华测认证

信息安全管理体系认证规则

文 件 编 号：CTI-ISMS-2025

文 件 版 本： A/01

生 效 日 期： 2025-08-15

批 准 人：

华测认证有限公司

CTI International Certification

序号	文件状态			创建日期	编制人	审核人	批 准
0	A/00			2025-06-12	古跃东	孙健	周璐
序号	**修订章节**	**修订内容摘要**	**修订状态**	**修订日期**	**修订人**	**审核人**	**批 准**
1	3.2-3.4/4.2.2/7/附录 A	1、增加认证人员能力要求； 2、增加审核时间规定； 3、增加证书恢复、扩大、缩小的规定； 4、增加附录 A 5、描述性修订	A/01	2025-08-15	古跃东	孙健	周璐

目录

1 目的、范围和认证依据

1.1 本规则用于规范华测认证有限公司（以下简称：CTI）开展的信息安全管理体系认证认证活动。

1.2 认证依据：ISO/IEC 27001《信息安全 网络安全 隐私保护 安全管理体系 要求》

1.3 本规则依据认证认可相关法律法规，结合相关技术标准，对信息安全管理体系认证实施过程作出具体规定，明确 CTI 对信息安全管理体系认证过程的管理责任，保证信息安全管理体系认证活动的规范有效。

2 华测认证的基本要求

2.1 CTI 按照 GB/T 27021.1/ISO/IEC 17021-1《合格评定 管理体系审核认证机构要求 第 1 部分：要求》管理信息安全管理体系认证所涉及的认证能力、内部管理和工作过程。

2.2 CTI 建立内部制约、监督和责任机制，实现培训（包括相关增值服务）、审核和作出认证决定等工作环节相互分开，以符合公正性要求。

2.3 CTI 提供的信息安全管理体系认证可结合其他管理体系认证活动进行。

3 对认证人员的基本要求

3.1 认证审核人员应当取得中国认证认可协会（CCAA）的信息安全管理体系注册审核员资格。

3.2 ISMS 审核员、技术专家能力准则

3.2.1 基本要求

ISMS 审核员应具备如下知识和经验：

a) 具备大学本科（含）以上学历，适宜的高等教育学科专业包括： 数学与应用数学 、信息与计算科 学 、应用物理学 、地理信息科学、统计学、应用统计学、电气工程及其自动化 、电子信息工程、电子科学与技术、通信工程、微电子科学与工程 、光电信息科学与工程 、信息工程 、自动化 、计算机 科学与技术 、软件工程 、网络工程 、信息安全、 物联网工程 、 数字媒体技术 、信息管理与信息系统、审计学、信息资源管理、电子商务、集成电路设计与集成系统、电子信息科学与技术、电信工程及管理 、智能科学与技术、空间信息与数字技术、电子与计 算机工程、密码学、人工智能等专业。

b) 在信息技术方面具备至少 4 年的全职实际工作经历，其中至少 2 年的工作经历来自与信息安全有关的职责或职能；

c）接受了充足的 ISMS 审核培训（原则上至少 5 天的培训，特殊情况下经管理者代表确认其能力较强，可以适当减少培训时间），且已证实具备依据 ISO/IEC 27001 实施 ISMS 审核的技能；

d）在作为审核员实施 ISMS 审核前，已获得 ISMS 审核经验。应通过作为实习审核员，在 ISMS 注册级别审核员的监督下，实施至少 1 次 ISMS 初次认证审核（第一阶段和第二阶段）或再认证审核，和至少 1 次监督审核来获得该经验。首次注册审核员资格，该审核经验应至少有 15 个 ISMS 现场审核人日且应在近 3 年内获得。参与审核时，应包括评审文件与风险评估、评估实施情况和报告审核情况；

e） 具备相关的且合乎时宜的经验；

f） 通过持续的专业发展，保持当前在信息安全和审核方面的知识和技能是最新的。

g) 有能力依据 ISO / IEC 27001 审核 ISMS。

3.2.2 审核员初始资格

审核员初始资格的教育经历、工作经历、专业工作经历必须满足 CCAA-101 《管理体系审核员注册准则》2.3 的相关要求及附录 A.6 信息安全管理体系审核员特定要求。成功注册为 CCAA 的 ISMS 审核员及以上的注册资格，即为获得 ISMS 审核员资格，资格保持执行 CCAA 《管理体系审核员注册准则》的规定。

3.2.3 ISMS 审核员能力准则

CTI 通过下述方式验证审核员知识和经验的方式：

a）经承认的、ISMS 特定的资格；

b）注册为审核员；

c）参加 ISMS 培训课程并获得相关的个人证书；

d）最新的持续专业发展记录，如：培训记录等；

e）由另一个 ISMS 审核员见证的 ISMS 审核。

3.2.3.1 总体要求

通过验证审核组成员的背景经验、特定培训或情况说明，确保审核员至少具备：

a）信息安全的知识；

b）与受审核的活动相关的技术知识；

c）管理体系的知识；

d）审核原则的知识。

e）ISMS 监视、测量、分析和评价的知识。

审核员应有能力将客户 ISMS 中信息安全事件的现象追溯到 ISMS 的相应要素；应有关于上述项目的适当工作经历且实际应用过这些项目。

3.2.3.2 信息安全管理术语、原则、实践和技术

审核员应具备以下知识：

a）ISMS 特定文件的结构、层级和相互关系；

b）信息安全管理相关的工具、方法、技术及其应用；

c）信息安全风险评估和风险管理；

d）ISMS 适用的过程；

e）当前可能与信息安全相关的或可能面临信息安全问题的技术。

3.2.3.3 信息安全管理体系标准和规范性文件

参与 ISMS 审核的审核员，应具有以下知识：

a）ISO/IEC 27001 的所有要求；

b）ISO/IEC 27001 附录 A 中的所有信息安全控制及其实施的知识。

3.2.3.4 业务管理实践

参与 ISMS 审核的审核员，应具有以下知识：

a） 行业的信息安全最佳实践和信息安全规程；

b） 信息安全的策略和业务要求；

c） 通用业务管理的概念、实践，以及方针、目标和结果之间的关系；

d） 管理过程和相关的术语。

注：这些过程也包括人力资源管理、内部沟通、外部沟通和其他的相关支持过程。

3.2.3.5 客户的业务领域

参与 ISMS 审核的审核员，应具有以下知识：

a） 特定的信息安全领域、地域和管辖范围的法律法规要求；

注：具备法律法规要求的知识，不意味着要有深厚的法律背景。

b） 与业务领域相关的信息安全风险；

c） 与客户业务领域相关的通用术语、过程和技术；

d） 相关业务领域的实践。

3.2.3.6 客户的产品、过程和组织

审核组所有成员作为一个整体，应具有以下知识：

a） 了解组织类型、规模、治理、结构、职能和关系，包括外包。以便准确评价对开发和实施 ISMS 和认证活动的影响；

b） 广义上的复杂运营；

c） 了解适用于产品或服务的法律法规要求。

3.2.4 ISMS 技术专家能力准则

1）技术专家学历、专业、工作经历、信息安全专业工作经历同审核员的要求一致，具备信息安全技术和信息安全方面的实际工作经验，该工作经验足以担任技术专家；

2）能力应不低于审核员的专业能力要求（审核经验、持续的专业发展要求除外）。

3.2.5 ISMS 审核组长能力准则

晋升为审核组长前，应至少参与 3 次 ISMS 审核的所有阶段（all stages），包括初次的范围识别与策划、评审文件与风险评估、评估实施情况和正式地报告审核情况。且通过审核组长考试后，在具备见证资格的审核员指导和监督下进行的审核中见证审核组长能力：

a. 具备管理认证审核过程和审核组的知识和技能；

b. 具备有效的口头和书面沟通能力。

经评价合格后，授予其 ISMS 组长资格；具备组长资格的审核员可以作为现场见证人，承担 ISMS 体系的初始审核能力见证、组长能力见证、审核员专业能力见证（有相应专业）、持续能力见证、实习审核员晋级见证等，对被见证人的见证结果，由见证人填写《审核员现场审核见证评定报告》。

