隐私信息管理体系
认证实施规则

（ICAS-PIMS-2020　V1.3）

2020 年 11 月 11 日发布　　2020 年 11 月 11 日实施
2026 年 4 月 28 日修订并发布

目录

1 适用范围

- 本规则适用于上海英格尔认证有限公司（以下简称 ICAS）对申请认证和获证的各类组织开展隐私信息管理体系的认证活动。
- 本规则依据认证认可相关法律犯规，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 ICAS 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。

2 认证依据

ISO/IEC 27701:2025 信息安全、网络安全和隐私保护一隐私信息管理体系一要求与指南

3. 认证程序

3.1 认证申请

3.1.1 ICAS 应向申请认证的组织（以下简称认证委托人）至少公开以下信息：

（1）可开展隐私信息管理体系认证业务的范围，以及获得认可的情况。

（2）认证授予、保持、扩大、缩小、暂停或撤销的工作程序。

（3）认证证书样式。

（4）申诉、投诉程序。

（5）分支机构和办事机构的名称、业务范围、地址等。

3.1.2 ICAS 应当要求认证委托人提交以下资料：

（1）隐私信息管理体系认证申请书。

（2）法律地位的证明文件的复印件（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。若隐私信息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）隐私信息管理体系覆盖的活动所涉及法律法规要求的相关证书等的复印件（适用时）。

（4）隐私信息管理体系适用的相关法律、法规、标准和规范清单。

（5）多场所和外包情况说明（适用时）。

（6）隐私信息管理体系已有效运行 3 个月以上的证明材料。

（7）其他与认证审核有关的必要文件。

3.2 申请评审

ICAS 应对认证委托人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。申请条件应包括但不限于以下：

（1）隐私信息管理体系已有效运行 3 个月以上，体系运行期间及建立体系前的一年内未受到主管部门严重的行政处罚；

（2）申请范围不超出资质许可范围、不超过 ICAS 业务范围；

（3）取得国家、地方市场监督管理部门或有关机构注册登记的法人资格（或其组成部分）；

（4）未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”的企业；

（5）至少完成一次隐私信息管理体系内部审核，并进行了管理评审。

对于申请材料齐全、符合要求的，ICAS 可决定受理认证申请；对不符合上述要求的，ICAS 应通知认证委托人补充和完善，或者不受理认证申请。

ICAS 应完整保存认证申请的审查确认工作记录。

3.3 签订认证合同

在实施认证审核前，ICAS 应与认证委托人签订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）认证委托人获得认证后持续有效运行隐私信息管理体系的承诺。

（2）认证委托人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）认证委托人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受到主管部门行政处罚。

③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；隐私信息管理体系覆盖的活动范围变更；隐私信息管理体系和重要过程的重大变更等。

④出现影响隐私信息管理体系运行的其他重要情况。

（4）认证委托人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管理体系认证证书和相关文字、符号误导公众。

（5）拟认证的隐私信息管理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，认证机构和认证委托人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。合同里应明确认证费用应由认证委托方向 ICAS 直接支付。

3.4 审核准备

3.4.1 审核策划

ICAS 根据认证委托人的规模、特性、隐私信息安全的复杂程度和业务类别的风险程度等因素对认证全过程进行策划，制定审核方案。

3.4.2 审核组

（1）审核组内至少有一名隐私信息管理体系的专职审核员全程参与审核过程；

（2）审核组内的审核员应取得 CCAA 注册的信息安全管理体系审核员资格，并经 ICAS 考核评价后取得隐私信息管理体系审核员资格；审核组成员的专业能力经 ICAS 评定并满足要求；

（3）审核组由审核组长和审核员组成，并至少有一名相应认证业务范围的隐私信息管理体系专业审核员。审核小组如果仅有一名审核员，该审核员应有能力履行适用于该审核的审核组长职责并有能力完成满足整个审核组的能力要求。

