北京中瑞泰纳凯新认证有限公司

Beijing Cotecna Kaixin Certification Co., Ltd.

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：KCB-GZ-20

发布日期：2022-03-01

修订日期：2026-03-31

实施日期：2026-04-01

版　　次：H2

批准发布：赵舒芳

1. 适用范围

1.1 本规则用于规范机构对用于“隐私信息安全管理体系”开展的认证活动。

注：本规则以下内容中以“PIMS”指代“隐私信息安全管理体系”，“PII”为英语（Personally Identifiable Information）的缩写，可译为“个人可识别信息”。

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 ISO 27701 隐私信息安全管理体系认证实施过程做出具体规定，本机构从事该项认证活动的各项职能均应当遵守本规则，以保证认证活动的规范有效。

2. 对认证审核人员的基本要求

2.1 隐私信息安全管理体系 ISO 27701 是信息安全管理体系 ISO 27001 在隐私信息安全管理方面的扩展。认证审核员应当具有中国认证认可协会（CCAA）确认的 ISO 27001 信息安全管理体系审核员注册资格。

2.2 认证人员应当经过 ISO 27701 隐私信息安全管理体系标准的培训、考核，考试合格后才可从事此项认证审核活动。

2.3 认证人员还要学习掌握相关的法律法规及专业知识，对任何关于客户的专有的未加公布的信息予以保密。

3. 认证依据

ISO/IEC 27701-2019《安全技术 - ISO/IEC 27001 和 ISO/IEC 27002 的隐私信息管理扩展 - 要求和指南》

4. 初次认证程序

4.1 受理认证申请

4.1.1 申请方申请的基本条件

（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，依据国务院办公厅发布的现行《法律、行政法规、国务院决定设定的行政许可事项清单》），并处于有效期内；

（3）已按认证标准建立管理体系，且运行满三个月；

（4）当前未被行政监管部门责令停产停业整顿；

（5）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；

（6）其他应具备的条件。

4.1.2 本机构要求申请组织提交以下资料：

（1）认证申请书，申请书应包括申请认证的 PIMS 范围及其涵盖的"隐私信息安全管理体系”有效人数。若组织使用了其他管理体系，还应说明 PIMS 与这些管理体系的关系。

（2）法律地位的证明文件的复印件。若“隐私信息安全管理体系”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）PIMS 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。

（4）有效的管理体系文件以及运行满 3 个月的证据，例如：PIMS 范围、策划如何实现隐私信息安全管理体系管理计划和业务连续性方案时所形成的文件等。

（5）与隐私信息安全利用和管理相关的法规要求。

（6）PIMS 认证范围内的隐私信息安全业务类型。

（7）PIMS 认证范围内的隐私信息安全业务类型的风险水平。

4.1.3 合同体系认证部对申请组织提交的申请资料进行评审，根据申请认证的 PIMS 活动范围及场所、管理体系 的有效人数、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。

4.1.4 对符合 4.1.1、4.1.2 要求的，可决定受理认证申请并实施合同评审；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。

4.1.5 签订认证合同

通过合同评审后，实施认证审核前，申请评审人员应与认证申请方签署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 PIMS 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，应及时向机构通报：

a） 客户及相关方有重大投诉；

b） PIMS 认证范围覆盖的业务活动被相关监管部门认定不合格；

c） PIMS 认证范围覆盖的业务活动发生重大事件。

d） 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；PIMS 覆盖范围的变更；PIMS 和重要管理过程的重大变更等。

e） 出现影响 PIMS 正常运行的其他重要情况。

f） 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，不利用 PIMS 认证证书和相关文字、符号误导公众认为其业务活动通过认证。

g） 在认证审核实施过程及认证证书有效期内，本机构和申请组织各自应当承担的责任、 权利和义务。

h） 认证服务的费用、 付费方式及违约条款。

4.2 策划审核

4.2.1 审核时间

4.2.1.1 为确保认证审核的完整有效，应以附录 A 所规定的审核时间为基础，根据申请组织 PIMS 覆盖范围的业务活动与个人可识别信息相关性的复杂程度以及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。

