信息安全管理体系认证实施规则

受控状态:

文件编号：CAS-GZ-006

版　　次：B/0 版

编　　制：技术部

审　　核：余淑玲

批　　准：任志刚

杭州中奥质量认证有限公司

Hangzhou Chinao Quality Certification Co.,Ltd

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	A/0：根据认监委 9 号公告等要求修订	全面修订	2025.05.14	2025.06.17	任志刚
2	B/0：根据认监委认证规则整改要求进行修订	全面修订	2025.09.04	2025.10.04	任志刚

目 录

.....

1 适用范围

本规则用于规范公司开展信息安全管理体系的认证活动。本规则明确了杭州中奥质量认证有限公司（以下简称 CAS）对信息安全管理体系认证过程的管理责任和管理要求，以确保公司持续具备开展信息安全管理体系认证的能力。保证公司信息安全管理体系认证活动的规范性、有效性、一致性和公正性。

本规则适用于本公司依据 ISO/IEC27001 《信息安全、网络安全和隐私保护信息安全管理体系要求》开展的信息安全管理体系认证活动全过程的管理，确保认证活动符合国家认证认可相关的法律法规和的要求，满足第三方认证制度的要求，是公司提供认证服务的规范性文件，必要时，在认证合同中补充相关的要求。

本认证规则在认证双方签订合同时予以确认和采用。

2 认证依据及可获取链接

ISO/IEC27001《信息安全、网络安全和隐私保护信息安全管理体系要求》

本规则认证所依据认证标准的获取渠道：ISO IEC 27001-2022 信息安全管理体系 要求-认证标准-欢迎访问杭州中奥质量认证有限公司官网！

也可向我机构认证申请与受理人员索取，联系电话：0571-88193831 邮箱：za@zoiso.cn

3 相关文件

《信息技术服务管理体系认证实施规则》

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-CC11《多场所组织的管理体系审核与认证》

CNAS-CC105《确定管理体系审核时间(QMS、EMS、OHSMS)》

CNAS-CC106《CNAS-CC01 在一体化管理体系审核中的应用》

GB/T 19011《管理体系审核指南》

GB/T 27007《合格评定合格评定用规范性文件的编写指南》

GB/T 27060《合格评定良好操作规范》

ISO/IEC 27001《信息安全、网络安全和隐私保护信息安全管理体系要求》

ISO/IEC 27000《信息技术-安全技术-信息安全管理体系-概念与词汇》

4 术语与定义

4.1 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。

4.2 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。

4.3 获证组织——已经获得本机构管理体系认证证书的组织。

4.4 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。

4.5 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。

4.6 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。

4.7 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。

4.8 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。

4.9 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。

4.10 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：

对信息安全管理体系而言，发生重大信息泄露、系统或网络中断事故等；

4.11 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。

4.12 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。

4.12 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：获证组织发生的信息安全事故、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。

5 对 CAS 的要求

5.1 基本要求

CAS 应具备信息安全管理体系资质，并持续满足已获资质的要求。

CAS 应当按照《中华人民共和国认证认可条例》和《认证机构管理办法》的相关规定，通过网站或者其他形式向社会公布认证规则及相关信息并保证公示信息真实、有效，我公司网站公示信息如下：

（1）本公司开展的认证业务范围，以及本公司的资质；

（2）开展认证活动所依据的认证规则、认证标准、认证流程、收费标准；

（3）授予、拒绝、保持、更新、暂停（恢复）或撤销认证以及扩大或缩小认证范围的程序；

（4）本公司管理体系认证申请书和认证合同；

（5）相关信息的保密规定；

（6）认证证书、认证标志及相关使用规定；

（7）对认证过程的申诉、投诉规定及渠道；

（8）本公司遵守上级主管部门部门对于加强认证规则管理的承诺。

本认证规则在我机构官网（CAS-GZ-006-A0 信息安全管理体系认证实施规则-认证规则-欢迎访问杭州中奥质量认证有限公司官网！）公示。

也可通过电话 0571-88193831 或邮箱 za@zoiso.cn 联系获取。

5.2 公正性要求

建立内部制约、监督和责任机制，实现培训学习、审核和作出认证决定等环节的相互分开，以确保认证审核的公正性。

CAS 承诺对所实施的认证活动公正性负责，不允许商业、财务或其他压力损害公正性。《公正性声明与保密承诺》发布在 CAS 网站上，对公正性的管理按照《公正性与保密工作管理程序》之规定实施。

5.3 利益相关方的需求和期望

为确保公正性，CAS 成立了公正性委员会，评估公正性风险。公正性委员会成员由各利益相关方组成，管理体系利益相关方包括：认证机构的人员、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）的代表等。建立程序以识别各利益相关方的需求和期望，并每年定期召开公正性风险评估会议，就影响公正性的事宜向其征询意见。按照程序文件规定，对认证规则的验收审查，组织利益相关方参加。

6 人员能力及审核组要求

6.1 认证人员及审核组要求

认证审核人员必须取得信息安全管理体系认证注册资格，并得到 CAS 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。

认证人员应当遵守与认证认可相关的法律法规及规范性文件的要求，具有从事认证工作的基本职业操守：信息安全、客观、公正、廉洁，不冒名顶替其他认证人员实施审核，不编制虚假或严重失实的文件，不出具虚假或严重失实的认证记录和报告，不编造学习经历、工作经历和审核经历。认证人员对信息安全管理体系的认证结论、认证结果的真实性承担相应责任。

