挪亚检测认证集团有限公司

NOA Testing & Certification Group Ltd

信安系列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	2015.7.27	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
2/2	根据实际操作情况修正认证流程要求	2025.5.14	张智超/杨万霞

评审部门	使用部门
信安部、技术委员会、合规技术部	信安部、技术委员会

1、适用范围

1.1对本规则用于规范挪亚检测认证集团有限公司（以下简称“ NOA”)开展管理体系认证活动。

1.2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，保证认证活动规范有效。

2、管理要求

2.1 GB/T 27021.1/ISO/IEC 17021-1《合格评定 管理体系审核认证机构要求》及ISO/IEC27006-2《对提供信息安全管理系统审计和认证的机构的要求-第2部分:隐私信息管理系》其他相关系列标准要求

2.2 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。

2.3 提供的管理体系认证可结合其他管理体系认证活动进行。

3、对认证人员的要求

3.1 审核人员应当具有相应管理体系注册资格。

3.2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。

3.2.1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。

3.3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。

4、认证依据

ISO 27034-1《信息技术 安全技术 应用软件安全保障 第 1 部分：总则》

ISO 27034-2《信息技术 安全技术 应用软件安全保障 第 2 部分：实施指南》

ISO 27034-3《信息技术 安全技术 应用软件安全保障 第 3 部分：应用软件安全能力成熟度模型》

ISO 27034-5《信息技术 安全技术 应用软件安全保障 第 5 部分：应用软件安全控制》

ISO 27034-6《信息技术 安全技术 应用软件安全保障 第 6 部分：应用软件安全事件响应》

 Copyright ©NOA Testing & Certification Group Ltd. 2021

ISO 27034-7《信息技术 安全技术 应用软件安全保障 第 7 部分：应用软件安全审计》

ISO/IEC 27701《安全技术 针对 ISO/EC 27001和 ISO/IEC 27002在隐私信息管理的扩展要求和指南》

ISO/IEC 27017《信息技术 安全技术 基于ISO/EC27002云服务的信息安全控制实施规范》

ISO/IEC 27018《信息技术安全技术 个人可识别信息(PI)处理者在公有云中保护PI的实践指南》

ISO/IEC 29151《信息技术 安全技术 个人识别信息保护行为准则》

5、初次认证程序

5.1 受理认证申请

5.1.1 认证申请组织应具备以下条件：

（1）取得市场监督管理部门或有关机构注册登记的执照或其它证明。

（2）已取得相关法规规定的行政许可（适用时）。

（3）生产、加工的产品或提供的服务符合中华人民共和国相关法律、法规和有关规范的要求。

（4）与认证审核有关的必要文件。

（5）建立和实施了管理体系，且运行时间满3个月的运行要求。

（6）未列入严重违法失信企业名单。

5.2 申请评审

5.2.1 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）管理手册、适用性声明。

（3）营业执照或其它证明文件。

（4）行政许可文件证明文件（适用时）。

（5）其他需要的文件。

5.2.2 申请组织已获得ISO/IEC 27001认证证书，或者与该认证同时申请。且本次认证的认证范围、物理边界、有效人数等不超过其所依据的ISO/IEC 27001认证范围、物理边界、有效人数等。

5.2.3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。

5.2.4 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，

 Copyright ©NOA Testing & Certification Group Ltd. 2021

或者不受理认证申请。

5.3 应完整保存认证申请的审查确认记录。

5.4 签订认证合同

在实施认证审核前，应与申请组织订立认证合同。

5.5 审核组和审核计划

5.5.1 审核时间

5.5.1.1 为确保认证审核的完整有效，应以相关的认可文件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、质量安全风险程度、认证要求和员工人数等情况，核算并拟定完成审核工作需要的时间。在特殊情况下，可以减少审核时间，但减少的时间不得超过30％。

5.5.1.2 整个审核时间中，现场审核时间不应少于删减后审核时间的70％。 和其它体系结合审核时，可根据结合程度进行删减，最后不超过20%。

5.5.2 审核组确定

5.5.2.1 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。

5.5.2.2 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。

5.5.2.3 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。

5.5.3审核计划

5.5.3.1 审核组长接受审核任务后，应制定审核计划，并在审核开始前或结合首次会议和受审核方确认。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。

5.5.3.2 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的厂所进行。

5.5.3.3 为使现场审核活动能够观察到产品生产或服务活动情况，现场审核应安排在企业正常经营活动时进行。

5.5.3.4 在审核活动开始前，审核组应和受审核方确认审核安排。遇特殊情况临时变更计划时，应与受审核方协商后修改审核计划。

5.6 实施审核

5.6.1 审核组应当按计划完成审核计划的工作。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）。

 Copyright ©NOA Testing & Certification Group Ltd. 2021

5.6.2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。

5.6.3 审核过程：

5.6.3.1 初次认证审核，分为第一、二阶段实施审核。

5.6.3.2 第一阶段审核应至少覆盖以下内容：

（1）确认申请组织实际情况与管理体系文件描述的一致性。

（2）若未与ISO27001同时申请认证，申请组织的ISO27001运行情况及其证书有效性。

（3）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，确认管理体系是否运行。

（4）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。

（5）与申请组织讨论确定第二阶段审核安排。

5.6.3.3 一阶段审核是否需要进入申请组织现场，参照对应程序文件要求执行 。

5.6.3.4 审核组应将第一阶段审核中的结论告知申请组织。

5.6.3.5 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，如第一阶段审核没有发现重大问题，可以直接进行二阶段的审核。

