

信息安全/信息技术服务 管理体系认证规则

版 本 号： 第 B 版

文件编码： HZZA-CX29

发布日期： 2022 年 11 月 17 日

实施日期： 2022 年 11 月 17 日

发放编号：

受控状态：

编制： 技术部

批准： 任志刚

中国 · 杭州

文件和资料修改记录

序号	修订说明	修订条款	修订日期	实施日期	批准
1	根据 CNAS-CC01 (ISO/IEC 17021: 2015) 等要求进行修订	全面修订	2022. 11. 17	2022. 11. 17	任志刚

1 目的范围

编制本规则的目的是为了为了满足《中华人民共和国认证认可条例》、《认证机构管理办法》和认可机构规范的要求，旨在阐述申请信息安全管理体系认证和信息技术服务管理体系认证、实施管理体系认证和保持管理体系认证等方面的要求。

本认证规则适用中奥认证有限公司（以下简称 CAS 或本机构）实施信息安全管理体系和信息技术服务管理体系认证，满足第三方认证制度要求，是本机构提供管理体系认证服务的准则。本认证规则在认证双方签订合同时进行确认并采用。

2 引用文件

CNAS-CC01 《管理体系认证机构 要求》

CNAS-CC170 《信息安全管理体系认证机构要求》

CNAS-CC175 《基于 ISO/IEC 20000-1 的服务管理体系认证机构的要求》 CNAS-CC11

《多场所组织的管理体系审核与认证》

GB/T19011 《管理体系审核指南》

《信息技术服务管理体系认证实施规则》

3 术语和定义

3.1 申请方——拟向本机构提出管理体系认证申请的组织。

注：申请方可以是接受管理体系认证的组织自身，也可以是依据法律法规或合同有权要求审核的任何其他组织。

3.2 受审核方——以取得本机构的管理体系认证为目的而接受本机构认证审核的组织。

3.3 获证组织——已经获得本机构管理体系认证证书的组织。

3.4 初次认证——对初次接受管理体系认证的组织是否符合相应的管理体系认证要求所实施的审核和评价活动。

3.5 监督——在认证证书有效期内，对获证组织是否持续满足管理体系认证要求所实施的审核和评价活动。

3.6 再认证——在认证证书有效期届满前，对提出延续认证资格要求的组织所实施的审核和评价活动。

3.7 认证证书——由本机构签发的证实组织的管理体系满足特定的管理体系标

准的要求和体系中要求的任何补充规定的文件的要求。

3.8 严重不符合——影响管理体系实现预期结果的能力的不符合。

注：严重不符合包括下列情况及与之类似的情况：

a 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；

b 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。

3.9 轻微不符合——不影响管理体系实现预期结果的能力的不符合。

3.10 事故——获证企业在管理体系实施过程中，发生的造成死亡、疾病、伤害、损坏或者其他损失的意外情况，如：

a) 对信息安全管理而言，发生重大信息泄露、系统或网络中断事故等；

b) 对信息技术服务管理体系而言，因未能有效提供信息技术服务，造成重大影响等；

3.11 争议——申请方或受审核方与本机构在认证过程中就认证程序和认证技术不同意见的书面表述。

3.12 申诉——申请方或受审核方对本机构做出的与其期望的认证状态有关的不利决定所提出的重新考虑的书面请求。

注：不利决定包括：拒绝接受申请，拒绝继续进行审核，要求采取纠正措施，变更认证范围，不予认证、暂停或撤销认证，阻碍获得认证的任何其他措施。

3.12 投诉——任何组织或个人向本机构表达的，有别于申诉并希望得到答复的，对本机构或获得本机构认证的组织的活动或产品不满意的书面表示。

注：不满意包括：获证组织发生的产品质量问题、发生安全事故或环境污染事故、认证证书和标志的违规使用、本机构或其工作人员违反认证机构或管理体系认证有关规定的行为等。

4 认证模式

本机构首先对受审核方的管理体系进行初次审核，经过评定，确认是否批准认证；通过认证之后，在认证证书的有效期内对获证客户的管理体系进行监督，确认是否持续满足认证要求。

5 认证申请

5.1 申请管理体系认证的基本条件

1) 申请方应具有明确的法律地位。如：公司、集团、商行、企业事业单位、研究机构、慈善机构、代理商、社团或上述组织的部分或组合。

2) 申请方按相应的管理体系标准建立了文件化的管理体系（信息安全管理体系应包括适用性声明）。

3) 初次认证现场审核前，申请方的管理体系至少运行三个月，并且已经进行了一次完整的内部审核和管理评审。

5.2 申请管理体系的要求

5.2.1 申请的提出

1) 申请方向本机构提交一份正式的、其授权代表签署的管理体系认证申请书，申请书可以从本机构网站或审核部人员中获得，如果申请方管理体系覆盖多场所，需要填写《多场所清单》；若是多名称申请方申请管理体系认证时，需要向本机构明示多名称的组织结构与认证责任、产品责任等内容的必要表述，填写《多名称组织清单》；认证申请书中包括申请组织的生产、经营或服务活动范围及活动情况的说明；

