	文件编号：ZFC-RZGZ-116
	发行版本：A/0
	实施日期：2025.10.30

山东中梓富检认证有限公司

隐私管理体系认证规则

编　　制：

审　　核：

批　　准：

ZFC-RZGZ-116隐私管理体系认证规则

目录

1 适用范围

1.1 本规则用于规范本机构对申请认证和获证的各类组织按照 ISO/IEC 27701:2025《信息安全，网路安全和隐私保护，隐私信息管理体系 要求和指南》进行隐私管理体系的认证活动。

1.2 本规则旨在结合认证认可相关法律法规及国家《质量发展纲要（2011-2020 年）》和技术标准，对隐私管理体系认证实施过程作出具体规定，强化本机构对认证过程的管理和责任。

1.3 本规则是对本机构从事隐私管理体系认证活动的基本要求，本机构从事该项认证活动应当遵守本规则。

2 对本机构的要求

2.1 获得国家认监委批准、取得从事管理体系认证的备案资质。

2.2 建立可满足 GB/T 27021《合格评定 管理体系审核认证机构要求》的内部管理体系，以使从事的隐私管理体系认证活动符合法律法规及技术标准的规定。

2.3 建立内部制约、监督和责任机制，实现受理、培训（包括相关增值服务）、审核和做出认证决定等环节的相互分开。

3 对本机构认证人员的要求

认证人员应当满足对学历、工作年限等要求，通过本机构内部培训并考核合格，取得本机构授权或委任。认证人员应当遵守与从业相关的法律法规，对认证活动及作出的认证审核报告和认证结论的真实性承担相应的法律责任。

3.1 认证人资格经历要求

3.1.1 教育经历：应符合下列高等教育经历要求：大学专科（含） 以上学历。

3.1.2 工作经历：应符合下列工作经历要求：大学本科（含）以上学历审核员申请人应具有至少 4 年全职工作经历，大专学历申请人应具有至少 6 年全职工作经历。

3.1.3 培训经历：应接受本机构通用和专业课程培训，并通过书面考核。

3.2 审核员和审核原则要求

3.2.1 审核员应具备下列要求:

----有道德，即公正、可靠、忠诚、诚信和谨慎；

----思想开明，即愿意考虑不同意见或观点；

----善于交往，即灵活地与人交往；

----善于观察，即主动地认识周围环境和活动；

----有感知力，即能了解和理解环境；

----适应力强，即容易适应不同处境；

----坚定不移，即对实现目标坚持不懈；

----明断，即能够根据逻辑推理和分析及时得出结论；

----自立，即能够在同其他人有效交往中独立工作并发挥作用；

----坚忍不拔，即能够采取负责任的及合理的行动，即使这些行动可能是非常规的和有时可能导致分歧和冲突；

----与时俱进，即愿意学习，并力争获得更好的审核结果；

----文化敏感，即善于观察和尊重受审核方的文化；

----协同力，即有效地与其他人互动，包括审核组成员和受审核方人员；

----健康，即身体健康状况良好。

3.2.2 审核员应按照下列原则进行工作:

----诚实正直：职业的基础

对审核而言，诚信、正直、保守秘密和谨慎应是最基本的。

----公正表达：真实、准确地报告的义务

审核发现、审核结论和审核报告应真实和准确地反映审核活动。报告在审核过程中遇到的重大障碍以及在审核组和受审核方之间没有解决的分歧意见。

----职业素养：在审核中勤奋并具有判断力

审核员应珍视他们所执行的任务的重要性以及审核委托方和其它相关方对自己的信任。具有必要的能力是一个重要的因素。

----保密性：信息安全

审核员应审慎使用和保护在审核过程中获得的信息。

----独立性：审核的公正性和审核结论的客观性的基础

审核员应独立于受审核的活动，并且不带偏见，没有利益上的冲突。审核员在审核过程中应保持客观的心态，以保证审核发现和结论仅建立在审核证据的基础上。

----基于证据的方法：在一个系统的审核过程中，得出可信的和可重现的审核结论的合理方法审核证据应是可证实的。由于审核是在有限的时间内并在有限的资源条件下进行的，因此审核证据是建立在可获得的信息样本的基础上。抽样的合理性与审核结论的可信性密切相关。

