上海扬标认证有限公司

隐私信息管理体系认证规则

编　　号：　YB-PIMS-01/2024

版本/修改：　　A/2

受控 状态：　　受 控

分　发 号：　　01

版本/修改	编修	批准	编写/修订日期	生效日期
A/1	马汝超	毛其中	2025 年 6 月 15 日	2025 年 6 月 15 日
A/2	马汝超	毛其中	2026 年 4 月 29 日	2026 年 4 月 29 日

目录

1 适用范围

1.1 本规则用于规范上海扬标认证有限公司(以下简称“本机构”)依据相关标准在中国境内开展的隐私信息管理体系认证活动。

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，明确本机构对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 本规则是本机构在隐私信息管理体系认证活动中的基本要求，所有认证人员在该项认证活动中应遵守本规则。

1.4 本规则覆盖可颁发的证书包括：隐私信息管理体系认证证书

2 认证依据

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》

3 本机构需遵守的基本要求

3.1 坚守认证公正性，不将认证结果与审核员薪酬挂钩；对认证活动中知悉的国家秘密、商业秘密、信息承担保密义务，通过协议约束认证人员履行保密责任。

3.2 合理管控审核员工作量，单个审核员周期年内管理体系现场审核总时长不超过 180 天，超期审核结果无效，需在 1 个月内重新审核；有效证书数量与审核员数量匹配，人均不超过 50 张/周期年。

3.3 不委派未取得有效管理体系审核员注册资格的人员实施审核，不使用 “证书可在国家认监委网站查询” 等表述进行宣传。

4 对认证人员的基本要求

4.1 认证人员应当严格遵守《中华人民共和国认证认可条例》《认证机构管理办法》等认证认可相关法律法规、部门规章、规范性文件及本机构隐私信息管理体系认证各项管理制度，恪守诚实信用、客观公正、独立严谨、廉洁自律的职业操守，全面对本人参与的 PIMS 认证活动真实性、合规性与有效性承担直接责任，严禁在认证活动中存在弄虚作假、简化程序、违规判断等行为。

4.2 从事 PIMS 认证审核工作的人员，需取得国家认证认可监督管理委员会确定的注册机构

（中国认证认可协会 CCAA）核发的正式质量管理体系 QMS 审核员和信息安全管理体系 ISMS 审核员，注册证书处于有效状态且注册执业机构与本机构一致。
4.3 认证人员需严格遵守周期年现场审核时长限制，不得接受已超出年度审核时长的审核委派，严禁擅自承接未经本机构正式安排的 PIMS 认证审核项目。
4.4 认证人员应主动识别并以书面形式向本机构申报近 3 年内任职、持股、提供咨询服务、亲属关联、经济往来等可能影响认证公正性的利益冲突情形；因未履行利益冲突申报义务导致认证结果失实、不公正的，需承担经济赔偿、内部处分及配合监管调查等相应连带责任。
4.5 认证人员需按要求完成 CCAA 规定的继续教育培训，同时必须参加本机构组织的 ISO/IEC 27701:2025 标准专项培训、PIMS 专业技能培训、认证法规与公正性管控培训，所有培训需考核合格，经公司人资部审批后，方可持续从事 PIMS 认证相关工作，确保专业能力持续满足认证要求。

5 认证程序

5.1 认证申请

5.1.2 认证委托人申请 PIMS 认证，应当具备下列条件：
（1）具有合法有效的主体资格；
（2）取得法律法规要求的行政许可、资质证书（适用时），且均在有效期内；
（3）已依据 ISO/IEC 27701:2025 建立隐私信息管理体系并运行满 3 个月，完成内部审核与管理评审；
（4）因自身原因被原认证机构暂停、撤销 PIMS 管理体系认证证书的，已满 1 年；
（5）原发证机构被撤销管理体系认证资质的，已满 3 个月；
（6）未被行政监管部门责令停产停业整顿；
（7）未被列入国家企业信用信息公示系统、信用中国严重违法失信名单；
（8）近 1 年内未发生重大信息安全事件、隐私泄漏事件，未受到安全部门及相关重大行政处罚；
（9）近 1 年内国家监督抽查不合格的，已完成整改并经监管部门确认合格；
（10）符合法律法规及相关规定的其他条件。

