ICS 03.120.20
A 00

中华人民共和国国家标准

GB/T 27021.1—2017/ISO/IEC 17021-1:2015
代替 GB/T 27021—2007

合格评定　管理体系审核认证机构要求　第1部分:要求

Conformity assessment—Requirements for bodies providing audit and certification of management systems—Part 1:Requirements

(ISO/IEC 17021-1:2015,IDT)

2017-11-01 发布　　2018-05-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

GB/T 27021《合格评定　管理体系审核认证机构要求》为系列国家标准，GB/T 27021 系列标准已经确定的部分包括：

——第 1 部分：要求；

——第 2 部分：环境管理体系审核与认证机构能力要求；

——第 3 部分：质量管理体系审核与认证机构能力要求；

——第 4 部分：大型活动可持续性管理体系审核与认证机构能力要求；

——第 5 部分：资产管理体系审核与认证机构能力要求；

——第 6 部分：业务连续性管理体系审核与认证机构能力要求；

——第 7 部分：道路交通安全管理体系审核与认证机构能力要求。

本部分为 GB/T 27021 的第 1 部分。

本部分按照 GB/T 1.1—2009 给出的规则起草。

本部分代替 GB/T 27021—2007《合格评定　管理体系审核认证机构的要求》，与 GB/T 27021—2007 相比，除编辑性修改外主要技术变化如下：

——修改了术语“公正性”定义内容（见 3.2，2007 年版的 3.2）；

——修改了术语“管理体系咨询”定义内容（见 3.3，2007 年版的 3.3）；

——增加了“认证审核”“客户”“审核员”“能力”“管理体系认证审核时间”等术语（见 3.4～3.17）；

——增加了 4.8“基于风险的方法”（见 4.8）；

——修改了 5.2“公正性的管理”（见 5.2，2007 年版的 5.2）；

——修改了第 6 章“结构要求”（见第 6 章，2007 年版的第 6 章）；

——删除了“维护公正性的委员会”（见 2007 年版的 6.2）；

——修改了第 7 章“资源要求”（见第 7 章，2007 年版的第 7 章）；

——增加了其他考虑（见 7.1.4）；

——修改了第 8 章“信息要求”（见第 8 章，2007 年版的第 8 章）；

——删除了“获证客户目录”（见 2007 年版的 8.3）；

——修改了第 9 章“过程要求”（见第 9 章，2007 年版的第 9 章）；

——增加了规范性附录 A 提供对承担各类认证职能所要求的知识和技能（见附录 A）；

——增加了资料性附录 B 提供对人员能力评价可能采用的方法（见附录 B）；

——增加了资料性附录 C 提供能力确定和保持过程的示例（见附录 C）；

——增加了资料性附录 D 提供期望的个人行为的示例（见附录 D）；

——增加了资料性附录 E 提供审核和认证过程的示例（见附录 E）。

本部分使用翻译法等同采用 ISO/IEC 17021-1:2015《合格评定　管理体系审核认证机构要求　第 1 部分：要求》（英文版）。

与本部分中规范性引用的国际文件有一致性对应关系的我国文件如下：

——GB/T 19000—2016　质量管理体系　基础和术语（ISO 9000:2015，IDT）

——GB/T 27000—2006　合格评定　词汇和通用原则（ISO/IEC 17000:2004，IDT）

为了便于使用，本部分对 ISO/IEC 17021-1:2015 做了下列编辑性修改：

——用“获证客户”替代 4.1.2b）中“管理体系获得认证的组织”（the organizations whose management systems are certified）；

——用“获证客户”替代 5.2.3 注 2 中“管理体系获得认证的组织”(organizations whose management systems are certified)。

本部分由全国认证认可标准化技术委员会(SAC/TC 261)提出并归口。

本部分起草单位:中国合格评定国家认可中心、国家认证认可监督管理委员会、中国认证认可协会、中国质量认证中心、方圆标志认证集团有限公司、广州赛宝认证中心服务有限公司、北京赛西认证有限责任公司、中国船级社质量认证公司、上海质量体系审核中心、华夏认证中心有限公司。

本部分主要起草人:费杨、任青钺、郝静、林峰、汪修慈、穆瑾、王瑜、黄俊梅、谭平、刘险锋、张瑜、王雪峰。

本部分所代替标准的历次版本发布情况为:

——GB/T 27021—2007。

引　言

管理体系认证(如对组织的环境管理体系、质量管理体系或信息安全管理体系的认证)是一种保证方法,用以确保组织已实施了与其方针及相关管理体系标准的要求一致的、用以管理其活动、产品和服务相关方面的体系。

本部分规定了对管理体系审核和认证机构的要求。它对从事质量、环境及其他管理体系审核与认证的机构提出了通用要求。本部分将这类机构称为认证机构。贯彻这些要求旨在确保认证机构以有能力、一致和公正的方式实施管理体系认证,以促进国际和国内承认这些机构并接受它们的认证。本部分为促进对管理体系认证的承认提供了基础,这种承认有利于国际贸易。

管理体系认证是独立地证明组织的管理体系:

a) 符合规定要求;

b) 能够自始至终实现其声明的方针和目标;

c) 得到有效实施。

因此,诸如管理体系认证的合格评定活动为组织、组织的顾客及利益相关方提供了价值。

第4章阐述了可信的认证所依据的原则。这些原则有助于用户理解认证的本质属性,并为第5章～第10章做了必要的铺垫。这些原则构成了本部分要求的基础,但其本身并不是可供评审的要求。第10章为认证机构通过建立管理体系来保障和证实其始终满足本部分要求提供了两种可供选择的途径。

认证活动是构成从申请评审到认证终止的整个认证过程的活动。附录E展现了许多认证活动能够相互作用的方式。

认证活动包括对组织的管理体系的审核。认证机构通常以认证文件或证书的形式证明组织的管理体系符合特定的管理体系标准或其他规范性要求。

本部分适用于各种类型管理体系的审核与认证。为实现利益相关方的期望,可能需要对其中一些要求,特别是那些关于审核员能力的要求补充附加准则。

在本部分中:

——"应"表示要求;

——"宜"表示建议;

——"可以"表示允许;

——"能够"表示一种可能性或能力。

ISO/IEC 导则第2部分中对这些助动词做了更详细的说明。

合格评定　管理体系审核认证机构要求
第1部分:要求

1　范围

GB/T 27021的本部分包含了所有类型管理体系审核与认证机构的能力、一致性和公正性的原则与要求。

按照本部分运作的认证机构不必提供所有类型的管理体系认证。

管理体系认证,是一种第三方合格评定活动(见ISO/IEC 17000:2004的5.5),因此实施这种活动的机构是第三方合格评定机构。

注1:管理体系的示例:质量管理体系、环境管理体系和信息安全管理体系。

注2:本部分中,管理体系认证称为"认证",实施认证的第三方合格评定机构称为"认证机构"。

注3:认证机构可以是非政府的或政府的,具有或不具有法定权力。

注4:本部分可作为认可、同行评审或其他审核过程的准则文件。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

ISO 9000　质量管理体系　基础和术语(Quality management systems—Fundamentals and vocabulary)

ISO/IEC 17000　合格评定　词汇和通用原则(Conformity assessment—Vocabulary and general principles)

3　术语和定义

ISO 9000和ISO/IEC 17000界定的以及下列术语和定义适用于本文件。

3.1

获证客户　certified client

管理体系已获认证的组织。

3.2

公正性　impartiality

客观性的存在。

注1:客观性意味着利益冲突不存在或已解决,不会对认证机构的后续活动产生不利影响。

注2:其他可用于表示公正性的要素的术语有:独立、无利益冲突、没有成见、没有偏见、中立、公平、思想开明、不偏不倚、不受他人影响、平衡。

3.3

管理体系咨询　management system consultancy

参与建立、实施或保持管理体系。

示例1:筹划或编制手册或程序。

示例2:对管理体系的建立和实施提供具体的建议、指导或解决方案。

注1：如果与管理体系和审核有关的培训课程仅限于提供通用信息，那么组织培训并作为培训者参与培训不被视为咨询，即培训者不宜针对特定的客户提出解决方案。

注2：为过程或体系的改进提供通用信息，而不是针对特定客户的解决方案，不被视为咨询。此类通用信息可以包括：

——解释认证准则的含义和意图；

——识别改进机会；

——解释相关的理论、方法学、技巧或工具；

——分享关于相关良好实践的非保密信息；

——所审核的管理体系未覆盖的其他管理方面。

3.4

认证审核　certification audit

由独立于客户和依赖认证的各方的审核组织实施的、对客户的管理体系进行以认证为目的的审核。

注1：在下面的定义中，第三方认证审核简称为“审核”。

注2：认证审核包括初次审核、监督审核和再认证审核，还可以包括特殊审核。

注3：认证审核通常由依据管理体系标准要求提供符合性认证的认证机构的审核组实施。

注4：两个或两个以上审核组织合作审核同一个客户，称作联合审核。

注5：一个客户同时按照两个或两个以上管理体系标准的要求接受审核，称作结合审核。

注6：一个客户已将两个或两个以上管理体系标准要求的应用整合在一　单一的管理体系中，并按照一个以上标准接受审核，称作一体化审核。

3.5

客户　client

其管理体系为认证目的接受审核的组织。

3.6

审核员　auditor

实施审核的人。

3.7

能力　competence

能够应用知识和技能实现预期结果的本领。

3.8

向导　guide

客户指派的协助审核组的人。

3.9

观察员　observer

与审核组同行，但不实施审核的人。

3.10

技术领域　technical area

以与特定类型管理体系及其预期结果有关的过程的共性为特征的领域。

注：参见7.1.2注。

3.11

不符合　nonconformity

未满足要求。

3.12

严重不符合　major nonconformity

影响管理体系实现预期结果的能力的**不符合**(3.11)。

注：严重不符合可能是下列情况：

——对过程控制是否有效或者产品或服务能否满足规定要求存在严重的怀疑；

——多项轻微不符合都与同一要求或问题有关，可能表明存在系统性失效，从而构成一项严重不符合。

3.13

轻微不符合　minor nonconformity

不影响管理体系实现预期结果的能力的**不符合**(3.11)。

3.14

技术专家　technical expert

向审核组提供特定知识或专业意见的人。

注：特定知识或专业意见与所审核的组织、过程或活动有关。

3.15

认证方案　certification scheme

应用相同的规定要求、特定规则与程序的，与管理体系有关的合格评定制度。

3.16

审核时间　audit time

策划并完成一次完整有效的客户组织管理体系审核所需要的时间。

3.17

管理体系认证审核时间　duration of management system certification audits

审核时间(3.16)的一部分，包括从首次会议到末次会议之间实施审核活动的所有时间。

注：审核活动通常包括：

——举行首次会议；

——审核实施中的文件评审；

——审核中的沟通；

——向导和观察员的作用和责任；

——信息的收集和验证；

——形成审核发现；

——准备审核结论；

——举行末次会议。

4　原则

4.1　总则

4.1.1　本章所述原则是本部分中后续的特定绩效要求和说明性要求的基础。本部分未就所有可能发生的情况给出特定要求。在出现未预料到的情况时，宜应用这些原则作为决策的指南。这些原则不是要求。

