江西腾标认证有限公司

隐私信息管理体系认证规则

受控状态：（ 受控 ）

文件编号：TB-GZ-044

版本号：B/2

编制：技术部

审核：张辉根

批准：周春阳

首次发布日期：20221220　　首次实施日期：20221220　　第6次修改实施：20260423

目录

1. 适用范围

1.1. 本规则用于规范依据ISO /IEC 27701:2025信息安全、网络安全和隐私保护-隐私信息管理系统-要求与指导标准开展的隐私信息管理体系认证活动。

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，明确江西腾标认证有限公司（以下简称：TB）对认证过程的管理责任，保证通过认证企业隐私信息管理体系认证活动的规范有效。

1.3. 本规则是TB与申请获证组织在企业隐私信息管理体系认证活动中的基本要求，TB在该项认证活动中应当遵守本规则。

2. 规则性参考文件

认证依据：ISO /IEC 27701:2025信息安全、网络安全和隐私保护-隐私信息管理系统-要求与指导

注：本规则内容引用的文件提及的标准时，均指认证活动发生时该标准、规则规范的有效版本。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。

3. 术语和定义

采用上述规范性引用文件提出的术语和定义。

4. 对认证人员的要求

4.1. 认证审核员

应取得任意一个质量管理体系/环境管理体系/职业健康安全管理体系/信息安全管理体系/信息技术服务管理体系/能源管理体系/HACCP/食品管理体系/森林认证/知识产权管理体系的审核员注册证书，并且通过ISO /IEC 27701:2025信息安全、网络安全和隐私保护-隐私信息管理系统-要求与指导培训考试合格，可以实施隐私信息管理体系的认证审核。

4.2. 合同评审与审核策划人员

应取得任意一个管理体系审核策划和合同评审人员资格，并且通过ISO /IEC 27701:2025信息安全、网络安全和隐私保护-隐私信息管理系统-要求与指导考试合格，可以实施隐私信息管理体系审核策划和合同评审。

4.3. 认证决定人员

1) 应取得任意一个管理体系的认定决定资格的人员，并且通过ISO /IEC 27701:2025信息安全、网络安全和隐私保护-隐私信息管理系统-要求与指导考试合格，方可实施认定决定。
2) 认证决定人员应为TB的认证人员，不得为审核组成员。
3) 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。

注：认证人员应当遵守与从业相关的法律法规，对认证审核活动及相关认证审核记录和做出的认证审核报告、认证结论的真实性承担相应的法律责任。

5. 初次认证程序

5.1. 受理认证申请

5.1.1. TB应向认证委托人（申请组织）至少公开以下信息：

1) 可开展认证业务的范围、获得认可的（如有）情况以及分包境外认证机构业务的情况。
2) 开展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ISO /IEC 27701:2025信息安全、网络安全和隐私保护-隐私信息管理系统-要求与指导建立隐私信息管理体系，且运行满3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) 若之前获得的隐私信息管理体系认证证书因组织自身原因被原发证机构暂停、撤销或注销的，应已满一年（适用时）；若原发证机构被国家认监委撤销资质的，应已满三个月（适用时）；
7) 其他应具备的条件。

5.1.3. TB应当要求认证委托人至少提交以下资料：

1) 认证申请书：申请书应包括申请认证的生产、经营或服务活动范围及活动情况的说明。
2) 法律地位的证明文件的复印件：若隐私信息管理体系覆盖多场所活动，应提交多场所清单，并附上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行政许可证明、资质证书、强制性认证证书等的复印件。
4) 隐私信息管理体系成文信息（适用时）。
5) 依据ISO /IEC 27701:2025信息安全、网络安全和隐私保护-隐私信息管理系统-要求与指导建立的隐私信息管理体系成文信息。
6) 其他应提交的与认证申请范围相关的资料。

5.1.4. 认证标准换版

1) TB会严格执行国家认监委发布的管理体系认证标准换版工作要求，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。
2) 当认证依据标准发生换版时，TB应在换版标准发布后及时告知获证组织，并明确过渡期安排。获证组织应在过渡期内完成体系文件的调整，并通过监督审核或再认证审核验证对新版标准的符合性。
3) 对于不愿或不能在过渡期内完成标准换版的获证组织，TB应按规定做出暂停或撤销认证证书的处理。

5.2. 申请评审

5.2.1. 评审内容与能力确认

TB申请评审人员应当对认证委托人的认证申请资料是否齐全进行确认，对其有效性进行审查，并保持评审记录，以证明TB能够对拟实施认证的申请方完成以下工作：

1) 明确申请的认证范围；
2) 界定隐私信息管理体系所覆盖的范围；
3) 确定实施审核所需的能力；

4) 考虑认证委托人申请的认证范围、场所及活动的复杂性，确定完成审核需要的审核时间；
5) 确认体系已运行 3 个月以上。

5.2.2. 受理申请：

1) 对符合5.1.2.条款要求的，TB可决定受理认证申请；
2) 对不符合5.1.2.条款要求的，TB将通知申请方补充和完善，或不受理认证申请，审核部应自申请之日起30日内通知认证委托人，说明理由并退回申请资料；
3) 对被执法监管部门责令停业整顿或被列入“国家企业信用信息公示系统”和“信用中国”等发布的严重失信主体相关名录的认证委托人，TB不受理其认证申请。

5.3. 签订认证合同及相关责任

5.3.1. 认证合同

在实施认证审核前，TB审核部将对申请材料进行评审，审查确认受理认证申请后，由TB总经理或具有法人代表授权资格的人员签署与申请认证组织委托人（即申请组织）订立具有法律效力的书面认证合同《管理体系认证合同》，明确认证服务的费用、付费方式和违约条款，及认证委托人、TB（认证机构）和获证组织的责任。认证费用应由认证委托人向TB（认证机构）直接支付。

5.3.1.1. 合同应至少包含以下内容：

1) 认证委托人（即申请组织）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（即申请组织）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（即申请组织）承诺获得认证后发生以下情况时，应及时向TB通报。
   ① 认证委托人（即申请组织）及相关方有重大投诉，被行政监管部门责令停产停业整顿；
   ② 被行政监管部门抽查不合格，或抽查不合格但已按相关规定整改合格。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；
   ③ 发生被行政监管部门责令停产停业整顿的重大事故；
   ④ 相关情况发生变更，包括但不限于：
   a. 法律地位、生产经营状况、组织状态或所有权变更；
   b. 取得的行政许可资格、强制性认证或其他资质证书变更；
   c. 法定代表人、最高管理者变更；
   d. 生产经营或服务的工作场所变更；
   e. 隐私信息管理体系覆盖的活动范围变更；
   f. 隐私信息管理体系重要过程的重大变更等。
   ⑤ 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（即申请组织）承诺获得认证后正确使用认证证书、认证标志和有关信息，不利用隐私信息管理体系认证证书和相关文字、符号误导公众，使其认为其产品或服务通过认证。
5) 拟认证的隐私信息管理体系覆盖的活动范围。
6) 在认证审核实施过程及认证证书有效期内，TB和获证组织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，《管理体系认证合同》一经签字生效，双方必须认真执行。如签订合同的一方不能履行合同，提出后协商解决；若终止合同，则所产生的经济损失由责任方承担。

