隐私信息管理体系认证
实施规则

文件编号：QB-GZ-2023-08

文件版本：B/0

编写人员：左海军

审批人员：陈 勇

批准人员：张 凤

发布日期：2023 年 09 月 05 日　2025-08-28 换版　　实施日期：　2023 年 09 月 05 日

序号	修改人	修改内容	版次	批准人	修改日期	备 注
01	左海军	按照国家认证认可监督管理委员会公告2025年第9号文件要求修改	A/1	张凤	2025.06.05	
02	左海军	按照国家认证认可监督管理委员会认证规则《备案检查意见》及《认证规则检查问题释疑讲解》要求修改	B/0	张凤	2025.08.28	

目 录

1. 适用范围

1.1 为规范本机构隐私信息管理体系（以下简称 PIMS)认证工作，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 本规则规定了本机构实施 PIMS 认证的程序与管理的基本要求，是本机构从事 PIMS 认证活动的基本依据。

1.3 本规则认证对象适用于任何规模、类型和性质的组，但国家明文规定不能用于认证活动的组织除外。

2. 认证依据

《信息安全-网络安全-隐私保护-信息安全管理体系要求》(ISO/IEC27001:2022)）和《安全技术 ISO/IEC27701 和 ISO/IEC27702 对隐私信息管理的扩展-要求和指南》（ISO /IEC 27701:2019)，本规则涉及的认证依据和其他标准和要求，均以最新有效版本为准。

3. 对认证机构的基本要求

3.1 本机构获得国家认监委批准、取得从事隐私信息管理体系认证的资质。

3.2 开展 PIMS 认证活动，应当围绕国家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 认证能力、内部管理和认证活动符合 GB/T 27021.1-2017/ISO/IEC17021-1:2015《合格评定 管理体系审核认证机构要求第 1 部分:要求》，以确保本机构持续满足开展 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。本机构应能证明已对其开展的 PIMS 认证活动可能引发的风险进行了评估，对可能引发的责任做出了充分安排（如保险或储备金)。

3.5 建立认证人员管理制度，包括认证人员的能力要求准则，选择、评价和聘用程序，以及能力提升机制。确保从事 PIMS 认证的人员持续具备相应素质和能力。

3.6 PIMS 认证业务范围的风险级别《隐私管理体系认证机构认证业务范围分类与分级》附录 A。

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，确保在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

向第三方透漏（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。

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，对认证审核活动及相关认证审核记录和认证审核报告的真实性承担相应的法律责任。

4.2 认证审核员应当取得国家认监委确定的认证人员注册机构颁发的信息安全管理体系审核员注册资格及隐私信息管理体系标准的培训。

4.3 不得发生影响认证公正性的行为，应主动告知认证机构他们所了解的任何可能使其或认证机构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性认证结果的，认证人员应当负有连带责任（如承担因此造成的经济损失）。

4.4 按要求完成人员注册/保持注册所要求的继续教育培训，以及机构要求的能力（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。

5. 认证程序

5.1 认证申请

5.1.1 本机构向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) 开展 PIMS 认证活动所依据的认证标准或其他规范性要求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）或撤销认证以及扩大或缩小认证范围的程序规定；

(4) 拟向组织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) 认证证书有效、暂停、注销或者撤销的状态

(8) 对认证过程和结果的申诉、投诉规定；

(9) 认证标准换版的规定；

(10) 认证实施规则；

(11) 其他需要公开的信息。

5.1.2 本机构要求申请组织至少提交以下资料：

(1) 取得法人资格（或其组成部分)；

(2) 取得相关法规规定的行政许可（适用时)；

(3) 已按认证标准建立 PIMS 体系，且运行满三个月；

(4) 具有一个已文件化且已实施的 PIMS,客户的 PIMS 应符合 ISO /IEC27701 和认证所要求的其他文件；

(5) 因获证组织自身原因被原发证机构暂停、撤销认证证书已满一年（适用时)；

(6) 未被行政监管部门责令停业整顿；

(7) 未被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) 一年内未发生行政监管部门责令停产整顿的重大隐私信息安全事故；

(9) 一年内未发生国家监督抽查（以下简称“国抽”）不合格，或发生国抽不合格但已按相关规定整改合格；

(10) 其他应具备的条件。

5.1.3 机构应要求认证委托人提供以下信息和文件资料：

(1) 认证申请书，包括认证委托人的名称、地址、认证标准、申请的认证范围、认证范围内组织人员数量及影响体系有效性的外包过程；

(2) 法律地位的证明性文件，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性文件并提交多场所清单；

(3) 申请认证范围所涉及的法律法规要求的行政许可文件、资质证书、强制性产品认证证书等；

(4) 组织机构及职责（可随体系文件)；

(5) 项目工艺流程/服务流程及生产和（或）服务的班次及轮班情况；

(6) PIMS 体系运行满足三个月的证据；

(7) 一年内所发生的隐私信息安全事故相关的行政处罚、国抽不合格，质量事故、一年内所发生的其他隐私信息安全抽查不合格的情况以及整改情况；

(8) 其他需要提供的文件。

5.2 申请评审

5.2.1 机构对认证委托人提交的申请文件和资料实施申请评审，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，以确定是否受理认证申请并保存相应评审记录。