4.2.1.2 整个审核时间中， 现场审核时间不应少于总审核时间的 80%。

4.2.2 审核组

4.2.2.1 体系认证部应当根据 PIMS 规模和复杂程度选择具备相关能力的审核员组成审核组。审核组中的审核员承担审核任务和责任。审核组至少包括 1 名专职审核员，并确保该专职审核员全程参与管理体系认证审核活动。

4.2.3 审核计划

4.2.3.1 审核组应为每次审核制定书面的审核计划（第一阶段审核不要求正式的审核计划）。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。

4.2.3.2 如果 PIMS 覆盖范围包括在多个场所进行相同或相近的活动，且这些场所都处于申请组织授权和- 控制下，审核组可以在审核中对这些场所进行抽样， 但应根据相关要求实施抽样以确保对所抽样本进行的审核对 PIMS 包含的所有场所具有代表性，抽样要求见附录 B。如果不同场所的活动存在明显差异、或不同场所间存在可能对隐私信息安全管理体系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。

4.2.3.3 为使现场审核活动能够观察到隐私信息安全管理体系活动情况， 现场审核应安排在认证范围覆盖的隐私信息安全管理体系活动正常运行时进行。

4.2.3.4 在审核活动开始前，审核组应将审核计划交申请组织确认， 遇特殊情况临时变更计划时，应及时将变更情况通知申请组织， 并协商一致。

4.3 实施审核

4.3.1 审核组应当按照审核计划的安排完成审核工作。 除不可预见的特殊情况外，审核过程中不得随意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，申请组织的最高管理者及与 PIMS 相关的职能部门负责人员应该参加会议。参会人员应签到，审核组应当保留首、 末次会议签到表。申请组织要求时，审核组成员应向申请组织出示身份证明文件。

4.3.3 审核过程及环节

4.3.3.1 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。如果需要更长的时间间隔，应重新实施第一阶段审核。

4.3.3.2 第一阶段审核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 PIMS 成文信息描述的一致性，特别是体系成文信息中描述的业务活动、部门设置和职责与权限、PII 等是否与申请组织的实际情况相一致。

（2）结合现场情况，审核申请组织了解和实施 ISO 27701:2019 标准的情况，评价 PIMS 运行过程是否实施了内部审核与管理评审，确认 PIMS 是否已运行并且超过 3 个月。

（3）确认申请组织建立的 PIMS 覆盖的活动内容和范围、体系覆盖范围内有效人数、业务过程和场所，遵守适用的法律法规及强制性标准的情况。

（4）结合 PIMS 覆盖的特点，识别对隐私信息安全管理体系目标的实现具有重要影响的关键点： 业务影响分析和风险评估、PII 控制程序，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。对 PIMS 成文信息不符合现场实际、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。

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， 但应记录未在现场进行的原因：

（1）申请组织已获本机构颁发的其他有效认证证书，本机构已对申请组织 PIMS 有充分了解。

（2）本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， 第一阶段审核应在受审核方的隐私信息安全管理体系现场进行。

4.3.3.4 审核组应通过电话或其他网络方式与申请组织进行沟通，了解受审核方的基本情况和体系运行情况。 形成第一阶段审核报， 并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 第二阶段审核应当在申请组织现场进行。重点是审核 PIMS 符合 ISO27701:2019 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过程控制的有效性。

(2) 为实现隐私信息安全管理体系管理方针，而在相关职能、层次和过程上建立隐私信息 安全管理体系管理目标是否具体适用、可测量并得到沟通、监视。

(3) 对 PIMS 覆盖的业务活动与个人可识别信息的控制和处理有关的关键点的控制，如：

a) 业务影响分析及控制情况；

b) 风险评估及中断风险的处理；

c) PII 的确定和选择，评价是否有效；

d) PII 文件(法规、外来文件、内部文件)的建立和实施，包括 PII 当事人和处理人；

e) PII 保护的密码控制及设备。

(4) 申请组织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) PII 的管理(目标、 访问、记录、 更改或删除)。