3.2.6 审核员专业能力评价

3.2.6.1 能力评价准则

1） 总则

审核员专业能力分为技术能力和专业业务能力。

a） 技术能力包含通用信息安全技术及通用信息技术领域能力，通过教育专业、技术工作经历来评价。

b） 审核员专业评价到中类，专业类别的划分见附录 A 中，依照审核员专业工作经历、培训、审核经历等对被评价人进行评价，通过审核记录审查、笔试、面谈、现场见证、意见反馈等方式完成能力评价。

c） 针对附录 A 中一级风险的专业，其专业能力只能从工作经验获取，不接收通过审查、笔试、培训、面试、现场见证的方式获取。

2） 评价准则如下：

专业风险等级 能力准则		一级	二级	三级
技术能力准则	信息安全与信息技术相应专业	四年及以上软/硬件生产/技术服务相关工作经历	两年软/硬件生产/技术服务相关工作经历	
	其他专业	十年及以上软/硬件生产/技术服务相关工作经历	八年及以上软/硬件生产/技术服务相关工作经历	
专业业务能力准则	专业工作经历	具备 4 年相关专业工作经历；当相关工作经历不足 4 年时，被评价人需具备该领域高级技术职称或者在国家级报刊、杂志上发布学术论文。	1）具备 2 年相关专业工作经历； 2）当相关工作经历不足 2 年时，被评价人需具备该领域中级技术职称或者在国家级报刊、杂志上发布学术论文。或按照无专业工作经历要求进行评价	

	无专业工作经历	不能授权一级风险的专业代码，终止评价	1）完成指定知识的培训，并通过考试； 2）如有必要，在专业审核员指导下完成专业审核任务 2 次
能力确认方式		现场见证	现场见证或书面见证

注：

1、专业风险等级管理：

公司针对二级和三级风险中类专业代码的审核员能力评价要求，采取就高不就低的风险管理原则，审核员能力要求统一按照二级风险能力进行评价，专业代码的风险等级只区分一级和非一级风险。

2、审核员初始评价与专业评价

信息安全审核员获取任何一个大类专业能力初始评价，须通过现场见证。实习审核员转正时现场见证评价同时安排 04.08 专业见证。通常情况下即使认证范围产品与服务不属于 04.08 专业， 在审核过程中依然可以针对信息技术部门按照 04.08 专业进行验证。

3、扩专业验证管理

被评价人具有除 04.08 专业以外所申请评价的大类专业时，可采用书面验证方式；否则应采用现场验证方式。

4、见证免除条件：

1）二、三级专业领域：凡是参加并主持公司信息安全管理体系专业领域审核作业指导书或能力分析报告编写工作的人员，按照上述条件可以免除见证直接赋予专业代码；

2）一级专业领域：除满足上述二、三级专业领域的条件以外，还需要同时满足下列条件：

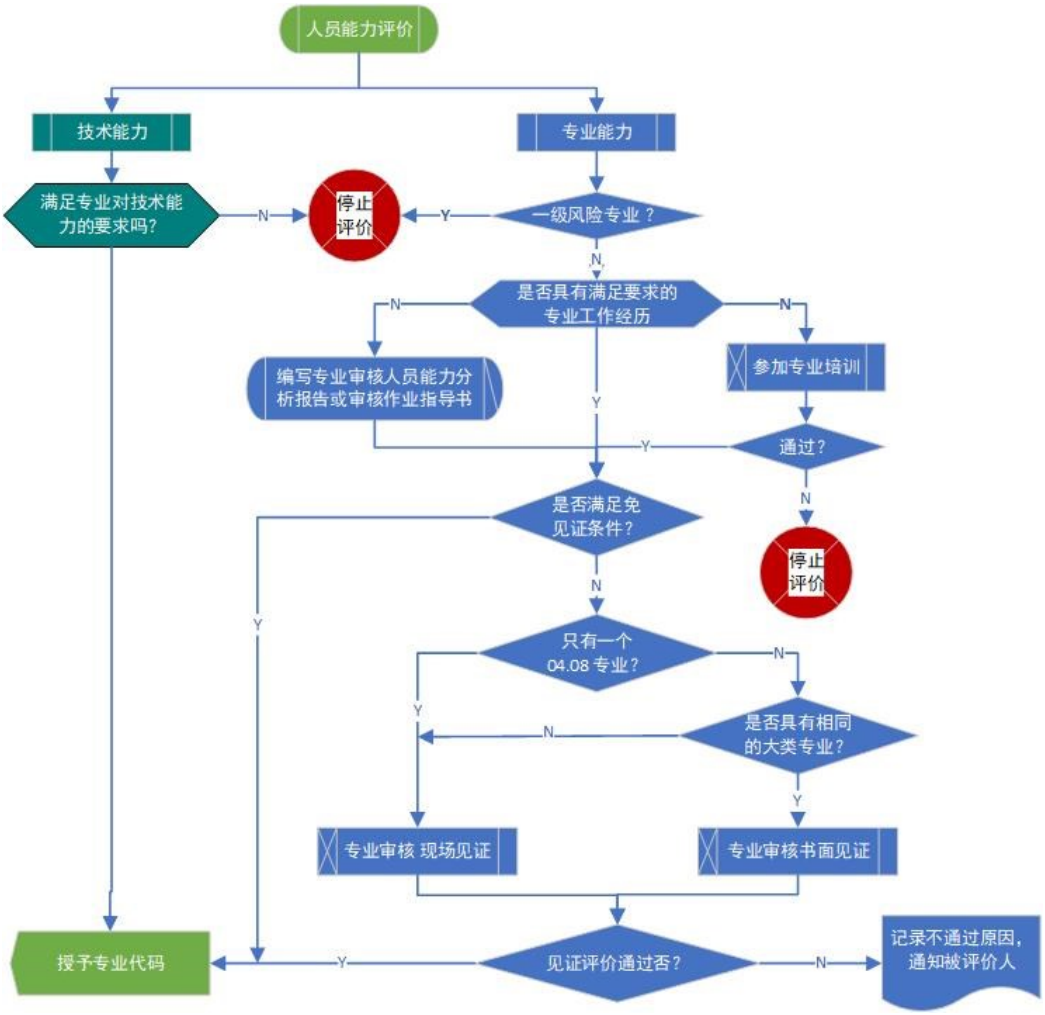
a) 正式信息安全管理体系 正式审核员审核经历≥10 年 并且审核项目的总数≥100 家；

b) 信息技术与信息安全技术 专业工作经历≥10 年

c) **与申请的一级风险 专业领域相关的工作经历≥10 年**

3.2.6.2 专业能力评价流程

信息安全管理体系 审核员专业 能力评价流程图如下 ：



3.2.6.3 专业能力评价

1) 技术能力

信息安全管理体系审核员的技术能力，主要评价与信息技术和信息安全技术相关的受教育的专业和工作经历。

信息安全与信息技术相应专业：信息与计算科学 、电子信息工程、电子科学与技术、通信工程、计算机科学与技术 、 软件工程 、网络工程 、信息安全、 物联网工程 、 数字媒体技术 、 信息管理与信息系统 、 集成电路设计与集成系统 、 电子信息科学与技术 、电信工程及管理 、电子与计算机工程 、密码学、人工智能专业等信息技术相关专业。

相关的工作经历包含但不限于：信息应用系统软/硬件开发与系统运维、网络设计与运维、工业领域智能控制系统设计与运维、电子产品的设计。

随着信息技术和信息安全技术的不断发展，同时与各行各业不断的融合，涌现出了大量跨行业 的专业和应用领域 例如：语音识别、云计算、虚拟技术和 AI 智能技术等。对受教育专业和相关工作经历类别不可能穷尽列出，在评价技术能力时重点考虑被评议案人，本科受教育（学习的课程）和工作经历与信息技术和安全技术关联程度。