3.3 审核员行为规范要求

审核员均应遵守 CCAA 检查员行为规范。所有申请人均应签署声明，承诺遵守行为规范：

----遵纪守法、敬业诚信、客观公正；

----努力提高个人的专业能力和声誉；

----帮助所管理的人员拓展其专业能力；

----不承担本人不能胜任的任务；

----不介入冲突或利益竞争，不向任何委托方或聘用机构隐瞒任何可能影响公正判断的关系；

----不讨论或透露任何与工作任务相关的信息，除非应法律要求或得到委托方和聘用单位的书面授权；

----不接受受审核方及其员工或任何利益相关方的任何贿赂、佣金、礼物或任何其它利益，也不应在知情时允许同事接受；

----不有意传播可能损害审核工作或人员注册过程的信誉的虚假或误导性信息；

----不以任何方式损害 CCAA 及其人员注册过程的声誉，与针对违背本准则的行为而进行的调查进行充分的合作；

----不向受审核方提供相关咨询。

3.4 投诉

本机构依据认监委《申诉、投诉和争议处理程序规则》，处理针对审核员违反行为规范的行为的投诉。

3.5 认证机构认证人员管理要求

3.5.1 认证机构应建立相应认证人员管理制度并有效实施。

3.5.2 认证人员管理制度文件至少应包括：

a)认证人员能力评价系统的建立与实施；

b)认证人员现场见证活动的要求和实施；

c)见证评价人员和申请信息、资料核实人员的评价、选择、培训与指定；

d)专业能力评定人员及审核员专业能力评定要求（适用时）；

e)认证人员培训管理与实施等。

3.5.3 认证机构应对申请人资格经历的真实性进行核实，并对申请人个人素质、知识和技能是否符合本准则注册要求进行审核，做出备案决定。

3.6 资格处置

3.6.1 认证机构应对申请人申报的有关资格经历的信息、资料的完整性和真实性进行核实。若申请人隐瞒虚假信息或提供误导性信息，造成严重后果的，将按照《注册人员资格处置规则》给予警告、暂停备案资格，直至撤销备案资格的处置。

3.6.2 对违反行为规范、不满足注册准则要求的各级别审核员，经调查核实，认证机构将按照《注册人员资格处置规则》给予警告、暂停备案资格，直至撤销备案资格的处置。

3.6.3 备案人员因个人原因不再保持备案资格，可以书面形式向本机构申请注销。

3.7 审核人员资格要求

审核人员应具备质量、环境或职业健康安全管理体系 CCAA 任一注册审核员资格或碳足迹/温室气体审核员资格等其他注册审核员资格，且经过公司隐私管理体系相关知识培训合格。

4 初次认证程序

4.1 受理认证申请

4.1.1 认证机构应向申请认证的组织（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）本机构的授予、保持、扩大、更新、缩小、暂停或撤销认证及其证书等环节的制度规定。

（3）认证证书样式。

（4）对认证决定的申诉程序。

（5）分支机构和办事机构的名称、业务范围、地址等。

4.1.2 认证机构应当要求申请组织提交以下资料：

（1）认证申请书，包括申请组织的隐私管理、生产经营或服务活动等情况的说明。

（2）法律地位的证明文件（包括：企业营业执照、事业单位法人证书、社会团体登记证书、非企业法人登记证书、党政机关设立文件等）的复印件。若隐私管理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）。

（3）隐私管理体系覆盖的活动范围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）多场所活动、活动分包情况。

（5）隐私管理体系手册及必要的程序文件。

（6）隐私管理体系覆盖的产品或服务的质量/环境/安全标准清单。

（7）隐私管理体系已有效运行 3 个月以上的证明材料。

（8）其他与认证审核有关的必要文件。

4.1.3 认证申请的审查确认

认证机构应对申请组织提交的申请资料进行审核，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）申请组织为达到隐私管理体系目标而建立了文件化的隐私管理体系建设。