5.3.1.2. 认证费用：

应由认证委托人（即申请组织）直接支付给江西腾标认证有限公司（TB）；

1) 可接受的支付形式包括：
   ① 认证委托人自身支付；

② 认证委托人的上级单位或下级关联单位代为支付时，需提供关联关系证明及授权文件，TB保留记录；

③ 个体工商户可由经营者个人支付。

2) 除个体工商户外，其他类型认证委托人的认证费用不得以个人名义支付。

3) 对于本规则生效前已签订的、不符合上述要求的认证合同，认证委托人应与TB签署补充协议或重新签署合同予以规范。

5.3.1.3. 合同变更：

对签订的合同内容的任何变更，审核部应与申请组织签订补充协议。对变更申请进行评审通过后，将其作为合同附件由TB存档。该申请与原合同具有同等的法律效力。

5.3.2. 认证活动相关责任：

5.3.2.1. 认证过程、活动引发的责任及处理由TB总经理负责作出安排。

5.3.2.2. TB和认证委托人关系、活动均应以双方签订的合同书为依据，涉及合同书范围以外的活动，须经双方商定，发生责任问题以书面文件为准，对确属TB的责任，由TB总经理作出具体安排，组织有关部门分析原因，制定纠正和纠正措施，并与认证委托人协商妥善解决。

1) 属TB认证机构的责任

① 审核活动不符合认证标准和公司管理体系认证文件要求；

② 审核活动中发生违反科学性、公正性现象；

③ 审核活动中审核人员违反审核纪律、发生泄密行为；

④ 审核结论与事实不符；

⑤ 违反认证合同的双方约定。

2) 属于认证委托人的责任

① 申请的管理体系覆盖产品、过程范围、体系覆盖人数与现场提供的审核范围不符；

② 管理体系建立和运行未按认证标准要求和体系文件规定实施；

③ 违反认证证书和认证标志的使用规定；

④ 对认证审核中发生的不符合项不能按规定采取纠正和预防措施，使其满足认证要求；

⑤ 违反认证合同书和双方约定。

5.4. 审核方案和审核策划

5.4.1. 认证周期：

TB依据 GB/T 19011《管理体系审核指南》 等文件，根据认证委托人的 风险和复杂程度，策划整个认证周期的审核方案，以清晰地识别所需的审核活动。认证周期包括：

1) 初次认证审核；

2) 认证决定后第一年的第一次监督审核；

3) 认证决定后第二年的第二次监督审核；

4) 认证决定后第三年、在认证到期前进行的再认证审核；

5) 特殊审核，包括：已认可的认证转换审核、扩大认证范围审核、调查投诉审核、组织变更审核、认证要求变更审核等。

5.4.2. 审核方案

1) TB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。

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

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，应覆盖管理体系所有要求，以及覆盖认

证范围内的典型体系活动和服务。认证证书有效期内的监督审核累计应覆盖本体系所有要求。

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。

5) TB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隐私信息管理体系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。

5.4.3. 审核范围

1) TB根据认证委托人拟申请的或已获得认证的范围以及其审核时所提供的临时场所的业务范围，并结合组织行业或行政许可的范围如营业执照、行业资质证书的范围进行确定，通过现场审核活动进一步加以确认。

2) TB根据隐私信息管理体系认证的特点，按照CNAS-TRC-012:2017《管理体系认证机构认证业务范围分类指南》的要求对认证业务范围进行分类管理。

5.4.4. 审核时间

1) 审核时间是指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。

① 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。

② 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。

2) 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%。如果审核人日计算后结果包括小数，宜将其调整为最接近的半人日数。

3) TB应建立文件化的结合审核时间确定方法，本体系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%。

4) 本体系认证审核时间要求详见附录A。

5.4.5. 多场所抽样方案

原则上，认证的初次审核及后续的监督和再认证审核宜在认证委托人（即申请组织）认证范围内的每个场所进行。

1) TB应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。

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隐私信息管理体系风险的评价。

3) 对涵盖相同活动、过程及隐私信息管理体系风险类型的多个相似场所可进行抽样审核，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 监督审核：Y = 0.6 X；

③ 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。

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) 分场所审核人日的计算方法参见 5.4.4，且现场审核时间不得少于表中所确定的现场审核时间的 50%。

5.4.6. 组建审核组

5.4.6.1. TB认证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，选择具备相关资格、能力

和经验的审核员组成审核组成员，并确保审核组具备与拟执行的审核任务相适宜的能力。审核组中应至少有 1 名TB的专职审核员，并确保该专职审核员在实施隐私信息管理体系第一阶段审核的审核员，还应参加隐私信息管理体系第二阶段审核。

5.4.6.2. TB在安排审核组成员时，还应关注到：

1) 审核组长：TB应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隐私信息管理体系专业人员（专业领域审核员或技术专家），当实施隐私信息管理体系和其他管理体系实施结合审核时，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。

注：A99小管理体系认证审核组全部由正式审核员组成，TB不安排实习审核员参与审核活动。

3) 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。
4) 审核组成员不得与认证委托人存在利益关系。

5.4.6.3.审核实施前，审核组应获得以下应用文件：

1) 审核实施规范
2) 审核方案策划文件
3) 审核任务书
4) 审核文件包
5) 认证委托人的体系文件
6) 获得指导审核实施的三级作业文件（必要时）
7) 法律法规的清单（必要时）

5.4.7. 审核计划

1) TB依据ISO /IEC 27701:2025信息安全、网络安全和隐私保护-隐私信息管理系统-要求与指导要求，对申请获证组织的隐私信息管理体系制定每次现场审核的审核计划。
2) 审核计划至少包括以下内容：
   ① 审核目的；
   ② 审核准则；
   ③ 审核范围；
   ④ 现场审核的日期、时间安排和场所，现场审核持续时间；
   ⑤ 审核组成员（其中：审核员标明认证人员注册号；专业领域审核员和技术专家应标明专业代码、工作单位及专业技术职称，兼职审核员和在职技术专家应注明工作单位。）
   ⑥ 审核任务安排。
3) 在审核活动开始前，审核组应将审核计划交认证委托人确认，审核组成员中如有认证委托人认为可能与其利益发生冲突的人员时，有权要求更换。遇特殊情况临时变更计划时，应及时将变更情况通知认证委托人，并协商一致。

5.5. 实施审核

5.5.1. 总则：

隐私信息管理体系认证审核应安排在认证委托人（即申请组织）的现场实施，现场审核应安排在认证范围覆盖的典型活动或服务处于正常运行状态下进行。对于存在季节性或非连续性生产/服务情况的，审核时间应安排在覆盖认证范围的活动发生时。包括初次认证审核、认证周期内的每年度的监督审核、再认证审核和特殊审核等。