2) 专业能力

专业能力是指理解与掌握专业领域产品实现过程与活动以及业务流程的管理控制特点，从而可以准确识别与评价其中的信息和信息安全风险与威胁。专业能力的获取主要通过两种方式 ：

a）专业工作经历：主要考虑评价被评价人从事与专业领域相关工作的 经历 ，包括但不限于产品实现过程与活动中的设计、管理、服务等工作经历。

b）专业培训：一级风险的专业领域不认可通过培训所获得的专业能力，通过专业培训所获取的专业能力 仅限于非一级风险的专业领域。专业培训的具体要求参见下列条款 。

专业能力的评价主要审核被评价人的专业工作经历的证明和 参加并考试通过专业培训的证据。

3) 专业培训要求

a） 培训内容 ：

当通过培训或审核经历 所获得的专业能力时，培训的内容至少包含但不限于：

i. 适用于专业领域产品实践过程中法律法规和强制标准

ii. 专业领域产品实现过程和活动以及业务流程特点

iii. 产品实现过程中 关键设备 控制方法

iv. 专业领域产品实现过程和活动中 所产生的信息 和信息种类

v. 典型的关键信息 以及信息安全风险 和目前常见的 安全风险控制措施

vi. 专业领域产品实践过程和活动 中所涉及的计算机 网络 信息系统 安全管理的措施

b） 培训方式 ：

当通过培训或审核经历 所获得的专业能力时，培训的形式有下列两种 ：

i. 课堂培训：通过线下 课堂 或线上虚拟课堂 进行培训

ii. 审核现场培训（相当于获得专业领域 审核经历 ）：在具有同等专业代码的审核员指导下被评价人与神与指导人员同组审核，被评价人提交审核记录；评价人对审核记录进行审核 并签字确认 。

两种培训方式各有优缺点，采用 课堂培训内容连贯、逻辑性较强；并且可以覆盖所有的培训内容。但对没有专业领域工作经验的审核员，可能存在对产品实践过程和活动不直观，理解不到位、不全面；审核现场培训可以直观的看到产品实现过程与活动，较快地专业领域产品实现过程和活动具体含义，从而理解与识别专业领域产品实现过程和活动中的信息与信息种类，通过产品流或业务流转换成信息流 ，进而识别与信息相关的资产，实现信息安全风险的识别与评价，充分理解审核现场所采用的相应的风险控制措施。 公司可以依据具体的实际情况 选择培训的方式 。

c） 培训效果验证

i. 课堂培训可采用试卷的方式对培训内容被掌握的程度进行验证；

ii. 审核现场培训由现场同组审核 指导老师 ，对被评价人提交的现场审核记录进行评价 并给出评价结果 。必要时，公司可安排面试对被评价人应掌握的专业领域的知识内容进行验证 。

4) 能力验证

对信息安全审核员的专业能力的验证采用现场见证和书面见证两种方式，在上述人员能力评价准则中规定了采用现场见证与书面见证的条件和要求，本节规定两种见证的方式方法，以及免于验证的条件 。

a) **现场见证：现场见证的专业领域要求，区分一级风险和非一级风险。**

验证类别	**验证要求**	
	一级风险专业	**非一级风险专业**
验证安排	见证人具有该专业代码，被见证人与见证人安排在同一个审核小组	
验证时长	4-8 小时	2-4 小时
验证内容	应安排审核对应的业务过程和信息技术能力。	应安排审核对应的业务过程。

b) **书面见证：**

书面见证仅针对非一级风险专业领域 ，一级风险的专业领域 不能采用书面见证的方法！ 书面见证通常分成两部分：

i. 对被评价人进行专业领域的产品与服务实现过程的培训（由外部培训机构实施的对应专业培训同样被接受），通过授课老师（或组织者）对被评价人理解和掌握专业领域内容程度进行评价，保存评价结果记录或证书。

ii. 结合信息安全大类专业能力分析报告和中类专业培训内容，评价被评价审核员是否具备该专业的信息安全风险识别、分析、评价和处置能力，可以通过对面试（面试报告）、研讨会发言（会议纪要）、书面答题（考试卷）进行评价。判断被评价人是否具备该专业领域信息安全审核能力。

c) 免验证条件

满足下列条件的审核员 可以免验证环节 ， 直接赋予专业代码 ：

类型名称	**免验证条件**	
	一级风险专业	**非一级风险专业**
通用要求	凡是参加并主持公司信息安全管理体系专业领域审核作业指导书或专业能力分析编写工作的人员，按照评价准则进行评价后，并同时满足下列条件，可以免除见证直接赋予专业代码；	
技术能力	与信息技术和信息安全技术相关的 工作经历 ≥10 年	满足评价准则要求
专业能力	与中类 专业领域业务过程相关的工作经历 ≥10 年	满足评价准则要求
审核能力	具有信息安全管理体系审核源 审核资质≥10 年，审核的项目总数≥50 个 。	具有信息安全管理体系审核源 审核资质≥4 年

3.3 其他认证人员能力准则

3.3.1 申请评审人员

3.3.1.1 初始资格

1) 大专以上学历或同等学历；

2) 接受入门培训，并考核合格，具备 ISMS 标准和规范及审核的基础知识。培训内容：ISMS 标准和规范性文件、ISMS 领域业务范围分类、与业务领域有关的通用术语/过程/技术

和风险，公司质量手册，认证项目受理、认证项目申请评审、认证审核、再认证审核、转换审核、特殊审核、审核人日数等有关程序和规定、相关法律法规、公司认证工作管理软件等。

3.3.1.2 能力准则

1）了解 ISMS 体系标准和规范文件

2）熟悉 ISMS 认证业务范围分类与分级、熟悉认证工作程序，掌握多场所抽样的要求及运用，识别管理体系的有效人数；

3）熟悉与客户业务领域相关的通用术语、过程、技术和风险的知识；

4）熟悉客户的产品、过程、组织类型、规模、治理、结构、职能以及 ISMS 的开发与实施和认证活动之间的关系，包括外包的职能等的知识；

5）能根据申请方申请认证的管理体系所覆盖的产品和活动范围的专业技术特点进行评审，识别并能准确的确定：

a)申请的认证业务范围所需的行政、行业许可资质，提供的资料是否满足要求；

b)认证范围的专业类别，判定该类别是否在公司认证业务范围内，确定认证范围的初步描述；

6）掌握 ISMS 审核时间的计算方法，能根据申请组织的规模、范围确定审核的人日数（包括结合审核、联合审核）；

7）掌握 CTI 有关认证证书转换的规定，能准确评审证书转换申请是否符合相关规定，是否可以接受，并能确定转换审核的形式和审核时间。

8）具备相关技术领域的专业能力分析中对申请评审人员的专业知识和技能要求。

3.3.2 审核方案管理人员

3.3.2.1 初始资格

同 3.3.1.1 初始资格

3.3.2.2 能力准则

1）了解 ISMS 体系标准和规范文件；

2）2）熟悉 ISMS 认证业务范围分类与分级、熟悉认证工作程序，掌握多场所抽样的要求及运用，识别管理体系的有效人数；

3）熟悉与客户业务领域相关的通用术语、过程、技术和风险的知识；

4）熟悉客户的产品、过程、组织类型、规模、治理、结构、职能和关系，包括外包的职能等的知识；

5） 能迅速查询 CTI 所有级别审核员具有的专业范围；

6） 具有与审核员、受审核方进行沟通、协调的能力；

7） 能根据公司《认证工作程序》的要求，对每个审核项目的整个认证周期的审核活动进行策划，并安排审核任务，做到：

a) 及时、合理的安排各类体系的初审，尽可能满足客户的需求；

b) 掌握客户再认证的情况、在接受再认证申请时应考虑历次审核和纠正措施的结果；掌握客户监督审核的周期时间，并合理安排审核，防止审核安排超周期；

c) 下达审核委托及时、准确，能根据审核方案的目的、范围与深度合理安排审核任务，确保审核组审核能力满足审核任务要求，做到：

—— 指派的审核组长、组员满足审核能力的要求及人员使用规定要求；

—— 无论是多体系结合审核还是单体系审核，能确保审核组每个体系至少有一名专业审核员或满足需要的技术专家；

—— 能及时为审核组提供审核所需的相关信息和资料；

—— 能将审核安排与客户进行沟通，得到客户的同意。

8）具备 ISMS 技术领域的专业能力分析中对审核方案管理人员的专业知识和技能要求。

3.3.3 认证决定人员

3.3.3.1 初始资格

大专以上学历，具备 ISMS 审核员资格或具备初始资格要求的工作经历；具有一定的专业技术知识和经验，理解适用的标准及认证要求；

3.3.3.2 能力准则

1）应具备相关知识，能够验证认证范围的适宜性、范围的变更以及变更对审核有效性的影响，特别是识别接口与依赖关系的持续有效性和相应的风险。

2）具备通用的管理体系、审核过程和程序、审核原则、 实践和技巧的相关知识；

3）具备信息安全管理术语、原则、 实践和技术方面的知识，包括：ISMS 特定文件的结构、 层级和相互关系，信息安全风险评估和风险管理，ISMS 适用的过程，与信息安全相关