4.1.4 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，综合确定是否有能力受理认证申请。

4.1.5 对符合 4.1.3、4.1.4 要求的，认证机构可决定受理认证申请；对不符合上述要求的，认证机构应通知申请组织补充和完善，或者不受理认证申请。

4.1.6 认证机构应完整保存认证申请的审查确认工作记录。

4.1.7 签订认证合同

在实施认证审核前，认证机构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隐私管理体系建设的承诺。

（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或被媒体曝光事件。

②生产的产品或服务被执法监管部门认定不符合法定要求。

③发生产品或服务的质量安全事故。

④发生环保、消防、安监、劳动等行政处罚。

⑤被法院裁定未按合同约定履行相关责任。

⑥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、管理者代表变更；生产经营或服务的工作场所变更；隐私管理体系覆盖的活动范围变更；隐私管理体系和重要过程的重大变更等。

⑦出现影响隐私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；不擅自利用隐私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）拟认证的隐私管理体系覆盖的生产或服务的活动范围。

（6）在认证审核及认证证书有效期内各次监督审核中，认证机构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。

4.2 制定审核计划

4.2.1 审核时间

4.2.1.1 为确保认证审核的完整有效，公司根据申请组织具体情况，按附录 A 隐私管理体系人天计算表计算基本审核人天，核算并拟定完成审核工作需要的时间。特殊情况下，可以合理的增加或减少审核时间，理由应充分。

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 第一阶段审核

管理体系初次审核通常由第一阶段审核和第二阶段审核两个阶段组成。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质量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核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管理体系认证证书，通过对其文件和资料的审核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。

第一阶段审核可包括对文件审核的进一步确认。

（1）第一阶段审核的目的是通过对组织管理体系涉及的关键活动、危险源及其影响，方针及目标策划情况来了解组织的管理体系，了解评价受审核方管理体系建立及实施的基本情况，为策划第二阶段提供关注的重点。

（2）第一阶段审核，首先对受审核方管理体系文件进行审核，出具《文件评审报告》，并将《文件评审报告》反馈给受审核方。文件修改的符合性在一阶段审核前或一阶段现场确认，需要时，申请方对

管理体系文件作适当修改后，再次报送公司进行评审。文件审核确认不影响现场审核时，方可安排一阶段审核。

（3）一阶段审核结束前，审核组将与受审核方进行沟通，通报第一阶段审核结论。在第一阶段审核中，如发现组织存在不符合一并开具在《一阶段管理体系审核报告》中。并与申请组织讨论确定第二阶段审核安排。

（4）根据发现问题的严重程度决定是否需在不符合整改验证后进行二阶段审核。

4.2.3 第二阶段审核

4.2.3.1 确认第一阶段审核问题得到纠正或需进入现场验证而不影响二阶段审核时，方可进行第二阶段审核；现场审核时，认证范围覆盖的产品生产或服务活动应在正常运行；第一、二阶段审核的时间间隔不宜超过 3 个月，超过该期限，公司将调整审核方案。

4.2.3.2 审核涉及受审核方申请范围内所有的产品、过程和职能部门，并覆盖标准所有条款。对于多场所，根据抽样原则确定审核场所。第二阶段审核至少覆盖以下内容：

（1）在第一阶段审核中识别的二阶段审核关注的重点内容的监视、测量、报告和评审记录的完整性和有效性；

（2）为实现总目标而建立的各层级目标是否具体、有针对性、可测量并且可实现；

（3）对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或者自我评价是否有效。

4.2.3.3 审核组采用抽样的方法，通过交谈、调阅文件与记录以及查看现场等方式，收集受审核方管理体系运行证据。如发现组织存在违反审核依据的情况，审核组将视问题的严重程度及其产生的影响，出具《二阶段阶段审核报告》。对于发现的不符合根据严重程度分为：一般或严重。一般不符合关闭期限自审核后 30 日内，严重不合格最长关闭期限不超过 90 日。

