中鸿认证（江苏）有限公司

隐私信息管理体系认证实施规则

规则编号：ZHCC-R-08

文件版本：C/3

受控状态：受控文件

编写人员：技术部

审核人员：韩自鹤

批准人员：丁泽林

发布日期：2023年4月12日

修订日期：2026年9月21日

实施日期：2026年9月21日

目录

1 适用范围 1

2 认证依据 1

3 对 ZHCC 的基本要求 1

4 对认证人员的基本要求 4

5 认证程序 6

5.1 认证申请 6

5.2 申请评审 7

5.3 认证合同及相关责任 8

5.4 审核方案和审核策划 9

5.5 实施审核 12

5.6 初次认证审核 13

5.7 监督审核 15

5.8 再认证审核 16

5.9 特殊审核 16

5.10 不符合项及其验证 17

5.11 审核报告 18

5.12 认证决定 19

6 认证证书和认证标志 21

6.1 总则 21

6.2 认证证书 22

6.3 认证标志 24

7 认证证书的暂停、撤销、注销和恢复 24

7.1 总则 24

7.2 认证证书的暂停 24

7.3 认证证书的撤销 26

7.4 认证证书的注销 26
7.5 认证证书的恢复 26
8 申诉（投诉）处理 27
9 信息公开与报告 27
10 认证记录 28
11 其他 29
11.1 认证标准换版 29
11.2 内部审核 30
11.3 同行评议 30
11.4 PIMS 技术服务 30
11.5 认证数据安全 30
12 附则 30
附录 A 隐私信息管理体系认证业务范围分类与风险级别 33
附录 B 隐私信息管理体系认证审核时间要求 36

隐私信息管理体系认证实施规则

1 适用范围

1.1 为规范中鸿认证（江苏）有限公司（以下简称 ZHCC）隐私信息管理体系（以下简称 PIMS）认证活动，根据《中华人民共和国认证认可条例》和《认证机构管理办法》等法律法规，结合相关技术标准制定本规则。

1.2 本规则规定了 ZHCC 实施 PIMS 认证的程序与管理的基本要求，是 ZHCC 从事 PIMS 认证活动的基本依据。

1.3 在中华人民共和国境内从事 PIMS 认证活动应遵守《中华人民共和国认证认可条例》、《认证机构管理办法》及本规则。

1.4 ZHCC 遵守本规则的规定，并不意味着可免除其所承担的法律责任。

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 要求和指南》

注：当上述认证依据发生换版或更改时，其最新版本适用本规则。 当等同采用的国家标准发布时，也适用于本规则。

3 对 ZHCC 的基本要求

3.1 本规则制定发布后 30 日内通过国家认证认可监督管理委员会（以下简称国家认监委）的“认证认可业务信息统一上报平台”进行备案。

3.2 开展 PIMS 认证活动，应当围绕国民经济和社会发展目标，重点服务于经济社会高质量发展，不得影响国家安全和社会公共利益，不得违背社会公序良俗。

3.3 内部管理和认证活动符合 GB/T 27021.1/ISO/IEC 17021-1《合格评定 管理体系审核要求 第 1 部分：要求》和 ISO/IEC 27701:2025《信息安全、网络安

全和隐私保护 隐私信息管理体系审核认证机构要求》，确保持续满足开展 PIMS 认证的基本要求。

3.4 建立风险防范机制，对从事 PIMS 认证活动可能引发的风险和责任采取合理有效措施。ZHCC 对 PIMS 认证活动引发的风险进行了评估，对引发的责任作出了充分安排。

3.5 建立认证人员管理制度，明确认证人员的能力准则、选择条件、聘用和评价程序，以及能力提升机制。确保从事 PIMS 认证的人员持续具备相应职业素养和能力。

3.6 应具有与认证业务相匹配的 PIMS 审核员，目前 PIMS 审核员应具备 ISMS 正式审核员注册资格，同时参加内部的隐私信息管理专业技术培训且考核合格；当 CCAA 推出 PIMS 领域审核员注册或确认准则的情况后，应具有 CCAA 注册或确认的 PIMS 审核员资格。在拟开展的 PIMS 认证业务范围（认证业务范围分类见附录 A），具备 2 名（含）以上 PIMS 专业领域审核员。ZHCC 结合认证业务范围识别相关专业的学历和专业隐私信息管理工作经历。相应认证业务范围的专业领域审核员，应取得 CCAA 正式 ISMS 审核员注册资格，并具备如下条件之一：