的法律法规要求；

4）了解 ISMS 体系标准和规范文件；

5）具备与相关业务领域实践有关的通用术语和风险知识；

6）具备客户的产品、过程、组织类型、规模、治理、结构、职能和关系的相关知识。

7）能正确评价审核过程、审核发现、审核报告和审核组的推荐意见，做出复核的意见，包括：

a)评审做出认证决定必要的报告和其他相关信息；

b)与审核组就审核发现交换意见（必要时）；

c)与审核组一起解决审核实施过程中发现的问题（必要时）；

d)决定已获得的证据是否充分，以签发认证证书；

e)将决定形成文件；

f)向审核组提出反馈（必要时）。

8) 具备相关技术领域的专业能力分析中对认证决定人员的专业知识和技能要求。

9）认证决定人员专业评价准则同审核员专业业务能力评价准则。

3.4 认证人员能力评价及持续监督

申请评审人员、审核方案管理人员、人员能力评价人员、认证规则和认证方案制定人员按本领域评价并授权。获授权人员可在授权范围内独立开展相应的管理工作；认证决定人员通过书面评价按照领域及专业授权。

ISMS 认证人员：申请评审、审核方案管理人员、认证决定人员、审核员、认证规则及认证方案制定人员、能力评价人员的能力评价、持续监督与评价的其他要求参照 CTIP10《管理体系认证人员能力准则和评价程序》执行，认证人员可以通过 CTI 提供持续专业发展机会以及自学等方式获得专业持续发展，例如获取工作经验、辅导、交流和研讨等，以确保认证人员的能力满足相关要求，确保认证实施的有效性。根据认证人员评价周期内的评价结果，对其进行复核，并保存最新评价结果

3.5 认证人员应当遵守与从业相关的法律法规，对认证审核活动及相关认证审核记录和认证审核报告的真实性承担相应的法律责任。

4 初次认证程序

4.1 受理认证申请

4.1.1 认证申请组织应具备以下条件：

（1）取得国家工商行政管理部门或有关机构注册登记的法人资格或其组成部分；

（2）已取得相关法规规定的行政许可（适用时）；

（3）建立和实施了企业信息安全管理体系，且有效运行 3 个月以上，至少完成一次内审、管理评审；

（4）在一年内，未发生违反国家相关法律法规的事故；

（5）三年内未因违反相关法律法规而被其他认证机构撤销信息安全管理体系认证证书；

（6）未被执法部门责令停业整顿或在全国企业信用公示系统中被列入“严重违法企业名单”。

（7）申请组织需符合工信部联协[2010]394 号文《关于加强信息安全管理体系认证安全管理的通知》的要求， 以及有关主管部门/监管部门对信息安全管理体系认证的管理要求（如工信部 2011 年第 21 号公告《工业和信息化部加强政府部门信息技术外包服务安全管理》等）。

（8）申请组织具有一个已文件化且已实施的、符合 ISO/IEC27001 和认证所要求的其他文件的 ISMS。

4.1.2 认证申请组织应提交的文件和资料：

（1） 认证申请书，包括以下方面：

a） 申请认证的组织名称、注册地址、经营地址、联系人、职务、联系方式、认证类型、认证依据；

b） 体系建立、内审、管理评审时间；

c） 体系覆盖的人数以及根据业务、组织、位置、资产和技术等方面的特性所确定的 ISMS 的范围和边界，包括对任何范围、删减的详细说明和正当性理由；

d） 经营场所、分场所、临时场所以及各场所从事的活动等；

e） 不同 IT 平台的数量、隔离网络的数量；

f） 保密和敏感信息声明；

g） 提供咨询服务机构和人员信息；

h） 申请组织对 CTI 的资质、诚信守法记录或认证人员身份背影的要求以及适用的、最新的与保守国家秘密或维护国家安全有的法律法规要求，包括相关方的要求和客户自身的要求。以便 CTI 判断是否具备为申请组织实施认证活动的资格或条件；

i） 关于认证活动的限制条件(如出于安全和/或保密等原因，存在时)。

j） 申请组织 ISMS 范围不允许 CTI 接触的信息资产\CTI 接触这些信息资产应满足的法律要求、相关方要求及申请组织的要求等；

（2）法律地位的证明文件的复印件。若信息安全管理体系覆盖多场所活动，应附每个场所的法律地位证明文件的复印件（适用时）；

（3）信息安全适用性声明 SOA；信息安全风险评估报告、剩余风险评估报告、风险处置计划；适用的法律法规的标准的清单；信息安全组织架构图和职责说明；保密和敏感信息声明表。

（4）信息安全管理体系成文信息；

（5）其他需要的文件。

4.1.3 申请评审

CTI 对申请认证组织提交的申请资料进行评审，根据申请认证的活动范围及场所、员工人数、完成认证活动所需时间和其他影响认证活动的因素，综合确定是否受理认证申请。以确保：

(1)识别申请组织的行业类别和与之相应的信息安全管理过程的特性和服务要求；

(2)掌握国家对相应行业的信息安全管理体系认证的管理要求；

(3)结合企业实际情况确认认证范围描述，确保：

认证范围描述应与组织实际情况一致；

认证范围活动描述应能充分展示企业的实际能力。

(4)组织根据业务、组织、位置、资产和技术等方面的特性，确定 ISMS 的范围和边界，包括对任何范围删减的详细说明和正当性理由进行了说明；应注意删减条款应符合 ISMS 标准的要求；

(5)申请组织 ISMS 范围是否存在不允许 CTI 接触的保密、敏感信息及资产，CTI 接触信

息资产应满足的法律要求、相关方要求及申请组织的要求等，CTI 应评审是否满足所有这些要求，否则不应在认证活动中接触客户的相关信息资产，并告知客户。

(6)解决了 CTI 与申请组织之间任何已知的理解差异；

(7)已根据特定的申请组织的具体情况分析对其实施审核和认证所需的能力，CTI 有能力实施认证活动；

(8)评审管理体系有效运行 3 个月以上，并确保已完成内部审核和管理评审后方可实施审核。

(9)对于 ISMS 和 ITSMS 的结合审核，申请评审人员应特别关注组织的审核范围、临时场所等信息，以便为审核方案的策划提供必要的输入。

对被执法监管部门责令停业整顿或在全国企业信用信息公示系统中被列入“严重违法企业名单”的申请组织，CTI 不应受理其认证申请。

4.1.4 评审结果处理

申请材料齐全并符合有关要求的，予以受理认证申请。未通过申请评审的，CTI 书面通知申请组织在规定时间内补充和完善，或不受理认证申请并明示理由。

4.1.5 签订认证合同

在实施认证审核之前，CTI 与认证申请组织订立具有法律效力的书面认证合同，明确拟认证的范围，以及在认证审核实施过程及认证证书有效期内，认证机构和申请组织各自应当承担的责任、权利和义务。合同应至少包含以下内容：