4.1.2　认证的总体目标是使所有相关方相信管理体系满足规定要求。认证的价值取决于第三方通过公正、有能力的评定所建立的公信力的程度。认证的利益相关方包括(但不限于)：

a)　认证机构的客户；

b)　获证客户的顾客；

c)　政府部门；

d)　非政府组织；

e)　消费者和其他公众。

4.1.3　建立信任的原则包括：

——公正性；

——能力；
——责任；
——公开性；
——保密性；
——对投诉的回应；
——基于风险的方法。

注：本部分在第4章给出了认证的原则，ISO 19011:2011第4章给出了与审核有关的原则。

4.2 公正性

4.2.1 公正，并被认为公正，是认证机构提供可建立信任的认证的必要条件。重要的是所有内部和外部人员都意识到公正性的必要性。

4.2.2 客户支付的认证费用是认证机构的收入来源，也是对公正性的潜在威胁，这一点得到公认。

4.2.3 认证机构根据其所获得的符合(或不符合)的客观证据做出决定，且不受其他利益或其他各方的影响，对于获得和保持信任是必不可少的。

4.2.4 对公正性的威胁可能包括，但不限于：

a) 自身利益：此类威胁源于个人或机构依其自身利益行事。在认证中，财务方面的自身利益是一种对公正性的威胁；
b) 自我评审：此类威胁源于个人或机构评审自己所做的工作。认证机构对由其进行管理体系咨询的客户实施管理体系审核属于此类威胁；
c) 熟识(或信任)：此类威胁源于个人或机构对另外一人过于熟悉或信赖，而不去寻找审核证据；
d) 胁迫：此类威胁源于个人或机构察觉受到公然或暗中的强迫，如威胁用他人取而代之或向主管告发。

4.3 能力

4.3.1 认证活动涉及的所有职能的认证机构人员的能力是认证提供信任的必要条件。

4.3.2 能力也需要由认证机构的管理体系来支撑。

4.3.3 认证机构管理的一个关键问题是具有一个得到实施的过程，来为参与审核和其他认证活动的人员建立能力准则，并按照准则实施评价。

4.4 责任

4.4.1 始终一致地达到实施管理体系标准的预期结果和符合认证要求的责任，在于获证客户而不是认证机构。

4.4.2 认证机构有责任对足够的客观证据进行评价，并在此基础上做出认证决定。根据审核结论，如果符合性的证据充分，认证机构做出授予认证的决定；如果符合性的证据不充分，则不授予认证。

注：任何审核都是基于对组织管理体系的抽样，因此并不保证管理体系100%符合要求。

4.5 公开性

4.5.1 为获得对认证的诚信性与可信性的信任，认证机构需要提供获取有关审核过程、认证过程和所有组织认证状态(即认证的授予、保持，认证范围的扩大或缩小，认证的更新、暂停、恢复或者撤销)的适当、及时信息的公开渠道，或公布这些信息。公开性是获得或公布适当信息的一项原则。

4.5.2 为获得或保持对认证的信任，认证机构宜向特定利益相关方提供获取特定审核(如为回应投诉而做的审核)结论的非保密信息的适当渠道，或公布这些信息。

4.6 保密性

为了享有获取充分评价管理体系符合性所需信息的特权，认证机构不透露任何保密信息是至关重要的。

4.7 对投诉的回应

依赖认证的各方期望投诉得到调查。认证机构应当使依赖认证的各方相信，在投诉经查明有效时，认证机构将对这些投诉进行适当的处理，并为解决这些投诉做出适当的努力。当投诉表明出现错误、疏忽或不合理行为时，对投诉做出有效回应是保护认证机构及其客户和其他认证使用方的重要手段。对投诉进行适当处理将维护对认证活动的信任。

注：为了向认证的所有用户证明认证的诚信性与可信性，需要在公开性和保密性（包括对投诉的回应）等原则之间取得适当的平衡。

4.8 基于风险的方法

认证机构需要考虑与提供有能力的、一致的和公正的认证相关的风险。风险可能与下列方面有关（包括但不限于）：

——审核目的；
——审核过程中的抽样；
——真正的和被感知到的公正性；
——法律法规问题和责任问题；
——所审核的客户组织及其运行环境；
——审核对客户及其活动的影响；
——审核组的健康和安全；
——利益相关方的认知；
——获证客户做出的误导性声明；
——标志的使用。

5 通用要求

5.1 法律与合同事宜

5.1.1 法律责任

认证机构应为一个法律实体，或一个法律实体内有明确界定的一部分，以便认证机构能够对其所有认证活动承担法律责任。政府的认证机构因其政府地位而被视为法律实体。

5.1.2 认证协议

认证机构与每个客户之间应有在法律上具有强制实施力并符合本部分相关要求的提供认证服务的协议。此外，如果认证机构有多个办公场所或客户有多个场所，则应确保授予认证的认证机构与客户之间具有覆盖认证范围内所有场所的在法律上具有强制实施力的协议。

注：一项协议可以由多个相互引用或以其他方式相互联系的协议来实现。

5.1.3 认证决定的责任

认证机构应对与认证有关的决定（包括授予、拒绝、保持认证，扩大或缩小认证范围，更新、暂停、在

暂停后恢复、撤销认证)负责,并应保持做出上述决定的权力。

5.2 公正性的管理

5.2.1 合格评定活动应以公正的方式实施。认证机构应对其合格评定活动的公正性负责,不应允许商业、财务或其他压力损害公正性。

5.2.2 认证机构最高管理层应对管理体系认证活动的公正性做出承诺。认证机构应具有政策,表明其理解公正性在实施管理体系认证活动中的重要性,对利益冲突加以管理,并确保其管理体系认证活动的客观性。

5.2.3 认证机构应有过程以持续地识别、分析、评估、处置、监视与认证活动引起的利益冲突相关的风险,并将其形成文件,包括认证机构的各种关系引起的冲突。当存在对公正性的威胁时,认证机构应将其如何消除或最大限度减小此类威胁形成文件,并予以证实,并将任何残留风险形成文件。所作的证实应包括所有已识别的潜在威胁,无论其产生于认证机构内部还是其他个人、机构或组织的活动。当某种关系对认证机构的公正性构成不可接受的威胁时(如认证机构的全资子公司向其申请认证),认证机构不应提供认证。

最高管理层应审查任何残留风险并决定其是否处于可接受的水平。

风险评估过程应包括识别适宜的利益相关方,并就影响公正性(包括公开性和公众认知)的事宜向其征询意见。向适宜的利益相关方征询意见应以均衡的、任一方不处于支配地位的方式进行。

注 1:认证机构公正性的威胁可能源自其所有权、法人治理结构、管理层、人员、共享资源、财务、合同、培训、营销以及给介绍新客户的人销售佣金或其他好处等。

注 2:利益相关方可能包括:认证机构的人员和客户,获证客户的顾客,行业协会代表,政府监管机构或其他政府部门的代表,或非政府组织(包括消费者组织)的代表。

注 3:满足本条征询意见要求的一种方式是使用一个由这些利益相关方组成的委员会。

5.2.4 认证机构不应对另一认证机构的质量管理体系进行认证。

5.2.5 认证机构及同一法律实体的任何其他部分以及处于认证机构的组织控制[见 9.5.1.2b)]之下的任何实体不应提供或推荐管理体系咨询,也不应为管理体系咨询提供报价。本条款同样适用于政府中被识别为认证机构的那一部分。

注:本条不排除认证机构与其客户之间交流信息的可能性(例如解释发现或澄清要求)。

5.2.6 认证机构及同一法律实体的任何其他部分向认证机构的获证客户提供内部审核是对公正性的严重威胁。因此,认证机构及同一法律实体的任何其他部分以及处于认证机构的组织控制[见 9.5.1.2b)]之下的任何实体不应向获证客户提供内部审核。一种公认的减轻这种威胁的方式是,如果认证机构对某个管理体系提供了内部审核,则不应在内部审核结束后至少两年内对该管理体系进行认证。

注:参见 5.2.3 注 1。

5.2.7 如果客户接受了与认证机构有关系的机构的管理体系咨询,这是对公正性的严重威胁。一种公认的减轻这种威胁的方式是,认证机构在咨询结束后至少两年内不应对该管理体系进行认证。

注:参见 5.2.3 注 1。

5.2.8 认证机构不应将审核外包给管理体系咨询机构,因为这一做法将对认证机构的公正性构成不可接受的威胁(见 7.5)。本条款不适用于 7.3 所述的作为签约审核员的个人。

5.2.9 认证机构活动的营销或报价不应与管理体系咨询机构的活动有联系。如果任何咨询机构的链接或声明宣称或暗示选择某认证机构将使认证更为简单、容易、迅速或廉价,则该认证机构应采取措施纠正这种不当表述。认证机构不应宣称或暗示选择某咨询机构将使认证更为简单、容易、迅速或廉价。

5.2.10 为确保没有利益冲突,参与了对客户管理体系咨询的人员(包括管理人员)不应被认证机构用于针对该客户的审核或其他认证活动。一种公认的减轻该威胁的方式是在咨询结束后至少两年内不应使用该人员。

5.2.11 认证机构应采取措施,以应对其他人员、机构或组织的行为对其公正性产生的威胁。

5.2.12 认证机构所有可以影响认证活动的人员(内部或外部的)或委员会应公正行事,且不应允许商业、财务或其他方面的压力损害公正性。

5.2.13 认证机构应要求内部和外部的人员告知他们所了解的任何可以使其或认证机构陷入利益冲突的情况。认证机构应记录并利用这些信息识别他们或其所在单位的活动对公正性产生的威胁,且应在他们能够证明没有利益冲突之后再使用这些内部或外部人员。

5.3 责任和财力

5.3.1 认证机构应能证明已对认证活动引发的风险进行了评估,并对各个活动领域和运作地域的业务引发的责任作了充分的安排(如保险或储备金)。

5.3.2 认证机构应评估其财务状况和收入来源,并证明其公正性始终没有受到商业、财务和其他方面压力的损害。

6 结构要求

6.1 组织结构和最高管理层

6.1.1 认证机构应将其组织结构、管理层和其他认证人员及各委员会的职责、责任和权力形成文件。当认证机构是一个法律实体内有明确界定的一部分时,该文件应说明认证机构与该法律实体间的权力关系以及与同一法律实体内其他部分的关系。

6.1.2 认证机构的结构和管理方式应维护认证活动的公正性。

6.1.3 认证机构应确定对下列各项具有全部权力和责任的最高管理层(委员会、小组或个人):

a) 与认证机构运作有关的政策的制定以及过程和程序的建立;
b) 政策、过程和程序实施的监督;
c) 确保公正性;
d) 认证机构财务的监督;
e) 管理体系认证服务和认证方案的开发;
f) 审核与认证的实施和对投诉的回应;
g) 认证决定;
h) 在需要时,授权委员会或个人代表最高管理层开展规定的活动;
i) 合同安排;
j) 为认证活动提供充分的资源。

6.1.4 认证机构应有关于任何参与认证活动的委员会的任命、权限和运行的正式规则。

6.2 运行控制

6.2.1 认证机构应有过程对其分支办公室、合伙人、代理、特许经营者等交付的认证活动进行有效控制,不论其法律地位、关系或地理位置如何。认证机构应考虑这些活动给认证机构的能力、一致性和公正性带来的风险。

6.2.2 认证机构应考虑与所从事活动相适宜的控制水平和方法,包括其过程、运作的技术领域、人员的能力、管理控制线、汇报以及远程访问操作系统(包括记录)。

7 资源要求

7.1 人员能力

7.1.1 总体考虑

认证机构应有过程来确保其人员对其运作涉及的管理体系类型(例如质量管理体系、环境管理体

系、信息安全管理体系)和地域有适宜的相关知识与技能。

7.1.2 能力准则的确定

认证机构应有过程,以确定参与管理和实施审核及其他认证活动的人员的能力准则。应根据每类管理体系标准的要求,针对每个技术领域和认证过程中的每项职能确定能力准则。该过程的输出应是形成文件的所要求知识和技能的准则,这些知识和技能是有效地实施审核与认证任务以实现预期结果所必需的。附录A明确了认证机构应为特定职能确定的知识和技能。如果已经为特定的标准或认证方案建立了附加的特定能力准则(例如ISO/IEC TS 17021-2、ISO/IEC TS 17021-3或ISO/TS 22003),这些附加的特定能力准则应得到应用。

注:取决于不同的管理体系标准,术语"技术领域"的应用方式可以有所不同。对于任何管理体系,该术语都与管理体系标准范围内的产品、过程和服务有关。技术领域可由特定认证方案(例如ISO/TS 22003)定义;或者可以由认证机构定义。该术语用于涵盖不同管理体系领域传统使用的一些其他术语,例如"范围""类别""行业"等。