4.2.3.4 审核末次会议前，审核组将与受审核方负责人进行沟通。在末次会议上，宣布审核结论，并明确对不符合纠正措施的实施要求。

4.2.3.5 现场审核结论包括“同意推荐认证注册”、“推迟推荐认证注册”或“不予推荐认证注册”三种。对审核中发现的不符合，受审核方应采取纠正措施，并经审核组验证。验证的方式有书面验证和现场验证两种。验证合格后，审核组方能将《管理体系审核报告》及相关资料报公司，提交技术委员会审议，对因受审核方原因，未能在规定期限内完成的纠正措施，审核组长可以修改结论。

4.2.3.6 审核实施前，审核组制定书面的审核计划（包括多场所抽样计划），以便为有关各方就审核活动的安排和实施达成一致提供依据。如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方，并协商一致。

4.2.4 审核组

认证机构应当根据隐私管理体系覆盖的活动范围及规模选择具备相关能力的审核员组成审核组。

4.2.5 审核计划

4.2.5.1 认证机构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（其中：审核员应标明备案证书号）。

4.2.5.2 通常情况下，初次认证二阶段审核、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。

如果隐私管理体系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隐私管理体系的正确审核。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隐私管理体系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。

4.2.5.3 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。

4.2.5.4 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，参会人员应签到。

4.3.3 审核过程及环节

4.3.3.1 初次认证审核，进入现场前需要提交相关申请资料，机构对申请资料进行合同评审，机构对申请资料进行合同评审，以便确定是否进入现场实施审核。

4.3.3.2 申请资料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隐私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 ISO/IEC 27701:2025《信息安全，网路安全和隐私保护，隐私信息管理体系 要求和指南》标准要求的情况，隐私管理体系运行过程中是否实施了内部审核与管理评审，确认隐私管理体系是否已有效运行并且超过 3 个月。

对隐私管理体系文件不符合现场实际、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，不予受理。

（3）确认申请组织建立的隐私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）结合隐私管理体系覆盖活动的特点识别对隐私管理体系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）与申请组织现场审核安排。

4.3.3.3 审核应当在申请组织现场进行。重点是审核隐私管理体系符合 ISO/IEC 27701:2025《信息安全，网路安全和隐私保护，隐私信息管理体系 要求和指南》标准要求和有效运行情况，应至少覆盖以下内容：

（1） 重要审核点的监视、测量、报告和评审记录的完整性和有效性。

（2）为实现总的隐私管理体系目标而建立的各层级隐私管理目标是否具体、有针对性、可测量并且可实现。

（3）对隐私体系管理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或自我评价是否有效。

4.3.4 发生以下情况时，审核组应终止审核，并向认证机构报告。

（1）申请组织对审核活动不予配合，审核活动无法进行。

（2）申请组织的隐私管理有重大缺陷，不符合 ISO/IEC 27701:2025《信息安全，网路安全和隐私保护，隐私信息管理体系 要求和指南》标准的要求。

（3）发现申请组织存在重大隐私管理体系隐私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、审核组成员及其个人备案信息。

（4）审核活动的实施日期和地点。

（5）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；对隐私管理体系目标实现情况的评价，应同时叙述测量方法。

（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 认证机构应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，认证机构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，认证机构应要求申请组织分析原因，并要求申请组织在规定期限内采取措施进行纠正。

4.5.2 认证机构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。

4.6 认证决定

4.6.1 认证机构应该在对审核报告、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，做出认证决定。

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 认证机构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 4.4 条要求，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，认证机构已评审、接受并验证了纠正和纠正措施及其结果的有效性。

①未能满足隐私管理体系标准的要求。

②制定的隐私管理体系目标不可测量、或测量方法不明确。

③对实现隐私管理体系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在持续改进隐私管理的有效性方面存在缺陷，实现隐私管理体系目标有重大疑问。

