认 证 规 则

隐私信息管理体系认证规则

编 号：ZXB-PIMS-01-2025

受 控 状 态：受 控

版本	编修	审核	批准	编写/修订日期	发布日期
A/0	崔海军	张京梅	郑宇兵	20250418	20250530
A/0	崔海军	张京梅	郑宇兵	20250825	20250825
A/1	郭冬梅	郭冬梅	郑宇兵	20260521	20260521

管理体系手册编制/修订履历

版本	修订内容	编写日期/修订日期	发布日期
A0	新编	20250418	20250530
A0	增加认证标志的要求内容	20250825	20250825
A1	修改：认证领域备案错误；认证规则中未明确认证费用由认证委托人向认证机构直接支付；规则未明确第一阶段审核和第二阶段审核间隔最短不应少于 5 日，最长不应超过 6 个月；认证依据文本非正式发布版，包括国际标准上传非官方翻译版；认证规则文本中未列明认证标志；规则未明确每次监督审核间隔不应超过 12 个月且每个日历年至少有一次监督审核（再认证的年份除外）；规则未明确认证审核组应至少有 1 名认证机构专职审核员全程参与审核过程；规则未明确实习审核员不能独立组成审核组；规则中审核人日少于市场监管总局（国家认监委）或认可机构明确的审核时间；规则未明确管理体系认证审核应在认证委托人现场且认证委托人的生产或服务处于正常运行时进行；规则未明确第一阶段非现场审核的确适用情形；认证规则公开网址不能直接显示规则全文且未提供具体的电话号码获取全文；规则未明确再认证审核内容；认证规则公开网址不能直接显示规则全文且未提供具体的邮箱获取全文；规则未明确现场审核应对最高管理者发挥对管理体系领导作用的情况进行面对面审核；规则未明确不符合项纠正和纠正措施及其验证应明确验证方式和验证时限；规则内容中引用了其他认证机构内部文件的，但是未附引用的文件；未在认证规则中明确认证审核员应具备的管理体系认证审核员注册资格；未明确多场所抽样方案；规则中审核人日少于质量管理体系认证审核时间；	20260521	20260521

目 录

一、前言

大数据时代的到来，为我们带来了空前的便利，随着大数据在各个领域的渗透逐渐加深，个人隐私泄露的风险也愈加严重，人们对信息安全的关注日益提升，全球多个国家和地区相继出台了一系列隐私保护的法律法规，当前几乎所有的组织都有处理个人信息 (PII) 的情况，保护 PII 不仅是法律要求，也是社会需要。

因此，新标准 ISO/IEC 27701 隐私信息管理体系应势而生。助力组织为 GDPR 合规展现、保护用户隐私和个人信息合规管理提供了更多相关指南。2019 年 8 月 6 日，国际标准化组织 ISO 和国际电工委员会 IEC 正式对外发布 ISO/IEC 27701 隐私信息管理体系标准。这标志着信息安全、隐私与个人信息保护，在国际间法律与法规的合规展现有了一致性的标准。

该标准填补了目前隐私信息管理体系的空白，将隐私保护的原则、理念和方法，融入到信息安全保护体系中，并且对 PII 控制者和 PII 处理者进行了较为详细且落地性强的规定，细化了隐私信息管理的要求，给组织在隐私保护和信息安全方面给出了指导建议。作为一个国际通用的隐私信息管理工具，能够有效的协助组织对隐私风险进行识别、分析，采取措施将风险降到可接受水平并维持该水平，并建立隐私保护体系，从管理与技术等多方面满足国内外的监管合规要求。

二、适用范围

2.1 本规则用于规范众信标（北京）认证有限公司（以下简称：ZXB）对申请认证和获证的各类组织按照信息管理的扩展要求和指南 ISO /IEC 27701:2025《信息安全、网络安全和隐私保护-隐私信息管理体系-要求与指南》标准建立适用于 PIMS 文件审核、编制审核计划及现场前的准备、审核组内部会议、第一阶段/第二阶段现场审核、不符合、对受审核方体系评价、监督审核、再认证等审核相关活动。

2.2 本规则适用于各类组织，包括但不限于企业、政府机构、事业单位、社会团体等。这些组织在其运营过程中，涉及对个人可识别信息（PII）进行收集、保存、传输、处置、使用、共享、转让、披露和委托处理等活动，均可依据本规则申请隐私信息管理体系认证。无论是大型跨国企业，还是小型初创公司；无论是传统行业，如制造业、金融业，还是新兴的互联网、大数据行业，只要存在处理 PII 的行为，都能适用本认证规则，以提升自身在隐私信息管理方面的能力和水平，增强社会公信力和市场竞争力。

三、认证依据用技术规范、技术规范强制性要求或者标准

3.1 ISO /IEC 27701:2025《信息安全、网络安全和隐私保护-隐私信息管理体系-要求与指南》：该标准详细规定了作为 PII 控制者和 PII 处理者的组织在隐私信息管理方面的特定目标和控制措施，从管理体系层面为组织提供全面指导，确保组织对隐私风险进行有效识别、分析，并采取相应措施，以符合高级别的隐私保护合规要求。