5.5.2. 审核记录：

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，可补充使用图片/音像作为记录。
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。TB应保留首、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。
3) 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。最高管理者不熟悉组织自身的质量方针、质量目标，未亲自参与并推动本体系实施的，认证审核应不予通过。

5.5.3. 终止审核：

发生下列情况的，审核组应向TB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。

5.5.4. 文件评审

1) 文件评审的目的是评价认证委托人的管理体系文件是否满足标准要求、过程识别是否充分、方针和目标是否符合认证委托人的实际等。
2) 审核组长应获得认证委托人文件（手册、程序文件等成文信息）及相关清单。当文件审核不能足以了解认证委托人管理体系运行的基本情况时，应对有关的作业文件进行审核。
3) 由审核组长或经组长委托的专业审核员对组织的体系文件进行书面审核，审核组长需在文件审查报告上签字，其审查结果《文件审核报告》应发给认证委托人进行确认。

5.6. 初次认证审核

5.6.1. 总则

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。
2) 第一阶段与第二阶段应连续进行，两个阶段现场审核活动之间的审核时间间隔最短不应少于 5 日，最长不应超过 6 个月。如因特殊原因需要超过6个月才能实施第二阶段审核的，应重新实施第一阶段审核。

5.6.2. 第一阶段审核

1) 第一阶段审核原则上应在受审核方生产经营或服务现场进行，目的是通过了解认证委托人的本体系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。
2) 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、服务、设施设备、工艺流程、现场运作以及适用的质量标准；
   ② 评审认证委托人本体系对应的体系文件，确认其与认证委托人业务活动及服务相吻合；
   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隐私信息管理体系标准的情况，特别是对隐私信息管理体系关键绩效、过程和运行及目标识别情况
   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 确认认证委托人隐私信息管理体系认证范围、体系覆盖范围内有效人数和场所；
   ⑦ 认证委托人的体系运行和服务符合相关法律法规及强制性标准的情况。

   仅在满足以下条件时，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，并

确保通过文件审查等方式达到了第一阶段审核的目的：

① 认证委托人已获得TB认证机构颁发的其他领域的有效认证证书，TB已对认证委托人隐私信息管理体系有充分了解；

② 认证委托人获得了经认可机构认可的其他认证机构颁发的有效的本体系认证证书，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。TB认证机构应记录未在现场进行第一阶段审核的理由。

③ TB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。审核组应将第一阶段审核情况形成书面文件，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，要及时提醒认证委托人特别关注。

3) TB应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。

4) TB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. 目的：

第二阶段审核以评价认证委托人管理体系的实施情况为目的，应重点确认：

1) 认证委托人是否遵守了隐私信息管理体系的方针、目标和程序；

2) 隐私信息管理体系是否符合ISO /IEC 27701:2025信息安全、网络安全和隐私保护-隐私信息管理系统-要求与指导标准的所有要求；

3) 隐私信息管理体系是否正在实现管理方针与目标，并关注体系运行的有效性。

5.6.3.2. 审核实施与重点覆盖内容：

1) 审核组应按期到认证委托人现场实施审核。

2) 审核组长要保证审核组成员了解认证委托人的情况，明确审核组组员的分工，并据此编制各自现场审核检查清单。

3) 审核应重点验证本体系符合认证依据ISO /IEC 27701:2025信息安全、网络安全和隐私保护-隐私信息管理系统-要求与指导标准的要求及有效运行情况，应至少覆盖以下内容：

① 为实现方针而在相关职能、层次和过程设定的目标是否具体、适用，并得到贯彻；

② 资源配置能否支撑目标实现；

③ 对隐私信息管理体系覆盖的过程与活动的管理及控制情况，包括信息交流和管理措施的落实；

④ 承诺和评价机制的建立及实施有效性；

⑤ 建立和持续改进隐私信息管理体系机制的有效性，改进时是否保持体系完整性；

⑥ 认证委托人实际工作记录的真实性。对真实性存疑的证据应予以记录，并在审核结论及认证决定时予以考虑；

⑦ 依据隐私信息管理体系关键绩效、目标和指标，对绩效进行监视、测量、报告和评审；

⑧ 认证委托人实施隐私信息管理体系的能力及在符合适用法律法规要求方面的绩效；

⑨ 认证委托人管理过程的运作控制；

⑩ 认证委托人的内部审核和管理评审；

⑪ 针对隐私信息管理体系方针的管理职责。

5.6.3.3. 审核范围确认：

通过了解认证委托人的基本情况、现场分布、隐私信息管理体系过程等情况，确认审核范围。

5.6.4. 审核过程及环节

审核组应当全员完成审核计划的全部工作。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（技术专家除外）。

5.6.4.1. 首次会议：

1) 审核组全体成员、认证委托人的最高管理者（或其他书面授权的其他高级管理层成员）、管理体系相关部门负责人参加会议，当认证委托人有要求时，审核组应向认证委托人出示身份证明文件，会议由审核组长主持，填写现场审核首次会议签到表。
   ① 最高管理者不能参加的，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。
   ② TB 应保留首次会议签到记录、图片 / 音像证明材料。
2) 首次会议内容包括：
   ① 介绍审核组成员和认证委托人管理者代表介绍参会的成员；
   ② 说明审核类型、目的、范围和审核依据；
   ③ 适用时，确认以往评审或审核发现的状态；
   ④ 简要说明基于抽样审核方法、程序；
   ⑤ 明确审核发现的方法、审核结论分级的三种情况和审核结论的依据；
   ⑥ 确认审核计划的各项安排；确认在审核中将告知认证委托人审核进程及任何关注点；
   ⑦ 确认审核组与认证委托人之间的正式沟通渠道，确定审核陪同人员；
   ⑧ 介绍由于审核组成员的到场对组织可能形成的良好生产规范 GMP 的管理方法，落实审核组必要的工作条件和支持；
   ⑨ 说明保密承诺；
   ⑩ 询问限制条件；说明审核可能被终止的条件的信息；
   ⑪ 确认审核组可获得所需的资源和设施，以及适用于审核组工作安全事项、应急和安保程序；
   ⑫ 说明审核纪律、审核员规范声明、介绍对审核发现、审核结论（包括抱怨和申诉、投诉）的反馈渠道的信息；
   ⑬ 其他需要澄清的问题；
   ⑭ 让认证委托人提问的机会；
   ⑮ 对认证委托人选择 TB 认证和接待表示感谢。

5.6.4.2. 审核中的沟通

1) 审核组进行现场审核时，每天用于核算工作量的审核时间不宜少于 8 小时，其中应保证有充足的时间用于收集客观证据。
2) 在审核实施过程中，审核组长应定期向认证委托人通报审核进展及相关情况。当现场审核中发现的，如：人数、审核范围等与审核任务书上不一致或获得的审核证据表明不能达到审核目的时，审核组长应及时与认证委托人核查需要并向审核部报告，以确定采取适当的行动。