7.1.3 评价过程

认证机构应有形成文件的过程,以应用所确定的能力准则,对所有参与管理和实施审核及其他认证活动的人员进行初始能力评价,并持续监视其能力和绩效。认证机构应证实其评价方法是有效的。这些过程的输出应是识别出有能力的人员,即被证实具有审核与认证过程不同职能所需的能力水平的人员。在认证机构内,人员为其活动绩效承担责任前,能力应得到证实。

注1:附录B介绍了一些可用于能力评价的评价方法。

注2:附录C提供了一个能力确定和保持流程的示例。

7.1.4 其他考虑

认证机构应有获取必要的专业知识与技能的途径,以在其运作涉及的所有技术领域、管理体系类型和地域等方面获得与认证活动直接相关的建议。这些建议可由外部人员或认证机构人员提供。

7.2 参与认证活动的人员

7.2.1 认证机构应有足够的、有能力的人员以对其各种类型与范围的审核方案以及其他认证工作进行管理和支持。

7.2.2 认证机构应聘用或有途径获得足够数量的审核员(包括审核组长)和技术专家,以覆盖其所有活动并满足审核工作量的需要。

7.2.3 认证机构应使所有相关人员清楚自己的任务、责任和权力。

7.2.4 认证机构应有过程来选择、培训、正式任用审核员,选择并培养认证活动使用的技术专家。审核员的初始能力评价应包括在审核中应用所需知识与技能的本领的证实。在审核中应用所需知识与技能的本领应由有能力的评价者在对审核员审核的见证中确定。

注:在上述的选择和培训过程中可以考虑所期望的个人行为。所期望的个人行为是影响一个人实施特定职能的能力的特性。对个人行为的了解能使认证机构能够发挥人员的强项并尽可能减小其弱点的影响。附录D介绍了所期望的个人行为,它们对参与认证活动的人员是重要的。

7.2.5 认证机构应有实现和证实有效审核的过程。该过程应确保所使用的审核员和审核组长具备通用的审核知识与技能以及特定技术领域审核所需的知识与技能。

7.2.6 认证机构应确保审核员(需要时,包括技术专家)充分了解其审核过程、认证要求和其他相关要求。认证机构应使审核员和技术专家有途径获取指导审核和提供认证活动所有相关信息的现行有效的文件化程序。

7.2.7 认证机构应识别培训需求,并向审核员、技术专家和其他参与认证活动的人员提供或使其有机会参加特定的培训,以确保他们胜任所从事的工作。

7.2.8 做出授予、拒绝、保持、更新、暂停、恢复或撤销认证或者扩大或缩小认证范围等决定的小组或个人应理解适用的标准和认证要求，并经证实有能力评价审核过程的结果，包括审核组的相关推荐意见。

7.2.9 认证机构应确保所有参与审核和其他认证活动的人员均有令人满意的绩效。认证机构应有形成文件的过程，以根据这些人员的使用频率及其活动的风险水平来监视他们的能力和绩效。认证机构尤其应根据人员的绩效来复核并记录他们的能力，以识别培训需求。

7.2.10 认证机构应在监视每个审核员时考虑该审核员被认为有能力的每个管理体系类型。形成文件的审核员监视过程应把现场评价、审核报告复核及客户或市场反馈相结合。认证机构应在文件要求中详细说明该程序。在设计监视方式时，应使正常认证过程所受干扰最小(尤其是从客户角度来看)。

7.2.11 认证机构应定期对每位审核员的绩效进行现场评价。现场评价的频率应取决于根据所有可获得的监视信息确定的现场见证需求。

7.3 外部审核员和外部技术专家的使用

认证机构应要求外部审核员和外部技术专家通过书面协议承诺其遵守认证机构适用的政策并按照认证机构的规定实施相关过程。该协议应含有关于保密及公正性的条款，并要求外部审核员和外部技术专家向认证机构说明现在或以前与可能派其审核的组织的关系。

注：使用个人或另一组织的单个雇员作为外部审核员或技术专家不构成外包。

7.4 人员记录

认证机构应保持人员(包括认证活动实施人员、管理人员和行政人员)的最新记录，包括相关的资格、培训、经历、隶属关系、专业状况和能力的记录。

7.5 外包

7.5.1 认证机构应说明可以进行外包(即向另一个组织分包，由其代表认证机构提供部分认证服务)的条件。认证机构应与每个承担外包服务的机构就相关安排(包括保密和利益冲突)签订在法律上具有强制实施力的协议。

7.5.2 授予、拒绝、保持认证，扩大或缩小认证范围，更新、暂停、恢复或者撤销认证的决定不应外包。

7.5.3 认证机构应：

a) 对外包给另一机构的所有活动负责；

b) 确保外包服务承担机构及其使用的人员符合认证机构的要求和本部分的适用要求，包括能力、公正性和保密；

c) 确保外包服务承担机构及其使用的人员与拟审核的组织没有可能损害公正性的关系(无论是直接的还是通过任何其他雇主发生的关系)。

7.5.4 认证机构应有过程，以对认证活动的所有外包服务承担机构进行批准和监视，且应确保其参与认证活动的所有人员的能力记录得到保持。

注 1：对于 7.5.1～7.5.4，当认证机构聘用个人或其他组织的雇员来补充资源或专业能力时，如果认证机构与个人签约，以使其在认证机构的管理体系下运作(见 7.3)，不构成外包。

注 2：对于 7.5.1～7.5.4，“外包”与“分包”视为同义词。

8 信息要求

8.1 公开信息

8.1.1 认证机构应在其运营的所有地域中保持(通过出版物、电子介质或其他方式)并主动公布下列方面的信息：

a) 审核过程；
b) 授予、拒绝、保持、更新、暂停、恢复或撤销认证或者扩大或缩小认证范围的过程；
c) 其运作涉及的管理体系类型和认证方案；
d) 认证机构的名称和认证标志或徽标的使用；
e) 对索要信息的请求、投诉和申诉的处理过程；
f) 公正性政策。

8.1.2 认证机构应在有请求时提供下列方面的信息：
a) 其运作涉及的地域；
b) 特定认证的状态；
c) 特定获证客户的名称、相关的规范性文件、认证范围和地理位置(国家和城市)。

注1：在特殊情况下，可以根据客户的请求(如出于安全原因)对某些信息的公开程度做出限制。

注2：认证机构也可以通过任何方式主动公开8.1.2中的信息，例如在其网站上。

8.1.3 认证机构向客户或市场提供的信息(包括广告)应准确且不使人产生误解。

8.2 认证文件

8.2.1 认证机构应以其选择的任何方式向获证客户提供认证文件。

8.2.2 认证文件应标明：
a) 每个获证客户的名称和地理位置(或多场所认证范围内总部和所有场所的地理位置)；
b) 授予认证、扩大或缩小认证范围、更新认证的生效日期，生效日期不应早于相关认证决定的日期；

注：当证书失效一段时间时，认证机构在满足下列条件时，可以在证书上保留原始的认证日期：
——清晰标示了当前认证周期的开始时间和截止时间；
——把上一认证周期截止时间连同再认证审核的时间一起标示。

c) 认证有效期或与认证周期一致的应进行再认证的日期；
d) 唯一的识别代码；
e) 审核获证客户时所用的管理体系标准和(或)其他规范性文件，包括发布状态的标示(例如修订时间或编号)；
f) 与活动、产品和服务类型等相关的认证范围，适用时，包括每个场所相应的认证范围，且没有误导或歧义；
g) 认证机构的名称、地址和认证标志；可以使用其他标识(如认可标识、客户的徽标)，但不能产生误导或含混不清；
h) 认证用标准和(或)其他规范性文件所要求的任何其他信息；
i) 在颁发经过修改的认证文件时，区分新文件与任何已作废文件的方法。

8.3 认证资格的引用和标志的使用

8.3.1 认证机构对其授权获证客户使用的任何管理体系认证标志应有管理规则。这些规则应确保可以从标志追溯到认证机构。标志或所附文字不应使人对认证对象和授予认证的认证机构产生歧义。标志不应用于产品或产品包装之上，或以任何其他可解释为表示产品符合性的方式使用。

注：ISO/IEC 17030对使用第三方标志提供了补充信息。

8.3.2 认证机构不应允许其标志被获证客户用于实验室检测、校准或检验的报告或证书。

8.3.3 认证机构应对在产品包装上或附带信息中声明获证客户的管理体系通过认证有管理规则。产品包装的判别标准是其可从产品上移除且不会导致产品分解、碎裂或损坏。附带信息的判别标准是其可分开获得或易于分离。型号标签或铭牌被视为产品的一部分。声明决不应暗示产品、过程或服务以

这种方式得到了认证。声明应包含对下列的引用：

——获证客户的标识(例如品牌或名称)；

——管理体系的类型(例如质量、环境)和适用标准；

——颁发证书的认证机构。

8.3.4 认证机构应通过在法律上具有强制实施力的安排，要求获证客户：

a) 在传播媒介(如互联网、宣传册或广告)或其他文件中引用认证状态时，应符合认证机构的要求；

b) 不做出或不允许有关于其认证资格的误导性说明；

c) 不以或不允许以误导性方式使用认证文件或其任何部分；

d) 在其认证被撤销时，按照认证机构的指令立即停止使用所有引用认证资格的广告材料(见9.6.5)；

e) 在认证范围被缩小时，修改所有的广告材料；

f) 不允许在引用其管理体系认证资格时，暗示认证机构对产品(包括服务)或过程进行了认证；

g) 不得暗示认证适用于认证范围以外的活动和场所；

h) 在使用认证资格时，不得使认证机构和(或)认证制度声誉受损，失去公众信任。

8.3.5 认证机构应正确地控制其所有权，并采取措施处理认证状态的错误引用或认证文件、标志或审核报告的误导性使用。

注：此类措施可以包括要求纠正或采取纠正措施、暂停认证、撤销认证、公告违规行为以及必要的法律措施。

8.4 保密

8.4.1 认证机构应通过在法律上具有强制实施力的协议，对在其各个层次(包括代表其活动的委员会、外部机构或个人)从事认证活动时获得或产生的所有信息的管理负责。

8.4.2 认证机构应将其拟对公众公开的信息提前告知客户。所有其他信息均应视为保密信息，客户自己公开的信息除外。

8.4.3 除本部分有要求外，关于特定获证客户或个人的信息，未经其书面同意，不应向第三方披露。

8.4.4 当法律要求认证机构或者合同安排(例如与认可机构签订的)授权认证机构提供保密信息时，除法律禁止外，认证机构应将拟提供的信息提前通知有关客户或个人。

8.4.5 从其他来源(如投诉人、监管机构)获得的关于客户的信息应根据认证机构的政策按保密信息处理。

8.4.6 认证机构的人员，包括代表认证机构工作的任何委员会成员、合同方、外部机构人员或个人，除法律有要求外，应对从事认证机构的活动时获得或产生的所有信息予以保密。