认证人员不得发生影响认证公正性和有效性的行为；不得参与近两年内本人咨询过或工作过的组织的认证活动；不得接受认证委托人及其相关利益方的礼金、礼品或其他不当利益；不得到获证组织报销与本次审核无关的食宿交通等费用。

6.2 认决人员能力

认决人员进行认证申请评审和做出认证决定。认决人员应是具有能力的信息安全管理体系审核员，具有信息安全管理体系的技术审查和评审的经历和能力。

7 申请和合同评审

7.1 认证申请

CAS 应要求申请组织的授权代表至少提供以下必要的信息：

7.1.1CAS 应要求申请组织的授权代表至少提供以下必要的信息：

（1）认证申请书

（2）申请组织的法律地位的证明文件（包括：企业营业执照、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，复印件加盖公章。若信息安全管理体系覆盖多场所活动，应附有每个场所的法律地位证明文件的复印件并填写多场所清单（适用时）。

（3）提供法律法规要求的行政许可证明、资质证书、强制性认证证书等的复印件（如生产许可证、3C 证书等），复印件加盖公章。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。

（4）信息安全管理体系成文信息，例如：信息安全管理方针、目标，信息安全管理体系策划所需要的文件，信息安全管理体系的边界覆盖的范围，信息安全附录适用情况（信息安全适用性声明 SOA）、内审报告、管评报告、法律法规识别、重要信息资产清单等。

（5）信息安全管理体系已有效运行 3 个月以上的证明材料。

（6）多场所活动、活动分包情况。

（7）在一年内，未发生违反国家相关法律法规，未因负面情况受到相关监管部门处罚或媒体曝光，或未因负面情况而被其他相关认证机构撤销管理体系认证证书。提供 1 年内没有发生过重大

事故的声明或查询结果。

（8）信息收集文件，包括但不限于：

a．组织的资源管理

b．组织的过程及过程信息安全管理

c．组织的风险管理

（9）企业已通过的其他体系认证（提供复印件）

（10）适用的法律法规清单

（11）其他与认证审核有关的必要文件

7.2 不予受理情况

存在以下情况的组织，本公司不受理其认证申请：

（1）被全国企业信用信息公示系统或者政府其他信用公示系统列入严重违法失信名单的。

（2）被执法监管部门责令停业整顿期间的

（3）一年内被国家级行政抽查发现其产品质量存在严重不合格并予公布的。

（4）一年内发生重、特大事故（事件）的。

（5）其他被政府主管部门认定或被媒体曝光有不符合、违法失信行为，且尚在处理期间的。

7.3 审核人日的确定

7.3.1 企业员工有效人数确认

员工有效人数包括:

1）在认证范围内涉及到的所有全职员工，包括每个班工作的员工。

2）在审核时出现的可等同于全职员工计算的非永久性员工（如季节性员工、临时工和合同工）以及兼职员工。

7.3.2 多现场的确认

7.3.2.1 抽样方法

当客户组织有很多现场满足下面三个准则, 审核必须使用多现场认证抽样方法:

a)所有现场运行在同一个信息安全管理体系下,该信息安全管理体系被集中管理和内部审核、并集 中统一进行管理评审;

b) 所有现场被包括在客户组织的内部信息安全管理体系审核方案和程序中;

c) 所有现场被包括在客户组织的内部信息安全管理体系管理评审方案和程序中;

尽最大可能，初次认证合同评审必须识别现场间的差异以满足确定的适宜的抽样水平。

7.3.2.2 抽样准则

认证机构抽取一个有代表性数量的现场需要考虑：

1) 总部和各分现场的内审结果

2) 管理评审的结果

3) 各现场规模的变化

4)各现场经营目的的变化

5)信息安全管理体系的复杂度

6) 在不同现场信息安全体系的复杂度

7) 工作惯例的变化

8) 所从事活动的变化

9) 关键信息系统或信息系统处理的敏感信息间的潜在相互影响

10) 任何不同的法规要求

有代表性的样本是从客户组织的信息安全管理体系认证范围内的所有现场挑选出来的; 这种抽样选择是基于在反映以上素的判断选择并考虑了随机抽样原理基础上做出的。

7.3.2.3 抽样数量

每次审核最少访问的场所数量是：

初次认证审核：样本的数量应为场所数量的平方根（y＝ √x ），计算结果向上取整为最接近的整数，其中 y 为将抽取场所的数量、x 为场所总数。

监督审核：每年的抽样数量应为场所数量的平方根乘以 0.6 即（y＝0.6 √x ），计算结果向上取整为最接近的整数。

再认证审核：样本的数量应与初次审核相同。然而，如果证明管理体系在认证周期中是有效的，样本的数量可以减少至乘以系数 0.8 即（y＝0.8 √x ），计算结果向上取整为最接近的整数。