2) 申请方需要提交的其他资料和承诺

a) 申请方的法律地位证明文件，如：营业执照、事业单位法人证书、社会团体登记证书、非企业法人登记证书等的复印件（加盖申请方公章）；若管理体系覆盖多场所活动或多名称，应附每个场所或名称的法律地位证明文件的复印件（适用时）；

b) 国家、地方或行业有要求时，申请方具有规定的行政认可文件，其申请认证范围应在法律地位文件和行政认可文件核准的范围内；

c) 多场所活动、活动分包情况；管理体系成文信息（适用时）；

d) 管理体系覆盖的产品、活动或服务适用的法律法规、标准清单；

e) 管理体系已有效运行三个月以上的证明材料；

f) 申请认证的范围；申请方的资源管理、过程管理、风险管理等方面的信息；信息安全管理体系需要提交适用性说明。

g) 申请方承诺遵守国家的法律、法规及其他要求，承诺始终遵守认证的有关规定，承担与认证有关的法律责任，并有义务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；

h) 申请方在一年内，未发生信息安全泄露事故或信息技术服务事故（包括已经或可能严重损害国家安全、社会秩序、公共利益或获证客户及其相关方的合法权益）或被执法 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”或违反国家相关法规，虚报、瞒 报获证所需信息的情况；

i) 申请方向本机构说明对认证机构资质要求或认证人员身份背景的要求，以及适用的与保守国家秘密或维护国家安全有关的法律法规要求，并说明是否存在因包含保密性或 敏感性信息而不能提供给审核组核查的任何管理体系文件或记录的情况。

j) 组织按照本机构《管理体系认证申请书》要求提交申请资料时，受理人员应与申请人进行确认，提交资料是否包含申请组织保密性或敏感性信息。在不影响申请评审和文件审核的前提下，申请方可以对提交资料进行相应的处理，删除其中的保密性或敏感性信息；

k) 申请方承诺获得本机构认证后，按规定使用认证证书和认证标志和有关信息，不得擅自利用管理体系认证证书的文字、符号误导公众认为其产品或服务通过认证。在证书有效期内，按合同支付认证费用，并按规定接受监督；

l) 申请方承诺获得本机构认证后按照本机构要求向本机构通报管理体系变更的信息和其他可能影响管理体系持续满足认证标准要求的能力的事宜的信息，一般包括：客户及相关方有重大投诉；所提供的信息技术服务或信息安全服务被执法监管部门列入“黑名单”；发生信息安全泄露事故或信息技术服务重大事故；相关情况发生变更（包括：法律地位、生产经营状况、组织机构或所有权变更、资质证书变更；法定代表人、最高管理者、管理者代表发生变更；服务的工作场所变更；管理体系覆盖的活动范围变更；管理体系和重要过程的重大变更等）；出现影响管理体系运行的其他重要情况；

m) 认证审核期间，申请方能够提供与拟认证范围相关的产品/服务/活动现场。

5.2.2 管理体系申请的评审

本机构应根据认证依据、程序文件等的要求，在三个工作日内对申请组织提交的认证申请书及其相关资料进行评审并保存评审记录，做出评审结论，以确

定：

- 1) 所需要的基本信息都得到提供；
- 2) 申请方的行业类别和与之相对应的管理体系所管理的过程特性和管理要求；
- 3) 国家对相应行业的管理要求；
- 4) 本机构与申请方之间任何已知的理解差异得到消除；
- 5) 本机构有能力并能够实施认证活动；
- 6) 申请方申请的认证范围、申请方的运作场所、完成审核需要的时间和任何其他影响认证活动的因素；
- 7) 本机构建立关于审核人日的确定要求，根据受审核方的规模、特性、业务复杂程度、管理体系涵盖的范围、认证要求和其承担的风险等因素核算并确定审核人日，以确保审核的充分性和有效性。将确定后的人日数记录在审核方案中，审核人日的确定规则执行《审核人日数确定原则及审核人日表》中的要求。

5.2.3 建立审核方案

在管理体系认证申请评审完成后，本机构应针对申请组织建立审核方案（申请方可以称之为受审核方），并由专职人员负责管理审核方案。

审核方案范围与程度的确定是基于受审核方的规模和性质，以及受审核方管理体系的性质、功能、复杂程度以及成熟度水平。

审核方案应包括在规定的期限内有效和高效地组织和实施审核所需的信息和资源，其内容包括但不限于以下几个方面：

- 1) 审核方案的目标；
- 2) 审核的范围与程度、数量、类型、持续时间、地点、日程安排；
- 3) 审核准则；
- 4) 审核方法；
- 5) 审核组的选择；
- 6) 所需的资源，包括交通和食宿；
- 7) 处理信息安全、信息技术服务的保密性以及其它类似事宜。

5.2.4. 确定审核组

本机构应根据受审核方的行业、规模和业务复杂程度组建审核组，指派审核组长。审核组组建要求如下：

认证审核人员必须取得相应管理体系认证注册资格，并得到本机构的专业能力评价，以确定其能够胜任所安排的审核任务。

审核组应由能够胜任所安排的审核任务的审核员组成。必要时可以补充技术专家以增强审核组的技术能力。

具有与管理体系相关的管理和法规等方面特定知识的技术专家可以成为审核组成员。技术专家应在审核员的监督下进行工作，可就受审核方或获证组织管理体系中技术充分性事宜为审核员提供建议，但技术专家不能作为审核员。

6 审核实施

6.1 审核依据

受审核方与本机构确认的审核依据如下：

a) 信息技术服务管理体系标准：ISO/IEC 20000-1:2018 《信息技术服务管理 第一部分：服务管理体系要求》；

b) 信息安全管理标准：GB/T 22080-2016/ISO/IEC 27001:2013 《信息技术安全技术信息安全管理标准》；

c) 审核准则还应包括受审核方所适用的信息安全/信息技术服务方针、目标、适用性声明（信息安全管理标准适用）、程序、标准、法律法规、操作规范、合同要求或行业规范等。

6.2 审核过程

6.2.1 初次认证审核

初次认证审核分两个阶段实施：第一阶段和第二阶段。

第一阶段审核的目的是了解受审核方的基本信息、审核管理体系文件，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，为第二阶段审核提供关注点。

