）申请组织在相关职能和层次上建立了信息安全目标，信息安全目标是否具体适用、可测量并得到沟通、监视；

（3）对信息安全管理体系覆盖的过程和活动的管理及控制情况；

（4）在第一阶段审核中识别的重要审核点的过程控制的有效性；

（5）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；

（ 6）申请组织的内部审核和管理评审的有效性。

6.3.5 发生以下情况时，审核组应向机构报告，认证机构同意后终止审核。

（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。

6.4 审核报告

6.4.1 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）实施审核的过程以及偏离计划的情况，特别是对二阶段的各项审核要求应逐项就审核证据、审核发现和审核结论进行详细描述；

（7）对信息安全目标实现情况进行评价；

（8）识别出的不符合项；

（9）审核组对是否通过或保持认证的意见。

6.4.2 CHTC 在作出认证决定后 30 个工作日内将审核报告提交申请组织，申请组织请妥善保管审核报告、不符合报告及其纠正材料等相应材料。

6.4.3 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，CHTC 应将此报告及终止审核的原因提交给申请组织。

6.5 不符合项的纠正和纠正措施及其结果的验证

对审核中发现的不符合项，审核组将出具书面不符合报告。申请组织应进行原因分析，并提出纠正和纠正措施。如果在第二阶段结束后 6 个月内，不符合的纠正和纠正措施不能得到审核组或 CHTC 接受和验证，则审核组在推荐认证前要再实施一次第二阶段审核。

6.6 复核及认证决定

五洲恒通 CHTC

6.6.1 复核

6.6.1.1 检查审核过程中产生的所有信息（如记录、数据、报告等）及结果，确保其完整性和准确性。

6.6.1.2 验证审核过程，确保其符合 CHTC 的相关程序和相关标准要求。

6.6.2 认证决定

6.6.2.1 本机构在对审核报告、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，综合考虑其他来源获得的补充信息做出认证决定。

6.6.2.2 认证决定人员应为 CHTC 管理控制下的人员，审核组成员不得参与对审核项目的认证决定。

6.6.2.3 CHTC 在做出认证决定前应确认如下情形：

（1）审核报告符合本规则第 6.4 条要求，审核组提供的审核报告及其他信息能够满足做出认证决定所需要的信息；

（2）反映以下问题的不符合项，CHTC 已评审、接受并验证了纠正和纠正措施的有效性；

①在持续改进信息安全管理体系的有效性方面存在缺陷，实现信息安全目标有重大疑问；

②制定的信息安全目标不可测量、或测量方法不明确；

③对实现信息安全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）CHTC 对其他一般不符合项已评审，并接受了申请组织计划采取的纠正和纠正措施。

6.6.2.4 在满足 6.6.2.3 条要求的基础上，当有充分的客观证据证明申请组织满足下列要求的，可评定该申请组织符合信息安全管理体系认证要求，本机构向其颁发信息安全管理体系认证证书：

（1）申请组织的信息安全管理体系符合认证依据的要求且运行有效；

（2）认证范围覆盖的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。

6.6.2.5 当申请组织不能满足上述要求的，则评定该申请组织不符合信息安全管理体系认证要求，本机构将以书面形式告知申请组织并说明其未通过认证的原因。

（1）受审核方的信息安全管理体系有重大缺陷，不符合 ISO/IEC 27001:2022 标准的要求；

（2）发现受审核方存在重大质量、环境、安全问题或有其他与环境管理相关的严重违法违规行为。

6.6.3 CHTC 在颁发认证证书后，应当在 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。

7 监督审核程序

7.1 本机构将对持有本机构的信息安全管理体系获证组织进行跟踪，监督获证组织持续运行符合信息安全管理体系认证要求。

7.2 为确保达到 7.1 条要求，CHTC 应根据获证组织的信息安全管理体系安全风险程度或其他特性，确定对获证组织的监督审核的频次。

7.2.1 作为最低要求，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。

7.2.2 超过期限而未能实施监督审核的，应按 9.1 或 9.2 条处理。

7.3 监督审核的时间不少于初次审核人日数的 1/3。

7.4 监督审核的审核组，应符合 6.2.2 条和 6.3.1 条的要求。

7.5 监督审核应在获证组织现场进行，且应满足第 6.2.3.3 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产品和服务的，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和服务。审核时至少覆盖以下内容：

