



体系认证实施规则

MSCI090232-2025

版本号：A1

信息安全管理体系统认证实施规则

Certification Rules for Information Security Management
System

2025 年 06 月 05 日发布

2025 年 06 月 05 日实施

广东质检中诚认证有限公司



目 录

1. 目的和范围	1
2. 认证人员要求	1
3. 认证依据	1
4. 初次认证程序	1
5. 监督审核程序	7
6. 再认证程序	8
7. 暂停、撤销、注销、恢复认证证书	9
8. 认证证书要求	10
9. 受理组织的申诉	11
10. 与其他管理体系的结合审核	11
11. 认证记录的管理	11
12. 其他	11
附录 A 信息安全管理体系认证的业务范围分类与分级	12



前言

本文件由广东质检中诚认证有限公司（以下简称 CTC）制定、发布，版权归 CTC 所有。任何组织及个人未经 CTC 许可，不得以任何形式全部或部分转载、使用本文件。

本文件持续修订，如需要获取最新版本，请登录 CTC 网站（www.qtcctc.org）获取，或联系 CTC 电话（020-89232208）获取。

如对本文件的获取、内容、使用有疑问，可联系 CTC 相关认证工程师。

本文件于 2025 年 6 月 5 日首次发布。

本文件修订记录：

版本	修订时间	主要修订内容
A0	2025 年 6 月 5 日	首次发布
A1	2025 年 8 月 25 日	1. 增加版本号； 2. 增加前言； 3. 修改封面、页眉、页脚； 4. 在 4.2.3.2 条款中增加多场所的抽样要求； 5. 在 4.3.3.3 条款第（3）部分增加一阶段非现场的条件； 6. 增加证书注销和恢复要求。



1. 目的和范围

1.1 本规则用于规范广东质检中诚认证有限公司（以下简称中诚认证）对申请认证和获证的各类组织按照信息安全管理体系标准建立信息安全管理体系的认证管理活动。

1.2 本规则是对中诚认证从事信息安全管理体系认证活动的基本要求，从事该项认证活动的人员应当遵守本规则。

2. 认证人员要求

2.1 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。

2.2 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。

3. 认证依据

3.1 GB/T 22080-2016/ISO/IEC27001:2013 《信息技术 安全技术 信息安全管理体系 要求》。

3.2 ISO/IEC 27001:2022 《Information security, cybersecurity and privacy protection - Information security management systems - Requirements》（信息安全 网络安全和隐私保护 信息安全管理体系 要求）。

3.3 GB/T 22080-2025/ISO/IEC27001:2022 《网络安全技术 信息安全管理体系 要求》。

注：以上认证依据为不同版本，结合实际需求选取其中一个标准开展认证活动。

4. 初次认证程序

4.1 受理认证申请

4.1.1 中诚认证需通过网站或文件向申请认证的组织（以下简称“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) 对认证过程的申诉程序；

4.1.2 中诚认证将要求申请组织至少提交以下资料：

- (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（包括组织营业执照、事业单位法人证书、社会团体登记证书、非组织法人登记证书、党政机关设立文件等的复印件）；
- (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) 若管理体系覆盖多场所活动，附各场所法律地位证明文件和（或）关系证明的复印件（适用时）；
- (5) 本组织信息安全管理体系建立及实施情况，包括管理手册等成文信息；
- (6) 管理体系已有效运行三个月以上的证明材料。

4.1.3 认证申请的评审

4.1.3.1 中诚认证应对申请组织提交的申请资料进行评审，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。

4.1.3.2 根据申请组织申请的认证范围、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国家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，不受理其认证申请。

4.1.3.3 中诚认证将完整保存认证申请评审的工作记录。

4.1.4 对符合 4.1.3 要求的，中诚认证可决定受理认证申请；对不符合上述要求的，中诚认证将通知申请组织补充和完善，或者不受理认证申请。

4.1.5 签订认证合同

在实施认证审核前，应与申请组织订立具有法律效力的书面认证合同。注：已签订认证合同的申请组织也称为客户。



4.2 审核策划

4.2.1 审核时间

4.2.1.1 为确保认证审核的完整有效，中诚认证根据申请组织信息安全管理体系覆盖的活动范围、信息安全背景和风险、组织规模等情况，核算并拟定完成审核工作需要的时间。具体执行《审核时间管理程序》。