在初次认证审核、每次再认证审核以及作为监督的一部分在每个日历年至少一次的审核中，都应对中心职能（详见第 5 章）审核。

当 CAS 对拟认证或获证管理体系涵盖的过程、活动进行风险分析，发现涉及下列因素的特殊情况时，应增加抽样的数量或频率。

场所的规模和员工的数量；

过程、活动以及管理体系复杂程度和风险水平；

工作方式的差异（如：倒班）；

所从事过程、活动的差异；

投诉记录，以及纠正措施和预防措施的其他相关方面；

与跨国经营有关的任何方面；

内部审核和管理评审的结果。

如果组织的分支机构分为不同等级（如：总部办公室/中心办公室，全国性办公室，地区办公室，地方分支），上述的初次认证审核抽样模式适用于每个等级的场所。

示例：1 个总部办公室：每个审核周期（初次审核、监督审核或再认证审核）都访问；

4 个全国性办公室：样本数量＝2，至少 1 个为随机抽样；

27 个地区办公室：样本数量＝6，至少 2 个为随机抽样；

1700 个地方分支：样本数量＝42，至少 11 个为随机抽样

地区办公室的样本中宜至少覆盖到每个全国办公室控制的地区办公室。地方分支的样本中宜至少覆盖到每个地区办公室控制的地区分支。

7.3.3 多现场审核人日说明

多现场审核人日计算方式为 0.5 人日*抽样数量（0 为无多现场）

企业实际审核人日计算公式：

初审人日/监督人日/再认证人日+多现场人日

下述初审/监督/再认证人日确认标准为未考虑多现场的人日标准，最终人日确认时需加多现场审核人日。

7.3.2 审核人日确定标准

CAS 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参考附录 B。

7.3.3 监督审核人日说明

在最初的认证周期中，每年监督审核时间通常为初审时间的 1/3（如果企业人数发生变化，按最新的人数重新测算需要的“初审时间”）。监督周期内发生特殊事故、事件等，按需增加审核人日，最少的监督审核时间为 1 天。

7.3.4 再认证审核人日说明

再认证审核的人日时间通常是按初审认证审核人日计算结果的 2/3，最少的再认证审核时间为 1 天，如果上一周期有重大的不符合提出（严重不符合或重复发生的不符合项），认证人日可以增加。

7.4 申请评审（合同评审）

本机构应根据认证依据、程序文件等的要求，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）CAS 与申请方之间任何已知的理解差异得到消除；

（5）CAS 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）CAS 认证申请评审人员依据附录 A 确定认证审核专业类别。

（8）在评审表中记录依据 7.3 确定的审核人日

8 认证实施程序

8.1 初次认证

8.1.1 建立审核方案

在管理体系认证申请评审完成后，CAS 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。

CAS 审核方案策划人员负责针对每一认证客户建立认证周期内的审核方案，初次认证的审核方案应当包括两阶段初次审核、认证决定之后的监督审核和第三年在认证到期前进行的再认证审核。审核方案应清晰地识别所需的审核活动，这些审核活动用以证实受审核组织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。

注：一个认证周期通常为三年（有特定行业认证方案的除外），从初次认证（或再认证）决定算起，至认证的终止日期截止。

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、人日、地点等；

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)处理信息安全的保密性以及其它类似事宜

8.1.2 确定审核时间及审核组

8.1.2.1 审核时间的确定：依据合同评审及审核方案策划结果确定的审核人日来策划具体的审核时间安排；

8.1.2.2CAS 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。审核组组建原则见第 6 章。

8.1.2.3 本公司提前将审核组成员的姓名、在审核组内身份和审核时间通知给受审核方，使受审核方有足够的时间对所指派审核员提出意见或异议。

如有异议，本公司对审核组进行调整后通知受审核方。如无异议，则正式任命审核组，并为审核组配备审核文件。受审核方可以拒绝审核组某成员的正当理由是：

a)该成员在两年之内曾是或仍然是受审核方的雇员；

b)该成员在两年之内向受审核方提供过旨在建立或保持管理体系的咨询服务；

c)受审核方提出，并经核实，该成员有违背行为准则的行为；

d)其他有影响独立性和公正性的情况。

8.1.3 现场审核的准备

8.1.3.1 文件审核：

审核组长负责审核受审核方提交的部分信息安全管理体系文件，必要时，文件审核范围可扩大到受审核方其它支持性文件。文件审核的结论将及时通知受审核方,只有在文件审核发现的主要问题得到解决或澄清后才能进入受审核方现场开展审核。

8.1.3.2 编制审核计划：

审核组长负责编制审核计划，并提前书面通知受审核方，审核计划发布前应经本公司相关管理人员批准，并得到受审核方确认。对于多场所的管理体系应考虑多场所抽样准则抽样审核。

审核计划至少包括以下内容：审核目的，审核准则，审核范围和边界，拟实施现场审核的日期、时间安排（现场审核活动预期的时间和持续时间）和场所（包括临时场所的访问的日期和时间），审核组成员信息及审核任务安排。

注：专业审核员和技术专家时应当在审核计划中予以明确。

如果信息安全管理体系覆盖范围包括在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授权和控制下，认证机构可以在审核中对这些场所进行抽样，但应根据相关要求实施抽样以

确保对所抽样本进行的审核对信息安全管理体系包含的所有场所具有代表性。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信息安全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。

为使现场审核活动能够观察到产品生产或服务活动情况，现场审核应安排在认证范围覆盖的产品生产或服务活动正常运行时进行。

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

8.1.4 一阶段审核

8.1.4.1 一阶段审核实施

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。

信息安全管理体系一阶段审核必须为现场审核。

审核组需查看企业信息资产、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、信息安全标准附录在企业的适用情况确认等，以确认：

