ICS 03.100.01
A 90

中华人民共和国国家标准

GB/T 38701—2020/ISO 28003:2007

供应链安全管理体系　对供应链安全管理体系审核认证机构的要求

Security management systems for the supply chain—Requirements for bodies providing audit and certification of supply chain security management systems

(ISO 28003:2007,IDT)

2020-03-31 发布　　2020-09-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前言 …… Ⅰ
引言 …… Ⅱ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　认证机构的原则 …… 2
5　通用要求 …… 3
6　结构要求 …… 5
7　资源要求 …… 6
8　信息要求 …… 10
9　过程要求 …… 12
10　认证机构的管理体系要求 …… 22
附录A（资料性附录）　对审核时间确定过程的导则 …… 26
附录B（规范性附录）　多场所组织的审核准则 …… 28
附录C（规范性附录）　审核员的教育、工作和审核经历及培训时间 …… 31
附录D（规范性附录）　审核员能力要求 …… 32
参考文献 …… 34

前　言

本标准按照GB/T 1.1—2009给出的规则起草。

本标准使用翻译法等同采用ISO 28003:2007《供应链安全管理体系　对供应链安全管理体系审核认证机构的要求》。

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

——GB/T 19011—2003　管理体系审核指南(ISO 19011:2002,IDT)

本标准由全国公共安全基础标准化技术委员会(SAC/TC 351)提出并归口。

本标准起草单位：中国标准化研究院、中国合格评定国家认可中心、中国网络安全审查技术与认证中心、中国质量认证中心、江苏辉源供应链管理有限公司、国网山东省电力公司、方圆标志认证集团有限公司、福建你他共创网络科技有限公司、中国认证认可协会、江苏省质量和标准化研究院、北京城市系统工程研究中心。

本标准主要起草人：秦挺鑫、延静清、魏军、潘英、白元龙、孙世军、宋跃炜、叶耀华、王晶晶、翟季青、王延维、崔伟、王皖、韦晓晴、吴康宁、任青钺、张剑、孙兵、李正祥、曾繁仰、陈伟、汪勇。

引　言

本标准供实施供应链安全管理体系审核与认证的机构使用。供应链安全管理体系认证是第三方合格评定活动(见 ISO/IEC 17000:2004 中 5.5),实施这种活动的机构是第三方合格评定结构,在本标准中称这类机构为"认证机构",这一用语不妨碍那些具有其他名称但从事本标准范围内活动的机构使用本标准。实际上,本标准适用于任何参与供应链安全管理体系评定的机构。

供应链安全管理体系认证是对组织已实施了与其方针一致的供应链安全管理体系提供保证的一种方法。

供应链安全管理体系认证将由经承认的机构[例如国际认可论坛(IAF)的成员]认可的认证机构来实施。

本标准规定了对认证机构的要求。遵守这些要求旨在确保认证机构以有能力、一致和可信赖的方式实施供应链安全管理体系认证,以促进国际和国内承认这些机构并接受它们的认证。本标准作为促进供应链安全管理体系认证得到承认的基础,有助于国际贸易。

供应链安全管理体系认证独立地验证组织的供应链安全管理体系:

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;并

c) 得到有效实施。

因此,供应链安全管理体系认证为组织、组织的顾客及利益相关方提供价值。

本标准旨在作为承认认证机构提供供应链安全管理体系认证的能力的依据。本标准可作为承认认证机构提供供应链安全管理体系认证的能力的依据(承认的形式可包括通告、同行评审、监管部门或产业联盟的直接承认)。

认证活动包括对组织的供应链安全管理体系的审核。当一个组织的供应链安全管理体系符合某一特定标准(例如 ISO 28000)或其他规定要求时,这种符合性通常是以认证文件或认证证书的形式来证明的。

建立自身的供应链安全管理体系(包括 ISO 28000 供应链安全管理体系、其他特定的供应链安全管理体系要求、质量体系、环境管理体系或职业健康与安全管理体系与供应链安全管理体系的整合)由拟认证的组织完成。除相关法律有相反要求之外,由组织决定如何安排这些体系的构成。管理体系各部分间的整合程度因组织而异。因此,在更广泛的组织中整合供应链安全管理体系时,依据本标准运作的认证机构考虑其客户的文化和习惯是适当的。

供应链安全管理体系　对供应链安全管理体系审核认证机构的要求

1　范围

对于依据管理体系规范和标准(例如 ISO 28000)提供供应链安全管理体系审核与认证的机构,本标准给出了原则和要求。本标准规定了对认证机构及其相关审核员的最低要求,识别了审核和认证客户组织时对保密性的独特要求。

对供应链安全管理体系的要求可能来自多个方面,本标准的制定旨在帮助对符合 ISO 28000《供应链安全管理体系规范》和其他供应链安全管理体系国际标准要求的供应链安全管理体系实施认证。本标准的内容也可用于支持基于其他特定的供应链安全管理体系要求的供应链安全管理体系认证。

本标准:

——对应用 ISO 28000(或其他特定的供应链安全管理体系要求)的认证机构认可提供了一致的指导;

——明确了适用于依据供应链安全管理体系标准要求(或其他特定的供应链安全管理体系要求)实施供应链安全管理体系审核与认证的规则;

——向客户提供关于其供方获得认证的方式的必要信息和信心。

注 1:供应链安全管理体系认证有时也称为"注册",认证机构有时称为"注册机构"。

注 2: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 3:本标准可作为认可、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(包括所有的修订版)适用于本文件。

ISO/IEC 17000:2004　合格评定　词汇和通用原则(Conformity assessment—Vocabulary and general principles)

ISO 19011:2002　管理体系审核指南(Guidelines for quality and/or environmental management systems auditing)

ISO 28000　供应链安全管理体系规范(Specification for security management systems for the supply chain)

3　术语和定义

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

供应链安全管理体系已获得有资格的第三方认证的组织。

3.2

公正性　impartiality

实际存在的并被认识到的客观性。

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：客观、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

管理体系咨询和/或相关的风险评估　management system consultancy and/or associated risk assessments

参与设计、实施或保持供应链安全管理体系，以及实施风险评估。

示例：

a) 筹划或编制手册或程序；

b) 对供应链安全管理体系的建立和实施提供具体的建议、指导或解决方案；

c) 实施内审；

d) 实施风险评估与分析。

注：如果与供应链安全管理体系或审核有关的培训课程仅限于提供可在公共场合自由获取的通用信息，那么组织培训并作为培训者参与培训不被视为咨询，即培训者不针对特定的公司提出解决方案。

4 认证机构的原则

4.1 总则

4.1.1 本章所述原则是本标准中后续的特定绩效要求和说明性要求的基础。本标准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供应链安全管理体系、过程或产品(包括服务)满足规定要求。认证的价值取决于第三方通过对管理体系、过程或产品(包括服务)进行公正、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：

a) 公正性；

b) 能力；

c) 责任；

d) 公开性；

e) 保密性；

f) 对投诉的处理。

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。

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 为获得和保持信任，认证机构必须能够证明其认证决定是基于所获得的符合(或不符合)的客观证据，且不受其他利益或其他各方的影响。

4.2.4 对公正性的威胁包括：

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供应链安全管理体系咨询的客户实施供应链安全管理体系审核属于此类威胁，因此不可接受。
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

认证机构的组织架构所支撑的人员能力是认证提供信任的必要条件。能力是经证实的有效应用适当知识和技能的本领。

4.4 责任

4.4.1 符合认证要求的责任在于客户组织而不是认证机构。

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推荐。根据审核推荐，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：审核证据应可以验证。由于审核的时间和资源有限，审核证据基于对可获取信息的抽样。对审核结论的信任程度是与抽样的恰当使用密切相关的。

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、暂停、缩小范围或撤消)的适当、及时信息的公开渠道，或公布这些信息。公开性是指可以获取或公布信息。

4.5.2 为获得或保持对认证的信任，认证机构需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与认证要求的符合性所需信息的特权，认证机构需对任何关于组织供应链安全管理体系的敏感信息、专有信息和/或与漏洞相关的信息予以保密。

4.7 对投诉的处理

依赖认证的各方期望投诉得到调查。在投诉经查明有效时，认证机构宜使依赖认证的各方相信，认证机构将对投诉进行适当的处理，并为解决投诉做出适当的努力。

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(包括对投诉的处理)等原则之间取得适当的平衡。

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

认证机构与客户组织之间应有在法律上具有强制实施力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获证客户有多个场所，则认证机构应确保授予认证并颁发证书的认证机构与获证客户之间有清晰覆盖客户每一个获认证场所的在法律上具有强制实施力的协议。该协议应清楚说明按照哪些标准和/或其他规范性文件进行认证。

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、保持、更新、扩大、缩小、暂停和撤消认证)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 认证机构最高管理层应对供应链安全管理体系认证活动的公正性做出承诺。认证机构应具有可公开获取的声明，表明其理解公正性在实施供应链安全管理体系认证活动中的重要性，对利益冲突加以管理，并确保其供应链安全管理体系认证活动的客观性。

