BCC

隐私信息管理体系

认证实施规则

文件编号： **GF 022**

版本号： **V1.3**

编制： 郑超

修订： 张艳

审核： 齐蕊

批准： 陶然亭

发布单位：新世纪检验认证有限责任公司（规则全文中简称 **BCC**）

初始发布日期：2020 年 12 月 11 日 修订日期：2026 年 6 月 3 日 实施日期：2026 年 6 月 3 日

目 录

版本号	文件编号	文件名称	修订内容	修订人	修订时间
V1.0	GF 022	隐私信息管理体系认证实施规则	1.本规则拆分自原 GF106 2.按照 2025 年 8 月 5 日反馈、8 月 22 日认监委和认研中心培训内容修改规则相关内容	郑超	2025.8.28
V1.1	GF 022	隐私信息管理体系认证实施规则	1.编辑性修订	郑超	2025.9.17
V1.2	GF 022	隐私信息管理体系认证实施规则	根据国认监发【2025】9 号《国家认监委关于进一步规范管理体系认证活动切实提升认证有效性的通知》要求修订。	郑超	2026.1.28
V1.3	GF 022	隐私信息管理体系认证实施规则	根据认证规则备案反馈的问题，新版标准变更	张艳	2026.6.3

1. 适用范围

1.1. 为规范隐私信息管理体系（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. 本规则规定了新世纪检验认证有限责任公司（以下全文中简称 BCC、我机构）开展隐私信息管理体系（PIMS）的程序与基本要求，是新世纪检验认证有限责任公司从事 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. 新世纪检验认证有限责任公司遵守本规则的规定，并不意味着可免除其所承担的法律责任。

2. 认证依据

BCC 对适用范围中相应的管理体系认证依据如下：

领域缩写	标准名称	标准号
PIMS	**隐私信息管理体系**	**ISO27701:2025**

3. 基本要求

3.1. 从事 PIMS 认证，应在国家认证认可监督管理委员会（以下简称国家认监委）备案本认证规则并保持有效状态。

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. BCC 内部管理和认证活动应符合 GB/T 27021.1/ISO/IEC 17021-1《合格评定管理体系审核认证机构要求第 1 部分：要求》确保持续满足开展 PIMS 认证的基本要求。

3.4. BCC 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。BCC 应能证明其已对 PIMS 认证活动引发的风险进行了评估，对引发的责任做出了充分安排（如保险或储备金）。

3.5. BCC 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. BCC 及其认证人员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。

3.7. BCC 及其认证人员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，不向第三方透漏，认证行政监管有要求的除外。

3.8. BCC 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。

3.9. BCC 拥有的 PIMS 有效认证证书的数量应与 BCC 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。

3.10. 不得委派未取得 BCC 内部 PIMS 注册资格的审核员开展 PIMS 认证审核活动。

3.11. 不得以“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. 审核员至少具备经 CCAA 注册的任一管理体系正式审核员资格，并取得 BCC 内部批准的 PIMS 审核员注册资格。

4.3. 审核员不得接受超出其注册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 BCC 其所了解的任何可能使本人或 BCC 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）。

4.5. 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 BCC 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. 认证过程管理人员能力要求：隐私信息管理体系申请评审人员、审核方案管理人员、认证决定管理人员、认证决定人员、认证规则制定人员、人员能力评价人员，应了解 ISO/IEC 27701:2025 标准及 PIMS 相关知识，并获得相应岗位授权。