（1） 具有本科 （含）以上学历：在中风险认证业务范围内具有至少 2 年（含）以上该专业的隐私信息管理工作经历或具有该专业的中级 （含） 以上技术职称；在高风险认证业务范围内具有至少 3 年 （含） 以上该专业的隐私信息管理工作经历或具有该专业高级技术职称；

注 1：隐私信息管理工作包括隐私信息管理、隐私信息管理技术研究与开发及服务、隐私信息管理相关测评、隐私信息管理教学等。

注 2: ZHCC 参考 CNCA-ISMS-01:2026《信息安全管理体系认证规则》附录 A 基础上，确定了附录 A PIMS 认证业务范围的风险级别。

(2) 取得 CCAA 正式 ISMS 审核员注册资格后，参加该认证业务范围隐私信息管理专业技术

培训且考核合格，并且在 PIMS 专业领域审核员或技术专家的指导下完成一定数量的 PIMS 专业审核活动：中风险认证业务范围不少于 4 次 10 个现场审核人日，高风险认证业务范围不少于 6 次 20 个现场审核人日；

（3） 作为项目主要参加人，在该专业完成一定数量的隐私信息管理标准的制定、科研项目 （应用于相应行业 / 过程的隐私信息管理） 和设计开发等隐私信息管理专业技术工作。其中，高风险认证业务范围至少为 2 项，中风险认证业务范围至少为 1 项；

(4) 低风险的认证业务范围，具有 PIMS 审核员资格。

3.7 应对其认证活动的公正性负责，不允许商业、财务或其他压力损害公正性。如：不得将申请认证的组织 （以下简称认证委托人） 是否获得认证与参与认证审核的审核员及其他人员的薪酬挂钩。

3.8 对认证活动中所知悉的国家秘密、商业秘密负有保密义务。应通过在法律上具有强制实施力的协议，确保认证活动中所获得的信息在未经认证委托人书面同意的情况下，不向第三方透露，认证行政监管有要求的除外。

3.9 应对 PIMS 认证活动的真实性、有效性负责，加强认证人员的管理及素质、能力提升，合理安排审核员的工作量。每个审核员参加包括 PIMS 在内的管理体系现场审核时间的总和不应超过 180 天 / 周期年。

3.10 ZHCC 拥有的 PIMS 有效认证证书的数量应与机构 PIMS 审核员数量相匹配，人均每个审核员匹配的包括 PIMS 在内的管理体系有效认证证书总数不应超过 50 张 / 周期年。3.11 不委派未取得 PIMS 资格的审核员开展 PIMS 认证审核活动。

3.12 不以“认证证书在国家认监委网站可查” 或近似表述进行广告宣传。

4 对认证人员的基本要求

4.1 遵守认证认可相关法律法规、部门规章及规范性文件的要求，具有从事认证工作的基本职业操守，对认证活动及其结果的真实性和有效性承担相应责任。

4.2 审核员应已获得 PIMS 审核员资格。

4.3 审核员不得接受超出其资格的认证审核任务。

4.4 不得发生影响认证公正性的行为，应主动告知 ZHCC 其所了解的任何可能使本人或 ZHCC 陷入利益冲突的情况。因认证人员未履行告知义务而导致非公正认证结果的，认证人员应当负有连带责任 （如承担因此造成的经济损失）。

4.5 按要求接受人员注册 / 保持注册所要求的继续教育培训，以及 ZHCC 要求的能力 （包括知识和技能） 提升活动，以持续具备从事 PIMS 认证工作相适宜的能力。

4.6 审核员应具备以下知识：

（1） 隐私信息管理，包括 ISO/IEC 27701;