第二阶段审核的目的是评价受审核方管理体系实施的符合性和有效性。

信息安全管理标准和信息技术服务管理体系的第一阶段必须到现场审核。

信息技术服务管理体系第一阶段与第二阶段现场审核间隔不少于 5

个工作日且不多于 60 个工作日。

审核组对在第一阶段和第二阶段审核中收集的所有信息和证据进行汇总分析，评价审核发现并形成审核结论。

6.2.1.1 第一阶段审核

审核组结合受审核方的管理体系运行目标和体系覆盖活动的专业特点，根据受审核方提供的管理体系文件、体系运作过程、运作场所和现场的具体情况、内部审核与管理评审策划和实施情况，确认受审核方对标准的理解和实施的程度、对目标的实现具有重要影响的关键点、相关的法律法规要求的遵守情况以及管理体系范围，审核第二阶段审核所需资源的配置情况，并与申请方商定第二阶段审核的细节，以确定第二阶段审核安排。

信息技术服务管理体系确认：参与服务提供的其他方及管理情况、服务点数量及分布情况，以及十三个 IT 服务过程流程及职责分配、服务项目情况等。

信息安全管理确认：信息资产、风险分析及 不可接受风险处置情况、信息安全服务的项目情况等。

评价受审核方是否策划和实施了内部审核与管理评审，以及管理体系实施的程度能否 证明其已为第二阶段审核做好准备。

如果发生任何将影响管理体系的重要变更，本机构可能将重复整个或部分第一阶段审核。第一阶段审核的结果可能导致推迟或取消第二阶段审核。

6.2.1.2 第二阶段审核

审核组现场评价受审核方管理体系的实施情况，包括符合性和有效性。

第二阶段审核至少包括以下方面：

- a) 与适用的管理体系标准和其他规范性文件的所有要求的符合情况；
- 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) 管理体系和绩效中与遵守法律有关的方面；
- d) 受审核方过程的运作控制；
- e) 内部审核和管理评审实施情况；
- f) 管理职责的落实，包括针对方针的管理职责；

g)为实现总目标而建立的职能层次目标的策划和实现情况;

h)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发现及结论之间的联系。

6.2.1.2.1 信息技术服务管理体系还应包括的内容如下:

审核组应要求受审核方证实其对信息技术服务管理过程的分析和组织运作实施了适当的控制措施,包括:

1) 服务交付过程(服务级别管理、服务报告、服务连续性与可用性管理、信息技术服务的预算与核算、能力管理、信息安全管理);

2) 关系过程(业务关系管理、供方管理);

3) 处理过程(事件管理、问题管理);

4) 控制过程(配置管理、变更管理);

5) 发布和部署过程(发布、部署管理)。

6) 识别和控制了其参与信息技术服务管理体系活动的其他方在服务管理体系边界内的接口,知晓了来自于这些接口的、对服务管理体系和服务的风险,并实施了适当的控制措施。

6.2.1.2.2 信息安全管理体系还应包括的内容如下:

审核组要求受审核方证实其对信息安全管理过程的控制包括:

1) 基于风险评估和风险处置过程,确定控制目标和控制;

2) 所制确定的控制、适用性声明、风险评估和风险处置过程的、信息安全方针、信息安全目标之间的一致性;

3) 控制措施(控制的实施),考虑了内外部环境与相关的风险,以及受审核方对信息安全过程及控制措施的监视、测量与分析,以确定控制措施得以实施,且实施有效并达到其所规定的目标。

6.2.1.3 信息技术管理体系和信息安全管理体系与其他管理体系结合审核

6.2.1.3.1 信息技术服务管理体系文件和信息安全管理体系文件与其他管理体系文件的整合情况:

受审核方可将信息技术服务管理体系和信息安全管理体系文件的进行整合,也可将信息技术服务管理体系文件和(或)信息安全管理体系文件与其他管理

体系文件（如：质量管理体系）整合。如果体系文件是结合的，应能清晰地识别出受审核方的信息技术服务管理和（或）信息安全管理体的相关内容。

6.2.1.3.2 管理体系结合审核

信息技术管理体系和信息安全管理体系与其他管理体系结合审核时，按以下管理要求 执行：

a) 对各体系分别界定审核范围。对审核方案策划及实施过程的必要调整、审核时间的确定等进行有效管理。

b) 必须以审核活动满足信息技术服务管理体系和信息安全管理体系认证所有要求为前提，并且审核不应该由于结合审核而受到负面影响。在审核报告中应清晰体现所有与信息 技术服务管理体系和信息安全管理体系有关的重要要素的描述。

6.2.2 监督活动

6.2.2.1 监督活动的方式

本机构采用现场监督审核和日常监督（如：关注国家有关部门发布的质量信息公报、关注获证客户相关方的信息、获证客户有关信息的日常跟踪、审查获证客户及其运作的说明、要求获证客户提供文件和记录等）相结合的方式。

6.2.2.2 获证后监督审核的内容

a) 体系保持和任何变更情况（如资源、过程、组织结构、已识别的关键控制点等）；

b) 顾客投诉的情况；

c) 涉及管理体系变更的范围； d) 内部审核和管理评审；

e) 信息技术服务管理体系审核服务目录（参与服务提供的其他方、服务点）的变化情况。信息安全管理体系审核《适用性声明》及版本的变化情况；

f) 管理体系实施的有效性；

g) 为持续改进而策划的活动的进展；

h) 针对上次审核中确定的不符合所采取的措施和效果；

i) 证书和标志的使用和（或）任何其他对认证资格的引用。j) 适当时，其他选定的范围。

获证客户应保存全部投诉记录，需要时提供认证机构。

本机构根据以上信息对获证客户管理体系进行再评价，确认其是否持续满足认证要求。

对于监督审核合格的获证组织，作出保持其信息技术服务管理体系认证/信息安全管理体系认证资格的决定；否则，应暂停、撤销其相应的认证资格。

监督审核时，如获证客户没有按要求关闭不符合，将可能导致认证证书的暂停。

6.2.2.3 监督审核的频次

在证书有效期内，获证客户须接受监督审核。

本机构至少每个日历年（再认证的年份除外）进行一次监督审核，监督审核的最长时间间隔不超过 12 个月。初次认证和再认证后的第一次监督审核应从认证决定日期起 12 个月内进行；监督审核的最长时间间隔不超过 12 个月。

