隐私信息管理体系认证（PIMS）规则

编　号：YB-PIMS-01/2024

版　本：A/1

编制：马汝超

审核：左　磊

批准：毛其中

2025 年 06 月 10 日修订发布　　2025 年 06 月 15 日实施

上海扬标认证有限公司

目录

1 标准简介

ISO/IEC 27701：2019 是国际标准化组织（ISO）和国际电工组织（IEC）发布， 该标准建立在 ISO/IEC 27001 和 ISO/IEC 27002 要求的基础之上，在隐私方面提供了必要的额外要求。规定了建立、实施、维护和持续改进隐私相关所特定的信息安全管 理体系的要求。该标准可以提供通用数据保护法规（GDPR《通用数据保护条例》)要求的数据隐私和信息安全标准。为了有效地管理隐私，它包含用于个人身份信息（PII)处理器和控制器的结构。

实施 ISO27701 将创建一个隐私信息安全管理体系，简称 PIMS.

使用 ISO27701 认证作为数据安全性标准，可以向客户和利益相关者展示您的公司支持 GDPR 合规性和隐私法规。此外，它还可以确保您拥有他们可以信任的有效系统。通过使用控件降低个人和公司潜在的信息安全和隐私风险，您可以创建一个更值得信赖的品牌。

新发布的 ISO27701 认证标准既适用于 PII 的控制器（以及联合控制器）也适用于 PII 的处理器（包括子处理器），而不管其运营所在的管辖区和部门如何，并且还包括对 GDPR 和 ISO/IEC29100（隐私标准框架),ISO/IEC 27701 和 ISO/IEC 29151 安全框架。

1.1 ISO 27701 与各标准之间的关系

ISO 27701 是 ISO 27001 和 ISO 27002 在隐私方面的扩展。

ISO 27002 为 ISO 27001 提供风险处置具体的控制目标和控制措施。

ISO 29100、ISO 27701、ISO 29151 均为隐私方面的标准，有不同的侧重点，ISO 29100、ISO 29151 与 ISO 27701 互为补充。

ISO 27001 帮助企业建立 ISMS，通过有效的风险管理来保护和管理组织的所有信息，从数据安全方面满足 GDPR 的部分要求。

ISO 27701 加入了隐私保护的额外要求，更全面地覆盖了 GDPR 的要求。

2 适用范围

2.1 本规则用于规范上海扬标认证有限公司（以下简称“扬标”）对申请认证和获证的各类组织按照 ISO/IEC 27701 建立的个人隐私信息安全管理体系认证活动。

2.2 本规则旨在遵守认证认可相关法律法规及国家技术标准，对个人隐私信息安

全管理体系认证实施过程做出具体规定，确保扬标对认证过程的管理和相应责任。

2.3 本规则是对扬标从事个人隐私信息安全管理体系认证活动的基本要求，公司各部门从事该项认证活动应当遵守本规则。

3 认证基本原则

3.1 公正性：保持公正，是提供第三方认证的必要条件。公司通过合同评审、技术评审、审核准备和实现等过程控制，确保审核过程是公正的、客观的，为认证过程和证书提供社会公信力。

3.2 能力：能力是指经证实的应用知识和技能的本领。公司通过审核人员管理机制，保障人员能力是提供可建立信心的认证审核的必要条件。

3.3 责任：公司基于合理抽样、足够的客观证据基础上进行审核和评价，并在此基础上做出认证决定。

3.4 开放性：为确保诚信性与可信性，公司采用透明运营的方式，公布有关个人隐私信息安全管理体系认证审核过程和状态的适宜、及时的信息，或提供获取上述信息的公开渠道。

3.5 保密性：公司采取措施对任何关于客户的专有重要敏感信息予以保密，但对于享有获取充分评价认证审核符合性所需信息的特别权利是必不可少的。

3.6 对投诉的回应：公司依据《投诉和申诉流程》，对投诉和申诉进行调查和适当处理。

4 对认证人员的要求

为了确保审核能力，公司基于 ISO 19011 及国家和行业法规的要求，对个人隐私信息安全管理体系审核员、主任审核员、技术专家进行资格审批和管理。成为审核员，需要满足以下条件要求：

4.1 职业素养的要求

审核人员应具备以下职业素养：

1）独立性：保持独立性和客观性，不带偏见，无利益冲突。

2）道德行为：诚信、正直、保守秘密和谨慎。

3）公正表达：真实准确反映审核活动、发现、结论和报告。

4）职业素养：具备职业谨慎和判断力，具备从事审核、认证所需的技能。

注：独立性、道德行为、公正表达和职业素养等原则参考了 GB/T 19011 中的相应内容。

4.2 审核员的能力

扬标依据 ISO 17021 要求，对每个技术领域所需的能力，对相关具体的认证方案，认证活动中的职责和作用进行了确定。审核员的能力通过使用能力审查表格被扬标确认和记录。个人隐私信息安全管理体系审核员需要收集以下教育、知识和技能以确认其能力：