4.2.1.2 整个审核时间中，现场审核时间不应少于 80%。

4.2.2 审核组

4.2.2.1 中诚认证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和技术专家组成审核组。审核组中的审核员应承担审核责任。

4.2.2.2 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。

4.2.2.3 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。

4.2.3 审核计划

4.2.3.1 中诚认证应制定书面的审核计划交审核组实施。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。

4.2.3.2 通常情况下，初次认证审核、监督审核和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。如果信息安全管理体系覆盖范围包括在多个场所进行相同或相近的活动，且这些场所都处于申请组织授权和控制下，可以在审核中对这些场所进行抽样，但应根据相关要求实施抽样以确保对所抽样本进行的审核对信息安全管理体系包含的所有场所具有代表性。如果不同场所的活动存在明显差异，或不同场所间存在可能对信息安全管理有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。多场所抽样规则参照《管理体系多场所认证审核管理规定》的有关要求。

4.2.3.3 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。

4.2.3.4 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。

4.3 实施审核



4.3.1 审核组应当全员完成审核计划的全部工作。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。

4.3.2 审核组应当会同申请组织按照程序顺序召开首、末次会议。审核组应当提供首、末次会议签到表。

4.3.3 审核过程及环节

4.3.3.1 初次认证审核，分为第一、二阶段实施审核。

4.3.3.2 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文件描述的一致性，特别是体系文件中描述的产品或服务、部门设置和负责人、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，审核申请组织有关人员理解和实施信息安全管理体系标准要求的情况，审核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有效运行。
- (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、申请组织的员工人数、活动过程和场所，遵守相关法律法规及技术标准的情况。
- (4) 结合信息安全管理体系覆盖活动的特点识别对信息安全管理体系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。不具备二阶段审核条件的，不应实施二阶段审核。

4.3.3.3 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) 申请组织已获中诚认证颁发的其他认证证书，中诚认证已对申请组织信息安全管理体系有充分了解。
- (2) 中诚认证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，通过对其提交文件和资料的审查可以达到第一阶段审核的目的和要求。
- (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质量管理体系认证证书，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，第一阶段审核应在申请组织的生产经营或服务现场进行。

4.3.3.4 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。

4.3.3.5 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，间隔时间至少为 0.5 天。

4.3.3.6 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标准要求 and 有效运行情况，应至少覆盖以下内容：

- (1) 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。
- (2) 为实现方针而在相关职能、层次和过程上建立目标是否具体适用、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) 申请组织实际工作记录是否真实。
- (5) 申请组织的内部审核和管理评审是否有效。

4.3.4 发生以下情况时，审核组应终止审核，并向中诚认证报告。

- (1) 申请组织对审核活动不予配合，审核活动无法进行。
- (2) 申请组织信息安全管理体系有重大缺陷，不符合标准的要求。
- (3) 发现申请组织存在重大问题或有其他严重违法违规行为。
- (4) 其他导致审核程序无法完成的情况。

4.4 审核报告

4.4.1 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) 审核的申请组织活动范围和场所。
- (3) 审核组组长、审核组成员。
- (4) 审核活动的实施日期和地点。
- (5) 叙述各项要求及管理体的审核工作情况，应逐项就审核证据、审核发现和审核结论进行详细描述；



(6) 识别出的不符合项。不符合项的表述，应基于客观证据和审核依据，用写实的方法准确、具体、清晰描述，易于被申请组织理解。不得用概念化的、不确定的、含糊的语言表述不符合项。

(7) 审核组对是否通过认证的意见建议。

4.4.2 审核报告应随附必要的用于证明相关事实的证据或记录，包括文字或照片摄像等音像资料。

4.4.3 中诚认证需将最终审核报告提交申请组织，并保留签收或提交的证据。

4.4.4 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，中诚认证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。

4.5 不符合项的纠正和纠正措施及其结果的验证

4.5.1 对审核中发现的不符合项，中诚认证将要求申请组织分析原因，并要求申请组织在规定的期限内采取措施进行改进。

4.5.2 中诚认证将对申请组织所采取的纠正、原因分析和纠正措施及其结果的有效性进行验证。

4.6 认证决定

4.6.1 中诚认证指定具备相应专业能力且未参与审核的一个或一组人员,对审核档案进行复核，并在对审核报告、不符合项的纠正和纠正措施及其结果进行综合审查基础上，作出认证决定。