由于获证组织的（季节）业务特点及其内部审核安排等原因，可以合理选取和安排监督周期及时机，在认证证书有效期内的监督审核必须覆盖信息技术服务管理体系/信息安全 管理体系认证范围内的所有业务活动。

获证客户因未在规定的时间内实施监督审核而暂停认证证书的，监督审核恢复后，下次审核时间应按原计划时间计算。

若发生下述情况则需增加监督频次，或安排提前较短时间通知的审核：

- a) 获证客户对管理体系进行了重大更改或发生重大问题；
- b) 有足够信息表明获证客户发生了组织机构、服务变更等影响到其认证基础的更改；
- c) 获证客户出现信息安全泄露事故或信息技术服务质量事故或用户提出对相关管理体系运行效果的投诉未得到处理时；
- d) 其他需要考虑的情况。

6.2.3 再认证

获证客户在证书有效期满前至少三个月，须提出再认证申请。再认证审核的目的是验证作为一个整体的组织管理体系全面的持续符合性和有效性，以及认证范围的持续相关性和适宜性。

再认证审核的程序和要求参照 6.2.1 条实施。

在对获证客户的日常监督中，发现获证客户的出现严重影响管理体系运作的

重大变更时，或对获证客户的投诉分析和其他信息表明获证客户不再满足认证要求时，将安排特殊审核

或与获证客户商定提前安排再认证审核。

再认证审核还需关注信息技术服务管理体系和信息安全管理体系在认证周期内的绩效，包括调阅以前的监督审核报告。

对于多场所或结合审核的认证，再认证审核应确保现场审核具有足够的覆盖范围，以提供对信息技术服务管理体系和信息安全管理体系认证的信任。

再认证时通常可不进行一阶段审核，但当获证客户的管理体系和获证客户的内外部运作环境有重大变化时，再认证审核活动可能需要有第一阶段审核。

再认证审核时，获证客户应在当前认证证书到期前接受本机构的审核，并对于审核组开具的不符合在规定的时间内按要求关闭，否则，因认证客户的原因导致本机构不能在原认证证书到期后 6 个月内作出认证决定的，再认证审核失效。

6.2.4 特殊审核

6.2.4.1 扩大认证范围审核

针对已获证的客户，本机构对扩大认证范围的申请进行评审，确定能否予以扩大的决定所需的审核活动，这一工作可与监督审核同时进行。

6.2.4.2 提前较短时间通知的审核为调查投诉、对变更做出回应或对被暂停的获证客户进行追踪，需要在提前较短时间通知获证客户后对其进行的审核。

- 1) 向获证客户说明并使其提前了解将在何种条件下进行此类审核；
- 2) 指派具有丰富经验的审核员组成审核组。

6.3 实施现场审核活动

审核组在现场审核前与受审核方沟通，确认审核安排，说明首末次会议议程。

审核组按照审核计划中日程安排实施审核，通过查阅受审核方的文件和记录、与过程和活动的岗位人员面谈、座谈、观察服务形成过程和活动等适当方法，抽样收集并验证有关的信息，必要时，进行测试，形成审核发现，确认审核情况。

在审核过程中，审核组及时与受审核方沟通，通报审核进程，确认审核证据，解决分歧。当审核发现表明不能达到审核目的时，应说明理由，商定后续措施。

如果需要改变审核目的和范围或终止审核时，应经审核派出机构评审和批准

后实施。审核组长在现场审核结束前，与受审核方沟通现场审核的信息，请受审核方对发现的问题和不符合报告进行确认，并商定对不符合的后续措施的安排，确认审核结论。审核组编制审核报告并提交受审核方。

审核报告属本机构所有，如果在审核后续活动中（含本机构进行认证决定期间）有所更改，本机构将重新向受审核方提供审核报告。请受审核方妥善保管审核报告、不符合报告及其纠正材料等相应材料。

7 认证注册结果的条件和程序

7.1 批准认证注册的条件和程序

7.1.1 本机构批准认证注册的条件如下：

- a) 受审核方的申请材料真实、准确、有效；
- b) 受审核方建立和实施的相关管理体系符合认证标准/规范性文件要求，审核组提出 推荐认证的结论意见；
- c) 受审核方申请认证范围在法律地位文件和资质规定的范围内；
- d) 国家或地方或行业有要求时，受审核方申请认证范围内的组织单元、服务及其过程和活动已满足适用的法律法规的要求；
- e) 审核证据表明管理评审和内部审核的安排已实施、有效且得到保持，并已进行了一次覆盖管理体系所有要求的完整内部审核；
- f) 审核中发现的不合格在规定期限内已经采取纠正/纠正措施，经本机构本次审核组组长或组员进行验证，且验证有效。
- g) 至少近一年来，受审核方申请认证范围内未发生信息安全泄露事故或信息技术服务事故或国家检查不合格；
- h) 受审核方已与本机构签署认证合同，承诺始终遵守认证的有关规定，并按照认证合同规定缴纳认证费用。

7.1.2 批准认证注册的程序

- a) 本机构向获证客户提供认证有关信息的公开文件，使其知悉并理解本机构的要求；
- b) 申请方向本机构正式提交认证申请书和相关附件；
- c) 根据申请方管理体系申请信息进行申请评审，并已确认受理认证申请；

d)满足 7.1.1 批准认证注册的条件,经本机构审定,受审核方在认证范围内已满足批准认证资格的条件,同意批准认证;

e)本机构向认证客户颁发认证证书,要求获证方按规定使用认证标志。7.2 拒绝认证注册的条件和程序

7.2.1 拒绝认证注册的条件

a)认证客户信息未通过本机构的申请评审,评审为不予受理认证申请;

b)本机构审核组现场审核结论为“不推荐认证注册”;

c)初次认证第二阶段后,受审核方未在规定的时间内按要求关闭不符合,或未按规定接受本机构再次实施的二阶段审核;