（1）受审核方的管理体系得到策划和实施，并进行了有效的内审与管评；

（2）受审核方的管理体系已运行超 3 个月，并有足够的证据证明其运行情况；

（3）受审核方对运行的管理体系进行了监视、测量、分析和评价，并有充分的证据；

（4）受审核方对管理体系进行了有效的持续改进；

（5）受审核方是否识别并遵守了相关的法律法规；

（6）受审核方有充足的资源保障二阶段审核的进行；

（7）收集关于客户的管理体系范围、过程和场所的必要信息，包括：

a)客户的场所

b)使用的过程和设备

c)所建立的控制的水平（特别是客户为多场所时）

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。

8.1.4.2 审核范围变更

在审核过程中，审核组发现企业活动不能覆盖审核范围时，与受审核方说明理由，商定后续措

施。填写信息变更评审表，经 CAS 评审批准后实施。

8.1.4.3 一阶段审核结束后的活动

审核组在一阶段结束后应将第一阶段审核情况形成书面文件告知受审核方。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，要及时提醒受审核方特别关注。

且审核组应结合受审核方的申请材料、审核方案以及一阶段审核的结果对二阶段审核做出具体安排，出具审核计划包括但不限于具体的时间安排、审核组成员对受审核方按部门活动以何种方式进行评价的安排、高层沟通的安排和会议的安排。审核组长应至少在实施现场审核之前，与受审核方就审核计划进行充分沟通，确保双方在理解上没有歧义。

8.1.5 二阶段审核

8.1.5.1 二阶段审核实施：

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。

J）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。

K）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。

L）信息资产的识别情况与信息风险识别控制情况等。

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，说明理由，商定后续措施。如果需要改变审核目的、审核范围或终止审核时，应经 CAS 评审批准后实施。

8.1.5.2 终止审核情况

二阶段审核过程中，当发生以下情况时，审核组应向本公司报告，经本公司同意后终止审核：

（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。

8.1.6 初次认证的审核结论

审核组应该对一阶段审核和现场审核中收集的所有信息和证据进行汇总分析，评价审核发现并就审核结论达成一致。

如果现场审核发现不符合项和观察项应开具不符合项报告或观察项报告，且获得受审核方认同。

现场审核结束，审核组应形成是否推荐认证注册的结论；审核组可以根据一阶段审核结果和二阶段审核的结果对受审核方的管理体系是否满足所有适用的认证依据的要求进行评价，并判断是否推荐认证注册。

现场审核结束后，受审核方不符合整改结束后，审核组长完成审核报告编制工作，并与受审核方进行沟通，确保双方对报告的理解上没有歧义。

8.2 监督审核

8.2.1 监督审核的方式

CAS 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。

8.2.2 监督审核内容

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)信息安全管理体系企业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。

监督审核必审要素：监督审核是现场审核，但不一定是对整个体系的审核，由于市场、季节性等原因，在每次监督审核时难以覆盖所有产品和服务的，在认证证书有效期内的监督审核需覆盖认证范围内的所有产品和服务。

获证客户应保存全部投诉记录，需要时提供认证机构。

CAS 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。

8.2.3 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。

初次认证后的第一次监督审核应当在认证证书签发日起 12 个月内进行。此后，监督审核应当至少每个日历年（应进行再认证的年份除外）进行一次，正常情况下，第二次监督应从第一次监督审核的评定决定日期起 12 个月内进行，特殊情况可以适当延长，但最晚两次监督审核的时间间隔不得超过 15 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。

超期而未能实施监督审核的，应按暂停证书或撤销证书的相关要求执行。

8.2.4 信息收集

在进行监督审核之前，CAS 需要收集获证组织的管理体系相关信息，以确定获证组织的管理体系相关信息是否发生变化。需要客户提供的信息包括以下几个方面：

a)基本信息，包括组织名称、地址、联系人、法人等信息的变化情况；

b)组织信息，包括范围、组织架构、人员数量等信息的变化情况；

c)管理体系相关信息，关键文件化信息的变化情况。

d)其他变更情况

8.2.5 信息评审

合评人员应对获证组织的信息确认文件进行评审，以确定：

1)获证组织的管理体系变化情况，尤其是管理体系范围的变化；

2)是否需要修订审核方案。

3）监督人日是否发生变化

8.2.6 确定审核时间及审核组

CAS 应根据获证组织的行业、规模和业务复杂程度组建审核组，和企业确认审核时间，指派审核组长。相关规定同 8.1.2 规定。

8.2.7 编制审核计划

审核组应结合获证组织的信息确认文件、审核方案对监督审核中现场审核的策划对现场审核做出具体安排，包括但不限于具体的时间安排、审核组成员对获证组织按部门和活动以何种方式进行评价的安排、高层沟通的安排和会议的安排。审核组长应至少在实施现场审核 3 个工作日之前，与获证组织就审核计划进行充分沟通，确保双方在理解上没有歧义。

信息安全的监督审核并不覆盖标准所有条款，监督审核的抽样采取抽样的方式进行，抽样准则为：

1)两次监督审核必须覆盖标准所有条款和所有部门；

2)标准中对信息安全管理过程有决定作用的条款和部门每次监督审核都需要抽到；

3)获证组织前一次审核的不符合项及相关条款在本次监督审核中需要抽到；

4)审核组认为重要的条款应考虑进行抽样。

8.2.8 现场审核

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 CAS 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及验证的安排。