教育：候选人要完成大学或类似的教育机构的学习。大学专业符合 ISO27001 要求。

经历：4 年在 IT 行业的全职实操工作场所经验，包括 2 年有关信息安全的职责。

培训：候选人－审核员- 必须完成 CCAA 信息安全审核员注册培训。

审核经历：在具有 ISO 9001 审核员资格的基础上，需要完成相应信息安全管理体系审核人天经历，及完成 ISMS 审核员资格见证过程，成为 ISMS 正式审核员。

4.3 项目负责人

基于培训和经验的基础上，产品经理必须具有资深的个人隐私信息安全管理知识和能力，有能力批准合同评审、确认认证项目范围的适当性、确定所需的资源的可用性，定义项目需求所需的能力、实施内部技术审查及审查所有内部确认和审核程序。

4.4 技术专家

技术专家可以为审核组提供技术支持与特定的知识输入，例如：

1）个人隐私信息安全维护和运行决策方法； 个人隐私信息安全配置管理；

2）个人隐私信息安全投资决策方法， 个人隐私信息安全相关的技术标准和法规要求；

3）系统工程、信息系统、可靠性管理；

4）行业特定的应用程序和管理等。

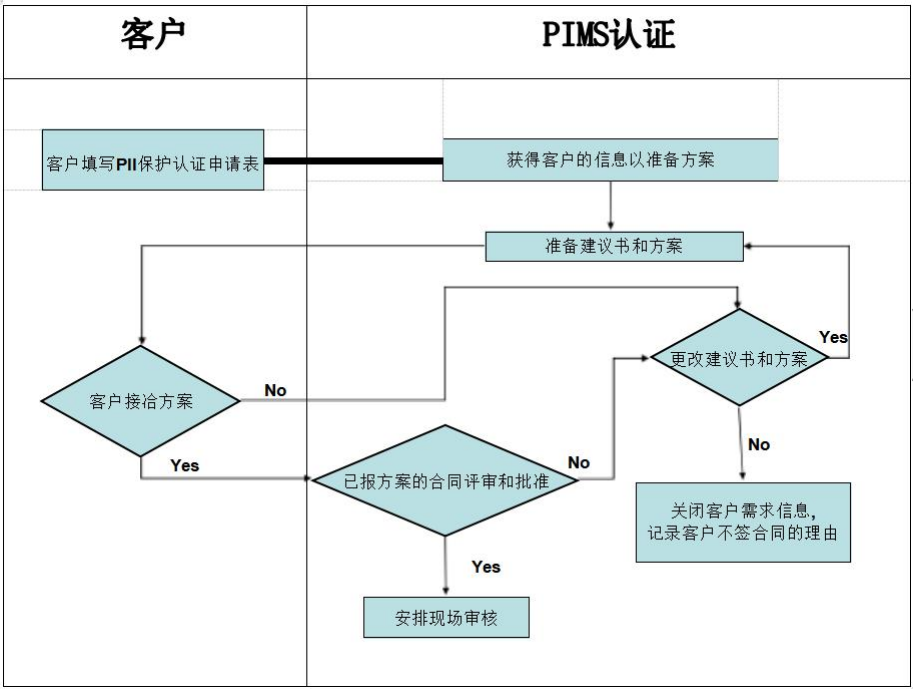
专家必须能够通过资格、工作经验、相关的专业知识证明其能力,但是他们不需要个人隐私信息安全管理体系审核的经验或培训。

4.5 认证决定人员能力

该体系认证决定人员的职能是做出认证决定。认证决定人员应是具有能力的个人隐私信息安全管理体系审核员，具有个人隐私信息安全管理体系的技术审查和评审的经历和能力。认证决定人员应进行人员能力评价并由总经理批准资格。

5 申请和合同评审

5.1 销售和申请评审流程



5.2 认证申请

收到潜在客户的要求，当地的销售人员会向组织发送 ISO/IEC27701 《认证申请表》 ，便于组织提供认证所需的信息。除了组织的一般信息外， 申请个人隐私信息安全管理体系认证还需要提供以下信息：

1）提出申请认证的范围（包括现场、多现场、总部）

2）审核类型 （初审、再认证、转证审核）

3) 认证认可

4) 审核语言

5）组织的主要活动、产品和服务

6）负责个人隐私信息安全管理的组织代表

7）个人隐私信息安全管理有效人数

8）个人隐私信息安全管理体系与哪些体系整合

9）与个人隐私信息安全利用和管理相关的法规要求

10）个人隐私信息安全管理认证范围内的个人隐私信息安全业务类型

11）个人隐私信息安全管理认证范围内的个人隐私信息安全业务类型的风险水平

5.3 审核人日数的确定

5.3.1 审核人日数的确定标准

审核时间确定基于个人隐私信息安全管理体系有效员工人数，计算审核的人日数

•每个产品的特定规则　　•客户现场和流程的复杂性

有效人数	A-审核时间（ISO27701）	B-审核时间（已通过 ISMS）
0-10	5	4
11-15	6	5
16-25	7	6
26-45	8.5	7
46-65	10	8
66-85	11	9
86-125	12	10
126-175	13	11
176-275	14	12
276-425	15	13
426-625	16.5	14
626-875	17.5	15
876-1175	18.5	16
1176-1550	19.5	17
1551-2025	21	18
2026-2675	22	19
2676-3450	23	20
3451-4350	24	21
4351-5450	25	22
＞5450	沿用以上规律	