5.6.4.3. 终止审核的条件：

审核过程中发生以下情况，审核组应向TB审核部报告，经TB研究同意后终止审核。

1) 认证委托人对审核活动不配合，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。

5.6.4.4. 信息的收集和验证

1) 审核组成员由陪同人员引导到各部门、过程进行审核，各部门应指定代表和有关人员参加；
2) 审核组成员通过面谈、查阅文件、记录、现场观察等方式来收集客观证据；
3) 审核组成员采用适当的抽样对收集的信息进行验证，并与审核准则相比较，只有当收集的信息得到证实时方可作为审核证据；
4) 审核组在审核中，应注意调阅认证委托人内部和外部质量信息的记录，特别是认证委托人反馈的质量信

息，以确认认证委托人针对这些信息制定纠正措施及实施结果能否达到改进质量和达到认证委托人满意的程度。现场审核应填写审核记录并满足审核计划对审核过程的要求。

5.6.4.5. 形成审核发现

1) 审核组对照审核准则评价审核证据（在审核过程中所收集的任何其他适当的信息）的符合性。
2) 现场审核发现的不符合事实应开具书面不符合项报告，对不符合事实的描述应准确并具有可追溯性，判定不符合的性质以及违反了标准、组织的体系文件、法律法规的哪些条款准则的要求。对于不符合项，应依据认证标准判定，并在现场审核不符合项报告中明确标准的对应条款。
3) 不符合报告经审核员签字，审核组长复核后提交认证委托人的管理者代表签字确认。
4) 审核组长应尝试解决审核组与认证委托人之间关于审核证据或审核发现的任何分歧意见。对于未解决的分歧点，应予以记录。

5.6.4.6. 审核组内部决定规则

首先对不符合性质进行判断分级，然后对管理体系的适宜性、有效性和充分性做出整体评价，以便为认证决定或保持认证提供充分的信息。

1) 凡属下列之一，可判为严重不合格：
   ① 建立实施的管理体系与标准要求不符；
   ② 管理体系过程、活动有系统性或区域性的缺陷或严重失效；
   ③ 体系运行发生严重不符合，认证委托人反映强烈；
   ④ 发生严重安全事故，相关方反映强烈；
   ⑤ 严重违反质量手册和程序有关规定。
2) 凡属下列情况之一，可判为一般不合格：
   ① 孤立的人为错误，对体系要素或体系文件的要求而言是个别的、偶然的、孤立的、性质轻微的问题；
   ② 文件偶尔未被遵守，未造成严重后果；
   ③ 对系统不会产生重要影响的不合格等。
3) 考虑审核过程中固有的不确定因素，对审核结论达成一致；
4) 就任何必要的跟踪活动达成一致；
5) 其他未尽事宜说明

5.6.4.7. 管理体系整体评价

根据审核获取的证据，根据审核组的内部沟通结果，得出管理体系整体评价结论，在审核报告中体现。

5.6.4.8. 审核结论

1) 符合要求，有能力满足 ISO /IEC 27701:2025 信息安全、网络安全和隐私保护-隐私信息管理系统-要求与指导和适用法律、法规要求，同意推荐；
2) 存在不符合项，同意不符合项采取纠正措施并验证后推荐；根据不符合情况，由审核部确定现场关闭或书面关闭不符合项。对于现场关闭验证的，由审核组长或由审核部委派审核人员到现场验证对不符合项进行关闭以后，写出不符合项现场验证报告，并按程序进行认证审批。
3) 有严重不符合项，且短期内不可能进行纠正，则总体评价为不合格，不推荐认证注册。

5.6.4.9. 向认证委托人通报情况

在审核组内部决定会议（如遇延期或不予通过现场审核必须向TB领导报告）后，应向认证委托人管理层报告审核情况，并提供书面的关于认证委托人的隐私信息管理体系是否符合规定的认证要求的说明，包括不符合项和审核结论，并充分听取认证委托人意见。

5.6.4.10. 末次会议

1) 参加会议人员一般同首次会议，会议签到应填写现场审核末次会议签到表。

① 认证委托人的最高管理者不能参加末次会议的，应在会前向审核组提供书面说明，并由其书面授权的代表参加。

② TB应保留末次会议签到记录、图片 / 音像证明材料。

2) 末次会议程序，会议由审核组长主持其内容：

① 重申审核目的、范围、依据；说明审核情况，向认证委托人说明所收集的审核证据基于对信息的抽样，因而会有一定的不确定性；提出不合格报告，包括：审核发现的任何分级；

② 对认证委托人的本体系建立、运行的适宜性、有效性和充分性进行总体评价；请认证委托人提出问题。审核组与认证委托人之间关于审核发现或结论的任何分歧意见应得到讨论并尽可能获得解决。任何未解决的分歧意见应记录并提交TB。

③ 宣布审核结论和纠正措施验证要求等后续事宜；

④ 说明认证证书的使用要求；

⑤ 说明监督审核要求的有关内容；

⑥ 再次重申保密承诺、审核员规范声明；说明投诉的处理、申诉过程；

⑦ 对认证委托人给予审核组工作的支持、配合与接待表示感谢；

⑧ 末次会议记录应予以保存。

5.6.4.11.有关认证审核信息反馈事宜

1) 《认证证书信息确认表》作为印制认证证书的凭据，应由认证委托人填写（如认证委托人对中英文对照填写有困难，可只填写中文部分，英文可委托 TB 翻译，但应签署免责声明），并经审核组长审查确认（中文部分）签字，认证委托人需加盖公章确认。

2) 审核员需要填写审核经历表时，认证委托人给予证实并盖章。

3) 《审核人员工作质量反馈表》请认证委托人填写评价意见，盖章后传真或直接寄 TB 审核部，以便其对审核人员的工作质量进行评价和管理。

5.6.4.12.审核记录

作为编制审核报告和为认证决定提供支持性客观证据的基础，审核记录宜突出对选取的样本中那些对于判断组织管理体系与审核准则符合程度（符合与不符合）是至关重要的、必不可少的关键信息。

5.7. 特殊审核

5.7.1. 体系认证范围的扩大

1) 当获证组织申请扩大认证范围时，应向TB提出书面申请，并提供与扩大认证范围相适应的相关证据（包括管理体系文件）。审核部审查是否受理，并签订扩大认证范围的合同补充协议。

