隐私信息安全管理体系认证实施规则

受控状态：受　控

文件编号：QP-I-66D

版　　次：　D/0

发布日期：2026 年 08 月 15 日

实施日期：2026 年 08 月 15 日

编　　制：邹恒

批　　准：蔡梅红

严禁复制 严禁复制 严禁复制

程序文件修改记录表

修改日期	修改人	修改次	原文内容	修改后内容	实施日期
2023.12.20	邹恒	A/0		新制定	2023.12.20
2026.01.09	邹恒	B/0		依据备案检查问题修订	2026.01.09
2026.04.22	邹恒	C/0	/	依据备案检查问题，和管理体系认证新规则要求	2026.04.22
2026.8.15	邹恒	D/0	/	增加管理体系要求和过程	2026.8.15

严禁复制 严禁复制 严禁复制

1. 适用范围

1.1 本认证规则适用于上海爱尚恩典认证有限公司（以下简称：ASED）开展隐私信息安全管理体系认证实施规则，本认证规则在认证双方签订合同时予以确认和采用。本规则用于规范依据 ISO/IEC 27701:2025《信息安全、网络安全和隐私保护 隐私信息管理系统 要求和指南》在中国境内开展隐私信息安全管理体系认证活动。

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，对管理体系认证实施过程作出具体规定，明确认证机构对认证过程的管理责任，保证管理体系认证活动的规范有效。

1.3 本规则是认证机构在管理体系认证活动中的基本要求，在该项认证活动中应当遵守本规则。

认证依据：

ISO/IEC 27701:2025

2. 对认证机构的基本要求

2.1 本机构获得国家认监委批准、取得从事隐私信息安全管理体系认证的资质，本规则在认监委备案后，方可开展隐私信息安全管理体系认证。

2.2 建立可满足 GB/T 27021.1《合格评定 管理体系审核认证机构要求 第一部分要求》，以使从事的隐私信息安全管理体系认证活动符合法律法规及技术标准的规定。

2.3 在开展隐私信息安全管理体系认证活动的专业范围，应具备 2 名（含）以上专业领域隐私信息安全管理体系审核员，专业领域审核员具体到大类.

2.4 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）、审核和作出认证决定等环节的相互分开。

3. 对认证人员的要求

3.1 认证管理人员包括机构主要认证规则和方案制定人员、认证人员能力评价人员、认证决定或复核人员、认证审核方案管理人员、认证申请评审人员、认证审核人员、质量负责人等：

1）应通过 ISO/IEC 27701:2025《信息安全、网络安全和隐私保护 隐私信息管理系统 要求和指南》标准知识及相关法律法规的培训，并经考试合格。

2）掌握相应管理岗位所涉及的知识和技能。

3.2 审核员：取得中国认证认可协会（CCAA）质量管理体系正式审核员资格。

上海爱尚恩典认证有限公司 程序文件 隐私信息安全管理体系认证实施规则 版本状态: D/0 生效日期: 2026-08-15 文件编号：QP-I-66D 页码: 第 3页 共 22 页

3.3 专业审核员即承担隐私信息安全管理体系专业支持的审核员:

经过确认的审核员，按照附录 A 评定专业能力，应具有相关领域与隐私信息安全管理体系认证有关的管理工作经历（包括但不限于隐私信息安全管理体系的策划、实施、运作、咨询、审核、教学经历）或隐私信息安全管理技术工作经历（在合规、内审、法务、风控等相关领域的工作经历）；专业领域审核员专业能力评定，应满足相应领域管理体系认证规则 3.6 及其释义的要求，获认可的业务范围，审核员专业领域可依据认可的相关要求进行评定，经过评价具备该领域能力。

3.4　审核组长

3.4.1 审核员至少经过 2 个项目的现场审核，经过机构评价为组长资格。

3.4.2 具备其他领域管理体系审核组长能力的审核员，经过机构对隐私信息安全管理相关知识评价合格后可评价具备组长能力。

3.5 技术专家

大专或以上学历，至少两年以上附录 A 专业涉及的隐私信息安全管理或技术工作经历，经考评合格。

3.6 认证决定或复核人员

为经本机构授权、对认证结果作出决定的人员，其中负责专业支持的专业人员具备与专业审核员或技术专家相同的专业教育与工作经历条件，经考评合格。

4. 初次认证程序

4.1 受理认证申请

4.1.1 本机构向申请认证的组织（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 申请管理体系认证，认证委托人应满足相应管理体系认证规则 5.1.2 的要求，应提供以下资料：