8.2.9 监督审核的审核结论

审核组应该对监督审核中收集的所有信息和证据进行汇总分析，评价审核发现并就审核结论达成一致。

如果现场审核发现不符合项和观察项应开具不符合项报告或观察项报告，且获得受审核方认同。

现场审核结束，审核组应形成是否推荐保持认证注册的结论；审核组可以根据现场监督审核的结果对获证组织的管理体系是否满足所有适用的认证依据的要求进行评价，并判断是否推荐保持认证注册。

现场审核结束后，受审核方不符合整改结束，审核组长完成审核报告编制工作，并与受审核方进行沟通，确保双方对报告的理解上没有歧义。

8.3 再认证

8.3.1 再认证要求

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。

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。

8.3.2 信息收集

在进行再认证审核之前，CAS 需要收集获证组织的管理体系相关信息，以确定获证组织的管理体系相关信息是否发生变化。需要客户提供的信息包括以下几个方面：

a．基本信息，包括组织名称、地址、联系人、法人等信息的变化情况；

b．组织信息，包括范围、组织架构、人员数量等信息的变化情况；

c．管理体系相关信息，关键文件化信息的变化情况。

d.其他变更情况

8.3.3 信息评审

合评人员应对获证组织的信息确认文件进行评审，以确定：

1)获证组织的管理体系变化情况，尤其是管理体系范围的变化；

2)是否需要修订审核方案。

3）再认证及后续监督人日数是否发生变化

8.3.4 重新建立审核方案

根据受审核方最新信息参照 8.1.1 执行建立新的审核方案。

8.3.5 确定审核时间及审核组

CAS 应根据获证组织的行业、规模和业务复杂程度组建审核组，和企业确认审核时间，指派审核组长。相关规定同 8.1.2 规定。

8.3.6 编制审核计划

审核组应结合获证组织的信息确认文件、审核方案对监督审核中现场审核的策划对现场审核做出具体安排，包括但不限于具体的时间安排、审核组成员对获证组织按部门和活动以何种方式进行评价的安排、高层沟通的安排和会议的安排。审核组长应至少在实施现场审核 3 个工作日之前，与获证组织就审核计划进行充分沟通，确保双方在理解上没有歧义。

信息安全的再认证审核需覆盖标准所有适用条款及受审核方所有活动。

8.3.7 现场审核

再认证现场审核的程序和要求参照 8.1.5 条实施。

7.3.8 再认证的审核结论

再认证现场审核的审核结论参照 8.1.6 条实施。

8.4 特殊审核

8.4.1 扩大认证范围审核

对于已授予的认证，本公司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，也可以单独进行，对扩大认证范围的评审、审核策划和实施等过程依据《认证业务范围专业管理及扩大缩小认证认证/认可范围管理程序》规定实施。

8.4.2 提前较短时间通知的审核

CAS 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)CAS 应说明并使获让客户提前了解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,CAS 在指派审核组时给予更多的关注。

8.4.3 暂停、撤销认证资格、缩小认证范围

8.4.3.1 暂停、撤销认证资格

CAS 已制定了暂停、撤销认证资格的相关程序文件，并规定审核后续措施。

1）发生以下情况(但不限于)时,CAS 将暂停获证客户的认证资格:

——获证客户的信息安全管理体系持续地或严重地不满足认证要求，包括对信息安全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;

——不承担、履行认证合同约定的责任和义务的；

——被有关执法监管部门责令停业整顿的；

——持有的与信息安全管理体系范围有关的行政许可证明、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的；

——获证客户主动请求暂停；。

——其他应当暂停认证资格的；

在暂停期间，获证客户的信息安全管理体系认证暂时无效。如果造成暂停的问题已解决,本公司恢复被暂停的认证资格。如果客户未能在规定的时限内解决造成暂停的问题,认证机构应撤销其认证资格。注:多数情况下,暂停将不超过 6 个月。

2）获证客户有以下情形之一的，本公司在获得相关信息并调查核实后 5 个工作日内撤销其认证资格：

——被注销或撤销法律地位证明文件的。

——被国家市场管理总局列入信用严重失信企业名单

——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的。

——拒绝接受国家产品质量监督抽查的。

——出现重大的产品和服务等质量安全事故，经执法监管部门确认是获证组织违规造成的。

——有其他严重违反法律法规行为的。

——暂停认证证书的期限已满但导致暂停的问题未得到解决或纠正的（包括持有的与信息安全管理体系范围有关的行政许可证明、资质证书、强制性认证证书等已经过期失效但申请未获批准）。

——没有运行信息安全管理体系或者已不具备运行条件的。

——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。

——其他应当撤销认证证书的。

3）撤销认证资格后，本公司及时收回撤销的认证证书。若无法收回，本公司及时在相关媒体和网站上公布或声明撤销决定。

4）本公司暂停或撤销认证资格在本公司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。

5）本公司采取有效措施避免各类无效的认证证书和认证标志被继续使用。

8.4.3.2 缩小认证范围审核

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,CAS 将缩小其认证范围，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。这类审核活动可以和监督审核同时进行。也可以依据客户申请资料经文件评审后作出认证决定。

