



卓耀认证中心有限公司
ZHUOYAO CERTIFICATION CENTER CO., LTD.

本规则通过公司官网(www.zhuoyaorz.com)公开



隐私信息管理体系认证实施规则

文件编号：ZYCC-ZY-YSXX-001

版 次：A1

编 制：审核部

审 核：郭敬肖

批 准：杨超杰

2026 年 06 月 03 日发布

2026 年 06 月 03 日实施

卓耀认证中心有限公司



1 适用范围

1.1 本规则用于规范依据隐私信息管理体系认证实施规则进行的认证活动。

1.2 本规则依据认证认可相关法律法规，结合相关技术标准，对隐私信息管理体系认证实施过程作出具体规定，明确中心对隐私信息管理体系认证过程的管理责任，保证隐私信息管理体系认证活动的规范有效。

1.3 本规则是中心在隐私信息管理体系认证活动中的基本要求，隐私信息管理体系认证活动中应当遵守本规则。

2 认证依据

ISO /IEC 27701:2019《安全技术 — 隐私信息管理体系》

3 对认证审核人员的基本要求

3.1 认证审核员应当取得 CCAA 管理体系审核员注册资格及中心组织的隐私信息管理体系认证规则的相关培训。

3.2 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。

4 初次认证程序

4.1 受理认证申请

4.1.1 中心应当要求申请组织至少提交以下资料：

- (1) 取得合法主体资格，并处于有效期内；
- (2) 取得相关法律法规规定的行政许可（适用时），并处于有效期内；
- (3) 已按认证依据标准建立隐私信息管理体系，且运行满三个月
- (4) 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。
- (5) 法律地位的证明文件的复印件。若体系覆盖多场所活动，应附每个场所的法律地位证明文件的复印件（适用时）。



(6) 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。

(7) 体系成文信息(适用时)。

4.1.2 中心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, 中心不应受理其认证申请。

4.1.3 对符合 4.1.1、4.1.2 要求的, 中心可决定受理认证申请; 对不符合上述要求的, 中心应通知申请组织补充和完善, 或者不受理认证申请。

4.1.4 签订认证合同

在实施认证审核前, 中心应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体系发生重大变更时, 应及时向中心通报;

(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, 中心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。认证服务的费用、付费方式及违约条款。认证费用应由认证委托人向本中心直接支付。

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, 中心应以附录 A 所规定的审核时间为基础, 根据申请组织体系覆盖的活动范围、特性、技术复杂程度、风险程度、认证要求和体系覆盖范围内的有效人数等情况, 核算并拟定完成审核工作需要的时间。



4.2.2 审核组

4.2.2.1 中心应当根据体系覆盖的活动的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。

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。

4.2.2.4 审核组应至少有 1 名本中心的专职审核员，并确保该专职审核员全程参与管理体系审核过程。

4.2.3 审核计划

4.2.3.1 中心应为每次审核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）。

4.2.3.2 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。

4.2.3.3 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。

4.3 实施审核

4.3.1 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。

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，认证委托人的最高管理者及与体系相关的职能部门负责人员应参加首、末次会议，本中心应保留首、末次会议签到记录、图片/音像证明材料。认证委托人的最高管理者不能参加首、末次会议的，应由获得书面授权的其他高级管理层成员参会，审核组应记录最高管理者缺席理由。申请组织的最高管理者应当接受审核组关于管理体系职责履行情况的访谈。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。