5.1.3 认证委托人应当提交下列申请信息与文件资料：
（1）PIMS 认证申请表，包含认证委托人名称、地址、认证依据标准、申请认证范围、体系覆盖有效人数、影响体系有效性的外包过程及上下游供应商管控信息；
（2）合法主体资格证明文件，覆盖多个法律实体的，应提供各实体的证明文件；
（3）认证范围对应的行政许可文件、资质证书、强制性认证证明（适用时）；
（4）组织机构及管理职责说明；
（5）生产/服务流程、班次及轮班情况和季节性信息；
（6）隐私信息管理体系运行满 3 个月的证实材料，包括体系文件、内部审核报告、管理评审报告、运行记录；
（7）近 1 年内隐私、网络安全事件及整改验证材料（适用时）；
（8）本规则规定的其他相关资料。

5.2 申请评审

5.2.1 对认证委托人提交的申请信息和文件资料进行完整性、真实性、合规性核查，确认认证范围、隐私信息管理体系运行状态、专业能力匹配性，明确是否受理 PIMS 认证申请，并完整保存申请评审记录。

5.2.2 同时满足下列要求的，方可受理 隐私信息管理体系（PIMS）认证申请：

（1）认证委托人符合本规则 5.1.2 规定的全部申请条件；

（2）具备对应认证业务范围的审核实施能力与专业人员配置；

（3）与认证委托人就认证范围、审核安排、评审要求、费用及双方责任达成一致。

5.3 认证合同

5.3.1 隐私信息管理体系（PIMS）认证活动应当签订具有法律效力的书面认证合同，明确认证服务内容、认证费用、支付方式、履约期限、违约责任，以及认证委托人、获证组织的权利、义务与责任。认证费用应当由认证委托人直接支付，不得通过第三方代为支付。

5.3.2 认证合同应当明确，对符合认证要求的认证委托人及时颁发认证证书，对获证组织隐私信息管理体系运行情况实施有效监督，并按规定公开认证证书信息；因认证资质被注销、撤销导致获证组织 PIMS 认证证书无法有效保持的，应当及时告知并妥善处置，承担合同约定或法律认定的相应责任。

5.3.3 认证委托人应当遵守认证程序要求，如实提供全部信息与文件资料，配合认证监管部门监督检查和认证投诉调查，及时向认证实施方通报隐私信息管理体系及本规则 5.1.2 所列条件的变更情况。

5.4 审核方案和审核策划

5.4.1 审核方案

应对每一认证委托人建立认证周期内的审核方案，清晰识别并覆盖全部所需审核活动。

初次认证审核方案应包含两阶段初次认证审核、获证后的监督审核与认证到期前的再认证审核；再认证审核方案应包含再认证审核、获证后的监督审核与后续再认证审核。

初次认证审核与再认证审核应完整覆盖 ISO/IEC 27701:2025 全部条款，以及认证范围内的典型过程与业务活动；认证证书有效期内的监督审核应累计覆盖标准全部要求。

初次认证及再认证后的首次监督审核，应在认证证书签发之日起 12 个月内完成，后续监督审核间隔不得超过 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）。

针对认证委托人多班次生产、服务活动，应结合各班次管控水平策划审核覆盖范围，每次审核至少审核一个班次的现场活动，未审核班次应书面记录理由。

5.4.2 审核时间

审核时间包含现场审核时间及审核策划、文件评审、审核报告编制等非现场时间，以人日为计量单位，1 人日为 8 小时，不得通过延长单日工作时长缩减审核人日。

审核时间应以本规则附录 B 为基础，结合认证委托人有效人数、隐私信息管理体系风险类型确定，减少审核时间的比例不得超过附录 B 基准时间的 30%，现场审核时间不得低于确定总

审核时间的 80%，审核人日含小数的，调整为最接近的半人日。
隐私信息管理体系与其他管理体系实施结合审核的，总审核时间不得低于各体系单独审核时间之和的 80%。

5.4.3 多场所抽样方案

应建立文件化的多场所组织审核抽样规则，留存抽样及审核时间确定的全部记录。
多场所抽样应基于隐私信息管理体系运行风险与业务过程一致性开展评价。
相同业务、同类过程且风险等级一致的相似场所可实施抽样审核，抽样数量按以下要求计算并向上取整：
（1）初次认证审核：抽样数量 Y=√X（X 为相似场所总数）；
（2）监督审核：抽样数量 Y=0.6√X；
（3）再认证审核：抽样数量 Y=0.8√X。
业务、过程不相似的多场所，初次认证与再认证审核应逐一实施现场审核；监督审核应抽取不少于 30% 的场所，且每次审核必须覆盖核心职能部门，后续监督审核应选取不同场所。
分场所现场审核时间不得低于附录 B 确定基准时间的 50%。