5.2.2 认证机构应识别和分析由认证活动引起的利益冲突的可能性并将其形成文件，包括认证机构的各种关系引起冲突的可能性。有关系不一定都会引起利益冲突。但是，如果任何关系对公正性构成风险，认证机构应将其如何消除或最大限度减小此类风险形成文件，并应能向 6.2 所指的委员会证实。所做的证实应包括所有已识别的潜在利益冲突来源，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。

5.2.3 当某种关系对认证机构的公正性产生不可消除的威胁时(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。

5.2.4 认证机构不应对另一认证机构的管理体系认证活动进行认证。

5.2.5 认证机构及同一法律实体的任何其他部分不应提供供应链安全管理体系咨询和/或相关的风险评估，也不应为供应链安全管理体系咨询和/或风险评估提供报价。本条款同样适用于政府中被识别为认证机构的那一部分。

5.2.6 认证机构及其所属法律实体的任何其他部分不应向获证客户提供内部审核。本条款同样适用于政府中被识别为认证机构的那一部分。

5.2.7 如果咨询机构与认证机构之间的关系对认证机构的公正性构成了不可接受的威胁，而客户接受了该咨询机构的供应链安全管理体系咨询和/或相关的风险评估或内部审核，则认证机构不应对该供应链安全管理体系进行认证。

注 1：在供应链安全管理体系咨询和/或相关风险评估或内部审核结束后经过至少两年时间，是将对公正性的威胁降至可接受水平的一种方式。

注 2：对 5.2.2 和 5.2.4 的注：威胁认证机构公正性的关系可能源自其所有权、法人治理结构、管理层、人员、共享资源、财务、合同、营销以及给介绍新客户的人销售佣金或其他好处。

注 3：对 5.2.6 和 5.2.7 的注：由审核员提出解决方案(针对已识别的不符合或改进机会)的内部审核被视为对公正性有不可接受的威胁。

5.2.8 认证机构不应将审核外包给对认证机构的公正性构成不可接受的威胁的机构(见 7.5)。

5.2.9 认证机构活动的营销不应与提供供应链安全管理体系咨询和/或相关风险评估的机构的活动有联系。如果任何咨询机构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，参与了对客户供应链安全管理体系咨询和/或相关风险评估的人员(包

括管理人员),在咨询结束后两年内,不应被雇佣从事针对该客户的审核或认证活动。

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能使其或认证机构陷入利益冲突的情况。认证机构应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。

注:如果已知组织雇佣的审核员提供了供应链安全管理体系咨询和/或相关的风险评估,则在咨询结束后的两年内,这个事实将被视为对公正性有高度威胁。

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,并向 6.2 所指的委员会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 认证机构的组织结构应为其认证提供信任。

6.1.2 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;
b) 政策和程序实施的监督;
c) 认证机构财务的监督;
d) 审核与认证的实施和对投诉的回应;
e) 认证决定;
f) 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;
g) 合同安排;
h) 为认证活动提供充分的资源。

6.1.3 认证机构应将其组织结构形成文件,并明确管理层和其他认证人员及各委员会的任务、责任和权力。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。

6.1.4 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 维护公正性的委员会

6.2.1 认证机构的结构应维护认证机构活动的公正性,并具有一个进行下列活动的委员会:

a) 协助制定与认证活动公正性有关的政策;
b) 阻止认证机构的所有者有任何倾向使商业或其他因素妨碍其一致地提供客观的认证活动;
c) 对影响认证可信度的事宜(包括公开性和公众认识)提出建议。

注:该委员会也可被委以其他任务或职责,但这些附加的任务或职责不宜削弱其确保公正性的基本作用。

6.2.2 该委员会的组成、权限、任务、权力、成员能力和责任均应正式形成文件,并由认证机构最高管理层授权,以确保:

a) 各方利益均衡,以使任一利益方不处于支配地位(认证机构的内部或外部人员视为一个利益

方，且不宜居支配地位）；

b） 获取所有必要的信息，使其能够履行自己的职能（见 5.2.2 和 5.3.2）；

c） 如果认证机构最高管理层不尊重委员会的建议，委员会应有权采取独立措施（如报告主管部门、认可机构或利益相关方）。采取独立措施时，委员会应遵守 8.5 中与客户和认证机构相关的保密要求。

注：虽然该委员会不能代表所有利益方，但是认证机构宜识别和邀请关键利益方。这些利益方可能包括：认证机构的客户，供应链安全管理体系获证客户的顾客，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。

7 资源要求

7.1 管理层和人员的能力

7.1.1 认证机构应确保参与供应链安全管理体系审核与认证的所有人员有能力胜任其承担的工作。

认证机构应有过程来确保其人员对其运作涉及的供应链安全管理体系类型和地域有适宜的相关知识、技能和经验。

认证机构应确定与特定认证方案相关的每个技术领域所需的资格和能力，以及认证活动的每项职能所需的资格和能力。

认证机构应确定在履行特定职能前证实能力的方法，应保留确定的记录。

7.1.2 认证机构在确定认证实施人员的能力要求时，除了那些直接实施审核与认证活动的人员，还应考虑管理层和行政人员所承担的职能。

7.1.3 认证机构应有获取必要的专业知识与技能的途径，以在其运作涉及的技术领域、供应链安全要素类型和地域等方面获得与认证直接相关的建议。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 认证机构自身应有具备足够能力的人员，以对各种类型与范围的审核方案进行管理并实施其他认证工作。

7.2.2 就接触保密信息而言，认证机构应确保委派实施供应链安全管理体系认证审核的人员和技术专家，在对验证工作期间所获保密信息保守秘密方面能得到信任，并确保他们没有造成安全问题。见 7.4。

7.2.3 委派实施供应链安全管理体系审核的人员至少应具备 ISO 19011:2002 中 7.2、7.3.1、7.3.2 和 7.4 阐述的与供应链安全管理和风险分析相关的个人素质、知识、技能和教育经历。

7.2.3.1 供应链安全管理体系审核员应具备风险分析、关键控制点分析、风险管理方法学和信息保密方面的能力。包括但不限于以下方面：

a） 理解供应链安全管理标准或规范的要求（如：ISO 28000）。

b） 理解供应链流程和关键控制点分析，理解供应链相关过程和实务的知识。

c） 威胁识别：

——理解威胁，如物理的、生物的、化学的、计算机网络的和放射性的威胁。

d） 风险评估和分析：

——理解风险评估和分析的原理。

e） 风险的最小化、降低与控制：

——理解最小化、降低与管理风险的原理；

——安全方法学和技术的知识，尤其是预防措施和技术。

f） 应急的策划与准备：

——政府和第一响应者的作用的知识；

——突发事件通报原则的知识；

——突发事件缓解、响应和恢复的知识。

7.2.3.2 每一位供应链安全管理体系审核员还应成功地完成了培训(见附录C或等效的)，并能证明在安全方法学、风险分析和管理原理的理解和应用方面是有能力的，同时宜是注册的管理体系审核员。

7.2.3.3 每一位供应链安全管理体系审核员应参加与其特定的资格要求相适应的持续培训。认证机构应每年评审针对其审核员的目标培训计划，培训内容包括：安全方法学、风险分析与管理原理、关键控制点分析、审核技巧、特别是7.2.3.1提到的能力要求。培训应：

a) 基于对上述学科和能力项进行需求分析的结果而策划；

b) 保留培训记录；

c) 包括审核案例分析以评价审核员的能力；

d) 有信息支持且审核员宜能获取这些信息，如：适用的管理体系标准应用的解释，常见问题解答，研讨会记录、针对案例的标准的纠正；

e) 按照培训要求得到评价，且认证机构应根据培训效果采取适当的措施；

f) 由有资格的培训教师实施。

7.2.3.4 供应链安全管理体系审核员应具备至少五年与风险分析和管理相关的经历，或者两年按照最佳行业实践及标准审核的经历。

7.2.3.5 供应链安全管理体系审核员应保证每年至少五次的相关审核，或者每年至少完成10人日的现场审核，以保持其资格。

7.2.3.6 认证机构应能证明每一位审核员在被认为有能力的特定专业类别具有恰当的培训和工作经历，并记录能力(ISO 19011:2002中5.5 c)。

7.2.4 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。

7.2.5 认证机构应使所有有关人员清楚自己的任务、责任和权力。

7.2.6 认证机构应有明确的过程来选择、培训、正式任用和监视审核员以及选择认证活动使用的技术专家。审核员的初始能力评价应包括一次对被评价者现场审核的观察。

7.2.7 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恰当的知识与技能。这一过程应基于ISO 19011提供的指南转化为适当的文件要求(特别见ISO 19011:2002中的第7章及附录C)。

7.2.8 供应链安全管理体系审核员应具备适用于所审核的供应链、工业和商业领域的安全知识和经验。

7.2.9 供应链安全管理体系审核员应具有或经过培训获得并证实附录D所描述的能力。

7.2.10 能力应通过笔试进行验证，考试的及格线设定宜仅使那些证实全面理解模块内容且达到课程目标的人员通过。

7.2.11 认证机构应确保审核员(需要时，包括技术专家)熟悉认证活动、认证要求、审核方法和其他相关要求。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。