（3）认证机构对其他不符合项已评审，并接受了申请组织计划采取的纠正和纠正措施。

4.6.4 在满足 4.6.3 条要求的基础上，认证机构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）申请组织的隐私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 认证机构在颁发认证证书后，应当在 30 个工作日内按照规定的要求将相关信息报送国家认监委。

国家认监委在其网站（www.cnca.gov.cn）开设专栏向社会公开各认证机构上报的认证证书等信息。

4.6.7 认证机构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。

5 监督审核程序

5.1 认证机构应对持有其颁发的隐私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隐私管理体系持续符合要求。

5.2 为确保达到 5.1 条要求，认证机构应根据获证组织的产品或服务的隐私管理体系隐私程度或其他特性，确定对获证组织的监督审核的频次。

5.2.1 作为最低要求，在初次认证审核后至少 12 个月内应进行一次监督审核。此后，每次监督审核的时间间隔不超过 12 个月。

5.2.2 在达到监督审核期限而有证据表明获证组织暂不具备实施监督审核的条件时，可以适当延长监督审核期限，但最长间隔不能超过 15 个月。

5.2.3 超过期限而未能实施监督审核的，应按 7.2 或 7.3 条处理。

5.3 监督审核的时间，应不少于按 4.2.1 条计算审核时间人日数的三分之一，但审核时间应不少于 1 天。特殊情况下，可以合理的增加审核时间，理由应充分。

5.4 监督审核的审核组，应符合 4.2.5 条和4.3.1 条的要求。

5.5 监督审核应在获证组织现场进行，且应满足第4.2.5.3 条确定的条件。由于产品生产的季节性原因，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。

5.6 监督审核时至少应审核以下内容：

（1）上次审核以来隐私管理体系覆盖的活动及运行体系的资源是否有变更。

（2）按 4.3.3.2 条要求已识别的重要关键点是否按隐私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）隐私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）总隐私管理体系目标及各层级诚信目标是否实现。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。

（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相关的规定。（适用时）

（7）内部审核和管理评审或自我评价是否规范和有效。

（8）是否及时接受和处理投诉。

（9）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。

5.7 监督审核的审核报告，应按 5.6 条列明的审核要求逐项描述审核证据、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。

5.8 认证机构根据监督审核报告及其他相关信息，做出继续保持或暂停、撤销认证证书的决定。

6 再认证程序

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

6.2 认证机构应按 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。

在隐私管理体系及获证组织的内部和外部环境无重大变更时，再认证审核审核时间应不少于按4.2.1 条计算人日数的三分之二。

6.3 认证机构参照 4.6 条要求做出再认证决定。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 暂停或撤销认证证书

7.1 认证机构应制定暂停、撤销认证证书或缩小认证范围的规定，并形成文件化的管理制度。

7.2 暂停证书

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

（1）隐私管理体系持续或严重不满足认证要求，包括对隐私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）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。

7.2.2 认证证书暂停期不得超过 6 个月。但属于 7.2.1 第（5）项情形的暂停期可至相关单位作出许可决定之日。

7.2.3 认证机构暂停认证证书的信息，应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。

7.3 撤销证书

7.3.1 获证组织有以下情形之一的，认证机构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）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）出现重大的产品或服务等质量安全事故，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）没有运行隐私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。

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

7.4 认证机构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。

7.5 认证机构有义务和责任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。

8 认证的拒绝、保持、扩大、缩小、恢复的条件和程序

8.1 拒绝认证资格的条件和程序

8.1.1 拒绝认证资格的条件

a)认证客户信息未通过 ZFC 的申请评审，评审为不予受理认证申请；

b)ZFC 审核组现场审核结论为“不推荐认证注册”；

c)认证客户的管理体系有重大缺陷，不符合认证标准的要求，或认证客户存在重大安全、环境问题及与认证范围内相关严重违法违规行为，经 ZFC 的审定结论为不予认证注册；

d)初次认证第二阶段后，认证客户未在规定的时间内按要求关闭不符合，或未按规定接受 ZFC 再次实施的二阶段审核；

e)再认证审核后，认证客户未在规定的时间内按要求关闭不符合（包括 ZFC 审定提出的不符合）；

f)除以上情况外，ZFC 的审定结论为不予认证注册。

8.1.2 拒绝认证注册的程序

a)符合 8.1.1 条件之一，经 ZFC 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)ZFC 向认证客户发出《不予认证注册通知》。