(6) 申请组织的内部审核和管理评审是否有效。

(7) 不符合和纠正措施是否有效。

(8) PII 的泄露及应急处理。

(9) PII 的共享、转让和披露

4.3.4 发生以下情况时，审核组应向认证机构报告，经认证机构同意后终止审核。

(1) 受审核方对审核活动不予配合，审核活动无法进行。

(2) 受审核方实际情况与申请材料有重大不一致。

(3) 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) 申请组织活动范围和场所。

(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) 叙述从 4.3 条列明的程序及各项要求的审核工作情况，其中：对 4.3.3.5 条的各项审核要求应 逐项描述或引用审核证据、审核发现和审核结论；对隐私信息安全管理体系目标和管理过程及 PII 管 理绩效实现情况进行评价。

(7) 识别出的不符合项。

(8) 审核组对是否通过认证的意见建议。

4.4.2 本机构保留用于证实审核报告中相关信息的证据。

4.4.3 本机构在做出认证决定后 30 个工作日内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，本机构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

对审核中发现的不符合，BCK 应要求受审核方在规定的时限内进行原因分析，采取相应的纠正措施。BCK 应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，在下次审核时验证。

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。

对于受审核方未能在规定的时限内完成对不符合所采取措施的情况，BCK 不应作出授予认证、保持认证或更新认证的决定。

4.6 认证决定

4.6.1 技术部在对审核报告、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 认证决定人员应为机构管理控制下的人员，审核组成员不得参与对审核项目的认证决定。

4.6.3 技术部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，审核组提供的审核报告及其他信息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，审核组已评审、接受并验证了纠正和纠正措施的有效性。

① 在持续改进 PIMS 的有效性方面存在缺陷，实现 PII 管理目标有重大疑问。

② 制定的 PII 管理目标不可测量、或测量方法不明确。

③ 对实现 PII 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 其他严重不符合项。

（3）审核组对其他一般不符合项已评审， 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，审核组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 PIMS 符合标准要求且运行有效。

（2）认证范围覆盖的隐私信息安全管理体系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或者存在以下情况的， 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。

（1）受审核方的 PIMS 有重大缺陷，不符合 ISO27701:2019 标准的要求。

（2）发现受审核方存在 PII 管理问题或有其他与隐私信息安全管理体系相关严重违法违规行为。

4.6.6 本机构在颁发认证证书后 30 个工作日内按照规定的要求将认证结果相关信息报送国家认监委。

5. 监督审核程序

5.1 本机构对持有其颁发的 PIMS 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 PIMS 并符合认证要求。

5.2 为确保达到 5.1 条款要求，本机构根据获证组织的 PII 管理的管理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证书签发日起 12 个月内进行。此后，监督审核应至少每个日历年(应进行再认证的年份除外)进行一次，且两次监督审核的时间间隔不得超过 15 个月。

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。

5.2.3 获证企业的隐私信息安全管理体系在国家有关部门监督抽查中被查出不合格时， 自国家有关部 门发出通报起 30 日内，本机构应对该企业实施监督审核。

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 1/3。

5.4 监督审核的审核组，应符合 4.2.2 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 4.2.3.3 条确定的条件。 由于各种原因，在每次监督审 核时难以覆盖所有隐私信息安全管理体系活动的，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 PII 管理活动。

5.6 监督审核时至少应审核以下内容：

(1) 上次审核以来 PIMS 覆盖的活动及影响体系的重要变更及运行体系的资源是否有变更。

(2) 按 4.3.3.2 (4)条要求己识别的重要关键点是否按 PIMS 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) PIMS 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) 隐私信息安全管理体系目标、绩效是否达到 PIMS 确定值。如果没有达到，获证组织是否运 行内审机制识别了原因、是否运行管理评审机制确定并实施了改进措施。

