

挪亚检测认证集团有限公司

ISO/IEC 27701隐私信息管理体系

认证实施规则

文件编号：NOAQC/NSH/S/OD-65

编写主责部门：信安部

版次	修订章节及主要修订内容概述	首次/修订生效日期	审核/核准
1/0	初次制定	2021.5.8	岑川/杨万霞
2/0	增加项目受理要求及审核时间策划要求	2024.6.11	石尚淑/杨万霞
2/1	格式调整	2024.10.9	张智超/杨万霞
评审部门		使用部门	
信安部		信安部	

1、 目的

制定本规则旨在结合认证认可相关法律法规和技术标准对审核组织隐私信息管理体系实施审核过程作出具体规定，明确公司对认证过程的管理责任，保证认证活动的规范有效。

2、 适用范围

2.1 本规则用于规范挪亚检测认证集团有限公司（以下简称“NOA”）开展ISO/IEC 27701隐私信息管理体系（PIMS）认证活动。

2.2 制定本规则旨在结合认证认可相关法律法规和技术标准对审核组织管理体系实施过程作出具体规定，明确公司对认证过程的管理责任，保证认证活动的规范有效。

3、 管理要求

3.1 遵循ISO/IEC 17021-1《合格评定 管理体系审核认证机构要求》、ISO/IEC 27001《信息技术 安全技术 信息安全管理体系要求》、ISO/IEC 27701《信息技术 安全技术 隐私信息管理体系要求》及其他相关系列标准要求。

3.2 建立内部制约、监督和责任机制，实现培训、认证和认证决定等工作环节相互分开，以符合公正性要求。

3.3 提供的管理体系认证可结合其他管理体系认证活动进行。

4、 对认证人员的要求

4.1 认证人员必须具备相应的资质和专业知识，能够理解和应用ISO/IEC 27001标准的要求。

4.2 认证人员应接受过ISO/IEC 27001标准及相关审核技巧的培训。

4.3 认证规则、认证方案制定人员和合同评审人员、认证决定人员、人员能力评价人员、审核方案管理人员应经评价确认满足 NOA 人员能力的要求。

4.3.1 如认证规则、认证方案制定人员和认证决定人员、人员能力评价人员同时为审核员时，对其审核员资格的评价可替代其认证管理人员的能力评价。

4.4 认证人员应当遵守与从业相关的法律法规，对认证活动及作出的认证审核报告和认证结论的真实性承担相应的法律责任。

5、 认证依据

GB/T 27021.1 dit ISO/IEC 17021-1《合格评定 管理体系审核认证机构要求》

ISO/IEC 27001 《信息技术 安全技术 信息安全管理体系要求》

ISO/IEC 27701 《信息技术 安全技术 隐私信息管理体系要求》

6、 初次认证程序

6.1 受理认证申请

6.1.1 认证申请组织应具备以下条件：

- (1) 取得国家工商行政管理部门或有关机构注册登记的法人资格；
- (2) 已取得相关法规规定的行政许可（适用时）；
- (3) 提供的服务/产品符合中华人民共和国相关法律、法规和有关规范的要求；
- (4) 法律法规要求的行政许可证明、资质证书等的复印件；
- (5) 与认证审核有关的必要文件；
- (6) 建立和实施了管理体系，且有效运行3个月以上；
- (7) 在一年内，未发生违反国家相关法律法规，未列入严重违法失信企业名单；
- (8) 已获得27001证书或同时在NOA申请27001和27701的结合审核；
- (9) 组织申请的IPMS的业务范围不能超过ISMS的业务范围。

6.2 申请评审

6.2.1 认证申请组织应提交的文件和资料：

- (1) 认证申请书，包括申请组织的生产经营或服务活动等情况的说明；
- (2) 申请组织从事的活动符合相关认证规则 and 法律法规的规定；
- (3) 营业执照组织机构代码证书复印件；
- (4) 行政许可文件证明文件（适用时）；
- (5) 管理体系文件；
- (6) 如果不是27001和27701结合审核的情况，需要提供27001证书编号；
- (7) 其他需要的文件。