7.2.12 认证机构应仅使用审核员和技术专家从事已证实他们具备能力的那些认证活动。

注：为特定审核组指派审核员和技术专家的要求见第9章。

7.2.13 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，以使他们获得认证要求和过程的知识。

7.2.14 做出授予、保持、更新、扩大、缩小、暂停或撤消认证等决定的小组或个人应具备足够的知识和经验，以评价审核过程和审核组的推荐意见。

7.2.15 认证机构应确保所有参与审核和认证活动的人员均有令人满意的表现。认证机构应有形成文件的程序和准则，以根据这些人员的使用频率及其活动的风险水平来监视和衡量他们的表现。认证机构尤其应根据人员的表现来复核他们的能力，以识别培训需求。

7.2.16 形成文件的审核员监视程序应把现场见证、审核报告复核及客户或市场反馈相结合，并应基于ISO 19011提供的指南转化成适当的文件要求。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)。

7.2.17 认证机构应定期对每位审核员的表现进行现场见证。现场见证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明确的适用的政策和程序。该协议应含有关于资格、保密及独立于商业和其他利益的条款，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。

认证机构应确保所有独立的外部审核员和技术专家都经过了安全调查，并且受到认证机构保密协议的约束。

注：依据上述协议使用单个审核员和技术专家不构成7.5所述的外包。

7.4 人员记录

认证机构应保持认证活动涉及每个人的最新记录，包括相关的资格、培训、经历、隶属关系、专业状况和能力。

7.4.1 安全调查

认证机构应建立对候选供应链安全管理体系审核员进行安全审查的过程并形成文件。

认可机构也应确保其评审员满足这些要求。

对审核员安全审查的过程应形成文件，并应通过适当方式使申请供应链安全管理体系认证或审核的组织以及其他利益相关组织(适用时)能够获得。

审核员应由其所在认证机构进行安全调查。安全调查过程应包括以下内容。

7.4.2 背景核查

认证机构应对所有人员和承担供应链安全管理体系审核的审核员与技术专家进行犯罪背景的核查。可行时，这些核查应凭借国家安全核查机构或警方。否则，认证机构应在最高管理层监督之下，通过内部审查过程进行记录核查和安全调查的审查评价/面试，来核查人员的适宜性和诚实性。审查过程应包括对候选供应链安全管理体系审核人员所提交证明文件的审查、面试以及对诸如护照、身份卡、工作许可证、驾驶执照和工作介绍信等文件的审查。实施供应链安全管理体系审核员面试的人员应按本标准7.4.3的过程接受任命和审查。

7.4.3 面试

认证机构应建立一个在最高管理层监督之下的分级面试制度。

最高管理层应指定一名经过面试和审查已确认值得信赖且具备必要的能力和判断力的负有责任的管理者，对候选供应链安全管理体系审核员和技术专家进行审查。该负有责任的管理者应通过审查候选人所提交的证明文件、面试和持续监视来评价候选供应链安全管理体系审核员和技术专家的可信度与适宜的行为特征。

7.4.4 工作经历

每位候选供应链安全管理体系审核员应能提供至少五整年的连续工作经历的证据，这些经历应经过当前或以往雇主的证实。自我聘用的候选供应链安全管理体系审核员应提供其他适当的证明文件，以证明雇用记录具有同等信心和可信度。

7.4.5 身份卡(ID卡)

应发给每位供应链安全管理体系审核员一张存有下列信息的身份卡(ID卡)：

——照片；

——姓、名；

——国籍；

——卡号；

——认证机构的名称和徽标；

——防止更改和伪造的标志和特征。

需要时，接受审核的组织应当可以获得供应链安全管理体系审核员的保密承诺。

7.4.6 记录

认证机构的程序应包括对违约的供应链安全管理体系审核员实施处理的过程，宜包含调查期间对审核员实施暂停等组织纪律程序。认证机构应按其认为并证明恰当的期限保存记录。确定记录保存期限时宜考虑到国家、国际或其他法定要求。

7.4.7 审核员责任

宜使审核员明白并做出书面声明，表明其知道违规行为将可能导致纪律处罚、民事责任和刑事诉讼。

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(包括资格、保密和利益冲突)签订在法律上具有强制实施力的协议。

注1：这里可包括外包给其他认证机构的情况。依据合同使用审核员见7.3。

注2：本标准中，“外包”与“分包”视为同义词。

7.5.2 认证决定不应外包。

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) 对授予、保持、更新、扩大、缩小、暂停或撤消认证负责；

c) 确保外包服务承担机构使用的人员符合认证机构的要求和本标准的适用要求，包括能力、公正性和保密；

d) 确保外包服务承担机构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)；

e) 由特定机构提供外包服务应征得客户的同意；

f) 负责处理申诉和投诉。

7.5.4 认证机构应有形成文件的程序，以对认证活动的所有外包服务承担机构进行资格审查和监视，且应保持其审核员资格的记录。

8 信息要求

8.1 公开信息

8.1.1 认证机构应保持并在有请求时提供关于其活动及其运作地域的信息。

8.1.2 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。

8.1.3 认证机构应使授予、暂停或撤消认证的信息可公开获取。

8.1.4 当任何一方提出请求时,认证机构应提供确认某一认证是否有效的途径。

注 1:如果信息分散在多个来源(如印刷文件或电子文档,或两者结合),宜通过一个系统(如唯一性编码系统或互联网上的超级链接)来确保可追溯性并避免不同来源之间的歧义。

注 2:在特殊情况下,可根据客户的请求(如出于安全原因)对某些信息的公开程度做出限制。

8.2 认证文件

8.2.1 认证机构应以其选择(见 8.1.4 中注 1)的任何方式向获证客户提供认证文件。

8.2.2 认证文件的生效日期不应早于认证决定的日期。

8.2.3 认证文件应标明:

a) 获得供应链安全管理体系认证的客户组织的每一场所的名称和可识别的物理位置;

b) 授予、扩大或更新认证的日期;

c) 与再认证周期相一致的认证有效期;

d) 唯一的识别代码;

e) 审核获证客户时所用的标准和(或)其他规范性文件,包括版本和(或)修订;

f) 与客户供应链安全管理体系内所从事活动相适宜的认证范围,包括服务、过程等,适用时包括每个场所的认证范围;

g) 认证机构的名称和(或)认证标志;

注:在认证机构获得相应授权的情况下,可以带有其他标志(如认可标识);然而,认证机构作为证书颁发机构宜保证标志不产生误导和含混不清。

h) 认证用标准所要求的任何其他信息。

8.3 获证客户目录

认证机构应以其选择的任何方式保持有效认证的目录,并使其可公开获取。该目录应至少说明每个获证客户的名称、相关的规范性文件、活动和组织要素的范围和地理位置(国家和城/镇)。

注:该目录是认证机构的专有资产。

8.4 认证资格的引用和标志的使用

8.4.1 认证机构对其授权获证客户使用的任何标志应有管理政策。该政策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消费者所见的产品包装之上,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 提供了对使用第三方标志的指南。

8.4.2 认证机构不应允许其标志被用于实验室检测、校准或检查的报告,这里将此类报告视为产品。

8.4.3 认证机构应要求客户组织:

a) 在传播媒介(如互联网、文件、宣传册或广告)中引用认证状态时,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) 在其认证被暂停或撤消时，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 9.6.3 和 9.6.6）；

e) 在认证范围被缩小时，修改所有的广告材料；

f) 不允许在引用其供应链安全管理体系认证资格时，暗示认证机构对任何供应链或供应链中任何要素进行了认证；

g) 不得暗示认证适用于认证范围以外的活动；

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。

8.4.4 认证机构应正确地控制其所有权，并采取措施识别和处理认证状态的错误引用或认证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、撤消认证、公告违规行为以及必要的法律措施。

8.5 保密

8.5.1 认证机构应具有政策和相关安排，以确保其各个层次（包括代表其活动的委员会、外部机构或个人）对从事认证活动时获得、产生的保密信息予以保密，并通过在法律上具有强制实施力的协议落实上述政策和安排。

8.5.2 认证机构应将其拟对公众公开的信息（如 4.5.1 与 8.3 中定义的）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。

8.5.3 除本标准有要求外，关于特定客户或个人的信息，未经其书面同意，不应向第三方披露。当法律或法定机构要求认证机构向第三方提供保密信息时，除法律限制或法定机构的要求外，认证机构应将拟提供的信息提前通知有关客户或个人。

8.5.4 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。

8.5.5 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，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。

8.5.6 认证机构应能获得并使用确保保密信息（如文件、记录）安全处理的设备/设施。

8.5.7 认证机构向其他机构（如认可机构、建立在同行评审基础上的协议集团）公开保密信息时，应将这一行动通知相关的监管机构及其客户。

8.6 认证机构与其客户间的信息交换

8.6.1 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、保持、缩小、扩大、暂停、撤消认证以及再认证的过程。

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) 认证机构对拟接受审核的客户的要求：

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）提供条件。

e) 对获证客户根据 8.4 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) 投诉和申诉处理程序的信息。

8.6.2 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。

注：为确保实施本条款，认证机构可能需要与获证客户在合同中做出安排。

8.6.3 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，以确保获证客户及时将可能影响供应链安全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，例如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) 获证供应链安全管理体系覆盖的运作范围；
e) 供应链安全管理体系和过程的重大变更。