2) 审核部确定审核组后，由专人针对扩大范围的内容进行文件审查，并实施必要的审核活动，以作出是否可以扩大的决定。

3) 扩大认证范围的条件：

① 管理体系符合认证标准要求；

② 相关活动和服务质量符合法规/标准要求；

③ 管理体系有效运行，并具有满足规定管理目标的能力。

5.7.2. 认证范围的缩小

1) 当获证组织的某些已认证范围不能持续满足标准要求时，或获证组织主动申请缩小认证范围时，TB应办理认证范围缩小手续。

2) 有下列情况之一者，TB应缩小获证组织认证范围：

① 获证组织认证范围内的部分过程不再符合认证标准要求；

② 获证组织不再进行该范围内的活动或不愿再保持该范围的认证资格；

③ 获证组织被暂停后，未能在规定时限内解决造成暂停的问题，TB将根据实际情况撤销或缩小其认证范围。

3) 认证范围的缩小应经认证决定人员做出认证决定，经总经理或管理者代表批准后，由综合部制作并发放经认证范围缩小的认证证书。

4) TB相关部门应与获证组织进行沟通，正确说明缩小认证范围的情况。

5.7.3. 提前较短时间通知的审核

1) 适用情形：在以下情形中，TB可能进行提前较短时间（如至少提前24小时）通知的审核：

① 处理投诉：接到投诉后需即刻启动调查，如需现场取证，应书面通知认证委托人，通知内容应包括投诉详情、调查人员等信息；

② 跟踪变更或暂停状态：因认证委托人发生重大变更，或为验证被暂停认证委托人整改情况而需进行的追踪审核。

2) 审核组安排：此类审核一般安排原审核组长或审核组成员担任组长。若为处理投诉进行调查，应提前与认证委托人沟通调查组成员情况。

3) 不予通知的审核：以下情形可实施不予通知的审核：

① TB内部为确保证书有效性而进行的随机抽查；

② 应相关监管部门要求进行的“飞行检查”；

③ 认证委托人在认证合同中已明确承诺无条件配合此类审核。

6. 监督审核程序

TB应对持有TB颁发的隐私信息管理体系认证证书的组织（以下简称获证组织）进行有效跟踪，依据审核方案对获证组织开展监督审核，并监督获证组织持续运行本体系及ISO /IEC 27701:2025信息安全、网络安全和隐私保护-隐私信息管理系统-要求与指导标准符合认证要求及有效性。

6.1. 监督审核频次与实施

TB应根据获证组织的本体系成熟度或其他特性，确定对获证组织的监督审核的频次。

6.1.1. 在认证证书三年有效期内，对获证组织管理体系运行情况每年按计划进行监督审核。

1) 初次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；

2) 此后，每次监督审核间隔不应超过12个月，且每个日历年至少有一次监督审核（再认证的年份除外）；

3) 超过期限而未能实施监督审核的，按10.4.1条暂停认证证书处理。

6.1.2. 如果认证委托人对其管理体系进行了重大的更改，或者发生了影响到其认证基础的变更时，可根据获证组织的具体情况及管理体系成熟度在认证审核方案中考虑和调整增加监督审核频次。

6.1.3. 获证组织在行政监管部门抽查中被发现问题时，自国家市场监督管理总局发出通报起30日内，TB应对该获证组织实施监督审核。

6.1.4. 监督审核应在获证组织现场进行，且现场审核应安排在认证范围覆盖本体生活费活动正常运行时进行。由于产品生产的季节性原因，在每次监督审核时难以覆盖隐私信息管理体系典型活动和服务的，在认证证书有效期内的监督审核需覆盖认证范围内的典型活动和服务。

6.2. 监督审核实施程序

6.2.1. 审核部负责提前3个月与监审的获证组织联系，制定监督审核方案，审核方案中应明确：

1) 确定审核时机、多场所抽样方案；

2) 要求获证组织的最高管理者参与审核访谈，以确认获证组织反贿赂管理体系与标准的持续符合性和运行的有效性。

6.2.2. 每次监督审核的人日数应依据认证获证组织的具体情况确定，不得低于初次认证审核总人日数的

1/3（即≥30%），任何人日数的增减情况及原因说明予以记录。

6.2.3. 审核部负责组建满足专业要求的审核组，并基于运行环节与企业沟通的结果、审核组专业能力配备等情况及时调整审核方案，经审核部部长审查批准，签发《审核任务书》。

6.2.4. 审核组长负责依据审核方案策划结果、审核任务书，编制审核实施计划，对审核活动进行具体安排。

1) 每次监督审核应尽可能覆盖隐私信息管理体系认证范围内的典型活动与服务及有代表性的典型活动和服务过程，并确保在认证证书有效期内，所有监督审核能覆盖隐私信息管理体系认证范围内的全部典型活动和服务及有代表性的活动和服务过程；

2) 在编制实施计划时，应重点关注获证组织的变更以及隐私信息管理体系绩效的持续改进，审查内容至少包括：

① 上次内部审核和管理评审是否规范和有效；
② 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；
③ 获证组织的内部审核是否覆盖所有部门和关键流程，是否形成完整审核记录并落实整改措施；
④ 管理体系在实现组织方针、目标方面的有效性，质量目标及质量绩效是否达到体系确定值；若未达到，获证组织是否运行内审机制识别原因、是否运行管理评审机制确定并实施改进措施；
⑤ 为持续改进管理体系而策划的活动的进展；
⑥ 对管理体系持续的运作控制：按要求对已识别的重要关键点是否按本体系的要求正常和有效运行；
⑦ 任何变更：上次审核以来隐私信息管理体系覆盖的活动及影响体系的重要变更、运行体系的资源是否有变更；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规定；
⑧ 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；
⑨ 管理体系相关投诉的处理：是否及时接受和处理投诉；
⑩ 上次审核后发生的质量事故（或体系相关事件）的调查与处理；
⑪ 针对管理体系运行中发现的问题或投诉，是否及时建立并实施有效的改进措施。

3) 审核组长在现场审核中如发现人数与审核任务书不一致、审核范围的扩大等情况时，需及时与审核部联系，以便采取措施。

6.2.5. 对于任何严重不符合或其他可能导致暂停或撤销认证的情况，审核组长应向技术部报告，由技术部组织具备适宜能力且未实施该审核的人员进行复核，以确定能否保持认证。

6.2.6. 认证资格保持的条件：

① 管理体系能持续满足认证标准要求；
② 服务/活动质量稳定，服务及时，履行承诺，获证组织满意；
③ 本体系持续有效运行，保持自我改进和自我完善的机制；
④ 再认证审议结论时，还应考虑和评价获证组织在认证有效期内隐私信息管理体系整体的持续有效性。

6.2.7. 审核组应编制审核报告，对报告中的要求应逐项描述，并做出建议TB给予继续保持、暂停、撤销认证资格的推荐性结论。如果发现不合格，获证组织应在规定的时间内采取有效纠正措施，并经审核组长验证合格后提交技术部。

6.2.8. 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。

6.2.9. 监督审核的时间安排：初次认证及再认证后的第一次监督应在认证证书签发之日起12个月内进行；每次监督审核间隔不应超过12个月，且每个日历年至少有一次监督审核（再认证的年份除外）。

6.3. 建立通报制度和不定期的监督

6.3.1. 通报内容：在认证证书有效期内，获证组织应明确职能部门和责任人员，如发生下列情况应及时主动地向TB通报情况，必要时TB将要求获证组织提供有关投诉记录和采取纠正措施的记录。管理体系发生相关变更包括但不限于：

