

挪亚检测认证集团有限公司

ISO/IEC 20000信息技术服务管理体系 认证实施规则

文件编号：NOAQC/NSH/S/OD-143

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
1/1	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信息技术服务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 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ISO 20000信息技术服务管理体系（ITSMS）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 20000《信息技术服务管理》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 20000标准的要求。

4.2 认证人员应接受过ISO/IEC 20000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 20000《信息技术服务管理》

6、 认证程序

6.1 认证申请

6.1.1 认证机构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) 认证范围；
- (2) 认证工作程序；
- (3) 认证依据；
- (4) 证书有效期；
- (5) 认证收费标准。

6.1.2 认证申请组织应具备以下条件：

- (1) 法人资格证明（工商营业执照、事业单位法人证书或社会团体法人登记证书）；
- (2) 取得相关法规规定的行政许可文件（适用时）；
- (3) 从事的业务活动符合中华人民共和国相关法律、法规、信息技术服务标准和有关规范的要求；
- (4) 对信息技术服务管理体系认证范围涉及的业务活动的描述，包括利用信息技术为部或外部顾客的业务过程提供支持的说明；
- (5) 已按认证依据和相关要求建立和实施了文件化的信息技术服务管理体系；
- (6) 体系有效运行3个月以上，并且已完成内部审核和管理评审。

6.1.3 上述必要信息应使NOA能够确定：

- (1) 申请组织的行业类别和服务要求；
- (2) 申请认证的范围；
- (3) 申请组织的一般特征，包括其名称、物理场所的地址、利用信息技术为内部或外部顾客的业务过程提供支持的说明、过程和运作的重要方面以及任何相关的法律义务；
- (4) 申请组织与申请认证的领域相关的一般信息，包括其活动，人力与技术资源，以及适用时，其在一个较大实体中的职能和关系；
- (5) 申请组织采用的所有影响符合性的外包过程的信息；
- (6) 接受与信息技术服务管理体系有关的咨询的情况。

6.2 申请评审

6.2.1 认证申请组织应提交的文件和资料：

NOA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) 识别申请组织的行业类别和与之相应的信息技术服务提供过程的特性和服务要求；
- (2) 掌握国家对相应行业的信息技术服务管理体系认证的管理要求；
- (3) 申请组织及其管理体系的信息充分，可以进行审核；
- (4) 认证要求已有明确说明并形成文件，且已提供给申请组织；
- (5) 解决了认证机构与申请组织之间任何已知的理解差异；
- (6) 认证机构有能力并能够实施认证活动；

(7) 考虑了申请的认证范围、申请组织的运作场所、完成审核需要的时间和任何其他影响认证活动的因素。

6.2.2 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。

6.2.3 应完整保存认证申请的审查确认记录。

6.2.4 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。

6.3 现场审核的准备

6.3.1 确定审核组

6.3.1.1 认证审核人员必须取得信息技术服务管理体系认证注册资格。

6.3.1.2 审核组应由取得信息技术服务管理体系认证注册资格的审核员组成，其中至少有一名专职审核员。必要时可以补充技术专家以增强审核组的技术能力。

6.3.1.3 具有信息技术服务、信息技术服务法规等方面的特定知识的技术专家可以成为审核组成员。技术专家应在审核员的监督下进行工作，可就受审核方管理体系中技术充分性事宜为审核员提供建议，但技术专家不能作为审核员。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。