8.6.4 供应链安全管理体系的信息

认证机构应制定程序，确保客户供应链安全管理体系运行的信息能够在认证机构、客户和允许获得信息的其他相关方之间可靠传递。认证机构应确保将该程序及时通知客户和其他相关方。

9 过程要求

9.1 适用于所有审核的通用要求

9.1.1 审核方案应包括至少由两阶段构成的初次审核、监督审核和再认证审核。审核方案的确定和任何后续调整应考虑客户组织的规模，其供应链安全管理体系和过程的范围与复杂程度，以及经过证实的供应链安全管理体系有效性水平和以前审核的结果。

9.1.2 认证机构应确保其审核计划基于 ISO 19011 中为编制审核计划提供的指南所转化成的适当的文件要求。应为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。

9.1.3 认证机构应有根据实现审核目标所需的能力来选择和任命审核组(包括审核组长)的过程。该过程应基于 ISO 19011 提供的指南转化成的适当的文件要求。

9.1.4 认证机构应有正式的规定和/或合同条款来确保每个审核组成员以公正的方式开展工作。每位审核组成员应在接受审核委托前，将任何已知的现在、以前或可预见到的与受审核组织的关系情况告知认证机构(见 5.2.9、5.2.12 和 7.4)。

9.1.5 认证机构应按照形成文件的程序确定审核时间，用以在认证范围所包含的场所中完成对客户供应链安全管理体系的完整而有效的审核。

9.1.6 安全威胁对于每一个业务场所都是独特的，因此一个组织认证范围内的所有业务场所均应接受审核。组织应对每一个场所进行了威胁及风险评估并应实施相应的运行控制。同样，对于非业务场所(如提供行政支持服务的场所)的安全威胁也是独特的，但其活动的特性可能对供应链安全只构成较低的风险。认证机构应对所有的业务场所进行审核，且对其他非业务场所进行风险评估并实施与其风险相称的审核。

认证机构确定的每一个场所/地点的审核时间和确定审核时间的合理性应基于附录 A 和附录 B 的要求，并应予以记录。在确定审核时间时，认证机构宜考虑(但不限于)以下方面：

a) 相关供应链安全管理体系标准的要求；
b) 复杂程度；
c) 规模；
d) 风险；
e) 技术和法规环境；
f) 场所的数量和对多场所的考虑。附录B给出了对运行多场所组织的要求。

审核人日数应基于附录A中的人日表。虽然附录A是资料性附录，但是对于一个供应链上运营的公司，审核人日数不太可能少于附录A给出的人日数。

9.1.7 对于经营多个业务场所的组织，即使这些场所的活动实质上相同，抽样也是不适宜的。认证范围中的每一个场所都应被审核到，然而，当一些场所的供应链安全管理体系及活动相同时，或许可减少这些场所的审核时间；或者，当一些非业务场所主要从事行政活动且对供应链安全没有重大影响时，可以对这些非业务场所抽样。在这些情况下，认证机构应对每一个场所进行风险评估并制定一个基于风险的审核方案，该过程应确保认证机构对组织的供应链安全管理体系进行恰当的审核。此要求在附录B中有进一步的描述。

9.1.8 当审核计划的编制工作被分配给审核组长以外的其他人员时，审核组长应对计划进行评审并批准。

9.1.9 认证机构应明确说明审核组的任务，并告知客户组织。认证机构应要求审核组：

a) 检查和验证客户组织与供应链安全管理体系相关的结构、方针、过程、程序及相关文件(记录)；
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、实施并保持了过程和程序，以便为建立对客户组织供应链安全管理体系的信任提供基础；
d) 告知客户其方针、目标、指标和结果之间的任何不一致，以使其采取措施。

9.1.10 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，以使客户组织能够对某一审核员或技术专家的任命表示反对，并在反对有效时使认证机构能够重组审核组。

9.1.11 认证机构应提前与客户组织就审核计划进行沟通，并商定审核日期。

9.1.12 认证机构应有实施现场审核的过程。该过程应基于由ISO 19011中提供的指南转化成的适当的文件化程序。

注1：除了访问有形场所(如工厂)外，“现场”还可以包括远程访问包含供应链安全管理体系评价相关信息的电子化场所。

注2：ISO 19011中的术语“受审核方”指被审核的组织。

9.2 初次审核与认证

9.2.1 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) 申请组织的一般特征，包括其名称、物理场所的地址、过程和运作的重要方面以及任何相关的法律义务；
c) 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；
d) 申请组织寻求认证的标准或其他要求；
e) 接受与供应链安全管理体系有关的咨询的情况。

9.2.2 申请评审

9.2.2.1 在实施审核前，认证机构应对认证申请及补充信息进行评审，以确保：

a) 关于申请组织及其供应链安全管理体系的信息充分，可以进行审核；

b) 认证要求已有明确说明并形成文件，且已提供给申请组织；

c) 解决了认证机构与申请组织之间任何已知的理解差异；

d) 认证机构有能力并能够实施认证活动；

e) 考虑了申请的认证范围、申请组织经营场所的位置和数量、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)；

f) 应保持决定实施审核的理由的记录。

9.2.2.2 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(见 7.2.7)。

9.2.2.3 如果认证机构考虑申请组织已获得认证或接受的其他审核，则应收集充足的、可验证的信息，以证明对审核方案的任何调整的合理性，并予以记录。

9.2.2.4 完成申请评审后，认证机构应向申请者通报是否接受了申请。不接受申请的原因应传达给申请者。

9.2.2.5 在开始审核之前，认证机构应和申请组织签订一份协议(见 5.1.2)，该协议：

a) 明确开展工作的范围，包括拟认证的范围和场所的具体情况；

b) 要求申请组织提供认证所需的所有信息；

c) 要求申请组织遵守认证要求。

9.2.2.6 对于扩大认证范围的申请，认证机构应进行可行性评审和必要的审核活动，来确定是否可以准予该范围的扩大。

9.2.2.7 认证机构应任命(见 9.1.3)审核组。组成审核组的所有审核员(必要时，还有技术专家)作为一个整体应具备认证机构按 9.2.2.2 确定的对申请组织实施认证的能力。认证机构应根据审核员和技术专家具备的能力(如 7.2.5 所述)来选择审核组，并可以使用内部和外部的人力资源。

9.2.2.8 认证机构应指定将进行认证决定的人员，以确保具有实施认证决定的适宜能力(见 7.2.9)。

9.2.2.9 审核组需要具备一定的背景，以确保成员理解与所审核体系有关的要求。每个审核组都应对其审核的体系所属的技术与行业部门具备总体上的理解和背景。审核组应有能力确定一个特定的供应链安全管理体系是否充分满足标准的要求。

9.2.2.10 上文要求：认证机构委派实施供应链安全管理体系审核的每个审核组需要知道，对通常的过程和程序，哪些要素对所审核的供应链是必需的。审核组应具备必要的能力(包括行业或监管方面的资质)，在确保体系满足规定要求方面有足够信心确定体系是否覆盖了这些必需的要素。

9.2.2.11 在某些情况下，特别是当有关键要求和特殊程序时，审核组的背景知识可以通过情况介绍会、专项培训或专家参与的方式加以补充。认证机构可以给审核组加派非审核员的专家。如果认证机构使用技术专家，那么认证机构的管理控制体系应对这种情况做出规定，并且为保持其能力最新做出安排。文件中应包括如何选择技术专家以及如何保证其能力的具体细节。认证机构可以依靠外部帮助，如工业或专业机构。

认证机构应确保执行本条款的人员受到和审核员一样的保密性和公正性要求的约束。

9.2.3 初次认证审核

供应链安全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。

9.2.3.1 第一阶段审核

9.2.3.1.1 第一阶段审核应编制审核计划，审核计划应包括 9.1.2 和 9.2.3.1.2 规定的要点。

9.2.3.1.2 通常，审核组对客户组织的供应链安全管理体系的第一阶段审核应在现场进行。在特殊情况下，第一阶段可以不进行现场访问。不进行现场访问的决定应有正当理由并予记录，且应告知客户这样做可能会给第二阶段的审核带来风险。该理由宜基于组织的规模、位置、风险的考虑和已了解到的情况等。

9.2.3.1.3 第一阶段审核应：

a) 评价申请组织的场所和现场的具体情况，并与客户组织的人员进行讨论，以确定第二阶段审核的准备情况；

b) 审查客户组织理解和实施标准要求的情况，特别是对供应链安全管理体系的关键绩效或重要因素、过程、目标和运作的识别情况；

c) 收集并审查关于客户组织的供应链安全管理体系范围、已完成的风险评估、过程和场所的必要信息，以及相关的法律法规要求和遵守情况(如：申请组织运作相关的法律因素和识别的风险等)；

d) 审查第二阶段审核所需资源的配置情况，并与客户组织商定第二阶段审核的细节；

e) 结合可能的重要因素充分了解客户的供应链安全管理体系和现场运作，以便为策划第二阶段审核提供关注点；

f) 评价客户组织是否策划和实施了内部审核与管理评审，以及供应链安全管理体系的实施程度能否证明客户组织已为第二阶段审核做好准备。

9.2.3.1.4 认证机构应将第一阶段审核结果形成文件并告知客户组织，包括识别任何引起关注的、在第二阶段审核中可能被判定为不符合的问题。

9.2.3.1.5 对于第一阶段审核过的供应链安全管理体系的任何部分，被确定为实施充分、有效并符合要求的，第二阶段可以不必再对其审核。然而，认证机构应确保供应链安全管理体系中已审核的部分持续符合认证要求。在这种情况下，第二阶段的审核报告中应包含这些审核发现，并清楚地表述第一阶段审核已经确立的符合性。

