



挪亚检测认证集团有限公司

NOA Testing& Certification Group Ltd.

信息安全服务资质认证实施规则

Number: NOAQC/NSH/P/OD-25

Controlled: Yes ☒ No ☐

Issue Number: 1

Revise No.: 0

Draw up: Technical Dept.

Reviewed by: General Manager

Approval: General Manager

Implementation Date: Aug.30,2021

信息安全服务资质认证实施规则

1 适用范围

本实施规则适用于挪亚检测认证集团有限公司（以下简称“NOA”）对信息安全服务资质认证活动。

2 认证依据

对特定类别的信息安全服务，有具体的评价标准。例如，信息安全应急处理服务资质认证的依据是《网络与信息安全应急处理服务资质评估方法》（YD/T 1799-2008），信息安全风险评估服务资质认证的依据是《信息安全技术信息安全风险评估规范》（GB/T 20984-2007）与《信息安全服务资质认证实施细则》（ISCCC-SV-001）。

3 认证基本程序

- 认证申请
- 审查策划
- 初次认证
- 认证决定
- 保持认证
- 认证证书要求

4 认证申请

4.1 申请组织提出申请

4.1.1 申请组织以书面的形式提交《信息安全服务资质认证申请书》以及相关材料。资料包含但不限于：

1) 申请组织的基本情况：

- 组织简介（经营范围、规模、人员、服务设施投入状况、财务情况等）
- 组织机构框架图（含信息安全服务结构图）及主要负责人名单和联系方式（必要时）；
- 统一社会信用代码的营业执照复印件；
- 有效期内的涉及国家法规强制要求的许可文件；
- 已获认证情况，如 ISMS/ITSMS 体系认证证书复印件等；

2) 信息安全服务的相关信息：

- 信息安全服务范围和服务内容；
- 建立并实施的相关信息安全服务文件清单及文件；
- 影响信息安全服务符合性的任何外包过程的信息；
- 服务总蓝图（至少提供服务流程），以及适用时为服务运作提供支持的主要服务设施（含服务用品）；
- 涉及多个服务场所时，各场所的名称、地址及其服务内容；
- 自评报告（内审报告，管评报告）；
- 其他相关资料。

4.1.2 自评估表，包含但不限于：

- 组织根据认证依据所进行的符合性评价；

- 评价结论所需要的证据材料，证据材料必须完整清晰。

4.2 合同评审

合同评审人员在收到上述申请资料后对申请资料进行评审，综合各方面的因素后确认能否受理。确定信息安全服务资质认证人数、认证领域类别、等级和认证模式。

评审内容包括但不限于：

- 申请组织基本信息以及产品/服务相关信息的充分性，了解组织特点，确定申请组织法律地位的合法性，必要时，通过公开网站验证提供信息的真实性、有效性；
- 申请组织对应认证要求的信息是否已全部获知，并愿意遵守；
- 对于认证要求的理解上的分歧是否已得到解决，包括在相关标准或规范性文件方面是否达成一致；
- NOA 的专业能力是否满足审查实施的要求，包括认证审查人员和认证决定人员的能力是否满足要求；

当出现以下情况之一时，NOA 将拒绝或终止认证申请，流程结束。

- 申请组织未提出相应申请和/或签定认证协议，或申请组织不具备法人或法人授权代表资格，不能履行并接受本文件的有关规定的；
- NOA 的专业能力是否满足审查实施的要求，包括认证审查人员和认证决定人员的能力是否满足要求；
- 申请组织不是在中华人民共和国境内的合法经营企业；
- 根据应遵守的法规、准则、协议规定，NOA 不能受理的某项申请；

- 有证据证明申请组织在向 NOA 提供有关文件和信息时或在接受审查时，有弄虚作假行为；
- 有证据表明申请组织在最近有重大的信息安全服务问题；
- 由于申请组织方面的原因，无法获得受理申请所需要的资料或证据；
- 本文件所规定的或 NOA 视具体情况所确定的或 NOA 与申请组织或协议方达成的要求，条件尚未满足。

对于符合要求的申请组织，审查其提交材料的完善程度，和认证申请表的填写情况。对于材料不齐的，通知申请组织补充材料，再次进行审查。

4.3 受理认证

市场人员以与申请组织约定的形式通知申请组织接受服务认证申请，然后进行报价，在收到报价确认后，NOA 和申请组织签订《认证服务合同》。

5 认证方案策划

5.1 策划认证方案

NOA 通过对编制审查计划、确定审查时间与人日、选择和安排审查组、多服务场所抽样、实施审查、编制审查报告以及进行认证决定等各过程进行管理，以确保认证活动的符合性、有效性。