1) 法律地位、生产经营状况、组织状态或所有权变更；
2) 取得的行政许可资格、强制性认证或其他资质证书变更；
3) 法定代表人、最高管理者、管理者代表变更；
4) 生产经营或服务的工作场所变更；
5) 隐私信息管理体系覆盖的活动范围变更；
6) 隐私信息管理体系和重要过程的重大变更；
7) 获证组织在认证证书有效期内发生以下情况时，应在知悉之日起5个工作日内向TB通报：
   ① 受到与认证范围相关的行政处罚；
   ② 国家或地方监督抽查中发现认证范围内活动存在不合格（含已整改完成的情形）；
   ③ 发生与质量管理体系相关的重大舆情事件。

6.3.2. 不定期的监督：根据6.4.1条发生的影响管理体系认证基础的更改或运行的重大变化，不能满足认证标准和获证组织要求时，可决定立即实施不定期的监督审核，并根据监督结果，视情节作出处理决定。

7. 再认证程序:

7.1. 再认证安排

认证证书期满前，若获证组织申请继续持有隐私信息管理体系认证证书， TB应当依据审核方案实施再认证审核，以判断获证组织的本体系作为一个整体与标准的持续符合性和运行的有效性。

7.1.1. 审核实施要求

1) 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。
2) 在认证周期届满前3个月，审核部应与获证组织联系再认证事宜，并安排再认证审核。
3) 审核策划人员应在审核任务书中明示证书的到期时间，提醒审核员在认证证书到期前提交经验证后的审核资料，以便技术部有充足的时间做出认证决定。
4) 再认证审核可以和暂停恢复的现场审核同时安排。

7.1.2. 审核时间与策划依据

1) 再认证审核的审核时间应按初审人日数确定方法（如5.4.4.），根据获证组织当前有效人数和体系风险类型确定，不少于初次认证审核时间的2/3。
2) 策划时应考虑获证组织最近一个认证周期内的体系绩效，包括调阅以往的监督审核报告。审核组长应对获证组织获证以来的管理体系总体变化趋势进行评价，对薄弱环节应作为再认证的审核重点。

7.2. 审核内容

7.2.1. 再认证审核至少应包括下列现场审核内容：

1) 结合其内部环境和外部环境的变化情况，确认获证组织管理体系的有效性及认证范围的持续相关性和适宜性；
2) 管理体系绩效持续改进的证实；
3) 管理体系在实现获证组织目标和体系预期结果方面的有效性。

7.2.2. 其他应关注的细节：

1) 结合内部和外部变更（如组织、产品、法规、标准、流程、场所、获证组织等方面发生的重大变化以及因改进而发生的变更），通过绩效数据的分析、内审、管理评审等提供的信息的评价，了解组织保持管理体系完整性的措施，以及管理体系在经历了各种变更影响下的有效性保持；
2) 经证实的对保持管理体系有效性并改进管理体系，以提高整体绩效的承诺；
3) 在经历各种变更下，管理体系是否还能支持认证范围所覆盖的对象。认证范围是否需要做必要的调整。

7.3. 超期与未完成的处理

1) **超期申请的处理：**对获证组织超出认证证书有效期提出的再认证申请，审核部应按照初审对待。
2) **未完成审核的后果**

① 如果在认证终止日期前，未能完成再认证审核或不能验证对严重不符合实施的纠正和纠正措施，则不应推荐再认证，也不应延长认证的有效期。TB应告知获证组织并解释（说明）后果。

② 再认证审核的认证决定最迟应在原认证证书到期之日起6个月内完成。若未能在该时限内完成，TB应按照初次认证审核程序重新实施审核。

7.4. 认证有效期与恢复

7.4.1. **认证有效期与颁证日期：**如果在当前认证的终止日期前成功完成了再认证活动，新认证的终止日期可以基于当前认证的终止日期（即从上一次到期日期起延续一个周期），新证书上的颁证日期应不早于再认证决定日期。

7.4.2. **认证终止后的恢复：**在认证终止后，如果TB能够在6个月内完成未尽的再认证活动，则可以恢复认证，否则应至少进行现场审核才能恢复认证。恢复后的证书生效日期应不早于再认证决定日期，到期日期应基于上一个认证周期。

7.5. 认证更新决定

TB应根据再认证审核的结果，以及认证周期内的体系评价结果和认证使用方的投诉，做出是否更新认证的决定。

8. 不符合项的纠正和纠正措施及其结果的验证

8.1. 不符合项的基本要求

1) 不符合项包括不符合项的明确说明、性质，认证委托人应改进的主要方面。适用时，对以前不符合采取的纠正措施有效性的验证情况。
2) 不符合项的表述，应基于客观证据和审核依据，用写实的方法准确、具体、清晰描述，易于被认证委托人理解。不应用概念化的、不确定的、含糊的语言表述不符合项。

8.2. 原因分析与纠正措施要求

对审核中发现的不符合项，TB应要求认证委托人在规定的时限内进行原因分析，并采取相应的纠正措施。

1) TB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制定纠正措施计划，由TB在下次审核时验证。
2) 如果为了验证纠正和纠正措施的有效性，将需要补充一次全面的或有限的审核，或者需要文件化的证据（需要在未来的审核中确认），则TB应告知认证委托人。

8.3. 纠正措施验证方式

1) **书面材料的验证：**由审核组长或其他级别审核人员，对认证委托人不符合项分析原因采取纠正措施的实施结果的书面证实材料进行验证。满足要求后，应在纠正措施验证栏内签署意见予以关闭。
2) **现场验证的安排：**对于需到现场进行验证的，审核部需下达经批准的审核任务书，原则上由原审核组长或审核组成员进行现场验证。审核部也可另派审核人员进行现场验证，证实其满足要求后签署意见，对不符合项进行关闭，并提交现场验证情况记录。

3） **验证完成：**当所有不符合项完成验证关闭后，由审核组长填写《管理体系认证决定审批表》。

8.4. 不符合项验证时限

认证委托人应在以下规定时限内完成对不符合项的纠正和纠正措施，并经审核组验证有效：

1） **初次认证审核：**严重不符合项的纠正措施验证，应在第二阶段现场审核结束之日起 6个月 内完成；一般不符合项的验证时限由审核组根据实际情况在不符合报告中确定。

2） **监督审核：**严重不符合项的纠正措施验证，应在监督审核结束之日起 3个月 内完成。轻微不符合可按照本条第3)款的规定，在下次审核时验证。

3） **再认证审核：**所有不符合项的纠正措施验证，应在 原认证证书有效期届满前完成。

8.5. 超期未完成验证的后果

若认证委托人未能在上述规定时限内完成对不符合所采取的纠正措施并经验证有效，TB不应做出授予认证、保持认证或更新认证的决定。

9. 审核报告与认证决定

9.1. 审核报告基本要求

9.1.1. TB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，并在审核报告上签字确认。

9.1.2. 审核报告应准确、简明和清晰，反映认证委托人管理体系的真实状况，描述对照本体系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。