5.4.4 组建审核组

应依据审核能力与公正性要求组建审核组，至少 1 名参与第一阶段审核的人员应参加第二阶段审核，审核组应满足以下配置：
（1）配备具备相应管理能力与审核技能的审核组长；
（2）配备至少 1 名与认证委托人业务范围匹配的专业人员；
（3）配备至少 1 名专职审核员，全程参与审核全过程。
技术专家仅提供专业技术支持，不实施审核活动，不计入审核人日。
实习审核员不能独立组成审核组；

实习审核员须在正式审核员指导下参与审核，不计入审核人日，数量不得超过审核组内正式审核员数量。
审核组成员不得与认证委托人存在利益关联关系。

5.4.5 审核计划

应依据审核方案制定每次现场审核计划，计划应明确审核目的、审核准则、审核范围、现场审核日期与场所、审核组成员及任务分工，标注审核人员注册信息、专业能力及工作单位。
现场审核应安排在认证委托人生产、服务活动正常运行期间实施。
现场审核开始前，应将审核计划提交认证委托人确认，需临时调整的，应经双方协商一致并留存记录。

5.5 实施审核

5.5.1 隐私信息管理体系（PIMS）认证的初次认证审核、监督审核、再认证审核及各类特殊审核，均应在认证委托人的生产、经营或服务现场实施。
5.5.2 审核过程应采用中文进行记录，审核记录应真实、完整、可追溯，可辅以图片、音视

频资料作为补充证明材料。

5.5.3 审核组应组织召开首次会议与末次会议，认证委托人的最高管理者或经书面授权的高级管理层成员应参加会议，审核组应留存会议签到记录、现场影像等证明材料；最高管理者或授权人员无故缺席的，审核应终止。

5.5.4 审核组应对认证委托人最高管理者在隐私信息管理体系中的领导作用、承诺与履职情况进行重点审核，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，包括对方针、目标、风险管控、体系推动落实等内容的掌握与执行情况，最高管理者未有效履行领导职责的，审核结论为不通过。

5.5.5 出现下列情形之一的，审核组应终止现场审核，并形成书面说明：

（1）认证委托人拒不配合审核工作，导致审核无法正常开展；

（2）认证委托人主要负责人或授权高层无故缺席首次会议、末次会议；

（3）认证委托人实际情况与申请材料、体系文件存在重大不符，影响审核结论；

（4）存在其他导致审核程序无法正常完成的情形。

5.6 初次认证审核

5.6.1 初次认证审核须分两个阶段实施，第一阶段审核与第二阶段审核的时间间隔最短不少于 5 日，最长不超过 6 个月；间隔超出最长期限的，应当重新实施第一阶段审核。

5.6.2 第一阶段审核旨在全面了解认证委托人的隐私信息管理体系建设与运行准备情况，评审体系文件与 ISO/IEC 27701:2025 标准的符合性，核实申请信息与实际情况的一致性，确认认证委托人已完成内部审核和管理评审，明确认证范围、体系覆盖有效人数与场所，核查相关合规性，最终确定是否具备开展第二阶段审核的条件，并明确第二阶段审核重点。

满足以下任意一条，第一阶段审核可采用非现场方式实施（高风险项目不适用），具体适用情形如下，：

（1）低风险类别；

（2）认证委托人已获得本机构颁发的其他领域有效管理体系认证证书（如质量管理体系、环境管理体系、职业健康安全管理体系认证证书、信息安全管理体系认证证书、信息技术服务管理体系认证证书），且体系运行成熟、无不良认证记录；