（1）申请组织获得认证后持续有效运行信息安全管理体系的承诺。

（2）申请组织对遵守认证认可相关法律法规，协助认证监管部门的监督检查，对有关事项的询问和调查如实提供相关材料和信息的承诺。

（3）申请组织承诺获得认证后发生以下情况时，应及时向认证机构通报：

①客户及相关方有重大投诉。

②发生信息安全事故。

③相关情况发生变更，包括：法律地位、生产经营状况、组织状态或所有权变更；取得的行政许可资格；法定代表人、最高管理者变更；生产经营或服务的工作场所变更；信息安全管理体系覆盖的活动范围变更；信息安全管理体系和重要过程的重大变更等。

⑤出现影响信息安全管理体系运行的其他重要情况。

（4）申请组织承诺获得认证后正确使用认证证书、认证标志和有关信息，不利用信息安全管理体系认证证书和相关文字、符号误导公众认为其产品或服务通过认证。

（5）拟认证的信息安全管理体系覆盖的生产或服务的活动范围。

（6）在认证审核实施过程及认证证书有效期内，认证机构和申请组织各自应当承担的责任、权利和义务。

（7）认证服务的费用、付费方式及违约条款。

4.2 审核策划

4.2.1 审核方案

4.2.1.1 CTI 应针对每一认证组织建立认证周期内的审核方案，以清晰地识别所需的审核活动。

4.2.1.2 初次认证的审核方案应包括两阶段初次审核、获证后的监督审核和认证到期前进行的再认证审核。

注：一个认证周期通常为 3 年，从初次认证（或再认证）决定算起，至认证的有效期截止。

4.2.1.3 初次认证审核和再认证审核是对认证组织完整体系的审核，应覆盖 ISO/IEC 27001 标准的所有要求。认证证书有效期内的监督审核应覆盖 ISO/IEC 27001 标准的所有要求。

4.2.1.4 初次认证及再认证后的第一次监督审核应在证书签发起 12 个月内进行。此后，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，且两次监督审核的时间间隔不得超过 15 个月。

4.2.1.5 CTI 应考虑认证组织不同班次完成的过程，以及其所证实的对每个班次的信息安全控制水平来策划对不同班次实施的审核程度，以确保审核的有效性：

（1）每次审核应至少对其中的一个班次的生产或服务的活动现场进行审核；

（2）对于未审核的班次，应记录不对其审核的理由。

4.2.2 审核时间

4.2.2.1 初次认证审核时间

初次审核时间，包括第一、第二阶段审核时间的总和。基于组织控制下工作的、所有班次的人员的数量，以及按照 CC170 规定可以转换为有效人数的之和来识别审核时间的起点。具

体计算审核时间的流程如下：

1）按照规则计算申请组织的有效人数，有效人数作为查表得出基准审核人日的基数；有效人数是考虑以下因素计算得出：

a) 组织的在认证范围内的、处于组织控制下工作的、所有班次的全职员工；

b) 组织在认证范围内的、处于组织控制下工作的、所有班次的兼职员工；

c) 当组织在认证范围内、处于组织控制下工作的人数中如存在很大比例从事某些相同的活动时，可以按照下列规则减少通过上述计算得出的组织控制下的人数。

审核人日：表 1 中所引用的“审核时间”，是根据审核中花费的“审核人日”来阐述的，计算基础是一个 8 小时的工作日。

临时场所：是认证文件所注明的场所之外的位置，其活动在认证范围内并在规定的时间周期内实施。此类场所范围可从大项目管理场所到较小的服务或安装场所。

2）ISMS 审核时间基础表

表 1.ISMS 审核时间

在组织控制下工作的人员的数量	ISMS 初次审核审核时间（审核人日）	在组织控制下工作的人员的数量	ISMS 初次审核审核时间（审核人日）
1 ~ 10	5	626 ~ 875	17.5
11 ~ 15	6	876 ~ 1175	18.5
16 ~ 25	7	1176 ~ 1550	19.5
26 ~ 45	8.5	1551 ~ 2025	21
46 ~ 65	10	2026 ~ 2675	22
66 ~ 85	11	2676 ~ 3450	23
86 ~ 125	12	3451 ~ 4350	24
126 ~ 175	13	4351 ~ 5450	25
176 ~ 275	14	5451 ~ 6800	26
276 ~ 425	15	6801 ~ 8500	27
426 ~ 625	16.5	8501 ~ 10700	28

＞ 10700	沿用以上规律

4.2.2.2 调整审核时间

每个组织所需的时间取决于认证范围内组织规模、复杂程度、审核范围等诸多因素。无论考虑了何种调整因素，应确保分配了充足的审核时间，以完成一次对客户 ISMS 完整且有效的审核。对审核时间的增加或减少及调整理由填写在《IS、SM 信息领域认证申请评审表》中。对表 1 中审核时间的减少不应超过 30%。

需要增加审核时间的其他因素，例如：

1) 复杂的后勤，在 ISMS 范围中涉及不止一处建筑物或地点；
2) 员工所说的语言超过一种（需要翻译或审核员个人无法独立工作），提供的文件使用了一种以上的语言；
3) 为了确认管理体系认证范围内永久场所的活动，需要访问临时场所的活动；
4) 适用于 ISMS 的标准和法规数量很多；
5) ISMS 的复杂程度（例如，信息的关键程度、ISMS 的风险状况）；
6) ISMS 范围内所开展的业务的类型；
7) 在 ISMS 各部分的实施过程中，所应用的技术的水平和多样性[例如，不同 IT 平台的数量、隔离网络的数量]；
8) ISMS 范围内所使用的外包和第三方安排的程度；
9) 信息系统开发的程度；
10) 场所的数量和灾难恢复场所的数量；

允许减少审核时间的因素，例如：

1) 没有风险或者低风险的产品/过程；
2) 过程只涉及单一的常规活动（例如，只有服务）；
3) 在组织控制下工作的雇员大部分是从事相同的任务；
4) 对组织已经有些了解（例如，如果组织获得了同一个认证机构的、另一个标准的认证）；
5) 客户的认证准备情况较好（例如，已经获得了另一个第三方认证方案的认证或承认）；
6) 高度成熟的管理体系（同一认证机构审核 6 次以上，）

策划和编制报告一起所用的时间，通常不宜使总的现场“审核时间”减少到根据上述所计算出的时间的 70%以下。当策划和/或编制报告需要增加时间时，这不应成为减少现场审核时间的理由。审核员旅途时间未计在内，这应在表中所给出的审核时间的基础上另外增加。

4.2.2.3 多场所审核时间的确定

根据上述对认证范围所计算出的总的现场审核人日数，应根据场所与管理体系的相关性和所识别的风险，分配到不同的场所。并在《IS、SM 信息领域认证申请评审表》记录分配过程及结果。

初次认证和监督的总时间，是各场所和总部的审核时间之和，它不应低于当在单一场所实施所有工作时间（例如组织的所有雇员在同一场所），根据运营的规模和复杂性所计算出的审核时间。

4.2.2.4 监督及再认证审核时间

初次认证/再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。此后，监督审核应至少每个日历年（应进行再认证的年份除外），两次监督审核间隔最长不超过 15 个月。当获证组织信息安全务管理体系发生重大变更，或发生重大问题、服务质量事故、客户投诉等情况时，公司视情况可增加监督的频次。

对一个组织的监督时间宜与初次审核时间成比例，每年用于监督审核的时间总量大约至少是初次审核时间的 1/3。当审核 ISMS 的变更（例如，审核新的或发生变更的控制）时，应增加监督审核的时间。

用于再认证审核的全部时间，应取决于所规定的、任何以往审核的结果。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，至少是同一组织初次认证审核时间的 2/3。

CTI 将适时地核查其监督审核及再认证审核时间策划的合理性，确认监督审核方案策划及再认证审核策划是否考虑客户组织的变更等因素的影响，必要时对监督审核审核或再认证审核时间予以调整以确保审核的结果足以证实获证组织 ISMS 的适宜性、充分性和有效性。