8.4.7 认证机构应有确保保密信息得到安全处理的过程以及适用的设备和设施。

8.5 认证机构与其客户间的信息交换

8.5.1 认证过程和要求的信息

认证机构应向客户提供并为其更新以下信息：

a) 对认证活动整个过程的详细说明，包括申请、初次审核、监督审核和授予、拒绝、保持认证、扩大或缩小认证范围、更新、暂停或恢复或者撤销认证的过程；

b) 认证依据的规范性要求；

c) 申请、初次认证和保持认证资格所需费用的信息；

d) 认证机构对客户的要求：

1) 遵守认证要求；

2) 为实施审核做出所有必要的安排，包括在初次认证、监督、再认证和解决投诉时，为检查文

件和接触所有过程与区域、记录及人员提供条件；

3) 适用时，为接纳到场的观察员(如认可评审员或实习审核员)提供条件；

e) 对获证客户根据 8.3 的要求在各类沟通中引用认证资格时的权利和责任(包括要求)予以说明的文件；

f) 投诉和申诉处理过程的信息。

8.5.2 认证机构的变更通知

认证机构应以适当方式将其认证要求的任何变更通知获证客户。认证机构应验证每个获证客户符合新的要求。

8.5.3 获证客户的变更通知

认证机构应做出在法律上具有强制实施力的安排，以确保获证客户即时将可能影响管理体系持续满足认证标准要求的能力的事宜通知认证机构，包括(但不限于)与下列方面有关的变更：

a) 法律地位、经营状况、组织状态或所有权；

b) 组织和管理层(如关键的管理、决策或技术人员)；

c) 联系地址和场所；

d) 获证管理体系覆盖的运作范围；

e) 管理体系和过程的重大变更。

认证机构应采取适当的行动。

9 过程要求

9.1 认证前的活动

9.1.1 申请

认证机构应要求申请组织的授权代表提供必要的信息，以便认证机构确定：

a) 申请认证的范围；

b) 特定认证方案所要求的申请组织的相关详细情况，包括其名称、场所的地址、过程和运作的重要方面、人力资源和技术资源、职能、关系以及任何相关的法律义务；

c) 识别申请组织采用的所有影响符合性的外包过程；

d) 申请组织寻求认证的标准或其他要求；

e) 是否接受过与拟认证的管理体系有关的咨询，如果接受过，由谁提供咨询。

9.1.2 申请评审

9.1.2.1 认证机构应对认证申请及补充信息进行评审，以确保：

a) 关于申请组织及其管理体系的信息足以建立审核方案(见 9.1.3)；

b) 解决了认证机构与申请组织之间任何已知的理解差异；

c) 认证机构有能力并能够实施认证活动；

d) 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(语言、安全条件、对公正性的威胁等)。

9.1.2.2 在申请评审后，认证机构应接受或拒绝认证申请。当认证机构基于申请评审的结果拒绝认证申请时，应记录拒绝申请的原因并使客户清楚拒绝的原因。

9.1.2.3 根据上述评审，认证机构应确定审核组及进行认证决定需要具备的能力。

9.1.3 审核方案

9.1.3.1 应对整个认证周期制定审核方案，以清晰地识别所需的审核活动，这些审核活动用以证实客户的管理体系符合认证所依据标准或其他规范性文件的要求。认证周期的审核方案应覆盖全部的管理体系要求。

9.1.3.2 初次认证审核方案应包括两阶段初次审核、认证决定之后的第一年与第二年的监督审核和第三年在认证到期前进行的再认证审核。第一个三年的认证周期从初次认证决定算起。以后的周期从再认证决定(见 9.6.3.2.3)算起。审核方案的确定和任何后续调整应考虑客户的规模，其管理体系、产品和过程的范围与复杂程度，以及经过证实的管理体系有效性水平和以前审核的结果。

注 1：附录 E 提供了一个典型的审核与认证过程的流程图。

注 2：下面列举了建立或修改审核方案时可能需要考虑的其他事项，在确定审核范围和编制审核计划时可能也需要考虑这些事项：

——认证机构收到的对客户的投诉；

——结合、一体化或联合审核；

——认证要求的变化；

——法律要求的变化；

——认可要求的变化；

——组织的绩效数据[例如缺陷水平、关键绩效指标(KPI)数据等]；

——利益相关方的关注。

注 3：如果特定的行业认证方案有规定，认证周期可以不为 3 年。

9.1.3.3 监督审核应至少每个日历年(应进行再认证的年份除外)进行一次。初次认证后的第一次监督审核应在认证决定日期起 12 个月内进行。

注：为了考虑诸如季节或有限时段的管理体系认证(例如临时施工场所)等因素，可能有必要调整监督审核的频次。

9.1.3.4 如果认证机构考虑客户已获的认证或由另一认证机构实施的审核，则应获取并保留充足的证据，例如报告和对不符合采取的纠正措施的文件。所获取的文件应为满足本部分要求提供支持。认证机构应根据获取的信息证明对审核方案的任何调整的合理性，并予以记录，并对以前不符合的纠正措施的实施进行跟踪。

9.1.3.5 如果客户采用轮班作业，应在建立审核方案和编制审核计划时考虑在轮班工作中发生的活动。

9.1.4 确定审核时间

9.1.4.1 认证机构应有形成文件的确定审核时间的程序。认证机构应针对每个客户确定策划和完成对其管理体系的完整有效审核所需的时间。

9.1.4.2 在确定审核时间时，认证机构应考虑(但不限于)以下方面：

a) 相关管理体系标准的要求；

b) 客户及其管理体系的复杂程度；

c) 技术和法规环境；

d) 管理体系范围内活动的分包情况；

e) 以前审核的结果；

f) 场所的数量和规模、地理位置以及对多场所的考虑；

g) 与组织的产品、过程或活动相关联的风险；

h) 是否是结合审核、联合审核或一体化审核。

注 1：往返于审核场所之间所花费的时间不计入管理体系认证审核时间。

注 2：认证机构在制定文件化过程时，可以使用 ISO/IEC TS 17023 建立的指南来确定管理体系认证审核时间。

在已为特定的认证方案确定了特定的准则时，例如 ISO/TS 22003 或 ISO/IEC 27006，这些特定准

则应得到采用。

9.1.4.3 认证机构应记录管理体系审核的时间及其合理性。

9.1.4.4 未被指派为审核员的审核组成员(即技术专家、翻译人员、观察员和实习审核员)所花费的时间不应计入上面所确定的审核时间。

注:使用翻译人员可能需要额外增加审核时间。

9.1.5 多场所的抽样

当客户管理体系包含在多个地点进行的相同活动时,如果认证机构在审核中使用多场所抽样,则应制定抽样方案以确保对该管理体系的正确审核。认证机构应针对每个客户将抽样计划的合理性形成文件。一些特定的认证方案不允许抽样,如果特定认证方案已经建立了具体准则(例如 ISO/TS 22003),应采用这些准则。

注:当多场所不是覆盖相同的活动时,抽样是不适宜的。

9.1.6 多管理体系标准

认证机构在提供依据多个管理体系标准进行认证时,审核策划应确保充分的现场审核,以提供对认证的信任。

9.2 策划审核

9.2.1 确定审核目的、范围和准则

9.2.1.1 审核目的应由认证机构确定。审核范围和准则,包括任何更改,应由认证机构在与客户商讨后确定。

9.2.1.2 审核目的应说明审核要完成什么,并应包括下列内容:

a) 确定客户管理体系或其部分与审核准则的符合性;

b) 确定管理体系确保客户满足适用的法律、法规及合同要求的能力;

注:管理体系认证审核不是合规性审核。

c) 确定管理体系在确保客户可以合理预期实现其规定目标方面的有效性;

d) 适用时,识别管理体系的潜在改进区域。

9.2.1.3 审核范围应说明审核的内容和界限,例如拟审核的场所、组织单元、活动及过程。当初次认证或再认证过程包含一次以上审核(例如覆盖不同场所的审核)时,单次审核的范围可能并不覆盖整个认证范围,但整个审核所覆盖的范围应与认证文件中的范围一致。

9.2.1.4 审核准则应被用作确定符合性的依据,并应包括:

——所确定的管理体系规范性文件的要求;

——所确定的由客户制定的管理体系的过程和文件。

9.2.2 选择和指派审核组

9.2.2.1 总则

9.2.2.1.1 认证机构应有根据实现审核目的所需的能力以及公正性要求来选择和任命审核组(包括审核组长以及必要的技术专家)的过程。如果仅有一名审核员,该审核员应有能力履行适用于该审核的审核组长职责。审核组应整体上具备认证机构按照 9.1.2.3 确定的审核能力。

9.2.2.1.2 决定审核组的规模和组成时,应考虑下列因素:

a) 审核目的、范围、准则和预计的审核时间;

b) 是否是结合、联合或一体化审核;

c) 实现审核目的所需的审核组整体能力(见表 A.1);

d) 认证要求(包括任何适用的法律、法规或合同要求);

e) 语言和文化。

注:结合审核或一体化审核的审核组长宜至少对一个标准有深入的知识,并了解该审核所使用的其他标准。

9.2.2.1.3 审核组长和审核员所需的知识和技能可以通过技术专家和翻译人员补充。技术专家和翻译人员应在审核员的指导下工作。使用翻译人员时,翻译人员的选择要避免他们对审核产生不正当影响。

注:技术专家的选择准则根据每次审核的审核组和审核范围的需要为基础确定。

9.2.2.1.4 实习审核员可以参与审核,此时要指派一名审核员作为评价人员。评价人员应有能力接管实习审核员的任务,并对实习审核员的活动和审核发现最终负责。

9.2.2.1.5 审核组长在与审核组商议后,应向每个审核组成员分配对特定过程、职能、场所、区域或活动实施审核的职责。所进行的分配应考虑到所需的能力、有效并高效地使用审核组以及审核员、实习审核员和技术专家的不同作用和职责。在审核进程中,为确保实现审核目的,可以改变工作分配。

9.2.2.2 观察员、技术专家和向导

9.2.2.2.1 观察员

认证机构与客户应在实施审核前就审核活动中观察员的到场及理由达成一致。审核组应确保观察员不对审核过程或审核结果造成不当影响或干预。

注:观察员可以是客户组织的成员、咨询人员、实施见证的认可机构人员、监管人员或其他有合理理由的人员。

9.2.2.2.2 技术专家

认证机构应在实施审核前与客户就技术专家在审核活动中的作用达成一致。技术专家不应担任审核组中的审核员。技术专家应由审核员陪同。

注:技术专家可以就审核准备、策划或审核向审核组提出建议。

9.2.2.2.3 向导

每个审核员应由一名向导陪同,除非审核组长与客户另行达成一致。为审核组配备向导是为了方便审核。审核组应确保向导不影响或不干预审核过程或审核结果。

注 1:向导的职责可以包括:

a) 为面谈建立联系或安排时间;

b) 安排对现场或组织的特定部分的访问;

c) 确保审核组成员知道并遵守关于现场安全和安保程序的规则;

d) 代表客户观察审核;

e) 应审核员请求提供澄清或信息。

注 2:适宜时,受审核方也可以担任向导。

9.2.3 审核计划

9.2.3.1 总则

认证机构应确保为审核方案中确定的每次审核编制审核计划,以便为有关各方就审核活动的日程安排和实施达成一致提供依据。

注:不期望认证机构在建立审核方案时,为每次审核都编制审核计划。

9.2.3.2 编制审核计划

审核计划应与审核目的和范围相适应。审核计划至少应包括或引用:

a) 审核目的；
b) 审核准则；
c) 审核范围，包括识别拟审核的组织和职能单元或过程；
d) 拟实施现场审核活动(适用时，包括对临时场所的访问和远程审核活动)的日期和场所；
e) 预计的现场审核活动持续时间；
f) 审核组成员及与审核组同行的人员(例如观察员或翻译)的角色和职责。

注：审核计划的信息可以包含在一个以上的文件中。

9.2.3.3 审核组任务的沟通

认证机构应明确说明审核组的任务。认证机构应要求审核组：

a) 检查和验证客户与管理体系标准相关的结构、方针、过程、程序、记录及相关文件；
b) 确定上述方面满足与拟认证范围相关的所有要求；
c) 确定客户组织有效地建立、实施并保持了管理体系过程和程序，以便为建立对客户管理体系的信任提供基础；
d) 告知客户其方针、目标及指标的任何不一致，以使其采取措施。

9.2.3.4 审核计划的沟通

认证机构应提前与客户就审核计划进行沟通，并商定审核日期。

9.2.3.5 审核组成员信息的通报

认证机构应向客户提供审核组每位成员的姓名，并在客户请求时使其能够了解每位成员的背景情况。认证机构应留出足够的时间，以使客户能够对某一审核组成员的任命表示反对，并在反对有效时使认证机构能够重组审核组。