（4）必要时，可以配备技术专家，以保证审核组的整体能力覆盖组织的隐私信息安全管理体系范围所

需的专业审核能力要求。审核组中每一位审核员不必具有同样的能力，但是审核组的整体能力需要足以实现审核目标。

（5）审核员承担审核责任；技术专家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负责指导的正式审核员承担责任；实习审核员在审核员的指导下参与审核，不计入审核时间。

3.4.3 审核时间

ICAS 应制定确定审核时间的文件。

ICAS 根据认证委托人隐私信息管理体系覆盖的范围、特性、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，以确保认证审核的完整有效。

a、审核时间包括在客户场所的现场时间，以及在现场以外实施策划、文件审查、与客户人员之间的相互活动和编写报告等活动的时间。旅途（往返途中或在场所之间的途中）以及其他任何中断休息不能计入现场的管理体系认证审核时间。

注：我国除香港特别行政区、澳门特别行政区、台湾地区外，审核时间通常不包括旅途时间和午饭时间。

b、审核时间以人日计，1 人日为 8 小时，在策划阶段，不宜通过增加每个工作日的工作小时数来减少审核人日数。

c、实施现场审核的时间通常不宜少于审核时间的 80%。

注：此处所述的现场审核时间不包括第一阶段在现场实施的文件审查所用时间。

d、通常情况下，第一阶段现场审核所需的审核时间不多于初次认证审核总的现场审核时间的 30%。

e、根据拟审核客户的认证领域，按照确定的审核时间，可根据客户隐私信息管理的具体实施情况及其他因素等，对审核时间进行调整。审核时间进行调整时，减少量不应超过 30%，增加/减少人天的理由（必要时包括证据）应予以记录并保留。

f、若隐私信息管理体系与其他管理体系进行结合审核时，若组织的一体化程度成熟度高，酌情减少审核人日，但最多减少量不得多于 20%。

3.4.4 审核计划

ICAS 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。在现场审核活动开始前，审核计划应经认证委托人确认和接受。若认证委托人对审核计划提出异议且合理时，应对审核计划进行调整。若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认证委托人，并协商一致。

3.4.5 多场所

通常情况下，初次认证审核、监督审核和再认证审核应在认证委托人申请认证的范围涉及到的各个场所现场进行。

如果隐私信息管理体系覆盖范围包含在多个场所进行相同或相近的活动，且这些场所都处于认证委托人授权和控制下，ICAS 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所抽样本进行的审核对隐私信息管理体系包含的所有场所具有代表性。如果不同场所的活动存在明显差异、或不同场所存在可能对隐私信息管理有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。

3.5 实施审核

隐私信息管理体系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。

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、隐私信息管理体系相关职能部门负责人应参加首、末次会议，ICAS 保留首末次会议签到记录及相关图片/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。

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隐私信息管理体系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

3.6 初次认证审核

3.6.1 初次认证审核，分为一、二阶段实施审核。

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。如果需要更长的时间间隔，应重新实施第一阶段审核。

3.6.2 一阶段审核

一阶段审核的目的是调查申请人是否已具备实施认证审核的条件和确定二阶段审核的关注点。

一阶段审核应至少覆盖以下内容：

（1）审核认证委托人隐私信息管理体系的体系文件；

（2）结合现场情况，确认认证委托人实际情况与隐私信息管理体系文件描述的一致性，特别是体系文件中描述的环境、范围、部门设置等是否与认证委托人的实际情况相一致。

（3）审核认证委托人有关人员理解和实施 ISO/IEC27701 标准要求的情况，评价隐私信息管理体系运行过程中是否实施了内部审核与管理评审，确认隐私信息管理体系是否已有效运行并且超过 3 个月。