审核时间计算表

5.3.2 审核人日数的计算与调整

5.3.2.1 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	采用的方法	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 员，从事重复或 相似过程(用户信息 安全控制的终端用 户）	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。	人数平方根， 四舍五入到更高的 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 + √400+（（（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）。

5.3.2.1 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。无人值守现场增加 0.5 人天。

5.3.2.2 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。

5.3.2.3 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 ISO 27001 认证。ISO 27001 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 的性能；

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。

5.3.2.4 调整因素

5.3.2.5 增加审核时间：

需要额外审核时间的其他因素包括：

•涉及 PIMS 范围内多个建筑物或地点的复杂物流；

•会说一种以上语言的工作人员（需要翻译或阻止个别审核员工作）或以一种以上语言提供的文件；

•需要访问临时现场以确认其管理的永久现场的活动系统须经认证；

•处理敏感的个人数据

•行业或处理高敏感度的额外或异常数据保护方面或监管条件信息（例如国家安全、犯罪记录等）

5.3.2.6 缩短审核时间：

允许缩短审核时间的其他因素包括：

•无/低风险产品/流程；

•涉及单一一般活动的过程（例如仅服务）；

•在组织控制下从事相同任务的人比例很高；

•客户对认证的高度准备（例如，已经通过另一个第三方认证或认可）；

•不负责系统/软件的设计和开发

•不是面向 B 到 C（直接面向消费者）；

•仅限国内/本地业务（没有与个人身份信息/隐私相关的若干规定）

•经主管当局批准的行为准则或公司约束性规则；

5.3.3 培训审核员

审核持续时间不包括审核员接受培训的时间和技术专家的时间。

5.3.3.1 理由和记录

审核时间计算步骤记录在模板“合同评审表”（ ISO 27701）中。

对于每个调整系数，说明如何将其应用于组织以及批准的削减水平。

审核人天的判定步骤记录在模板“合同评审表”（ISO27701）中。

5.3.3.2 审核类型

5.4.1.1 初始审核

上述计算的审核持续时间适用于初始审核（第 1 阶段+第 2 阶段）。

第一阶段的持续时间通常在初始审核总持续时间的 20%到 30%之间，第二阶段审核不少于 1 天。它必须至少是初始审核总持续时间的 50%，计划和报告不得超过整个审核持续时间的 30%；

5.4.1.2 监督审核

在初始认证周期内，每年用于监督的总时间约为初始认证审核所花时间的 1/3。最低年度监督审核时间为 1 天。

当采用 6 个月监督时，年度监测时间除以 2，四舍五入到下一个整数。

5.4.1.3 再认证审核

重新认证审核时的合同评审应考虑最新的组织结构信息（考虑到上一个周期中发生的所有更改）和审核时间的计算方式是对那家公司的初步审核。

重新认证审核的时间是该计算结果的 2/3，而不是原始初始认证审核时间的 2/3。如果在上一个周期（重大或未完成）中发布了大量不符合项，则可以增加时间。

5.4.1.4 多现场审核

与 YB《多现场审核管理规定》中的要求相同。

5.4.1.5 基于样本的方法

如果一个客户组织有多个现场满足以下三个标准，那么多个现场的基于示例的方

法。

认证审核应用于：

a） 所有营业点均在同一 PIMS 下运营，PIMS 由中央管理和审核，并受中央管理管理评审；

b） 所有地点都包括在客户组织的内部 PIMS 审核计划中；

c） 所有营业点均包含在客户组织的 PIMS 管理审查计划中。

初始合同评审应尽可能确定现场之间的差异，以便确定取样水平。样品应根据以下列出的因素进行部分选择，部分非选择性，并应导致选择不同地点的代表性范围，不排除抽样的随机因素。至少 25%的应随机抽取样品。

5.4.1.6 取样标准

认证机构在考虑到

a) 总部和现场的内部审核结果，

b) 管理评审的结果，

c) 场地大小的变化，

d) 现场商业目的的变化，

e) 个人信息管理系统的复杂性，

f) 不同地点信息系统的复杂性，

g) 工作实践的变化，

h) 所开展活动的变化，

i) 与关键信息系统或处理敏感信息的信息系统的潜在互动，

j) 任何不同的法律要求。

从客户范围内的所有现场中选择一个具有代表性的样本组织的 PIM;该选择应基于判断性选择，以反映 B 项中提出的因素以及一个随机元素。这种选择不必在审核过程开始时进行。一旦中央办公室的审核完成。在任何情况下，应将样本中包含的地点通知中央办公室。这可以是相对较短的通知，但应留出足够的时间进行审核准备。

5.4.1.7 样本大小

多现场组织的审核和抽样方法，其中所有现场的性能都非常相似过程/活动。确定在审核现场时所采取的样本，作为审核和认证的一部分多现场组织。 应记录多点取样

的每次申请，以证明其正在进行操作根据本文件。

以下计算是 YB 用于多现场组织抽样的基本程序。最小数量每个审核现场的访问次数：

•初始审核：样本大小应为远程现场数量的平方根：（y= √x），四舍五入到上整数。

•监督审核：年度样本的大小应为远程现场数量的平方根，0.6 作为 a 系数（y=0.6√x），四舍五入到上整数。

•再认证审核：样本大小应与初始审核相同。然而，在管理制度经过三年的实践证明是有效的，样本规模可以缩小乘以系数 0.8，即：（y=0.8 √x），四舍五入到上整数。