(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) 针对体系运行中发现的问题或投诉，及时制定并实施了有效的改进措施。

5.7 在监督审核中发现的不符合项，审核组应要求获证组织分析原因，规定时限要求获证组织完成纠正和纠正措施并提供纠正和纠正措施有效性的证据。审核组应采用适宜的方式及时验证获证组织对不符合项进行处置的效果。

5.8 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或引用审核证据、审核发现和审核结论。

5.9 技术部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，本机构应当实施再认证审核， 并决定是否延续 认证证书。

6.2 本机构仍应按 4.2.2 条和 4.3.1 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， 制定再认证审核计划。

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 4.2.1 条计算人日数的 2/3。

6.3 对再认证审核中发现的严重不符合项，审核组应规定时限要求获证组织实施纠正与纠正措施， 并在原认证证书到期前完成对纠正与纠正措施的验证。

6.4 技术部按照 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。

6.5 如果在当前认证证书的终止日期前完成了再认证活动并决定换发证证书，新认证证书的终止日期可以 基于当前认证证书的终止日期。新认证证书上的颁证日期应不早于再认证决定日期。

如果在当前认证证书终止日期前，审核组未能完成再认证审核或对严重不符合项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。

在当前认证证书到期后， 如果审核组能够在 6 个月内完成未尽的再认证活动，则可以恢复认证， 否则应至少进行一次第二阶段审核才能恢复认证。认证证书的生效日期应不早于再认证决定日期， 终止日期应基于上一个认证周期。

7. 暂停、恢复或撤销认证证书

7.1 本机构应制定暂停、撤销认证证书或缩小认证范围的规定和文件化的管理制度，规定和管理制度应满足本规则相关要求。对认证证书的暂停和撤销处理应符合管理制度，不得随意暂停或撤销认证证书。

7.2 暂停证书

7.2.1 获证组织有以下情形之一的，应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：

——管理体系持续或严重不满足认证要求的，包括文件与实际业务运作严重脱离；

——不满足适用的法律法规要求，且未采取有效纠正措施的；

——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；

——持有的与管理体系范围有关的行政许可文件、资质证书等过期失效的；

——不能按照规定的时间间隔接受监督审核或再认证审核的；

——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；

——不承担、履行认证合同约定的责任和义务的；

——被有关行政监管部门责令停业整顿的；

——主动请求暂停的；

——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；

——其他应暂停认证证书的。

7.2.2 认证证书暂停期不得超过 6 个月。但属于 7.2.1 第(4)项情形的暂停期可至相关单位作出许可决定 之

日。

7.2.3 本机构以适当方式公开暂停认证证书的信息，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。

7.3 恢复证书

7.3.1 获证组织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间内没有使用、引用认证资格（如广告宣传）和使用认证标志；

7.3.2 经 BCK 审定，确认获证客户在暂停认证资格的认证范围内已恢复符合相关的认证要求，作出同意恢复认证资格的结论，颁发恢复通知书并公告。

7.4 撤销/注销证书

7.4.1 获证组织有以下情形之一的，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：

——被注销或撤销法律地位证明文件的；

——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；

——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；

——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。

7.4.2 本机构暂、恢复或撤销/注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。

7.4.3 获证组织须按国家认监委（CNCA）、认可委规定，从接到撤销/注销通知书之日起立即停止使用带有认证标志的认证证书、对外宣传资料和/或产品包装。

对撤销/注销认证资格的获证组织的违规活动，一切后果由该获证组织自行承担。

8. 认证证书和认证标志

8.1 认证证书

管理体系认证证书的内容包括：

a)证书名称；

b)认证注册号（即认证证书编号）；

c)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

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；

d)获证组织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）；

e)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；

f)认证依据的认证标准，所采用的当时有效版本的完整标准号；

g)公司的名称、地址和认证标识（适用时）；

h)公司的印章和公司法人的签字；

i)相关的认可标识及认可注册号（适用时）；

j)为便于社会监督，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”，同时注明公司官网查询途径。

8.2 初次认证证书有效期最长为 3 年。再认证的认证证书有效期不超过最近一次有效认证证书截止期再加 3 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。