5. 认证程序

5.1. 认证申请

5.1.1. BCC 应向申请认证的社会组织(以下称申请组织)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，以及分包境外认证机构业务的情况；

(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) 当前未被行政监管部门责令停产停业整顿；

(5) 当前未列入“国家认证委托人信用信息公示系统”和“信用中国”发布的严重违法失信名单；

(6) 一年内发生严重信用与 PIMS 相关的问题；

(7) 一年内未发生被行政监管部门责令停产停业整顿的与 PIMS 相关的事故；

(8) 其他应具备的条件。

5.1.3. 申请组织的授权代表签署《管理体系认证申请书》，并至少提供以下必要的申请信息及资料：

（1） 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法律法规要求的行政许可文件、资质证书等；

（4） 组织机构及职责；

（5） 生产/服务的流程、班次及轮班情况和季节性信息；

（6） 适用性声明（如涉及）、资产列表（如涉及）；

（7） 保密协议（如涉及）、敏感区域的声明（如涉及）；

（8） 申请组织对 BCC 的资质、诚信守法记录或认证人员身份背影的要求以及适用的、最新的与保守国家秘密或维护国家安全有的法律法规要求，以便 BCC 判断是否具备为申请组织实施认证活动的资格或条件；

（9） 关于认证活动的限制条件(如出于安全和/或保密等原因，存在时)。

（10） 在认证审核之前，BCC 要求客户组织报告是否存在因包含保密性或敏感性信息而导致不能提供给审核组的相关信息。BCC 应确定是否能在缺少这些信息的情况下得到充分审核。如果 BCC 的结论是若不核查已识别的保密性或敏感性信息就不能对管理体系进行充分的审核，那么 BCC 将会告知客户只有在适当的访问安排获得许可后才能进行认证审核。

（11） PIMS 运行满三个月的证据；

（12） 一年内所发生的与 PIMS 有关的重大事故事件、重大舆情以及整改情况（适用时）；

（13） 其他需要提供的文件。

(1)

5.2. 申请评审

5.2.1. 应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. BCC 申请评审人员应根据认证依据、程序等要求，及时对申请组织提交的申请文件和资料进行评审并保存评审记录，以确保：

(1) 申请认证的范围；

(2) 审核依据/审核准则；

(3) 关于申请组织及其 PIMS 的信息充分，足以建立审核方案；

(4) 解决了 BCC 与申请组织之间任何已知的理解差异；

(5) BCC 有能力并能够实施认证活动；

(6) 组织接受 PIMS 认证咨询的情况；

(7) 通过对申请的认证范围、申请组织的生产经营场所、员工人数、PIMS 文件以及任何其他影响认证活动的因素（语言、安全条件、对公正性的威胁等）的考虑，确定是否受理认证申请；

5.2.3. 只有满足以下条件的，BCC 才可以受理认证申请：

(1) 认证委托人已具备受理条件（见 5.1.2）；

(2) BCC 具备实施认证的能力；

(3) 双方就认证事宜达成一致。

5.2.4. 不予受理的情形：

(1) 申请组织不满足 5.1.2 任一项的要求时；

(2) 申请组织近一年内发生严重信用问题，或重大与 PIMS 事故的；

(3) 其他不予受理的情形。

5.2.5. BCC 应将申请评审的结果告知认证委托人。

5.2.6. 对于 PIMS，BCC 不接受认证转换。对于新的认证委托人，应按照初次认证开展认证活动。

5.3. 认证合同及相关责任

5.3.1. 通过申请评审的，BCC 应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、BCC 和获证组织的责任。认证费用应由认证委托人向 BCC 直接支付。

5.3.2. BCC 应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，通过其官方网站（www.bcc.com.cn）向社会公布认证证书信息；因 BCC

批准资质注销或被撤销导致获证组织 PIMS 认证证书无法有效保持的，需及时告知获证组织并做出妥善处理，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 BCC 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 BCC 对投诉的调查，及时向 BCC 通报 PIMS 及 5.1.2 中条件的变更情况，承担选择的 BCC 资质被撤销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 BCC 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 BCC 通报 PIMS 及 5.1.2 中条件的变更情况，承担选择的 BCC 资质被撤销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. 审核方案管理人员**应**确保**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 27701:2025 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累计应覆盖 ISO/IEC 27701:2025 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**。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. 审核方案策划时**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) 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. 为确保认证审核的完整有效，BCC 根据附录 A 所规定的审核时间为基础，根据申请组织管理体系覆盖的活动范围、特性、技术复杂程度、风险程度、认证要求和体系覆盖范围内的有效人数等情况，核算并拟定完成审核工作需要的时间。