（2） 个人可识别信息 (PII) 的识别与处理；

（3） 设计和默认状态下的隐私保护；

(4) PIMS 的监视、测量、分析和评价；

(5) 与隐私信息管理和 PII 处理相关的信息安全风险；

(6) 隐私信息管理的政策和业务要求。

4.7 审核组全体成员应共同具备以下知识：

(1) 与隐私信息管理和 PII 处理相关的工具、方法、技术及其应用；

(2) 隐私事件追踪；

(3) 隐私信息风险评估、隐私影响评估及相关方法和风险管理；

(4) 适用于 PIMS 的过程；

（5） 可能涉及隐私问题的当前技术；

（6） ISO/IEC 27701 包含的所有控制及其实施；

（7） 适用于隐私信息管理和 / 或 PII 处理的法律要求 （如特定行业法律和地方隐私法律）；

(8) 行业隐私良好实践和隐私程序。

4.8 审核员应满足以下经验要求：

（1） 具有至少四年全职工作经验和专业工作经验（见 3.6）；

（2） 已完成至少一次 PIMS 领域的现场审核，或具有相关规则制定和技术文件编制经验；

（3） 通过持续专业发展保持隐私信息管理方面的最新知识和技能。

4.9 负责评审审核报告和作出认证决定的人员应具备以下知识：

(1) ISO/IEC 29100 中提出的隐私框架；

(2) ISO/IEC 27701;

(3) 与隐私相关的法律法规要求；

(4) 根据 ISO/IEC 27701 确定管理体系范围 （特别是 PII 控制者和 PII 处理者方面）， 能够验证范围的适当性以及范围的变更。

4.10 负责评审审核报告和作出认证决定的人员应总体了解：

(1) 隐私信息风险评估、隐私影响评估和风险管理；

(2) 适用于 PIMS 的过程。

5 认证程序

5.1 认证申请

5.1.1 ZHCC 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 ZHCC 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备案资格已满三个月 （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) 一年内未发生重大及以上级别的网络安全与隐私信息管理事件；

注：网络安全与隐私信息管理事件级别依据 GB/T 20986 判定。

(9) 其他应具备的条件。

5.1.3 ZHCC 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网络安全与隐私信息管理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) 生产 / 服务的流程、班次及轮班情况；

(6)PIMS 运行满三个月的证据；

(7) 一年内所发生的与网络安全与隐私信息管理相关的行政处罚以及整改情况（适用时）；

（8） 其他需要提供的文件。

5.2 申请评审

5.2.1 ZHCC 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，ZHCC 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) ZHCC 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，ZHCC 可实施认证转换，否则应按照初次认证开展认证活动：

(1) ZHCC 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 （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） ZHCC 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 ZHCC 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，ZHCC 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、ZHCC 和获证组织的责任。认证费用应由认证委托人向 ZHCC 直接支付。

5.3.2 ZHCC 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，通过官网或者其他形式向社会公布认证证书信息；因本规则备案被退回导致获证组织 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 ZHCC 对投诉的调查，及时向 ZHCC 通报 PIMS 及 5.1.2 中条件的变更情况，承担选择 ZHCC 但本规则备案被退回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 ZHCC 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 ZHCC 通报 PIMS 及 5.1.2 中条件的变更情况，承担选择 ZHCC 但本规则备案被退回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 ZHCC 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 所有要求，以及认证范围内的主要隐私信息管理风险及所涉及的典型过程 / 活动、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 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。初次认证及再认证后的一个认证周期内的审核方案中，应包括至少两次监督审核。监督审核的安排应同时满足以下要求：

（1）第一次监督审核应在证书签发之日起 12 个月内进行，第二次监督审核应在认证证书签发之日起 24 个月内进行；

（2）两次监督审核的时间间隔不应超过 12 个月，即本次监督审核的开始日期距上一次监督审核的结束日期不超过 12 个月；

（3）除再认证的年份外，监督审核每个日历年需要进行 1 次。

5.4.1.5 ZHCC 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生产或服务活动现场进行审核；

(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。

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 ZHCC 按照附录 B 所规定的隐私信息管理体系审核时间要求，考虑认证委托人有效人数、PIMS 风险级别等因素，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 PIMS 风险级别见附录 A。