8.2 保持认证资格的条件和程序

8.2.1 保持认证资格的条件

a)获证客户的法律地位、行政许可文件持续符合国家的最新要求，并且认证范围在法律地位文件和行政许可文件规定的范围内；

b)获证客户持续遵守认证有关的规定，包括变更的规定；

c)获证客户在认证范围内的组织单元、产品、服务及其过程和活动持续满足适用的最新法律法规的要求，如发生不满足时及时采取有效的措施；

d)获证客户于获证期内，认证范围内涉及的产品/服务/活动未发生重大事故和国家检查不合格；

e)获证客户在获证期间未发生误用认证证书和认证标志，如有发生能及时有效地采取纠正和纠正措施，并将误用产生的影响降至最少程度；

f)获证客户对顾客或相关方的重大投诉和关切能及时有效地处理；

g)获证客户能按照 ZFC 要求及时通报管理体系和重要过程变更等信息；

h)按时接受监督审核,经现场审核获证客户的管理体系持续符合认证标准/规范性文件要求，审核组结论为“保持认证”；

i)获证客户履行与ZFC 签署认证合同中规定的责任和义务，并按照认证合同规定缴纳认证费用。

8.2.2 保持认证资格的程序

a)满足8.2.1 保持认证资格的条件，监督审核后，经 ZFC 派出的审核组长确认和 ZFC 审查后认为获证客户在认证范围内能持续满足保持认证资格的条件，同意保持认证资格，由 ZFC 签发确认证书并向获证客户发放；

b)在认证证书有效期内如有认证要求变更，获证客户接受变更的认证要求，并经 ZFC 验证在认证范围内管理体系满足变更的要求，可保持认证资格。

8.3 扩大认证范围的条件和程序

扩大认证范围内的组织单元、产品、服务及其过程和活动。

8.3.1 扩大认证范围的条件

a)获证客户保持认证资格有效。

b)获证客户申请扩大的认证范围在法律地位文件范围内。国家、地方或行业有要求时，获证客户拟扩大的认证范围具有有效的行政许可文件；

c)国家或地方或行业有要求时，获证客户在申请扩大认证范围内的组织单元、产品、服务及其过程和活动，已满足适用的法律法规的要求；

d)获证客户的管理体系覆盖申请扩大的认证范围，并符合认证标准/规范性文件要求；

获证客户按照认证规定缴纳补充认证费用。

8.3.2 扩大认证范围的程序

a)ZFC 向获证客户提供与扩大认证范围有关信息的公开文件，获证客户知悉并理解；

b)获证客户向ZFC 正式提交扩大认证范围的申请和相关附件；

c)需要时，获证客户与ZFC 补充签署或修订认证合同，并按照规定补充缴纳认证费用；

d)满足8.3.1扩大认证范围的条件，经 ZFC 审核、审定，认为获证客户在申请扩大认证范围内已满足批准认证资格的条件，同意批准扩大认证范围，认证证书的注册号和有效期保持不变；

e)ZFC 向获证客户送交新认证证书，同时收回原证书。

8.4 缩小认证范围的条件和程序

缩小认证范围内的组织单元、产品、服务及其过程和活动。

8.4.1 缩小认证范围的条件

a)获证客户认证范围内部分产品/服务、区域等不再符合认证标准/规范性文件和其他要求；

b)获证客户不愿再继续保持认证范围内的部分产品、服务、区域等认证资格；

c)获证客户缩小认证范围应不包括为缩小认证隐私的情况。

8.4.2 缩小认证范围的程序

a)获证客户向ZFC 正式提交缩小认证范围的申请，或 ZFC 提出缩小获证客户认证范围的建议，并提供理由和证据。ZFC 的审定意见和日常监督结果也可作为认证范围缩小的信息来源和理由，经认证双方沟通后达成一致意见；

b)需要时，获证客户应与 ZFC 修订认证合同；

c)经 ZFC 审定，认为获证客户在申请缩小认证范围不会对仍保持的认证范围产生影响，同意批准缩小认证范围，收回原认证证书，换发认证证书或附件，认证证书的注册号和有效期保持不变。