9.3 初次认证

9.3.1 初次认证审核

9.3.1.1 总则

管理体系的初次认证审核应分两个阶段实施：第一阶段和第二阶段。

9.3.1.2 第一阶段

9.3.1.2.1 策划应确保第一阶段的目的能够实现，应告知第一阶段需实施的任何现场活动。

注：第一阶段不要求正式的审核计划(见 9.2.3)。

9.3.1.2.2 第一阶段的目的为：

a) 审查客户的文件化的管理体系信息；
b) 评价客户现场的具体情况，并与客户的人员进行讨论，以确定第二阶段的准备情况；
c) 审查客户理解和实施标准要求的情况，特别是对管理体系的关键绩效或重要的因素、过程、目标和运作的识别情况；
d) 收集关于客户的管理体系范围的必要信息，包括：
   ——客户的场所；
   ——使用的过程和设备；
   ——所建立的控制的水平(特别是客户为多场所时)；
   ——适用的法律法规要求；

e) 审查第二阶段所需资源的配置情况，并与客户商定第二阶段的细节；

f) 结合管理体系标准或其他规范性文件充分了解客户的管理体系和现场运作，以便为策划第二阶段提供关注点；

g) 评价客户是否策划和实施了内部审核与管理评审，以及管理体系的实施程度能否证明客户已为第二阶段做好准备。

注：如果至少第一阶段的部分活动在客户场所实施，这能有助于达到上述目的。

9.3.1.2.3 认证机构应将第一阶段目的是否达到及第二阶段是否准备就绪的书面结论告知客户，包括识别任何引起关注的、在第二阶段可能被判定为不符合的问题。

注：第一阶段的输出不必满足审核报告的所有要求(见 9.4.8)。

9.3.1.2.4 认证机构在确定第一阶段和第二阶段的间隔时间时，应考虑客户解决第一阶段识别的任何需关注问题所需的时间。认证机构也可能需要调整第二阶段的安排。如果发生任何将影响管理体系的重要变更，认证机构应考虑是否有必要重复整个或部分第一阶段。认证机构应告知客户第一阶段的结果有可能导致推迟或取消第二阶段。

9.3.1.3 第二阶段

第二阶段的目的是评价客户管理体系的实施情况，包括有效性。第二阶段应在客户的现场进行，并至少覆盖以下方面：

a) 与适用的管理体系标准或其他规范性文件的所有要求的符合情况及证据；

b) 依据关键绩效目标和指标(与适用的管理体系标准或其他规范性文件的期望一致)，对绩效进行的监视、测量、报告和评审；

c) 客户管理体系的能力以及在符合适用法律法规要求和合同要求方面的绩效；

d) 客户过程的运作控制；

e) 内部审核和管理评审；

f) 针对客户方针的管理职责。

9.3.1.4 初次认证的审核结论

审核组应对在第一阶段和第二阶段中收集的所有信息和证据进行分析，以评审审核发现并就审核结论达成一致。

9.4 实施审核

9.4.1 总则

认证机构应有实施现场审核的过程。该过程应包括审核开始时的首次会议和审核结束时的末次会议。

当审核的任何部分以电子手段实施时，或拟审核的场所为虚拟场所时，认证机构应确保由具备适宜能力的人员实施此类活动。在此类审核活动中获取的证据应足以让审核员对相关要求的符合性做出有根据的决定。

注："现场"审核可以包括对包含管理体系审核相关信息的电子化场所的远程访问。也可以考虑使用电子手段实施审核。

9.4.2 召开首次会议

应与客户的管理层(适用时，还包括拟审核职能或过程的负责人员)召开正式的首次会议。首次会议通常由审核组长主持，会议目的是简要解释将如何进行审核活动。详略程度可与客户对审核过程的熟悉程度相一致，并应考虑下列方面：

a) 介绍参会人员，包括简要介绍其角色；
b) 确认认证范围；
c) 确认审核计划（包括审核的类型、范围、目的和准则）及其任何变化，以及与客户的其他相关安排，例如末次会议的日期和时间，审核期间审核组与客户管理层的会议的日期和时间；
d) 确认审核组与客户之间的正式沟通渠道；
e) 确认审核组可获得所需的资源和设施；
f) 确认与保密有关的事宜；
g) 确认适用于审核组的相关的工作安全、应急和安保程序；
h) 确认可得到向导和观察员及其角色和身份；
i) 报告的方法，包括审核发现的任何分级；
j) 说明可能提前终止审核的条件；
k) 确认审核组长和审核组代表认证机构对审核负责，并应控制审核计划（包括审核活动和审核路径）的执行；
l) 适用时，确认以往评审或审核的发现的状态；
m) 基于抽样实施审核的方法和程序；
n) 确认审核中使用的语言；
o) 确认在审核中将告知客户审核进程及任何关注点；
p) 让客户提问的机会。

9.4.3 审核中的沟通

9.4.3.1 在审核中，审核组应定期评估审核的进程，并沟通信息。审核组长应在需要时在审核组成员之间重新分配工作，并定期将审核进程及任何关注告知客户。

9.4.3.2 当可获得的审核证据显示审核目的无法实现，或显示存在紧急和重大的风险（例如安全风险）时，审核组长应向客户（如果可能还应向认证机构）报告这一情况，以确定适当的行动。该行动可以包括重新确认或修改审核计划，改变审核目的或审核范围，或者终止审核。审核组长应向认证机构报告所采取行动的结果。

9.4.3.3 如果在现场审核活动的进行中发现需要改变审核范围，审核组长应与客户审查该需要，并报告认证机构。

9.4.4 获取和验证信息

9.4.4.1 在审核中应通过适当的抽样来获取与审核目的、范围和准则相关的信息（包括与职能、活动和过程之间的接口有关的信息），并对这些信息进行验证，使之成为审核证据。

9.4.4.2 信息获取方法应包括（但不限于）：

a) 面谈；
b) 对过程和活动进行观察；
c) 审查文件和记录。

9.4.5 确定和记录审核发现

9.4.5.1 应确定审核发现（概述符合性并详细描述不符合），并予以分级和报告，以能够为认证决定或保持认证提供充分的信息。

9.4.5.2 可以识别和记录改进机会，除非某一管理体系认证方案的要求禁止这样做。但是属于不符合的审核发现不应作为改进机会予以记录。

9.4.5.3 关于不符合的审核发现应对照具体要求予以记录，包含对不符合的清晰陈述（详细标识不符合

所基于的客观证据)。应与客户讨论不符合,以确保证据准确且不符合得到理解。但是,审核员应避免提示不符合的原因或解决方法。

9.4.5.4 审核组长应尝试解决审核组与客户之间关于审核证据或审核发现的任何分歧意见,未解决的分歧点应予以记录。

9.4.6 准备审核结论

在末次会议前,由审核组长负责,审核组应:

a) 对照审核目的和审核准则,审查审核发现和审核中获得的任何其他适用的信息,并对不符合分级;
b) 考虑审核过程中固有的不确定性,就审核结论达成一致;
c) 就任何必要的跟踪活动达成一致;
d) 确认审核方案的适宜性,或识别任何为将来的审核所需要的修改(例如认证范围、审核时间或日期、监督频次、审核组能力)。

9.4.7 召开末次会议

9.4.7.1 应与客户的管理层(适用时,还包括所审核的职能或过程的负责人员)召开正式的末次会议,并记录参加人员。末次会议通常由审核组长主持,会议目的是提出审核结论,包括关于认证的推荐性意见。不符合应以使其被理解的方式提出,并应就回应的时间表达成一致。

注:"被理解"不一定意味着客户已经接受了不符合。

9.4.7.2 末次会议还应包括下列内容,其详略程度应与客户对审核过程的熟悉程度一致:

a) 向客户说明所获取的审核证据基于对信息的抽样,因而会有一定的不确定性;
b) 进行报告的方法和时间表,包括审核发现的任何分级;
c) 认证机构处理不符合(包括与客户认证状态有关的任何结果)的过程;
d) 客户为审核中发现的任何不符合的纠正和纠正措施提出计划的时间表;
e) 认证机构在审核后的活动;
f) 说明投诉和申诉处理过程。

9.4.7.3 客户应有机会提出问题。审核组与客户之间关于审核发现或结论的任何分歧意见应得到讨论并尽可能获得解决。任何未解决的分歧意见应予以记录并提交认证机构。

9.4.8 审核报告

9.4.8.1 认证机构应为每次审核向客户提供书面报告。审核组可以识别改进机会,但不应提出具体解决办法的建议。认证机构应享有对审核报告的所有权。

9.4.8.2 审核组长应确保审核报告的编制,并应对审核报告的内容负责。审核报告应提供对审核的准确、简明和清晰的记录,以便为认证决定提供充分的信息,并应包括或引用下列内容:

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) 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;
k) 与审核类型的要求一致的审核发现(见 9.4.5)、对审核证据的引用以及审核结论;
l) 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;
m) 已识别出的任何未解决的问题;
n) 适用时,是否为结合、联合或一体化审核;
o) 说明审核基于对可获得信息的抽样过程的免责声明;
p) 审核组的推荐意见;
q) 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;
r) 适用时,对以前不符合采取的纠正措施有效性的验证情况。

9.4.8.3 审核报告还应包含:

a) 关于管理体系符合性与有效性的声明以及对下列方面相关证据的总结:
——管理体系满足适用要求和实现预期结果的能力;
——内部审核和管理评审的过程;
b) 对认证范围适宜性的结论;
c) 确认是否达到审核目的。

9.4.9 不符合的原因分析

对于审核中发现的不符合,认证机构应要求客户在规定期限内分析原因,并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。

9.4.10 纠正和纠正措施的有效性

认证机构应审查客户提交的纠正、所确定的原因和纠正措施,以确定其是否可被接受。认证机构应验证所采取的任何纠正和纠正措施的有效性。所取得的为不符合的解决提供支持的证据应予以记录。应将审查和验证的结果告知客户。如果为了验证纠正和纠正措施的有效性,将需要补充一次全面的或有限的审核,或者需要文件化的证据(需要在未来的审核中确认),则认证机构应告知客户。

注:可以通过审查客户提供的文件化信息,或在必要时实施现场验证来验证纠正和纠正措施的有效性。验证活动通常由审核组成员完成。

9.5 认证决定

9.5.1 总则

9.5.1.1 认证机构应确保做出授予或拒绝认证、扩大或缩小认证范围、暂停或恢复认证、撤销认证或更新认证的决定的人员或委员会不是实施审核的人员。被指定进行认证决定的人员应具有适宜能力。

9.5.1.2 认证机构指定的认证决定人员[不包括委员会(见 6.1.4)成员]应为认证机构的雇员,或者是一个处于认证机构组织控制下的实体的雇员;或者与认证机构或上述实体具有在法律上有强制实施力的安排。认证机构的组织控制应为下列情况之一:

a) 认证机构拥有另一实体的全部或多数所有权;
b) 认证机构在另一实体的董事会中占多数;
c) 在一个通过所有权或董事会控制联结而成的法律实体网络中(认证机构处于其中),认证机构对另一实体有形成文件的权力。