4.2.2.5 特殊审核时间

特殊审核涉及：

- 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；

特殊审核认证除遵循《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管理程序》的规定外，其中扩大范围审核时间，对于所扩范围的初次审核，审核时间应根据在当前认证范围内增加的人员和场地的数量，按照 4.2.2.1 条款的方法来计算。

扩大 ISMS 范围所需的审核时间，应增加到审查客户获证 ISMS 所需的审核时间中。当扩大范围审核是结合监督审核或再认证审核进行时，应至少增加为 0.5 天(审核人日)；当扩大范围审核是单独进行时，相应的时间应至少为 1.0 天(审核人日)。

4.2.3 多场所的抽样

当客户拥有满足以下 a 至 c 的多个场所时，CTI 可以考虑使用基于抽样的方法进行多场所认证审核：

a. 所有的场所在同一 ISMS 下运行，并接受统一的管理、内部审核和管理评审；

b. 所有的场所都包含在客户的 ISMS 内部审核方案中；

c. 所有的场所都包含在客户的 ISMS 管理评审方案中。

CTI 使用基于抽样的方法时，应有适宜的程序以确保：

a. 在初次的合同评审时，最大程度地识别场所之间的差异，以便确定适宜的抽样水平；

b. 结合以下因素，抽取具有代表性的场所：

1) 总部及其他场所的内审核结果；
2) 管理评审的结果；
3) 场所规模的 差异 ；
4) 各场所业务目的 差异 ；
5) 不同场所的信息系统复杂程度；
6) 工作 实践 的差异 ；
7) 所实施的 活动差异 ；
8) 控制的设计与运行差异
9) 与关键的信息系统或处理敏感之间潜在交互 ；

10) 任何不同的法律要求 ；

11) 地域和文化因素；

12) 场所的风险状况；

c. 发生在特定场所的信息安全事件 。

d. 从客户 ISMS 范围内的所有场所中选择具有代表性的样本，该选择应基于一个可体现上述 b)中所列因素的判定，同时也考虑随机因素；

e. 在授予认证之前，CTI 审核了 ISMS 中每个具有重大风险的场所；

f. 根据上述要求设计审核方案，且审核方案要在三年内覆盖 ISMS 认证范围内的代表性样本；

g. 无论是在总部还是在单个场所发现不符合，纠正措施规程的实施适用于包括在认证范围内的总部和所有场所。

审核应关注客户总部为确保一个 ISMS 运用于所有场所并在运行层面上实施统一管理所进行的活动。审核应关注上述所有事项。

4.2.4 审核组

CTI 根据信息安全管理体系认证覆盖的活动的专业技术领域选择具备相关能力的审核员组成审核组，必要时选择技术专家参加审核组。审核组中的审核员承担审核任务和责任。

技术专家主要负责提供认证审核的技术支持，不作为审核员实施审核，不计入审核时间，其在审核过程中的活动由审核组中的审核员承担责任。

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，不单独出具记录等审核文件，其在审核过程中的活动由审核组中的审核员承担责任。

4.2.5 审核计划

4.2.5.1 审核组长为每次审核制定书面的审核计划（第一阶段审核不要求正式的审核计划）。审核计划至少包括以下内容：审核目的、审核准则、审核范围、现场审核的日期和场所、现场审核持续时间、审核组成员（其中：审核员应标明认证人员注册号；技术专家应标明专业代码、工作单位及专业技术职称）。

4.2.5.2 若信息安全管理体系覆盖范围包括多个场所进行相同或相近的活动，且这些场所都处于申请组织的授权和控制下，可以根据 CTI 多现场组织审核抽样的有关要求，在审核

中对这些场所进行抽样。如果不同场所的活动存在明显差异、或不同场所间存在可能对 ISMS 管理有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。

4.2.5.3 为使现场审核活动能够观察到产品生产和服务活动涉及的信息安全管理情况，现场审核将安排在认证范围覆盖的活动正常运行时进行。

4.2.5.4 审核计划应考虑所确定的信息安全控制措施。

4.2.5.5 如适宜，审核计划应识别在审核中使用的网络支持的审核技术。

注：网络支持的审核技术可包括：例如，电话会议、网络会议、基于网络的交互式通信和远程电子访问 ISMS 文件和（或）ISMS 过程。对这些技术的关注，将提高审核的有效性和效率，并支持审核过程的完整性。

4.2.5.6 在审核活动开始前，审核组长应将审核计划提交申请组织确认，遇特殊情况临时变更计划时，应及时将变更情况通知申请组织，并协商一致。

4.3 实施审核

4.3.1 审核组应当按照审核计划的安排完成审核工作。除不可预见的特殊情况外，审核过程中不得更换审核计划确定的审核员。

4.3.2 审核组应当会同申请组织按照程序顺序召开首、末次会议，申请组织的最高管理者及与信息安全管理体系相关的职能部门负责人员应该参加会议。参会人员应签到，审核组应当保留首、末次会议签到表。申请组织要求时，审核组成员应向申请组织出示身份证明文件。

4.3.3 审核过程及环节

4.3.3.1 初次认证审核，分为第一、二阶段实施审核。

4.3.3.2 第一阶段审核应至少覆盖以下内容：

（1）结合现场情况，确认申请组织实际情况与信息安全管理体系成文信息描述的一致性，特别是体系成文信息中描述的产品和服务、部门设置和职责与权限、生产或服务过程等是否与申请组织的实际情况相一致。

（2）结合现场情况，审核申请组织理解和实施 ISO/IEC 27001 标准要求的情况，评价信息安全管理体系运行过程中是否实施了内部审核与管理评审，确认信息安全管理体系是否已运行并且超过 3 个月。

（3）确认申请组织建立的信息安全管理体系覆盖的活动内容和范围、体系覆盖范围内有效人数、过程和场所，遵守适用的法律法规及强制性标准的情况。

（4）结合信息安全管理体系覆盖产品和服务的特点识别对 ISMS 设计、风险评估和处置（包括所确定的控制）、信息安全方针和目标，以及特别是客户申请认证范围的审核准备情况，并结合其他因素，科学确定重要审核点。

（5）与申请组织讨论确定第二阶段审核安排。对信息安全管理体系成文信息不符合现场实际、相关体系运行尚未超过 3 个月或者无法证明超过 3 个月的，以及其他不具备二阶段审核条件的，不应实施二阶段审核。

4.3.3.3 审核组应将第一阶段审核情况形成书面文件告知申请组织。对在第二阶段审核中可能被判定为不符合项的重要关键点，要及时提醒申请组织特别关注。

4.3.3.4 第二阶段审核应当在申请组织现场进行。重点是审核信息安全管理体系符合 ISO/IEC 27001 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的 ISMS 管理必需的过程控制措施的有效性。

（2） 最高管理者的领导力和对信息安全方针与信息安全目标的承诺；

（3） ISO/IEC 27001 中所列的文件要求；

（4）再次确认一阶段审核过程中所确定的认证范围和物理与逻辑边界；

（5）评估与信息安全有关的风险，以及评估可产生一致的、有效的、在重复评估时可比较的结果；

（6）基于风险评估和风险处置过程，确定控制目标和控制；

（7）信息安全绩效和 ISMS 有效性，以及根据信息安全目标对其进行评审；

（8）所确定的控制、适用性声明、风险评估与风险处置过程的结果、信息安全方针与目标，它们相互之间的一致性；

（9）控制的实施，考虑了外部环境、内部环境与相关的风险，以及组织对信息安全过程和控制的监视、测量与分析，以确定控制是否得以实施、有效并达到其所规定的目标；

（10）方案、过程、规程、记录、内部审核和对 ISMS 有效性的评审，以确保其可被追溯至管理决定和信息安全方针与目标。

4.3.4 发生以下情况时，审核组应向认证机构报告，经认证机构同意后终止审核。

（1）受审核方对审核活动不予配合，审核活动无法进行。

（2）受审核方实际情况与申请材料有重大不一致。

（3）其他导致审核程序无法完成的情况。

4.4 审核报告

4.4.1 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，至少包括以下内容：

（1）申请组织的名称和地址；

（2）申请组织活动范围和场所；

（3）审核的类型、准则和目的；

（4）审核组组长、审核组成员及其个人注册信息；

（5）审核活动的实施日期和地点，包括固定现场和临时现场；对偏离审核计划情况的说明，包括对审核风险及影响审核结论的不确定性的客观陈述；

（6）评价客户在选择实施 ISMS 标准的附录 A 信息安全风险控制措施集时，针对删减不适用条款理由的合理性；明确增加的控制措施来源和评价增加的控制措施适宜性、有效性。叙述从 4.3 条列明的程序及各项要求的审核工作情况，其中对 4.3.3.4 条的各项审核要求应逐项描述或引用审核证据、审核发现和审核结论；评价客户在选择实施 ISMS 标准的附录 A 信息安全风险控制措施集时，针对删减不适用条款理由的合理性；明确增加的控制措施来源和评价增加的控制措施适宜性、有效性。