3.2 GB/T 22080/ISO/IEC 27001《信息技术 安全技术 信息安全管理体系要求》：作为信息安全管理体系的基础标准，其为隐私信息管理体系提供了必要的信息安全管理框架和基础要求。组织在构建隐私信息管理体系时，需遵循该标准中关于信息安全管理的通用要求，如信息安全策略制定、风险评估与处置、人力资源安全、物理和环境安全、通信和操作管理等方面的要求，以保障 PII 在整个生命周期中的安全性。

四、对认证人员的要求

4.1 认证人员基本要求

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。

4.2 隐私信息管理体系审核员资质要求

4.2.1 隐私信息管理体系审核员，应至少具备 ISMS 审核员资格或者 ITSMS 审核员资格；或者或者具备 CCAA 注册的 QMS 审核员资格并且具有数字化转型或两化融合资格，并参加了 ISO/IEC 27701 标准培训考试合格,由技术部评价可获得人工智能管理体系资格。

4.2.2 需通过 ISO/IEC 27701 标准基础知识及相关从业法律法规的培训，并经过考试合格；

4.2.3 掌握相应隐私信息管理体系的知识和技能，经 ZXB 人员能力评价，确认符合要求，方可获得隐私信息管理体系审核员资格。

4.3 隐私信息管理体系认证人员专业能力评价准则，参考 ZXB-CX-11 认证人员管理程序。

五、认证程序

5.1 认证申请

5.1.1 认证机构应向认证委托人至少公开以下信息：

（1）可开展的认证业务范围，获得认可的情况， 以及分包境外认证机构业务的情况；

（2）开展 PIMS 认证活动所依据的认证标准以及相关的认证方案、认证流程；

（3）授予、拒绝、保持、更新、暂停（恢复）、注销、撤销认证证书以及扩大或缩小认证范围的程序规定；

（4）拟向认证委托人获取的信息以及保密规定；

（5）认证收费标准；

（6）认证证书、认证标志及相关的使用规定；

（7）对认证过程和结果的申诉、投诉规定；

（8）认证标准换版的规定（适用时）；

（9）“提前较短时间通知的审核” 的情形；

（10）其他需要公开的信息。

5.1.2 提出认证申请时，认证委托人应具备以下条件：

（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）已按认证标准建立 PIMS，且运行满三个月；

（4） 因获证组织自身原因被原发证机构暂停、注销或撤销 PIMS 认证证书已满一年（适用时）；

（5）原 PIMS 认证证书发证机构被国家认监委撤销 PIMS 认证资质已满三个月（适用时）；

（6） 当前未被行政监管部门责令停产停业整顿；

（7）当前未列入 “ 国家企业信用信息公示系统”和 “信用中国”发布的严重违法失信名单；

（8）其他应具备的条件。

5.1.3 认证机构应要求认证委托人提供以下信息和文件资料：

（1）认证申请，包括认证委托人的名称、地址、认证依据的标准、 申请的认证范围、

认证范围内人员数量及影响体系有效性的外包过程；

（2）法律地位的证明文件，当 PIMS 覆盖多个法律实体时，应提供每个法律实体的法律地位证明文件；

（3）申请认证范围所涉及的信息技术法律法规要求的行政许可文件、资质证书等（适用时）；

（4）组织机构及职责；

（5）信息技术服务的流程、班次及轮班情况；

（6）PIMS 运行满三个月的证据；

（7）其他需要提供的文件。

5.2 申请评审

5.2.1 认证机构应建立并实施相应程序，对认证委托人提交的申请信息和文件资料实施申请评审，仔细鉴别申请信息和文件资料的真伪，确定是否受理认证申请，并保存相应评审记录。

5.2.2 满足以下条件的，认证机构可以受理认证申请：

（1）认证委托人已具备受理条件（ 见 5.1.2）；

（2）认证机构具备实施认证的能力；

（3）双方就认证事宜达成一致。

5.2.3 对于新的认证委托人，仅在同时满足下列情况的前提下，认证机构可实施认证转换，否则应按照初次认证开展认证活动：

（1）认证机构具有认证委托人申请认证的 PIMS 认证范围的认可资格；

（2）认证委托人持有其他被认可的认证机构（原认证机构）颁发的带认可标识的 PIMS 认证证书（原认证证书）；

（3）原认证证书处于有效期内，未被原认证机构实施暂停或撤销；

（4）原认证机构认证业务正常运行，不存在认可资格到期、被暂停或撤销的问题；

（5）认证机构应获得认证委托人初次认证审核报告或最近一次的再认证审核报告、监督审核报告、审核中发现的不符合及其纠正措施。

5.2.4 认证机构应将申请评审的结果告知认证委托人。

5.3 认证合同及相关责任

5.3.1 通过申请评审的，认证机构应与每个认证委托人签订具有法律效力的认证合同，明确认证服务的费用、付费方式和违约条款，及认证委托人、认证机构和获证组织的责任。认证费用应由认证委托人向认证机构直接支付。