8.4 认证标志：

BCK 的认证标志如下图所示：

8.5 认证证书和认证标志适用要求

1）认证证书和标志只能由获证方在获准认证范围内使用，不准以任何方式转让、出售或借用、冒用。使用时必须与获证方单位名称和产品名称放在一起。

2）认证证书有效期三年，在有效期内，经公司年度监督审核通过后，颁发保持认证注册资格通知书，与主证书一并使用，证书才能继续有效，获证方方可继续使用管理体系认证证书和认证标志。

3）认证标志可以用于组织有关文件、文具、邮政信件和出版物等组织介绍宣传材料上，但不得用于获证组织的产品上或以其他可能误导的方式，暗示其产品、过程或服务已通过我公司认证。如果用于运输的包装箱上使用该标志，必须声明箱子中产品的生产商已通过管理体系认证并符合具体的认证标准。

4）对于检验和校准实验室的管理体系的认证，由于检验报告或实验室报告被视作产品，因此认证标志不能使用在这些报告上。

5）获证方在标志使用方案报公司批准后方可正式使用。获证组织应当在认证范围内使用认证证书和认证标志，不得利用管理体系认证证书、认证标志和相关文字、符号，误导公众认为其产品、服务已通过认证。

6）使用标志图案时，必须根据公司提供的图样按比例放大或缩小，不得变形使用。

7）获证方不得进行被公司认为误导顾客的错误宣传，一经发现不正确宣传证书和标志的误导使用，公司将采取监管措施直至撤销认证资格，必要时采取法律手段。

8）获证方认证证书缩小范围时，应修改所有的广告宣传材料。

9）获证客户如要在产品包装上或附带信息中声明通过管理体系认证，需包含以下内容：

—— 获证客户的标识（例如品牌或名称）；

—— 管理体系的类型和适用标准；

—— 颁发证书的认证机构。

使用认证标识时，应同时附有明确的声明以避免导致对该产品、过程或服务通过认证。产品包装的判别标准是其可从产品上移除且不会导致产品分解、碎裂或损坏。附带信息的判别标准是其可分开获得或易于分离。型号标签或铭牌被视为产品的一部分。

8.6 认证证书和标志的暂停使用和恢复

8.6.1 当获证方被公司暂停认证注册资格时，获证方应暂停证书和标志的使用。

8.6.2 当获证方被公司批准恢复认证资格时，公司应及时通知其恢复使用认证证书和标志。

9. 受理组织的申诉

申请组织或获证组织对认证决定有异议时，机构应接受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申诉人。

书面通知应当告知申诉人，若认为本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。

10. 认证记录的管理

10.1 本机构建立认证记录保存制度，记录认证活动全过程并妥善保存。

10.2 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。

10.3 以电子文档方式保存记录的，应采用不可编辑的或可追溯的电子文档格式。

11. 其他

11.1 本规则内容提及 IS02770 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。

11.2 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， 并经审核员审核现场确认与原件一致。

附录 A PIMS 认证审核时间要求

PIMS 认证审核时间要求

为确保认证审核的完整有效，根据申请组织 PIMS 覆盖的范围、业务活动与 PII 相关性的复杂程度以及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。