PIMS 中包含的每个存在重大风险的场所在认证之前都要经过认证机构的审核。

审核方案应根据上述要求进行设计，并涵盖范围内具有代表性的样本三年内获得 PIMS 认证。

如果在总部或单个现场发现不符合项，纠正措施程序，适用于总部或证书覆盖的所有场所。

审核应处理客户组织总部的活动，以确保单一的 PIMS 适用于所有现场和在操作级别提供集中管理。审核应解决上述所有问题。

如果 YB 对管理层涵盖的活动进行风险分析，则应增加样本的大小或频率需认证的系统表明了与以下因素有关的特殊情况：

•现场规模和员工人数（例如一个现场超过 50 名员工）；

•活动和管理系统的复杂性或风险水平；

•工作实践的变化（例如轮班工作）；

•所开展活动的变化；

•投诉记录和纠正和预防措施的其他相关方面；

•任何跨国方面；以及

•内部审核和管理评审的结果。

在这种情况下，确定并记录抽样计划和方法。

当组织有一个分公司的等级体系时（例如总（中央）办公室、国家办事处、地区办事处、地方办事处等分支机构），上述初始审核抽样模型适用于每个级别。

5.4.1.8 附加场地

在申请加入已认证的多现场网络的新现场组时，每个新现场组应作为确定样本量的一个独立的集合。在证书中包含新组之后，新地点应与先前地点累积，以确定样本

量，以供日后监督检审核或再认证审核。

如有新的地盘申请加入已获认证的多地盘组织，则该地盘在加入前须接受审核包括在证书中，以及审核计划中的监督。

5.4.1.9　多现场组织的审核方法

审核计划应包括所有现场的认证（第 2 阶段）、监督审核和再认证审核。

在一个日历年内，应涵盖 30%的现场，四舍五入至整数。每次审核将包括中心功能。为第二次监督审核选择的场所通常与为第一次监督审核选择的场所不同，审核计划的设计应确保认证涵盖的所有过程在每个周期内对范围进行审核。

6 审核准备

该流程适用于各种审核的准备过程， 以及个人隐私信息安全管理体系认证过程的一阶段、二阶段、监督审核、转换审核和再认证审核。

6.1 团队分配 ： 审核组应具备必要的能力以覆盖个人隐私信息安全管理体系审核的范围，必要时，应包括合格专家的技术支持。当个人隐私信息安全管理体系审核与另外标准进行结合审核时，审核组在涵盖的标准认证范围内均应具备相应的能力。