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 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 70%。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 ZHCC 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 ZHCC 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 多场所抽样应基于与认证委托人活动或过程性质相关的 PIMS 风险的评价。 5.4.3.3 对涵盖相同活动、过程及 PIMS 风险级别的多个相似场所 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=√x

2）监督认证审核：Y=0.6√x

1）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。

5.4.3.4 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。

5.4.3.5 确定多场所组织的现场审核时间时，可依据附录 B 计算出总的现场审核人日，将总的现场审核人日分配到不同的场所；分场所审核人日的计算方法也可参见 5.4.2, 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%。

5.4.4 组建审核组

5.4.4.1 ZHCC 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：ZHCC 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 专业人员 （专业领域审核员或技术专家）。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 ZHCC 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 实习审核员不能独立组成审核组，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 ZHCC 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 审核员编号，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生产或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。

5.4.5.4 审核计划应考虑 PIMS 控制要求。

5.5 实施审核

5.5.1 PIMS 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，ZHCC 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隐私信息管理方针、隐私信息管理目标，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 ZHCC 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，包括其产品和服务、信息资产、支持性设施、生产 / 服务流程、现场运作、主要隐私信息管理风险、适用的隐私信息管理标准；

(2) 评审认证委托人 PIMS 体系文件 （含适用性声明）， 确认其与认证委托人产品和服务实现过程的隐私信息管理相吻合；

(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 标准的情况，特别是对隐私信息管理风险、PIMS 关键绩效、过程、隐私信息管理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) 认证委托人的产品和服务实现过程的隐私信息管理符合网络安全与隐私信息管理法律法规的情况。

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) 认证委托人已获得本 ZHCC 颁发的其他管理体系认证领域的有效认证证书，ZHCC 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 ZHCC 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。

ZHCC 记录未在现场进行第一阶段审核的理由。

5.6.2.3 ZHCC 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 ZHCC 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 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 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) 认证委托人隐私信息管理过程的运作控制；

(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 ZHCC 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 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主要隐私信息管理风险及所涉及的典型过程 / 活动、产品和服务，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主要隐私信息管理风险及所涉及的所有典型过程 / 活动、产品和服务。

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；

(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；

(9) 上次审核后发生的重大及以上级别网络安全与隐私信息管理事件的调查与处理。

5.7.4 监督审核的时间应根据获证组织当前有效人数和 PIMS 风险级别确定，不少于依据附录 B 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，ZHCC 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 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和 PIMS 风险级别来确定，不少于依据附录 B 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，ZHCC 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、重大及以上级别的网络安全与隐私信息管理事件，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） ZHCC 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，ZHCC 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，ZHCC 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 ZHCC 对认证委托人所采取的纠正措施的有效性进行验证。

对于轻微不符合，ZHCC 要求认证委托人在规定的时限内进行原因分析并完成整改。轻微不符合的验证时限和验证方式应满足以下要求：

(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 6 个月内完成；

(3) 再认证：在原认证证书到期后 6 个月内完成。

轻微不符合的验证由审核组长安排进行，验证方式为整改资料书面审查。

对于明显极轻微，仅影响局部的不符合，也可要求认证委托人制定整改计划，并结合下一次现场审核进行验证。

认证委托人可以针对轻微不符合制定纠正措施计划，由 ZHCC 在下次审核时验证。

5.10.3 严重不符合的验证时限和验证方式应满足以下要求：

(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。

严重不符合的验证由 ZHCC 安排进行，验证方式为针对严重不符合的现场专项审核。 关于严重不符合未在验证时限完成验证的，应按以下要求处置：

（1）初次认证审核的严重不符合在 6 个月内未完成验证的，ZHCC 在验证期限截止后 30 日内重新实施一次第二阶段审核；

（2）监督审核的严重不符合在 3 个月内未完成验证的，表明获证组织 ISMS 运行有效性存在问题，ZHCC 暂停或撤销认证证书；

（3）再认证审核的严重不符合未在认证证书到期前完成验证的，认证证书到期自动失效。获证组织再次申请认证的，ZHCC 按初次认证开展认证活动，满足 5.6.2.2 的情况下第一阶段审核 可不在认证委托人现场实施。