（4）确认认证委托人建立的隐私信息管理体系覆盖的活动内容和范围、体系覆盖范围内有效人数、活动过程和场所，遵守相关法律法规及强制性标准的情况。

（5） 结合隐私信息管理体系覆盖活动的特点，识别对隐私信息目标的实现具有重要影响的关键点，并结合其他因素，确定重要审核点。

（6）与认证委托人讨论确定第二阶段审核安排。对隐私信息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，以及其他不具备二阶段审核条件的，不应实施二阶段审核。

在下列情况，一阶段审核可以不在认证委托人现场进行，但应记录未在现场进行的原因：

（1）认证委托人已获本认证机构颁发的其他有效认证证书，ICAS 已对认证委托人隐私信息管理体系有充分了解。

（2）ICAS 有充足的理由证明认证委托人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。

（3）认证委托人获得过其他经认可的认证机构颁发的有效的隐私信息管理体系认证证书，通过对其

文件和资料的审查可以达到一阶段审核的目的和要求。

除以上情况之外，一阶段审核应在认证委托人的生产经营或服务现场进行。

审核组应将一阶段审核情况形成书面文件告知认证委托人。对在二阶段审核中可能被判定为不符合项的重要关键点，要及时提醒认证委托人特别关注。

3.6.3 二阶段审核

二阶段审核应在具备实施认证审核的条件下进行，一阶段审核提出的影响实施二阶段审核的问题应在二阶段审核前得到解决。

二阶段审核的目的是评价认证委托人管理体系实施的符合性和有效性，判断是否推荐认证注册。

二阶段审核应当在认证委托人现场进行。重点是审核隐私信息管理体系符合 ISO/IEC27701 标准要求和有效运行情况，应重点关注但不限于以下方面的内容：

（1）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）为实现隐私信息目标而在相关职能、层次和过程上建立的隐私信息目标是否具体适用、有针对性、可测量并可实现。

（3）认证委托人隐私信息体系的建立和实施。

（4）认证委托人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。

（5）认证委托人的内部审核和管理评审是否有效。

3.7 监督审核

ICAS 应对持有其颁发的隐私信息管理体系认证证书的组织（以下称获证组织）进行有效跟踪，监督获证组织持续运行隐私信息管理体系并符合认证要求。

3.7.1 监督审核的频次

ICAS 应根据获证组织的隐私信息风险程度或其他特性，确定对获证组织的监督审核的频次。监督审核应至少每年进行一次。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，第二次监督审核在认证证书签发之日起 24 个月内进行，且距离上次审核结束不超过 12 个月。超过期限而未能实施监督审核的，应按暂停处理。

在获证组织的隐私信息管理发生重大变化或发生影响隐私信息管理绩效的重大事故时，ICAS 应视情况增加监督审核的频次，以保证监督审核的有效性。

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。

超过期限而未能实施监督审核的，应按暂停、撤销处理。

监督审核的审核组，应符合 3.4.2 的要求。

3.7.2 监督审核时应包括但不限于以下内容：

（1）上次审核以来隐私信息管理体系覆盖的活动及运行体系的资源是否有变更。

（2）已识别的重要关键点是否按隐私信息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）总隐私信息目标及各层级隐私信息目标是否实现。如果没有实现，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）针对体系运行过程中发现的问题或投诉，及时制定并实施了有效的改进措施。

3.7.3 监督审核结果评价

监督审核的审核报告，应按审核要求逐项描述或引用审核证据、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。

ICAS 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。

3.8 再认证

隐私信息管理体系的认证证书有效期为 3 年。

3.8.1 认证证书期满前，若获证组织申请继续持有认证证书，在认证证书有效期满前 3 个月，向 ICAS 提出再认证申请，并提交相关资料。ICAS 将实施再认证审核，以评价获证组织是否持续满足隐私信息管理体系标准和相关法律法规等的要求，决定是否延续认证证书。