6.2 审核计划：审核计划应明确认证范围内的所有过程。审核计划应采用扬标审核计划的文件模板，并在审核前发送给审核组成员和客户。

6.3 监督审核计划：监督审核计划应与客户沟通商定后完成，需考虑以下内容：

•范围的变化

•认证范围内个人隐私信息安全业务的增加或减少

•与合规性相关的议题

•以往的整改措施

当在一个审核现场存在监管合规问题，审核组长应该分配适当的时间，审查客户的纠正/预防措施相关的问题。监督审核至少每年一次。

7 认证审核

7.1 现场和非现场审核

7.1.1 审核时间包括现场审核时间和审核员所花费的策划、报告的非现场时间。现场所用的时间不少于总人天的 80%。

7.1.2 当需要额外时间进行策划和编制报告时，应考虑增加策划和编制报告的时间，但不能由此减少现场审核时间。

7.2 一阶段审核

7.2.1 一阶段审核的目的和重点如下：
1）审核组织的管理体系文件；

2）评估客户的场所、地点和有效人数的具体情况，并与客户人员进行讨论，以确定二阶段审核的准备情况；

3）评审客户的状态以及对标准要求的理解，特别是对关键绩效、风险等级、关键个人隐私信息安全、过程、目标和管理体系的运行方面；

4）收集和确定必要的信息资料，包括管理系统的范围，过程，场所，以及相关的法律和法规合规性；

5）评审二阶段审核的资源分配，与客户针对二阶段审核的具体安排达成共识；

6）确认审核时间，策划时考虑场所的复杂程度（园区、个人隐私信息安全、多个建筑…）和过程。

7）评价内部审核和管理评审是否策划和实施， 评价管理体系的实施水平证明客户为二阶段审核做好准备；

8）一旦该组织在一阶段后宣布“准备就绪”，就需要进行二阶段审核，评估客户是否满足 ISO 27701 国际标准的所有要求。

7.2.2 一阶段审核的输出包括：

- 批准的一阶段审核计划
- 审核报告以及二阶段的建议
- 建议的二阶段审核计划

• 文件评审发现/ 或二阶段审核担心成为不符合的事项。

7.2.3 一阶段审核所产生的关注事项应在 90 天内关闭或在较早的二阶段审核前关闭。在审核组组长推荐的情况下，可以进入二阶段审核过程。

7.3 二阶段审核

7.3.1. 二阶段审核是完整过程、完整条款、完整体系的审核。审核组长必须确保在审核过程中标准适用的所有条款的要求被验证。

7.3.2. 二阶段审核的目的是评价个人隐私信息安全管理体系实施的有效性，二阶段审核是现场审核。至少应包括以下内容：

• 关于符合适用管理体系标准或其他规范性文件的所有要求的信息和证据；

• 风险评估、绩效监控、测量、报告和对关键绩效目标指标的评审（符合适用的管理体系标准或其他规范性文件的期望）

• 客户管理体系与法律合规性

• 客户过程的运行控制

• 内部审核和管理评审

• 方针政策和管理职责

• 规范性要求与公司政策、绩效目标和指标之间的联系，任何适用的法律要求，职责，人员的能力，操作，程序，绩效数据和内部审核结果和结论。

7.3.3. 二阶段审核完成后编制审核报告，包括二阶段的审核发现。二阶段发现的不符合项应在二阶段审核最后一天的 90 天内进行整改关闭。如果不符合（一阶段、 二阶段、监督审核和再认证审核）在审核结束后的 90 天内没有关闭，应在 90 天期限结束后，最多 15 天内进行现场后续访问。

7.3.4 如果跟踪访问和不合格关闭未在上述期限内结束，审核被认为是无效的。
不符合关闭后，最终审核报告应递交给客户。并由 POV 做出认证决定。

7.4 不合规议题

如果审核员发现或怀疑个人隐私信息安全管理体系可能存在不符合相关法律/法规，这个信息应该清楚地传达给客户。审核员应确保任何适用的外部报告的要求。

8 审核实现

8.1 首次会议

应与客户的管理层举行一次正式的首次会议，如有必要应包括负责拟审核部门或过程的人员，并应记录与会人员。首次会议应由审核小组组长主持，其目的是简单说明审核活动将如何开展，并应包括下列信息。说明的详细程度视客户熟知的审核过程的程度而定。

a）介绍参与人员，包括简介其角色；
b）确认认证的范围；

c）与客户确认审核计划（包括审核的类型和范围、目标和依据）、任何变化以及其他相关安排，如末次会议的日期和时间、审核小组和客户管理层之间的临时会议；

d）确认审核小组和客户之间的正式沟通渠道；

e）确认具备审核小组所需的资源和设施；
f）确认保密相关问题；

g）确认审核小组的相关工作安全、紧急及安全事项；
h）确认陪同人员和观察员，其角色和职责；

i）报告方式，包括对审核发现的分级；
j）审核可能提前终止的情况；

k）审核组长及审核小组对审核负责，且应控制审核计划的执行，包括审核活动和审核线索；

l）如适用，确认前次审查或审核发现的状态；
m）根据抽样进行审查所需使用的方法和过程；

n）确认审核中使用的语言；

o）确认在审核中，将会向客户及时通报审核进度及任何关注的问题；
p）客户提问的机会。

参加首次会议的关键人员有：总经理或相当人员、部门（审核相关）负责人、管理层代表。

8.2　观察员及陪同人员

8.2.1 观察员

安排观察员出席现场审核及其理由应在实施审核前得到 YB 和客户的认可和同意。

审核小组应确保观察员不会影响或介入审核过程或审核结果。观察员可以是客户组织成员、顾问、见证认证机构人员、监管人员或其他合理的人员。

8.2.2 陪同人员：

每位审核员均应有由一名陪同人员陪伴，审核组长与客户另行同意的情况除外。陪同人员分配给审核小组协助审核。审核小组应确保陪同人员不会影响或介入审核过程或审核结果。陪同人员的职责包括：

a) 及时联系和安排访谈；

b) 安排访问现场或组织的具体部分；

c) 确保审核小组成员了解并遵守有关现场安全和保安过程制度；

d) 代表客户见证审核；

e) 根据审核员的要求提供澄清或信息。

f) 语言或专用术语翻译

8.3 不符合项和审核发现

8.3.1 审核员应在审核报告中提出并记录不符合项出现的领域。客户将调查其根　源，并向扬标提出纠正措施建议。报告还应包含合理的个人隐私信息安全管理体系的改进机会。小组组长应与客户商定如何处理并关闭不符合项。

8.3.2 轻微不符合项；可采用小组组长批准的纠正措施计划，在规定的时间内提供改善证据，将在下一次访问时验证纠正措施的实施。

8.3.3 严重不符合项；纠正和纠正措施在 90 天内关闭，通过文件/记录证据审查验证，或如合适且经客户同意，通过在额外的跟踪访问验证。
对于换发新证，将限制纠正和纠正措施的时间，以便在证书过期前实施措施。

8.3.4 提出改进机会时，小组组长应确保确实是改进机会而非下述定义中的不符合项：

1) 严重不符合项

客户体系中没有提及解决标准的某一要求；

频繁的或无故不遵循公司体系中的具体书面要求；

未能达到系统要求的基本目的；

客户管理体系未能达到法律或法规的要求*；

标准或公司体系的同一要求出现多个轻微不符合项；
公司无故不纠正不符合项。

2）轻微不符合项 ：所审核的体系未能满足规定要求，但不属于严重不符合项。

3）改进机会：当前符合过程/活动/文件，但可以通过改进过程的效率或有效性为客户带来利益。

4）观察项：需要关注地方，过程、文件或活动目前符合要求，但如果不改进的话可能造成体系、产品或服务要求的不符合。

8.4 末次会议

8.4.1 应与客户的管理层举行一次正式的末次会议，如有必要应包括被审核部门或过程的负责人员，并应记录与会人员。末次会议应由审核组长主持，其目的是陈述审核结论，包括发证相关建议。任何不符合项应以客户可以理解的方式进行陈述，并应就相应的回应时间安排达成一致。