注:对于政府认证机构,同一政府内部的其他部分可视为通过所有权与该认证机构相联系。

9.5.1.3 处于认证机构组织控制下的实体的雇员或与该实体有合同的人员,应同认证机构雇员或与认证机构有合同的人员一样满足本部分要求。

9.5.1.4 认证机构应记录每项认证决定,包括从审核组或其他来源获得的任何补充信息或澄清。

9.5.2 作出决定前的行动

认证机构在做出授予或拒绝认证、扩大或缩小认证范围、更新、暂停或恢复或者撤销认证的决定前，应有过程对下列方面进行有效的审查：

a) 审核组提供的信息足以确定认证要求的满足情况和认证范围；

b) 对于所有严重不符合，认证机构已审查、接受和验证了纠正和纠正措施；

c) 对于所有轻微不符合，认证机构已审查和接受了客户对纠正和纠正措施的计划。

9.5.3 授予初次认证所需的信息

9.5.3.1 为使认证机构做出认证决定，审核组至少应向认证机构提供以下信息：

a) 审核报告；

b) 对不符合的意见，适用时，还包括对客户采取的纠正和纠正措施的意见；

c) 对提供给认证机构用于申请评审(见 9.1.2)的信息的确认；

d) 对是否达到审核目的的确认；

e) 对是否授予认证的推荐性意见及附带的任何条件或评论。

9.5.3.2 如果认证机构不能在第二阶段结束后 6 个月内验证对严重不符合实施的纠正和纠正措施，则应在推荐认证前再实施一次第二阶段。

9.5.3.3 当认证从一个认证机构转换到另一个认证机构时，接受认证机构应有过程获取充分的信息以做出认证决定。

注：特定认证方案可能有认证转换的具体规则。

9.5.4 授予再认证所需的信息

认证机构应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，做出是否更新认证的决定。

9.6 保持认证

9.6.1 总则

认证机构应在证实获证客户持续满足管理体系标准要求后保持对其的认证。认证机构满足下列前提条件时，可以根据审核组长的肯定性结论保持对客户的认证，而无需再进行独立复核和决定：

a) 对于任何严重不符合或其他可能导致暂停或撤销认证的情况，认证机构有制度要求审核组长向认证机构报告需由具备适宜能力(见 7.2.8)且未实施该审核的人员进行复核，以确定能否保持认证；

b) 由具备能力的认证机构人员对认证机构的监督活动进行监视，包括对审核员的报告活动进行监视，以确认认证活动在有效地运作。

9.6.2 监督活动

9.6.2.1 总则

9.6.2.1.1 认证机构应对其监督活动进行设计，以便定期对管理体系范围内有代表性的区域和职能进行监视，并应考虑获证客户及其管理体系的变更情况。

9.6.2.1.2 监督活动应包括对获证客户管理体系满足认证标准规定要求情况的现场审核。监督活动还可以包括：

a) 认证机构就认证的有关方面询问获证客户；

b) 审查获证客户对其运作的说明(如宣传材料、网页);
c) 要求获证客户提供文件化信息(纸质或电子介质);
d) 其他监视获证客户绩效的方法。

9.6.2.2 监督审核

监督审核是现场审核,但不一定是对整个体系的审核,并应与其他监督活动一起策划,以使认证机构能对获证客户管理体系在认证周期内持续满足要求保持信任。相关管理体系标准的每次监督审核应包括对以下方面的审查:

a) 内部审核和管理评审;
b) 对上次审核中确定的不符合采取的措施;
c) 投诉的处理;
d) 管理体系在实现获证客户目标和各管理体系的预期结果方面的有效性;
e) 为持续改进而策划的活动的进展;
f) 持续的运作控制;
g) 任何变更;
h) 标志的使用和(或)任何其他对认证资格的引用。

9.6.3 再认证

9.6.3.1 再认证审核的策划

9.6.3.1.1 再认证审核的目的是确认管理体系作为一个整体的持续符合性与有效性,以及与认证范围的持续相关性和适宜性。认证机构应策划并实施再认证审核,以评价获证客户是否持续满足相关管理体系标准或其他规范性文件的所有要求。上述策划和实施应及时进行,以便认证能在到期前及时更新。

9.6.3.1.2 再认证活动应考虑管理体系在最近一个认证周期内的绩效,包括调阅以前的监督审核报告。

9.6.3.1.3 当管理体系、组织或管理体系的运作环境(如法律的变更)有重大变更时,再认证审核活动可能需要有第一阶段。

注:此类变更可能在认证周期中的任何时间发生,认证机构可能需要实施特殊审核(见 9.6.4),该特殊审核可能需要或不需要两阶段审核。

9.6.3.2 再认证审核

9.6.3.2.1 再认证审核应包括针对下列方面的现场审核:

a) 结合内部和外部变更来看的整个管理体系的有效性,以及认证范围的持续相关性和适宜性;
b) 经证实的对保持管理体系有效性并改进管理体系,以提高整体绩效的承诺;
c) 管理体系在实现获证客户目标和管理体系预期结果方面的有效性。

9.6.3.2.2 对于严重不符合,认证机构应规定实施纠正与纠正措施的时限。这些措施应在认证到期前得到实施和验证。

9.6.3.2.3 如果在当前认证的终止日期前成功完成了再认证活动,新认证的终止日期可以基于当前认证的终止日期。新证书上的颁证日期应不早于再认证决定日期。

9.6.3.2.4 如果在认证终止日期前,认证机构未能完成再认证审核或不能验证对严重不符合实施的纠正和纠正措施(见 9.5.2),则不应推荐再认证,也不应延长认证的效力。认证机构应告知客户并解释后果。

9.6.3.2.5 在认证到期后,如果认证机构能够在 6 个月内完成未尽的再认证活动,则可以恢复认证,否则应至少进行一次第二阶段才能恢复认证。证书的生效日期应不早于再认证决定日期,终止日期应基于上一个认证周期。

9.6.4 特殊审核

9.6.4.1 扩大认证范围

对于已授予的认证，认证机构应对扩大认证范围的申请进行评审，并确定任何必要的审核活动，以做出是否可予扩大的决定。这类审核活动可以和监督审核同时进行。

9.6.4.2 提前较短时间通知的审核

认证机构为调查投诉、对变更做出回应或对被暂停的客户进行追踪，可能需要在提前较短时间通知获证客户后或不通知获证客户就对其进行审核。此时：

a) 认证机构应说明并使获证客户提前了解(如在 8.5.1 所述的文件中)将在何种条件下进行此类审核；

b) 由于客户缺乏对审核组成员的任命表示反对的机会，认证机构应在指派审核组时给予更多的关注。

9.6.5 暂停、撤销或缩小认证范围

9.6.5.1 认证机构应有暂停、撤销或缩小认证范围的政策和形成文件的程序，并规定认证机构的后续措施。

9.6.5.2 发生以下情况(但不限于)时，认证机构应暂停获证客户的认证资格：

——客户的获证管理体系持续地或严重地不满足认证要求，包括对管理体系有效性的要求；

——获证客户不允许按要求的频次实施监督或再认证审核；

——获证客户主动请求暂停。

9.6.5.3 在暂停期间，客户的管理体系认证暂时无效。

9.6.5.4 如果造成暂停的问题已解决，认证机构应恢复被暂停的认证。如果客户未能在认证机构规定的时限内解决造成暂停的问题，认证机构应撤销或缩小其认证范围。

注：多数情况下，暂停将不超过 6 个月。

9.6.5.5 如果客户在认证范围的某些部分持续地或严重地不满足认证要求，认证机构应缩小其认证范围，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。

9.7 申诉

9.7.1 认证机构应有受理和评价申诉并对之做出决定的形成文件的过程。

9.7.2 认证机构应对申诉处理过程各个层次的所有决定负责。认证机构应确保参与申诉处理过程的人员没有实施申诉涉及的审核，也没有做出申诉涉及的认证决定。

9.7.3 申诉的提出、调查和决定不应造成针对申诉人的任何歧视行为。

9.7.4 申诉处理过程应至少包括以下要素和方法：

a) 受理、确认和调查申诉的过程，以及参考以前类似申诉的结果，决定采取何种措施以回应申诉的过程；

b) 跟踪和记录申诉，包括为解决申诉而采取的措施；

c) 确保采取任何适当的纠正和纠正措施。

9.7.5 收到申诉的认证机构应负责收集和验证所有必要的信息，以确定申诉的有效性。

9.7.6 认证机构应确认收到了申诉，并应向申诉人提供申诉处理的进展报告和结果。

9.7.7 对申诉的决定应由与申诉事项无关的人员做出，或经其审查和批准，并应告知申诉人。

9.7.8 认证机构应在申诉处理过程结束时正式通知申诉人。

9.8 投诉

9.8.1 认证机构应对投诉处理过程各层级的决定负责。

9.8.2 投诉的提交、调查和决定不应造成针对投诉人的任何歧视行为。

9.8.3 认证机构在收到投诉时，应确认投诉是否与其负责的认证活动有关，并在经确认有关时予以处理。如果投诉与获证客户有关，认证机构在调查投诉时应考虑获证管理体系的有效性。

9.8.4 对于针对获证客户的有效投诉，认证机构还应在适当的时间将投诉告知该客户。

9.8.5 认证机构应有受理和评价投诉并对之做出决定的形成文件的过程。该过程涉及投诉人和投诉事项的方面应满足保密要求。

9.8.6 投诉处理过程应至少包括以下要素和方法：

a) 受理、确认和调查投诉的过程，以及决定采取何种措施以回应投诉的过程；

b) 跟踪和记录投诉，包括为回应投诉而采取的措施；

c) 确保采取任何适当的纠正和纠正措施。

注：ISO 10002 为投诉的处理提供了指南。

9.8.7 收到投诉的认证机构应负责收集与核实对投诉进行确认所需的一切信息。

9.8.8 在可能时，认证机构应确认收到了投诉，并应向投诉人提供投诉处理的进展报告和结果。

9.8.9 对投诉的决定应由与投诉事项无关的人员做出，或经其审查和批准，并应告知投诉人。

9.8.10 在可能时，认证机构应在投诉处理过程结束时正式通知投诉人。

9.8.11 认证机构应与获证客户及投诉人共同决定是否应将投诉事项公开，并在决定公开时，共同确定公开的程度。

9.9 客户的记录

9.9.1 认证机构应对所有客户（包括所有提交申请的组织、接受审核的组织和获得认证或被暂停或撤销认证的组织）保持审核及其他认证活动的记录。

9.9.2 获证客户记录应包括以下内容：

a) 申请资料及初次认证、监督和再认证的审核报告；

b) 认证协议；

c) 适用时，多场所抽样方法的理由；

注：抽样方法包括为审核特定管理体系和（或）在多场所审核中选取场所而做的抽样。

d) 确定审核时间的理由（见 9.1.4）；

e) 纠正与纠正措施的验证；

f) 投诉和申诉及任何后续纠正或纠正措施的记录；

g) 适用时，委员会的审议和决定；

h) 认证决定的文件；

i) 认证文件，包括与产品（包括服务）、过程相关的认证范围，适用时，包括每个场所相应的认证范围；

j) 建立认证的可信度所需的相关记录，如审核员和技术专家能力的证据；

k) 审核方案。

9.9.3 认证机构应保证申请组织和客户记录的安全，以确保满足保密要求。运送、传输或传递记录的方式应确保保密。

9.9.4 认证机构应有关于记录保存的形成文件的政策和程序。获证客户及以往获证客户的记录保存期应为当前认证周期加上一个完整的认证周期。

注：某些情况下，记录需按法律规定保存更长的时间。

10 认证机构的管理体系要求

10.1 可选方式

认证机构应建立、实施和保持一个文件化的、能够支撑并证实其始终满足本部分要求的管理体系。认证机构除了满足 ISO/IEC 17021 本部分第 5 章至第 9 章的要求外，还应按照下列要求之一建立管理体系：

a) 通用的管理体系要求(见 10.2)；

b) 与 ISO 9001 一致的管理体系要求(见 10.3)。

10.2 方式 A：通用的管理体系要求

10.2.1 总则

认证机构应建立、实施和保持一个能够支撑并证实其始终满足 ISO/IEC 17021 本部分要求的管理体系并形成文件。

认证机构最高管理层应为认证机构的活动制定政策和目标，并形成文件。最高管理层应提供证据，以证实其对按 ISO/IEC 17021 本部分要求建立和实施管理体系的承诺。最高管理层应确保认证机构的政策在组织的各个层次上得到理解、实施和保持。