5.3.2 认证机构应及时向符合认证要求的认证委托人颁发认证证书，对获证组织 PIMS 运行情况进行有效监督，通过其网站或者其他形式向社会公布认证证书信息； 因认证机构批准资质注销或被撤销导致获证组织 PIMS 认证证书无法有效保持的，需及时告知获证组织并作出妥善处理，并承担由此导致的获证组织在合同上约定或法律认定的经济损失。

5.3.3 认证委托人应遵守认证程序要求，如实提供相关材料和信息，配合认证行政监管部门的监督检查和认证机构对投诉的调查，及时向认证机构通报 PIMS 及 5.1.2 中条件的变更情况，承担选择的认证机构资质被撤销而带来的认证活动终止、认证证书无法使用的风险。

5.3.4 获证组织应遵守认证程序要求，如实提供相关材料和信息，通过 PIMS 认证后持续有效运行 PIMS，配合认证行政监管部门的监督检查和认证机构对投诉的调查，在广告、宣传等活动中正确使用认证证书、认证标志和有关信息，及时向认证机构通报 PIMS 及 5.1.2 中条件的变更情况，承担选择的认证机构资质被撤销而带来的认证证书无法使用的风险。

5.4 审核方案和审核策划

5.4.1 审核方案

5.4.1.1 认证机构应针对每一认证委托人建立认证周期内的审核方案， 以清晰地识别所需的审核活动。

5.4.1.2 初次认证的审核方案应包括两阶段初次认证审核、获证后的监督审核和认证到期前的再认证审核。再认证的审核方案应包括再认证审核、获证后的监督审核和认证到期前的再认证审核。

5.4.1.3 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 27701:2025《信息安全、网络安全和隐私保护-隐私信息管理体系-要求与指南》所有要求， 以及认证范围内的典型信息技术服务。认证证书有效期内的监督审核累

计应覆盖 ISO /IEC 27701:2025《信息安全、网络安全和隐私保护-隐私信息管理体系-要求与指南》所有要求。

5.4.1.4 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。此后，监督审核间隔不应超过 12 个月。

5.4.1.5 认证机构应考虑认证委托人不同班次完成的过程，以及其所证实的对每个班次的 PIMS 控制水平来策划对不同班次实施的审核程度， 以确保审核的有效性：

（ 1 ）每次审核应至少对其中一个班次的信息技术服务活动现场进行审核；

（2 ）未审核其他班次信息技术服务活动现场的，应记录未审核的理由。

5.4.2 审核时间

5.4.2.1 审核时间包括在认证委托人现场的审核时间以及在现场审核以外实施策划、文件审核和编写审核报告等活动的时间。审核时间以人日计，1 人日为 8 小时，不应通过增加工作日的工作小时数以减少审核人日数。

如果认证委托人工作日的实际工作时间不足 8 小时，则应延长现场审核天数以满足审核时间要求。

5.4.2.2 认证机构应以附录 A 所规定的审核时间为基础，考虑认证委托人有效人数等因素，建立文件化的不同审核类型审核时间（包括现场审核时间）的确定方法。

5.4.2.3 每次审核的审核时间确定过程应形成记录，尤其是减少审核时间的理由，减少的审核时间不得超过附录 A 所规定的审核时间的 30%，现场审核时间不得少于所确定的审核时间的 80%。如果审核人日计算后结果包括小数，应将其调整为最接近的半人日数。

5.4.2.4 认证机构应建立文件化的结合审核时间确定方法，PIMS 和其他管理体系实施结合审核的，结合审核的总审核时间不得少于多个单独体系所需审核时间之和的 80%。

5.4.3 多场所抽样方案

5.4.3.1 认证机构应建立并实施文件化的多场所组织认证抽样的规则，策划并保留多场所组织的抽样及审核时间确定的记录。

5.4.3.2 对涵盖相同活动、过程的多个相似场所 PIMS 可进行抽样审核，抽样数量应不少于按以下方法计算的结果：

（1）初次认证审核：$Y = \sqrt{X}$；

（2）监督审核：$Y = 0.6\sqrt{X}$；

（3 ）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。

5.4.3.3 对多个非相似场所，则不应抽样，初审和再认证审核应当逐一到各场所进行审核。监督审核应抽取不少于 30%的场所进行审核，且每次审核均应包括中心职能部门。第二次监督审核选取的场所通常不同于第一次监督审核所选取的场所。

5.4.3.4 分场所审核人日的计算方法参见 5.4.2，且现场审核时间不得少于依据附录 A 所确定的现场审核时间的 50%。

服务点审核人日应与审核组在该服务点所需完成的审核活动相匹配，通常每个服务点的现场审核时间不少于 0.25 人日。

对每个场所（包括服务点）单独计算的现场审核时间进行汇总，得出的多场所总现场审核时间不应小于依据附录 A 计算出的总现场审核时间。

5.4.4 组建审核组

5.4.4.1 认证机构应根据实现审核目的所需的能力和公正性要求组建审核组，至少 1 名实施第一阶段审核的审核员应参加第二阶段审核，每个审核组应包括：

（1）审核组长：认证机构应建立并实施审核组长的选择、培训以及任用的管理制度；审核组长应当具有管理和领导审核组达成审核目标的知识和技能，其能力应至少满足 GB/T 19011《管理体系审核指南》中对审核组长的通用要求;