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 A 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，宜将其调整为最接近的半人日数。

5.4.2.4. PIMS 不与其他领域结合审核，也不能通过结合审核的方式减少审核时间。

5.4.3. 多场所抽样方案

5.4.3.1. BCC 已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的相似性。

5.4.3.3. 对涵盖相同活动、过程及 PIMS 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：$Y=\sqrt{X}$

(2) 监督审核：$Y=0.6\sqrt{X}$

(3) 再认证审核：$Y=0.8\sqrt{X}$

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. 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. 审核方案管理人员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，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：BCC 已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专业人员（专业领域审核员或技术专家）；

(3) 至少 1 名专职审核员，并确保专职审核员全程参与审核过程。

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。

5.4.4.5. 审核组中还可能包括一同进入认证委托人现场的观察员、翻译人员、认可机构的评审员及其他外部人员。审核组中的审核员应承担审核任务和责任。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。

5.4.5. 审核计划

5.4.5.1. 审核组长应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 审核员注册号，专业领域审核员和技术专家应标明专业代码，兼职审核员和在职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。

5.5. 审核实施

5.5.1. 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、管理体系相关职能部门负责人应参加首、末次会议，并应保留首、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。

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 PIMS 方针、目标，未亲自参与并推动管理体系实施的，认证审核应不予通过。

5.5.5. 发生下列情况的，审核组应向 BCC 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，包括其活动、产品和服务、设施设备、工艺流程、现场运作以及适用的标准；

(2) 评审认证委托人管理体系文件，确认其与认证委托人业务活动及产品和服务相吻合；

(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 ISO/IEC 27701:2025 标准的情况，特别是对管理体系关键绩效、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) 确认认证委托人认证范围、体系覆盖范围内有效人数和场所；

(7) 认证委托人符合相关法律法规及强制性标准的情况。

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 BCC 颁发的其他领域的有效认证证书，BCC 已对认证委托人 PIMS 有充分了解；

(2) 再认证审核未能在认证证书到期前完成现场审核，并按照初次认证开展认证活动时，此种情况下第一阶段审核可不在申请组织现场实施。

审核方案管理人员应记录未在现场进行第一阶段审核的理由。

5.6.2.3. BCC 审核组应将第一阶段审核发现形成文件并告知认证委托方，包括任何应引起关注的、在第二阶段审核中可能被判定为不符合的问题。

5.6.2.4. 审核组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，应及时通知审核方案管理人员并终止认证活动。

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 27701:2025 标准要求的符合性和体系的有效性。

(1) 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：认证委托人与标准的符合情况及证据；

(2) 依据 AIMS 关键绩效、诚信目标和指标，对绩效进行的监视、测量、报告和评审；

(3) 认证委托人实施 AIMS 的能力以及在遵守相关法律法规与合规义务方面的绩效；

(4) 认证委托人风险控制过程及承诺兑现过程的运作控制；

(5) 认证委托人的内审和管理评审；

(6) 针对认证委托人方针与承诺落实的管理职责。

5.7. 监督审核

5.7.1. BCC 应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 27701:2025 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典型产品/服务及有代表性的生产/服务过程，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典型产品/服务、有代表性的生产/服务过程。

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) 上次审核后发生的与隐私信息管理有关的事故的调查与处理。

5.7.4. 实施监督审核的时间，应与初次认证审核（第 1 阶段＋第 2 阶段）的时间成比例，即每年实施监督审核的总时间约为初次认证审核时间的三分之一，至少为 1 个审核人日。再认证审核时间至少为该初次审核所需时间的三分之二，至少为 1 个审核人日。

5.8. 再认证审核

5.8.1. 再认证证书有效期满前，获证组织申请继续持有认证证书的，BCC 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/IEC 27701:2025 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，确认获证组织管理体系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管理体系绩效，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来确定，不少于依据附录 A 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，应对获证组织扩大认证范围的申请进行评审，策划并实施必要的审核活动，并在该审核活动中验证获证组织的管理体系的适宜性和有效性，以作出是否可予扩大的决定。扩大认证范围的审核活动可单独进行，也可和对获证组织的监督审核或再认证一起进行。