（1）上次审核以来信息安全管理体系覆盖的活动及影响体系的重要变更及运行体系的资源是否有变更；

（2）按 6.3.4.2（4）条要求已识别的重要关键点是否按信息安全管理体系的要求在正常和有效运行；

（3）对上次审核中确定的不符合项采取的纠正和纠正措施是否继续有效；

（4）信息安全管理体系覆盖的活动涉及法律法规规定的，是否持续符合相关规定；

（5）信息安全目标及环境绩效是否达到信息安全管理体系确定值。如果没有达到，获证组织是否运行内审机制识别了原因、是否运行管理评审机制确定并实施了改进措施；

（6）获证组织对认证标志的使用或对认证资格的引用是否符合《认证认可条例》及其他相关规定；

（7）内部审核和管理评审是否规范和有效；

（8）是否及时接受和处理投诉；

（9）针对体系运行中发现的问题或投诉，及时制定并实施了有效的改进措施。

7.6 对于监督审核中发现的不符合，获证组织应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。本机构将对获证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。

7.7 监督审核的审核报告按照 6.4 要求逐项描述或引用审核证据、审核发现和审核结论。本机构将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。

8 再认证程序

8.1 信息安全管理体系认证证书有效期满前，需要延续认证有效期的获证组织可向本机构提出再认证申请。

8.2 经申请评审后，CHTC 在前认证证书有效期满前安排再认证审核，按 6.2.2 条和 3.3.1 条要求组成审核组。按照 6.2.3 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。再认证程序与初次认证程序一致。在获证组织的信息安全管理体系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审核。

8.3 再认证审核的时间根据信息安全管理体系审核时间规定的相关要求进行确定，再认证审核时间不少于初次审核人日数的 2/3。

8.4 对于再认证审核中发现的不符合，获证组织应在规定时限内完成纠正和纠正措施，并在认证证书到期前获得 CHTC 对其所采取的纠正和纠正措施实施有效的验证。

8.5 本机构按照 6.6 的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。

8.6 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。

如果在当前认证证书终止日期前，认证机构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。

在当前认证证书到期后，如果认证机构能够在 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。

9 认证证书及认证标志

9.1 认证证书

9.1.1 信息安全管理体系认证证书有效期为 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。

9.1.2 信息安全管理体系认证证书至少包括以下内容：

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

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

（3）信息安全管理体系符合 ISO/IEC 27001:2022 标准的表述；

（4）证书编号；

（5）本机构名称、地址和认证标志；

（6）证书颁证日期、证书有效期的起止年月日；

证书注明：本证书的有效性依据本公司的定期监督结果获得保持，在一个监督周期后，本证书与年度《维持认证注册的通知》共用方为有效。

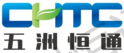
（7）相关的认可标识及认可注册号（适用时）；

（8）证书查询方式。CHTC 除公布认证证书在本机构网站上的查询方式外，还在证书上注明：“证书有效状态可以通过国家认证认可监督管理委员会官方网站 www.cnca.gov.cn 或 CHTC 网站查询”，以便于社会监督。

9.2 认证标识

9.2.1 准许使用的标志样式

获证组织可在广告、宣传品、信笺、名片、展销会或其他业务洽谈会场合等使用认证标识或认证证书，以宣传企业的管理体系认证状态，不得暗示该范围之外的业务也获得了认证。根据认证结果允许客户使用的认证标志如下所示，标志的制作和使用应符合 CHTC 的相关规定。



认证标志可等比例放大、缩小、变色使用，但不得变形。

9.2.2 获证组织不能利用管理体系认证标识和相关文字、符号，误导公众认为其产品、服务已通过认证。

9.2.3 当认证证书被暂停、注销或撤销认证时，应立即停止使用认证证书和带有认证标志的所有文件和宣传资料。

9.3 认证证书管理

对不符合认证要求的获证组织，CHTC 应对其认证证书进行处理，认证证书处理包含暂停、撤销和注销三种方式。

9.3.1 暂停认证证书

获证组织有下列情形之一，CHTC 应在调查核实后的 5 个工作日内暂停认证证书。

（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

五洲恒通

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）持有的与信息安全管理体系范围有关的行政许可证明、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；

（5）主动请求暂停的；

（6）其他应当暂停认证证书的情况。

暂停期限最长为6个月，但属于8.1第（4）项情形的暂停期可至相关单位作出许可决定之日。

CHTC应以适当方式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，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。

在暂停期间，获证组织的信息安全管理体系认证暂时无效。CHTC在获证组织完成对造成暂停的不符合的纠正和纠正措施进行确认后，恢复被暂停的认证。如果获证组织未能在CHTC规定的时限内完成对不符合的纠正和纠正措施，CHTC应撤销或缩小其认证范围。

