BSC-03-W-01-PI-2026

版号：A/0

隐私信息管理体系认证规则

编制：丁　睿　2026.07.13

审核：王学武　2026.07.22

批准：董新峰　2026.07.29

三星九千认证
Beijing Sanxing 9000 Certification Body Co.,Ltd.

发布/实施日期：2026 年 7 月 29 日

目 录

1 适用范围

1.1 为规范信息安全、网络安全和隐私保护—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》《认证机构管理办法》等法律法规、部门规章和行政规范性文件，结合相关国际标准制定本规则。

1.2 本规则规定了北京三星九千认证有限公司（以下简称“公司”）依据 ISO/IEC27701:2025 实施 PIMS 认证的程序和管理要求，是公司从事 PIMS 认证活动、认证委托人建立和保持认证以及认证人员实施审核和认证决定的基本依据。

1.3 本规则适用于在中华人民共和国境内对承担个人可识别信息（以下简称“PII”）控制者和/或 PII 处理者角色的组织实施 PIMS 认证。认证范围可以覆盖组织全部或部分处理活动，但应当边界清晰、职责完整，且不得规避对认证范围内重大隐私风险的评价。

1.4 本规则仅设置“PII 控制者”和“PII 处理者”两类认证角色，不将联合 PII 控制者设置为独立认证角色。多个组织共同决定 PII 处理目的和处理方式时，认证委托人应当按照 PII 控制者申报，并接受对其自身决定权、责任分配和接口控制有效性的审核；认证证书不单列“联合控制者”身份。

1.5 组织同时承担 PII 控制者和 PII 处理者角色时，应当按照具体 PII 处理活动分别识别角色、责任、适用控制措施和证据。公司应分别形成审核结论，并在认证范围和认证证书中

清晰表述两类角色及对应活动，不得以笼统的“同时适用”替代角色判定。

1.6 PIMS 认证证明获证组织在确定的认证范围和认证角色内建立并有效运行符合认证依据的管理体系，不表示公司对其具体 PII 处理活动作出合法性保证，也不减免获证组织依法承担的责任。

2 认证依据

《信息安全、网络安全与隐私保护—隐私信息管理体系—要求与指南》（ISO/IEC27701:2025）。

注：本规则实施时，认证依据以正式发布的标准文本为准。GB/T27021.1/ISO/IEC17021-1 和 ISO/IEC27706:2025 为公司实施审核与认证的运行要求，不作为获证组织认证证书中列明的认证依据。

3 对认证机构的基本要求

3.1 公司应当在国家认监委认证规则备案系统完成本规则备案并公开后，方可依据本规则开展认证活动。

3.2 开展 PIMS 认证活动，应当围绕国家经济和社会发展目标，重点服务数字经济高质量发展和个人信息权益保护，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 公司的内部管理和认证活动应当符合 GB/T27021.1/ISO/IEC17021-1、ISO/IEC27706:2025 以及国家认

监委关于管理体系认证的有关规定，并持续具备实施PIMS认证所需的公正性、能力、一致性和责任安排。

3.4 公司应当建立风险防范机制，对PIMS认证活动可能引发的法律、合规、专业判断、信息泄露、公正性和声誉风险进行识别、评价和处置，并对认证活动引发的责任作出充分安排，包括购买保险或者建立合理的储备金。

3.5 公司应当建立PIMS认证人员管理制度，明确能力准则、选择条件、聘用、授权、监视、绩效评价和能力保持要求，确保参与申请评审、审核方案管理、审核、技术复核、认证决定以及申诉投诉处理的人员持续具备与其职责相适应的能力。

3.6 公司在拟开展的PIMS认证业务范围内，应当至少具备2名经能力评价合格的PIMS专业领域审核员。专业领域能力应当结合附录A的业务范围、组织认证角色、PII处理特征、适用法律法规以及技术环境进行识别。

PIMS专业领域审核员除具备管理体系审核能力外，还应当至少具备下列一项条件：

（1）具有本科（含）以上学历，且在中风险业务范围具有2年（含）以上与隐私保护、个人信息保护、信息安全、数据治理、法律合规相关的工作经历；在高风险业务范围具有3年（含）以上相关工作经历；

（2）具有相关专业中级（含）以上技术职称或者法律职业资格、信息安全相关专业资格，并具有2年（含）以上相关工作经历；

（3）具有5年（含）以上与拟评价业务范围相匹配的PII处理、隐私工程、信息安全、数据合规或者审计工作经历。

3.7 公司应当对PIMS专业领域进行适当细分，建立覆盖认证业务范围的能力分析和评价准则。人员能力评价应当有文件化证据，不得仅以培训经历或者通用审核员资格替代专业领域能力评价。

3.8 公司应当建立对审核人员审核活动的监视、见证和评价制度，对审核人员能力进行持续评价。扩大至高风险业务范围或者新增控制者/处理者角色授权前，应当完成相应能力评价。