表一 员工有效人数与审核时间的关系

有效人数	A 模式 PI 基点人日	B 模式 通过 IS 扩展 PI 的现场审核人日	C 模式 IS 结合审核的 PI 现场审核人日
1-10	**4.5**	**(1).PI 的初审现场审核人日:** 按照 IS 的初审现场审核时间的 70%计算 例如: IS 的初审现场审核人日:5.0 PI 的初审现场审核人日:5.0*70%=3.5 **(2).PI 的监督现场审核人日** 3.5*1/3=1.5 **(3).PI 的再认证现场审核人日** 3.5*2/3=2.5	**(1).PI 初审结合 IS 初审\再认证:** 在 IS 体系的初审现场审核时间的基础上,增加 30%,如:IS 初审现场审核时间 4.0 人日,IS 结合 PI 的初审现场审核人日 4.0*30%+4.0=5.2,修约为 5.5 **(2).PI 初审结合 IS 监督:** PI 人日仍按照如上(1).IS 初审现场人日的*30%计算 **(3).PI 监督/再认证结合 IS 监督/再认证:** PI 人日按照如上(1)计算后*1/3,再认证同理过程 (1)计算后*2/3
11-15	5.5		
16-25	6.5		
26-45	7.5		
46-65	8.5		
66-85	9.5		
86-125	10.5		
126-175	11.5		
176-275	12.5		
276-425	13.5		
426-625	14.5		
626-875	15.5		
876-1175	16.5		
1176-	17.5		
1551-2025	18.5		
2026-2675	19.5		
2676-	20.5		
3451-	21.5		
4351-5450	22.5		
5451-6800	23.5		
6801-	24.5	**使用 BC 模式的前提条件:PI 的认证范围与 IS 相同**	
8501-10700	25.5		
>10700	与上述进程		

（一）审核人日数的计算与调整

（1）员工有效人数：

*涉及认证范围的所有专职人员，包括所有班次的人员。

*全职人员在轮班和/或重复或类似过程中工作（信息安全的最终用户控件） *部分时间的兼职人员和员工

*以季节性/工作量为基础的工人 雇员的有效人数应根据以下考虑因素计算：

人员类别	采用方法	有效人数估算
所有班次的员工= 全职及管理人员	这些人主要负责政策制定，战略决策，管理和治理信息安全控 制和全面控制管理系统实施情况和有效性。通常是高层管理人 员，过程负责人/部门负责人。	100%
所有班次的全职人	这种人员采取轮班制，从事的过程和操作是相似且连续的。最	人数平方根，四舍

员，从事重复或相似过程（用户信息 安全控制的终端用 户）	终用户通常会包括那些在监督下工作，参与技术活动，执行类 似的&重复性任务， 例如软件开发， 测试， 等，使用信息安全 的最终用户控制， 没有任何决策权。 这个人手可能是流动岗位 人员或根据涉及的工作量来指定的。	五入到更高的整数。
兼职人员 雇员 部分范围	取决于工作时间，兼职人员人数和部分雇员可能会减少或增加 并转化为同等数量的专职人员。（例如 30 名每天工作 4 小时的兼 职人员相当于 15 个全职人员）。	人数/8 小时数/实际小时 结果数字四舍五 入到下一个视为的最高整数 1 FTE （基于 100% ）。
季节性/基于工作量工人	这些是工作量或季节性工人在高峰时期受雇于某些行业（例如 为特定项目租用的资源能力，基于交付的紧迫性项目等）。 这 些可能会或可能不会轮班在审核当天可能不可用。 因此， 根据 部署周期，采用 50%的系数。	季节/项目总数 人 x 他们的月数 雇用/12 x 50%。 以 100%为基础的 1 FTE。

示例：对于拥有 500 名员工的软件开发组织，人力的分工为：

•管理人员-50

•软件开发人员和测试人员-400 •共用人力资源，他们也为不在范围内的其他项目工作-50 人，每天 3 个小时，因此，计算的工时将基于：

100%的管理人员+做重复性工作（开发人员和测试人员）的人力平方根+ FTE 那将是 50 +M400+（（（50X3） / 8） = 70 + 19 =89。要分配审核人天为 12。