3.8.2 再认证的审核程序与初次认证审核程序基本相同。在隐私信息管理体系及获证组织的内部和外部环境无重大变更时，再认证可省略第一阶段审核。

3.8.3 再认证审核重点关注以下的内容：

(1) 结合内部和外部环境的变化情况，判断认证委托人隐私信息管理体系的有效性和认证范围的持续适宜性；

(2) 获证组织在本认证周期内的管理绩效；

(3) 本认证周期内，获证组织隐私管理体系的运行是否促进了管理方针和目标的实现。

3.8.4 ICAS 根据再认证审核结果做出决定。对再认证审核中发现的不符合项，ICAS 将按 3.10 条要求实施纠正和纠正措施并进行验证，验证在原证书有效期满前完成。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。

3.9 特殊审核

3.9.1 扩大认证范围

获证组织拟变更认证范围（如：扩大认证范围等）时，应向 ICAS 提出申请，并按要求提交相关资料。

ICAS 根据获证组织的申请进行评审，策划和实施适宜的审核活动，并做出是否可予扩大的认证决定。这些审核活动可单独进行，也可与获证组织的监督审核或再认证一起进行。

3.9.2 提前较短时间通知的审核

为调查投诉、企业安全事故、对变更做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：

（1）ICAS 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，ICAS 应在指派审核组时给予更多的关注。

（3）获证组织在发生安全事故的，自安全监管部门发布通报之日起 30 日内，须对该组织实施专项监督审核。

3.10 不符合项及其验证

3.10.1 对审核中发现的不符合项，ICAS 应出具书面不符合报告，要求受审核方规定的时限内进行原因分析，采取相应的纠正措施。时限由审核组与受审核方协商确定，但轻微不符合项最长时限不超过一个月（初次认证时限三个月），严重不符合项最长时限不可超过 3.10.3 规定的时限。

3.10.2 ICAS 对受审核方所采取的纠正措施的有效性进行验证。受审核方可以针对轻微不符合制定纠正措施计划，由 ICAS 在下次审核时验证。

3.10.3 严重不符合的验证时限应满足以下要求：

（1）初次认证：最长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。

3.10.4 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。

3.11 审核报告

审核组应对审核活动形成书面审核报告，由审核组长签字。审核报告应对认证委托人隐私信息管理体系的符合性和有效性进行全面描述和评价，至少包括以下内容：

（1）认证委托人的名称和地址。

（2）认证委托人活动范围和场所。

（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，包括固定现场和临时现场；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）叙述审核程序及各项要求的审核工作情况，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；对隐私信息管理目标实现情况进行评价。

（7）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，准确、具体、清晰描述，易于被认证委托人理解。不得用概念化的、不确定的、含糊的语言表述不符合项。

（8）审核组对是否通过认证的意见建议。

3.12 认证决定

3.12.1 ICAS 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的基础上，做出认证决定。审核组成员不得参与对审核项目的认证决定。

对于符合要求的认证委托人，ICAS 向其颁发隐私信息管理体系认证证书；对于不符合要求的认证委托人，ICAS 应以书面的形式告知其未通过认证的原因。

3.12.2 ICAS 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）提出隐私信息管理体系认证申请时，认证委托人应具备的条件；

（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管理体系符合 ISO/IEC 27701 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。

3.12.3 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。

3.12.4 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，ICAS 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。

3.12.5 认证委托人不能满足 3.12.2 要求的，ICAS 应告知其未通过认证的原因。

4 认证证书和认证标志

4.1 总则

1）ICAS 制定认证证书及标志的控制程序，规定正确使用隐私信息管理体系认证证书和**认证标志**的要求。

2）获证组织可以在认证有效期内使用隐私信息管理体系认证标志和相关认可标识，并接受 ICAS 的监督管理。

3）获证组织应当在有关宣传中正确使用隐私信息管理体系认证证书和认证标志，不得在产品上仅标注隐私信息管理体系认证标志而不注明组织通过隐私信息管理体系认证及认证机构名称。