3.9 公司应当对外包过程实施有效控制。认证决定不得外包。公司不得将申请评审、审核方案管理和认证决定整体委托给认证咨询机构或者与认证咨询存在利益关系的组织实施。

3.10 公司应当建立保护认证委托人和其他相关方信息的制度。审核过程中接触的PII、处理记录、数据流图、系统配置、事件记录和监管材料均应当按其敏感程度采取访问控制、加密、留存期限和安全销毁措施。非为形成充分审核证据所必需，不得复制原始PII。

3.11 公司不得以国家统一推行的认证制度、行政审批或者监管合规检查名义宣传PIMS认证，不得作出“通过认证即当然符合法律法规”或者其他可能误导社会公众的表述。

4 对认证人员的基本要求

4.1 从事PIMS认证审核的人员应当具备相应管理体系审核能力，并经公司评价、授权。审核组长应当具有组织和管理审核活动、综合判断管理体系有效性以及形成审核结论的能力。

4.2 PIMS审核员应当取得中国认证认可协会注册的信息安全管理体系审核员资格，并在注册资格有效期内承担审核任务。实习审核员可以在具备相应能力的审核员指导下参与审核，但不得独立承担审核任务或者作出审核结论。

4.3 PIMS审核员应当理解ISO/IEC 27701:2025的结构、术语和要求，掌握控制者与处理者角色判定、隐私风险评估与处置、PII主体权利、隐私影响评估、处理记录、委托处理、跨境传输、保留与删除、隐私事件管理以及信息安全控制等知识。

4.4 PIMS审核员应当能够基于实际决定权和处理行为判定认证委托人的认证角色，不得仅依据合同名称、组织自我声明或者业务习惯作出结论。对于同一组织承担多种角色的，应当能够按处理活动分解审核范围和适用控制措施。

4.5 专业技术专家可以为审核组提供特定法律、行业、技术或者业务知识，但不得独立实施审核或者作出审核结论。审

核组使用专业技术专家时，应当明确其任务并由审核员对其工作结果负责。

4.6 参与认证决定的人员应当具备评价审核过程完整性、审核证据充分性、角色判定合理性、认证范围准确性及不符合项处置有效性的能力，并且未参与被评价认证项目的审核。

4.7 认证人员应当遵守保密、公正和职业道德要求，与认证委托人存在咨询、雇佣、财务或者其他可能影响公正性的关系时，应当主动申报并回避。

4.8 公司应当根据标准、法律法规、技术和威胁环境的变化，对认证人员实施持续专业发展和必要的再评价。PIMS 审核人员每年应当完成与隐私保护、个人信息保护或者信息安全相关的持续学习活动。

5 认证程序

5.1 认证申请

5.1.1 公司应当向拟申请认证的组织至少公开下列信息：

（1）可开展认证业务的范围、认证依据和本认证规则；

（2）认证申请、评审、审核、认证决定、监督、再认证、证书状态管理以及申诉投诉处理程序；

（3）控制者、处理者以及同时承担两类角色时的申报和证书表述要求；

（4）认证收费标准或者收费方法；

（5）认证证书、认证标志及认证状态引用的使用要求；

（6）认证双方的权利、义务和责任；

（7）认证证书有效、暂停、撤销或者注销状态的查询方式。

5.1.2 认证委托人应当具备明确的法律地位。认证范围涉及行政许可、强制性资质或者其他法定条件的，应当取得相应资格并在有效期内。分支机构或者组织的一部分提出申请时，应当说明其与法人主体的关系以及承担 PIMS 责任和资源配置的权限。

5.1.3 提出认证申请时，认证委托人的 PIMS 应当按照 ISO/IEC27701:2025 建立并运行不少于 3 个月，已完成覆盖认证范围的内部审核和管理评审，并能够提供体系运行有效性的记录。

5.1.4 认证委托人及认证范围内的相关组织在申请前 12 个月内，不应当存在因故意或者重大过失侵害个人信息权益而受到责令停业整顿、吊销许可或者营业执照等严重行政处罚的情形；不存在尚未得到有效处置、足以影响 PIMS 有效性的重大 PII 泄露或者其他重大隐私事件。存在其他行政处罚、监管措施、投诉争议或者事件的，应当如实说明并提供整改证据。