6.2.2 根据申请组织申请的认证范围、生产经营场所、员工人数、完成审核所需时间和其他影响认证活动的因素，综合确定是否有能力受理认证申请。

6.2.3 对符合要求的，可受理认证申请；对不符合上述要求的，将通知申请组织补充和完善，或者不受理认证申请。

6.3 应完整保存认证申请的审查确认记录。

6.4 签订认证合同

在实施认证审核前，应与申请组织订立具有法律效力的书面认证合同。

6.5 审核组和审核计划

6.5.1 审核时间

6.5.1.1 审核时间的确定

除了ISO/IEC27006:2015 9.1.4.1之外，NOA确定审核ISO27701需要花费的额外审核时间。

对PIMS特定方面所需的审计时间至少应为：

-30%的审计时间（如果审计客户是PII控制器）；

-20%的审计时间（如果审计客户是PII处理器）；

-50%的审计时间（如果审计客户同时是PII控制器和处理器）。

根据ISO/IEC27006:2015 9.1.4和附件B，为相同的ISO/IEC27001认证范围计算。

PIMS初始审计（第1阶段和第2阶段）的额外审计时间对于PII处理者至少为2.5天，对于PII控制者至少为3天，对于PII处理者和PII控制者至少为3.5天。

如果该组织已经通过ISMS（ISO/IEC27001）认证，并且PIMS初审与ISMS审核分开进行（即ISMS监督审核或ISMS再认证审核），则应在审核时间中至少增加0.5个审核天，以验证ISMS（特别是其管理体系方面，如内部审计和管理评审）是否按照ISO/IEC27701中的规定扩展到包括 PIMS的控制。

6.5.2 审核组确定

6.5.2.1 应当根据管理体系覆盖的活动的专业技术领域选择具备相关能力的审核员和技术专家组成审核组。审核组中的审员应承担审核责任。

6.5.2.2 技术专家主要负责提供审核的技术支持，不作为审核员实施审核,不计入审核时间。

6.5.2.3 审核组可以有实习审核员，其要在审核员的指导下参与审核，不计入审核时间，在审核过程中的活动由审核组中的审核员承担责任。

6.5.3 审核计划

6.5.3.1 审核组长接受审核任务后，应制定书面的审核计划给审核组成员和受审核方，审核计划至少包括以下内容：审核目的、审核范围、审核过程、审核涉及的部门和场所、审核持续的时间、审核组成员。

6.5.3.2 通常情况下，初次认证审核、监督审核和再认证审核应在申请组织申请认证的范围涉及到的各个场所现场进行。如管理体系包含在多个场所进行相同或相近的活动，且这些场所都处于该申请组织授权和控制下，可对这些场所进行抽样，但应制定合理的抽样方案以确保对各场所管理体系的正确审核。如果不同场所的活动存在根本不同、或不同场所存在可能对体系管理产生显著影响的区域性因素，则不能采用抽样审核的方法，应当逐一到各现场进行审核。

6.5.3.3 为使现场审核活动能够观察到产品生产或服务活动情况，现场审核应安排在认证范围覆盖的产品生产或服务活动正常运行时进行。

6.5.3.4 在审核活动开始前，审核组应将书面审核计划交申请组织确认。遇特殊情况临时变更计划时，应及时将变更情况书面通知受审核的申请组织，并协商一致。

6.6 实施审核

6.6.1 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员（技术专家和实习审核员除外）。

6.6.2 审核组应当会同申请组织召开首、末次会议，首末次会议应有签到表。

6.6.3 审核过程及环节

6.6.3.1 初次认证审核，分为第一、二阶段实施审核。

6.6.3.2 第一阶段审核应至少覆盖以下内容：

(1) 结合现场情况，确认申请组织实际情况与管理体系文件描述的一致性，特别是体系文件中描述的产品或服务、部门设置和负责人、生产或服务过程等是否与申请组织的实际情况相一致。