9.1.3. 审核报告至少应包括或引用以下内容

1） TB（认证机构）名称；

2） 认证委托人的名称和地址及其代表；

3） 审核类型（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） 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活动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质量目标之间存在的差距和改进机会；

13） 行政监管部门在相关方面抽查的不合格情况，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管理体系的重要变更（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。

9.1.4. 注意事项

1) 如果认证委托人有多个不在同一地址的现场，应在报告中说明；
2) 如果认证委托人对报告持不同意见，如某些问题双方无法统一，可记入检查结果，记录应予以保存，并随审核资料一起提交TB。

9.2. 审核记录的留存

1) 审核报告一式两份，认证委托人一份，TB一份。审核组应保留签收和提交的证据，并随审核资料一同上交。
2) TB应保留用于证实审核报告中相关信息的审核记录。

9.3. 终止审核的报告

发生以下情况时，审核组应向TB报告，经TB同意后终止审核。

1) 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。

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，TB应将此报告提交给认证委托人。

9.4. 认证决定

9.4.1. 认证决定的基本要求

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。

1) TB应在对审核报告、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。
2) 认证决定人员应为TB的认证人员，并不得为审核组成员，能力应满足关于TB资质审批的相关要求。
3) 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。

注：当认证委托人不能满足以上要求的，TB应以书面形式告知认证委托人未通过认证的原因。

9.4.2. 授予、更新、扩大认证决定的条件：

TB应有充分的证据确认认证委托人满足下列条件的，做出授予、更新、扩大认证范围的决定：

1) 首先应满足5.1.2.与5.1.3.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) 认证委托人的本体系符合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。

9.4.3. 监督审核的认证决定简化条件

对于监督审核，TB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) TB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。

9.4.4. 认证决定与批准

1) 认证决定的方式为认证决定人员审定，审定时需在《管理体系认证决定审批表》上签字；如认证决定中存在重大问题时，提交 TB 技术部进行决定，并做出处理。

2) 当出现影响批准认证的事宜时，信息获取部门应及时向技术部传递信息，以保证认证决定的有效性。
3) 如果认证审定结果与审核组提交的报告存在差异，技术部应及时通知审核员，由审核员与认证委托人沟通、说明原因，并由技术部向认证委托人发送书面通知。
4) 总经理根据认证决定人员签字的《管理体系认证决定审批表》附有关资料批准认证注册；《管理体系认证决定审批表》需经总经理/法人代表签字方能制作证书。
5) TB 应记录每项认证决定，包括从审核组或其他来源获得的任何补充信息或澄清。
6) TB 在颁发认证证书后，应当在 30 个工作日内按照规定要求将认证结果相关信息报送国家认监委；认证证书和认证标志的管理执行相关程序。

10.认证标志和认证证书

10.1. 总则

TB制定并实施《管理体系认证证书和认证标志、认可标识使用规则》，要求获证组织正确使用隐私信息管理体系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》相关规定。

10.1.1. 证书与标志使用要求

1) 获证组织可以在认证证书有效时使用认证证书和认证标志，并接受TB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。
2) 获证组织应当在广告等有关宣传中正确使用认证标志，不得仅标注认证标志，只有在注明获证组织通过隐私信息管理体系认证及TB（认证机构）名称的情况下，方可标注。
3) TB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。

10.1.2. 认证标志要求：TB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。

10.2. 认证证书管理

10.2.1. 证书颁发与有效期

1) TB应及时向认证决定符合要求的组织出具认证证书，认证证书的有效期最长为3年。认证证书有效期自签发之日起计算，至3年后对应日期的前一日终止；证书的签发日期不应早于做出认证决定的日期。
2) 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。

10.2.2. 证书编号：对每张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。

10.2.3. 证书语言：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。

10.2.4. 证书内容要求：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) 获证组织管理体系所覆盖的活动、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) 认证证书对应所采用的认证依据应采用当时有效版本的完整标准号；
4) 认证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经审核合格此证书方继续有效”的提示信息；
5) 认证证书的编号（或唯一的识别代码）；

6) TB（认证机构）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：全国认证认可信息公共服务平台（认e云）的查询路径，以及TB官网公示查询方式。

10.2.5. 认证证书变更：获证组织名称、注册地址、认证范围等信息发生变更时，应向TB提交书面申请及相关证明材料。TB审核确认后，可换发认证证书。换发证书的证书编号不变，有效期不变，颁证日期为换证日期。

10.3. 认证证书的暂停、撤销、注销和后续管理

公司建立并实施《保持认证管理程序》，不得随意暂停、撤销和注销认证证书。

10.3.1. 认证证书暂停：

获证组织有以下情形之一的，TB应在调查核实后5日内暂停其认证证书，并保留相应证据：

1) 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；
2) 不满足管理体系适用的法律法规要求，且未采取有效纠正措施；
3) 受到与管理体系相关的行政处罚，且尚未完成整改的；
4) 发生重大隐私信息管理体系事故，反映获证组织管理体系运行存在重大缺陷；
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) 持有的与管理体系认证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，包括但不限于：
   ① 第一次监督审核未能在认证证书签发之日起 12 个月内开展；
   ② 第二次监督审核未能在认证证书签发之日起 24 个月内开展；
   ③ 本次监督审核距离上次监督审核超过 12 个月。
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业整顿的；
11) 发生与质量相关重大舆情的；
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。

TB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。暂停期间，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，TB应恢复其认证证书，并保留相应证据。

10.3.2. 认证证书撤销

获证组织有以下情形之一的，TB 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：

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体系运行或服务等重大安全事件的；
5) 管理体系没有运行或者已不具备运行条件的；
6) 不承担、履行认证合同约定的责任和义务，情节严重且拒不整改的；
7) 严重违反TB认证程序要求，提供虚假材料或信息情节严重的；

8) 其他应撤销认证证书的。

10.3.3. 认证证书注销

获证组织主动申请不再保持认证证书时，TB 应确认在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。

10.3.4. 后续管理程序

1) **暂停的办理：**证书暂停由审核部提出，认证决定阶段提出暂停由技术部提出，暂停应经提出部门主管领导审批。综合部负责统一变更办公系统内的相应信息及上报CCAA。综合部负责制作和发放“暂停认证证书和标志通知书”。“暂停认证证书和标志通知书”中应有暂停具体原因、暂停的起始日期和暂停期限，应明确并声明在暂停期间客户不得以任何方式使用认证证书、认证标识或引用认证信息。

2) **恢复的办理：**本着“谁办理谁跟踪”的原则，恢复应由暂停提出部门办理。公司有关部门要与认证暂停客户保持信息沟通、联系，了解该客户采取纠正措施进展的动态情况，以便对暂停的恢复做出及时安排。