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，ZHCC 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 ZHCC 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 标准的符合性和有效性的客观证据信息，以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) ZHCC 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隐私信息管理风险识别和控制情况、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隐私信息管理目标之间存在的差距和改进机会；

(13) 与网络安全、隐私信息管理相关的行政处罚，以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 PIMS 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）；

(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；

(20) 对委托方隐私信息管理风险评估的审核概述或相关引用。

5.11.4 ZHCC 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，ZHCC 将此报告提交给认证委托人。

5.12 认证决定

5.12.1 ZHCC 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 ZHCC 的专职认证人员，并不得为审核组成员，能力应满足关于 ZHCC 认证决定人员的相关要求。认证决定过程不得外包，证决定过程必须在中华人民共和国境内实施，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 ZHCC 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 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。

认证决定过程包括对审核报告等认证记录的复核，并做出认证决定，该过程可由一个人或一组人完成；如果是一组人，其中做出最终认证决定的人员应为 ZHCC 的专职认证人员；ZHCC 可选择兼职技术专家为认证决定提供技术支持。

授予、更新、扩大认证范围的决定，必须基于对审核的发现、不符合及其验证结果等信息的综合评价，并有充分证据证明已满足 5.12.2 的所有要求。

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，ZHCC 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。

ZHCC 保证在获证组织的认证证书到期前完成再认证审核的认证决定，使再认证证书与原证书无缝连接；在获证组织的认证证书到期前未完成再认证决定的，ZHCC 保证关注后续认证活动的时效性。重点关注以下情形：

（1）再认证审核开具轻微不符合的，轻微不符合的关闭（对纠正措施计划的评审和接受）和认证决定，可在原认证证书到期后 6 个月内完成。

（2）再认证审核开具严重不符合的，严重不符合的关闭（对纠正措施有效性的验证）需要在证书到期前完成，认证决定应在原认证证书到期后 6 个月内完成。

（3）在原认证证书到期后 6 个月内仍未完成认证决定的，获证组织应重新申请认证。重新申请认证时，ZHCC 按初次认证审核开展认证活动。

5.12.5 认证委托人不能满足 5.12.2 要求的，ZHCC 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，ZHCC 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) ZHCC 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。 对监督审核不单独进行“保持认证的认证决定”的前提是，ZHCC 建立了文件化的监督审核的监视机制，并保留实施了监视的证据。

监督审核的发现可能导致认证证书暂停或撤销时，ZHCC 按 5.12 条款的要求进行认证决定。监督审核的结论涉及认证证书变更的（如扩大认证范围、变更证书信息等），ZHCC 也按本规则 5.12 条款的要求进行认证决定。

6 认证证书和认证标志

6.1 总则

6.1.1 ZHCC 制定了文件化的认证证书和认证标志管理制度，要求获证组织正确使用隐私信息管理体系认证证书和 ZHCC 认证标志。该制度符合国家认监委关于认证证书和认证标志管理的相关要求，如《认证证书和认证标志管理办法》等，避免误导公众或侵犯公共利益。。

6.1.2 获证组织可以在认证证书有效时使用隐私信息管理体系认证证书和认证

标志，并接受 ZHCC 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。

ZHCC 结合监督审核和再认证审核，现场查看获证组织对认证证书和认证标志的使用情况。同时，ZHCC 根据掌握的获证组织的认证证书状态变化情况，对获证组织正确使用认证证书和认证标志履行告知和监督义务。

获证组织仅可在认证证书处于有效状态的情况下使用该认证证书，如认证证书处于暂停期间、被撤销或注销后，ZHCC 要求获证组织不得使用认证证书和认证标志；认证证书被暂停、撤销或注销的，获证组织应及时对正在使用的认证证书和认证标志进行处理，如包装或宣传材料等不可再继续使用认证证书和认证标志的信息，原印制有认证证书和认证标志信息的包装或宣传材料等应进行妥善（一般是销毁或封存）处理。