NOA 基于以下几个方面的考虑，为实施所要求的各个审查任务确定需要的时间：

- 服务组织的行业特点、规模和运作的复杂程度；
- 服务场所的数量；

- 服务领域类别、范围；
- 技术和法规环境；
- 服务接触方式；
- 所使用的测评方法和技术；
- 服务活动的外包情况；
- 与服务活动相关联的风险。

5.2 确定审查人日

为确保认证审查的完整有效，NOA 根据组织信息安全服务资质认证所覆盖的资质领域类别、等级、范围内的有效人数、多场所数量等情况，核算并拟定审查工作所需要的时间。特殊情况下，可以合理的增加或减少审查时间，理由应充分。任何人天数减少或增加的理由均应给予记录。

5.3 选择和安排审查组

根据申请组织的服务领域类别、等级、服务特性及活动/过程的技术特点，NOA 从注册服务审查员中选取工作经历相似、经验丰富的有能力的审查员组成审查组，在审查组的专业能力不足的情况下，可由技术专家提供服务审查的技术支持。技术专家不作为审查员实施审查，不计入审查时间。

5.4 多服务点选取方案

理论上应对申请组织的所有服务网点进行审查，但一般情况下客观条件不允许如此。对于重复设立的、功能相似的服务场所，NOA 将依据 CNAS-SC25 选取具有代表性的样本进行审查。

样本选取时应关注以下因素，以确保所选择的样本场所之间的差异性尽可能的大：

- 申请组织的特性，如业务量、服务产品数量等；
- 内部审核和管理评审或以往认证审核的结果；
- 投诉记录以及纠正措施和预防措施的其他相关方面；
- 各服务场所在规模上的显著差异；
- 不同场所在实施服务管理方面的差异；
- 任何不同的法规要求；
- 业务活动的差异及复杂程度；
- 不同地域及其分布。

5.5 选择评价技术

NOA 按照服务认证方案的要求和适用的服务评价标准/规范，对申请组织的信息安全服务进行评价。评价工作至少由一位审查员负责。

信息安全服务资质认证选择的评价技术为服务管理审核，旨在证实特定服务持续符合服务规范或认证技术规范要求的能力。

6. 初次认证

NOA 委派审查员或技术专家组成审查组，在申请组织正常生产/服务时间内，观察组织的信息安全服务活动。审查时采用查阅文件和记录、询问工作人员、观察现场、访问顾客、体验等方式，充分搜集与申请组织信息安全

服务相关的信息。审查组长为每次审查活动编写《信息安全服务资质认证评价报告》，并对报告的内容负责。报告应提供对审查的准确、简明和清晰的记录，以便为认证决定提供充分的信息。

对于审查过程中发现的任何应引起关注的或可能被判定为不符合的问题以适当的方式告知申请组织。

审查报告包括但不限于以下内容：

- 申请组织的基本情况（包括名称、地址等）；
- 审查的类型（如初审、监督或再认证）、目的、服务领域类别、等级和准则；
- 审查组成员及审查时间；
- 与有关认证要求符合性的陈述（包括发现和任何不符合）；
- 审查结论。

对于审查组发现的不符合项，申请组织应及时采取整改措施，审查组书面审核或现场验证不符合项整改措施实施的有效性。整改措施实施期限原则上不超过六十个工作日。审查组验证不符合项的整改措施后，向 NOA 提交现场审查报告。

7 认证决定

7.1 认证决定

认证决定人员应根据审查组提交的审查资料、以及受审查方提交的整改证据以及从评价过程之外获取的任何可作为认证决定依据的信息（如来自行

政监管部门、顾客、行业协会的信息等)进行综合评价,最终做出认证决定。
审查组成员不得参与对审查项目的认证决定。

在做出认证决定前应确认如下情形:

- 审查资料和审查信息完整;
- 审查组已对所有不符合事项审查、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。