（1）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。认证委托人应取得合法主体资质，认证申请时管理体系运行应满 3 个月，并处于有效期；若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）；

（2）组织机构代码证书的复印件（如果已经换发了三证合一营业执照，则不用提供此材料）。

（3）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。认证委托人获得全部相关行政许可（开工所需要具备的全套前置资质文件，例如，工业产品生产许可证、特种设备、危化品运输、排污备案等）且已满三个月，并处于有效期；拟认证范围与营业执照、生产许可等行政许可文件的范围应一致，不得超范围认证。

（4）从事建筑工程、安装、勘察、监理及装饰装修、房地产开发、物业管理、特许经营、销售及有固定分支机构等组织需填写：《多现场清单》并加盖组织公章。有效的管理体系文件（手册、程序文件等，证明体系运行超过三个月）；

（5）组织管理手册、程序文件等；

（6）无手册、程序的，提供以下管理文件：

1）组织简介、确定隐私信息安全管理体系的范围、标准条款不适用说明；

2）方针、目标、管理体系组织结构图、主要过程、职责与过程/要素分配表；

3）组织过程策划、运作和控制、检验、监视和改进所需的管理文件（如工艺流程图、管理制度文件、操作规程等）；

（7）组织管理体系运行满三个月以上的证明。

（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 本机构对申请组织提交的申请资料进行审查，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信息安全管理目标而建立了文件化的隐私信息安全管理体系。

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

严禁复制 严禁复制 严禁复制 严禁复制 严禁复制

4.1.6 本机构应完整保存认证申请的审查确认工作记录，归入申请组织认证档案。

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信息安全管理体系的承诺。

（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。

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发生重大产品或服务的质量环境安全安全事故。

④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、最高管理者变更；生产经营或服务的工作场所变更；隐私信息安全管理体系覆盖的活动范围变更；隐私信息安全管理体系和重要过程的重大变更等。

⑤出现影响隐私信息安全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；不擅自利用隐私信息安全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）拟认证的隐私信息安全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。

（8）认证费用应由认证委托人向认证机构直接支付。

4.2 制定审核方案额审核策划

4.2.1　审核方案

4.2.1.1　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。

4.2.1.2　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。

严禁复制 严禁复制 严禁复制 严禁复制 严禁复制

4.2.1.3　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 隐私信息管理系统 要求和指南》所有要求，以及认证范围内的典型产品和服务。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 隐私信息管理系统 要求和指南》所有要求。

4.2.1.4　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；第一次监督审核应在证书签发日起 12 个月内进行，第二次监督审核应在证书签发日起 24 个月内进行，且两次监督审核的间隔不得超过 12 个月；再认证审核应在证书签发日起 36 个月内完成；

4.2.1.5　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隐私信息安全管理体系 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的一个班次的生产或服务的活动现场进行审核；

（2）未审核其他班次生产或服务活动现场的，应记录未审核的理由。

4.3.1 审核时间

4.3.1.1 为确保认证审核的完整有效，本机构以附录 B 所规定的审核时间为基础，根据申请组织隐私信息安全管理体系覆盖的活动范围、特性、技术复杂程度、隐私信息安全管理安全风险程度、认证要求和员工人数等情况，核算并拟定完成审核工作需要的时间。

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。

4.3.1.2 认证机构应以附录 B 所规定的审核时间为基础，考虑认证委托人有效人数、隐私信息安全管理体系风险类型等因素，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。不同业务范围参照风险类型示例见隐私信息安全管理体系风险专业小类风险分级。

4.3.1.3 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 B 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，宜将其调整为最接近的半人日数。