6.1.3 获证组织应当在广告等有关宣传中正确使用隐私信息管理体系认证标志，不得在产品上仅标注隐私信息管理体系认证标志，只有在注明获证组织通过隐私信息管理体系认证及 ZHCC 名称的情况下，方可在产品包装上标注隐私信息管理体系认证标志。

隐私信息管理体系认证标志和证书信息，仅可在产品可以分割的包装（指包装可以从产品上移除且不会导致产品分解、碎裂或损坏）上使用，需使用中文注明获证组织通过信息安全管理体系认证及中鸿认证（江苏）有限公司的名称，以免与产品和服务认证标志混淆而误导公众。

6.1.4 ZHCC 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 ZHCC 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。

存在以下情况的，ZHCC 不能按照再认证签发认证证书：

（1）原证书到期前未完成再认证现场审核的；

（2）原证书到期前未完成严重不符合的整改和验证的；

（3）原证书到期后 6 个月内未完成再认证审核的认证决定的。

6.2.4 对每张 PIMS 认证证书应赋予一个认证证书编号，认证证书编号应遵循一定的规律。

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 所采用的当时有效版本的完整标准号；

（4） 认证证书应包括适用性声明的版本；

注：如果适用性声明的变更没有改变认证范围中控制的覆盖范围，则不要求更新认证证书。

(5) 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可继续有效的提示信息；

(6) 认证证书编号 （或唯一的识别代码）；

(7) ZHCC 名称、地址；

(8) 认证标志、相关的认可标识及认可注册号 （适用时）；

(9) 认证证书信息及认证证书状态的查询途径；

(10) “隐私信息管理体系” 字样。

（11） 组织在认证范围内每项活动、产品或服务所承担的角色 （即组织作为个人信息控制者和 / 或个人信息处理者的身份）。

(12) 认证范围内每项活动、产品或服务所处理的个人信息主体类别（如员工、客户）。

6.3 认证标志

ZHCC 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。

7 认证证书的暂停、撤销、注销和恢复

7.1 总则

ZHCC 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，ZHCC 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) 受到与网络安全、隐私信息管理相关的行政处罚，且尚未完成整改的；

(4) 发生重大及以上级别网络安全、隐私信息管理事件，反映获证组织 PIMS 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 PIMS 认证范围有关的行政许可文件、资质证书等过期失效的；

(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产停业整顿的；

(11) 发生与网络安全、隐私信息管理相关重大舆情的；

(12) 主动请求暂停的；

(13) 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；

(14) 其他应暂停认证证书的。

7.2.2 ZHCC 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，ZHCC 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，ZHCC 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重大及以上级别网络安全、隐私信息管理事件的；

(5)PIMS 没有运行或者已不具备运行条件的；

(6) 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，ZHCC 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。

7.5 认证证书的恢复

7.5.1 证书恢复的条件

获证客户对存在问题采取整改措施并在规定的时限内，解决了造成暂停的问题，认证资格的恢复符合相关的认证要求，同时在暂停期内没有使用、引用认证证书（如广告宣传）和使用认证标志。

7.5.2 证书恢复的程序

获证客户在规定时限内解决了造成暂停的问题后，向公司提出恢复使用认证证书申请并提供证明资料，可分两种情况：一种可立即办理恢复手续，经确认后 办理恢复手续；另一种要经现场评审确认后办理恢复手续，根据暂停的原因，经 评定后作出证书恢复 / 现场评审确认的评定意见确认后办理恢复手续。

7.5.3 在机构确认原因消除后，按流程进行恢复，机构将恢复信息上网公示，并向获证客户发送恢复通知，通知获证客户恢复认证证书和认证标志使用和宣传。

8 申诉（投诉）处理

8.1 ZHCC 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 ZHCC 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 ZHCC 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。ZHCC 对申诉人 （投诉人）、申诉 （投诉） 事项的信息应予以保密。

8.3 ZHCC 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）。

9 信息公开与报告

9.1 ZHCC 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 ZHCC 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 ZHCC 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。ZHCC 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。