对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”的申请组织，认证机构不应受理其认证申请。

5.2.2 满足以下条件的，本机构可以受理认证申请：

(1) 认证委托人已具备受理条件（见 5.1.2）；

(2) 本机构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，本机构按照初次认证开展认证活动，无论其是否持有其他本机构颁发的 PIMS 有效证书。

5.2.4 本机构应将申请评审的结果告知认证委托人补充和完善，或者不受理认证申请。

5.3 认证合同

5.3.1 通过申请评审的，在实施认证审核前，本机构应与认证委托人签订具有法律效力的认证合同，以明确认证委托人和本机构的责任。

5.3.2 本机构的责任至少包括：

(1) 及时向符合认证要求并已缴纳认证费用的组织颁发认证证书，通过其网站或者其他形式向社会公布获证信息；

(2) 对获证组织 PIMS 体系运行情况进行有效监督，发现获证组织的 PIMS 不能持续符合认证要求的，应及时暂停或者撤销其认证证书；

(3) 因本机构原因（如机构或其 PIMS 认证资质被注销或撤销）导致获证组织 PIMS 证书无法有效保持的，需及时告知获证组织并做出妥善处理，并承担由此导致的获证组织的经济损失。

5.3.3 获证组织的责任至少包括：

(1) 遵守认证程序要求，认证过程如实提供相关材料和信息，通过 PIMS 认证后持续有效运行 PIMS；

(2) 申请组织对遵守认证认可相关法律法规，配合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。配合本机构对投诉的调查；

(3) 应当在广告、宣传等活动中正确使用认证证书、认证标志和有关信息，认证证书注销或被暂停、撤销的，不得继续使用该证书和相关认证标志、信息，不利用隐私信息管理体系认证证书和相关文字、符号误导公众认为其产品或服务通过认证；

(4) 发生如下情况，应及时向本机构通报：发生重大隐私信息安全事故、受到市场监管部门行政处罚、被市场监管部门公布存在信息安全不符合、被媒体曝光存在信息安全问题、PIMS 不能正常运行或发生重大变更，以及其他应通报的情况、客户及相关方有重大投诉，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，出现影响隐私信息管理体系运行的其他重要情况等;

(5) 承担选择本机构的风险，如：因本机构资质被撤销而带来的认证证书无法使用的风险;

(6) 按合同约定及时向本机构缴纳认证费用.

5.4 审核方案和审核策划

5.4.1 审核方案

5.4.1.1 本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。

5.4.1.2 初次认证的审核方案应包括两阶段初次审核、获证后的监督审核和认证到期前进行的再认证审核。

注：一个认证周期通常为 3 年，从初次认证（或再认证）决定算起，至认证的有效期截止。

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/IEC27701:2019 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应覆盖 ISO/IEC27701:2019 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证书签发起 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 12 个月。

5.4.1.5 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 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的一个班次的生产或服务的活动现场进行审核;

(2) 对于未审核的班次，应记录不对其审核的理由。

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的实施策划、文

件审核和编写审核报告等活动的时间。审核时间以人天计，1 人天为 8 小时。如果每天的实际工作时间不足 8 小时，则应延长审核天数以满足人天要求。

5.4.2.2 本机构应以附录 B 所规定的审核时间为基础，考虑认证委托人有效人数\风险因素复杂程度、PIMS 风险类型等因素，建立文件化的不同类型审核的审核时间（包括现场审核时间）的确定方法。不同行业 PIMS 信息安全风险因素复杂程度附录 A

5.4.2.3 每次审核的审核时间的确定过程应形成记录，尤其是减少审核时间的理由，减少的时间不得超过附录 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%。

5.4.2.4 本机构应建立结合审核时间的确定方法，PIMS 和其他管理体系实施结合审核时，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

5.4.3.1 抽样原则

5.4.3.1.1 机构根据申请组织 PIMS 所覆盖活动的复杂性、规模以及各场所间的差异，确定抽样水平的基础， 只要抽样原则中有任何一方面未得到满足，均不能用抽样的方法实施审核。

5.4.3.1.2 在每个个案中，机构均需要检查申请组织的场所在何种程度上按照相同的程序和方法生产，或提供本质上同类的产品或服务。只有在确认拟进行多场所审核的各个场所都符合本文件规定的抽样条件后，才可将抽样程序用于这些场所。