4）ICAS 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。

4.2 认证证书

4.2.1 ICAS 应及时向认证决定符合要求的组织出具认证证书，认证证书的签发日期不应早于做出认证决定日期。

4.2.2 隐私信息管理体系认证证书有效期最长为三年。

4.2.3 对于未能在原认证证书到期前完成再认证决定的，获证组织的隐私信息管理体系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。

4.2.4 ICAS 对每张隐私信息管理体系认证证书赋予一个认证证书编号，认证证书编号应遵循 ICAS 制定的认证证书编号规则；隐私信息管理体系 认证证书编号由 ICAS 机构代码、发证年份号、隐私信息管理体系简写、顺序号、认证周期、认可机构代码和子证书号构成，格式如下：

XXXX XX A XXXX R0（1、2、… ）XX -X。

4.2.5 ICAS 的隐私信息管理体系认证证书在中华人民共和国境内使用的，应使用中文版本。

4.2.6 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) 认证证书名称，即隐私信息管理体系认证证书；

(2) 认证证书编号；

(3) 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

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；

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。

(4) 隐私信息管理体系认证覆盖的范围；

(5) 认证依据，隐私信息管理体系的认证标准 ISO/IEC 27701 所采用的当时有效版本的完整标准号；

(6) 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；；

(7) 认证机构的名称、地址；

(8) 认证证书签发人或其授权人的签字；

(9) 认证标志、相关的认可标识及认可注册号（适用时）；

(10) 证书信息及证书状态的查询途径：

ICAS 在证书上注明：“证书信息及有效性可在国家认监委官方网站(www.cnca.gov.cn)上查询，也可通 过登录英格尔官方网站或致电英格尔客户服务部进行查询。”

4.3 认证标志及使用要求

4.3.1 ICAS 自行制定的认证标志的式样、文字和名称，不违反法律、行政法规的规定，不与国家推行的认证标志相同或者近似，不妨碍社会管理，不有损社会道德风尚。

4.3.2 认证标志

隐私信息管理体系认证标志

ISO/IEC 27701

4.3.3 ICAS 制定认证标志的使用规则，授权获证客户只能在证书有效期内以及已获认证的范围内，有条件使用 ICAS 认证证书及其认证标志。获准使用的认证标志必须完整，不得将其变形使用。ICAS 对获证客户是否正确使用认证证书及其认证标志进行监督。

4.3.4 ICAS 的认证证书及其认证标志可以展示在文件、网站、已被认证的工作场所、销售场所、广告和宣传资料中，但不可利用管理体系认证证书和相关文字、符号，误导公众认为认证证书覆盖范围外的管理体系，或产品、服务获得了认证。企业必须在使用标识的同时，声明本企业通过相应的管理体系认证，不得误导使用者认为该标识为产品认证标识或服务认证标识。

4.3.5 获证客户可以在相应的管理体系认证证书覆盖的业务范围内在相关场合有条件的使用 ICAS 认证标志。如在有关文件、办公场所、销售场所和出版物上使用。

5 认证证书的暂停、恢复、撤销、注销和缩小范围

ICAS 建立认证授予、拒绝、保持、变更、暂停、恢复、撤销和注销的管理程序，对认证资格进行暂停、

撤销和注销等进行管理，按规定处理证书的暂停、撤销和注销。

5.1 认证证书的暂停

5.1.1 获证组织存在但不限于以下情况的，ICAS 应在调查核实后暂停其认证证书：

(1) 获证组织的隐私信息管理体系持续或严重不满足认证要求，包括对隐私信息管理体系运行有效性的要求；

(2) 不满足隐私信息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) 获证组织不承担、履行认证合同约定的责任和义务的；