9.4 ZHCC 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。ZHCC 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 获证组织发生重大及以上级别网络安全与隐私信息管理事件的，ZHCC 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 ZHCC 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《中华人民共和国电子

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 ZHCC 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）。

11 其他

11.1 认证标准换版

认证标准换版后，ZHCC 及时制定认证标准换版工作方案，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

ZHCC 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

ZHCC 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 ZHCC 可为组织提供 ISO/IEC 27701 贯标服务，但不代替组织编制 PIMS 文件、开展内部审核和管理评审，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 ZHCC 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

ZHCC 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。

12 附则

12.1 术语及释义

12.1.1 认证人员：指从事认证活动的人员，及 ZHCC 的业务管理人员。

12.1.2 认证委托人：申请认证并接受认证审核的组织。

12.1.3 PIMS 认证业务范围：以与 PIMS 预期结果有关的过程的共性为特征的领域。

注：认证业务范围类别与隐私信息管理体系范围内的产品、过程和服务有关，认证业务范围也被称作 “技术领域”“行业” 等。

12.1.4 认证转换：一个已获认可的认证机构为了颁发自己的认证证书，而承认另一个已获认可的认证机构颁发的现行有效的管理体系认证证书。

12.1.5 审核时间：策划并完成一次完整有效的管理体系审核所需要的时间。

12.1.6 现场审核时间：审核时间的一部分，包括从首次会议到末次会议之间实施审核活动的所有时间。

12.1.7 严重不符合：影响管理体系实现预期结果的能力的不符合。

注：严重不符合可能是下列情况：

－对过程控制是否有效存在严重的怀疑。

－多项轻微不符合都与同一要求或问题有关，可能表明存在系统性失效，从而构成一项严重不符合。

12.1.8 轻微不符合：不影响管理体系实现预期结果的能力的不符合。

12.1.9 个人可识别信息（personally identifiable information, PII）：（a）可用于建立信息与相关自然人之间关联，或（b）直接或间接与自然人相关联的信息。

注 1：本定义中的 “自然人” 指个人信息主体（3.4）。判断个人信息主体是否可被识别时，应考虑持有数据的隐私相关方或任何其他方可能合理使用的所有手段，以建立个人可识别信息集与自然人之间的关联。

注 2：在我国立法、行政、司法领域，个人可识别信息，也叫个人信息。

【定义及注 1 来源：ISO/IEC 29100:2024，3.7】

12.1.10 个人信息控制者（PII controller）：决定个人信息处理目的和方式的隐私相关方（一个或多个），不包括为个人目的使用数据的自然人。

注 1：个人信息控制者有时会指示他人（如个人信息处理者）代表其处理个人信息，但处理责任仍由个人信息控制者承担。

【来源：ISO/IEC 29100:2024，3.8】

12.1.11 个人信息处理者（PII processor）：代表个人信息控制者并按照其指示处理个人可识别信息的隐私相关方。

【来源：ISO/IEC 29100:2024，3.10】

12.1.12 隐私信息管理体系（privacy information management system, PIMS）：应对因个人信息处理可能产生的隐私影响而建立的管理体系。

【来源：ISO/IEC 27701:2025，3.23】。

12.2 ZHCC 接受认证行政监管部门依照本规则的规定对管理体系认证活动实施监督管理，发现违法违规行为，依法依规接受处理。

12.3 本规则由 ZHCC 负责解释。

附录 A 隐私信息管理体系认证业务范围分类与风险级别

PIMS 认证业务范围分类与风险级别

大类	中类/小类	风险级别	中类/小类名称	分类内容
1	政务			
	1.01	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
	1.02	高	税务机关	
	1.03	高	海关	
	1.04	中	其他	如政党，政协，社会团体等
2	公共			
	2.01	高	通信、广播电视	
	2.02	高	新闻出版	包括互联网内容的提供
	2.03	中	科研	涉及特别重大项目的应提升为高
	2.04	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
	2.05	高	医疗服务	
	02.05.01	高	医疗服务	
	02.05.02	高	其他护理、与健康有关的照料服务	
	2.06	低	教育	
	2.07	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）