非现场审核应通过文件资料评审、线上沟通、远程核查等方式开展，确保审核深度与现场审核一致，审核组需完整留存非现场审核的相关记录（包括文件评审记录、线上沟通纪要、远程核查证据等），明确非现场审核的实施过程、审核结论及依据。 除上述可非现场实施的情形外，第一阶段审核应当在认证委托人现场实施，未在现场实施且未符合非现场适用情形的，需书面记录理由并说明原因。 第一阶段审核发现申请信息和文件资料存在虚假不实的，应当立即终止认证活动。

5.6.3 第二阶段审核必须在认证委托人现场实施，全面评价隐私信息管理体系的实际运行符合性与有效性，完整覆盖 ISO/IEC 27701:2025 标准要求，重点验证方针与目标落地、风险识别与管控、内部审核与管理评审实施、绩效监视测量、合规义务履行、管理职责落实等核心过程运行情况。

5.7 监督审核

5.7.1 监督审核用于验证获证组织隐私信息管理体系持续符合 ISO/IEC 27701:2025 标准要求且运行有效，应结合获证组织绩效、体系变更等情况实施，并访谈获证组织最高管理者，确认体系持续符合性与运行有效性。
5.7.2 每次监督审核应覆盖认证范围内的典型管控过程与业务活动，证书有效期内的全部监督审核应累计覆盖认证范围内所有典型产品、服务及管理核心过程。
5.7.3 监督审核应重点关注获证组织隐私信息管理体系的变更情况、绩效的持续改进，审核内容至少包含：内部审核与管理评审实施情况；以往审核不符合项纠正措施的落实与验证效果；隐私信息管理体系实现组织绿色目标与预期结果的有效性；持续改进策划与实施进展；管控过程的持续运作控制；隐私信息管理体系、认证范围、组织资质等重大变更情况；认证证书与认证标志的规范使用情况；相关投诉、申诉的处理情况；上一次审核后网络安全事件和隐私泄漏违规事件的调查与处置情况。
5.7.4 监督审核时间应根据获证组织有效人数、隐私信息管理体系风险类型确定，且不得少于依据本规则附录 B 确定的初次认证审核时间的三分之一。
5.7.5 获证组织认证范围包含季节性生产、服务活动的，监督审核应结合季节性特征策划，必要时分次实施监督审核，确保管控过程得到有效验证。

5.8 再认证审核

5.8.1 再认证审核应在认证证书有效期届满前实施，用于全面评价获证组织隐私信息管理体系作为整体与 ISO/IEC 27701:2025 的持续符合性，以及体系运行的持续有效性，确认是否批准继续保持认证证书。
5.8.2 再认证审核必须在获证组织现场实施，审核内容至少包含：
（1）结合内外部环境变化，确认隐私信息管理体系的适宜性、充分性、有效性及认证范围的持续相关性；
（2）隐私信息管理体系绩效持续改进的证实情况；
（3）隐私信息管理体系实现获证组织方针、目标及预期结果的有效性；
（4）风险识别、管控与环保违规预防的持续保障能力；
（5）合规义务履行、相关投诉与事件处置的持续有效性；
（6）上一认证周期内监督审核不符合项的整改与验证效果。
5.8.3 再认证审核策划应调取获证组织上一认证周期内全部监督审核报告、事件处置记录、投诉处理记录，综合评价体系持续运行效果。
5.8.4 再认证审核时间应根据获证组织当前有效人数、隐私信息管理体系风险类型确定，且不得少于依据本规则附录 B 确定的初次认证审核时间的三分之二。
5.8.5 未能在认证证书有效期届满前完成再认证现场审核的，应按初次认证程序重新开展认证活动，该情形下第一阶段审核可不在现场实施。

5.9 特殊审核

5.9.1 扩大认证范围
对已获证组织提出的隐私信息管理体系认证范围扩大申请，应进行申请评审，根据评审结果实施必要的审核活动，确认符合要求后方可批准扩大认证范围，扩大认证范围相关的审核活动可与监督审核合并实施。

5.9.2 提前较短时间通知的审核

为调查相关投诉、环保违规事件、认证范围变更，或对被暂停认证证书的获证组织进行跟踪验证，可在提前较短时间通知或不通知获证组织的情况下实施现场审核。实施此类审核前，应明确适用条件并告知获证组织，审核组指派应充分规避利益冲突，保障审核公正性。