4.3.1.4 结合审核：隐私信息安全管理体系不予其它管理体系结合审核。

4.3.1.5 审核计划中审核范围应覆盖关键场所、过程及分场所，不超出合法主体经营范围，与申请评审的认证范围保持一致；

4.3.1.6 审核计划应经认证委托人确认，并至少在现场审核实施前 3 日上传国家认监委；

4.3.1.7 审核场所应与认证委托人注册地址、实际运营地址保持一致；注册地址与实际运营地址不一致的，应符合所在地管理要求；

4.3.2 审核组

4.3.2.1 审核组由隐私信息安全管理体系审核员组成。当无专业审核员参与时，应选择具备专业能力的技术专家参加审核组，隐私信息安全管理实习审核员，不得接受独自开展隐私信息安全管理审核活动的审核任务，审核员应取得国家认监委确定的认证人员注册机构批准的 隐私信息安全管理审核员注册资格，审核组中的审核员应承担审核责任。

4.3.2.2 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。

4.4.3 审核计划

4.4.3.1 审核组根据本机构委派，制定书面审核计划并组织实施。 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。

4.4.3.2 初次认证审核、监督、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。

如果隐私信息安全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，抽样计算方法：

(1)初次认证审核：Y=√X

（2）监督审核：Y=0.6√X;

（3）再认证审核：Y=0.8√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.

4.2.3.3 如果不同场所的活动存在根本不同，则不能采用抽样审核的方法，应当逐一到各现场进行审核。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。

4.2.3.4 分场所审核人日的计算方法参见 4.2，且现场审核时间不得少于依据附录 B 所确定的现场审核时间的 50%。

4.2.3.5 为使现场审核活动能够观察到产品生产或服务活动情况，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。

4.2.3.6 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（技术专家除外）。审核组应具备 1 名专职审核员全程参与审核过程（包括现场审核及非现场审核），颁发子证书的分场所审核员中应具备至少 1 名专职审核员；应具备至少 1 名认证业务范围内专业领域审核员或技术专家；专业领域审核员应覆盖审核项目的全部业务范围；实习审核员数量不应超过正式审核员数量，实习审核员不能独立组成审核组；审核组成员与认证委托人应无利益关系，审核组任一成员 2 年内不得为认证委托人提供过技术服务（包括咨询、培训等）；

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，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）确认申请组织实际情况与隐私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）审核申请组织有关人员理解和实施 ISO/IEC 27701:2025《信息安全、网络安全和隐私保护 隐私信息管理系统 要求和指南》标准要求的情况，评价隐私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，确认隐私信息安全管理体系是否已有效运行并且超过 3 个月。对隐私信息安全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，应当及时终止审核。

（3）确认申请组织建立的隐私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）结合隐私信息安全管理体系覆盖活动的特点识别对管理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）与申请组织讨论确定第二阶段审核安排。

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：

（1）申请组织已获本认证机构颁发的其他认证证书，认证机构已对申请组织隐私信息安全管理体系有充分了解。

（2）申请组织获得过其他经认可的认证机构颁发的有效的隐私信息安全管理体系认证证书，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，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，使申请组织有充分的时间解决第一阶段中发现的问题。

4.3.3.6 第二阶段审核应当在申请组织现场进行。重点审核隐私信息安全管理体系符合 ISO/IEC 27701:2025《信息安全、网络安全和隐私保护 隐私信息管理系统 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）在第一阶段审核中识别的重要审核点的监视、测量、报告和评审记录的完整性和有效性。

（2）隐私信息安全管理目标及实现情况。

（3）对隐私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）申请组织的隐私信息安全管理体系有重大缺陷，不符合 ISO/IEC 27701:2025《信息安全、网络安全和隐私保护 隐私信息管理系统 要求和指南》标准的要求。

（3）发现申请组织存在重大质量安全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。

4.3.4 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；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；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）。

4.3.5 未书面授权其他高级管理层参加首末次会议的，最高管理者应参加首末次会议；

4.3.6 有书面授权其他高级管理层参加首末次会议的，被授权人应参加首末次会议，并应记录最高管理者缺席理由。最高管理者或授权的高级管理层成员未参加的，应终止审核；

4.3.7 最高管理者应在二阶段审核期间接受审核组线下面对面的访谈（不可授权）；

4.3.8 任一周期年内，认证机构拥有的单一管理体系人均证书数（含有效、暂停状态）应≤50 张/周期年，且所有管理体系的人均证书数（含有效、暂停状态）也应≤50 张/周期年。