8.4.4 恢复认证注册资格审核

在确定的认证注册资格暂停期限结束前，根据暂停原因，组织在规定期限内，向 CAS 审核部提出恢复认证注册资格，存在需整改要求的，应附有相关纠正措施和有效性验证材料；经本公司审定，确认获证组织的暂停认证资格的原因已消除，认证范围及活动已恢复符合信息安全管理体系的认证要求，CAS 将作出同意恢复认证资格的审定结论，并进行公告。

8.5 结合审核

当申请组织在运行信息安全管理体系的同时还运行了其他管理体系，若其他管理体系在 CAS 的认证业务范围内，CAS 可以根据申请组织的需求对管理体系进行单独的审核，或者对多个管理体系进行结合审核，但 CAS 需确保在结合审核的情形下，对诸如审核范围的界定、审核时间的确定、审核方案的策划等进行有效的管理。

对于结合审核，必须以审核活动满足体系认证所有要求为前提，并且审核的质量不应由于结合审核而受到负面影响。在审核报告中，应清晰体现所有与管理体系有关的重要要素的描述并易于识别。

8.6 不符合纠正的验证

审核组应当根据审核发现形成严重或轻微不符合，要求受审核方在规定的时限内对不符合进行原因分析、采取相应的纠正和纠正措施（轻微不符合可以是纠正措施计划）。

对于严重不符合，CAS 及审核组长应督促受审核方及时进行整改，并对其纠正和纠正措施的有效性进行验证。CAS 规定严重不符合项的验证时限，并至少满足：

（1）初次认证：在二阶段审核结束之日起 6 个月内完成；

（2）监督审核：在审核结束之日起 3 个月内完成；

（3）再认证：严重不符合应在证书到期前完成，一般不符合应在证书到期后 6 个月内完成。

对于组织未能在规定的时限完成对不符合所采取措施的情况，审核组不应当给予该受审核方推荐认证、保持认证或再认证换发认证证书的结论。

8.7 审核报告

CAS 就每次审核（一阶段除外）向受审核方提供完整详实的审核报告。审核组长应对审核报告的内容负责。

审核报告的内容应当反映受审核方管理体系的真实状况，描述对照相应认证标准的符合性和有效性的客观证据信息，及对认证结论的推荐意见。审核报告应重点反映受审核方管理体系所取得的绩效，受审核方实际情况与其预期管理体系目标之间存在的差距和改进机会。

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）受审核方的名称和地址及受审核方的代表。

（2）审核的类型（如初次、监督、再认证或特殊审核）、审核准则和审核目的；

（3）审核方范围，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；

（4）审核活动（现场或非现场，固定或临时场所）的实施日期和地点；

（5）任何偏离审核计划情况及其理由，包括对审核风险及影响审核结论的不确定性的客观陈述；任何影响审核方案的重要事项；

（6）审核组组长、审核组成员及其个人注册信息；任何与审核组同行的人员的相关信息；

（7）与审核类型的要求一致的审核发现、对审核证据的引用以及审核结论；

（8）适用时，上次审核后发生的影响客户管理体系的重要变更；

（9）已识别出的任何未解决的问题；

（10）适用时，是否为结合、联合或一体化审核；

（11）说明审核基于对可获得信息的的样过程的免责声明；

（12）审核组的推荐意见，即审核组对是否通过认证的意见建议；

（13）适用时，对认证文件和认证标志的使用的控制要求；

（14）适用时，对以前不符合采取的纠正措施有效性的验证情况；

（15）关于管理体系满足适用要求和实现预期结果的能力；叙述审核实施过程及各项要求的审核工作情况，对重点审核内容进行描述或引用审核证据、审核发现和审核结论；对信息安全目标和过程及信息安全绩效实现情况进行评价；

（16）内部审核和管理评审的过程；

（17）对认证范围适宜性评价；

（18）确认是否达到审核目的；

（19）本次审核识别出的不符合项。

CAS 保留用于证实审核报告中相关信息的证据。

CAS 在作出认证决定后 30 个工作日内将审核报告提交受审核方，并保留签收或提交的证据。

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，CAS 将此报告及终止审核的原因提交给受审核方，并保留签收或提交的证据。

8.8 复核及认证决定

CAS 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，作出认证决定。

CAS 认证决定或复核人员为认证机构管理控制下的人员，审核组成员不得参与对审核项目的认证决定。

CAS 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 8.7 中的要求，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，本公司已评审、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，实现信息安全目标有重大疑问;

②制定的信息安全目标不可测量、或测量方法不明确;

③对实现信息安全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其他不符合项：轻微不符合项，CAS 已进行了评审、接受了受审核方的纠正和纠正措施或计划采取的纠正和纠正措施；

⑤严重不符合项，CAS 已进行了评审、接受并验证了纠正和纠正措施的有效性；

在满足以上要求的基础上，CAS 有充分的客观证据证明受审核方满足下列要求的，评定该受审核方符合认证要求，向其颁发认证证书。

（1）受审核方具备应有的法定资格和资质，且其信息安全管理体系的运行基本符合标准要求，运行基本有效；

（2）认证范围覆盖的活动、产品和服务符合相关法律法规要求，未发生重大事故和严重违法行为；（注：授予的认证范围应当基于受审核方的法律地位文件及审核范围，不得大于其营业执照范围和行政许可范围以及审核范围。）

（3）受审核方按照认证合同规定履行了相关义务。

受审核方不能满足上述要求或者存在以下情况的，评定该受审核方不符合认证要求，以书面形式告知受审核方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，不符合标准的要求。