8.4.2 末次会议还应包括下列信息。具体详细程度应与客户熟知的审核过程一致：

a）告知客户，审核证据的收集是采用抽样方法，因此可能存在不确定性；
b）审核结果报告的方法和时间安排，包括对审核发现的分级；

c）认证机构处理不符合项的过程，包括任何与客户证书相关的结果；

d）客户对审核中识别的任何不符合项提出纠正和纠正措施的时间安排；

e）认证机构审核后的活动；

f）投诉处理和上诉过程信息。

8.4.3 应给客户提问和澄清的机会。任何审核小组和客户对于审核发现或结论的不同意见均应得到讨论，并尽可能解决。无法解决的意见分歧应予记录，并尽快报告当地产品经理。末次会议的与会者一般应为首次会议的与会者。

8.5 审核报告

8.5.1 每次审核（第一阶段和第二阶段、监督审核、转证审核及再认证），审核小组将撰写审核报告。

8.5.2 一般的做法是在现场完成报告，并在末次会议上向客户陈述。

如果需要额外工作，可在非现场完成审核报告，应在审核后 10 天内提交给扬标办公室，办公室审批后交给客户。

如果本地做法要求审核报告仅在不符合项关闭后提交，则最终报告应在不符合项关闭后 7 天内提交。

8.5.3 最终报告应由审核小组组长整合并总结。在初次审核中，第二阶段审核报告的总结部分应包括并总结第一阶段和第二阶段的发现。

8.5.4 审核员的记录是审核报告的重要组成部分，因此应得到保留，可以是审核员最初的手写稿，也可以转换成电子最终报告。

8.5.5 所有审核报告中均应包含或参考下列信息：

文件评审结果；

客户组织信息安全风险分析结果；

使用的审核总时间，以及文件审核、现场审核和报告所用时间的详细说明；
审核涉及的领域（如认证要求和被审核的场所），包括：

跟踪重大审核跟踪，

使用的审核方法，

观察结果，包括积极的（例如值得注意的特征）和消极的（例如潜在的不符合项），

已识别的任何不符合项的详细信息，并附有客观证据及其要求，

对客户组织的 PIM 符合认证要求的意见，

明确的不符合项声明，引用适用性声明的版本，

与客户组织以前的认证审核结果进行任何有用的比较（其中适用）。 对内部 PIMS 审核和管理评审的依赖程度；

审核小组就客户组织的个人信息管理系统是否应得到认证的建议，以及证明此建议的信息。

8.5.6 审核证据

完成的调查问卷、检查表、观察结果、日志或审核员注释可能构成审计报告的组成部分。

如果使用这些方法，这些文件应提交给认证机构，作为支持认证决定。审核过程中评估的样品信息应包括在审核报告中，或其他证明文件。

报告应考虑客户组织采用的内部组织和程序的充分性给 PIM 信心。

8.5.7 认证范围的验证

审核组应

•确保客户的信息安全和隐私风险评估和风险处理适当反映并延伸至认证范围内规定的活动范围，

• 确认这反映在客户的 PIM 范围和适用性声明中，

• 验证每个认证范围至少有一个适用性声明，

• 验证认证范围是否包括 P/I 处理。

应在客户 PIMS 范围和适用性声明中验证多站点范围。

8.6 发证和维持证书建议

8.6.1 第二阶段审核报告应包含授予或不授予证书的建议。

8.6.2 监督审核报告应包括任何可能导致证书暂停或撤销的问题。此类情况下，档案将提交技术经理进行审查或决定。

8.6.3 再认证审核报告应包括换发新证的建议。

8.7 跟踪审核

8.7.1 在认证周期的任何阶段（第二阶段、监督和再认证），如需要现场验证主要不符合项或多个轻微不符合项的纠正措施结果，审核组长应告知客户需进行额外的跟踪审核。

8.7.2 如果投诉不能远程解决或投诉的重要程度要求在下一次计划审核前解决，也可安排临时通知访问。临时通知访问也可在客户证书暂停后进行。这些审核的过程与任何一般审核相同，其范围将针对投诉调查或决定是否可以解除暂停。