6.3.2 确定审核人日

认证机构应根据申请组织的规模、特性、业务复杂程度、信息技术服务管理体系涵盖的范围、认证要求和其承担的风险等因素核算并确定审核人日，以确保审核的充分性和有效性。

6.3.3 审核时间的分配

(1) 在整个审核时间中，规划时间、进行审核中与公司人员进行询问的时间和审核报告的撰写时间应该合理分配。

(2) 规划时间、进行审核中与公司人员进行询问的时间和审核报告的撰写时间：这些活动所占用的时间不应超过总审核时间的30%。

(3) 现场审核时间：不应少于总审核时间的80%。

6.3.4 审核计划

6.3.4.1 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。

6.3.4.2 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。

6.3.4.3 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。

6.3.4.4 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。

6.4 实施审核

6.4.1 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）。

6.4.2 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。

6.4.3 审核过程

6.4.3.1 初次认证审核，分为第一、二阶段实施审核，第一阶段与第二阶段现场审核间隔应不少于5个工作日且不多于60个工作日。

6.4.3.2 第一阶段审核应至少覆盖以下内容：

- (1) 审核申请组织的信息技术服务管理体系文件；
- (2) 评价申请组织的运作场所和现场的具体情况，并与申请组织的人员进行讨论，以确定第二阶段审核的准备情况；
- (3) 审查申请组织理解和实施信息技术服务管理体系标准要求的情况；
- (4) 审查申请组织是否系统而充分地识别与所提供的服务相关的法律法规和其他要求及其遵守情况；
- (5) 审查第二阶段审核所需资源的配置情况，并与申请组织商定第二阶段审核的细节；
- (6) 结合申请组织信息技术服务管理体系方针和目标，了解其审核准备状态，为策划第二阶段的审核提供重点；

(7) 评价申请组织是否策划和实施了内部审核与管理评审，以及信息技术服务管理体系的实施程度能否证明其已为第二阶段审核做好准备。

6.4.3.3 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。

6.4.3.4 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。

6.4.3.5 第二阶段审核应在具备实施认证审核的条件下在申请组织的场所进行。如果第一阶段审核提出影响实施第二阶段审核的问题，这些问题应在第二阶段审核前得到解决。第二阶段审核的目的是通过在申请组织的现场进行系统、完整地审核，评价申请组织的信息技术服务管理体系是否满足所有适用的认证依据的要求，并判断是否推荐认证注册。应重点关注申请组织是否充分识别了信息技术服务管理过程的重要性，并证实与申请组织的信息技术服务活动是相适应的。认证机构应要求申请组织证实其对信息技术服务管理过程的分析和组织运作实施了适当的控制措施，应包括：

(1) 服务交付过程（服务级别管理，服务报告，服务连续性和可用性管理，信息技术服务的预算和核算，能力管理，信息安全管理）；

(2) 关系过程（业务关系管理，供方管理）；

(3) 处理过程（事件管理，问题管理）；

(4) 控制过程（配置管理，变更管理）；

(5) 发布过程（发布管理）。

6.4.3.6 审核组应该对第一阶段和第二阶段审核中收集的所有信息和证据进行汇总分析，评价审核发现并就审核结论达成一致。

6.4.4 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。

6.5 审核报告

6.5.1 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ISO 20000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。

6.5.2 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。

6.5.3 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。

6.6 不符合项的纠正和纠正措施及其结果的验证

6.6.1 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。

6.6.2 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。

6.7 认证决定

6.7.1 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。

6.7.2 审核组成员不得参与对审核项目的认证决定。

6.7.3 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。

6.7.4 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。

6.7.5 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。

6.7.6 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，监督审核的最长时间间隔不超过12个月。在认证证书有效期内的监督审核必须覆盖信息技术服务管理体系认证范围内的所有业务活动。

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) 体系保持和变化情况；
- (2) 顾客投诉情况；
- (3) 涉及变更的范围；
- (4) 内部审核与管理评审；
- (5) 服务目录的变化情况；
- (6) 对上次审核时提出的不符合所采取纠正措施的审查；
- (7) 标志的使用和（或）任何其他对认证资格的引用；
- (8) 适当时，其它选定的范围。

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，包括调阅以前的监督审核报告，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 对于多场所认证或依据多个管理体系标准进行的认证，再认证审核的策划应确保现场审核具有足够的覆盖范围，以提供对信息技术服务管理体系认证的信任

8.5 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。

8.6 根据再认证审核的结果，以及认证周期内的体系评价结果和认证使用方的投诉。获证组织继续满足认证要求并履行认证合同义务的，作出是否更新认证的决定。

9、特殊审核

9.1 扩大认证范围

对于已授予的认证，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信息技术服务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。

9.2 对调查投诉、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) 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，NOA在指派审核组时给予更多的关注。