① **技术部提出的暂停：**由审核部策划提前较短时间通知的审核，并通知客户和审核组长，待现场审核资料交回后，技术部认证决定通过，管理者代表审批，予以恢复。

② **因欠费暂停的：**获证组织在规定的时间内缴费的，由审核部直接办理恢复手续；

③ **因资质过期暂停的：**当持有的与隐私信息管理体系范围有关的安全生产许可证、资质证书等过期失效暂停，重新提交的申请已被受理但尚未换证原因暂停的，获证组织上交有效资质后，由审核部直接办理恢复手续；

④ **其他情况：**除上述 3 种情形外，由审核部安排审核组长现场确认是否具备恢复条件；如具备，由审核组长告知审核部，由审核部办理恢复手续。综合部负责制作和发放“恢复认证证书和标志通知书”。

3) 恢复现场审核

① 恢复审核的主要内容有：

a. 针对暂停原因，受审核方采取了纠正措施和预防措施，对其纠正措施和预防措施的适宜性和实施的有效性进行审核，并收集相关证据予以证实。

b. 如暂停原因为严重不符合未按期完成整改，应重点验证纠正措施的有效性，确认整改已到位。

c. 了解暂停期间受审核方是否按规定停止使用认证证书和认证标志。

d. 了解暂停期间受审核方管理体系是否正常运行，评价管理体系运行的有效性。

e. 审核员应根据上述审核内容，评价受审核方的暂停能否恢复，给予是否推荐恢复注册资格的结论。审核记录和审核报告中需对审核过程中了解的情况和结论予以明确记录。

② “恢复+监审”的审核要求

a. 审核部在策划“恢复+监审”的审核时，应提前与客户充分沟通，了解其针对暂停是否已完成整改和验收，必要时需客户提供相关证实材料。

b. 当本次审核的审核目的是“恢复+监审”时，审核员应先进行恢复审核。只有当审核组通过现场审核确认受审核方具备恢复认证资格后，方能进行正常的监督审核；如不具备恢复条件时，审核组应及时向审核部报告。

4) 证书撤销后续管理

① 在规定的期限内未解决造成暂停原因的，撤销的办理本着“谁暂停谁撤销”的原则，分别由审核部/技术部办理撤销手续。

② 管理体系认证证书一经撤销，即表明公司不再证明获证客户管理体系符合其特定的标准，终止了双方的认证关系，由综合部收回认证证书。

5) 其他要求：

① 管理体系认证证书状态的任何变更，综合部均上报 CNCA、CNAS 备案（CNAS 备案需认可后）。

② 对获证客户暂停、恢复、撤销等有关审批材料由办理部门负责存档。对于暂停、恢复、撤销认证证书和标志通知书随审核资料归档。

③ 公司暂停或撤销认证证书的信息在公司网站上公布，同时按规定程序和要求报国家认监委。

④ 公司采取有效措施避免各类无效的认证证书和认证标志被继续使用。

11. 受理组织的申诉（投诉）处理

TB 制定了《申诉投诉管理程序》，认证委托人对认证决定有异议的，可以向 TB 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 TB 提出投诉。

1) 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。TB对申诉人（投诉人）、申诉（投诉）事项的信息应予以保密。
2) TB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）。

12. 信息公开与报告

12.1. 信息通报制度

TB 建立并实施《信息通报管理规定》，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。

12.2. 审核计划上报

认 TB 应至少在现场审核实施前 3 日，将审核计划上报国家认监委。

12.3. 信息公开与上报

1) **认证结果报送：**TB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，与查询路径；
2) **查询途径公示：**TB应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，不得仅提供“国家认监委”或“全国认证认可信息公共服务平台（认 e 云）”查询路径。
3) **证书状态公开：**TB应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。
4) **证书状态上报：**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。

12.4. 重大事件自查

获证组织发生重大质量事故的，TB 应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。

13. 认证记录

13.1. 管理制度与保存期限

公司建立并实施了《认证档案管理规定》，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。

13.2. 认证记录内容

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。

13.3. 签名盖章要求

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。

13.4. 记录语言与格式

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。

13.5. 获证组织留存要求

为了证实认证活动的实施，除了 TB 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）。

注：获证组织对上述记录的保存期限不应少于认证证书有效期届满之日起2年。

14. 其他相关规定

14.1. 内部审核

TB 应建立并实施文件化的内部审核程序，确保至少每年对管理体系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。

14.2. 同行评议

TB 应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本体系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。

14.3. 技术服务

1) 认证机构可为组织提供本体系贯标服务，但不得代替组织编制隐私信息管理体系文件、开展内部审核和管理评审，严禁协助组织编造虚假管理体系文件、体系运行记录等。

2) 为确保没有利益冲突，参与对某组织隐私信息管理体系技术服务的人员，2 年内不应被认证机构安排针对该组织的审核或其他认证活动。

14.4. 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隐私信息管理体系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。

14.5. 其他：

1) 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，签字确认与原件一致。本公司可开展标准及相关技术标准的宣贯培训，促使组织全体员工正确理解和执行本标准。

2) 本规则依据《中华人民共和国认证认可条例》《认证机构管理办法》等相关法律法规及国家认证认可监督管理委员会发布的通用认证规则（包括但不限于《质量管理体系认证规则》等）制定。对于本规则未明确或与本规则存在不一致的通用性要求，以国家法律法规及通用认证规则为准。

15. 受理转换认证证书

隐私信息管理体系无需转换。

16. 相关文件

TB-GZ-01《项目受理管理规定》

TB-GZ-02《申请评审、受理和审核人日确定办法》

TB-GZ-03《审核方案管理规定》

TB-GZ-04《审核方案策划实施管理规定》

TB-CX-10《管理体系认证初次审核实施与控制程序》

TB-CX-12《保持认证管理程序》

TB-CX-19《认证证书和认证、认可标识及国际认证证书和互认标识使用控制程序》

TB-CX-13《申诉投诉管理程序》

TB-GZ-18《信息通报管理规定》

TB-GZ-17《多场所认证实施管理规定》

附录A. 隐私信息管理体系认证审核时间要求

隐私信息管理体系认证审核时间要求

有效人数	审核时间 第1阶段+第2阶段（人天）	有效人数	审核时间 第1阶段+第2阶段（人天）
≤15	2.5	876-1175	13
16-25	3	1176-1550	14
26-45	4	1551-2025	15
46-65	5	2026-2675	16
66-85	6	2676-3450	17
86-125	7	3451-4350	18
126-175	8	4351-5450	19
176-275	9	5451-6800	20
276-425	10	6801-8500	21
426-625	11	8501-10700	22
626-875	12	>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（如承包商人员）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，但往返多个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 被确定为低风险认证业务类别的，认证审核活动可根据需要在按照附录A计算所得审核时间的基础上，最多减少10%；被确定为中风险认证业务类别的，认证审核活动应按照附录A计算审核时间；被确定为高风险认证业务类别的，认证审核活动应在按照附录A计算所得审核时间的基础上，至少增加10%。

⑤ 监督人日为初审的 1/3；再认证人日为初审的 2/3；如有小数点按修约原则。