9.2.3.1.6 认证机构在确定第一阶段审核和第二阶段审核的间隔时间时，应考虑客户解决第一阶段审核中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审核的安排。

9.2.3.2 第二阶段审核

9.2.3.2.1 第二阶段审核应编制审核计划(见 9.1.2)。计划应遵循 ISO 19011 中的指南转化成的适当的文件要求，并应该考虑在第一阶段审核中获得的信息。

9.2.3.2.2 第二阶段审核应在客户组织的现场进行。第二阶段审核的目的是评价客户供应链安全管理体系的实施情况和有效性。

9.2.3.2.3 审核组应进行第二阶段审核以收集供应链安全管理体系符合标准和其他认证要求的审核证据。

9.2.3.2.4 审核组应审核足够数量的关于客户组织供应链安全管理体系以及对供应链安全管理体系的实施情况包括有效性进行合理评价的活动的样本。

9.2.3.2.5 作为审核的一部分，审核组应访问足够数量的员工，包括最高管理层和所审核设施的操作人员，以确保体系在客户组织中的各个部分得到实施和理解。

9.2.3.2.6 审核组应对在第一阶段和第二阶段审核中收集的所有信息和审核证据进行分析，以确定与所有认证要求的符合程度和不符合。审核组可以提出改进机会的建议，但是不应建议具体的解决方法。

9.2.3.2.7 第二阶段审核应至少覆盖对组织供应链安全管理体系以下方面的检查：

a) 与适用的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，对绩效进行的监视、测量、报告和评审；

c) 组织的供应链安全管理体系以及在遵守法律法规方面的绩效；

d) 运作控制；
e) 内部审核和管理评审；
f) 针对客户组织方针的管理职责；
g) 规范性要求、方针、绩效目标和指标、适用的法律要求、职责、人员能力、运作、程序、绩效数据和内部审核结果之间的联系。

9.2.3.2.8 完成第二阶段审核后应采取的行动至少应包括以下内容：
a) 离开审核地点前，应将所有确定并达成一致的不符合的记录留给客户；
b) 按照 9.2.4 的要求编制审核报告。

9.2.3.2.9 缺少或未能实施和保持符合一个或多个供应链安全管理体系要求，或者根据已有的客观证据，对组织持续满足要求的能力和供应链安全管理体系的有效性产生重大怀疑的情况，应该被确定为不符合。

认证机构可以规定缺陷和待改进的区域的不同等级(如严重和一般不符合，观察项等)。

9.2.4 初次认证的审核报告

9.2.4.1 认证机构应有形成文件的报告程序。

9.2.4.2 第一阶段的审核报告应包括对供应链安全管理体系文件的充分性、组织对关键绩效或重要因素的分析以及供应链安全管理体系的实施程度是否表明可以进行第二阶段审核的意见。第一阶段审核报告应对 9.2.3.1.3 要求的内容进行报告。

9.2.4.3 第二阶段审核报告应基于 ISO 19011 中的指南转化成的适当的文件要求来编制。

9.2.4.4 审核组提交给认证机构的审核报告应至少包括或涉及以下内容：
a) 注明审核客户。
b) 注明受审核方代表。
c) 注明认证机构。
d) 注明审核组组长和组员。
e) 审核目的。
f) 审核范围，尤其注明所审核的组织和职能单元或过程、所覆盖的时期及所评价的供应链要素。
g) 审核准则。
h) 引用的供应链安全管理标准和/或使用的其他规范性文件。
i) 现场审核活动的实施日期和场所，以及上次审核的日期。
j) 审核发现：
   1) 关于供应链安全管理体系实施情况和有效性的最重要的评论的总结，包括正面和负面的；
   2) 关于风险评估方法实施情况和有效性的最有建设性/有益的信息的概述和总结，包括正面和负面的；
   3) 审核中提出的针对具体标准要求的不符合；
   4) 上述每个不符合的关闭情况报告。
k) 审核结论：
   1) 供应链安全管理体系和风险评估方法的可信度；
   2) 审核组的推荐意见。

9.2.4.5 形成文件的程序至少应确保：第二阶段审核后，在双方同意的期限内，向受审核组织提交一份书面的客户审核报告。该报告包括供应链安全管理体系的有效性以及与所有标准要求符合性的正面与负面的审核发现与结论，尤其要包括内审过程的有效性和方针承诺的实现情况，还包括确定的任何不符合。

9.2.4.6 审核报告的所有权应归认证机构所有。当报告的内容包含安全敏感信息时，审核报告可以委

托组织保管，但审核报告的所有权和修改权仍归认证机构所有。

9.2.5 审核后续活动

9.2.5.1 为纠正已识别的不符合，认证机构应要求受审核组织说明为在规定的期限内消除所发现的不符合及其原因已采取或拟采取的具体纠正和纠正措施。

9.2.5.2 如需进行全面或部分的补充审核，或需要形成文件的证据（在后续的监督审核中予以确认），以确保纠正和纠正措施的有效性，认证机构应告知受审核的组织。这将根据所确定的不符合的类型和数量来确定。

9.2.5.3 认证机构应审查受审核组织所采取的纠正和纠正措施，以确定其充分性，如果已实施，则确定其有效性。

9.2.6 授予初次认证或扩大认证

9.2.6.1 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) 9.2.4 所指的报告；
b) 对不符合和对客户组织采取的纠正及纠正措施的意见；
c) 对提供给认证机构用于申请评审（见 9.2.2）的信息的确认；
d) 对是否授予认证的推荐性意见及附带的任何条件或评论。

9.2.6.2 认证机构应在评价审核结果和任何其他相关信息（如公共信息、客户对审核报告的意见）的基础上做出认证决定。

9.2.6.3 认证机构应确保参与认证决定的人员或委员会不是实施审核的人员。

9.2.6.4 认证机构在做出决定前应确认：

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) 对于属于下列情形之一的所有不符合，认证机构已经审查并接受了满足要求的纠正和纠正措施（包括为消除原因以防止再发生的措施）：
   1) 缺少或未能实施和保持符合一个或多个供应链安全管理体系的要求；或
   2) 根据已有的客观证据，对客户组织持续满足要求的能力和供应链安全管理体系有效性产生重大怀疑的情况。
c) 对于任何其他不符合，认证机构已接受了组织计划采取的纠正和包括防止再发生的纠正措施。

9.3 监督活动

9.3.1 总则

9.3.1.1 认证机构应对其监督活动进行设计，以便定期对供应链安全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供应链安全管理体系的变更情况。

9.3.1.2 监督活动应包括对获证客户供应链安全管理体系满足认证所依据标准及其他规范性文件规定要求的情况进行评价的现场审核。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和记录（纸质或电子介质）；
d) 其他监视获证客户绩效的方法。

9.3.1.3 认证机构应制定方案间隔足够短的时间实施定期的监督审核，以确认获证的供应链安全管理体系持续满足全部认证要求且持续有效。

9.3.1.4 初次认证后第一次监督审核的日期应从初次审核第二阶段结束时（如末次会议的日期）算起。

9.3.2 监督审核

9.3.2.1 监督审核是现场审核，但不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供应链安全管理体系在认证周期内持续满足要求保持信任。年度监督审核方案至少应包括对以下方面的审查：

a) 内部审核、安全评估与策划和管理评审；
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) 供应链安全管理体系在实现获证客户目标方面的有效性；
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。

9.3.2.2 监督审核应至少每年进行一次。

9.3.2.3 监督审核应编制审核计划(见 9.1.2)。

9.3.2.4 认证机构确定监督审核的审核时间时应考虑附录 A 中的指南并适当考虑下列因素：

a) 供应链过程和要素的风险种类；
b) 供应链要素、场所、过程和产品的数量；
c) 涉及供应链安全的雇员数量；
d) 随机抽样的规模；
e) 上次审核所发现不符合的数量；
f) 组织、产品或过程的变化。

9.3.3 监督审核报告

9.3.3.1 对于监督审核，审核组的报告应包括：

a) 所审核的供应链安全管理体系标准要求；
b) 认证要求满足情况的意见，包括有效性；
c) 上次审核发现的每个不符合的纠正措施实施有效性的验证情况；
d) 任何新的不符合。

此报告应基于 ISO 19011 中的指南所转化成的适当的文件要求来编制。

9.3.3.2 此报告应提交给获证客户和认证机构。

9.3.3.3 在监督审核中，当出现不符合或缺乏符合性证据时，认证机构应规定实施纠正和纠正措施的时限。

注：建议时限基于不符合的严重性和影响程度。

9.3.3.4 如需进行全面或部分的补充审核，或需要形成文件的证据(在后续的监督审核中予以确认)，以确保纠正和纠正措施的有效性，认证机构应告知受审核组织。这将根据所确定的不符合的类型和数量来确定。