10、暂停或撤销认证或缩小认证范围

10.1 暂停证书

10.1.1 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) 其他应当暂停认证证书的。

10.1.2 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。

10.1.3 在暂停认证期间，获证组织的信息技术服务管理体系认证证书暂时无效。认证机构应做出具有强制实施力的安排，以确保暂停认证期间避免获证组织继续宣传信息技术服务管理体系认证资格。认证机构应使认证证书的暂停信息可公开获取，并采取其认为适当的任何其他措施。

10.1.4 如果获证组织未能在认证机构规定的时限内解决造成暂停认证的问题，认证机构应撤销其信息技术服务管理体系认证或缩小其相应的认证范围。

10.1.5 如果获证组织在认证范围的某些部分持续地或严重地不满足认证要求，NOA缩小其信息技术服务管理体系认证范围，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。

10.1.6 与获证组织就撤销信息技术服务管理体系认证时的要求做出具有强制实施力的安排，以确保获证组织接到撤销认证的通知时，立即停止使用任何引用信息技术服务管理体系认证资格的广告材料。

10.2 证书的撤销

10.2.1 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，或者必维认

证已要求其纠正但超过6个月仍未纠正的。

(8) 其他应当撤销认证证书的。

10.3 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。

10.4 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。

11、 认证证书要求

11.1 管理体系认证证书应至少包含以下信息：

- (1) 认证证书名称，即信息技术服务管理体系认证证书；
- (2) 证书编号；
- (3) 获证组织名称、注册地址、受审核地址和邮政编码；
- (4) 认证依据；
- (5) 通过认证的服务类别；
- (6) 颁证日期、换证日期以及证书有效期的起止年月日。
- (7) 认证机构的名称及其标志；
- (8) 认证机构的印章和法定代表人代表或其授权人的签字；
- (9) 认可标识及认可注册号。