(2) 结合现场情况，审核申请组织有关人员理解和实施标准要求的情况，评价管理体系运行过程中是否已进行了内部审核与管理评审，确认管理体系是否已有效运行。

(3) 确认申请组织建立的管理体系覆盖的活动内容和范围、申请组织的员工人数、活动过程和场所，遵守相关法律法规及技术标准的情况。

(4) 结合管理体系覆盖活动的特点识别对产品的实现具有重要影响的关键点，以及是否得到了控制。

(5) 与申请组织讨论确定第二阶段审核安排。

6.6.3.3 审核组应将第一阶段审核中的问题以书面的形式告知申请组织，并按审核组要求进行整改。

6.6.3.4 第一阶段审核和第二阶段审核应安排适宜的间隔时间，使申请组织有充分的时间解决第一阶段中发现的问题。

6.6.3.5 第二阶段审核应当在申请组织现场进行。重点是审核管理体系符合标准要求和有效运行情况，应至少覆盖以下内容：

(1) 符合性评估：评估组织的产品和流程是否符合ISO 27701标准的具体要求。

(2) 风险管理：检查组织是否已经识别并评估了与产品和供应链相关的风险，并且是否已经实施了适当的风险缓解措施。

(3) 安全措施：评估组织是否已经实施了足够的安全措施来保护产品免受恶意软件或硬

件的威胁。

(4) 产品完整性：检查产品在设计、开发、生产和交付过程中是否保持了完整性。

(5) 监控和改进：评估组织是否有监控和测量程序来确保管理体系的有效性，并且是否有持续改进的机制。

(6) 不符合项的纠正措施：如果之前阶段的审核发现了不符合项，第二阶段审核将检查这些不符合项是否已经被纠正，并且是否采取了措施防止再次发生。

(7) 文档和记录：评估组织是否保持了必要的文档和记录，以证明其管理体系的运行和符合性。

(8) 员工意识和培训：检查组织是否对员工进行了适当的培训，以确保他们了解ISO 27001标准的要求和组织的安全管理措施。

(9) 应急准备和响应：评估组织是否有计划和程序来应对可能的安全事件，并且是否进行了定期的应急演练。

6.6.4 发生以下情况时，审核组应终止审核，并向NOA相关部门或人员报告。

(1) 申请组织对审核活动不予配合，审核活动无法进行。

(2) 申请组织的管理体系有重大缺陷，不符合标准的要求。

(3) 发现申请组织存在重大质量问题或有其他严重违法违规行为。

(4) 其他导致审核程序无法完成的情况。

6.7 审核报告

6.7.1 审核组应对审核活动形成书面审核报告，由申请组织代表确认。审核报告应准确、简明和清晰地描述审核活动的主要内容，至少包括：

(1) 审核范围：明确指出审核所覆盖的组织、产品、服务和过程。

(2) 审核目的和目标：描述审核的主要目的和目标。

(3) 审核日期和地点：列出审核进行的日期和地点。

(4) 审核组成员：列出参与审核的审核员姓名和角色。

(5) 审核方法和程序：简要说明使用的审核方法和遵循的程序。

(6) 审核发现：详细记录审核过程中发现的符合和不符合标准要求的证据。

(7) 不符合项：列出所有识别的不符合项，并提供足够的细节以便申请组织能够理解和纠正。

(8) 风险评估：如果适用，提供对识别风险的评估和建议的风险缓解措施。

(9) 审核结论：基于审核发现，提供关于组织管理体系是否符合ISO27701标准的结论。

(10) 建议和改进措施：基于审核发现，提出建议和改进措施以提高管理体系的有效性。

- (11) 审核报告的分发清单：列出所有应接收审核报告的组织和个人。
- (12) 附件：包括任何相关的附件，如审核检查表、访谈记录、观察记录等。
- (13) 审核报告的批准：由审核组长和申请组织代表签字确认。
- (14) 审核报告的日期：注明审核报告完成的日期。
- (15) 保密声明：如果适用，包括关于审核报告保密性的声明。