9.3.2 撤销证书

获证方有以下情形之一的，CHTC在调查核实后的5个工作日内撤销其认证证书， 并予以公告。

（1）被注销或撤销法律地位证明文件的；

（2）被市场监管总局列入质量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，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）拒绝接受国家监督抽查的；

（5）出现重大的产品和服务等质量、环境、安全事故，经执法监管部门确认是获证组织违规造成的；

（6）有其他严重违反法律法规行为的；

（7）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（包括持有的与信息安全管理体系范围有关的行政许可证明、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）；

（8）没有运行信息安全管理体系或者已不具备运行条件的；

（9）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CHTC已要求其纠正但超过2 个月仍未纠正的；

（10）其他应当撤销认证证书的。

撤销认证证书后，获证组织应及时交回撤销的认证证书。若无法收回，CHTC应及时在相关媒体和网站上公布或声明撤销决定。

9.3.3 注销认证证书

客户有下列情况之一的，将注销其认证注册资格：

（1）由于认证依据和技术条件的变更，客户达不到新要求的；

（2）客户主动申请注销证书。

五洲恒通

9.3.4 恢复认证证书

当暂停原因得到消除后，CHTC 对暂停认证证书予以恢复。

9.3.5 认证证书状态信息公布

认证证书状态应在变更的 10 日内公布相关信息，同时按规定要求报国家认监委。

10 与其他管理体系的结合审核

10.1 对信息安全管理体系和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 6.4 条要求，并易于识别。

10.2 结合审核的审核时间人日数，不得少于多个单独体系所需审核时间之和的 80%。

11 信息报告

11.1 获证组织信息通报

为确保信息安全管理体系认证持续有效，获证组织应建立信息通报制度，及时向认证机构通报以下信息：

（1）有关组织机构变化的信息；
（2）消费者投诉的信息；
（3）有关质量、环境、安全等重大事故的信息；
（4）被有关执法监管部门责令停业整顿的信息；
（5）监督或行业主管部门抽查不合格的信息；
（6）受到行政部门相关处罚信息；
（7）其他违反法律法规行为的信息；
（8）顾客重大投诉；
（9）其他重要信息。

11.2 认证变更

当获证方名称、地址、产品、标准发生变更时，应及时向 CHTC 提交书面的变更申请，经机构评价和确定是否同意实施变更。

11.3 信息报送

CHTC 遵照国家认监委的相关要求报送认证信息。

12 受理组织的申诉

申请组织或获证组织对认证决定有异议时，应在认证决定后 30 日内提出，CHTC 接受其申诉并及时进行处理，在 60 日内将处理结果形成书面通知送交申诉人。认证决定 30 日后提出的申诉 CHTC 可不予受理。

13 认证记录的管理

13.1CHTC 应当建立认证记录保持制度，记录认证活动全过程并妥善保存。

13.2 记录应当真实准确以证实认证活动得到有效实施，归档留存的时间为认证证书有效期届满或者被注销、撤销之日起 2 年以上，认证记录应当使用中文。

14 受理转换认证证书

14.1 CHTC 应当履行社会责任，严禁以牟利为目的受理不符合 GB/T 24001/ISO 14001 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。

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

14.3 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。

五洲恒通

14.4 被发证的机构撤销证书的，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。

15 记录的管理

15.1 CHTC 应记录认证活动全过程并妥善保存。

15.2 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。

15.3 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。

15.4 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。

16 其他

16.1 本规则内容提及 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》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。

16.2 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。

16.3 CHTC 可开展信息安全管理体系及相关技术标准的宣贯培训，促使组织的全体员工正确理解和执行信息安全管理体系标准。

17 收费

17.1 收费标准

（1）申请费：1000.00 元

（2）年金：2000.00 元

（3）注册费：2000.00 元

（4）审核费：3000.00 元/人日

17.2 收费要求

初次评价：申请费+审核费+注册费

监督：年金+审核费

再认证：注册费+审核费

五洲恒通

附件 1

信息安全管理体系审核时间表

在组织控制下工作人员的数量	初次审核时间（天）
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
8501-10700	28
＞10700	延以上规律

注：

1. 上表给出了初次审核天数平均值的起点，这个数值包括初次审核(第一阶段和第二阶段)的天数)。对工作人员数量、及审核时间还应考虑信息安全管理体系复杂程度和审核工作量相关的因素，详细要求执行 CNAS-CC170:2024《信息安全管理体系认证机构要求》
2. 监督审核时间大约是初审时间的 1/3，再认真审核时间大约是初次审核时间的 2/3。