5.9.2 提前较短时间通知的审核

为调查投诉、对变更做出回应或对被暂停认证资格的获证组织进行追踪，可能需要在提前较短时间通知获证组织后对其进行审核。此时：

(1) 应向获证组织说明并使其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，BCC 审核方案管理人员应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，BCC 审核组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. BCC 审核组长负责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 BCC 审核组在下次审核时验证。

5.10.3. 严重不符合的验证时限应满足以下要求：

(1) 初次认证：在第二阶段审核结束之日起 30 天内完成；

(2) 监督审核：在审核结束之日起 30 天内完成；

(3) 再认证：在原认证证书到期前完成。

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，BCC 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. 每次审核 BCC 均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，反映认证委托人管理体系的真实状况，描述对照认证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) BCC 信息；

(2) 认证委托人信息：客户的名称、注册地址、经营地址、联系地址、联系人、联系方式及其最高管理者授权人；

(3) 审核类型；审核准则；审核目的；

(4) 审核范围以及尽管在审核范围内但本次审核没有覆盖到的区域，尤其应明确所审核的组织单元或职能单元或过程以及审核所覆盖的时期；

(5) 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；

(6) 任何偏离审核计划的情况及其理由；

(7) 任何影响审核方案的重要事项；

(8) 注明审核组长、审核组成员及个人注册信息，包括任何与审核组同行的人员；

(9) 对认证范围适宜性的结论；

(10) 确认在审核范围内已按审核计划达到审核目的；

(11) 文件审查的情况；

(12) 不符合项的情况，包括不符合项的说明、性质和分布；

(13) 应用信息通信技术审核的范围，以及信息通信技术在实现审核目的方面的有效性；

(14) 对管理体系的符合性、有效性和充分性进行综合评价和相关证据的总结：包括组织的管理体系与认证要求的符合性和实现预期结果的能力的评价意见；归纳审核所有发现，判断管理体系是否满足覆盖的产品 / 服务的特定要求的能力；应重视正面评价综述的每项内容，同时明确指出组织管理体系运行中不到位或须关注、加强、改进、完善之处；包括所遇到的降低审核结论可靠性的不确定因素和（或）障碍；

(15) 提交认证证书信息确认表，作为最终颁发认证证书和进行认证公告的依据，由受审核组织填写，审核组长审查确认并签字；

(16) 审核组长与认证委托人确认组织有效人数；

(17) 与审核类型要求一致的审核发现、对审核证据的引用以及审核结论；

(18) 如有时，在上次审核后发生的影响客户管理体系的重要变更；

(19) 审核组和认证委托人之间没有解决的分歧意见；

(20) 适用时，是否为结合、联合或一体化审核；

(21) 说明审核基于对可获得信息的抽样过程的免责声明；

(22) 审核组的推荐意见；

(23) 适用时，接受审核的客户对认证文件和标志的使用进行着有效的控制；

(24) 适用时，对以前不符合采取的纠正措施有效性的验证情况；

(25) 商定的审核后续活动计划（如果有）；

(26) 关于内容保密的声明；

(27) 审核报告的分发清单；

(28) 认证委托人受到的行政处罚和发生的事故事件，以及相关原因分析和整改措施的有效性；

(29) 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；

5.11.4. 审核组应保留用于证实审核报告中相关信息的审核证据并提交 BCC。

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，BCC 应将此报告提交给认证委托人。

5.12. 认证决定

5.12.1. BCC 应在对审核报告、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，做出认证决定。

认证决定人员应为 BCC 的专职认证人员，并不得为审核组成员，能力应满足关于认证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。

5.12.2. 认证决定人员应确保有充分的证据确认认证委托人满足下列条件后，做出授予、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 27701:2025 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。

5.12.3. 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，BCC 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。

5.12.5. 认证委托人不能满足 5.12.2 要求的，BCC 应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，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) BCC 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. BCC 已制定管理要求，要求获证组织正确使用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。