5.4.3.1.3 本公司应保留每次多场所抽样的记录，该记录应证明公司是按照本文件进行操作的。

5.4.3.2 抽样条件

5.4.3.2.1 当每个场所均运行非常相似的过程、活动时，专业类别及风险处置方式相同。

5.4.3.2.2 并非所有满足“多场所组织 ”定义的组织都具备抽样的资格。

5.4.3.2.3 并非所有的管理体系标准都适合适于多场所认证。例如，当标准要求对差异性的当地因素审核时，对多场所的抽样是不适宜的。

5.4.3.2.4 为了通过审核获得对管理体系有效性的充分信任，认证机构应对在什么情况下进行场所抽样是不适宜的作出限制。认证机构应针对以下情况规定此类限制。

(1) 范围类别或过程、活动 (即基于对该类别或该活动相关的风险或复杂程度的 评估)；

(2) 具备多场所审核资格的场所规模；

(3) 为处理不同的过程、活动或不同的合同与法规系统，在当地运行管理体系的差异；

(4) 在组织管理体系之下运行的临时场所，即便这些临时场所未列入认证文件。

(5) 所有的场所在同一 PIMS 下运行，并接受统一的管理、内部审核和管理评审；

(6) 所有的场所都包含在客户的 PIMS 内部审核方案中；

(7) 所有的场所都包含在客户的 PIMS 管理评审方案中。

5.4.3.3 抽样方法

5.4.3.3.1 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。

5.4.3.3.2 至少 25%的样本应随机抽取。

5.4.3.3.3 考虑到下述规定，其余部分的选择应使得证书有效期内所选场所之间的 差异尽可能大。

5.4.3.3.4 场所选取应考虑，但不限于以下方面：

(1) 对场所内部审核、管理评审和/或以前认证审核的结果；

(2) 投诉记录以及纠正和预防措施的其他相关方面；

(3) 各场所在规模上的显著差异；

(4) 各场所业务目的的差异；

(5) 不同场所的信息系统的复杂程度；

(6) 管理体系以及在场所实施过程的信息安全类别及风险处置方式差异性；

(7) 工作实践的差异；

(8) 所实施的活动的差异；

(9) 控制的设计与运行的差异

(10) 与关键的信息系统或处理敏感信息的信息系统之间的潜在交互；

(11) 任何不同的法律要求；

(12) 地域和文化因素；

(13) 场所的风险状况；

(14) 发生在特定场所的信息安全事件。

(15) 在倒班安排和工作程序上的差异；

(16) 管理体系以及在场所实施过程的复杂程度；

(17) 上次认证审核后的变化；

(18) 管理体系的成熟度和组织的理解程度；

(19) 对于隐私信息管理体系，考虑信息安全问题和信息安全风险因素及其关联影响的程度；

(20) 文化、语言和法律法规方面的差异；

(21) 地理位置的分散程度；

(22) 场所是常设的、临时的或虚拟的。

5.4.3.3.5 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。

5.4.3.4 抽样基数

5.4.3.4.1 多场所的抽样基数是体系覆盖的具有可抽样性的所有多场所组织，比如组织有6个多场所，体系只覆盖5个多场所，其中4个多场所符合抽样原则和抽样条件，则该组织的抽样基数为4。

5.4.3.4.2 认证机构应对每个多场所组织每次应用抽样形成记录，证明其操作符合本文件要求。

5.4.3.5 抽样数量

5.4.3.5.1 该领域每次审核最少审核的场所数量是：

(1) 初次认证审核：样本的数量应为场所数量的平方根（$y=\sqrt{x}$），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。

(2) 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（$y=0.6\sqrt{x}$），计算结果向上取整为最接近的整数。

(3) 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（$y=0.8\sqrt{x}$），计 算结果向上取整为最接近的整数。

(4) 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。

(5) 当认证机构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：

a. 场所的规模和员工的数量；

b. 过程、活动以及管理体系复杂程度和风险水平；

c. 工作方式的差异（如：倒班）；

d. 所从事过程、活动的差异；

e. 投诉记录，以及纠正措施和预防措施的其他相关方面；

f. 与跨国经营有关的任何方面；

g. 内部审核和管理评审的结果。

(6) 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；

2 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按照第 5.4.3.5.1 条计算的最小抽样数量。

(7) 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），认证机构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。

5.4.3.6 增加场所

5.4.3.6.1 如果对已认证的多场所组织增加新场所或增加一组新的场所，认证机构应确定在证书中增加这些新场所前所需实施的必要活动。这应包括考虑是否对新 场所审核。

5.4.3.6.2 在新场所纳入证书后，需要确定后续监督或再认证审核的抽样数量。

5.4.3.6.3 分场所审核人日的计算方法参见 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 机构应根据实现审核目的所需的能力和公正性要求组建审核组，必要时可以选择技术专家参加审核组。审核组中的审核员承担审核任务和责任,每个审核组应包括：

(1) 审核组长，本机构应建立审核组长的选择、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/T19011《管理体系审核指南》标准中对审核组长的通用要求;

(2) 至少一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;

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,其在审核过程中的活动由审核组中的审核员承担责任。

5.4.4.3 实习审核员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 远程审核方法

5.4.5.1 PIMS 认证审核应在认证委托人的现场实施，初次认证以及认证周期内的每年度的监督审核和再认证审核活动，应包括访问认证委托人现场的现场审核。

5.4.5.2 因安全因素的考虑，审核组可在认证委托人的现场采用远程审核方法对认证委托人的某个过程的运作情况实施审核。

5.4.5.3 审核中采用远程审核方法的，远程审核时间不得超过现场审核时间的 30%，并应在审核计划、审核记录及审核报告中予以注明。

5.4.6 审核计划

5.4.6.1 认证机构应依据审核方案为每次现场审核制定审核计划。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 审核员注册号，专业审核员和技术专家应标明专业代码，在职技术专家应注明工作单位。