8.7.3. 如果进行跟踪审核，扬标办公室将与客户安排日期，同时与审核组长商定一位最适合进行现场跟踪审核的审核员。

8.8 不符合项的关闭

8.8.1 主任审核员应审核客户对不符合项响应的 3 部分内容：纠正、根本原因分析及纠正措施。在审查这四部分时，审核员要关注计划和计划得到实施的证据。

审核员应在末次会议上向客户简要陈述处理不符合项的时间安排，以及强制步骤。

8.8.2 可接受的实施证据包括：

a. 提供充分的证据证明计划已经根据响应的描述（并根据时间安排）得到实施。

b. 关闭报告的不符合项不一定要全面证据；某些证据可能在未来审核中验证纠正措施时进行审查。

9 认证决定

扬标认证技术中心应按规定的程序对所有的审核资料和评估报告进行评审、批准，做出认证决定，并及时向申请人送达认证决定和审核报告。

现场审核组成员不得参与该项目的认证决定。

认证通过的，扬标认证向申请人签发认证证书，证书有效期为 3 年。

9.1 证书内容

所有证书都应使用扬标的标准证书模版，至少应包含下列内容：

1）被认证的管理体系客户的名称和地址，多现场的认证应明确总部和所有其它场所，每个现场可以在附件中列出，总部应列在证书的主页上；地址必须精确到可以区分其场所而不导致混淆；

2）范围应指明提供的产品（包括服务），过程以及相应的个人隐私信息安全类别，当不同的现场涉及不同的过程和个人隐私信息安全时，应在证书上予以明确，每个场所范围的不同应在证书附件中体现；

3）管理体系标准或相关的管理体系规范文件及其版本或发布年度（如 ISO27701：2019）；

4）适当的产品，过程或服务；

5）日期：生效日期/批准日期。

6）办公室地址： 认证决定中心地址

7）签字（非强制）；证书号；认证周期内更改证书的日期。

9.2 证书有效性

9.2.1 认证周期 自认证决定之日起三年减一天。再认证的决定应该在三年周期内完成，应在现有证书的有效期之内做出。

9.2.2 如果再认证在原有证书到期前三个月内完成，则新的认证周期自原有证书失效日算起后延三年（原周期保持不变）。

9.2.3 如果现有证书有效期短于三年，则不需要重发证书将有效期延长到三年。

如果认证决定在现有的认证证书失效之后完成，则证书的连续性将被打破，新证书应自再认证的批准日期开始计算。

9.2.4 审核周期：监督审核和再认证审核的时间安排应以第二阶段审核的最后一天为基准。

9.2.5 延期：证书期满后不允许延期。参见“审核准备”。

9.3 技术评审

9.3.1 认证决定人员应通过人员能力评价经总经理任命并为该体系的审核员，且不应是该认证项目的审核组成员。认证决定人员或其指定人员按照评审标准进行报告的技术评审。

9.3.2 技术评审人员应保持评审过程的记录并包括接受认证的理由，将其记录应在证书申请表中。

9.4 认证决定中心审核

9.4.1 所有的技术评审的要求都满足后，下列文件应被提交到认证决定中心进行最终的认证决定审核：

证书申请表；
审核报告；

关闭妥当的不符合项报告；

再认证和转证审核中需要原有证书副本；
认证决定人员的评审记录。

9.4.2 认证决定中心依照评审准则做出最终的认证决定。

9.5 证书的发放

证书只有在做出正面的认证决定后才能发放，证书可以以硬拷贝或者电子版进行发放。最终的证书副本应在机构存档。

9.6 监督审核报告的技术评审

9.6.1 监督审核报告的评审作为审核员年度表现评估的一部分。如果审核员提出可能导致证书暂停或撤销的问题时，监督审报告由由该审核资格的认证决定人员进行评审。

9.6.2 在重再认证时，作为周期内管理体系的表现评审的一部分，应评审监督审报告，必要时应对再认证计划进行调整。在申请签署的时候提交监督审核报告的评审结果。

9.7 认证周期内的变更

在认证周期内发生了范围和场所的变化的时候，应得到认证决定中心的批准才能发放新的证书。

10 暂停、撤销和取消

暂停：是指在一定时间内禁止客户使用扬标的管理体系证书进行广告和推广。

撤销：是指扬标撤销客户的认证并要求客户返还其管理体系认证证书和认证标记,撤销通常是暂停之后客户不能提供有效的纠正措施，扬标采取的处理方法。

取消：是撤销客户的认证证书和认证标记并终止与客户的认证合同。取消应在合同中达成一致。

10.1 证书的暂停

10.1.1 证书的暂停期限最多不能超过六个月，在暂停期间客户不能使用认证证书进行广告和宣传活动。客户针对扬标在开具的书面不符合项不能采取有效的纠正措施时，扬标必须对证书进行暂停处理。

10.1.2 下面是暂停的一些情况举例：

1) 在特别监督审核中开具了严重不符合项，该不符合项显示客户没有能针对以往的不符合项采取有效的纠正措施。

2) 或不能在规定的时间内接受监督审核。

3) 或被发现认证标记使用不当，且在被指出后没有采取有效的解决措施。

10.1.3 在暂停后应采取下列措施：

1) 如果客户由于管理体系变更或恶化而担心下次例行的监督审核将出现严重不符合项而申请暂停，扬标应要求客户采取必要的纠正措施并继续实施计划的监督审核，以记录其实际情况。在现场审核客户后，由最长 90 天的期限以纠正书面不符合项，并安

排特殊监督。

2）如果在规定的时间内客户没有能解决不符合项的问题，则扬标办公室通知客 户的高层领导，其证书必须被暂停，此流程的书面通知应被发送到客户处，并保留递送的证据。

3）暂停期限不能超过 6 个月，此后应安排特殊监督审核以安排情况的评估。

4）如果在后续的特殊监督中客户的管理体系能被证明符合要求，则审核组长应做出继续注册的推荐意见，认证决定人员将批准客户证书的有效性的恢复，并按照正常时间安排监督审核。