(4) 被监管部门发现获证组织的体系运行存在问题，或责令停业整顿；

(5) 持有的行政许可证明、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) 获证组织主动请求暂停；

(9) 其他应当暂停认证证书的。

5.1.2 ICAS 将公开暂停的认证证书的信息，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。认证证书暂停期最长不超过 6 个月。

5.2 暂停恢复

如获证组织在暂停期间采取有效的纠正措施，造成暂停的原因已经消除，并且提供了有效的证据的，本机构经评审符合要求后，可恢复获证组织的认证证书。

5.3 认证证书的撤销

获证组织存在但不限于以下情况的，认证机构应在调查核实后撤销其认证证书：

(1) 获证组织的法律地位证明文件被注销或撤销的；

(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) 获证组织拒绝配合监管部门实施的监督检查，或对有关事项的询问和调查提供虚假材料或信息；

(4) 获证组织存在严重违反法律法规的行为；

(5) 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；

(6) 获证组织没有运行隐私信息管理体系，或已不具备运行隐私信息管理体系的条件的；

(7) 其他应该撤销认证证书的。

5.4 认证证书的注销

获证组织主动申请不再保持认证资格时，ICAS 注销其认证资格，并保留相应证据。

5.5 缩小认证范围

如果获证组织在认证范围内的某些部分持续地或严重地不满足认证要求，认证机构应缩小其隐私信息管理体系的认证范围，以排除不满足要求的部分。认证范围的缩小应与认证标准的要求一致。

ICAS 应在其网站上公布相关暂停或撤销认证证书的信息，并按规定程序和要求上报国家认监委。

ICAS 应采取有效的措施如日常监督确认等，以确保在暂停期间或撤销证书之后，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。

在任何组织提出请求时，ICAS 应正确说明获证组织的隐私信息管理体系认证证书被暂停、撤销或缩小的情况。

6 认证记录的管理

6.1 ICAS 将根据 ICAS05C《记录控制程序》对记录进行控制，记录认证活动全过程并妥善保存。

6.2 记录应当真实准确以证实认证活动得到有效实施。归档留存时间为两个认证证书有效期届满或者被注销、撤销之日起 2 年以上。

6.3 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。

7 申诉、投诉处理

ICAS 建立申诉、投诉处理程序，对申投诉的处理流程、处理要求做出规定。

受审核方或认证委托人对认证决定有异议的，可在 10 个工作日内向 ICAS 提出申诉。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。ICAS 对申诉人（投诉人）、申诉（投诉）事项的信息应予以保密。

ICAS 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）事项无关的人员做出，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）。

认为 ICAS 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。

8 信息公开与报告

8.1 ICAS 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）认证计划及认证结果；

（2）认证证书的状态；

（3）其他应报告的信息。

8.2 ICAS 应至少在审核实施前 3 天，将审核计划上报国家认监委相关网站，并应在上报认证证书信息的同时，上报管理体系审核结果信息。

8.3 ICAS 在颁发认证证书后，在 30 个工作日内，将认证结果相关信息报送国家认监委。ICAS 应通过公司网站或者其他形式，向公众提供查询认证证书有效性的方式。

8.4 ICAS 通过网站或者其他方式公开暂停、撤销、注销认证证书的信息，暂停证书的，还应明确暂停的起始日期和暂停期限。ICAS 应在暂停、撤销、注销认证证书之日起 2 个工作日内，按规定程序和要求报国家认监委。

9 对获证组织的信息通报要求及响应

9.1 为确保获证组织的隐私信息管理体系持续有效，ICAS应要求获证组织建立信息通报制度，及时向ICAS

通报以下信息：

(1) 业务、地点、组织机构变化等情况的信息（及时通报）；

(2) 组织的体系文件、隐私信息的变化；

(3) 影响隐私信息管理绩效实现的重大事故信息（及时通报）；

(4) 其他重要信息。

9.2 ICAS 应对上述信息以及收集到的相关公共信息进行分析，视情况采取相应措施，包括增加监督的审核频次和暂停或撤销认证证书。在发生影响隐私管理绩效实现的重大事故时，ICAS 需立即采取措施。

10 其他

本规则内容提及 ISO/IEC27701 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。