5.4.6.2 对于多场所审核，审核计划中应描述清楚多场所审核的安排，包括场地地址、距离总部的距离、审核时间、路途时间。

5.4.6.3 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。

5.4.6.4 现场审核开始之前，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。

5.5 实施审核

5.5.1 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，可使用图片、音像等作为补充材料。

5.5.2 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层（因特殊原因不能参加的，应授权高级管理层其他成员）、PIMS 相关职能部门负责人应参加会议，缺席

应记录理由。审核组应保留首、末次会议签到记录。审核组应按国家认监委的要求完成首、末次会议现场审核的网络签到。

5.5.3 发生下列情况时，审核组应向本机构报告，经同意后终止审核：

(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。

5.6 初次认证

初次认证审核采用文件评审和现场审核项结合的方式。

5.6.1 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，审核过程中不得更换审核计划确定的审核员。

5.6.2 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隐私信息管理体系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。

5.6.3 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必要时应有间隔，间隔最长不应超过 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。

5.6.4 第一阶段审核

5.6.4.1 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，包括其活动、产品和服务、设施设备、工艺流程、现场运作以及适用的隐私信息安全标准；

(2) 评审认证委托人 PIMS 体系文件，确认其组织业务活动及产品和服务相吻合；

(3) 审核认证委托人理解和实施 ISO/IEC27701:2019 标准的情况，特别是对 PIMS 关键绩效、过程和运行及信息安全风险因素有重大影响识别情况；

(4) 认证委托人是否为第二阶段审核做好准备，已实施了内审和管理评审；

(5) 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；

(6) 认证委托人的产品和服务符合隐私信息安全相关法律法规及强制性标准的情况。

(7) 审查第二阶段所需资源的配置情况，并与客户商定第二阶段的细节；

(8) 结合管理体系标准或其他规范性文件充分了解客户的管理体系和现场运作，以便为策划第二阶段提供关注点；

5.6.4.2 为达到第一阶段审核的目的和要求，除下列情况外，第一阶段审核活动应在认证

委托人现场实施：

(1) 认证委托人已获本机构颁发的其他领域的有效认证证书，认证机构已对认证委托人 PIMS 有充分了解；

(2) 认证机构有充足的理由证明认证委托人的信息安全风险因素特征明显，过程简单，通过对其提交文件和资料的审核可以达到第一阶段审核的目的和要求；

(3) 认证委托人获得了经认可机构认可的其他机构颁发的有效的 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。

认证机构应记录未在现场进行第一阶段审核的理由。

5.6.4.3 认证机构应将认证委托人是否具备二阶段审核条件的结论告知认证委托人，包括所识别的需引起关注的、在二阶段可能被判定为不符合项的问题。

5.6.4.4 第一阶段审核的时间应根据获证组织当前情况（如有效人数）确定，依据附录 B 所确定的初次认证现场审核时间的 1/3-1/4(如果计算后结果包括小数，宜将其调整为最接近的半人日数（如：将 5.3 个审核人日调整为 5.5 个审核人日，5.2 个审核人日调整为 5 个审核人日）).

(注：第一阶段现场审核所需的审核时间不宜少于 1 个人日。对于有效人数较少、风险较低的受审核组织可适当降低至 0.5 个人日。对于第一阶段为现场审核的项目，第二阶段现场审核时间不宜低于第一阶段和第二阶段总的现场审核时间的 70%;对于第一阶段为非现场审核的项目，第二阶段现场审核时间不宜低于 (根据增减因素) 调整后的总审核时间的 80%。)

5.6.4.5 第一阶段的结果应形成书面报告。在决定进行第二阶段之前，认证机构应审查第一阶段的审核报告，以便为第二阶段选择具有所需能力的审核组成员。

5.6.5 第二阶段审核

5.6.5.1 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/IEC27701:2019 标准要求的符合性和体系的有效性。

5.6.5.2 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/IEC27701:2019 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) 认证委托人过程的运作控制；

(5) 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；

(6) 认证委托人的内部审核和管理评审是否有效；

(7) 针对认证委托人 PISMS 方针的管理职责；

(8) 最高管理者的领导力和对方针与目标的承诺；

(9) 评估与信息安全有关的风险，以及评估可产生一致的、有效的、在重复评估时可比较的结果；

(10) 基于风险评估和风险处置过程，确定控制目标和控制；

(11) 信息安全绩效和 PISMS 有效性，以及根据信息安全目标对其进行评审；

(12) 所确定的控制、适用性声明、风险评估与风险处置过程的结果、方针与目标，它们相互之间的一致性；

(13) 信息安全控制的实施，考虑了外部环境、内部环境与相关的风险，以及组织对信息安全过程和控制的监视、测量与分析，以确定控制是否得以实施、有效并达到其所规定的目标；

(14) 客户证实对信息安全相关风险的评估与 PISMS 范围内的 PISMS 运行是相关的和充分的；

(15) 确定客户识别、检查和评价信息安全相关风险的规程及其实施结果是否与客户的方针、目标和指标相一致。

(16) 还应确定用于风险评估的规程是否健全并得到正确实施。

5.6.6 初审审核的时间应根据获证组织当前情况（有效人数和 PIMS 复杂程度）确定，不少于依据附录 B 所确定的初次认证审核时间(如果计算后结果包括小数, 宜将其调整为最接近的半人日数（如：将 5.3 个审核人日调整为 5.5 个审核人日，5.2 个审核人日调整为 5 个审核人日）)。