4.6.2 审核组成员不得参与对审核项目的认证决定。

4.6.3 中诚认证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 4.4 条要求，能够满足作出认证决定所需要的信息。
- (2) 审核组已对所有不符合事项评审、接受并验证了纠正、原因分析和纠正措施及其结果的有效性。

4.6.4 在满足 4.6.3 条要求的基础上，中诚认证有充分的客观证据证明申请组织满足下列要求的，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 信息安全管理体系 符合标准要求且运行有效。
- (2) 认证范围覆盖的产品或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。

4.6.5 申请组织不能满足上述要求的，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。

4.6.6 中诚认证在颁发认证证书后，将按照规定的要求将相关信息报送国家认监委。

4.6.7 中诚认证不得将申请组织是否获得认证与参与认证审核的审核员及其他人员的薪酬挂钩。

4.6.8 中诚认证在网站（www.qtctc.org）开设专栏向社会公开各中诚认证上报的认证证书等信息。

5. 监督审核程序

5.1 中诚认证应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，监督获证组织通过认证的信息安全管理体系持续符合要求。为确保达到要求，中诚认证应根据获证组织的产品或服务风险程度或其他特性，确定对获证组织的监督审核的频次。

5.1.1 为了对获证组织在认证周期内持续满足要求保持信任，公司将每年至少对其进行一次监督审核，监督审核方案从初审（再认证）完成后即开始策划，初次认证后的第一次监督审核应在认证决定起 12 个月内进行。两次监督审核的间隔时间一般不能大于 12 个月，特殊情况下初审后第 2 次或再认证后的监督客户可以向 CTC 提交书面申请要求推迟审核，审核管理部应对该申请进行审批（延长期最长不能超过 3 个月），并将审批结果及时通知被审核方。

5.1.2 超过期限而未能实施监督审核的，应按 7.1 或 7.2 条处理。

5.2 年度监督审核的时间，为按 4.2.1 条计算初次审核人日数的 1/3，可适当调整。但整个认证周期内监督审核总时间不得低于按 4.5.1 条计算初次审核人日数的 2/3。

5.3 监督审核的审核组，应符合 4.5.2 条的要求。

5.4 监督审核应在获证组织现场进行。由于产品生产季节性原因，在每次监督审核时难以覆盖所有产品的，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。

5.5 监督审核时至少应审核以下内容：

(1) 上次审核以来信息安全管理体系覆盖的活动及运行体系的资源是否有变更；



- (2) 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;
- (3) 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;
- (4) 目标及各层级社会责任目标是否实现; 目标没有实现的, 获证组织在内部管理评审时是否及时调查并采取了改进措施;
- (5) 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相关的规定;
- (6) 内部审核和管理评审是否规范和有效;
- (7) 是否及时接受和处理投诉;
- (8) 针对内审发现的问题或投诉的问题, 及时制定并实施了有效的持续改进。

5.6 监督审核的审核报告, 应按 4.4 条列明的审核要求描述审核证据、审核发现和审核结论。审核组应提出是否继续保持认证证书的意见建议。

5.7 中诚认证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. 再认证程序

6.1 认证证书期满前 90 天内, 若获证组织申请继续持有认证证书, 中诚认证应当实施再认证审核决定是否延续认证证书。

6.2 中诚认证应按 4.2.2 条要求组成审核组。按照 4.2.3 条要求并结合历次监督审核情况, 制定再认证计划并交审核组实施。审核组按照要求开展再认证审核。在信息安全管理体系及获证组织的内部和外部信息安全无重大变更时, 再认证审核可省略第一阶段审核, 但审核时间应不少于按 4.2.1 条计算人日数的 2/3。

6.3 中诚认证参照 4.6 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。



7. 暂停、撤销、注销、恢复认证证书

7.1 暂停证书

7.1.1 获证组织有以下情形之一的，经调查核实，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) 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) 主动请求暂停的。
- (6) 其他应当暂停认证证书的。

7.1.2 认证证书暂停期不得超过 6 个月。在暂停期间客户不能使用认证证书进行广告和宣传活动。

7.2 证书的撤销

7.2.1 获证组织有以下情形之一的，中诚认证将在获得相关信息并调查核实后撤销其认证证书。

- (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，或者对有关事项的询问和调查提供了虚假材料或信息的。
- (3) 出现重大的负面事件和事故，经执法监管部门确认或经中诚认证调查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，或者中诚认证已要求其纠正但超过 2 个月仍未纠正的。