认证机构最高管理层应分派下列职责和权力：

a) 确保管理体系所需的过程和程序得到建立、实施和保持；

b) 向最高管理层报告管理体系的绩效及任何改进需求。

10.2.2 管理体系手册

认证机构应在管理体系手册或其关联文件中反映 ISO/IEC 17021 本部分的所有适用要求。认证机构应确保所有相关人员可以获取手册和相关的关联文件。

10.2.3 文件控制

认证机构应建立程序以控制与 ISO/IEC 17021 本部分实施有关的文件(内部和外部的)。该程序应规定下列方面所需的控制：

a) 文件发布前，对其充分性与适宜性进行批准；

b) 对文件进行复审，必要时予以更新，并再次批准；

c) 确保文件的更改和现行修订状态得到识别；

d) 确保在使用场所可以获得适用文件的相关版本；

e) 确保文件保持清晰并易于识别；

f) 确保外来文件得到识别，并控制其分发；

g) 防止作废文件的非预期使用，并在因故保留作废文件时，对其做出适当的标识。

注：文件可以使用任何形式或类型的介质。

10.2.4 记录控制

认证机构应建立程序，以对识别、贮存、保护、检索和处置与 ISO/IEC 17021 本部分实施有关的记录以及记录保存期限规定所需的控制。

认证机构应建立程序以明确与其合同、法律责任相一致的记录保存期限。对这些记录的查阅应与保密安排相一致。

注：获证客户记录的要求见 9.9。

10.2.5 管理评审

10.2.5.1 总则

认证机构最高管理层应建立按策划的时间间隔对管理体系进行评审的程序，以确保管理体系（包括与 ISO/IEC 17021 本部分实施有关的明示的政策和目标）的持续适宜性、充分性和有效性。管理评审应至少每年进行一次。

10.2.5.2 评审输入

管理评审的输入应包括与下列方面有关的信息：

a) 内部审核和外部评审的结果；
b) 客户和利益相关方的反馈；
c) 维护公正性；
d) 纠正措施的状况；
e) 风险应对措施的状况；
f) 以往管理评审的后续措施；
g) 目标的实现情况；
h) 可能影响管理体系的变更；
i) 申诉和投诉。

10.2.5.3 评审输出

管理评审的输出应包括与下列方面有关的决定和措施：

a) 管理体系及其过程的有效性的改进；
b) 与 ISO/IEC 17021 本部分实施有关的认证服务的改进；
c) 资源需求；
d) 组织的方针、政策和目标的修订。

10.2.6 内部审核

10.2.6.1 认证机构应建立内部审核程序，以证明认证机构满足 ISO/IEC 17021 本部分要求，并有效地实施和保持了管理体系。

注：ISO 19011 为实施内部审核提供了指南。

10.2.6.2 认证机构应对内部审核方案进行策划，并在策划中考虑拟审核过程和区域的重要程度以及以往审核的结果。

10.2.6.3 内部审核应至少每 12 个月进行一次。如果认证机构能够证明管理体系按照 ISO/IEC 17021 本部分持续地有效运行并保持稳定，则可以减少内部审核的频次。

10.2.6.4 认证机构应确保：

a) 内部审核的实施人员具备能力，熟悉认证、审核和 ISO/IEC 17021 本部分的要求；
b) 审核员不审核自己的工作；
c) 将审核结果告知受审核区域的负责人员；
d) 根据内部审核结果及时采取适当的措施；
e) 识别任何改进的机会。

10.2.7 纠正措施

认证机构应建立识别和管理其运作中的不符合的程序。必要时，认证机构还应采取措施消除不符

合的原因，以防止其再次发生。纠正措施应与所遇到问题的影响程度相适应。该程序应明确对下列方面的要求：

a) 识别不符合(例如通过有效投诉和内部审核)；
b) 确定不符合的原因；
c) 纠正不符合；
d) 评价确保不符合不再发生的措施的需求；
e) 及时确定和实施所需的措施；
f) 记录所采取措施的结果；
g) 评审纠正措施的有效性。

10.3 方式B：与ISO 9001一致的管理体系要求

10.3.1 总则

认证机构应按照ISO 9001的要求，建立和保持一个能够支撑并证实其始终满足ISO/IEC 17021本部分要求的管理体系。该管理体系还应满足10.3.2～10.3.4的补充要求。

10.3.2 范围

为应用ISO 9001的要求，认证机构管理体系的范围应包括认证服务的设计和开发要求。

10.3.3 以顾客为关注焦点

为应用ISO 9001的要求，认证机构在建立管理体系时应考虑认证的可信性，而且不仅应关注客户需求，还应关注依赖其审核与认证服务的所有各方(如4.1.2所述)的需求。

10.3.4 管理评审

为应用ISO 9001的要求，认证机构应将认证活动使用方相关申诉和投诉以及公正性审查的信息作为管理评审的输入。

附 录 A
（规范性附录）
所要求的知识和技能

A.1 概述

表 A.1 明确了认证机构应为特定的认证职能确定的知识和技能。“√”指认证机构应确定相应的知识和技能的准则和深度。表 A.1 中规定的知识和技能在下文中有更详细的解释，表中用扩号注明了相应解释文本的编号。

表 A.1 知识和技能表

知识和技能	认证职能		
	实施申请评审以确定所需的审核组能力、选择审核组成员并确定审核时间	复核审核报告并做出认证决定	审核及领导审核组
业务管理实践的知识			√（见 A.2.1）
审核原则、实践和技巧的知识		√（见 A.3.1）	√（见 A.2.2）
特定管理体系标准和（或）规范性文件的知识	√（见 A.4.1）	√（见 A.3.2）	√（见 A.2.3）
认证机构过程的知识	√（见 A.4.2）	√（见 A.3.3）	√（见 A.2.4）
客户的业务领域的知识	√（见 A.4.3）	√（见 A.3.4）	√（见 A.2.5）
客户的产品、过程和组织的知识	√（见 A.4.4）		√（见 A.2.6）
与客户组织中的各个层级相适应的语言技能			√（见 A.2.7）
作记录和撰写报告的技能			√（见 A.2.8）
表达技能			√（见 A.2.9）
面谈技能			√（见 A.2.10）
审核管理技能			√（见 A.2.11）
注：风险和复杂程度是在决定这些职能中任何一项职能所需的专业能力的水平时考虑的其他因素。			

A.2 管理体系审核员能力要求

A.2.1 业务管理实践的知识

通用的组织类型、规模、治理、结构与工作场所实务、信息与数据系统、文件系统以及信息技术的知识。

A.2.2 审核原则、实践和技巧的知识

本部分规定的通用的管理体系审核原则、实务和技巧的知识，需足以实施认证审核及评价内部审核过程。

A.2.3 特定管理体系标准和(或)规范性文件的知识

认证所依据的管理体系标准或其他规范性文件的知识,需足以确定体系是否得到有效实施并符合要求。

A.2.4 认证机构过程的知识

认证机构过程的知识,需足以按照认证机构的程序和过程开展工作。

A.2.5 客户业务领域的知识

客户业务领域的通用术语、实践和过程的知识,需足以在管理体系标准或其他规范性文件的背景下理解该领域的期望。

注:业务领域可理解为经济活动(例如航空航天、化工、金融服务)。

A.2.6 客户产品、过程和组织的知识

与客户的产品或过程的类型相关的知识,需足以理解该组织如何运行,如何应用管理体系标准或其他相关规范性文件的要求。

A.2.7 与客户组织中的各个层级相适应的语言技能

能够用适宜的术语、措辞和话语与组织任何层次的人员有效地进行沟通。

A.2.8 作记录和撰写报告的技能

能够以足够的速度、准确度和理解力阅读和书写,以记录、做笔记以及有效地沟通审核发现和结论。

A.2.9 表达技能

能以容易理解的方式表述审核发现和结论。审核组长还要能够在公开场合(例如末次会议)表述与听众相适宜的审核发现、结论和推荐意见。

A.2.10 面谈技能

能够通过提开放式、经过良好构思的问题并倾听、理解和评价对方的回答来进行面谈,以获取信息。

A.2.11 审核管理技能

能够实施和管理审核,以在约定的时间框架内获取审核证据。审核组长还要能够主持会议以有效地交流信息,并能够分配任务或在必要时重新分配。

A.3 复核审核报告并做出认证决定的人员的能力要求

这类人员的职能可由一人或多人完成。

A.3.1 审核原则、实践和技巧的知识

本部分规定的通用的管理体系审核原则、实务和技巧的知识,需足以理解认证审核报告。

A.3.2 特定管理体系标准和(或)规范性文件的知识

认证所依据的管理体系标准或其他规范性文件的知识,需足以根据认证审核报告作出决定。

A.3.3 认证机构过程的知识

认证机构过程的知识，需足以根据提交复核的信息确定是否达到了认证机构的期望。

A.3.4 客户业务领域的知识

客户业务领域的通用术语、实践和过程的知识，需足以在管理体系标准或其他规范性文件的背景下理解审核报告。

A.4 实施申请评审以确定所需的审核组能力、选择审核组成员并确定审核时间的人员的能力要求

这类人员的职能可由一人或多人完成。

A.4.1 特定管理体系标准和(或)规范性文件的知识

知道认证依据的是什么管理体系标准或其他规范性文件。

A.4.2 认证机构过程的知识

认证机构过程的知识，需足以指派有能力的审核组成员以及准确地确定审核时间。

A.4.3 客户业务领域的知识

客户业务领域的通用术语、实践和过程的知识，需足以指派有能力的审核组成员以及准确地确定审核时间。

A.4.4 客户产品、过程和组织的知识

与客户的产品或过程的类型相关的知识，需足以指派有能力的审核组成员以及准确地确定审核时间。

附 录 B
（资料性附录）
可能的评价方法

B.1 概述

本资料性附录提供评价方法的示例，为认证机构提供帮助。

人员的评价方法可以分为五大类：记录审查、意见反馈、面谈、观察和考试。每一类评价方法可以进一步细分。下面简要说明了每类评价方法及其对于知识和技能评价的用处和局限性。不太可能只用其中任何一种方法就能确认能力。

B.2～B.6 所述的方法可以提供知识和技能的有用信息；这些方法如被设计成与 7.1.2 和 7.1.3 所述的能力确定过程输出的特定能力准则结合使用，会更有效。

附录 C 提供了一个能力确定和保持过程的示例。

B.2 记录审查

有些记录可以显示知识，例如显示工作经历、审核经历、教育和培训的简历或履历。

有些记录可以显示技能，例如审核报告或工作经历、审核经历、教育和培训的记录。

单凭上述记录不太可能构成能力的充分证据。

其他记录是证实能力的直接证据，例如对审核员实施审核的绩效评价报告。

B.3 意见反馈

来自以前雇主的直接反馈可以显示知识和技能，但重要的是要注意有时雇主会特意排除负面信息。

个人推荐函可以显示知识和技能。应聘者不大可能提供含有负面信息的个人推荐函。

同行的意见反馈可以显示知识和技能。这种反馈可能受到同行之间关系的影响。

客户的意见反馈可以显示知识和技能。对于审核员来说，这种反馈可能受到审核结果的影响。

单凭意见反馈并不是令人满意的能力证据。

B.4 面谈

面谈可有助于询问出知识、技能方面的信息。

人员招聘时的面谈可有助于从简历和过去的工作经历详细了解知识和技能的信息。

在绩效考评中进行面谈，可以提供知识和技能的具体信息。

在审核后的评审中与审核组面谈，可以提供关于审核员知识和技能的有用信息。它可以使评审者有机会了解审核员为什么作出某项决定、选择某一审核路径等。这一技巧可在见证审核后使用，也可在之后评价书面审核报告时使用。这一技巧可能对确定与特定技术领域有关的能力尤其有用。

能力证实的直接证据可以通过依据规定的能力准则进行结构化的、并得到适当记录的面谈而获得。

可以使用面谈来评估语言、沟通和人际技能。

B.5 观察

对人员实施任务的情况进行观察能够为能力(经证实的应用知识和技能来实现预期结果)提供直接证据。这种评价方法对所有职能、行政和管理人员以及审核员和认证决定人员都有用。对审核员实施的一次审核进行见证的局限性在于这次特定审核所具有的难易程度。