（2）至少 1 名与认证委托人所属认证业务范围相匹配的 PIMS 专业领域审核员。在必要时还应配备相关行业的信息技术服务管理技术专家。PIMS 和其他管理体系实施结合审核的，审核组还应包括其他管理体系的专业人员，确保专业人员的能力覆盖实施结合审核的全部管理体系;

（3）至少 1 名认证机构的专职审核员，并确保专职审核员全程参与 PIMS 审核过程。

5.4.4.2 技术专家主要负责为审核组提供技术支持，不作为审核员实施审核，不计入审核时间。

5.4.4.3 实习审核员应在正式审核员的指导下参加审核，不计入审核时间，其在审核过程中的活动由负责指导的正式审核员承担责任。审核组中实习审核员的数量不

得超过正式审核员的数量。

5.4.4.4 审核组成员不得与认证委托人存在利益关系。

5.4.5 审核计划

5.4.5.1 认证机构应依据审核方案制定每次现场审核的审核计划。审核计划至少包括：审核目的、审核准则、审核范围、现场审核的日期、时间安排和场所、审核组成员及审核任务安排。

其中，审核员应注明 PIMS 审核员注册号，专业领域审核员和技术专家应标明专业代码，兼职审核员和技术专家应注明工作单位。

5.4.5.2 现场审核应安排在认证委托人的信息技术服务处于正常运行时进行。

5.4.5.3 现场审核开始前，应将审核计划提交给认证委托人并经其确认。如需要临时调整审核计划，应经双方协商一致后实施。

5.5 实施审核

5.5.1PIMS 认证审核应在认证委托人的现场实施，包括初次认证审核以及认证周期内的每年度的监督审核、再认证审核和特殊审核。

5.5.2 审核组应按照审核计划实施审核，并采用中文记录审核过程，可补充使用图片/音像作为记录。

5.5.3 审核组应会同认证委托人召开首、末次会议，认证委托人的最高管理者、PIMS 相关职能部门负责人应参加首、末次会议，认证机构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。

5.5.4 审核组应通过面对面访谈等形式，对认证委托人的最高管理者在 PIMS 中发挥领导作用的情况进行重点审核，并保留现场图片/音像、审核记录等证明材料。最高管理者不熟悉组织自身的信息技术服务方针、信息技术服务目标，未亲自参与并推动 PIMS 实施的，认证审核应不予通过。

5.5.5 发生下列情况的，审核组应向认证机构报告后终止审核：

（1）认证委托人对审核活动不予配合，审核活动无法进行；

（2）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；

（3）认证委托人实际情况与申请材料有重大不一致；

（4）其他导致审核程序无法完成的情况。

5.6 初次认证审核

5.6.1 总则

初次认证审核应分为两个阶段实施：第一阶段审核和第二阶段审核。两个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。

5.6.2 第一阶段审核

5.6.2.1 第一阶段审核的目的是通过了解认证委托人的PIMS 和其对第二阶段的准备情况，确定其是否具备接受第二阶段审核的条件并策划第二阶段审核的关注点。第一阶段审核的内容包括但不限于以下方面：

（1）了解认证委托人的情况，包括其信息技术服务活动、设施设备、服务流程、现场运作以及适用的信息技术服务标准；

（2）评审认证委托人 PIMS 体系文件，确认其与认证委托人业务活动及信息技术服务相吻合；

（3）确认认证委托人申请信息和文件资料的真实性；

（4）审核认证委托人理解和实施 ISO /IEC 27701:2025《信息安全、网络安全和隐私保护-隐私信息管理体系-要求与指南》标准的情况，特别是对 PIMS 关键绩效、过程、信息技术服务目标和运作的识别情况；

（5）确认认证委托人是否为第二阶段审核做好准备， 已实施了内部审核和管理评审；

（6）确认认证委托人 PIMS 认证范围、体系覆盖范围内有效人数和场所；

（7）认证委托人的信息技术服务符合信息技术服务相关法律法规的情况。

5.6.2.2 为达到第一阶段审核的目的和要求，除下列情况外，第一阶段审核应在认证委托人现场实施：

（1）认证委托人已获本认证机构颁发的其他管理体系认证领域的有效认证证书，认证机构

已对认证委托人 PIMS 有充分了解；

（2）认证委托人获得了经认可机构认可的其他认证机构颁发的有效的 PIMS 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。

认证机构应记录未在现场进行第一阶段审核的理由。

5.6.2.3 认证机构应将认证委托人是否具备第二阶段审核条件的结论书面告知认证委托人，包括所识别的需引起关注的、在第二阶段可能被判定为不符合的问题。

5.6.2.4 认证机构通过第一阶段审核发现相关申请信息和文件资料存在虚假情况的，应终止认证活动。

5.6.3 第二阶段审核

5.6.3.1 第二阶段审核的目的是评价认证委托人 PIMS 的实施情况，包括对 ISO /IEC 27701:2025《信息安全、网络安全和隐私保护-隐私信息管理体系-要求与指南》 标准要求的符合性和体系的有效性。