5.9.3 获证组织认证范围内相关事项在国家监督抽查中被查出不合格的，自监管部门发出通报之日起 30 日内，应对该获证组织实施提前较短时间通知的专项审核，核实隐私信息管理体系运行有效性及整改情况。

5.10 不符合项及其验证

5.10.1 对审核中发现的不符合项，应要求认证委托人或获证组织在规定时限内开展原因分析，制定并落实对应的纠正措施。

5.10.2 应对不符合项纠正措施的有效性完成验证；轻微不符合项可由责任方制定纠正措施计划，在后续审核中一并完成验证。

5.10.3 严重不符合项的纠正措施有效性验证，应当符合下列时限要求：

（1）初次认证审核：自第二阶段审核结束之日起 6 个月内完成；

（2）监督审核：自审核结束之日起 3 个月内完成；

（3）再认证审核：在原认证证书有效期届满前完成。

5.10.4 认证委托人或获证组织未能在规定时限内完成不符合项纠正措施且未通过有效性验证的，不得作出授予认证、保持认证或再认证的决定。

5.11 审核报告

5.11.1 每次审核完成后，应向认证委托人或获证组织出具书面审核报告，审核组长对审核报告的真实性、准确性、完整性负责。

5.11.2 审核报告应客观、简明、清晰反映隐私信息管理体系运行实际状况，载明与 ISO/IEC 27701:2025 标准的符合性、运行有效性及认证推荐意见。

5.11.3 审核报告至少包含下列内容：

（1）认证实施机构名称；

（2）认证委托人或获证组织的名称、地址及授权代表；

（3）审核类型（初次认证、监督审核、再认证审核、特殊审核）；

（4）结合审核、联合审核情况（适用时）；

（5）审核准则；

（6）审核目的及完成情况确认；

（7）审核范围，包括受审核的组织、职能单元、过程、场所及审核时间；

（8）审核计划的偏离情况及理由；

（9）影响审核方案与审核结论的重要事项；

（10）审核组成员信息及同行人员信息；

（11）审核实施的日期、地点与方式；

（12）审核发现、审核证据及审核结论，重点说明管理体系管控过程、内部审核、管理评审、绩效及改进机会；

（13）上次审核后隐私信息管理体系重大变更情况（适用时）；

（14）审核组推荐意见及认证范围适宜性结论。
5.11.4 应完整留存审核证据、审核记录等支撑审核报告内容的全部资料。
5.11.5 对终止审核的项目，应出具书面终止审核报告，载明终止原因及已开展的审核工作，并送交认证委托人。

5.12 认证决定

5.12.1 应在对审核报告、不符合项纠正措施及验证结果、相关申请与运行信息进行全面复核与综合评价的基础上作出认证决定。认证决定人员应为专职人员，且不得为本次审核组成员，认证决定过程不得外包，所有认证决定必须在中华人民共和国境内作出。
5.12.2 有充分证据证明认证委托人或获证组织满足下列要求的，方可作出授予、更新或扩大认证范围的认证决定：
（1）符合本规则 5.1.2 规定的全部申请条件；
（2）严重不符合项已完成纠正措施并通过有效性验证，轻微不符合项已提交可接受的纠正措施或整改计划；
（3）隐私信息管理体系符合 ISO/IEC 27701:2025 标准要求且运行有效；
（4）已按照认证合同约定履行相关义务。
5.12.3 初次认证的认证决定应在第二阶段现场审核结束后 6 个月内完成，逾期未完成的，应在作出认证决定前重新实施第二阶段审核。
5.12.4 扩大认证范围的条件
同时满足以下条件的，方可批准扩大隐私信息管理体系认证范围：
（1）获证组织隐私信息管理体系已覆盖申请扩大的场所、产品或服务活动，并有效运行；
（2）针对扩大范围已完成必要的审核活动，确认符合 ISO/IEC 27701:2025 标准要求；
（3）获证组织当前认证证书状态正常，无未整改不符合项；
（4）扩大范围未超出获证组织法定经营范围及相关行政许可范围。
5.12.5 再认证的认证决定宜在原认证证书有效期届满前完成，最迟不得超过证书有效期届满后 6 个月。证书到期前未完成再认证现场审核，或严重不符合项未完成整改验证的，不得予以再认证，亦不得延长原证书有效期。
5.12.6 认证委托人或获证组织不满足认证要求的，应将未通过认证的原因以书面形式告知。
5.12.7 监督审核满足下列条件的，可依据审核组结论直接保持认证，无需另行独立作出认证决定：
（1）未发现严重不符合项及其他可能导致证书暂停、撤销的情形；
（2）获证组织认证信息无变更，未涉及扩大或缩小认证范围；
（3）已建立并有效运行监督审核监视机制，能够保障审核活动合规有效。