5.7 监督

5.7.1 例行监督

5.7.1.1 本机构应对获证组织进行有效跟踪，包括依据审核方案对获证组织开展的监督审核，以确认获证组织 PIMS 与 ISO/IEC27701:2019 标准的持续符合性和运行的有效性。

5.7.1.2 每次监督审核应尽可能覆盖认证范围内的有代表性的隐私信息安管理活动；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所有代表性的隐私信息安全管理活动。

5.7.1.3 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。

5.7.1.4 超过期限而未能实施监督审核的，应按暂停恢复审核、特殊审核 5.9.3 或 5.9.4 条处理。

5.7.1.5 获证企业的产品在环保监督抽查中被查出不合格时，自相关部门发出通报起 30 日内，本机构对该企业实施监督审核。

5.7.1.6 监督审核应重点关注获证组织的变更以及 PIMS 信息安全风险因素绩效的持续改进，监督审核的内容至少包括：

（1）管理体系的保持要素，如信息安全风险评估与控制的维护、PIMS 内部审核、管理评审和纠正措施；

（2）对上次审核中确定的不符合项采取的纠正措施及效果；

（3）PIMS 在实现客户方针的目标方面的有效性；

（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（含文件化管理体系的变更），所确定的控制的变更，及其引起的 SoA 的变更；

（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）客户证实对信息安全相关风险的评估与 PIMS 范围内的 PIMS 运行是相关的和充分的；

（10）确定客户识别、检查和评价信息安全相关风险的规程及其实施结果是否与客户的方针、目标和指标相一致。

（11）还应确定用于风险评估的规程是否健全并得到正确实施。

（12）对与相关信息安全法律法规的符合性进行定期评价与评审的规程的运行情况；

（13）控制的实施和有效性（根据审核方案来审查）。

5.7.1.7 监督审核的时间应根据获证组织当前情况（有效人数和 PIMS 信息安全风险因素的复杂程度）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(如果计算后结果包括小数，宜将其调整为最接近的半人日数（如：将 5.3 个审核人日调整为 5.5 个审核人日，5.2 个审核人日调整为 5 个审核人日）)。

5.7.2 非例行监督

出现下列情况之一时，DEOLIF 将对获证组织进行非例行监督审核：

——国家监督抽查获证组织产品出现不合格；

——获证组织发生用户严重投诉或被媒体曝光的；

——组织发生事故或安全生产行政主管部门采取法律行动的；

——组织发生信息安全事故或主管部门采取法律行动的；

——获证组织管理体系发生重大变更；

——其他需作非例行监督的情况。

5.8 再认证

5.8.1 获证组织拟继续持有认证证书的，应至少在认证证书到期前 3 个月向认证机构提出再认证申请，逾期则按初次认证申请处理。

5.8.2 本机构应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/IEC27701:2019 持续符合性和运行的有效性。

5.8.3 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，在认证到期后，如果认证机构能够在 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才能恢复认证。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。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 信息安全风险因素预期结果方面的有效性。

（4）客户证实对隐私信息安全相关风险的评估与 PIMS 范围内的 PIMS 运行是相关的和充分的；

（5）确定客户识别、检查和评价隐私信息安全相关风险的规程及其实施结果是否与客户的方针、目标和指标相一致。

（6）还应确定用于隐私信息安全风险评估的规程是否健全并得到正确实施

5.8.4 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 信息安全风险因素，包括调阅以往的监督审核报告。

5.8.5 再认证审核的审核时间应按 5.4.2 的要求，根据获证组织当前情况（有效人数和 PIMS 风险类型）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(如果计算后结果包括小数，宜将其调整为最接近的半人日数（如：将 5.3 个审核人日调整为 5.5 个审核人日，5.2 个审核人日调整为 5 个审核人日））。

5.9 特殊审核

5.9.1 扩大认证范围审核

1）由市场部传递的获证客户扩大认证范围的申请和客户提交的扩大认证范围申请，由合同评审岗对申请进行评审，确认受理后，调整审核方案。

2）审核部安排扩大认证范围审核，扩大认证范围审核可单独进行也可与定期监督或再认

证审核同时进行。与定期监督或再认证审核同时进行时应适当增加审核人日数。

3）扩大认证范围需审核内容：受审核方体系文件；与扩大产品和服务有关的运行策划和控制、产品和服务的要求、产品和服务的设计和开发、生产和服务提供、产品和服务的放行、产品和服务的监测分析和评价等内容，隐私信息管理体系还需关注到与扩大范围有关的信息安全风险因素、目标、合规义务、管理体系管控的运行策划和控制措施，隐私信息安全绩效监测等内容。

扩大认证范围审核的时间应根据获证组织当前情况（有效人数和 PIMS 复杂程度）确定，与监审结合审核时，不少于依据附录 B 所确定的监审认证审核时间，至少增加 0.5，扩大认证范围单独审核时不得少于 1 个人日(如果计算后结果包括小数，宜将其调整为最接近的半人日数（如：将 5.3 个审核人日调整为 5.5 个审核人日，5.2 个审核人日调整为 5 个审核人日））。

5.9.2 提前较短时间通知的审核

为调查投诉、隐私信息安全事故、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）认证机构应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，本机构应在指派审核组时给予更多的关注；