4.3.3 审核过程及环节

4.3.3.1 隐私信息管理体系认证的初次认证审核一般分为一、二两个阶段实施。

4.3.3.2 第一阶段审核侧重于体系的策划情况，包括文审和现场审核；一阶段审核是“准备性”审核，属非完整审核，只涉及一阶段审核相关的部门和人员，主要审核管理体系的策划部分。一阶段审核目的一是为了确定受审方管理体系是否已按认证依据标准建立并运行；二是为了第二阶段审核的实施进行准备。第二阶段侧重于体系的运行实施情况的审核，包括有效性，涉及全部门和全要素。二阶段审核是完整审核，涉及受审方管理体系覆盖范围内所有部门和所有人员，第二阶段审核是为了确认受审方管理体系是否符合认证依据标准的要求并有效运行，作出是否推荐认证注册的审核结论。一二阶段审核需在现场进行，一二阶段审核人日之和应不小于现场审核总人日，且第二阶段审核人日数通常不小于现场审核总人日的 70%。一二阶段审核时间间隔最短不应少于 5 日，最长不应超过 6 个月。如需要更长的时间间隔，应重新实施第一阶段审核。

4.3.3.3 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) 申请组织已获本认证机构颁发的其他有效认证证书，认证机构已对申请组织管理体系有充分了解。

(2) 认证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，通过对其提交文件和资料的审查可以达到第一阶段审核的目的和要求。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方的生产经营或服务现场进行。

4.3.3.4 二阶段审核

审核应当在申请组织现场进行。重点是审核体系符合标准要求和有效运行情况，应至少覆盖以下内容：

(1) 重要审核点的过程控制的有效性。

(2) 为实现管理体系方针而在相关职能、层次和过程上建立管理体系目标是否具体适用、可测量并得到沟通、监视。



(3) 对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。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。

4.3.4 发生以下情况时，审核组应向中心报告，经中心同意后终止审核。

(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。

(4) 认证委托人的最高管理者或经授权的高级管理层成员缺席首、末次会议。

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) 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，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 4.3 条列明的程序及各项要求的审核工作情况，其中：对 4.3.3.1 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。

4.4.2 中心应保留用于证实审核报告中相关信息的证据。

4.4.3 中心应在作出认证决定后 30 个工作日内将审核报告提交申请组织，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，中心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。

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，中心应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，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。中心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 4.6.5 条处理，或者按照 4.3.3.1 条重新实施审核。

4.6 认证决定

4.6.1 中心应该在对审核报告、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，作出认证决定。

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

4.6.3 中心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，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) 所有不符合项中心已评审、接受并验证了纠正和纠正措施的有效性。

4.6.4 在满足 4.6.3 条要求的基础上，中心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) 申请组织的体系符合标准要求且运行有效。

(2) 认证范围覆盖的项目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。

4.6.5 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) 受审核方的体系有重大缺陷，不符合标准的要求。

(2) 发现受审核方存在重大问题或有其他与产品和服务严重违法违规行为。

4.6.6 中心在颁发认证证书后，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。

5 监督审核程序

5.1 中心应对持有其颁发的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体系并符合认证要求。



5.2 为确保达到 5.1 条要求,中心应根据获证组织的产品和服务的风险程度或其他特性,确定对获证组织的监督审核的频次。初次认证及再认证后的第一次监督审核应在认证证书签发之日起 12 个月内进行(再认证年份除外)。

5.2.1 作为最低要求,监督审核应至少每个日历年进行一次,且两次监督审核的时间间隔不得超过 12 个月。

5.2.2 超过期限而未能实施监督审核的,应按 6.2 或 6.3 条处理。

5.2.3 获证企业的项目和服务被查出不合格时,自主管部门发出通报起 30 日内,中心应对该企业实施监督审核。

5.3 监督审核的审核组,应符合 6.2.2 条和 6.3.1 条的要求。

5.4 监督审核应在获证组织现场进行,且应满足第 4.2.3.3 条确定的条件。

5.5 监督审核时至少应审核以下内容:

(1) 上次审核以来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) 是否按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) 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) 管理体系目标及绩效是否达到体系确定值。

(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) 是否及时接受和处理投诉。

(8) 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。

5.6 在监督审核中发现的不符合项,中心应要求获证组织分析原因,规定时限要求获证组织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。