6 认证证书和认证标志

6.1 总则

6.1.1 获证组织仅可在认证证书有效状态下使用 PIMS 认证证书，并接受监督管理；认证证书处于暂停期间、被撤销或注销的，应立即停止全部使用行为。
6.1.2 获证组织应在宣传、推广活动中正确使用 PIMS 认证标志，不得在产品本体上单独标

注 PIMS 认证标志；在可分割产品包装上标注的，须同时注明获证组织通过隐私信息管理体系认证及认证实施机构名称，防止误导相关方。

6.1.3 发现获证组织存在证书、标志违规使用情形的，应要求其立即采取纠正措施，并全程跟踪验证整改效果。

6.2 认证证书

6.2.1 对通过认证评价的组织，应及时出具**隐私信息管理体系（PIMS）认证证书**，证书有效期最长为 3 年。

6.2.2 认证证书有效期自签发之日起计算，签发日期不得早于认证决定作出日期。

6.2.3 未在原认证证书到期前完成再认证决定的，原证书到期自动失效；重新核发再认证证书的，新证书有效期截止日不得超过原证书截止日加 3 年。

6.2.4 每张 PIMS 认证证书应赋予唯一编号，证书编号严格执行本规则附录 C 规定。

6.2.5 在中华人民共和国境内使用的 PIMS 认证证书，应当采用中文。

6.2.6 PIMS 认证证书信息应真实、准确、无歧义，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、认证范围覆盖的经营地址；多场所认证的，载明全部覆盖场所地址；

（2）获证组织隐私信息管理体系覆盖的产品、活动、服务范围及各场所对应认证范围；

（3）认证依据标准 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》的完整名称与标准号；

（4）证书签发日期、有效截止日期，以及须定期接受监督审核且合格后方可持续有效提示信息；

（5）认证证书唯一编号；

（6）认证实施机构名称、地址；

（7）认证标志、相关认可标识及认可注册号（适用时）；

（8）认证证书信息与状态的查询途径。

6.3 认证标志

6.3.1 自行制定的 PIMS 认证标志式样、文字、名称，不得违反法律法规规定，不得与国家统一自愿性认证标志或其他机构认证标志相同或近似，不得妨碍社会管理、有损社会道德风尚。