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) 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主要产品和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管理目标之间存在的差距和改进机会；
13) 行政监管部门在质量方面抽查的不合格情况，及相关原因分析和整改措施的有效性（适用时）；
14) 上次审核后发生的影响认证委托人 隐私信息安全管理体系 的重要变更（适用时 ）；
15) 获证组织对认证证书和认证标志使用的控制情况（适用时）；
16) 对以前不符合采取的纠正措施有效性的验证情况（适用时）；

严禁复制 严禁复制 严禁复制 严禁复制 严禁复制

17）已识别出的任何未解决的问题；

18）说明审核基于对可获得信息的抽样过程的免责声明；

19）审核组的推荐意见以及对申请的认证范围适宜性的结论。

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 本机构批准后将审核报告提交申请组织。

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，本机构将此报告及终止审核的原因提交给申请组织。

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，本机构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 本机构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。

1）认证委托人可以针对一般不符合制定纠正措施计划， 由认证机构在下次审核时验证。

2）严重不符合的验证时限应满足以下要求：

2.1）初次认证：在第二阶段审核结束之日起 6 个月内完成；

2.2）监督审核：在审核结束之日起 3 个月内完成；

2.3）再认证：在原认证证书到期前完成。

4.5.3 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，认证机构不应做出授予认证、保持认证或更新认证的决定。

4.6 认证决定

4.6.1 本机构认证决定人员在对审核报告、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 审核组成员不得参与对审核项目的认证决定。

4.6.3 认证决定人员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） 反映以下问题的不符合项，本机构已评审、接受并验证了纠正和纠正措施及其结果的有效性：

①未能满足隐私信息安全管理体系标准的要求。

②制定的隐私信息安全管理目标不可测量、或测量方法不明确。

严禁复制 严禁复制 严禁复制 严禁复制 严禁复制

③对实现隐私信息安全管理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在持续改进隐私信息安全管理体系的有效性方面存在缺陷，实现隐私信息安全管理目标有重大疑问。

⑤当用户根据产品标签使用投放到市场的产品或服务导致不合理的风险。

⑥产品存在显然不符合客户要求的技术参数和/或政府监管要求。

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

1）4.1.2 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 隐私信息安全管理体系 符合隐私信息安全管理体系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。

4.6.5 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。

4.6.6 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。

4.6.7 认证委托人不能满足隐私信息安全管理体系 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。

4.6.8 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。

4.6.9 在满足 4.6.3 条要求的基础上，对有充分的客观证据证明申请组织

满足下列要求的，本机构将评定该申请组织符合认证要求，向其颁发认证证书。

申请组织的隐私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。

4.6.10 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。

4.6.11 本机构在颁发认证证书后按照规定的要求将相关信息报送国家认监委。 本机构的认证证书信息可在国家认监委网站（www.cnca.gov.cn）上查询。

5．监督审核程序

5.1 本机构对隐私信息安全管理体系获证组织进行有效跟踪，监督获证组织通过认证的隐私信息安全管理体系持续符合要求。

5.2 为确保达到 5.1 条要求，本机构根据获证组织的产品或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。

5.2.1 作为最低要求，初次认证后的第一次监督审核应在认证决定日期起 12 个月内进行。第二次监督审核宜在第一次监督审核结束起 12 个月内进行。

5.2.2 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 4.3 条计算审核时间人日数的 1/3。

5.4 监督审核的审核组，应符合 3.2、3.3、3.4 条款的要求。

5.5 监督审核应在获证组织现场进行，且应满足第 4.2.3.3 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） 按 4.3.3.2 条要求已识别的重要关键点是否按隐私信息安全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） 隐私信息安全管理体系覆盖的活动涉及法律法规规定的，相关法律法规或技术标准是发生变化，是否持续符合相关规定。

（5） 隐私信息安全管理目标及各层级隐私信息安全管理目标是否实现。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。

（7） 内部审核和管理评审是否规范和有效。

（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 最高管理者或被授权的高级管理层成员应参加首末次会议，未参加的应终止审核；

5.8 最高管理者应在监督审核期间接受审核组线下面对面的访谈（不可授权）；

5.9 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。

5.10 本机构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，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 3.2、3.3、3.4 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。 在隐私信息安全管理体系及获证组织的内部和外部环境无重大变更时，再认证审核可省略第一阶段审核，但审核时间应不少于按 4.3.1 条计算人日数的 2/3。