9.3.4 保持认证

认证机构应在证实获证客户持续满足供应链安全管理体系标准要求后保持认证。认证机构满足下列条件时，可以根据审核组长的肯定性建议保持对组织的认证，而无需进一步的独立复核：

a) 对于任何可能导致暂停或撤消认证的不符合或其他情况，认证机构有制度要求审核组长启动由具能力相称(见 7.2.9)且未实施该审核的人员进行的复核，以确定能否保持认证；

b) 组长知道处理不符合和任何后续纠正措施的准则；
c) 认证机构有能力相称的人员对监督活动进行监视(包括对审核员的报告活动进行监视)以确认认证活动运作有效。

9.4 再认证

9.4.1 再认证周期

初次认证审核与再认证审核，或两次再认证审核之间的时间间隔不应超过3年。

9.4.2 再认证审核的策划

9.4.2.1 认证机构应策划和实施再认证审核，以评价获证客户是否持续满足相关规范性文件的所有要求。再认证审核的目的是确认供应链安全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。

9.4.2.2 再认证审核应考虑供应链安全管理体系在整个认证周期内的绩效，包括调阅以前的监督审核报告(见9.3.3)。

9.4.2.3 当供应链安全管理体系、获证组织或供应链安全管理体系的运作环境(如法律的变更)没有重大变更时，再认证审核活动不必进行第一阶段审核。

9.4.2.4 认证机构对于多场所或对多个供应链安全管理体系进行认证时，审核的策划应确保现场审核具有足够的覆盖范围，以提供对认证的信任。

9.4.2.5 宜考虑近期监督审核和获证客户内部审核的结果。审核策划应基于ISO 19011中的指南转化成的适当的文件要求。

9.4.2.6 再认证审核的审核时间应依据附录A中的指南确定。

9.4.3 再认证审核

再认证审核应包括现场审核(可以代替或扩展一次定期的监督审核)。再认证审核应关注下列供应链安全管理体系要求：

a) 供应链安全管理体系过程间有效的相互作用；
b) 结合内部和外部变更来看的整个供应链安全管理体系的有效性；
c) 经证实的对保持供应链安全管理体系有效性和改进，以提高整体绩效的承诺；
d) 获证供应链安全管理体系的运行促进组织方针和目标的实现。

9.4.4 再认证审核报告

9.4.4.1 对于再认证审核，审核组提交给获证客户和认证机构的审核报告应包括对于以下方面的意见：

a) 所审查的供应链安全管理体系，包括风险分析；
b) 认证要求的满足情况；
c) 对上次审核的每个不符合的纠正措施实施的持续有效性的审查和验证情况；
d) 受审核组织供应链安全管理体系的有效性。

9.4.4.2 在再认证审核中，当出现不符合或缺乏符合性证据时，认证机构应规定实施纠正与纠正措施的时限。

注：建议时限宜基于不符合的严重性和影响程度，且不宜太长以至于产生对认证可信性的质疑。

9.4.4.3 如需进行全面或部分的补充审核，或需要形成文件的证据(在后续的监督审核中予以确认)，以确保纠正和纠正措施的有效性，认证机构应告知受审核的组织。

9.4.5 再认证决定

9.4.5.1 认证机构应确保做出再认证决定的人员或委员会不是实施审核的人员。

9.4.5.2 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。

9.4.5.3 认证机构在做出决定前，应确认：

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) 对于属于下列情形之一的所有不符合，认证机构已经审核并接受了符合要求的纠正和纠正措施(包括为消除原因以防止再发生的措施)：

1) 未能保持满足供应链安全管理体系的一项或多项要求；

2) 根据已有的客观证据发现，对客户组织持续满足要求的能力和供应链安全管理体系有效性产生重大怀疑的情况。

c) 对于任何其他不符合，认证机构已接受了组织计划采取的纠正和包括防止再发生的纠正措施。

9.5 特殊审核

认证机构为调查投诉(见 9.8)、对变更(见 8.6.3)做出回应，可能需要在提前较短时间通知获证客户后对其进行审核。此时：

a) 认证机构应说明并使获证客户提前了解(如在 8.6.1 所述的文件中)将在何种条件下进行此类审核；

b) 由于组织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 暂停、撤消或缩小认证范围

9.6.1 认证机构应有暂停、撤消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。

9.6.2 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：

a) 客户的获证供应链安全管理体系持续地或严重地不满足认证要求，包括对供应链安全管理体系有效性的要求；

b) 获证客户不允许按要求的频次实施监督或再认证审核；

c) 获证客户主动请求暂停。

9.6.3 在暂停期间，客户的供应链安全管理体系认证暂时无效。认证机构应与其客户做出具有强制实施力的安排，以确保暂停期间避免客户继续宣传认证资格。认证机构应使认证资格的暂停信息可公开获取(见 8.1.3)，并采取其认为适当的任何其他措施。

9.6.4 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，认证机构应撤消或缩小其认证范围。

注：多数情况下，暂停不宜超过 6 个月。

9.6.5 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。

9.6.6 认证机构应与获证客户就撤消认证时的要求[见 8.4.3 d)]做出具有强制实施力的安排，以确保获证客户接到撤消认证的通知时，立即停止使用任何引用认证资格的广告材料。

9.6.7 在任何一方提出请求时，认证机构应正确说明客户的供应链安全管理体系认证被暂停、撤消或缩小的情况。

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 申诉处理过程的说明应可公开获取。

9.7.3 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。

9.7.4 申诉的调查和决定不应造成针对申诉人的任何歧视行为。

9.7.5 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。

9.7.6 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

客户和证书使用方(见 4.1.2 和 4.7)可能期望对投诉进行调查，并且如果确定有效，使他们相信投诉将得到适当处理并做出合理的努力来解决投诉。

注：有效解决投诉对认证机构、客户、授权认证机构的机构和其他认证使用方来说是防止过错、遗漏或不合理行为的一种重要方法。投诉得到适当处理时，对认证活动的信心就得到了维护。

9.8.1 对投诉处理过程的说明应可公开获取。

9.8.2 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供应链安全管理体系的有效性。

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

9.8.4 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。

9.8.5 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，包括为解决投诉而采取的措施；

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。

9.8.6 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。

9.8.7 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。

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

9.8.9 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。

9.8.10 认证机构应与客户及投诉人共同决定是否应将投诉事项及处理结果公开，并在决定公开时，共同确定公开的程度。对投诉保密的任何决定取决于与投诉相关的任何一方的要求，且应是合理的。

9.9 申请组织和客户的记录

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撤消认证的组织)保持审核及认证活动的记录。

9.9.2 获证客户记录应包括：

a) 申请资料及初次认证、监督和再认证的审核报告；
b) 任何减少审核时间的方法的理由；
c) 确定审核时间的理由(见 9.1.5)；
d) 纠正与纠正措施的验证；
e) 投诉和申诉及任何后续纠正或纠正措施的记录；
f) 适用时，委员会的审议和决定；
g) 认证决定的文件；
h) 认证文件，包括与产品(包括服务)、或过程(适用时)相关的认证范围；
i) 建立认证的可信度所需的相关记录，如审核员与技术专家资格和能力的证据。

9.9.3 认证机构应保证客户记录的安全，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(见 10.2.3)。

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。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

认证机构应建立和保持一个能够支撑并证实其始终满足本标准要求的管理体系。在建立管理体系时，认证机构应贯彻 10.1 或 10.2 的要求。

10.1 方式一：与 ISO 9001 一致的管理体系要求

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本标准要求的管理体系。该管理体系还应满足 10.1.1～10.1.4 的补充要求。

10.1.1 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。

10.1.2 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提高认证的可信性，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。

10.1.3 管理评审

为应用 ISO 9001 的要求，认证机构应将来自认证活动的使用方及利益相关方的相关投诉和申诉的信息作为管理评审的输入。

10.1.4 设计和开发

为应用 ISO 9001 的要求，认证机构在开发新的管理体系认证方案或将现有方案适于特殊情况时，应确保将 ISO 19011 中适用于第三方审核的指南作为设计输入。

10.2 方式二：通用的管理体系要求

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本标准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，以证实其对按本标准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任命一名有下列职责和权力的管理层成员，无论其是否有其他职责：

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。

10.2.1 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本标准的所有适用要求。认证机构应确保其人员可以获取手册和相关的关联文件。

10.2.2 文件控制

认证机构应建立程序以控制与本标准实施有关的文件(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) 对文件进行复审和必要的更新，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。

10.2.3 保持和销毁敏感性文件

认证机构应建立并实施程序，以确保顾客的安全敏感性文件、记录以及审核中获取的信息和数据(如审核员的笔记)在任何时候都是安全的，并应在归档和随后的销毁中合理考虑其安全等级。

经过适当水平的安全调查的认证机构员工和其他外部人员，应仅在需要时方可接触安全敏感性文件、数据和记录。

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、检索和处置与本标准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