定期对一个人进行见证,有助于确认持续的能力。

B.6 考试

笔试可为知识以及技能(后者取决于方法)提供良好的文件化证据。

口试可为知识提供良好的证据(取决于考官的能力),可提供关于技能的有限的结果。

实际操作考试可以提供关于知识和技能的平衡的结果(取决于考试过程和考官的能力)。实际操作考试的方法例如情景演练、案例分析、压力模拟和岗位实操考核等。

附 录 C
（资料性附录）
能力确定和保持过程的示例

图 C.1 的流程图显示了一种通过识别要完成的具体任务、识别实现预期结果所需的具体知识和技能来确定人员能力的方式。过程中使用了附录 B 描述的评价方法。

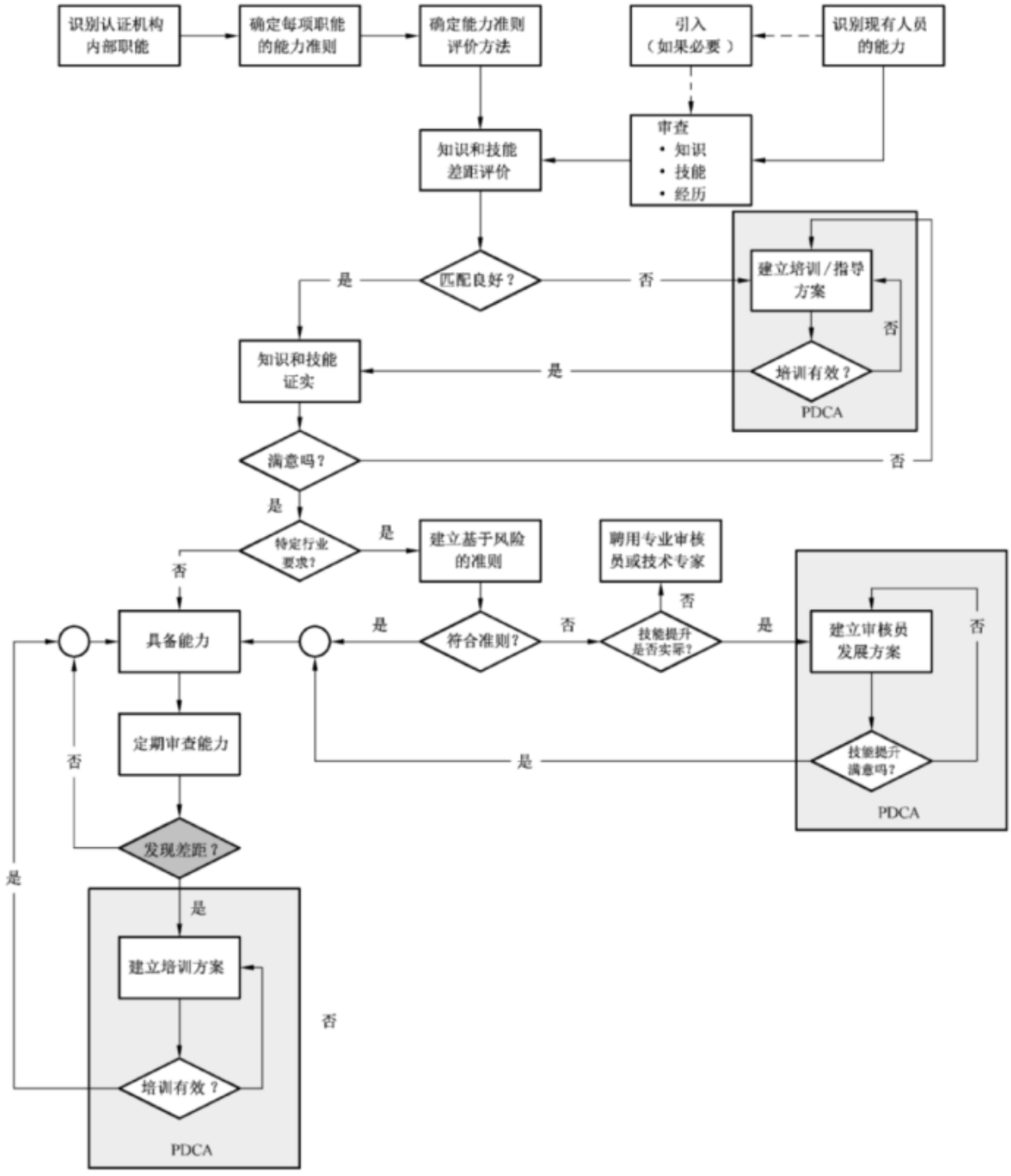

图 C.1 能力确定和保持过程示例

附 录 D
（资料性附录）
期望的个人行为

以下给出了对各类管理体系的认证活动参与人员重要的个人行为的示例：

a) 有道德，即公正、诚实、真诚、正直和谨慎；

b) 思想开明，即愿意考虑不同的意见或观点；

c) 有交际技巧，即得体地与人交往；

d) 合作，即与他人有效合作；

e) 观察敏锐，即积极地注意到周围的实际环境和活动；

f) 有感知力，即本能地意识到并能够理解遇到的情况；

g) 有适应能力，即易于根据不同的情况进行调整；

h) 坚韧，即坚持并专注于实现目的；

i) 明断，即根据逻辑推理和分析及时得出结论；

j) 独立自主，即独立地行事和履行职能；

k) 有职业水准，即在工作场所表现出礼貌、尽责和基本上专业的行为举止；

l) 有道德勇气，即愿意负责地、有道德地行事，即便这样做可能并不总是受到欢迎，或者有时可能遭到反对或引起对抗；

m) 有条理，即有效地管理时间、区分优先次序、策划，以及高效。

行为的确定是有条件的，弱点可能仅在特定情境下才显现出来。认证机构宜对识别出的任何对认证活动有不利影响的弱点采取适宜的行动。

附 录 E
（资料性附录）
审核和认证过程

图 E.1 代表了一个典型的流程。可以实施其他审核活动，例如文件审查和特殊审核。审核周期与认证周期之间的不同参见 9.2 和 9.3。

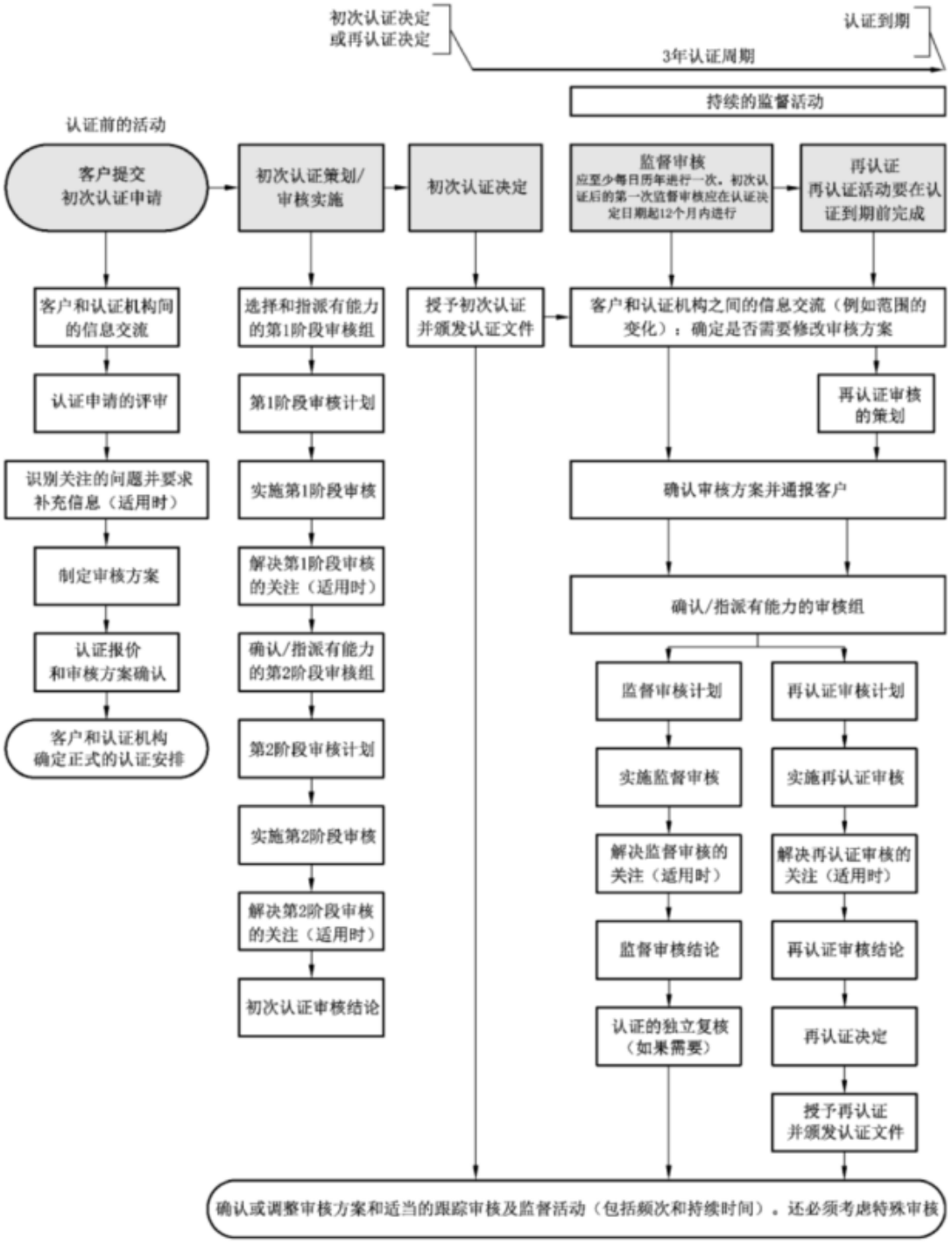

图 E.1 审核和认证过程的典型流程

参 考 文 献

[1] GB/T 19011—2013 管理体系审核指南(ISO 19011:2011,IDT)

[2] ISO 9001 Quality management systems—Requirements

[3] ISO 10002 Quality management—Customer satisfaction—Guidelines for complaints handling in organizations

[4] ISO 14001 Environmental management systems—Requirements with guidance for use

[5] ISO/IEC TS 17021-2 Conformity assessment—Requirements for bodies providing audit and certification of management systems—Part 2:Competence requirements for auditing and certification of environmental management systems

[6] ISO/IEC TS 17021-3 Conformity assessment—Requirements for bodies providing audit and certification of management systems—Part 3:Competence requirements for auditing and certification of quality management systems

[7] ISO/IEC TS 17021-4 Conformity assessment—Requirements for bodies providing audit and certification of management systems—Part 4:Competence requirements for auditing and certification of event sustainability management systems

[8] ISO/IEC TS 17021-5 Conformity assessment—Requirements for bodies providing audit and certification of management systems—Part 5:Competence requirements for auditing and certification of asset management systems

[9] ISO/IEC TS 17021-6 Requirements for bodies providing audit and certification of management systems—Part 6:Competence requirements for auditing and certification of business continuity management systems

[10] ISO/IEC TS 17021-7 Conformity assessment—Requirements for bodies providing audit and certification of management systems—Part 7:Competence requirements for auditing and certification of road traffic safety management systems

[11] ISO/IEC TS 17023 Conformity assessment—Guidelines for determining the duration of management system certification audits

[12] ISO/IEC 17030 Conformity assessment—General requirements for third-party marks of conformity

[13] ISO 20121 Event sustainability management systems—Requirements with guidance for use

[14] ISO/TS 22003 Food safety management systems—Requirements for bodies providing audit and certification of food safety management systems

[15] ISO 22301 Societal security—Business continuity management systems—Requirements

[16] ISO/IEC 27006 Information technology—Security techniques—Requirements for bodies providing audit and certification of information security management systems

[17] ISO 31000 Risk management—Principles and guidelines

[18] ISO 31010 Risk management—Risk assessment techniques

[19] ISO 39001 Road traffic safety(RTS)management systems—Requirements with guidance for use

[20] ISO 50003 Energy management systems—Requirements for bodies providing audit and certification of energy management systems

[21] ISO 55001 Asset management—Management systems—Requirements