5.6.3.2 第二阶段审核应在认证委托人的现场实施，至少覆盖以下内容：

（ 1 ）认证委托人 PIMS 与 ISO /IEC 27701:2025《信息安全、网络安全和隐私保护-隐私信息管理体系-要求与指南》标准的符合情况及证据；

（2）依据 PIMS 关键绩效目标和指标，对绩效进行的监视、测量、报告和评审；

（3）认证委托人实施 PIMS 的能力以及在符合适用法律法规要求方面的绩效；

（4）认证委托人信息技术服务过程的运作控制；

（5）认证委托人的内部审核和管理评审；

（6）针对认证委托人 PIMS 方针的管理职责。

5.7 监督审核

5.7.1 认证机构应对获证组织进行有效跟踪，依据审核方案对获证组织开展监督审核，并要求获证组织的最高管理者参与审核访谈， 以确认获证组织 PIMS 与 ISO /IEC 27701:2025《信息安全、网络安全和隐私保护-隐私信息管理体系-要求与指南》 标准的持续符合性和运行的有效性。

5.7.2 每次监督审核应尽可能覆盖认证范围内的典型信息技术服务，并确保在认证证书有

效期内的监督审核覆盖认证范围内的所有典型信息技术服务。

5.7.3 监督审核应重点关注获证组织的变更以及 PIMS 绩效的持续改进，监督审核的内容至少包括：

（1）内部审核和管理评审；

（2）对上次审核确定的不符合采取的纠正措施及效果；

（3）PIMS 在实现获证组织目标和 PIMS 预期结果方面的有效性；

（4）为持续改进而策划的活动的进展；

（5 ）持续的运作控制；

（6）任何变更，应包括服务目录的变化情况；

（ 7 ）认证证书、认证标志的使用和（或）任何其他对认证信息的引用；

（ 8 ）PIMS 相关投诉的处理。

5.7.4 监督审核的时间应根据获证组织当前有效人数确定，不少于依据附录 A 所确定的初次认证审核时间的 1/3。

5.8 再认证审核

5.8.1 认证证书期满前，获证组织申请继续持有认证证书的，认证机构应依据审核方案实施再认证审核， 以判断获证组织的 PIMS 作为一个整体与 ISO /IEC 27701:2025《信息安全、网络安全和隐私保护-隐私信息管理体系-要求与指南》 的持续符合性和运行的有效性。

5.8.2 再认证审核应在获证组织现场进行，并应在认证证书到期前完成。再认证审核的内容至少应包括：

（ 1 ）结合其内部环境和外部环境的变化情况，确认获证组织 PIMS 有效性及认证范围的持续相关性和适宜性；

（2）PIMS 绩效持续改进的证实；

（3）PIMS 在实现获证组织目标和 PIMS 预期结果方面的有效性。

5.8.3 再认证审核策划时应考虑获证组织最近一个认证周期内的 PIMS 绩效，包括调阅以往的监督审核报告。

5.8.4 再认证审核的审核时间应按 5.4.2 的要求，根据获证组织当前有效人数来确定，不少于依据附录 A 所确定的初次认证审核时间的 2/3。

5.9 特殊审核

5.9.1 扩大认证范围

对于已授予的认证，认证机构应对扩大认证范围的申请进行评审，并确定任何必要的审核活动，以作出是否可予扩大的决定。这类审核活动可以结合监督审核同时进行。

5.9.2 提前较短时间通知的审核

为调查投诉，对变更作出回应或对被暂停的客户进行追踪，可能需要在提前较短时间或不通知获证组织的情况下进行审核，此时：

（ 1 ）认证机构应说明并使获证组织提前了解将在何种条件下进行此类审核；

（2 ）由于获证组织缺乏对审核组成员的任命表示反对的机会，认证机构应在指派审核组时给予更多的关注。

5.10 不符合项及其验证

5.10.1 对审核中发现的不符合，认证机构应要求认证委托人在规定的时限内进行原因分析，采取相应的纠正措施。

5.10.2 认证机构应对认证委托人所采取的纠正措施的有效性进行验证。认证委托人可以针对轻微不符合制定纠正措施计划，由认证机构在下次审核时验证。

5.10.3 严重不符合的验证时限应满足以下要求：

（1）初次认证：在第二阶段审核结束之日起 6 个月内完成；

（2）监督审核：在审核结束之日起 3 个月内完成；

（3）再认证：在原认证证书到期前完成。

5.10.4 对于认证委托人未能在规定的时限内完成对不符合所采取措施的情况，认证机构不应作出授予认证、保持认证或更新认证的决定。

5.11 审核报告

5.11.1 认证机构应就每次审核向认证委托人提供书面的审核报告。审核组长应对审核报告的内容负责。

5.11.2 审核报告的内容应准确、简明和清晰，反映认证委托人 PIMS 的真实状况，描述对照 ISO /IEC 27701:2025《信息安全、网络安全和隐私保护-隐私信息管理体系-要求与指南》 标准的符合性和有效性的客观证据信息，及对认证结论的推荐意见。