6.4 认证证书处置要求

（1）证书信息发生变更的，获证组织应及时申请换发证书，原证书应交回或按要求作废处置；

（2）证书暂停、撤销、注销后，获证组织应立即停止全部使用行为，不得继续以认证名义开展宣传、经营活动；

（3）遗失、损坏证书的，可申请补发，补发证书内容及有效期与原证书保持一致；

（4）任何单位和个人不得伪造、变造、出租、出借、买卖认证证书和认证标志。

7 认证证书的暂停、恢复、撤销和注销

7.1 证书暂停

7.1.1 获证组织存在下列情形之一的，应当暂停其隐私信息管理体系认证证书，暂停期限最长不超过 6 个月：

（1）隐私信息管理体系持续或部分失效，与 ISO/IEC 27701:2025 标准要求存在明显差距，不能持续保证管理体系的有效性；

（2）合规要求未持续满足，受到环保类行政处罚且未完成有效整改；

（3）发生一般及以上信息安全和隐私泄漏违规事件，未按要求开展调查处置和纠正预防；

（4）未按本规则要求接受监督审核、再认证审核，或拒绝、阻碍审核活动正常开展；

（5）认证证书、认证标志使用不符合规定要求，且未及时整改；

（6）获证组织基本信息、隐私信息管理体系、认证范围、组织架构等发生重大变更，未及时通报；

（7）未按认证合同约定履行相关义务；

（8）国家或地方相关监督抽查结果不合格，未在规定期限内完成整改验证；

（9）其他影响认证有效性和公正性，需要实施证书暂停的情形。

7.1.2 证书暂停期间，获证组织不得使用认证证书和认证标志进行宣传、投标、经营推广等活动。

7.2 证书暂停后的恢复

7.2.1 恢复条件

获证组织在暂停期限内满足以下要求的，可恢复证书有效性：

（1）已针对暂停原因完成全面整改，并提交整改证据；

（2）经验证确认隐私信息管理体系恢复有效运行；

（3）符合本规则全部适用要求，无其他应当撤销、注销情形。

7.2.2 恢复程序

（1）获证组织提交恢复申请；

（2）实施必要的沟通或文件或现场验证；

（3）作出是否恢复证书的书面决定；

（4）恢复后更新证书状态并对外公开。

7.3 证书撤销

7.3.1 获证组织存在下列情形之一的，应当撤销其隐私信息管理体系认证证书，被撤销的证书不得恢复：

（1）证书暂停期满，未完成整改或整改后仍不符合认证要求；

（2）营业执照、主体资格证明或相关法定行政许可被吊销、注销；

（3）被列入国家企业信用信息公示系统、信用中国严重违法失信名单；

（4）发生重大及以上网络安全和隐私泄漏违规事件，造成严重社会影响或重大经济损失；

（5）隐私信息管理体系长期停止运行，不再具备持续保持认证的基本条件；

（6）以欺骗、贿赂、提供虚假材料等不正当手段取得认证证书；
（7）拒绝接受监管部门监督检查，或存在严重违反认证规则的行为；
（8）获证组织主动申请撤销证书；
（9）其他应当依法依规撤销认证证书的情形。

7.4 证书注销

7.4.1 获证组织存在下列情形之一的，应当注销其隐私信息管理体系认证证书，被注销的证书不得恢复：
（1）认证证书有效期届满，未申请再认证或再认证未通过；
（2）获证组织因停业、解散、破产等原因不再持续经营；
（3）获证组织正式提出书面注销申请，且无暂停、撤销等异常状态；
（4）获证组织缩小认证范围后，原证书相应内容不再适用，需换发证书并对原证书予以注销；
（5）其他应当予以证书注销的情形。
7.4.2 证书注销后，获证组织应立即停止一切与该认证相关的宣传和标志使用行为。

7.5 信息处置

7.5.1 证书暂停、撤销、注销决定作出后，应在 2 个工作日内更新证书状态信息，并按要求向监管平台报送。
7.5.2 获证组织在证书暂停、撤销、注销后仍违规使用证书及标志的，应依法依规采取相应处置措施，并通报相关方。

8 申诉（投诉）处理

8.1 明确受理范围、处理流程、职责权限、时限要求与记录管理要求，确保对认证委托人、获证组织及相关方提出的申诉和投诉进行公正、及时、有效的处理。
8.2 受理与认证活动相关的申诉、投诉，不得向申诉人、投诉人收取处理费用，相关处理成本纳入认证服务正常支出。
8.3 收到申诉或投诉后，应在 15 个工作日内告知申诉人、投诉人受理情况；对不予受理的，应书面说明理由。
8.4 处理申诉、投诉时应实行回避制度，与被申诉、投诉事项或相关方存在利益关联的人员不得参与处理工作。
8.5 申诉、投诉处理过程应独立于审核、认证决定活动，完整留存受理登记、调查核实、处理决定、反馈记录等全过程资料，确保可追溯。
8.6 一般申诉、投诉应在 60 日内完成处理并将书面结果反馈申诉人、投诉人；情况复杂需延长处理时限的，应提前告知相关方，延长时限最长不超过 30 日。
8.7 经核实申诉或投诉成立的，应及时采取纠正、纠正措施及必要的认证处置行为，保障相关方合法权益；处理结果涉及认证证书状态变更的，按本规则第 7 章相关规定执行。
8.8 对所有申诉、投诉及处理情况进行统计分析，识别潜在问题，持续改进认证活动。

9 信息公开与报告

9.1 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 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 在颁发认证证书后，次月 10 日前将认证结果相关信息报送国家认监委，通过机构网站，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 通过机构网站公开暂停、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。
9.5 获证组织发生重大以上级别网络安全事件或隐私泄漏事件的，应对该组织的认证过程进行自查，并按照认证行政监管部门的要求，在规定的时间内提供相关认证材料。