对于 ISO 27701 （公司已通过 ISO 27001 认证）的扩展，额外时间将为两天（2）。

（2） 单一现场组织 所有轮班在组织控制下工作的总人数是确定审核时间的起始点。 在组织控制下从事工作的兼职人员增加了在组织控制下工作的人数， 与全职员工相比，组织的控制与工作时间成比例， 这一决定应取决于与全职相比的工作小时数。

在偏远地区工作的员工（如在家工作）应被视为总部人数。为 DC/DR 等无人值守现场增加 0.5 人 天。

（3）多现场组织 所有现场的过程必须基本相同， 并且必须按照类似的方法程序操作。 如果考虑其中的一些现场执 行类似的操作， 但过程比其他现场少，则它们可能是有资格加入多现场认证方案的， 但是前提这些现 场是进行大多数过程的关键场所。

所有流程都要经过全面审核。 在不同地点通过关联流程开展业务的组织也有资格进行抽样（如果全部） 满足本文件的其他规定。

如果每个位置的流程不相似， 但有明确的关联，则抽样计划应至少包括组织实施的每个过程的一个示 例（例如， 设计/开发软件在一个位置，其他支持在多个其他位置）。

组织的管理体系应在一个集中控制和管理的计划之下， 并服从中央管理评审。 所有相关场所（包 括中央管理职能）应遵守本组织的内部审核计划， 并且所有内部审核都应在认证机构审核之前按照该 计划进行审核。

应证明组织的中央办公室以及整个组织都能满足审核的相关管理体系标准。这应包括对相关法规 的

考虑。组织应证明其有收集和分析数据（包括但不限于下列项目）的能力。

所有网站，包括中央办公室及其权威，并展示其权威性和发起组织变革的能力 如果需要：

•系统文件和系统变更；

•管理评审；

•事件；

•纠正措施评估；

•内部审核计划和结果评估；

•风险管理

•不同的法律要求。

并非所有符合多现场组织定义的组织都有资格进行抽样，例如： •所有现场执行显著不同的活动；

•客户要求对每个现场进行审核； •有一个行业计划或监管要求，规定每个现场都要进行系统审核。

（4） 审核时间计算表 审核时间图作为根据有效员工人数计算审核持续时间的起点。

B 列仅适用于已经通过本机构 ISO 27001 认证，且 ISO27001 认证范围应至少涵盖 ISO 27701 认证范围。在所有其他情况下，应使用 A 列。

分配的时间还考虑到以下因素，这些因素与 PIM 的复杂性有关，因此也与工作有关，需要审核 PIM：

a） PIMS 的复杂性（如信息的关键性、PIMS 的风险状况等）；

b） 在 PIMS 范围内开展的业务类型；

c） 先前证明 PIMS 的绩效；

d） 实施 PIMS 各组成部分所用技术的范围和多样性（例如不同 IT 平台、隔离网络的数量）；

e） PIMS 范围内使用的外包和第三方安排的程度；

f） 信息系统开发程度；

g） 现场数量和灾难恢复（ DR） 现场数量； 符合资格标准的组织可以由可取样的场地、不能取样的场地或两者的结合。审核时间必须足以进行有效的审核。

每个抽样地点的审核时间减少不得超过 50%。

例如，30%是 IAF MD 5 允许的最大审核时间减少，而 20%则被视为最大减少由中央职能部门执行的单 一管理体系过程和任何潜在的集中化流程（如采购）。如果使用翻译器，则增加 20%。不能对列 B 进行人 天减少。

附录 B 适用抽样审核的多场所组织的抽样要求

1 确认抽样数量

1.1 每次审核最少审核的场所数量是：

初次认证审核：样本的数量应为场所数量的平方根（y= √x ），计算结果向上取整为最接近的整数，其中 y 为将抽取场所的数量、x 为场所总数。

监督审核：每年的抽样数量应为场所数量的平方根乘以 0.6 即（y=0.6 √x ），计算结果向上取整为最接近的整数。

再认证审核：样本的数量应与初次审核相同。然而，如果证明管理体系在认证周期中是有效的，样本的数量可以减少至乘以系数 0.8 即（y=0.8√ x ），计算结果向上取整为最接近的整数。