5.11.3 审核报告至少应包括或引用以下内容：

（1）认证机构名称；

（2）认证委托人的名称和地址及其代表；

（3）审核类型（如初次认证、监督、再认证或其他类型）；

（4）结合、联合或一体化审核情况（适用时）；

（5）审核准则；

（6）审核目的及其是否达到的确认；

（7）审核范围，特别是标识出所审核的组织、职能单元或过程， 以及审核时间；

（8）任何偏离审核计划的情况及其理由；

（9）任何影响审核方案的重要事项；

（10）审核组成员姓名、身份及任何与审核组同行的人员；

（11）审核活动（现场或非现场，永久或临时场所）的实施日期和地点；

（12）应描述与审核类型要求一致的审核发现、审核证据（或审核证据的引用） 以及审核结论，重点反映认证委托人信息技术服务提供过程与控制情况、 内部审核和管理评审的过程、所取得的绩效，认证委托人实际情况与其预期信息技术服务目标之间存在的差距和改进机会；

（13）上次审核后发生的影响认证委托人 PIMS 的重要变更（适用时）；

（14）获证组织对认证证书和认证标志使用的控制情况（适用时）；

（15）对以前不符合采取的纠正措施有效性的验证情况（适用时）；

（16） 已识别出的任何未解决的问题；

（17）说明审核基于对可获得信息的抽样过程的免责声明；

（18）审核组的推荐意见以及对申请的认证范围适宜性的结论。

5.11.4 认证机构应保留用于证实审核报告中相关信息的审核证据。

5.11.5 对终止审核的项目，审核组应将终止审核的原因以及

已开展的工作情况形成报告，认证机构应将此报告提交给认证委托人。

5.12 认证决定

5.12.1 认证机构应在对审核报告、不符合的纠正措施及验证情况和其他信息进行复核、综合评价的基础上，作出认证决定。

认证决定人员应为认证机构的专职认证人员，并不得为审核组成员，能力应满足关于认证机构资质审批的相关要求。认证决定过程不得外包，认证决定须由中华人民共和国境内的工作人员作出。

5.12.2 认证机构有充分的证据确认认证委托人满足下列条件的，应作出授予、更新、扩大认证范围的决定：

（1）5.1.2 中的条件；

（2）对于严重不符合， 已评审、接受并验证了纠正措施的有效性；对于轻微不符合， 已评审、接受了认证委托人的纠正措施或计划采取的纠正措施；

（3）认证委托人的 PIMS 符合 ISO /IEC 27701:2025《信息安全、网络安全和隐私保护-隐私信息管理体系-要求与指南》 标准要求且运行有效；

（4）认证委托人按照认证合同规定履行了相关义务。

5.12.3 初次认证审核的认证决定应在现场审核后 6 个月内完成。否则应在推荐认证注册前再实施一次第二阶段审核。

5.12.4 再认证审核的认证决定宜在上一认证周期认证证书到期前完成，最迟应在认证证书到期之日起 6 个月内完成。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。

5.12.5 认证委托人不能满足 5.12.2 要求的，认证机构应以书面形式告知其未通过认证的原因。

5.12.6 对于监督审核，认证机构在满足下列条件时，可根据审核组长的肯定性结论保持对获证组织的认证，无需再进行独立的认证决定：

（1）监督审核未发现严重不符合及其他可能导致认证证书暂停、撤销的情况；

（2）获证组织认证信息未发生变更，不存在扩大、缩小认证范围的情况；

（3）认证机构建立了监督审核的监视机制并予以实施，可确保监督审核活动的有效性。

六、认证证书和认证标志

6.1 总则

6.1.1 认证机构应制定文件化的管理制度，要求获证组织正确使用 PIMS 认证证书和认证标志，以满足《认证证书和认证标志管理办法》相关规定。

6.1.2 获证组织可以在认证证书有效时使用 PIMS 认证证书和认证标志，并接受认证机构的监督管理。认证证书处于暂停期间、被撤销或注销后，不得继续使用认证证书和认证标志。

6.1.3 获证组织应当在广告等有关宣传中正确使用 PIMS 认证标志，只有在注明获证组织通过 PIMS 认证及认证机构名称情况下，方可使用 PIMS 认证标志。获证组织不得利用 PIMS 认证证书、认证标志或相关文字、符号，误导公众认为其信息技术服务通过认证。

6.1.4 认证机构发现获证组织未正确使用认证证书和认证标志的，应当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。

6.2 认证证书

6.2.1 认证机构应及时向认证决定符合要求的组织出具认证证书，认证证书的有效期最长为 3 年。

6.2.2 认证证书有效期的起算日期为认证证书签发日期，认证证书的签发日期不应早于作出认证决定的日期。

6.2.3 对于未能在原认证证书到期前完成再认证决定的，获证组织的 PIMS 认证证书到期后自动失效，直至获得新签发的再认证证书，新签发的再认证证书的终止日期不超过上一认证周期终止日期再加 3 年。