6.3 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， 以判断获证组织的隐私信息安全管理体系 作为一个整体与 ISO/IEC 27701:2025 持续符合性和运行的有效性。

6.4 最高管理者是指认证委托人申请认证范围活动的主要负责人或决策者，可以是一个人或一组人（认证委托人仅对其某个组成部分申请认证的，最高管理者可以是该组成部分的负责人）；

6.5 未书面授权其他高级管理层参加首末次会议的，最高管理者应参加首末次会议；

6.6 有书面授权其他高级管理层参加首末次会议的，被授权人应参加首末次会议，并应记录最高管理者缺席理由。最高管理者或授权的高级管理层成员未参加的，应终止审核；

6.7 最高管理者应在审核期间接受审核组线下面对面的访谈（不可授权）；

6.8 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 隐私信息安全管理体系 有效性及认证范围的持续相关性和适宜性；

2）隐私信息安全管理体系 绩效持续改进的证实；

3）隐私信息安全管理体系 在实现获证组织目标和 隐私信息安全管理体系 预期结果方面的有效性。

6.9 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 隐私信息安全管理体系绩效，包括调阅以往的监督审核报告。

6.10 对再认证审核中发现的不符合项，应按 4.5 条要求实施纠正和纠正措施并进行验证，验证应在原证书有效期满前完成。

6.11 认证机构参照 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. 暂停或撤销认证证书

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）隐私信息安全管理体系持续或严重不满足认证要求的，包括隐私信息安全管理体系文件与实际业务运作严重脱离；

（2）不满足隐私信息安全管理体系适用的法律法规要求，且未采取有效纠正措施的；

（3）受到与质量相关的行政处罚，且尚未完成整改的；

（4）发生重大质量事故，反映获证组织隐私信息安全管理体系运行存在重大缺陷的；

（5）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；

（6）持有的与隐私信息安全管理体系范围有关的行政许可文件、资质证书、强制性认证证书等过期失效的；

（7）不能按照规定的时间间隔接受监督审核的；

（8）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；

（9）不承担、履行认证合同约定的责任和义务的；

（10）被有关行政监管部门责令停业整顿的；

（11）发生与质量相关重大舆情的；

（12）主动请求暂停的；

（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，隐私信息安全管理体系认证证书暂时无效。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）经行政监管部门确认因获证组织违规而造成产品和服务等重大质量安全事故的；

（5）隐私信息安全管理体系没有运行或者已不具备运行条件的；

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，认证机构应确认在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。

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、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 隐私信息安全管理体系 覆盖多场所，应表述认证所覆盖的所有场所的地址信息。

（2）获证组织 隐私信息安全管理体系 所覆盖的产品、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 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

严禁复制 严禁复制 严禁复制 严禁复制 严禁复制

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）证书签发日期及有效期的起止年月日。

（8）相关的认证标志、认可标识及认可注册号（适用时）。

（9）证书查询方式。除公布认证证书在本机构网站上的查询方式外，还在证书上注明：“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。

8.2 初次发证认证证书有效期最长为 3 年，再认证证书截止日期为原证书截止日期向后延长三年。

8.3 本机构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。

9. 认证证书、标志使用和处置要求

9.1　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 工程建设施工企业质量管理体系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。

9.2　获证组织可以在认证证书有效时使用 工程建设施工企业质量管理体系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。

9.3　获证组织应当在广告等有关宣传中正确使用 工程建设施工企业质量管理体系认证标志，不得在产品上仅标注 工程建设施工企业质量管理体系认证标志，只有在注明获证组织通过 工程建设施工企业质量管理体系认证及认证机构名称的情况下，方可在产品包装上标注工程建设施工企业质量管理体系认证标志。

9.4　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。

10. 与其他管理体系的结合审核

隐私信息安全管理体系不能与其它管理体系进行结合审核。

11. 受理转换认证证书

11.1 我机构认真履行社会责任，严禁以牟利为目的受理认证转换。从其它机构转换至本机构的认证申请，如原认证获得 CNAS 的认可，执行认证证书的转换控制要求，满足要求的予

以转换，否则按新客户进行受理。

11.2 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，本机构接受获证组织的申诉，并按规定的程序进行受理、并及时进行处理，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，也可以向相关监管单位投诉。

13. 认证记录的管理

12.1 本机构建立认证记录保持制度，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证实认证活动得到有效实施。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。