5）如果审核员发现客户采取了纠正措施以解决不符合项的问题，但是还有部分措施没有得到实施，则审核组长可以推荐将暂停期延长三个月。

6）如果在特殊监督审核中审核组长认为客户不愿或不能关闭不符合项，则应向认证决定人员推荐撤销证书。这一特殊监督的决定应由认证决定人员验证并经总经理审批。

10.2 证书的撤销

10.2.1 证书的撤销是非常严肃的举措，只有当正常的纠正措施流程，包括暂停，都无法成功地证明其满足管理体系认证地要求时，才能采用。当认证决定人员收到撤销证书地推荐意见时，应遵守程序做出裁定意见。按照公司流程实施证书撤销。

10.3 合同的取消

10.3.1 合同的取消可以由客户自行提出，也可以由扬标撤销证书导致。

10.3.2 所有情况下，扬标应采取所有合理的努力以保持和抱怨客户或没有满足要求但愿意采取纠正措施的客户的合同；

10.3.3 如果客户要求取消合同，相关的认证决定人员应以书面的形式通知客户返还认证证书和认证标记。

10.3.4 如果合同的取消是由于上述结果导致，应在通知客户撤销证书的同时通知客户的高层管理者；

10.3.5 在上述任何情况，客户都应被要求返还认证证书和标记。扬标总部和相关的认证决定中心应得到通知，以更新其信息。

10.3.6 针对暂停和撤销认证的申诉：如果申述成功，并且证书被恢复，则其原有的认证周期和有效期保持不变。

11 受理申诉和投诉

11.1 申诉是指对扬标作出的决定或对扬标作出的投诉有效性决定的申诉。投诉是指对扬标提出的书面投诉。

11.2 所有申诉和投诉应当由扬标的技术评定部记录在案，技术评定部应当联络相关部门，解决申诉或投诉问题。申诉或投诉结果应进行记录。申诉和投诉流程和时间限制应当告知申诉人和投诉人。

11.3 申诉流程

接到申诉后，技术评定部负责人应当确定他/她自己是否与事件有关。如果是，指定一位合适合格且内部立场独立的人。如果不是，他/她可以进行调查。后续步骤包括：

1）答复申诉人申诉已收到并将处理;

2）通过审查申诉和关联文件（合同评审、核查报告、认证决定细节），调查申诉理由;

3）编写一份报告，并将报告同其他文件一起提交给技委会;

4）技委会审查案件，并根据技术评定部经理提交的申诉和报告作出决定;

5）技委会作出的决定应当告知申诉人。认证委员会作出的决定是权威性的、不可改变的。

11.4 投诉流程

11.4.1 接到投诉后，技术评定部经理应当确定他/她自己是否与事件有关。如果是，指定内部一位合适合格且立场独立的人。如果不是，他/她可以进行调查。在某些案件中，可以启动一次审核来进行调查，但必须告知客户相关理由。接下来的步骤是按照 扬标门户网站主页上的参考文件进行。 确认回执应当发送给投诉人，而且调查结果应当在适当的时候传达给投诉人。

11.4.2 为了管理每年的投诉，投诉应进行记录；

12 记录管理

12.1 目的和范围

本部分适用于所有证明符合扬标认证部程序的记录。规定了记录的标识，收集， 索引，查询，存档，储存，维护和处置的方法以确保它们可随时查阅和防止损坏和丢失。

12.2 责任

所有这些保管和维护上述规定的记录职责见 YB 组织架构概述。

12.3 记录

记录可以硬拷贝或电子存档。

12.4 标识，收集和索引

12.4.1 表 2 规定了用来证明与扬标认证部程序一致性的最低要求。 并非所有的记录都被保存在扬标认证的档案室；

12.4.2 应制定记录和保存期限表。应建立本地控制来确定资料的位置或者一个人 /一个部门负责记录的收集和维护。本地控制同时还描述如何索引记录和描述在什么阶段存档和最后被处置。

12.5 存档和储存

记录以保护它们不被破坏和变质的方式存档。在每一个规定的保留期限内，在存档或处置之前，当前的工作文件应当以可以随时供检索和使用的方式储存。

12.6 维护和处置

记录应当由合适的负责人来维护，就像在个人工作描述中的那样。

记录应当如下表所述，在保留期限满后存档和最终处置也要确保处理的保密性。

记录	最少保留期限
认证规则或实施细则	保持目前有些版本
管理评审	3 年
审核(核查) 计划时间表	3 年
内审（总部）	3 年

内审	3 年
外审	3 年
管理体系程序	保持目前有些版本
作废的程序和说明	3 年
标准和法规	保持目前有些版本
人事记录	直到离职，审核员，生产和销售加一个认证周期；讲师加一年
	人事主管加一年
投诉（内部）	3 年
投诉（外部）	6 年
纠正和预防措施记录	3 年
申诉	6 年
吊扣和取消证书	3 年
电脑系统	保持目前有些版本
客户（数据库）	保持目前有些版本
公正委员会	6 年
技委会	6 年
客户认证资料	一个认证周期加目前