5.1.5 认证委托人应当提交真实、完整、有效的认证申请材料，至少包括：

（1）认证申请书、法律地位证明、必要的行政许可或者资质证明；

（2）拟认证范围、组织边界、场所、组织单元、人员、主要系统和外包过程；

（3）认证角色声明及角色—处理活动矩阵，说明各类PII处理活动中组织作为控制者或者处理者的事实依据；

（4）PII处理活动清单和数据流说明，包括处理目的、PII和PII主体类别、规模、来源、接收方、存储地点、保留期限、跨境或者跨法域情况；

（5）适用的法律法规、监管要求、合同义务以及组织确定的其他要求清单；

（6）PIMS方针、目标、职责、风险评估和风险处置过程文件，适用性声明及其版本；

（7）隐私影响评估的准则和已实施评估的结果摘要；

（8）与控制者、处理者、次级处理者、共同参与处理活动的其他组织之间的合同或者责任接口说明；

（9）近12个月PII主体请求、投诉、隐私事件、监管检查、行政处罚及纠正措施的汇总信息；

（10）内部审核、管理评审及主要改进活动的记录；

（11）公司为确定专业能力、审核时间和审核方案所需的其他信息。

5.1.6 认证委托人声明为PII控制者的，应当说明其决定处理目的和处理方式的权限及其证据；声明为PII处理者的，应当说明其依据控制者书面指示实施处理的范围、限制和合同安排。

5.1.7 认证委托人同时承担两类角色的，应当按处理活动分别填报，不得仅以组织部门、信息系统或者客户类型作为角

色划分依据。同一处理链条中的角色发生变化时，应当说明触发条件和控制措施。

5.1.8 认证委托人对其提交材料的真实性、准确性和完整性负责。发现隐瞒重大隐私事件、虚构认证角色、缩小认证边界规避重大风险或者提供虚假材料的，公司应当不予受理或者终止认证。

5.2 申请评审

5.2.1 公司应当对认证申请及相关资料进行评审并保存记录，确认具备受理和实施认证的能力。申请评审至少包括：

（1）认证委托人的法律地位和开展相关活动的合法资格；

（2）认证依据、认证范围、组织边界、场所、过程和系统是否明确；

（3）控制者、处理者角色声明是否与实际决定权、合同约定和处理行为一致；

（4）PIMS 运行时间以及内部审核、管理评审的完成情况；

（5）PII 类别、PII 主体类别、处理规模、敏感程度、未成年人信息、自动化决策、公开披露、监控、跨境或者跨法域处理等复杂性；

（6）适用法律法规、监管要求和近 12 个月处罚、投诉、争议、隐私事件及整改情况；

（7）公司与认证委托人之间理解上的差异是否得到解决；

（8）公司是否具备相应专业领域、认证角色、技术和法域所需的人员能力和资源；

（9）审核时间、多场所抽样和审核方案是否能够保证获得充分、适宜的审核证据。

5.2.2 角色判定应当遵循实质重于形式原则。组织能够自主决定 PII 处理目的或者关键处理方式的，原则上判定为 PII 控制者；组织仅依据控制者的成文指示处理 PII，且不能将 PII 用于自身目的的，原则上判定为 PII 处理者。

5.2.3 对于角色证据相互矛盾、责任边界不清或者存在明显规避控制者义务情形的，公司应当要求认证委托人补充说明或者调整申请。无法作出可靠角色判定的，不应当受理认证申请。

5.2.4 对同时承担两类角色的申请，公司应当确认角色—处理活动矩阵覆盖全部拟认证活动，并据此确定适用控制集、审核时间、审核组能力和抽样方案。共同适用的信息安全控制可以整合审核，但两类角色特有控制及相应证据不得相互替代。

5.2.5 公司应当根据评审结果决定受理、补充材料或者不予受理，并将结果告知认证委托人。不予受理时，应当说明理由。

5.3 认证合同及相关责任

5.3.1 公司决定受理认证申请的，应当与认证委托人签订具有法律效力的认证合同。合同应当至少明确：

（1）认证依据、认证范围、认证角色、场所和预计认证周期；

（2）审核和认证活动的安排、收费标准、支付方式以及因范围或角色变化导致的费用调整机制；

（3）认证双方在资料提供、人员访问、场所和系统访问、保密、信息安全和PII保护方面的权利、义务和责任；

（4）认证委托人接受监督审核、再认证审核、特殊审核和必要的见证评价的义务；

（5）认证委托人发生组织、认证角色、处理目的、主要处理方式、PII类别、技术平台、场所、跨境安排、重大供应商或者重大隐私事件等变化时及时报告的义务；

（6）认证证书、认证标志和认证状态引用的使用要求，以及违规使用的处置；

（7）暂停、撤销、注销、缩小或者扩大认证范围的条件和程序；

（8）申诉、投诉和争议处理机制。

5.3.2 认证费用应当由认证委托人直接向公司支付。公司不得通过认证咨询机构或者其他可能影响公正性的中间机构收取认证费用。

5.3.3 公司及其人员应当依法履行保密义务。认证委托人应当在满足审核有效性的前提下，对提供给公司的PII进行最小化、去标识化或者脱敏处理，并告知访问限制。公司不得以保密为由降低必要审核深度。