14. 其他

本规则内容提及 ISO/IEC 27701:2025《信息安全、网络安全和隐私保护 隐私信息管理系统 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。

15. 保密

ASED 承诺为认证客户保密（提前告知认证客户的需公开信息除外）。对认证客户的保密信息如需公开或向第三方提供时，应将拟提供 的信息提前通知认证客（法律限制除外）。

如有证据表明，ASED 因对于接触到受审核方的商业、技术秘密，泄露给第三者（法律规定除外）的，将承担相应法律责任。

16. 附录

附件　A　　隐私信息安全管理体系认证业务范围分类表

附录　B　　隐私信息安全管理体系认证审核时间要求

严禁复制 严禁复制 严禁复制 严禁复制 严禁复制

附件　A　　隐私信息安全管理体系认证业务范围分类表

编号	大类名称	大类英文名称
01	农业、林业和渔业	Agriculture, forestry and fishing
02	采矿业和采石业	Mining and quarrying
03	食品、饮料和烟草	Food products, beverages and tobacco
04	纺织品及纺织制品	Textiles and textile products
05	皮革及皮革制品	Leather and leather products
06	木材及木制品	Wood and wood products
07	纸浆、纸及纸制品	Pulp, paper and paper products
08	出版业	Publishing companies
09	印刷业	Printing companies
10	焦炭及精炼石油制品的制造	Manufacture of coke and refined petroleum products
11	核燃料	Nuclear fuel
12	化学品、化学制品及纤维	Chemicals, chemical products and fibres
13	药品	Pharmaceuticals
14	橡胶和塑料制品	Rubber and plastic products
15	非金属矿物制品	Non-metallic mineral products
16	混凝土、水泥、石灰、石膏及其他	Concrete, cement, lime, plaster etc
17	基础金属及金属制品	Basic metals and fabricated metal products
18	机械及设备	Machinery and equipment
19	电和光学设备	Electrical and optical equipment
20	造船业	Shipbuilding
21	航空航天	Aerospace
22	其他运输设备	Other transport
23	其他未另分类制造业	Manufacturing not elsewhere classified
24	回收业	Recycling
25	供电业	Electricity supply
26	供气业	Gas supply
27	供水业	Water supply
28	建设业	Construction
29	批发和零售业；汽车、摩托、个人及家庭用品修理业	Wholesale and retail trade; Repair of motor vehicles, motorcycles and personal and household goods
30	宾馆及餐馆	Hotels and restaurants
31	运输、仓储和通信业	Transport, storage and communication
32	金融中介、房地产和租赁	Financial intermediation; real estate; renting
33	信息技术	Information technology
34	工程服务	Engineering services
35	其他服务	Other services
36	公共行政管理	Public administration
37	教育	Education
38	健康和社会工作	Health and social work
39	其他社会服务	Other social services

严禁复制 严禁复制 严禁复制 严禁复制 严禁复制

附录　B　　隐私信息安全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	2.5	876-1175	13
16-25	3	1176-1550	14
26-45	4	1551-2025	15
46-65	5	2026-2675	16
66-85	6	2676-3450	17
86-125	7	3451-4350	18
126-175	8	4351-5450	19
176-275	9	5451-6800	20
276-425	10	6801-8500	21
426-625	11	8501-10700	22
626-875	12	>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全职人员，（含每个班次的工作人员）。审核时将在场的非固定人员（季节性人员、临时人员、分包商和合同人员）和兼职人员也宜包括在有效人数内。在计算有效人数时，

1）兼职人员的数量可以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量；

2）如果企业由于技术和自动化水平较低，可能雇佣大量临时的非熟练人员，这种情况下宜适当减少这些人员的数量；

3）如果相当大部分员工从事相似的简单职能，例如：运送、流水线工作、装配线、现场值守等，同样宜适当减少人员的数量；

严禁复制 严禁复制 严禁复制

4）为使计算的审核时间充分覆盖所有的业务范围，可能需要包括正常工作时间之外的审核或者适合倒班的工作模式。

注 2、调整审核时间的考虑因素　在调整审核时间时，还需要考虑下列因素（但不限于这些因素）：

1）　增加审核时间的考虑因素：　认证机构在进行多场所审核时；

在业务方面，受法规管制的程度较高（例如金融、电力、电信、公共服务领域）；

在认证审核过程中，工作语言超过一种的（需要翻译或影响审核员个人独立工作）；复杂的后勤条件，在体系范围内涉及到不止一座建筑物或一处工作地点；体系覆盖了高度复杂的过程或相对数量大或独特的活动；审核活动中需要访问临时场所，以确定固定场地的管理体系达到认证的要求。