6.1.2. 获证组织可以在认证证书有效时使用管理体系认证证书和认证标志，并接受 BCC 的监督管理。认证证书处于暂停期间、被撤销或注销后，获证组织不得继续使用认证证书和认证标志。

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

6.1.4. 当 BCC 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. BCC 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。

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做出认证决定的日期。

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。

6.2.4. BCC 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，具体详见附录 B。

6.2.5. BCC 颁发中文证书；获证组织有需要时，可以颁发其他语言的认证证书，但以中文版为准。

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) 认证证书名称，即**“隐私信息管理体系认证证书”**；

(2) 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。

(3) 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）；

(4) 认证依据的认证标准 ISO/IEC 27701:2025 和 GB/T 22080-2025/ISO/IEC 27001:2022 所采用的当时有效版本的完整标准号；

(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继续有效的提示信息；

(6) 认证证书编号（或唯一的识别代码）；（编号规则见附录 B）

(7) BCC 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) BCC 的印章和总经理签名章；

6.3. 认证标志

使用 BCC 通用认证标志，样式如下：

BCC 的认证标志受法律保护，其他机构、组织或个人未经 BCC 的书面允许不得使用 BCC 认证标志。

7. 认证证书的暂停、撤销、注销、恢复认证或缩小认证范围

7.1. 总则

BCC 已建立并实施认证证书暂停、撤销、注销、恢复认证、缩小认证范围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、恢复认证或缩小认证范围

7.2.1. 获证组织有以下情形之一的，BCC 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，包括管理体系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的；

(3) 受到与隐私信息相关的行政处罚，且尚未完成整改的；

(4) 发生与此管理体系相关的重大事件（如失信事件、重大投诉等），反映获证组织管理体系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) 持有的与管理体系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 / 再认证审核的；

(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（含未按合同约定支付认证费用、未履行信息通报义务等）；

(10) 被有关行政监管部门责令停业整顿的；

(11) 发生与此管理体系相关重大舆情的；

(12) 主动请求暂停的；

(13) 监督审核期间发现的严重不符合，未在规定的期限内完成纠正措施的验证的；

(14) 由于获证组织原因，导致不符合项未在规定的时间内完成有效性验证并关闭的；审核结束后 180 天内未能通过认证决定；

(15) 出现国家、地方、行业相关监督抽查不合格的；

(16) 顾客对组织与此管理体系相关问题的重大投诉未能妥善处理并造成用户严重不满的；

(17) 其他应暂停认证证书的情形（如发生投诉经调查后属获证组织应负责任的、获证组织与 BCC 双方同意暂停认证资格等）。

7.2.2. 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，BCC 应恢复其认证证书，并保留相应证据。

7.2.4. 如果组织未能在规定的期限内解决造成暂停的原因，BCC 应撤销或缩小其认证范围。

7.2.5. 如果组织在认证范围的某些部分持续地或严重的不满足认证要求，BCC 应缩小其认证范围，以排除不满足要求的部分。认证范围的缩小应与认证标准的要求一致。

7.3. 认证证书的撤销

获证组织有以下情形之一的，BCC 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与管理体系相关的重大事故、严重不良影响事件的；

(5) 获证组织在证书有效期间受到相关执法监管部门处罚，且未能在规定时限内完成有效整改；

(6) 管理体系没有运行或者已不具备运行条件的（包括不再提供体系覆盖的所有产品和服务）；

(7) 审核未通过的；

(8) 监督审核时发现管理体系存在多项严重不符合规定要求，且在短期内无法有效纠正的；

(9) 获证组织虚报、瞒报获证所需关键信息的；

(10) 有严重违反法律法规的行为，或因违规行为造成严重影响的；

(11) 获证组织对相关方的重大投诉未能采取有效处理措施，造成严重后果的；

(12) 证书暂停期间因未按合同约定支付认证费用，超过暂停日期 90 天仍未支付的；

(13) 不承担、履行认证合同约定的责任和义务，情节严重的；

(14) 其他应撤销认证证书的情形。

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，BCC 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。