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(包括与本标准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。

10.2.5.1 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) 审核的结果；

b) 客户和本标准实施涉及的利益相关方的反馈；

c) 预防措施和纠正措施的状况；
d) 以往管理评审的后续措施；
e) 目标的实现情况；
f) 可能影响管理体系的变更；
g) 申诉和投诉。

10.2.5.2 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) 与本标准实施有关的认证服务的改进；
c) 资源需求。

10.2.6 内部审核

10.2.6.1 认证机构应建立内部审核程序，以验证认证机构满足本标准要求，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 内部审核应至少每年进行一次。如果认证机构能够证明管理体系按照本标准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资格，熟悉认证、审核和本标准的要求；
b) 审核员不应审核自己的工作；
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。

10.2.8 预防措施

认证机构应建立采取预防措施以消除潜在不符合的原因的程序。预防措施应与潜在问题的可能影响程度相适应。预防措施程序应明确对下列方面的要求：
a) 识别潜在的不符合及其原因；

b) 评价防止不符合发生的措施的需求；

c) 确定和实施所需的措施；

d) 记录所采取措施的结果；

e) 评审采取的预防措施的有效性。

注：纠正措施和预防措施的程序不一定要分别制定。

附 录 A
（资料性附录）
对审核时间确定过程的导则

表 A.1 根据组织的雇员数、复杂程度和/或风险（见注 8）确定初次审核（第一阶段＋第二阶段）所需的审核人日数。

表 A.1 初次审核的审核人日数

有效雇员数（见注 2）	平均人日（中复杂程度和/或风险）	最少人日（低复杂程度和/或风险）	典型人日（高复杂程度和/或风险）	当组织的安全管理体系与其他管理体系标准或安全准则整合认证时的可减少量
1（见注 9）	1	1	1	0
2～10	3	3	3	0
11～30	6	4	8	＜20%
31～100	8	5	11	＜20%
101～500	12	9	15	＜20%
501～2 000	15	10	20	＜20%

注：

当审核组需要翻译协助理解书面材料时，审核时间宜在上述审核人日的基础上增加 10%，若需口头翻译，则需再增加 10%的时间。通常，第一阶段审核约占上述审核人日的 1/3，第二阶段审核占剩余的部分。

人日数的计算指南

表 A.1 中审核人日数的起点基于有效雇员数确定。

1 宜考虑组织设施、场所、体系、过程和产品/服务的所有特征，并根据表 A.1 的合理因素进行适当的调整。增加的因素和减少的因素可以相抵消。所有在该审核人日表的基础上调整审核时间的情形，均应保持充分的证据和记录以证明调整的合理性。

尤其是对大的场所和组织，为了能考虑到所有场所和设施的特征，认证机构宜获得一份场地平面图以便计算审核人日。宜考虑的因素有：场所的薄弱点；邻近的资产；道路、河流和其他通道的入口等。

2 “有效雇员”是指在组织管理体系中描述的认证范围所覆盖的人员，包括其工作对受审核组织的安全有潜在影响的非长期（季节性的、临时的和分包的）雇员。认证机构宜与受审核组织就审核时机达成一致，以便最好地反映出组织接受审核的全部范围。可酌情考虑季节、月份、日期和轮班。

非全日制雇员宜换算为等效的全日制雇员，这取决于与全日制雇员工作小时数的比较。关于轮班对有效雇员数影响的计算见注 7。在计算有效雇员数时，宜适当考虑对供应链安全有影响的人员。例如：财务部门雇员的影响可能小于直接参与手工操作过程的雇员。

3 “审核时间”包括审核员或审核组策划审核的时间（适用时，包括非现场的文件审查）；与组织和其他相关人员、记录、文件和过程接触的时间以及编制报告的时间。在分配用于策划和编写审核报告的时间时，通常不宜使总的现场审核时间少于所分配“审核时间”的 80%。这适用于初次审核、监督审核和再认证审核。如需要增加策划和/或撰写报告的时间，也不能成为减少现场审核时间的理由。审核员的路途时间不包括在审核时间中，它是表中所列审核时间之外附加的。

4 “审核时间”是以审核所花费的“审核人日”来表示的，一个“审核人日”通常指完整的 8 h 正常工作日。在最初的策划阶段，不得通过增加每个工作日的工作小时数来减少审核人日数。

5 在第一个三年认证周期中，特定组织监督审核的时间宜与初次审核的时间成比例，每一年监督审核花费的总时

间约为初次审核花费时间的1/3。所策划的监督审核时间宜时常得到审查(至少在再认证时),以便考虑组织的变化和体系成熟度等。

6 实施再认证的总时间基于对前三年认证周期内管理体系的实施及其有效性评价的结果。再认证审核所需的时间宜与同一组织的初次认证审核所用的时间成比例,不宜少于同一组织在再认证时若实施初次审核所需时间的2/3。再认证审核时间多于例行监督审核时间,但当再认证审核与计划的例行监督审核一起实施时,再认证审核也要满足监督审核的要求。

7 如果组织运作的重要部分采用轮班制,且不同班次间活动的类型和工作强度没有显著区别,雇员总数可用以下方法折算:

不轮班的雇员数+轮班的雇员数/(班数−1)

8 复杂程度宜根据组织开展业务的数量和类型来确定。风险宜根据对风险影响准则的定性评估来确定,诸如:潜在的安全威胁,成为攻击目标的产品和/或服务的类型及可能性,地理位置,当地文化,安全事件的历史及发展趋势等。

9 只有一名有效雇员的组织是所有者或经营者,例如国际道路运输联盟(IRU)安全工具包确定的系统中进行经营的卡车主经营者。

附 录 B
（规范性附录）
多场所组织的审核准则

B.1 定义

B.1.1 多场所组织

B.1.1.1 多场所组织是指由不止一个场所提供供应链安全服务的组织。

B.1.1.2 一个多场所组织可以包含一个以上的法律实体，所有场所应与组织的总部具有法律或合同联系，且从属于同一个供应链安全管理体系。该供应链安全管理体系由总部规定、建立并进行持续的监视。这意味着，总部有权要求各场所在必要时采取纠正措施。适用时，宜在总部与各场所间的协议中对此做出规定。

多场所组织的例子可能有：

——以特许经营方式开展业务的组织；

——服务公司拥有分销/仓储、运输集散地、其他场所和物流所构成的网络，各场所实施相似的过程且运行相同的程序；

——有多个提供相同服务的分支和/或经营场所的公司。

B.2 组织的资格准则

B.2.1 安全威胁对于每一个业务场所都是独特的，因此一个组织认证范围内的所有业务场所均应接受审核。组织应已对每一个场所进行了威胁和风险评估并实施相应的运行控制。同样，对非业务场所（如提供行政支持服务的场所）的安全威胁也是独特的，但其活动的特性可能只对供应链安全构成较低的风险。认证机构应对所有的业务场所进行审核，且对其他非业务场所进行风险评估并实施与其风险相称的审核。

B.2.2 然而，满足 B.2.2.1 所述的两个条件时，逐个场所实施审核的要求可以放宽。

B.2.2.1 当所有场所都提供供应链服务，所有活动实质上都相同且全部按相同的方法和程序实施时，或许可以减少组织所经营的部分场所的审核人日数。然而，所有场所的特定威胁应经组织识别并进行了风险评估且在现场审核时得到认证机构的审核。考虑减少审核时应满足以下条件。

B.2.2.1.1 为实施安全评估和开发安全计划，组织应根据集中控制的过程集中管理和运行其供应链安全管理体系，并由一个集中的系统整理和审查来自各场所的以下相关数据：

——本地体系文件和体系变化；

——管理评审；

——改进目标、指标和管理方案；

——投诉、事件和纠正措施的评估。

组织的内部审核方案和审核结果评估应覆盖全部相关场所（包括集中管理职能），且在认证机构开始审核前已按照内部审核方案对每一个场所实施了内部审核。

组织应已针对每一个场所的特定威胁进行了安全风险评估并实施相应的运行控制。

B.2.2.1.2 组织应证明其总部已依据审核标准并考虑法规要求建立了供应链安全管理体系，且整个组织均满足认证标准的要求。

B.2.3 组织应证明其有能力从包括总部在内的全部场所收集和分析数据（包括但不限于以下项目），且

在需要时有权力和能力发起组织变更：

——体系文件和体系变化；

——管理评审；

——改进目标、指标和管理方案；

——投诉、事件和纠正措施的评估；

——内部审核的策划及审核结果的评估。

组织应已针对每一个场所的特定威胁进行了安全风险评估并实施相应的运行控制，并能通过记录证明所有场所(包括认证机构不审核的场所)控制有效。

B.2.4 如偏离附录 A 所述的审核人日数，或偏离对于认证范围内的所有场所“认证机构应审核所有场所”的作法时，认证机构应实施基于风险管理方法的文件化程序，以证明偏离本标准中审核时间和“所有场所应得到审核”作法的合理性。认证机构应考虑以下因素：

——行业范围或活动(即：基于与行业或活动相关的风险或复杂程度的评估)；

——适宜于多场所审核的场所类型与规模；

——供应链安全管理体系在各地实施的差异，诸如：需考虑当地法规、行为特征、恐怖主义和犯罪统计的威胁；在供应链安全管理体系中使用供应链安全计划来处理不同活动、不同合同或法规体系；