（2）发现受审核方存在重大质量安全问题或有其他与产品和服务质量相关严重违法违规行为，与信息安全相关的违法违规行为等。

CAS 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。

适用时，监督审核可以无需独立的认证决定，本公司可以根据审核组长的肯定性结论保持对受审核方的认证，除非需要暂停、撤销和变更认证证书的情况。

再认证审核的认证决定宜在上一认证周期认证证书到期前完成，最迟应当在证书到期之日起 6 个月内完成。

8.9 认证证书和认证标志

8.9.1 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。

认证证书中的获证组织及认证有关的信息应当真实、准确，不违反有关法规要求，认证证书应至少包含以下信息：

（1）获证组织名称、注册地址和统一社会信用代码，该信息应与其法律地位证明文件的信息一致；

（2）信息安全管理体系覆盖的生产经营或服务的地址，获证组织的信息安全管理体系所覆盖的产品、活动、服务的范围；若认证的信息安全管理体系覆盖多场所，应表述覆盖的所有场所的名称和地址信息。

（3）信息安全管理体系认证依据标准、技术要求等；

（4）证书编号。

（5）本公司名称（发证机构名称）。

（6）发证日期和有效期的起止年月日。

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。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。

（7）相关的认可标识及认可注册号（适用时）。

（8）证书查询方式。本公司除在本机构网站上公布认证证书的查询方式外，还在证书上注明：“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。

8.9.2 认证证书状态管理规定

8.9.2.1 认证证书在有效期内可分为以下四种基本状态：

1）有效

定义：获证组织的管理体系或产品持续符合认证标准和要求，认证证书处于正常、可使用的状态。

维持条件：

按时接受并通过监督审核；

按时接受并通过再认证审核；

持续遵守认证合同及本机构的相关规定；

及时缴纳认证费用；

未发生任何可能导致暂停或撤销的重大变更或不符合。

2）暂停

定义：获证组织的管理体系或产品出现暂时性的不符合，但尚未达到撤销程度。在暂停期间，认证证书暂时无效，获证组织不得对外宣称或使用认证资格进行宣传。

转换条件（出现以下情况之一即可暂停）：

获证组织未按时接受监督审核或再认证审核；

获证组织的管理体系或产品持续地或严重地不满足认证要求，但认为可在短期内采取纠正措施予以解决；

获证组织主动请求暂停；

获证组织未按时缴纳认证费用；

获证组织发生影响管理体系运行的重要变更（如地址、法人、关键设备、重要过程等）未及时通报，且未接受变更确认；

其他违反认证合同约定的行为。

暂停期限：通常不超过 6 个月。逾期未完成整改或恢复审核的，将予以撤销。

3）撤销/注销

定义：

撤销： 因获证组织严重违反认证要求或未能解决导致暂停的问题，由本机构主动做出的取消认证资格的决定。撤销具有惩戒性质。

注销： 因获证组织主动放弃认证资格、法人消亡或其他不可抗力因素，由双方协商终止认证合同。注销通常是自愿行为。

撤销条件：

在证书暂停期内，未能在规定期限内采取有效纠正措施并经验证；

审核中发现其管理体系存在严重失效或欺诈行为（如虚假宣传、提供虚假信息）；

发生重大质量、环境、安全事故，且直接影响管理体系的有效性；

拒不配合监督审核、再认证审核或问题调查；

认证要求发生变更后，获证组织未能在规定期限内满足新要求。

注销条件：

获证组织主动书面申请不再保持认证资格；

获证组织依法终止经营；

因不可抗力导致认证活动无法继续进行。

4）扩大/缩小认证范围

定义：在证书有效期内，对认证所覆盖的产品、服务、过程、场所等范围的变更。

转换条件：

扩大范围： 获证组织申请扩大范围，并通过本机构安排的审核（可能为专项审核或与监督审核结合），确认其符合扩展部分的标准要求。

缩小范围： 获证组织主动申请缩小范围，或其在监督审核中被发现某一部分范围持续不符合要求，经认证决定后予以缩小。

8.9.2.2 管理流程

状态监控与信息收集

市场部应建立证书状态监控清单，定期（如每月）审查证书有效性。信息收集来源包括：监督审核/再认证审核报告、获证组织主动通报、官方通告、媒体信息、投诉等。

状态变更启动

当发生本规定转换所述情况时，由审核部经理提出状态变更建议，并附上相关证据（审核报告、投诉记录、缴费情况、获证组织来函等）。

认证决定

暂停决定： 由审核部经理批准执行，并报认证决定委员会备案。

撤销/注销决定： 由审核部准备材料，提交技术决定委员会审议并做出最终决定。

范围变更决定： 由认证决定人员根据审核结论做出决定。

通知与公告

任何证书状态变更决定正式生效后，审核部应提前【7】个工作日书面正式通知获证组织，说明变更原因、依据和生效日期。

对于撤销、注销的证书，审核部应及时在本公司官方网站上进行公告，并按规定上报国家认证认可监督管理委员会（CNCA）。

记录与归档

证书状态变更过程中的所有记录，包括但不限于：状态变更审批表、通知函、相关证据材料、会议纪要等，均应由审核部统一归档保存，保存期限应符合认证规范要求。

8.9.3 认证证书及认证标志要求

本公司对认证证书和认证标志的使用要求以书面形式告知获证客户，获证客户误用认证证书和标志，可能导致认证资格的暂停或撤销。获证客户一旦发现误用认证证书和标志的，应立即采取纠正措施并报告本公司审核部。