10 认证记录

10.1 认证记录可采用纸质或电子形式，电子记录应采取防篡改、权限管控、备份等安全措施，防止记录丢失、损毁、篡改或泄露。
10.2 认证记录至少包含以下内容：
（1）认证申请资料及申请评审记录；
（2）审核方案、审核计划、审核人员专业能力与公正性评价记录；
（3）现场审核证据、审核记录、不符合项报告及纠正措施验证记录；
（4）审核报告及相关支撑材料；
（5）认证决定评审记录与认证决定文件；
（6）认证证书的申请、制作、签发、变更、暂停、撤销、注销全过程记录；
（7）监督审核、再认证审核、特殊审核的全部实施与评价记录；
（8）申诉、投诉受理与处理全过程记录；
（9）信息公开、信息报送及相关变更记录；
（10）与认证活动相关的其他重要过程记录。
10.3 认证记录应清晰、准确、规范，签署齐全，载明相关日期，能够客观反映对应认证活动的实施过程与结果。
10.4 认证记录的保存期限自认证证书有效期届满之日起计算，不得少于 3 年；涉及申诉、投诉、监管核查或法律纠纷的记录，应保存至相关事项处理完毕后再延续 3 年。
10.5 在监管部门核查、相关方合法查询时，能够及时、完整提供相应记录；未经允许不得向无关第三方提供认证记录。

11 附则

11.1 本规则术语参照 ISO/IEC 27701:2025 及认证认可法规，**隐私信息管理体系简称 PIMS**，严重不符合指影响体系实现目标的系统性失效。

11.2 本规则为认证机构内部执行及国家认监委备案文件，与法律法规冲突的，以法律法规为准。

11.3 本规则自备案通过之日起实施，由认证机构负责解释。

附录 A 隐私信息管理体系认证业务范围与风险分类

大类	中类	风险级别	中类名称	分类内容
01	政务			
	01.01	高	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	高	税务机关	
	01.03	高	海关	
	01.04	中	其他	如政党，政协，社会团体等
02	公共			
	02.01	高	通信、广播电视	
	02.02	高	新闻出版	包括互联网内容的提供
	02.03	中	科研	涉及特别重大项目的应提升为高
	02.04	中	社会保障	如社会保险基金管理、慈善团体 等。包括医疗保险
	02.05	高	医疗服务	
	02.06	低	教育	
	02.07	中	其他	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	高	金融	如银行、证券、期货、保险、资产管理等
	03.02	高	电子商务	以在线交易为主要特点，含网络游戏

	03.03	高	物流	包括邮政
	03.04	低	咨询中介	如法律、会计、审计、公证等
	03.05	中	旅游、宾馆、饭店	
	03.06	低	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	高	电力	包括发电和输、变、配电等
	04.02	高	铁路	
	04.03	高	民航	
	04.04	高	化工	
	04.05	高	航空航天	
	04.06	高	水利	
	04.07	中	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	中	信息与通信技术	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	中	冶金	
	04.10	中	采矿	含石油、天然气开采
	04.11	中	食品、药品、烟草	
	04.12	低	农、林、牧、副、渔业	
	04.13	低	其他	

附录 B 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
176 - 275	14	5451 - 6800	26
276 - 425	15	6801 - 8500	27
426 - 625	16.5	8501 - 10700	28
626 - 875	17.5	> 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）。 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 B 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 B 计算审核时间；高风险认证业务范围应在按照附录 B 计算所得审核时间的基础上，至少增加 10%。

附录 C 隐私信息管理体系认证证书编号规则

认证证书编号由认证机构代码、发证年份号、健康安全环境简写、 顺序号、认证周期、认可机构代码和子证书号构成，格式如下：

同一个组织的认证范围覆盖多个场所并需要颁发子证书时，子证 书编号为在主认证证书编号后加上“-”和序号，如-1（-2 ，-3， … … ）。

有效期内换发认证证书，认证证书编号中的机构注册号、年份号、 顺序号和认证

证书的有效期保持不变，应注明换证日期。

再认证完成后换发认证证书，按 C.1 规定重新赋予认证证书编号， 初次认证为“R0 ”，第一次再认证为 “R1 ”，第二次再认证为 “R2 ”， 依此类推。

撤销认证证书后，原认证证书编号废止，不再使用；