提前较短时间通知审核的时间应根据获证组织当前情况（有效人数和 PIMS 复杂程度）确定，审核时间至少为 1 个人日(如果计算后结果包括小数，宜将其调整为最接近的半人日数（如：将 5.3 个审核人日调整为 5.5 个审核人日，5.2 个审核人日调整为 5 个审核人日））。

（3）审核时间为 1-2 审核人日，根据项目情况确定。

5.9.3 暂停后的恢复

获证客户的证书被暂停后，当暂停的原因消除后，就可恢复其资格。对获证组织因其他情况（如发生了隐私信息安全事故、主管部门国家监督抽查不合格等）而导致的证书暂停，在暂停期内，需要企业写出书面申请，并写明企业已消除了暂停的原因和理由，并提供相应的证据。机构获得信息后，应安排暂停后的恢复审核。证书的恢复所进行的审核人日和审核实施，原则上按再认证的要求进行。

5.9.4 其它特殊审核

为调查投诉和对变更做出回应时可安排特殊审核，审核人日和审核的实施可按定期监督审核要求进行。

为调查投诉、对变更做出回应或对被暂停的获证客户进行的审核，可能需要在提前较短

时间通知获证客户。审核部在指派审核组时应充分考虑审核人员安排的合理性。

5.9.5 与其他管理体系的结合审核

5.9.5.1 对隐私信息管理体系和其他管理体系实施结合审核时，通用或共性要求应满足本规则要求，审核报告中应清晰地体现 5.11 条要求，并易于识别。

5.9.5.2 结合审核的审核时间人日数，不得少于多个单独体系所需审核时间之和的 80%。

5.9.6 认证机构转换审核

5.9.6.1 本机构当履行社会责任，严禁以牟利为目的受理不符合 ISO/IEC27701 标准、不能有效执行隐私信息管理体系的组织申请认证证书的转换。

5.9.6.2 本机构受理组织申请转换为本机构的认证证书，应该详细了解申请转换的原因，必要时进行现场审核。

5.9.6.3 如果机构考虑客户已获的认证或由另一认证机构实施的审核，则应获取并保留充足的证据，例如报告和对不符合采取的纠正措施的文件。所获取的文件应为满足本文件要求提供支持。机构应根据获取的信息证明对审核方案的任何调整的合理性，并予以记录，并对以前不符合的纠正措施的实施进行跟踪。

5.9.6.4 转换仅限于现行有效认证证书。被暂停或正在接受暂停、撤销处理的认证证书以及已失效的认证证书，不得接受转换申请。暂停撤销满一年的除外。

5.9.6.5 被发证的本机构撤销证书的，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，否则不应受理其认证申请。

5.10 不符合项纠正、纠正措施及其验证

5.10.1 对审核中发现的不符合项，本机构应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 认证机构应对认证委托人所采取的纠正措施的有效性进行验证。认证委托人可以针对轻微不符合项制定纠正措施计划，由认证机构在下次审核时验证。

5.10.3 严重不符合项的验证时限应满足以下要求：

(1) 初次认证：在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：在审核结束之日起 1 个月内完成。

5.10.4 一般不符合项的验证时限应满足以下要求：

(1) 初次认证：在二阶段审核结束之日起 3 个月内完成；

(2) 监督审核：在审核结束之日起 2 个月内完成；

(3) 再认证：在审核结束之日起 1 个月内完成。

5.10.5 对于认证委托人未能在规定的时限内完成对不符合项所采取措施的情况，认证机构不应做出授予认证、保持认证或更新认证的决定。

5.11 审核报告

5.11.1 认证机构应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/IEC27701:2019 标准的符合性和有效性的客观证据信息，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) 本机构名称；

(2) 认证委托人的名称和地址及其代表；

(3) 审核类型（例如初次、监督、再认证或其他类型审核）；

(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) 应描述与审核类型的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目标之间存在的差距和改进机会；

(13) 行政监管部门在隐私信息安全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 PIMS 的重要变更（适用时）；

(15) 认证委托人对认证证书和认证标志的使用进行着有效的控制（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认证范围适宜性的结论。

5.11.4 认证机构应保留用于证实审核报告中相关信息的证据。

5.11.5 认证机构应将审核报告提交认证委托人。

5.11.6 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，认证机构应将此报告提交给认证委托人。

5.11.7 本机构保留用于证实审核报告中相关信息的证据。

5.11.8 本机构在作出认证决定后 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。

5.11.9 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。

5.12 认证复核

5.12.1 本机构应在对审核报告、收集的证据信息、审核发现等其他信息进行认证复核、综合评价的基础上，做出认证决定。认证复核人员需要具备相应领域的能力。

5.12.2 本机构安排认证复核人员对于整个认证过程中形成的证据进行档案复核，确认认证审查过程及审查结论的公正性、有效性、真实性、完整性及充足性。

5.13 认证决定

5.13.1 认证机构应在对审核报告、不符合项的纠正措施及验证情况和其他信息进行认证复核、综合评价的基础上，做出认证决定。认证复核人员需要具备相应专业大类专业能力和相应领域的能力，认证决定人员应为本机构管理控制下的专职认证人员，并不得为审核组成员，能力应满足关于本机构资质审批的相关要求。认证决定过程不得外包，认证决定须由中华人民共和国境内的工作人员做出。