（7）识别出的不符合项；

（8）审核组对是否通过认证的意见建议。

4.4.2 CTI 保留用于证实审核报告中相关信息的证据。

4.4.3 CTI 应在作出认证决定后 30 个工作日内将审核报告提交申请组织。

4.4.4 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，CTI 应将此报告及终止审核的原因提交给申请组织，并保留签收或提交的证据。

4.5 不符合项的纠正和纠正措施及其结果的验证

对于审核中发现的不符合，审核组将出具书面不符合报告。CTI 将要求申请组织分析原

因，并提出纠正和纠正措施。对于严重不符合，将要求申请组织在最多不超过 6 个月期限内采取纠正和纠正措施。CTI 将对申请组织所采取的纠正和纠正措施及其结果的有效性进行验证。如果未能在第二阶段结束后 6 个月内验证对一般不符合或严重不符合实施的纠正和纠正措施，则应按 4.6.5 条处理，或者按照 4.3.3.4 条重新实施第二阶段审核。

4.6 复核和认证决定

4.6.1 CTI 在对审核报告、不符合项的纠正和纠正措施及其结果进行综合评价基础上，进行复核并作出认证决定。

4.6.2 复核和认证决定人员应为 CTI 管理控制下的人员，审核组成员不得参与对审核项目的认证决定。

4.6.3 CTI 在作出认证决定前应确认如下情形：

（1）审核报告符合本规则第 4.4 条要求，审核组提供的审核报告及其他信息能够满足作出认证决定所需要的信息。

（2）反映以下问题的不符合项，CTI 已评审、接受并验证了纠正和纠正措施的有效性。

①在持续改进信息安全管理体系的有效性方面存在缺陷，实现 ISMS 目标有重大疑问。

②制定的 ISMS 目标不可测量、或测量方法不明确。

③对实现 ISMS 目标具有重要影响的关键点的监视和测量未有效运行，或者对这些关键点的报告或评审记录不完整或无效。

④其他严重不符合项。

（3）CTI 对其他一般不符合项已评审，并接受了申请组织计划采取的纠正和纠正措施。

4.6.4 在满足 4.6.3 条要求的基础上，CTI 有充分的客观证据证明申请组织满足下列要求的，可评定该申请组织符合信息安全管理体系认证要求，向其颁发信息安全管理体系认证证书：

（1）申请组织的信息安全管理体系符合认证依据的要求且运行有效。

（2）认证范围覆盖的产品和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。

4.6.5　当申请组织不能满足上述要求的，则评定该申请组织不符合信息安全管理体系认证要求，CTI 将以书面形式告知申请组织并说明其未通过认证的原因。

（1）受审核方的信息安全管理体系有重大缺陷，不符合 ISO/IEC 27001 标准的要求。

（2）发现受审核方存在重大信息安全问题或有其他与信息安全相关严重违法违规行为。

4.6.6　CTI 在颁发认证证书后，应当在 30 个工作日内按照规定的要求将认证结果相关信息报送国家认监委

5　监督审核

5.1 CTI 将对颁发的信息安全管理体系认证证书的组织（以下称获证组织）进行有效跟踪，监督获证组织持续运行信息安全管理体系并符合认证要求。

5.2 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，监督审核应至少每个日历年（应进行再认证的年份除外）进行一次，且两次监督审核的间隔不超过 15 个月，当获证组织的信息安全管理体系发生重大变更，或企业发生重大失信行为时，CTI 将增加跟踪监督的频次。

5.3 超过期限而未能实施监督审核的，应按 7.2 或 7.3 条处理。

5.4 监督审核的时间应不少于初次认证审核人日数的 1/3。

5.5 监督审核的审核组应满足 4.2.4 要求。

5.6 监督审核应在获证组织现场进行。

5.7 监督审核时至少覆盖以下内容：

（1）文件化管理体系的变更、发生变更的区域（物理、系统、网络）；

（2）标准中证实 ISMS 保持有效运行的条款要求

（3）ISMS 在实现客户信息安全方针的目标方面的有效性；

（4）对与相关信息安全法律法规的符合性进行定期评价与评审的规程的运行情况；

（5）所确定的信息安全风险控制的变更，及其引起的 SoA 的变更；

（6）认证范围所涉及的控制措施实施和有效性；

（7）内部审核和管理评审是否规范和有效；

（8）是否及时接受和处理投诉；

（9）认证证书和标志的使用以及对认证资格的引用是否符合《认证认可条例》及其他相

关规定；

（10）针对体系运行中发现的问题或投诉，及时制定并实施了有效的改进措施。

5.8 对于监督审核中发现的不符合，获证组织应在规定时限内完成纠正和纠正措施并提供纠正和纠正措施有效性的证据。CTI 将对获证组织所采取的纠正和纠正措施及其结果的有效性进行验证。

5.9 监督审核的审核报告按照 5.7 条列明的审核要求逐项描述或引用审核证据、审核发现和审核结论。CTI 将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。

6 再认证程序

6.1 认证证书期满前，若获证组织申请继续持有认证证书，CTI 应当实施再认证审核，并决定是否延续认证证书。

6.2 CTI 应按 4.2.4 条要求组成审核组。按照 4.2.5 条要求并结合历次监督审核情况，制定再认证审核计划交审核组实施。

6.3 信息安全管理体系再认证程序与初次认证程序一致。在获证组织的信息安全管理体系及获证组织的内部和外部环境要素无重大变更时，再认证审核可省略第一阶段审核。

6.4 信息安全管理体系再认证审核的时间不少于初次认证审核人日数的 2/3。

6.5 对于再认证审核中发现的不符合，获证组织应在规定时限内完成纠正和纠正措施并提供纠正和纠正措施有效性的证据。CTI 将对获证组织所采取的纠正和纠正措施及其结果的有效性进行验证。

6.6 CTI 按照 4.6 的要求作出复核和再认证决定。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。

6.7 如果在当前认证证书的终止日期前完成了再认证活动并决定换发证证书，新认证证书的终止日期可以基于当前认证证书的终止日期。新认证证书上的颁证日期应不早于再认证决定日期。

如果在当前认证证书终止日期前，CTI 未能完成再认证审核或对严重不符合项实施的纠正和纠正措施未能进行验证，则不应予以再认证，也不应延长原认证证书的有效期。

在当前认证证书到期后，如果 CTI 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审核才能恢复认证。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。