8.5 恢复认证资格的条件和程序

8.5.1 恢复认证资格的条件

获证客户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内没有使用、引用认证资格（如广告宣传）和使用认证标志。

8.5.2 恢复认证资格的程序

a)在确定的认证资格暂停限期结束前，根据暂停原因，获证客户在规定期限内向ZFC 提出恢复认证资格；

b)需要时，获证客户应提交相关纠正措施和有效性验证材料；

c)获证组织已在 ZFC 规定的时限内解决造成暂停的问题，即可办理恢复手续，凡因体系运行不正常导致暂停的需要进行现场验证，按特殊审核程序办理恢复（特殊审核可与监督审核一并进行）；获证组织从接到 ZFC 恢复认证资格通知后，即可恢复认证证书和标志的正常使用。

9 认证证书要求

9.1认证证书应至少包含以下信息：

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

（2）隐私管理体系覆盖的生产经营或服务的地址和业务范围。若认证的隐私管理体系覆盖多场所，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）隐私管理体系符合 ISO/IEC 27701:2025《信息安全，网路安全和隐私保护，隐私信息管理体系 要求和指南》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。认证机构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。

9.2 认证证书有效期最长为 3 年。

9.3认证机构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。

10 与其他管理体系的结合审核

10.1 对隐私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 4.4 条要求，并易于识别。

10.2 如结合审核，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 受理转换认证证书

11.1 认证机构应当履行社会责任，严禁以牟利为目的受理不符合 ISO/IEC 27701:2025《信息安全，网路安全和隐私保护，隐私信息管理体系 要求和指南》标准、不能有效执行隐私管理体系的组织申请认证证书的转换。

11.2 认证机构受理组织申请转换本机构的认证证书，应该详细了解申请转换的原因，进行必要的现场审核。

11.3 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。

11.4 被执法监管部门责令停业整顿或列入“黑名单”的（如 7.2 条第［3］项）、被发证的认证机构撤销证书的（如 7.3 条），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。

12 受理组织的申诉

获证组织对认证决定有异议时，认证机构应接受获证组织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获证组织。

书面通知应当告知获证组织，若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。

13认证记录的管理

13.1 认证机构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。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。

13.3 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。

14 其他

14.1 本规则内容提及 ISO/IEC 27701:2025《信息安全，网路安全和隐私保护，隐私信息管理体系 要求和指南》标准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。

14.2 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，并经复印件提供者签章（签字）认可其与原件一致。

14.3 认证机构可采取必要措施帮助组织开展隐私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隐私管理标准。

附录

隐私管理体系
认证审核时间要求

企业有效人数	审核时间（天）	备注
1-95 人	1	
96-325 人	2	
326-525 人	2.5	
526-825 人	3	
826-1525 人	3.5	
1526-1825 人	4.5	
1826-2325 人	5	
2326-2625 人	5.5	
2626-3450 人	6	
3451-3950 人	6.5	
3951-4750 人	7	
4751--5750 人	7.5	
5751-6750 人	8	
6751-7750 人	8.5	
7751-8750 人	9	
8751-9750 人	9.5	
9751-10750 人	10	
10751-15750 人	10.5	
15751-20750 人	11	
20751-25750 人	11.5	
25751-30750 人	12	
30751-35750 人	12.5	
35751-40750 人	13	
40751-45750 人	13.5	
45751-50750 人	14	

注：1.有效人数，包括认证范围内涉及的所有全职人员，原则上以组织的社会保险登记证所附名册等信息为准。

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。