5.13.2 认证机构安排认证复核人员对于整个认证过程中形成的证据进行档案复核，确认认证审核过程及审核结论的公正性、有效性、真实性、完整性及充足性。

5.13.3 认证机构安排认证决定人员对于基于认证复核人员的复核结果，对于关键内容进行二次评审，最终作出认证决定,关键内容至少包括：

a）审核组提供的信息足以确定认证要求的满足情况和认证范围；

b）对于所有严重不符合，认证机构已审查、接受和验证了纠正和纠正措施；

c）对于所有轻微不符合，认证机构已审查和接受了客户对纠正和纠正措施的计划。

5.13.4 认证机构应有充分的证据确认认证委托人满足下列条件时，做出授予、更新、扩

大认证范围的决定：

（1）5.1.2 中的认证条件；

（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 总体符合 ISO/IEC27701:2019 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。

5.13.5 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。

5.13.6 再认证审核的认证决定应在上一认证周期认证证书到期前完成，否则应在推荐认证注册前再实施一次第二阶段审核。

5.13.7 认证委托人不能满足 5.12.4 要求的，认证机构应以书面形式告知并说明其未通过认证的原因。

5.13.8 对于监督审核，本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项及其他可能导致认证资格暂停、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）本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。

6. 认证证书和认证标志

6.1 总则

6.1.1 本机构应制定相应管理制度，要求获证组织正确使用 PIMS 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》中相关规定。

6.1.2 获证组织可以在认证有效期内使用 PIMS 认证标志，并接受本机构的监督管理。

6.1.3 获证组织应当在广告等有关宣传中正确使用 PIMS 认证标志，不得在产品上标注 PIMS 认证标志，只有在注明获证组织通过 PIMS 认证的情况下方可在产品的包装上标注 PIMS 认证标志。

6.1.4 本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。

6.2 认证证书管理

6.2.1 本机构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。

6.2.2 PIMS 认证证书的有效期最长为 3 年，初次认证证书有效期的起算日期为认证决定日期，再认证证书有效期的起算日期不得晚于最近一次有效认证证书的截止日期。

6.2.3 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。

6.2.4 认证证书在中华人民共和国境内使用的，证书使用的语言至少应包括中文。

6.2.5 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，当在认证证书上展示临时场所时，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/IEC27701:2019 所采用的当时有效版本的完整标准号；

（4）证书签发日期和有效截止日期，证书应注明：获证组织必须定期接受监督审核并合格此证书方可继续有效的提示信息。

（5）证书编号（或唯一的识别代码）；

（6）本机构名称、地址；

（7）认证标志、相关的认可标识及认可注册号（适用时）；

（8）证书信息及证书状态的查询途径。

6.3 认证标志管理

本机构暂未制定本领域认证标志。

7. 认证资格的暂停、撤销、注销和恢复

7.1 总则

认证机构对于认证资格有效、暂停、撤销、注销和恢复进行有效性管理，不得随意暂停、撤销和注销认证资格。

7.2 认证证书有效管理

通过认证决定的获证组织，本机构颁发认证证书，对于初审、再认证类型，在认证颁发

后的次月 10 号，将认证证书报送国家认监委，并将认证证书信息通过本机构官网予以公示。

7.3 认证证书的暂停

7.3.1 获证组织有以下情形之一的，认证机构应在调查核实后的 5 个工作日内暂停其认证资格，并保留相应证据：

(1) PIMS 持续或严重不满足认证要求的；

(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) 受到与信息安全相关的行政处罚；

(4) 发生较大或重大隐私信息安全事故，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 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资格和有关信息，包括认证证书和认证标志的使用，造成严重影响或后果的；

(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) 发生与隐私信息安全相关的重大舆情；

(12) 主动请求暂停的；

(13) 其他应暂停认证资格的。

7.3.2 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。

7.4 认证资格的撤销

获证组织有以下情形之一的，本机构应在获得相关信息并确认后 5 个工作日内撤销其认证资格，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) 认证资格的暂停期限已满，但导致暂停的问题未得到解决或有效纠正的；

(4) 因获证组织违规造成重大产品和服务等信息安全事故的；

(5) 有其他严重违反 PIMS 相关法律法规行为，受到相关行政监管部门处罚的；

(6) PIMS 没有运行或者已不具备运行条件的；

(7) 不按相关规定正确引用和宣传获得的认证信息，造成严重影响或后果，或者认证机构已要求其纠正但超过 1 个月仍未纠正的；

(8) 其他应撤销认证资格的。

7.5 认证资格的注销

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

7.6 认证资格的恢复

暂停期间，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资格，并保留相应证据，恢复认证资格的组织信息，应在 2 个工作日内，上报国家认监委。

7.7 认证证书和标志暂停使用和恢复

当获证组织被本机构暂停认证注册资格时，书面通知其暂停其证书和标志的使用。当获证组织被本机构批准恢复其认证资格时，由技术部发出书面通知其可以恢复使用认证证书和标志。