d)再认证审核后,获证客户未在规定的时间内按要求关闭不符合(包括本机构认证评定提出的不符合);

e)除以上情况外,本机构认证决定的结论为不予认证注册。

7.2.2 拒绝认证注册的程序

a)符合 7.2.1 条件之一,经本机构评审为不予受理认证或认证客户的管理体系不满足批准认证资格条件;

b)本机构向认证客户发出《不予认证注册通知》。7.3 保持认证注册资格的条件和程序

7.3.1 保持认证注册资格的条件

a)获证客户的法律地位、行政许可文件持续符合国家的最新要求,并且认证范围在法律地位文件和行政许可文件规定的范围内;

b)获证客户持续遵守认证有关的规定,包括变更的规定;

c)获证客户在认证范围内的组织单元、服务及其过程和活动持续满足适用的最新法律法规的要求,如发生不满足时及时采取有效的措施;

d)获证客户于获证期内,认证范围内涉及的服务/活动未发生重大事故和国家检查不合格;

e)获证客户在获证期间未发生误用认证证书和认证标志,如有发生能及时有效地采取纠正和纠正措施,并将误用产生的影响降至最少程度;

f)获证客户对顾客或相关方的重大投诉和关切能及时有效地处理;

g) 获证客户能按照本机构的要求及时通报管理体系和重要过程变更等信息；

h) 按时接受监督审核, 经现场审核获证客户的管理体系持续符合认证标准/规范性文件要求, 审核组结论为“保持认证”；

i) 获证客户履行与本机构签署认证合同中规定的责任和义务, 并按照认证合同规定缴纳认证费用。

7.3.2 保持认证注册资格的程序

a) 满足 7.3.1 保持认证资格的条件, 监督审核后, 经本机构派出的审核组长确认和本机构认证评审后认为获证客户在认证范围内能持续满足保持认证资格的条件, 同意保持认证资格, 由本机构签发确认证书并向获证客户发放；

b) 在认证证书有效期内如有认证要求变更, 获证客户接受变更的认证要求, 并经本机构验证在认证范围内管理体系满足变更的要求, 可保持认证资格。

7.4 扩大认证范围的条件和程序

7.4.1 扩大认证范围的分类

a) 获证客户名称增加、固定分场所增加、服务点增加；

b) 服务类别增加；

c) 服务形成主要过程增加, 如软件设计开发服务、软件测试服务。

7.4.2 扩大认证范围的条件

a) 获证客户保持认证资格有效。

b) 获证客户申请扩大的认证范围在法律地位文件范围内, 国家、地方或行业有要求时, 获证客户拟扩大的认证范围具有有效的行政许可文件；

c) 国家或地方或行业有要求时, 获证客户在申请扩大认证范围内的组织单元、产品、服务及其过程和活动, 已满足适用的法律法规的要求；

d) 获证客户的管理体系覆盖申请扩大的认证范围, 符合认证标准/规范性文件要求；

e) 获证客户按照认证规定缴纳补充认证费用。

7.4.3 扩大认证范围的程序

a) 本机构向获证客户提供与扩大认证范围有关信息的公开文件, 获证客户知

悉并理解；

b) 获证客户向本机构正式提交扩大认证范围的申请和相关附件；

c) 需要时，获证客户与本机构补充签署或修订认证合同，并按照规定补充缴纳认证费用；

d) 满足

7.4.1 扩大认证范围的条件，经本机构现场审核、认证评定后，认为获证客户在申请扩大认证范围内已满足批准认证资格的条件，同意批准扩大认证范围，认证证书的注册号和有效期保持不变；

e) 本机构向获证客户送交新认证证书，同时收回原证书。

7.5 缩小认证范围的条件和程序

7.5.1 缩小认证范围的分类

a) 获证客户固定分场所、服务网点缩小；

b) 服务类别减少；

c) 服务形成主要过程减少，如软件设计开发服务、软件测试服务； d) 多个组织认证减少组织数量。

7.5.2 缩小认证范围的条件

a) 获证客户认证范围内部分产品/服务、区域等不再符合认证标准/规范性文件和其他要求；

b) 获证客户不愿再继续保持认证范围内的部分服务、区域等认证资格；

c) 获证客户缩小认证范围应不包括为缩小认证风险的情况。

d) 如果获证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，本机构将缩小其管理体系认证范围。以排除部门组要求的部分。认证范围的缩小应与认证标准的要求保持一致。

7.5.3 缩小认证范围的程序

a) 获证客户向本机构正式提交缩小认证范围的申请，或本机构提出缩小获证客户认证范围的建议，并提供理由和证据。本机构的审定意见和日常监督结果也可作为认证范围缩小的信息来源和理由，经认证双方沟通后达成一致意见；

b) 需要时，获证客户应与本机构修订认证合同；

c)经本机构审定，认为获证客户在申请缩小认证范围不会对仍保持的认证范围产生影响，同意批准缩小认证范围，收回原认证证书，换发认证证书或附件，认证证书的注册号和有效期保持不变。

7.6 变更认证信息的条件和程序

7.6.1 变更认证信息的条件和分类

7.6.1.1 变更认证信息的条件 在认证证书有效内，获证客户因信息发生变更，导致与认证证书信息不一致时，应予以更新。

7.6.1.2 变更认证信息的分类：

- a)获证客户名称、住所变更；
- b) 认证地址变更；
- c)地名、邮编变更；
- d)企业人数变更，证书编号变更；
- e)证书范围中的服务、活动的变更（含临时服务场所）。