6.2.4 对每张 PIMS 认证证书应赋予一个认证证书编号，认证证书编号遵循 ZXB 制定的证书标号准则。

6.2.5 认证证书在中华人民共和国境内使用的，认证证书应使用中文。

6.2.6 认证证书的信息应真实、准确，不产生误导，并至少包含以下内容：

（ 1 ）获证组织名称、统一社会信用代码、注册地址、认证范围所覆盖的经营地址。若认证的 PIMS 覆盖多场所，应表述认证所覆盖的所有场所的地址信息；

注：认证证书中可不包括临时场所，在认证证书上展示临时场所的，应注明这些场所为临时场所。

（2）获证组织 PIMS 所覆盖的活动、服务的范围；包括每个场所相应的认证范围，且没有误导或歧义（适用时）；

（3 ）认证依据的认证标准 ISO /IEC 27701:2025《信息安全、网络安全和隐私保护-隐私信息管理体系-要求与指南》 所采用的当时有效版本的完整标准号；

（4）认证证书签发日期和有效截止日期，认证证书应注明：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；

（5 ）认证证书编号（或唯一的识别代码）；

（6）认证机构名称、地址；

（7）认证标志、相关的认可标识及认可注册号（适用时）；

（ 8 ）认证证书信息及认证证书状态的查询途径。

6.3 认证标志

认证机构自行制定的认证标志的式样、文字和名称，不得违反法律、行政法规的规定，不得与国家统一的自愿性认证标志或其他认证机构自行制定并公布的认证标志相同或者近似，不得妨碍社会管理，不得有损社会道德风尚。

ZXB 认证标志如下：

七、认证证书的暂停、撤销和注销

7.1 总则

认证机构应建立并实施认证证书暂停、撤销和注销的文件化的管理制度，不得随意暂停、撤销和注销认证证书。

7.2 认证证书的暂停

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 5 日内暂停其认证证书，并保留相应证据：

（ 1 ）PIMS 持续或严重不满足认证要求的，包括 PIMS 文件与实际业务运作严重脱离；

（2）不满足 PIMS 适用的法律法规要求，且未采取有效纠正措施的；

（ 3 ）受到与信息技术服务相关的行政处罚，且尚未完成整改的；

（4）拒绝配合市场监管部门的认证执法监督检查，或者提供虚假材料或信息的；

（5 ）持有的与 PIMS 认证范围有关的行政许可文件、资质证书等过期失效的；

（6）不能按照规定的时间间隔接受监督审核的；

（ 7 ）未按相关规定正确引用和宣传获得的认证证书和有关信息，包括认证证书和认证标志的使用；

（ 8 ）不承担、履行认证合同约定的责任和义务的；

（9）被有关行政监管部门责令停业整顿的；

（ 10）发生与信息技术服务相关重大舆情的；

（ 11 ）主动请求暂停的；

（ 12）监督审核时发现的严重不符合的纠正措施未能在 3 个月内完成验证的；

（ 13 ）其他应暂停认证证书的。

7.2.2 认证机构可根据暂停的原因和性质确定暂停期限，暂停期限最长不得超过 6 个月。

7.2.3 暂停期间，PIMS 认证证书暂时无效。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，认证机构应恢复其认证证书，并保留相应证据。

7.3 认证证书的撤销

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 日内撤销其认证证书，并保留相应证据：

（1）被注销或撤销法律地位证明文件的；

（2）被 “ 国家企业信用信息公示系统”和 “信用中国”列入严重违法失信名单的；

（3）认证证书的暂停期限已满，但导致暂停的问题未得到解决或有效纠正的；

（4）PIMS 没有运行或者已不具备运行条件的；

（5 ）其他应撤销认证证书的。

7.4 认证证书的注销

获证组织主动申请不再保持认证证书时，认证机构应确认不存在暂停或撤销情形后，注销其认证证书，并保留相应证据。

八、 申诉（投诉）处理

8.1 认证机构应建立并实施文件化的申诉（投诉）处理制度。认证委托人对认证决定有异议的，可以向认证机构提出申诉。任何组织和个人对认证过程和认证决定有异议的，可以向认证机构提出投诉。

8.2 申诉（投诉）的提交、调查和决定不应造成针对申诉人/投诉人的歧视。认证机构对申诉人（投诉人）、 申诉（投诉）事项的信息应予以保密。

8.3 认证机构应及时、公正、有效地处理申诉（投诉），采取必要的纠正措施。对申诉（投诉）的处理决定，应由与申诉（投诉）事项无关的人员作出，或经其审核和批准，并应在 60 日 内将处理结果书面告知申诉人（投诉人）。