9 认证转换

CAS 应当履行社会责任，严禁以牟利为目的受理不符合信息安全管理体系认证标准、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。

CAS 受理组织申请转换为本公司的认证证书，应该详细了解申请转换的原因，必要时进行现场访问。

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。已失效的认证证书可按初次认证受理。

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。

10 信息通报

10.1 需要通报的信息

获证客户应建立向 CAS 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) 信息安全管理体系：适用性声明及其版本发生变化。

10.2 信息通报的要求

信息通报执行以下要求：

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)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）；

c)其他重要信息。

10.3 信息通报相关规定

当认证要求变更时，本公司及时将变更的文件或要求发给所有获证的组织，同时，通过网络向社会公告。

CAS 根据认证要求变更的性质和内容，采取适当的方式对获证组织实施变更后的认证要求的有效性的验证，如文件审核、现场补充审核等；根据以上过程确认认证要求变更后获证组织的证书是否保持有效。

11 申诉、投诉、争议的处理

CAS 已建立了申诉、投诉、争议的处理程序。对本公司或审核人员违反国家认证法律法规、认证认可规范、缺乏公正性、对认证评价结果等有异议时，可向本公司提出申诉和投诉。本公司将在 30 日内将处理情况以书面形式给予答复。

对本公司在申诉、投诉、争议的处理有异议时，可向国家认证认可监督管理委员会提出申诉或投诉。

12 认证档案的管理

CAS 已建立认证档案管理制度，记录认证活动全过程并妥善保存。

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。

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。

所有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，但是原件必须妥善保存，保存时间至少应当与认证证书有效期一致。

13 其他

本规则内容提及信息安全管理体系标准时均指认证活动发生时该标准的有效版本。认证活动及认证证书中描述该标准号时，应采用当时有效版本的完整标准号。

本规则所提及的各类证明文件的复印件应是在原件上复印的，并经提交人员签字确认与原件一致。

认证机构可开展信息安全管理体系及相关技术标准的宣贯培训，促使组织的全体员工正确理解和执行信息安全管理体系标准。

附录 A ISMS 认证业务分类与分级

大类	中类	小类	级别	描述	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		二	医疗服务	
	02.06		三	教育	
	02.07		三	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		三	旅游、宾馆、饭店	
	03.06		三	其他	
04				产品的生产	产品包括软件、硬件、流程性材料和服务
	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	加工、生产、制造等工业企业	
		04.13.03	三	建筑工程施工及工程服务企业	
		04.13.04	三	物业服务企业	
		04.13.05	三	其他	

附录 B 信息安全管理体系认证审核时间要求

基本人日数计算表

雇员总数	初次审核时间			监督审核时间		再认证时间	
	总人日数	一阶段	二阶段	总人日数	现场时间	总人日数	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	

注：1.有效人数包括认证范围内涉及的所有人员（含每个班次的人员）。覆盖于认证范围内的非固定人员（如：承包商人员）和兼职人员也应包括在有效人数内。

2.对非固定人员（包括季节性人员、临时人员和分包商人员）和兼职人员的有效人数核定，可根据其实际工作小时数予以适当减少或换算成等效的全职人员数。

3.表中所列一二阶段人日示例为无增减系数情况下给出的现场审核时间（策划和编制报告一起所用的时间为 20%）。

组织存在增加审核时间的其他因素，例如： a) 复杂的后勤，在 ISMS 范围中涉及不止一处建筑物或地点；b) 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； c) 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；d) 适用于 ISMS 的标准和法规数量很多。应根据实际情况计算增加的系数。

组织存在允许减少审核时间的因素，例如： a) 没有风险或者低风险的产品/过程； b) 过程只涉及单一的常规活动（例如，只有服务）； c) 在组织控制下工作的雇员大部分是从事相同的任务； d) 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）； e) 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）； f) 高度成熟的管理体系。可根据实际情况计算减少的系数。为了确保能够实施有效的审核并确保可靠和可比较的结果，对表 B 中审核时间的 减少，不应超过 30%。

宜考虑上述因素，并根据这些因素对审核时间做出调整。这些因素可证实一次有效审核所需更多或更少的审核时间的合理性。增加时间的因素可被减少时间的因素冲抵。 在任何情况下，对审核时间表中的时间的调整，应保持足够的证据和记录来证实其变化的合理性。

最终现场审核时间可在计算增减系数后计算出的审核时间基础上乘以 80%（策划和编制报告一起所用的时间）得出。并对计算数据小数位按照 0.25（不含）以下取整为 0，0.25（含）~0.75（不含）取整为 0.5，0.75（含）取整为 1。

4.组织正常工作期间（如轮班制组织）安排的审核时间可以计入有效的管理体系认证审核时间，但往返多场所之间所花费的时间不应计入有效的信息安全管理体系认证审核时间。

5.本表所列时间为初次认证审核时间，监督审核时间为初审的 1/3，再认证审核时间为初审的 2/3，特殊审核时间依据审核方案策划具体约定。

6.与其他管理体系结合审核时间不低于单独审核时间的 80%。具体打折系数依据 CNAS-CC106 之规定测算和选取。