有充分的客观证据证明受审查方满足下列要求的,评定该申请组织符合认证要求,向其颁发认证证书。

- 申请组织的信息安全服务资质认证符合标准要求且运行有效;
- 认证范围覆盖的产品或服务符合相关法律法规要求;
- 申请组织按照认证合同规定履行了相关义务。

受审查方不能满足上述要求的,以书面形式告知受审查方并说明其未通过认证的原因。

7.2 对认证决定的申诉

申请组织对认证决定有异议时提出申诉,应及时进行处理,处理结果形成书面通知送交申请组织。

8 保持认证

8.1 监督审查

对获证组织实施监督,每年度(不超过12个月)进行一次监督评审。

在证书有效期内，若有以下情况发生时，NOA 将考虑增加监督的频次：

- 获证组织发生严重的事故、媒体曝光或顾客投诉，经查实为获证组织责任的；
- 获证组织发生重大变更时，包括法人、组织机构、有关职能、服务资源等；
- 认证依据发生变化时；
- 相关方对获证组织进行多次投诉；
- 发生其他特殊情况时。

监督审查至少包括以下内容：

- 在监督周期内信息安全服务资质的任何变更，包括组织机构、服务管理文件修改、主要负责人更换、服务场所范围的变化情况等；
- 对以往改进项纠正措施实施效果进行验证，有无遗漏问题或再发生；
- 相关方/顾客的投诉、申诉、争议的处理，确认组织采取补救措施的有效性以及重大投诉对认证保持的影响；
- 组织开展的持续改进活动，如内部审核、管理评审等；
- 认证证书、标志的使用情况。

认证决定人员对监督审查的结果进行评定。评定合格者，批准其继续保持认证资格、使用认证证书和标志。评定不合格者，将暂停其认证资格、使用认证证书和标志，并通知获证组织在两个月内限期整改。审查员对其纠正措施进行验证，验证通过的，恢复其认证资格、使用认证证书和标志；验证不通过的，降级或撤销其认证证书，并对外公告。

8.2 再认证

信息安全服务资质认证证书的有效期为 3 年。对于需要继续使用认证证书的证书持有人，在认证证书有效期满前 3 个月，向 NOA 提出再认证申请，并提交相关资料。

再认证按照初评程序进行，当申请组织的信息安全服务资质及其运行环境无重大变更时，再认证可省去文件审查过程。

9 认证证书要求

9.1 认证证书内容

NOA 向已满足认证要求的获证组织（以下简称“证书持有人”）提供正式的认证证书，该认证证书至少包括以下基本内容：

- 认证机构的名称及其认证标志；
- 证书持有人的名称、地址及其服务提供场所的地址；
- 资质领域及等级；
- 认证所依据的服务标准、技术规范或其他规范性文件；
- 发证日期和认证有效期；
- 证书编号；
- 其他需要标注的内容。

9.2 证书的有效性

获证组织对服务认证证书及标志的使用应符合 NOAQC/NSH/S/OD-07《认证证书、标志及审核报告使用规则》。

认证证书有效期为三年。证书的有效性依靠 NOA 定期的监督获得保持。

9.3 证书变更

证书上的内容发生变化时，或获证组织发生重大调整、人员变动较大、变更服务内容等时，证书持有者应向 NOA 提出变更申请，并提交相关材料。NOA 策划并实施适宜的审查活动，做出认证决定，确定是否可以变更。

对符合要求的，批准变更。换发新证书的，新证书的编号、批准有效日期保持不变，并注明换证日期。

9.4 证书的暂停、注销和撤销

证书的使用应符合NOA有关证书管理规定的要求。当证书持有者违反认证有关规定或服务水平达不到标准要求时，NOA按照有关规定对认证证书做出相应的暂停、撤销和注销的处理，并将处理结果进行公告。获证组织可以向NOA申请暂停、注销其持有的认证证书。

证书暂停期间，获证组织如果需要恢复认证证书，应在规定的暂停期限内向NOA提出恢复申请，NOA按照相关规定进行恢复处理。否则，NOA将撤销被暂停的认证证书。

9.5 认证标志

认证标志的加施依据《认证证书、标志及审核报告使用规则》

10 相关文件

- 1) NOAQC NSH S OD-06 《多场所认证管理要求》
- 2) NOAQC NSH S OD-07 《认证证书、认证标志及审核报告使用规则》
- 3) NOAQC NSH S OD-09 《申诉和投诉处理程序》

- 4) NOAQC NSH S UD-09 《通用认证审核管理程序》
- 5) NOAQC NSH S UD-11 《授予、保持、更新、扩大、缩小、暂停和撤销认证的管理程序》
- 6) NOAQC NSH S UD-14 《认证决定管理程序》