7.5. 认证证书失效

当发生下列情况时认证证书将自动失效：

(1) 获证组织的认证证书自然到期时；

(2) 获证组织通过再认证审核，并取得新的认证证书后，旧认证证书将自动失效；

(3) 获证组织通过标准转换审核，并取得新的认证证书后，旧认证证书将自动失效。

8. 信息公开与报告

8.1. BCC 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。

8.2. BCC 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。

8.3. BCC 通过其网站（www.bcc.com.cn）和 CNCA “全国认证认可信息公共服务平台（认 e 云）”向公众提供认证证书有效性查询。

8.4. BCC 通过其网站（www.bcc.com.cn）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。BCC 应在暂停、撤销、注销认证证书之日起 2 个工作日内，按规定程序和要求将相关信息报送国家认监委。

8.5. 获证组织发生与隐私信息有关的重大事故的，BCC 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。

9. 认证记录

9.1. BCC 已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。

9.2. 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。

9.3. 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《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。

9.4. 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。

9.5. 为了证实认证活动的实施，除了 BCC 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）

附录 A PIMS 审核时间表

在组织控制下从事涉及 PII 处理或加工工作，或可接触PII 的人员数量	PII - 控制者审核初始审核时间（审核人日）	PII - 处理者审核初始审计时间(审核人日)	PII -处理者+ 控制者审核时间，用于初始审核（ 审核人日）
1-10	4	3.5	6.5
11-15	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
2776-3450	14	9	21
3452-4350	14	10	22
4351-5450	15	10	22
5451-6800	16	10	23
6801-8500	16	11	24
8501-10700	17	11	25
>10700	沿用以上规律	沿用以上规律	沿用以上规律

注：我机构程序可以规定人数超过 10700 人时对审核时间的计算。该审核时间宜遵循表上表中的递进规律，与该表保持一致。

附录 B 证书编号规则

证书编号规则如下：

对同一个组织实施的同一个隐私信息管理体系认证，应使用同一个证书编号，认证机构代码	认证审核场所代码	发证年份号	管理体系缩写+标准版本代号	顺序号（五位）	认证周期	认可机构代码	子证书号/副本号
XXX	XX	XX	XX 或 XXX	XXXXX	R0(1,2,...)	XX	-X
数字	英文字母	数字	英文字母+数字	数字	英文字母+数字	数字	一数字
BCC 为：016	ZB-总部 SH-上海 BJ-北京 TJ-天津 KM-昆明 SY-沈阳 GZ-广州 JS-江苏 XA-西安 NJ-南京 XZ-徐州 CD-成都 SZ-深圳 HN-湖南 NM-内蒙古 TY-太原 CQ-重庆 WH-武汉 HF-合肥 …	认证证书签发年份：25-2025，26-2026，……	认证证书所属领域代号： PIMS	BCC 当年发出的该认证领域认证证书的顺序累计号：00001，00002，……	后缀表示初次认证或再认证换证号：初次认证为 R0，第一次再认证换证为 R1，第二次再认证换证为 R2，……	通过认可的填写认可机构代码，未通过认可代码为“00”。 CNAS 为：01 ANAB 为：04 UKAS 为：02 未通过认可的（即 BCC 证），为：00。 PIMS 领域为：00	多场所组织的子证书编号应与主证书的编号相关，在主证书编号后加子证书序号：-1，-2，…… 副本证书号在注册号后面加副本证书的分号：-A，-B…A，-B…

(1) 同一个组织的认证范围覆盖多个场所并需要颁发子证书时，在子认证证书编号后加上“-”和序号，如-1(-2，-3，…)。

(2) 有效期内换发证书，认证证书编号中的机构注册号、年份号、顺序号和认证的有效期保持不变，应注明换证日期。

(3) 再认证完成后换发证书，按 5.2.1 规定重新赋予认证证书编号，第一次再认证为“R1”，第二次再认证为“R2”，依此类推。

(4) 撤销证书后，原认证证书编号废止，不再使用。