6.7.2 认证决定后NOA需将最终审核报告提交申请组织，并保留电子版。

6.7.3 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，NOA将此报告及终止审核的原因提交给申请组织，并保留电子邮件发送和对方接受的证据。

6.8 不符合项的纠正和纠正措施及其结果的验证

6.8.1 对审核中发现的不符合项，审核组将开具不符合报告，申请组织应分析原因，说明为消除不符合已采取或拟采取的具体纠正和纠正措施，并在规定期限内采取措施进行整改。

6.8.2 审核组长将对所采取的纠正、原因分析和纠正措施及其结果的有效性进行验证。

6.9 认证决定

6.9.1 认证决定人员应根据审核组提交的审核资料以及受审核方提交的整改证据进行综合评价基础上，作出认证决定。

6.9.2 审核组成员不得参与对审核项目的认证决定。

6.9.3 在作出认证决定前应确认如下情形：

- (1) 审核资料和审核信息完整。
- (2) 审核组已对所有不符合事项评审、接受并验证了纠正、原因分析和纠正措施及其结果的有效性。

6.9.4 有充分的客观证据证明申请组织满足下列要求的，评定该申请组织符合认证要求，向其颁发认证证书：

- (1) 申请组织的管理体系符合标准要求且运行有效。
- (2) 认证范围覆盖的产品或服务符合相关法律法规要求。
- (3) 申请组织按照认证合同规定履行了相关义务。

6.9.5 申请组织不能满足上述要求的，以书面形式告知申请组织并说明其未通过认证的原因。

6.9.6 NOA在颁发认证证书后，将按照规定的要求将相关信息报送国家认监委。

7、 监督审核程序

7.1 NOA应对持有其颁发的管理体系认证证书的组织（以下称获证组织）进行有效跟踪，监督获证组织通过认证的管理体系持续符合要求。

7.2 应根据获证组织的产品或服务的质量风险程度或其他特性，确定对获证组织的监督审核的频次。

7.2.1 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。此后，监督审核至少每个日历年（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15个月。

7.2.2 超过期限而未能实施监督审核的，应按8.1或8.2条处理。

7.3 年度监督审核的时间，原则上为初次审核人日数的1/3，可适当调整。

7.4 监督审核的审核组，应符合5.5.2条的要求。

7.5 监督审核应在获证组织现场进行。

7.6 监督审核时至少应审核以下内容：

(1) 上次审核以来持续运行IPMS，考虑因客户组织的变化而对该系统所做更改的影响，并确认是否持续符合认证要求。

(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) 教育组织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。

(4) 总质量目标及各层级质量目标是否实现。目标没有实现的，是否及时调查并采取了改进措施。

(5) 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相关的规定。

(6) 内部审核和管理评审是否和有效。

(7) 是否及时接受和处理申诉投诉。

(8) 针对内审发现的问题或投诉的问题，及时制定并实施了有效的持续改进。

7.7 监督审核的审核报告，应按审核要求描述审核证据、审核发现和审核结论。审核组应提出是否继续保持认证证书的意见建议，包括先前发现的不符合项的解决信息，以及SOA的版本和自上次审核以来的重大变更。