中心应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。

5.7 监督审核的审核报告,应按 4.6 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。

5.8 中心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 暂停或撤销认证证书

6.1 中心应制定暂停、撤销认证证书或缩小认证范围的规定和文件化的管理制度，规定和管理制度应满足本规则相关要求。中心对认证证书的暂停和撤销处理应符合其管理制度，不得随意暂停或撤销认证证书。

6.2 暂停证书

6.2.1 获证组织有以下情形之一的，中心应在调查核实后的 5 个工作日内暂停其认证证书。

- (1) 体系持续或严重不满足认证要求，包括对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) 持有的与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。

6.2.2 认证证书暂停期不得超过 6 个月。但属于 6.2.1 第（4）项情形的暂停期可至相关单位作出许可决定之日。

6.2.3 中心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，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。

6.3 撤销证书

6.3.1 获证组织有以下情形之一的，中心应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，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) 有其他严重违法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,或者中心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。

6.3.2 撤销认证证书后,中心应及时收回撤销的认证证书。若无法收回,中心应及时在相关媒体和网站上公布或声明撤销决定。

6.4 中心暂停或撤销认证证书应当在其网站上公布相关信息,同时按规定程序和要求报国家认监委。

6.5 中心应采取有效措施避免各类无效的认证证书和认证标志被继续使用。

6.6 证书暂停期间,认证委托人如果需要恢复认证证书,应在规定的暂停期限内向中心提出恢复申请,中心按有关规定进行恢复处理。否则,暂停期满后中心将撤销被暂停的认证证书。

7 认证证书要求

7.1 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(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) 体系覆盖的经营或服务的地址和业务范围。

(3) 体系符合标准的表述。

(4) 证书编号。

(5) 中心名称。

(6) 有效期的起止年月日。证书应注明:获证组织必须定期接受监督审核并经审核合格此证书方继续有效的提示信息。

(7) 相关的认可标识及认可注册号(适用时)。

(8) 证书查询方式。中心除公布认证证书在本机构网站上的查询方式外,还应当在证书上注明:“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)上查询”,以便于社会监督。



7.2 初次认证证书有效期最长为 3 年。

7.3 中心应当建立证书信息披露制度。除向申请组织、认证监管部门等执法监管部门提供认证证书信息外，还应当根据社会相关方的请求向其提供证书信息，接受社会监督。

8 与其他管理体系的结合审核

8.1 对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 5.4 条要求，并易于识别。

9 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，中心应接受申诉并且及时进行处理，在 60 日内将处理结果形成书面通知送交申诉人。

书面通知应当告知申诉人，若认为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。

10 认证记录的管理

10.1 中心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。

10.2 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。

10.3 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。

10.4 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。

11 认证标志

11.1 通过认证并取得认证证书的企业可在获准认证的产品本体、铭牌、包装、随附文件（如说明书、合格证等）、操作系统、电子销售平台等位置使用或展示标识，样式见下图。





附录 A

审核时间要求

有效人数	审核时间 第 1 阶段+第2 阶段 (人天)	有效人数	审核时间 第 1 阶段+第2 阶段 (人天)
1-5	1.5	626-875	12
6-10	2	876-1175	13
11-15	2.5	1176-1550	14
16-25	3	1551-2025	15
26-45	4	2026-2675	16
46-65	5	2676-3450	17
66-85	6	3451-4350	18
86-125	7	4351-5450	19
126-175	8	5451-6800	20
176-275	9	6801-8500	21
276-425	10	8501-10700	22
426-625	11	>10700	遵循上述递进规律

注：1.有效人数包括认证范围内涉及的所有人员（含每个班次的人员）。覆盖于认证范围内的非固定人员（如：承包商人员）和兼职人员也应包括在有效人数内。

2.对非固定人员（包括季节性人员、临时人员和分包商人员）和兼职人员的有效人数核定，可根据其实际工作小时数予以适当减少或换算成等效的全职人员数。

3.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。