九、信息公开与报告

9.1 认证机构应建立并实施文件化的认证信息报告制度。按照国家认监委关于认证信息上报的要求，按时上报认证相关信息，至少包括：

（1）上一年度工作报告；

（2）社会责任报告；

（3）认证计划及认证结果；

（4）认证证书的状态；

（5）其他应报告的信息。

9.2 认证机构应至少在现场审核实施前 3 日，将审核计划上报国家认监委。

9.3 认证机构在颁发认证证书后，应在次月 10 日前将认证结果相关信息报送国家认监委。

认证机构应通过其网站或者其他形式， 向公众提供查询认证证书有效性的方式，不得仅提供 “ 国家认监委”或 “全国认证认可信息公共服务平台（认 e 云）”查询路径。

9.4 认证机构应通过其网站或者其他方式公开暂停、撤销、注销认证证书的信息。暂停认证证书的，还应明确暂停的起始日期和暂停期限。认证机构应在暂停、撤销、注销认证证书之日起 2 个工作日内，按规定程序和要求将相关信息报送国家认监委。

十、认证记录

10.1 认证机构应建立文件化的认证记录、认证资料归档留存制度，记录认证活动全过程并妥善保存。 归档留存期限为认证证书有效期届满之日起 2 年以上，或被注销、撤销之日起 2 年以上。

10.2 认证记录应真实、准确、完整，以证实认证活动得到有效实施。认证记录包括但不限于：

（1）认证申请书；

（2）认证申请评审记录；

（3）认证合同；

（4）审核方案，包括多场所抽样方法（适用时）；

（5 ）确定审核时间的理由（计算过程）；

（6）审核计划；

（7）首、末次会议签到表；

（8）现场审核记录；

（9）不符合报告及验证记录；

（10）审核报告；

（11）认证决定记录。

10.3 在认证证书有效期内，认证活动参与各方签字或者盖章的认证记录、资料等，应保存具有法律效力的原件，可以纸质文件或符合《电子签名法》规定的电子文件形式保存。签字或盖章的认证记录至少包括：

（1）认证申请书；

（2）认证合同；

（3）审核计划；

（4）首、末次会议签到表；

（5）不符合报告；

（6）认证决定的结论。

10.4 认证记录应使用中文，以电子文档形式保存认证记录的，应采用不可编辑的方式。

10.5 为了证实认证活动的实施，除了认证机构要保持上述认证记录外，获证组织应留存认证证书有效期内相应的认证记录，至少包括：

（1）认证合同；

（2）审核计划；

（3）首、末次会议签到表；

（4）不符合报告及原因分析和纠正措施；

（5）审核报告；

（6）暂停、撤销通知（适用时）。

十一、其他

11.1 认证标准换版

认证机构应按照国家认监委发布的管理体系认证标准换版工作要求，落实标准的换版工作，确保认证委托人能够及时获得新版标准认证。

11.2 内部审核

认证机构应建立并实施文件化的内部审核程序，确保至少每年对 PIMS 认证开展情况实施内部审核。内部审核应包括对本规则执行情况的自查，并保持相应记录和报告。

11.3 同行评议

认证机构应积极配合国家认监委组织安排的对本机构实施的同行评议活动，并在要求的时间内对同行评议中发现的 PIMS 认证活动存在的问题采取有效的纠正措施， 以持续符合本规则的要求。

11.4 PIMS 技术服务

11.4.1 认证机构可为组织提供 ISO /IEC 27701:2025《信息安全、网络安全和隐私保护-隐私信息管理体系-要求与指南》 贯标服务，但不得代替组织编制 PIMS 文件、开展内部审核和管理评审，严禁协助组织编造虚假管理体系文件、体系运行记录等。

11.4.2 为确保没有利益冲突，参与对某组织 PIMS 技术服务的人员，2 年内不应被认证机构安排针对该组织的审核或其他认证活动。

11.5 认证数据安全

认证机构应严格落实《中华人民共和国数据安全法》和《中华人民共和国网络安全法》等法律法规要求，在中华人民共和国境内开展 PIMS 认证活动中收集和产生的重要信息和数据应当在境内存储，确保信息和数据处于有效保护和合法利用的状态。

十二、记录管理

12.1 ZXB 应当建立认证纪录保持制度，记录认证活动全过程并妥善保存。

12.2 记录应当真实准确以正式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。

12.3 记录可以用纸质或电子文档的方式加以保存。

附录 A：隐私信息管理体系认证审核时间要求

有效人数	审核时间 第1 阶段+第2 阶段 （人日）	有效人数	审核时间 第1 阶段+第 2 阶段 （人日）
≤15	6	876—1175	18.5
16—25	7	1176—1550	19.5
26—45	8.5	1551—2025	21
46—65	10	2026—2675	22
66—85	11	2676—3450	23
86—125	12	3451—4350	24
126—175	13	4351—5450	25

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）。认证范围内覆盖的非固定人员（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确定，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.认证委托人正常工作期间（包括轮班）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路途时间不计入有效的管理体系认证审核时间。

4. 审核时间的计算：低风险认证业务范围可在按照附录 A 计算所得审核时间的基础上，最多减少 10%；中风险认证业务范围应按照附录 A 计算审核时间；高风险认证业务范围应在按照附录 A 计算所得审核时间的基础上，至少增加 10%。