5.6.3.6 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）在第一阶段审核中识别的重要审核点以及问题的整改情况。

（2）若未与ISO27001同时申请认证，对申请组织的ISO27001运行情况及相关审核资料确认。

（3）总目标以及各层级目标是否具体、有针对性、可测量并且可实现。

（4）对管理体系覆盖的过程和活动的管理及控制情况。

（5）申请组织实际工作记录与其自身文件要求的符合性。

（6）申请组织的内部审核和管理评审。

（7）改进机制和实施的总体绩效。

5.6.4 发生现场审核组应终止审核，并向 NOA相关部门或人员报告。

5.7 不符合项的纠正和纠正措施及其结果的验证

5.7.1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。

5.7.2 审核组长将对所采取的纠正情况进行验证。

5.8 审核报告

 Copyright ©NOA Testing & Certification Group Ltd. 2021

5.8.1审核组应对审核活动形成书面审核报告，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：

a) 注明认证机构；

b) 客户的名称和地址及客户的代表；

c) 审核的类型（例如初次、监督、再认证或特殊审核）；

d) 审核准则；

e) 审核目的；

f) 审核范围，特别是标识出所审核的组织或职能单元或过程，以及审核时间；

g) 任何偏离审核计划的情况及其理由；

h) 任何影响审核方案的重要事项；

i) 注明审核组长、审核组成员及任何与审核组同行的人员；

j) 认证所依据的ISO/IEC27001认证运行情况；

k) 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；

l) 与审核类型的要求一致的审核发现、对审核证据的引用以及审核结论；

m) 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；

n) 已识别出的任何未解决的问题；

o) 适用时，是否为结合、联合或一体化审核；

p) 说明审核基于对可获得信息的抽样过程的免责声明；

q) 审核组的推荐意见；

r) 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；

s) 适用时，对以前不符合采取的纠正措施有效性的验证情况。

5.8.2 认证决定后NOA需将最终的审核报告提交申请组织。

5.9 认证决定

5.9.1 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。

5.9.2 审核组成员不得参与对审核项目的认证决定。

5.9.3 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、接受了企业的纠正证据。

5.9.4 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：

 Copyright ©NOA Testing & Certification Group Ltd. 2021

（1）申请组织的管理体系符合标准要求。

（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。

5.9.5 申请组织不能满足上述要求的，应告知申请组织并说明其未通过认证的原因。

5.9.6 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。

6、监督审核程序

6.1 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。

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

6.2.1 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。

6.2.2 超过期限而未能实施监督审核的，应按8.1或8.2条处理。

6.3 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。

6.4 监督审核的审核组，应符合5.5.2条的要求。

6.5 监督审核应在获证组织现场进行。

6.6 监督审核时至少应审核以下内容：

（1）上次审核以来教育组织管理体系覆盖的活动及运行体系的资源是否有变更。

（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）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）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按规定进行。

（7）是否及时接受和处理投诉。

（8）针对内审发现的问题，是否及时制定并实施了有效的持续改进。

6.7 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。

6.8 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。

 Copyright ©NOA Testing & Certification Group Ltd. 2021

7、再认证程序

7.1 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。

7.2 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。

7.3 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。

7.4 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。

8、暂停或撤销认证证书

8.1 暂停证书

8.1.1 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。

（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）其他应当暂停认证证书的。

8.1.2 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。

8.2 证书的撤销

8.2.1 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等质量事故，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）。

 Copyright ©NOA Testing & Certification Group Ltd. 2021

（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的。

（8）其他应当撤销认证证书的。

8.3 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；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。

9、认证证书要求

9.1 管理体系认证证书应至少包含以下信息：

（1）获证组织名称、地址和组织统一社会信用代码。

（2）管理体系覆盖的生产经营或服务的地址和业务范围。

（3）管理体系符标准的表述。

（4）证书编号。

（5）认证机构名称。

（6）认证所依据的ISO/IEC27001的证书编号、适用性声明及版本号

（7）适用性声明及版本号

（7）证书签发日期及有效期的起止年月日。

（8）相关的认可标识及认可注册号（适用时）。

9.2 初次认证认证证书有效期最长为3年。再认证的认证证书有效期不超过最近一次有效认证证书截止期再加3年。

9.3 证书信息按认监委相关要求上报管理体系认证证书信息；亦可通过NOA官网进行查询。

10、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，并将处理结果通知申请组织。

11、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。

 Copyright ©NOA Testing & Certification Group Ltd. 2021