(8) 其他应当撤销认证证书的。

7.3 认证证书的注销

获证组织有下列情况之一时，将注销认证注册资格：

- (1) 获证组织申请注销认证证书的；
- (2) 认证证书有效期届满，未申请延续使用的；
- (3) 因换发新证书而注销旧证书的；
- (4) 其他原因需要注销认证证书的。

7.4 认证证书的恢复

暂停期间，受审核方如需恢复认证应在规定的暂停期限内，向中诚认证机构提出恢复申请，在证书暂停期内应就暂停原因进行有针对性地整改，验证通过后，方可恢复认证证书。

7.5 撤销认证证书后，中诚认证通知获证组织返还被撤销的证书及认证标志，不得继续使用证书及认证标志；并在中诚认证网站上公布或声明撤销决定。

7.6 中诚认证暂停或撤销认证证书信息在中诚认证网站上公布，同时将按规定程序和要求报国家认监委。

7.7 关于认证证书的变更，按《授予、拒绝、保持、更新、扩大、缩小、暂停、恢复、撤销和注销认证管理程序》实施。

8. 认证证书要求

8.1 认证证书应至少包含以下信息：

- (1) 获证组织名称、地址和统一社会信用代码；
- (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，应表述覆盖的相关场所的名称和地址信息；
- (3) 信息安全管理体系符合相关标准的表述；
- (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。

8.2 初次认证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。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认证证书，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。

8.3 证书信息按要求上报认证监管部门；此外，还可通过电话查询或书面向中诚认证查询。

8.4 认证证书变更后，应回收或者销毁旧证书。

8.5 认证证书及认证标志要求，按《认可标识、认证证书和标志使用的管理程序》执行。

9. 受理组织的申诉

获证组织对认证决定有异议时，中诚认证应接受获证组织申诉并且及时进行处理，在 60 个日历日内将处理结果形成书面通知送交获证组织。

10. 与其他管理体系的结合审核

10.1 对信息安全管理体系统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. 认证记录的管理

11.1 证明认证活动全过程满足相关法规、认可规则等适用要求的证据应予以保持并妥善保存。

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

11.3 记录可以用纸质或电子文档的方式加以保存。

12. 其他

本规则内容提及标准时均指认证活动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，均应采用当时有效版本的完整标准号。



附录 A

信息安全管理体系认证的业务范围分类与分级

大类	中类	级别	描述	备注
01	政务			
	01.01	一	国家机构	包括人大、政府、法院、检察院等，不含税务机关和海关
	01.02	一	税务机关	
	01.03	一	海关	
	01.04	二	其他	例如政党，政协，社会团体等
02	公共			
	02.01	一	通信、广播电视	
	02.02	一	新闻出版	包括互联网内容的提供
	02.03	二	科研	涉及特别重大项目的应提升为一级
	02.04	二	社会保障	例如社会保险基金管理、慈善团体等。包括医疗保险
	02.05	二	医疗服务	
	02.06	三	教育	
	02.07	三	其他	例如市政公用事业（水的生产和供应、污水处理、燃气生产和供应、热力生产和供应、城市水陆交通设施的维护管理等）
03	商务			
	03.01	一	金融	例如银行、证券、期货、保险、资产管理等
	03.02	一	电子商务	以在线交易为主要特点，含网络游戏
	03.03	一	物流	包括邮政
	03.04	三	咨询中介	例如法律、会计、审计、公证等
	03.05	三	旅游、宾馆、饭店	
	03.06	三	其他	
04	产品的生产			产品包括软件、硬件、流程性材料和服务
	04.01	一	电力	包括发电和输、变、配电等
	04.02	一	铁路	
	04.03	一	民航	
	04.04	一	化工	
	04.05	一	航空航天	



大类	中类	级别	描述	备注
	04.06	一	水利	
	04.07	二	交通运输	包括公路、水路、城市公共客运交通等，不含航空和铁路
	04.08	二	信息与通信技术	例如软、硬件生产及其服务，系统集成及其服务，数字版权保护等
	04.09	二	冶金	
	04.10	二	采矿	含石油、天然气开采
	04.11	二	食品、药品、烟草	
	04.12	三	农、林、牧、副、渔业	
	04.13	三	其他	