11.2 如果认证所覆盖产品(或服务)的类别及其所涉及的过程和覆盖的场所较多，需在证书附件上加以注明。

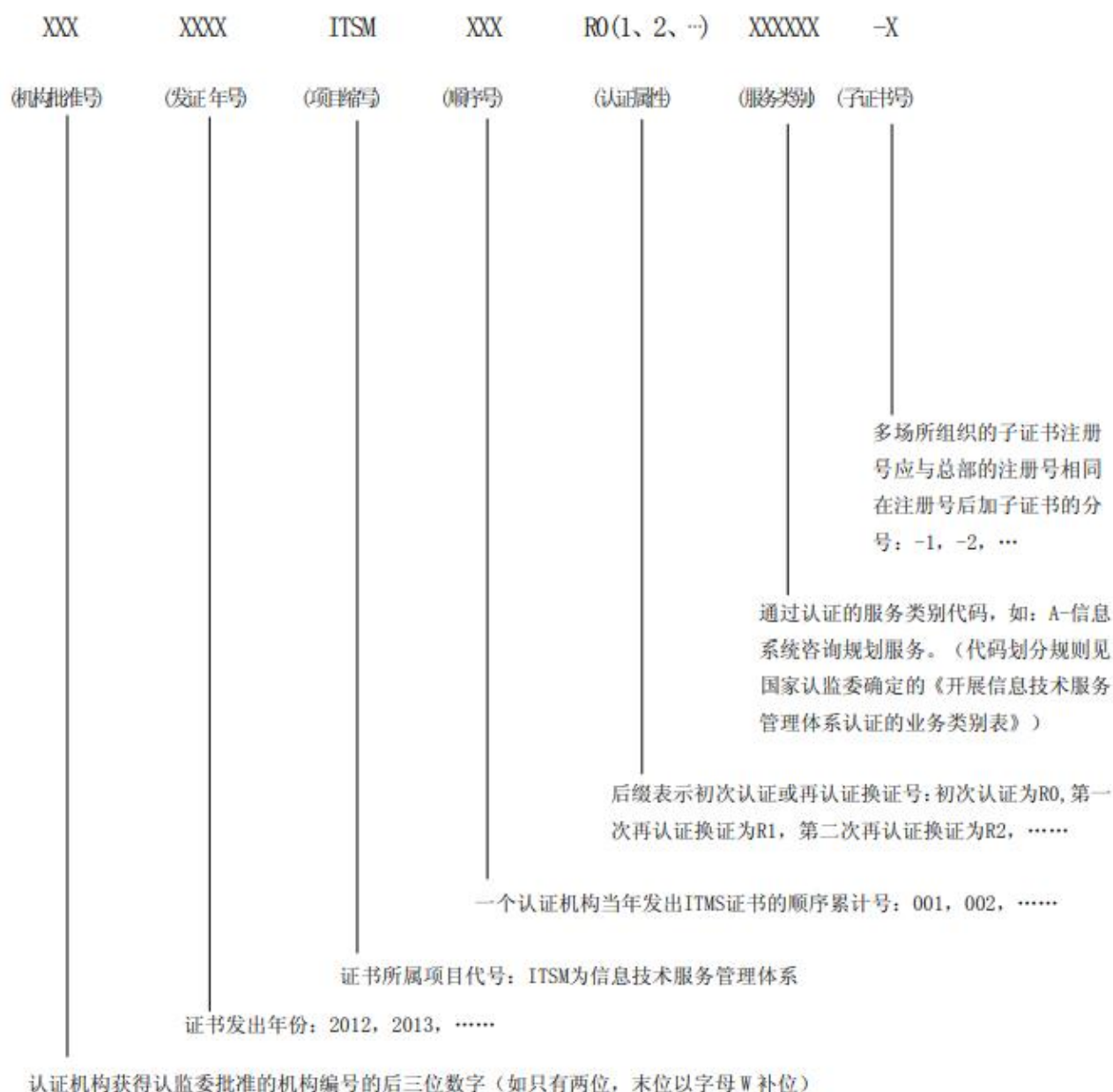
11.3 管理体系认证证书有效期最长为3年。

11.4 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。

12、 证书编号

12.1 证书编号

12.1.1 证书编号由认证机构批准号、获证年份号、信息技术服务管理体系的英文缩写、顺序号、认证属性、服务类别和子证书号构成，格式如下：



12.1.2 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, …)。

12.1.3 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。

12.1.4 再认证完成后换发证书，按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。

12.1.5 撤销证书后，原认证证书编号废止，不再它用。

12.1.6 认证证书上的认证机构名称应与相应的认证机构批准书上的名称一致。

12.2 NOA采取授权使用标识的方式来要求获证组织在认证结果的宣传和使用中采用本规则

确定的认证依据，同时注明通过认证的服务类别和认证证书编号。在认证证书被暂停期间或撤销后，应收回相应的授权。不应授权获证组织在产品上使用上述标识，或以表示产品合格的方式使用上述标识。

12.3 为确保获证组织的信息技术服务管理体系持续有效，要求获证组织建立信息通报制度，及时向认证机构通报以下信息：

- (1) 业务、地点、组织机构变化等情况的信息（及时通报）；
- (2) 顾客投诉的相关信息（每三个月通报一次）；
- (3) 组织的体系文件、服务目录信息的变化；
- (4) 有严重信息技术服务事故的信息（及时通报）；
- (5) 其他重要信息（视情况）。

12.4 对上述信息以及收集到的相关公共信息进行分析，视情况采取相应措施，包括增加监督审核频次在内的措施和暂停或撤销认证资格的措施。在发生重大客户投诉等严重情况时，认证机构需立即采取措施。

13、 与其他管理体系的结合审核

13.1 只要信息技术服务管理体系以及与其他管理体系的适当接口能够清楚地被识别，可以允许申请组织将信息技术服务管理体系文件与其他管理体系文件(例如，质量管理体系、环境管理体系，职业健康安全管理体系等)相结合。

13.2 管理体系结合审核

13.2.1 NOA可以仅提供信息技术服务管理体系认证服务，或结合信息技术服务管理体系认证提供其他管理体系认证服务。在结合审核的情形下，对诸如审核范围的界定、审核时间的确定、审核方案的策划等进行有效的管理。

13.2.2 可以把信息技术服务管理体系的审核和其他管理体系的审核相结合，但是这种结合必须以审核活动满足信息技术服务管理体系认证所有要求为前提，并且审核的质量不应由于结合审核而受到负面影响。在审核报告中，应清晰体现所有与信息技术服务管理体系有关的重要要素的描述并易于识别。

13.3 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。

14、 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。

15、 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。