	02.07.01	中	其他市政公用事业	例如市政公用事业（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）
	02.07.02	中	其他社会工作活动	例如向老年人和残疾人提供的不含住宿的社会工作活动，儿童日托活动，其他未另分类的不提供住宿的社会工作活动；兽医活动；废物的收集、处理、污染修复等
3	商务			
	3.01	高	金融	如银行、证券、期货、保险、资产管理等
	3.02	高	电子商务	以在线交易为主要特点，含网络游戏
	3.03	高	物流	包括邮政
	3.04	低	咨询中介	如法律、会计、审计、公证等
	3.05	中	旅游、宾馆、饭店	
	3.06	低	其他	
4	产品的生产			产品包括软件、硬件、流程性材料和服务
	4.01	高	电力	包括发电和输、变、配电等
	4.02	高	铁路	
	4.03	高	民航	
	4.04	高	化工	
	04.04.01	高	其他化工	
	04.04.02	高	石油化工	
	4.05	高	航空航天	
	4.06	高	水利	
4	4.07	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

	4.08	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
	4.09	中	冶金	
	4.1	中	采矿	含石油、天然气开采
	4.11	中	食品、药品、烟草	
	4.12	低	农、林、牧、副、渔业	
	4.13	低	其他	
	04.13.01	低	其他一般产品的生产和服务提供	纺织、皮革及皮革制品、木材及木制品、纸浆/纸及纸制品、印刷业、核燃料、橡胶和塑料制品、非金属矿物制品、混凝土/水泥/石灰/石膏及其他、造船业、铁路机车/摩托车/自行车及其他运输设备、家具/珠宝/乐器/体育用品/游戏用品及玩具/医疗及牙科器械和用品/其他/其他设备的修理、回收业、工程服务、其他服务、其他活动
	04.13.02	低	建设业	
	04.13.03	低	金属、机械及设备	基础金属及金属制品、机械及设备
	04.13.04	低	电和光学设备	
	04.13.05	低	汽车及其零部件	
	04.13.06	低	维修	汽车、摩托车、个人及家庭用品修理业

注：

1. ZHCC 基于附录 A 开展 PIMS 认证活动

2. 高风险、中风险、低风险也可表述为一级、二级、三级。

3. 01 大类下所有专业均不可受理。

附录 B 隐私信息管理体系认证审核时间要求

有效人数	PII 控制者审核时间（第 1 阶段 + 第 2 阶段）（人日）	PII 处理者审核时间（第 1 阶段 + 第 2 阶段）（人日）	PII 控制者+处理者审核时间（第 1 阶段 + 第 2 阶段）（人日）
<15	4	3.5	6.5
16-25	5	4	6.5
26-45	5	4	7
46-65	6	4.5	8
66-85	6	4.5	9
86-125	7	5	10
126-175	7	5	11
176-275	8	5.5	12
276-425	8	6	12
426-625	9	6	14
626-875	10	7	15
876-1175	11	7	16
1176-1550	12	8	17
1551-2025	13	8	19
2026-2675	13	9	20
2676-3450	14	9	21
3451-4350	14	10	22
4351-5450	15	10	22
5451-6800	16	10	23
6801-8500	16	11	24
8501-10700	17	11	25
>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%。

修订记录

发布日期	实施日期	版本	修订内容概要	拟制	审核	批准
2023.4.12	2023.4.12	A/0	新版发行	韩自鹤	张凯	张凯
2025.06.15	2025.06.15	C/0	增加证书更换、认证资格变更内容	孙敬	韩自鹤	丁泽林
2025.8.25	2025.8.25	C/1	依据《国家认监委关于加强认证规则管理的公告 2025 年第 9 号》进行修订	孙敬	韩自鹤	丁泽林
2026.04.20	2026.04.20	C/2	根据认监委规则备案整改	孙敬	韩自鹤	丁泽林
2026.09.21	2026.09.21	C/3	根据检查问题点进行整改	孙敬	韩自鹤	丁泽林