——在组织供应链安全管理体系下运作的临时场所的用途。

B.2.5 总部保持的记录应证明供应链安全管理体系及其在所有场所(包括未被认证机构访问到的)实施的有效性。

B.3 认证机构的资格准则

开始审核之前，认证机构应向组织提供本附录规定的关于组织资格准则的信息，如果准则的任何方面未得到满足，不宜继续进行。开始审核前宜告知组织，若在审核中发现与这些准则相关的不符合，将不会颁发认证证书。

B.3.1 合同评审

B.3.1.1 认证机构的程序宜确保最初的合同评审对拟认证的供应链安全管理体系所覆盖的活动的复杂程度和规模以及各场所间的差异加以识别，以作为确定抽样水平的基础。

B.3.1.2 认证机构应确定组织的总部作为其实施认证的合同方。

B.3.1.3 针对每个实例，认证机构宜核查各场所间在何种程度上按照相同的程序和方法生产或提供本质上属同类的产品或服务。认证机构只有在经核实确信拟包括在该多场所任务中的全部场所都符合组织的资格准则后，才可将抽样程序应用于该实例。

B.3.1.4 如果一个服务性组织中实施认证所覆盖的活动所在的全部场所没有同时准备好进行认证时，应要求组织事先告知认证机构拟包含在证书中的场所。

B.3.2 审核

B.3.2.1 在多场所程序之下，认证机构应有形成文件的程序来处理审核，这些程序应建立方法尤其使认证机构确信：同一个供应链安全管理体系管理着所有场所的活动并实际应用到了所有场所，B.2 中的所有准则均得到满足。

B.3.2.2 如果不止一个审核组参与了整个网络的审核/监督，认证机构宜指定一名审核组长负责汇总所有审核组的审核发现并编写一份总报告。

B.3.3 处理不符合

B.3.3.1 通过组织的内部审核或认证机构的审核，在任何一个场所发现不符合时，宜调查以确定其他场所是否可能受到影响。因此，认证机构宜要求组织对不符合进行审查以确定是否意味着适用于所有场所的全面的系统缺陷。若是，宜在总部和每一个场所采取纠正措施；否则，组织宜能向认证机构证明其采取有限的后续措施的合理性。

B.3.3.2 认证机构应要求提供上述措施的证据，并提高抽样频次直至对重新建立的控制措施感到满意为止。

B.3.3.3 在做认证决定过程中，若某一场所的活动存在不符合，可能对其他场所运作的符合性造成不利影响时，认证机构在得到满意的纠正措施前可以拒绝对整个网络认证。

B.3.3.4 在认证过程中，组织为克服由单一场所存在不符合造成的认证障碍，而力图把“有问题”的场所排除在认证范围之外，是不可接受的。

B.3.4 认证证书

B.3.4.1 应向组织颁发一份带有组织总部名称和地址的认证证书，认证相关的所有场所的名单应发布在认证证书或者认证证书引用的附录或其他文件上。证书的范围或其他引用文件中应清楚地注明，获得认证的活动是由名单上的场所构成的网络履行的。如果颁发给多场所的认证范围仅是组织总范围的一部分，应在认证证书和附录中清楚地表明所有场所的适用认证范围。

B.3.4.2 可向认证覆盖的每一场所颁发一份子证书，子证书应包含认证范围的全部或部分，并清楚地引用主证书。

B.3.4.3 如果总部或任何场所不满足保持认证必需的准则(见 B.3.2)，证书将被全部撤销。

B.3.4.4 认证机构应保持最新的多场所名单，意味着认证机构应要求组织向它通报任何场所的关闭。认证机构视未提供这些信息为认证证书误用，将按程序采取相应的措施。

B.3.4.5 经监督/再认证审核活动增加的场所可添加在已有的证书上。认证机构应有增加新场所的程序。

注：临时场所(例如，为实施特定活动组织因具体的运作或合同目的而获取或动用的场所)不应被包括在多场所认证方案中。

附 录 C
（规范性附录）
审核员的教育、工作和审核经历及培训时间

从事认证或类似审核的审核员的教育、工作经历、审核员培训和审核经历的水平示例见表 C.1。

表 C.1 从事认证或类似审核的审核员的教育、工作经历、审核员培训和审核经历的水平示例

项目	审核员	有其他管理体系经历的审核员	审核组长
教育	中等教育(见注 1)	同审核员要求	同审核员要求
全部工作经历	5 年(见注 2)	同审核员要求	同审核员要求
安全方面的相关工作经历(见注 8)	5 年全部工作经历中至少有 2 年，或者经过附录 D 所描述的培训	同审核员要求	同审核员要求
审核经历	作为实习审核员，在能胜任审核组长的审核员的指导和引领下完成 4 次完整审核且不少于 20 天的审核经历(见注 5)。审核宜在最近的连续 3 年内完成	至少 1 次覆盖审核规范或标准全部条款的完整审核，且结果满意(见注 5)	作为审核组长，在能胜任审核组长的审核员的指导和引领下完成 3 次完整审核且不少于 15 天的审核经历(见注 5)。审核宜在最近的连续 2 年内完成。(见注 7)
审核员培训	40 h 培训，包括： 16 h 审核员培训 8 h 管理体系(MS)专项培训	24 h 培训，包括： 8 h 管理体系(MS)专项培训(见注 6)	同审核员要求

注 1：中等教育是在国家教育体系中，初等教育阶段后，进入大学或类似教育机构前完成的那一部分。

注 2：如果已完成中等教育以后阶段的适当的教育，工作经历可减少一年。

注 3：安全方面的特定工作经历可与一般的工作经历同时发生。

注 4：安全方面的培训是为获得相关标准、法律、法规、原则、方法和技术的知识。

注 5：一次完整的审核是指覆盖了包括文件审查、现场审核活动的准备、现场审核活动的实施以及召开首次会议在内的所有步骤。总的审核经历宜覆盖全部管理体系标准。

注 6：有资格审核其他管理体系的审核员，不必重复 16 h 的通用审核员培训模块。

注 7：有资格领导其他管理体系的审核组长，只需证明其具备领导审核组应用安全管理体系标准或规范(例如 ISO 28000)要求的能力。

注 8：安全经历应包括风险识别、风险分析、风险控制和风险管理的正规的知识和技能。

附 录 D
（规范性附录）
审核员能力要求

本附录规定了供应链安全管理体系审核员的能力要求。

D.1 风险评估方法和工具

供应链安全管理体系审核员应具备以下知识和技能：

a) 理解对供应链的威胁；
b) 安全风险评估与分析的方法和技术；
c) 安全评估工具，包括现场安全调查和典型的输出文档；
d) 风险管理、降低和控制。

D.2 审核规范的要求和理解

供应链安全管理体系审核员应具备以下知识和技能：

a) 供应链安全管理体系标准或相关规范的内容、结构和应用；
b) 供应链安全管理体系标准或相关规范的目的和目标；
c) 供应链安全管理体系标准或相关规范所涉及的定义；
d) 供应链安全管理体系标准或相关规范在供应链不同环节的适用性。

D.3 影响供应链安全的政府及政府间的协定、倡议和计划

在本模块，审核员应能证明在以下方面的知识和技能：

a) 政府间不同的协定和倡议的历史背景和动因；
b) 影响安全的海关程序；
c) 货物清单/单证的最低要求；
d) 影响安全的政府及政府间的协定、倡议和计划；
e) 供应链特定的风险评估方法。

D.4 供应链的漏洞和威胁

供应链安全管理体系审核员应具备以下知识和技能：

a) 当前的安全漏洞、威胁和模式；
b) 探测技术；
c) 降低安全风险的监视、纠正和预防措施。

D.5 审核技术

经过本模块培训的审核员应能证明以下技能：

a) 审查和确认安全管理体系和计划，包括相关的风险评估文件；

b) 说明审核的方法及审核后续活动；
c) 说明审核员的职责和权限；
d) 说明与供应链安全管理体系认证有关的认证机构程序；
e) 说明授予和保持供应链安全管理体系认证证书的条件。

D.6 审核安全数据和信息

供应链安全管理体系审核员应具备敏感和保密安全数据与信息方面(包括给审核员带来的民事和刑事责任)的知识和技能。

D.7 应急策划、准备和响应以及事后恢复与措施

供应链安全管理体系审核员应具备应急策划、准备和响应以及事后恢复与措施(包括官方机构和第一响应者的作用、内部和外部信息通报原则和要求)方面的知识和技能。

参 考 文 献

[1] GB/T 27030—2006 合格评定 第三方符合性标志的通用要求(ISO/IEC 17030:2003,IDT)

[2] GB/T 19001—2000 质量管理体系 要求(ISO 9001:2000,IDT)

[3] ISO 10002 质量管理 顾客满意 组织处理投诉指南(Quality management—Customer satisfaction—Guidelines for complaints handling in organizations)

[4] ISO 17021 管理体系认证机构要求(Conformity assessment—Requirements for bodies providing audit and certification of management systems)