7 认证资格的暂停或恢复、撤销、注销、扩大或缩小认证范围

7.1 CTI 制定暂停、撤销认证证书或缩小认证范围的规定和文件化的管理制度，规定和管理制度应满足本规则相关要求。CTI 对认证证书的暂停和撤销处理应符合其管理制度，不得随意暂停或撤销认证证书。

7.2 暂停证书

获证组织有下列情形之一的，CTI 在调查核实后的 5 个工作日内将暂停其使用信息安全管理体系认证证书，暂停期限最长为六个月：

（1）信息安全管理体系持续或严重不满足认证要求，包括对信息安全管理体系运行有效性要求的，但尚未构成撤销认证资格的；

（2）不承担、履行认证合同约定的责任和义务

（3）被有关执法监管部门责令停业整顿；

（4）发生信息安全事故或被相关部门处罚，但尚不需立即撤销认证证书；

（5）未能按规定间隔期接受监督审核；

（6）主动申请暂停认证证书；

（7）其他应当暂停认证证书的。

CTI 应以适当方式公开暂停认证证书的信息，明确暂停的起始日期和暂停期限，并声明在暂停期间获证组织不得以任何方式使用认证证书、认证标识或引用认证信息。

7.3 撤销证书

获证组织有下列情形之一的，CTI 应在获得相关信息并调查核实后 5 个工作日内撤销其认证证书：

（1）被注销或撤销法律地位证明文件或有关的行政许可证明和资质证书；

（2）被国家市场监督管理总局列入信用严重失信企业名单；

（3）拒绝配合 CTI 或认证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；

（4）出现重大信息安全事故，经执法监管部门确认是获证组织违规造成；

（5）有其他严重违反法律法规行为的；

（6）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；

（7）没有运行信息安全管理体系或者已不具备运行条件的；

（8）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，或者认证机构已要求其纠正但超过 2 个月仍未纠正的；

（9）主动申请撤销认证证书的；

（10）其他应当撤销认证证书的。

7.4 注销证书

获证组织主动申请不再保持认证证书时，CTI 应确认在不存在暂停或撤销情形后，注销其认证证书，并保留相应证据。

7.5 暂停证书的恢复

获证组织接到暂停证书通知后，在规定时间内对证书暂停原因采取了纠正和纠正措施，经 CTI 验证，造成暂停的原因已消除的，CTI 将恢复其认证注册资格，并在 CTI 网站上公布相关信息，同时按规定程序和要求上报国家认监委。

7.6 扩大或缩小认证范围

（1）获证组织需扩大认证范围时应提出申请，CTI 将评审申请，确定必要的审核活动，以做出是否可予扩大的决定。

（2）如果认证范围覆盖的产品或服务部分停止业务或边界缩小或获证组织范围内某些部分不愿维持纳入认证范围，可提出缩小认证范围，CTI 将评审申请，确定必要的审核活动，以做出是否可予缩小的决定。

（3）认证范围扩大或缩小后，CTI 将换发变更后的认证证书，同时将相关信息上报国家认监委。

7.7 CTI 将以书面方式通知获证组织有关暂停或撤销信息安全管理体系认证证书的信息和要求，并在 CTI 网站上公布相关信息，同时按规定程序和要求报国家认监委。对于撤销认证证书的，CTI 将收回撤销的信息安全管理体系认证证书。

7.8 被暂停或撤销信息安全管理体系认证证书的获证组织，不得以任何方式使用认证证书、认证标识或引用认证信息。

8 认证证书及认证标志

8.1 信息安全管理体系认证证书至少包含以下信息：

（1）获证组织名称、地址和统一社会信用代码；

（2）认证覆盖的生产经营或服务的地址和业务范围。若认证的信息安全管理体系覆盖多场所，表述覆盖的相关场所的名称和地址信息；

（3）信息安全管理体系符合 ISO/IEC 27001 标准的表述；

（4）证书编号；

（5）证书颁证日期、证书有效期；

（6）CTI 名称、地址和认证标志。

（7）证书查询方式。CTI 除公布认证证书在本机构网站上的查询方式外，还应当在证书上注明：“本证书信息可在国家认证认可监督管理委员会官方网站（www.cnca.gov.cn）上查询”，以便于社会监督。

（8）相关的认可标识及认可注册号（适用时）

证书应注明：获证组织必须定期接受监督审核并经审核合格此证书方继续有效的提示信息。

8.2 信息安全管理体系认证证书有效期为 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。

8.3 CTI 按照认监委相关信息通报制度上报信息安全管理体系认证证书信息，除向申请组织、认证监管部门等执法监管部门提供认证证书信息外，还应当根据社会相关方的请求向其提供证书信息，接受社会监督。

8.4 认证证书和认证标志使用要求：按《管理体系认证标志、认可标识和认证状态声明管理规定》执行。

9 与其他管理体系的结合审核

9.1 当信息安全管理体系认证审核和其他管理体系认证审核结合实施时，应同时遵照本规则要求以及其他管理体系认证的相关要求。

9.2 结合审核的审核时间人日数，不得少于多个单独体系所需审核时间之和的 80%。

10 受理转换认证证书

10.1 CTI 应当履行社会责任，严禁以牟利为目的受理不符合 ISO/IEC 27001 标准、不能有效执行信息安全管理体系的组织申请认证证书的转换。

10.2 CTI 受理组织申请转换为本机构的认证证书，应该详细了解申请转换的原因，必要时进行现场审核。

10.3 转换仅限于现行有效认证证书。被暂停或正在接受暂停、撤销处理的认证证书以及已失效的认证证书，不得接受转换申请。

10.4 被发证的认证机构撤销证书的，除非该组织进行彻底整改，导致暂停或撤销认证证书的情形已消除，否则不应受理其认证申请。

11 申诉和投诉

11.1 申请组织或获证组织对认证决定有异议时，可向 CTI 提出申诉。CTI 自收到申诉之日起，在 60 日内进行处理，并将处理结果书面通知申诉人。

11.2 书面通知应当告知申诉人，若认为 CTI 未遵守认证相关法律法规或本规则并导致自身合法权益受到严重侵害的，可以直接向所在地认证监管部门或国家认监委投诉，也可以向相关认可机构投诉。

12 认证记录的管理

12.1 CTI 建立认证记录保持制度，记录认证活动全过程并妥善保存。

12.2 记录应当真实准确以证实认证活动得到有效实施。记录资料应当使用中文，保存时间至少应当与认证证书有效期一致。

12.3 以电子文档方式保存记录的，应采用不可编辑的电子文档格式。

12.4 具有相关人员签字的书面记录，可以制作成电子文档保存使用，原件宜妥善保存，保存时间至少应当与认证证书有效期一致。

13 收费

收费由 CTI 按照有关规定收取，认证委托方应按时、足额缴纳认证费用。

14 附录 A ISMS 认证业务范围分类与分级

大类	中类	小类	风险等级	内容	备注
01	政务				
	01.01		一	国家机构	包括人大、政府、法院、检察院等，不含税务机关和海关
	01.02		一	税务机关	
	01.03		一	海关	
	01.04		二	其他	例如政党，政协，社会团体等
02	公共				
	02.01		一	通信、广播电视	
	02.02		一	新闻出版	包括互联网内容的提供
	02.03		二	科研	涉及特别重大项目的应提升为一级
	02.04		二	社会保障	例如社会保险基金管理、慈善团体等。包括医疗保险
	02.05		一	医疗服务	
	02.06		三	教育	

	02.07		二	其他	例如市政公用事业（水的生产和供应、污水处理、燃气生产和供应、热力生产和供应、城市水陆交通设施的维护管理等）
03	**商务**				
	03.01		一	金融	例如银行、证券、期货、保险、资产管理等
	03.02		一	电子商务	以在线交易为主要特点，含网络游戏
	03.03		一	物流	包括邮政
	03.04		三	咨询中介	例如法律、会计、审计、公证等
	03.05		二	旅游、宾馆、饭店	
	03.06		三	其他	
04	**产品的生产**				
	04.01		一	电力	包括发电和输、变、配电等
	04.02		一	铁路	
	04.03		一	民航	
	04.04		一	化工	
	04.05		一	航空航天	
	04.06		一	水利	

	04.07		二	交通运输	包括公路、水路、城市公共客运交通等，不含航空和铁路
	04.08		二	信息与通信技术	例如软、硬件生产及其服务，系统集成及其服务，数字版权保护等
	04.09		二	冶金	
	04.10		二	采矿	含石油、天然气开采
	04.11		二	食品、药品、烟草	
	04.12		三	农、林、牧、副、渔业	
	04.13		三	其他	
		04.13.01	三	印刷	
		04.13.02	三	高自动化程度的产品生产	
		04.13.03	三	测绘	