1.2 当对拟认证或获证管理体系涵盖的过程、活动进行风险分析，发现涉及下列因素的特殊情况时，应增加抽样的数量或频率：

——场所的规模和员工的数量；

——过程、活动以及管理体系复杂程度和风险水平；

——工作方式的差异（如：倒班）；

——所从事过程、活动的差异；

——投诉记录，以及纠正措施和预防措施的其他相关方面；

——与跨国经营有关的任何方面；

——内部审核和管理评审的结果。

1.3 如果组织的分支机构分为不同等级（如：总部办公室/中心办公室，全国性办公室，地区办公室，地方分支），上述的初次认证审核抽样模式适用于每个等级的场所。示例：

1 个总部办公室：每个审核周期（初次审核、监督审核或再认证审核）都审核；

4 个全国性办公室：样本数量=2，至少 1 个为随机抽样；

27 个地区办公室：样本数量=6，至少 2 个为随机抽样；

1700 个地方分支：样本数量=42，至少 11 个为随机抽样。

地区办公室的样本中宜至少覆盖到每个全国办公室控制的地区办公室。地方分支的样本中宜至少覆盖到每个地区办公室控制的地区分支。这样可能导致每个等级的场所抽样数量超过计算的最小抽样数量。

1.4 抽样过程应作为审核方案管理的一部分。在任何时候（即：在策划监督审核之前、或组织的任何场所变更其结构时、或将在认证边界之内增加新的场所时），应预先评审审核方案中的抽样安排，以便在为保持认证对样本审核之前能确定抽样数量调整的需求。

2 确认抽样审核的场所

2.1 在初次认证审核、每次再认证审核以及作为监督的一部分在每个日历年至少一次的审核中，都应对中心职能审核。

2.2 样本中应有一部分根据以下因素选取，一部分随机抽取；并且其结果应选到在有代表性的不同场所，确保认证范围内覆盖的所有过程将被审核到，且使得证书有效期内所选场所之间的差异尽可能大。

2.3 至少 25%的样本应随机抽取。

2.4 场所选取应考虑，但不限于以下方面：

——对场所内部审核、管理评审和/或以前认证审核的结果；

——投诉记录以及纠正和预防措施的其他相关方面；

——各场所在规模上的显著差异；

——在倒班安排和工作程序上的差异；

——管理体系以及在场所实施过程的复杂程度；

——上次认证审核后的变化；

——管理体系的成熟度和组织的理解程度；

——文化、语言和法律法规方面的差异；

——地理位置的分散程度；

——场所是常设的、临时的或虚拟的。

2.5　并不是必须在审核过程一开始就完成抽样。也可能在完成对中心职能的审核时完成抽样。不论哪种情况，应将样本中所包括的场所通知中心职能。这可能是在相对较短时间内通知，但应给出充分的时间用于审核准备。

附件

文件更改记录

更改页	更改状态	更改内容	更改人	日期
10	有效	附录 A 人日计算	郝童霞	2024-1-31
全文	有效	补充认证标志及使用要求	胡娜娜	2025-05-23
全文	有效	认证规则名称和认证依据修改，补充恢复要求、抽样要求	胡娜娜	2025-08-12
全文	有效	LOGO 企业名 部门名 认证标志变更	付冉	2025-12-30
3、10	有效	新增要求“审核组至少包括 1 名专职审核员，并确保该专职审核员全程参与管理体系认证审核活动”；删除“9.与其他管理体系结合审核”	胡娜娜	2026-01-21
全文	有效	参考新版管理体系认证规则修订相应内容	胡娜娜	2026-03-31