7.8 当获证组织的认证资格被撤销后，应立即停止使用认证证书和标志

8. 申诉（投诉）处理

8.1 本机构应建立文件化的申诉（投诉）处理制度，并遵照执行。

认证委托人或认证委托人对认证决定有异议的，可以向本机构提出申诉。

任何组织和个人对认证过程和决定有异议的，可以向本机构提出投诉。

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。本机构对申诉人（投诉人）、申诉（投诉）事项的信息应予以保密。

8.3 本机构应及时、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）。

8.4 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，可以直接向本机构所在地市场监管部门或国家认监委投诉。

9. 信息公开与报告

9.1 本机构应建立文件化的认证信息报告制度，并遵照执行。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 本机构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。

9.3 本机构在颁发认证证书后，应在次月 10 日前，将认证结果相关信息报送国家认监委。

本机构颁发的认证证书通过其扫描证书上二维码、登录德利福认证（上海）有限公司官网（www.deolif.com）或国家认证认可监督委员会官网（www.cnca.gov.cn）的方式向公众提供可查询认证的有效性。

9.4 认证机构应通过扫描证书上二维码，登录德利福认证（上海）有限公司官网（www.deolif.com）、国家认证认可监督委员会官网（www.cnca.gov.cn）的方式公开暂停、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。本机构应在暂停、撤销、注销认证证书之日起 2 个工作日内，按规定程序和要求报国家认监委。

9.5 获证组织发生重大隐私信息安全事故的，认证机构应在事故发生之日起 5 个工作日内，暂停该认证证书。

9.6 再认证证生效后，机构应撤销原仍有效期内的证书。

10. 认证记录

10.1 本机构应建立文件化的认证记录、认证资料归档管理制度，记录认证活动全过程并妥善保存，归档留存时间为认证证书有效期届满或者被注销、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) 合同评审方案策划过程记录；

(3) 认证合同；

(4) 审核计划；

(5) 首、末次会议签到表；

(6) 现场审核记录；

(7) 不符合项报告及验证记录；

(8) 审核报告；

(9) 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纸质版原件。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) 不符合项报告及验证记录。

10.4 认证记录应使用中文，以电子文档的形式保存认证记录的，应采用不可编辑的方式。

11. 其他

11.1 认证标准换版

本机构应按照国家市场监管部门统一制订发布的 ISO /IEC 27701:2019 标准的换版工作要求，执行落实标准的换版工作，确保组织能够及时获得新版标准认证。

11.2 内部审核

认证机构应建立文件化的内部审核程序并遵照执行，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 认证数据安全

认证机构应严格落实《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。未经安全评估和网信等相关部门批准，认证机构不得向境外传输、提供、公开存储于中华人民共和国境内的数据。法律、行政法规另有规定的，依照其规定。

附件 A：隐私管理体系认证机构认证业务范围分类与分级

隐私管理体系认证机构认证业务范围分类与分级

大类	中类	级别	描述	备注
01	政务			
	01.01	一	国家机关	包括人大、政府、法院、检察院等，不含税务机关和海关
	01.02	一	税务机关	
	01.03	一	海关	
	01.04	二	其他	例如政党、政协、社会团体等
02	公共			
	02.01	一	通信、广播电视	
	02.02	一	新闻出版	包括互联网内容的提供
	02.03	二	科研	涉及特别重大项目的应提升为一级
	02.04	二	社会保障	例如社会保险基金管理、慈善团体等、包括医疗保险
	02.05	一	医疗服务	
	02.06	三	教育	
	02.07	二	其他	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）
03	商务			
	03.01	一	金融	例如银行、证券、期货、保险、资产管理等
	03.02	一	电子商务	以在线交易为主要特点，含网络游戏
	03.03	一	物流	包括邮政
	03.04	三	咨询中介	例如法律、会计、审计、公证等
	03.05	二	旅游、宾馆、饭店	
	03.06	三	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	一	电力	包括发电和输、变、配电等
	04.02	一	铁路	
	04.03	一	民航	
	04.04	一	化工	
	04.05	一	航空航天	
	04.06	一	水利	
	04.07	二	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	二	信息与通信技术	例如软、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	二	冶金	
	04.10	二	采矿	含石油、天然气开采
	04.11	二	食品、药品、烟草	
	04.12	三	农、林、牧、副、渔业	
	04.13	三	其他	

附件 B：《隐私信息管理体系认证审核时间表》

下表为初次认证的审核人日基数，具体审核时间需要考虑受审核方的规模、特性、业务复杂程度、涵盖的范围、认证要求和其承担的风险等因素。根据受审核方的特点在项目方案制定过程中可以在人日基数上进行增减。

审核人日包括一阶段审核、现场审核以及报告编写的时间。

当隐私信息管理体系与其他管理体系结合审核时，隐私信息管理体系的审核时间可根据结合审核的其他管理体系的特点进行减少。

监督审核的人日数为初次认证人日数的三分之一，再认证的人日数为初次认证人日数的三分之二，上述原则仅限于获证组织的认证范围和组织规模未发生变化的情况。

基本人日数计算表

雇员数量	初次审核时间（人日）	雇员数量	初次审核时间（人日）
1-10	5	876-1175	18.5
11-25	7	1176-1550	19.5
26-45	8.5	1551-2025	21
46-65	10	2026-2675	22
65-85	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	沿用以上规律