7.6.2 变更认证信息的程序

7.6.2.1 认证信息的变更需提交的资料

7.6.2.1.1 获证客户名称、住所变更应提交的资料

- a)获证客户的书面变更申请；
- b)获证客户是企业的，提供工商行政主管部门的变更核准证明及新营业执照复印件；其他性质的获证客户提供允许其设立的政府行政主管部门的相关文件；
- c)对于因改制、企业重组引起的名称变更，获证客户不能获得名称变更核准证明时，应提交组织以原名称和现名称名义的更名申请、政府有关部门的批文和原名称注销证明；并需因管理体系发生重大变更接受本机构的一次监督审核和审定；

d)有行政许可、资质等要求的获证客户，还应提供按新名称变更后的有关文件。

7.6.2.1.2 认证地址变更需要提交的资料

- a)获证客户的书面变更申请；
- b)有行政许可、资质等要求的获证客户，应提供变更后地址的法规要求的有

关文件。7.6.2.1.3 地名、邮编变更需要提交的资料

- a) 获证客户的书面变更申请;
- b) 当地政府的相关证明;
- c) 对有行政许可、资质等要求的获证客户, 应提供变更后地址的有关文件。

7.6.2.1.4 企业增加人数, 证书编号变更需要提交的资料, 获证客户提出企业增加人数时, 需提交变更企业人数和证书编号的书面申请。

7.6.2.1.5 证书范围中的服务、活动的变更需要提交的资料

- a) 获证客户的书面变更申请;
- b) 对有行政许可、资质等要求的认证范围, 还应提供相应文件复印件。

7.6.2.2 认证信息变更的办理流程

a) 获证客户根据

7.6.1 要求向本机构正式提交满足

7.6.2.1 要求的申请书和相关文件资料;

- b) 需要时, 获证客户需要接受本机构的现场审核;
- c) 经本机构审定, 认为获证客户满足认证信息变更的条件, 同意批准认证信息变更;
- d) 需要时, 收回原认证证书, 换发认证证书或附件, 认证证书的有效期保持不变。

7.7 暂停认证资格的条件和程序

7.7.1 暂停认证资格的条件

符合下列条件之一的获证客户, 本机构将暂停其认证证书:

1) 获证客户管理及服务体系持续或严重不满足认证要求, 包括对管理体系运行的有效性要求:

- a) 获证客户的管理体系发生重大变更, 不能持续符合认证标准/规范性文件要求;
- b) 获证客户监督审核期间发生严重影响体系运行的情况;
- c) 获证客户在认证范围内的组织单元、服务及其过程和活动不能满足适用的最新法律法规和标准的要求, 并未采取措施或措施无效;

d) 获证客户未按照认证要求的变更做出相应调整, 或调整不满足变更要求;

2) 获证客户不承担、履行认证合同约定的责任和义务。

- a) 获证客户未能在规定的期限内接受监督或再认证审核;
- b) 获证客户未履行与本机构签署认证合同中规定的责任和义务, 并对保持认证

资格产生重大影响；

c) 获证客户未按照认证合同规定缴纳认证费用；

d) 获证客户在获证期间发生误用认证证书和认证标志，并未能及时有效地采取纠正和纠正措施，以将产生的影响降至最少程度。

3) 获证客户在证书有效期间受到相关执法监管部门处罚，未按要求对此信息向本机构进行通报。

4) 获证客户被地方认证监管部门发现体系运行存在问题，如获证客户于获证期间在认证范围内发生国家抽检不合格，并未查明原因和采取补救措施。

5) 获证客户持有的行政许可证明、资质证书、强制性认证证书等过期失效，重新提交的申请已被受理但尚未换证。

a) 获证客户的法律地位、资质不再符合国家的最新要求；

b) 获证客户的认证范围已不在现行有效的法律地位文件和资质规定的范围内，但仍有可能在短期内符合规定要求。

6) 获证客户不接受或不配合认证认可监督管理部门的监督管理；

7) 获证客户主动请求暂停。

8) 获证客户发生了与信息安全泄露事故或信息技术服务有关的重大事故，反映出获证客户的体系建立及运行存在重大缺陷。

a) 获证客户于获证期间在认证范围内发生重大事故被媒体曝光、或未查明原因和采取补救措施；

b) 获证客户服务出现严重波动，未采取措施。

9) 其他原因需要暂停证书。

7.7.2 暂停认证资格的程序

a) 本规则提出对获证客户暂停全部或部分认证范围内认证资格的建议，并提供理由和证据，或由获证客户向本机构提出暂停认证资格的申请；

b) 必要时，本机构与获证客户沟通，核实证据；

c) 经本机构审定，认为获证客户在认证范围内全部或部分不再持续满足认证要求，但仍然有可能在短期内采取纠正措施的，同意批准暂停全部或部分认证范围的认证资格，并确定暂停期限，向获证客户颁发《认证处置决定通知书》，进行公告；

d) 获证客户按照《管理体系认证证书和认证标志、认可标识使用规则》停止使用认证证书和认证标志，在暂停期间，客户的管理体系认证暂时无效。

7.7.3 暂停期限

认证资格暂停期最长不超过 6 个月。

7.8 恢复认证资格的条件和程序

7.8.1 恢复认证资格的条件 获证客户已针对暂停认证资格的原因采取了有效的纠正措施，产生原因已经消除，认证资格的恢复符合相关的认证要求，同时已证实暂停期内没有使用、引用认证资格（如广告宣传）和使用认证标志。

7.8.2 恢复认证资格的程序

a) 在确定的认证资格暂停限期结束前，根据暂停原因，获证客户在规定期限内向本机构提出恢复认证资格的申请；

b) 需要时，获证客户应提交相关纠正措施和有效性验证材料；

c) 经本机构审定，确认获证客户在暂停认证资格的认证范围内已恢复符合相关的认证要求，做出同意恢复认证资格的结论，发放恢复使用认证证书和标志的通知和公告。

7.9 撤销认证资格的条件和程序

7.9.1 撤销认证资格的条件

符合下列条件之一的获证客户，本机构将撤销其认证证书：

a) 获证客户审核未通过。

b) 获证客户被注销或撤销法律地位证明文件

c) 获证客户拒绝配合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。

d) 获证客户出现重大的信息安全泄露事故或信息技术服务事故等，经执法监管部门确认是获证客户违规造成。

e) 获证客户在证书有效期内有其他严重违反法律法规行为，受到相关执法监管部门处罚。

f) 获证客户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。

- g) 获证客户没有运行管理体系或者已不具备运行条件
- h) 获证客户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；
- i) 获证客户发生了与信息安全泄露事故或信息技术服务有关的重大事故，反映出获证客户的体系建立及运行存在重大缺陷。
- j) 获证客户因换发新证而撤销旧证书。
- k) 获证客户不承担、履行认证合同约定的责任和义务。
- l) 获证客户主动放弃认证。
- m) 其他原因需要撤销证书。