7.8 认证决定人员根据监督审核报告及其他相关信息，作出继续保持或暂停、撤销认证证书的决定。

8、再认证程序

8.1 管理体系认证证书期满前，若获证组织申请继续持有认证证书，应当实施再认证审核决定是否延续认证证书。

8.2 按5.5.2条要求组成审核组。审核组长结合历次监督审核情况，评价上一周期的绩效，根据评价情况制定再认证计划。审核组按照要求开展再认证审核。

8.3 在管理体系及获证组织的内部和外部环境无重大变更时，再认证审核可不进行第一阶段审核，但审核时间应不少于初次审核所计算人日数的2/3。

8.4 允许实施纠正措施的时间应与不符合项的严重程度和体系风险成比例。

8.5 参照5.9条要求作出再认证决定。获证组织继续满足认证要求并履行认证合同义务的，向其换发认证证书。

9、 暂停或撤销认证证书

9.1 暂停证书

9.1.1 获证组织有以下情形之一的，经调查核实，在5个工作日内暂停其认证证书。

- (1) 管理体系持续或严重不满足认证要求，包括对管理体系运行有效性要求的。
- (2) 不承担、履行认证合同约定的责任和义务的。
- (3) 被有关执法监管部门责令停业整顿的。
- (4) 被地方认证监管部门或认可机构发现体系运行存在严重问题，需暂停证书的。
- (5) 主动请求暂停的。
- (6) 27001证书暂停的。
- (7) 其他应当暂停认证证书的。

9.1.2 认证证书暂停不得超过6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。

9.2 证书的撤销

9.2.1 获证组织有以下情形之一的，NOA将在获得相关信息并调查核实后撤销其认证证书。

- (1) 被注销或撤销法律地位证明文件的。
- (2) 拒绝配合监管部门实施的监督检查，或者对有关事项的询问和调查提供了虚假材料或信息的。
- (3) 出现重大的产品或服务的质量事故，经执法监管部门确认是获证组织违规造成的。
- (4) 有其他严重违法违反法律法规行为的。
- (5) 暂停认证证书的期限已满但导致暂停的问题未得到解决或纠正的（包括持有的行政许可证明、资质证书、强制性认证证书等已经过期失效但申请未获批准）。
- (6) 未运行管理体系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，或者必须认证已要求其纠正但超过6个月仍未纠正的。
- (8) 27001证书撤销的。
- (9) 其他应当撤销认证证书的。

9.3 撤销认证证书后，NOA通知获证组织不得继续使用证书及认证标志；并在NOA网站上公布撤销的信息。

9.4 暂停及撤销认证证书的消息将按规定程序和要求报认监委。

10、 认证证书要求

10.1 管理体系认证证书应至少包含以下信息：

- (1) 获证组织名称、地址和组织机构代码。
- (2) 管理体系覆盖的生产经营或服务的地址和业务范围的描述。若认证的管理体系覆盖多场所，应表述覆盖的相关场所的名称和地址信息。
- (3) 管理体系符标准的表述。
- (4) 证书编号。
- (5) 认证机构名称。
- (6) 证书签发日期及有效期的起止年月日。对初次认证以来未中断过的再认证证书，可表述该获证组织初次获得认证证书的年月日。
- (7) 27001证书编号。
- (8) 获证组织IPMS体系角色。
- (9) 获证组织27701适用性声明。
- (10) 相关的认可标识及认可注册号（适用时）。

10.2 管理体系认证证书有效期最长为3年。

10.3 证书信息按认监委相关要求上报管理体系认证证书信息；可通过电话查询或书面向NOA查询。

11、 认证范围的变更

11.1 获证组织业务范围变更时，应告知本机构，并按本机构的要求提交相关材料。

11.2 本机构根据获证组织的变更情况，策划并实施适宜的审核活动，并按照 5.9 要求做出关于是否扩大、缩小或变更认证范围的决定。相关审核活动可单独进行，也可结合获证组织的监督或再认证审核进行。

11.3 获证组织PIMS的业务范围不能超过ISMS的业务范围。

12、 与其他管理体系的结合审核

12.1 当管理体系认证审核和其他管理体系认证审核结合实施时，应同时遵照本规则要求以及

其他管理体系认证的相关要求。

12.2 当审核的管理体系和其他管理体系认证审核结合实施时，总审核人日数按照体系结合审核计算。

13、 受理组织的申诉

申请组织对认证决定有异议时提出申诉，应及时进行处理，在三十个工作日内将处理结果形成书面通知送交申请组织。

14、 认证记录的管理

证明认证活动全过程满足相关法规、认可规则等适用要求的证据应予以保持并妥善保存。记录可以用纸质或电子文档的方式加以保存。