2）　减少审核时间的考虑因素：体系成熟；业务过程低风险；对客户管理体系已有的了解（例如本中心已依据另一标准认证了该客户）；客户为认证所作的准备（例如已经获得另一个第三方合格评定制度的认证或承认）；

3）被确定为低风险认证业务类别的，认证审核活动可根据需要在按照附录 B 计算所得审核时间的基础上，最多减少 10%；被确定为中风险认证业务类别的，认证审核活动应按照附录 B 计算审核时间；被确定为高风险认证业务类别的，认证审核活动应在按照附录 B 计算所得审核时间的基础上，至少增加 10%。

活动的复杂程度低，例如

过程仅包含单一的一般性活动（例如仅包含服务）；以往审核（内部审核和认证机构审核）显示，所有班次都实施相同的活动，且有适当证据表明所有班次的表现相同；相当一部分员工从事相似的简单职能；

有一部分员工在组织的场所外工作，例如销售人员、司机、服务人员等，并且有可能通过记录审查来对其活动是否符合体系要求进行充分地审核。

本规则由上海爱尚恩典认证有限公司负责解释。

以下无内容

严禁复制 严禁复制 严禁复制 严禁复制 严禁复制

隐私信息安全管理体系认证证书

兹证明

XXXXXXXX 有限公司

注册地址：XXXXXXXXXXXXXXXXXXX

经营地址：XXXXXXXXXXXXXXXXXXX

其隐私信息安全管理体系已通过上海爱尚恩典认证有限公司的评审，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系统 要求和指南》标准

认证范围

XXXXXXXXXXXXXXXXXX

适用性声明：

认证证书编号：XXXXXXXXXXXXXXX

统一社会信用代码：XXXXXXXXXXXXXXX

本次证书发证日期：20XX 年 XX 月 XX 日

本次证书有效日期：20XX 年 XX 月 XX 日

认证经理：

第一次监审

20XX. XX 贴标

第二次监审

20XX. XX 贴标

本证书由上海爱尚恩典认证有限公司颁发，获证组织应在证书有效期内按规定执行年度监督审核，如到期未执行的，爱尚恩典有权收回该证书。认证资格是否有效可以登录 www.ascendchina.com.cn 查询。证书信息亦可在国家认监委网站 http://cx.cnca.cn 上查询。

爱尚恩典认证

地址：中国（上海）自由贸易试验区新金桥路 58 号银东大厦 28A 座

严禁复制 严禁复制

Privacy Information Security Management System Certification

To Certify

XXXX Co. , Ltd.

Registered Address: XXXXXXXXXXXXXXXXX
Business Address: XXXXXXXXXXXXXXXXX

Its Privacy Information Security Management System has passed the certification review of ASED, to meet

ISO/IEC27701:2025《Information security, cybersecurity and privacy protection—Privacy information management systems— Requirements and guidance》 Standard

Scope of approval

XXXXXXXXXXXXX

Statement of applicability:

Certificate number: XXXXXXXXXXXXX
Unified credit social code: XXXXXXXXXXXXX
Certificate of the issuance date: XX XXX 20XX
Certificate of the effective date: XX XXX 20XX
The authentication manager: _____

First supervision and examination: effective after labeling on 20XX.XX

Second supervision and examination: effective after labeling on 20XX.XX

This certificate issued by Shanghai Ascend Certification&Technical Co.,Ltd. The certificate is only valid with related permits when appropriated. The certificated organization must successful pass the annual surveillance audit to maintain the validity after the certificated approval date. It should be returned if the management system of certificated organization to fail to be in conformity with the certification standard. The effectiveness of the certification qualification can be log on www.ascendchina.com.cn to query. Certificate information also can inquire on http://cx.cnca.cn by national certification and accreditation.

Ascend Certification

Address:28A Yindong building,No.58,Xinjinqiaoroad,Pudong,Shanghai(China free trade area)