7.9.2 撤销认证资格的程序

经本机构核实与审定，确认获证客户在认证范围内的管理体系不再满足认证要求，做出撤销认证资格的结论，发放认证处置决定通知书并进行公告，获证客户不得再使用认证证书和认证标志。

8 认证证书和认证标志

8.1 认证证书和认证标志

8.1.1 认证证书

初次认证证书有效期最长为 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，如获证客户要求继续使用认证证书，应在证书有效期内接受再认证。

8.1.2 认证标志、认证用标准、认证注册号

执行《认证认证证书和标志、标识管理程序》文件中的要求 8.2 认证证书和认证标志的使用获证后按照《认证认证证书和标志、标识管理程序》的要求，正确使用认证证书和认证标志。

8.3 认证证书和认证标志的误用

误用认证证书和标志的类型及对误用认证证书和标志的处理见《认证认证证书和标志、标识管理程序》中规定。

获证客户一旦发现误用认证证书或认证标志，应立即采取纠正措施，并报告本

机构。

9 获证客户的信息通报

9.1 需要通报的信息

获证客户应建立向本机构通报最新信息的程序，并及时通报其重大投诉、国家监督检查结果、重大事故及获证客户变更的各种信息等，需要通报的信息包括（但不限于）以下内容：

- a) 组织名称，组织法人，隶属关系, 联系人，联系方式；
- b) 组织地址(包括：注册地址、认证地址、邮编)；
- c) 认证范围变化；体系覆盖人数；服务标准的变化；管理体系文件变化；
- d) 组织机构和职能分配；组织认证场所/服务点的增加；商标等信息；
- e) 信息技术服务管理体系：参与服务提供的其他方发生变更；
- f) 信息安全管理体系统：适用性声明及其版本发生变化。

9.2 信息通报的要求：

- a) 业务、地点、组织结构、体系文件变化等情况的信息（及时通报）；
- b) 信息技术服务管理体系：顾客投诉的相关信息每三个月通报一次；参与服务提供的其他方、服务点变化的信息；
- c) 有严重信息安全、信息技术服务事故（包括已经或可能严重损害国家安全、社会秩序、公共利益或获证客户及其相关方的合法权益）的信息（及时通报）；
- d) 其他重要信息。

10 认证要求变更的条件和程序

10.1 认证要求变更的条件

- a) 获证客户保持认证资格有效；
- b) 认证要求变更应在规定的时间前完成；
- c) 申请认证要求变更的获证客户应提交认证要求变更需求申请，并提交按新的认证要求进行体系调整的证据；

- d) 获证客户的管理体系已满足新的认证要求, 且已正常运行。

10.2 认证要求变更的程序

a)在认证要求变更转换期结束前至少 90 天，获证客户应向本机构提出认证要求变更申请；

b)本机构通过对获证客户实施年度监督审核或再认证审核，或应获证客户要求安排的认证要求变更的专项审核，评审调整后的管理体系对认证要求的符合性、适宜性和有效性；

c)经本机构审定，认为获证客户已满足批准认证资格的条件，同意批准认证范围，换发认证证书或附件，收回原证书，认证证书的注册号和有效期保持不变。

11 保密及公正性

执行《公正性和保密性管理程序》中的规定，并在本机构网站公示

12 申诉/投诉、争议及处理

执行《申诉、投诉与争议处理管理程序》中的规定。

13 信息安全、信息技术审核人日数

ISMS（信息安全）审核时间

雇员总数	初次审核时间			监督审核时间		再认证时间	
	总人天数	一阶段	二阶段	总人天数	现场时间	总人天数	现场时间
1-10	5	1	3	2	2	3.5	3
11-15	6	1.5	3.5	2	2	4	3.5
16-25	7	1.5	4.5	2.5	2	5	4
26-45	8.5	1.5	5.5	3	2.5	5.5	4.5
46-65	10	2	6	3.5	3	7	6
66-85	11	2.5	6.5	4	3.5	7.5	6
86-125	12	3	7	4	3.5	8	7
126-175	13	3	7.5	4.5	4	9	7.5
176-275	14	3	8.5	5	4	9.5	8
276-425	15	3.5	8.5	5	4	10	8
426-625	16.5	3.5	10	5.5	4.5	11	9
656-875	17.5	4	10	6	5	11.5	9.5
876-1175	18.5	4	11	6	5	12	10
1176-1550	19.5	4.5	11	6.5	5.5	13	10.5
1551-2025	21	5	12	7	6	14	11.5
2026-2675	22	5	13	7	6	15	12
2676-3450	23	5.5	13	7.5	6	15.5	12.5
3451-4350	24	5.5	13.5	8	6.5	16	13
4351-5450	25	6	14	8	6.5	17	13.5
5451-6800	26	6	15	8.5	7	17.5	14
6801-8500	27	6.5	15.5	9	7	18	15
8501-10700	28	6.5	16	9.5	7.5	19	15
>10700	遵循上述规律			初评 1/3		初评 2/3	

ITSMS（信息技术）审核时间

雇员总数	初次审核时间			监督审核时间		再认证时间	
	总人天数	一阶段	二阶段	总人天数	现场时间	总人天数	现场时间
1-15	3.5	0.5	2.5	1.5	1	2.5	2
16-25	4.5	1.0	3	1.5	1.5	3	3
26-45	5.5	1	3.5	2	1.5	4	3
46-65	6	1.5	3.5	2	2	4	3.5
66-85	7	1.5	4	2.5	2	5	4
86-125	8	1.5	5	3	2.5	5.5	4.5
126-175	9	2	5.5	3	2.5	6	5
176-275	10	2	6	3.5	3	7	6
276-425	11	2.5	6.5	4	3.5	7.5	6
426-625	12	3	6.5	4	3.5	8	7
656-875	13	3	7.5	4.5	4	9	7.5
876-1175	15	3.5	8.5	5	4	10	8
	遵循上述规律			初评 1/3		初评 2/3	

1.1 调整审核时间

应根据客户SMS和服务的所有具体属性，并根据这些属性因素对审核时间做出相应的调整。审核时间的调整应有合理的理由证明增加和（或）减少的审核时间是合理的。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SMS完整且

有效的审核。

对审核时间的增加或减少因素和合理性说明应明确记录在《管理体系审核实施评审及审核方案策划》中。

表2和表3显示了相关因素是如何影响表1中的审核时间。倒班是指在一个连续工作周期内运营的多个地点和（或）小组之间的工作交接或协同工作。

减少审核时间的因素

表2

序号	潜在的减少因素	应用说明
1	SMS和服务很少发生变化；	多年（不少于3年）提供的服务和对象没有变化：-5%
2	以往已证实了SMS的有效实施，例如：以前获得了另一家已认可的认证机构的认证；	仅可应用于减少一阶段审核人天数，或不实施一阶段现场审核：-5%
3	对SMS和一个或多个其他相关管理体系进行结合审	应关注ITSMS审核范围与其他管理体系范围：-5%
4	事先已了解组织，例如：组织已获得了同一家认证机构的其他标准的认证；	仅可应用于减少一阶段审核人天数，或不实施一阶段现场审核：-5%
5	单一的、简单的服务；	多年（不少于3年）提供的服务简单且单一，服务对象固定且风险等级低：-5%
6	所有班次实施完全相同的活动，如服务台；	需有适宜证据表明所有班次中具有同等的绩效：-5%
7	大部分参与服务管理的人员从事相似的单一职能；	需有适宜证据支撑：-5%
8	人数少的单一场所；	应根据业务具体情况确定，通常不建议应用这条理由减少人天数：-5%
9	对参与服务提供的其他方的依赖程度低；如：供方、内部团体或作为供方的顾客；	一般依赖度低的组织业务相对就复杂，所以一般情况此条不应单独作为减少人天数的理由：-5%

增加审核时间的因素

表3

序号	潜在的增加因素	应用说明
1	复杂的后勤，包括多重管理、多个工作场所、处于在同一时区或横跨多个时区；	应考虑场所间转换的路途时间，应在审核计划中明确不同场所之间路途时间的安排：+5%
2	不同地点之间语言差异的复杂性，例如员工说一种以上的语言（需要翻译或使得审核员无法独立工作）；	根据审核员口头与书面沟通能力具体确定，通常审核时间增加至1.5-2倍
3	SMS范围大或复杂，例如大量的服务、人员或地点，不易理解和维持的专业化服务；	服务类别多（2个专业中类及以上），每增加一个中类人天数增加10-20%
4	影响客户SMS的法律法规要求高；	行政许可资质管理范围内组织、政府行政组织，如：知识产权、隐私、食品、药品、特种设备、工业产品许可范围、医疗、航空、航天、核、政府行政机关等：+5%
5	不同的班次实施不同的活动；	审核应覆盖不同的运行班次服务场所：+5%
6	特定审核的SMS范围中包含临时场所；	根据临时场所提供服务的具体情况确定审核人天数，通常可按服务点对待：+5%
7	SMS范围内有复杂的业务过程；	SLA数量、供应商级别协议、运营级别协议数量：参照原人天数计算
8	高度依赖参与服务提供的其他方；如：供方、内部团体或作为供方的顾客；	如果实质服务是由其他方提供的应根据外包具体情况独立计算审核人天数。
9	经常有增加新服务、服务移除、服务转换或服务发生重大变更；	监督或变更时服务的变化情况较上次审核超半数的按再认证审核要求实施：+5%

1.2 其他管理体系标准认证对审核时间调整

如果组织通过了其他相关管理体系标准的认证，如ISO 9001和（或）ISO/IEC 27001，认证机构可以减少初次审核时间。

仅在满足以下条件时，方可根据获得了其他相关管理体系标准的认证而减少审核时间：

- a) 其他管理体系标准的认证是与所审核的SMS相关的;
- b) 任何现有的证书是有效的, 且已认可的认证机构在最近的 12 个月内对其至少实施了一次审核;
- c) 其他管理体系标准的认证范围, 是等同于或大于 ISO/IEC 20000-1 认证的范围; 审核时间的减少量, 应取决于客户服务管理体系与其他管理体系整合的程度。

无论客户是获得了何种其他相关管理体系标准的认证, 认证机构应确保为对客户SMS实施完整有效的审核分配了充足的时间。

注: 当同时审核两个或多个不同领域的管理体系时, 叫做“结合审核”; 当这些管理体系被整合到一个单一的管理体系时, 审核的原则和程序与结合审核相同。

1.3 监督与再认证时间

在确定实施监督审核和再认证审核所需的时间时, 应考虑

以下因素: a) 管理体系认证审核时间不低于总审核时间的 80%;

b) 年度监督审核, 可以是一次审核或多次审核, 其审核时间应不少于初次审核的 1/3; c) 再认证审核的审核时间, 不应少于初次审核的 2/3;

d) 调整后的监督审核时间应不低于 1 人天;

e) 调整后的再认证审核时间应不低于 2 人天。

本机构对本认证规则有最终解释权。