版本/ 版次	修订内容	修订日期	修订人
C/0	组织结构变化（部门合并）	2025.03.18	黄 云
C/1	合理化修订	2025.10.16	张道金
C/2	依国家认监委新版认证规则相关要求修订	2026.01.23	张道金

批准　　黄　云

审核　　/

制订　　张道金

发布日期	修订日期	实施日期
2020.10.27	2026.01.23	2026.01.23

1、目的和适用范围

1.1 目的

为规范信息安全管理体系认证业务活动过程，确保认证服务过程的合规、有效，保证认证服务质量，提升认证公信力，特制定本程序。

1.2 范围

本程序适用于中标通信息安全管理体系认证的询议价及申请受理、申请评审、合同签署、审核方案策划、策划审核、初次审核、实施审核、认证决定、保持认证、申诉/投诉与争议处理、客户的记录管理等过程的实施与控制。

2、引用文件

下列文件中的条款通过本文件的引用而成为本文件的条款。规范性引用文件中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

2.1 CNAS-CC01《管理体系认证机构要求》

2.2 CNAS-CC170《信息安全管理体系认证机构要求》

2.3 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》

3、术语定义

无。

4、工作职责

4.1 运营部

4.1.1 负责认证项目的询议价及申请受理、申请评审、审核方案的策划、审核组的选派，以及初次审核、监督审核、再认证审核、及特殊审核的实施。

4.2 技术部

4.2.1 负责认证决定、证书制作、以及证书状态管理的实施。

4.2.2 负责为运营部提供认证技术的支持。

4.3 行政部

4.3.1 负责为运营部提供认证人员的能力和数量的支持。

4.3.2 负责合同原件的保管。

4.4 总经理

4.4.1 负责认证项目的合同签署。

5、工作程序

5.1 询议价及申请受理

5.1.1 客户接洽

5.1.1.1 运营部接到客户的问询时，需了解客户的基本情况和需求，如：客户的业务活动类型、产品类型、地址、规模、希望的获证时间、差旅控制要求等与认证相关的信息，并解答客户的任何问题。告知申请 ISMS 认证的客户须符合国家对信息安全管理的法规或通知要求，例如工信部联协[2010]394 号，以及工信部 2011 年第 21 号等文件的要求，并要求客户承诺遵守相关要求。要求客户向中标通说明适用的关于认证机构的资质、诚信守法记录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，并即时更新该说明，以便中标通判断自已是否具备对该客户实施认证活动的资格或条件。同时根据《信息通报与处理管理程序》的要求，向客户提供公开信息、客户应具备的条件、认证过程和要求、《商务行为守则》（见附录 A）、《认证收费标准》（见附录 B）、等信息资料的获取渠道(中标通网站：www.zbtrz.cn)。

对客户的接洽实行首问责任制，首次接洽的人员对该项目负责到底。若了解到客户的基本情况和需求能满足受理条件，运营部业务人员告知客户提交申请资料，若不能够满足受理条件时，运营部业务人员告知客户不满足的具体原因，并提出相应的解决方案，若客户同意解决方案，运营部业务人员告知客户提交申请资料。

5.1.1.2 运营部及时跟踪客户，向具有意向的客户提供《认证申请表》、《认证合同书》及其附件资料模板，指导客户填写《认证申请表》、《认证合同书》及其附件资料，并要求其授权代表及时提交文件化的申请资料，申请资料至少包括以下文件：

a）认证申请表，至少包括拟认证组织的名称、地址、认证依据的标准、申请的认证范围、认证范围内人员数量及影响体系有效性的外包过程；

b）拟认证组织声明承诺、体系覆盖人员花名册、固定/临时多场所清单（适用时）、临时服务点清单（适用时）；

c）法律地位的证明文件,当ISMS覆盖多个法律实体时，应提供每个法律实体的法律地位证明文件；

d）申请认证范围内所涉及的网络安全法规要求的行政许可文件、资质证书等（适用时）；

e）组织机构及职责；

f）生产/服务的流程、班次及轮班情况；

g）依据ISO/IEC 27001标准建立的文件化信息安全管理体系，体系运3个月以上，已完成了内部审核和管理评审，如有多场所，内审及管理评审应覆盖多场所。

h）信息安全管理体系调查表：客户的信息安全风险因素、信息安全复杂因素；

i）信息安全管理体系的适用性声明；

j）一年内所发生的网络安全相关的行政处罚以及整改情况（适用时）

k）其他需要的文件。

5.1.1.3 客户提交的文件化申请资料信息必须清晰完整，以便中标通确定：

a）申请认证的范围；

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

c）识别客户采用的所有影响符合性的外包过程；

d）有关生产/服务和班次的详细信息；

e）客户寻求认证的标准或其他要求；

f）是否接受过与拟认证的管理体系有关的咨询，如果接受过，由谁提供咨询。

5.1.1.4 针对客户组织提交的ISMS，中标通须重点确保其体系内容结构是否满足ISO/IEC 27001的要求，其必要的信息安全控制是否满足了客户的策略与目标。客户须针对其适用的控制源及控制措施制定《信息安全适用性声明》和信息安全策略。客户组织的必要控制可以来自于ISO/IEC 27001附录A的控制措施，也可以是其自行设计的，也可以是从任何控制源中选取的，关键是控

制源及控制措施适合组织的信息资产风险控制的特点。只要能满足客户的策略与目标，即使组织的必要控制不是来自于ISO/IEC 27001附录A的控制措施，也可以获得ISO/IEC 27001认证。中标通不事先拟定客户ISMS实施的特殊方式或文件和记录的特殊格式。

5.1.1.5 对已获其他认证机构颁证的客户，按照《认证证书的转换管理程序》的要求提交证书转换申请所需的资料。

5.1.2 申请受理

运营部业务人员将收集到的客户信息，对照清单进行完整性评价，当发现不正确或缺失时要求客户补充提交，直至满足要求。

运营部业务人员或指定的信息录入人员将收集到的客户信息录入到ERP系统，并将客户提交的申请资料移交给申请评审人员。

5.2 申请评审

5.2.1 运营部申请评审人员依据提交的资料信息对照《认证申请受理评审表》对客户提交资料完整性、合规性进评价，评价结果填入《认证申请受理评审表》中。申请评审人员对申请资料满足要求的项目进行申请评审，以确定本公司是否具备实施该项目的能力（包括专业能力），评审结果填入《合同评审表》。当评审人员不具备专业知识时须由专业技术人员提供技术支持，判定客户是否符合认证申请受理条件，同时确定中标通系统内审核组及进行认证决定是否具备相应能力。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”的客户，中标通不受理其认证申请。

5.2.2 申请评审须充分、有效，并保存评审记录，做出评审结论以确保：

a)客户及其管理体系的信息足以建立审核方案；

b)识别客户的行业类别和与之相应的管理体系所管理的过程特性和管理要求；

c)识别国家对相关行业的管理要求是否满足,包括工信部联协[2010]394号文件，及2011年第21号公告等文件的要求；

d)中标通与客户之间的任何已知的理解差异得到解决；

e)中标通有能力并能够实施认证活动；

f）征询客户对中标通的认证机构资质、诚信守法记录或认证人员身份背景、信息安全与保密管理能力的要求，并评审是否满足要求；

g)申请的认证范围、员工人数、认证覆盖人数、客户的运作场所（如有多场所侧其提供的内审及管理评审资料应覆盖所有多场所）、完成审核需要的时间和任何其他影响认证活动的因素（语言、安全条件、对公正性的威胁等）；对于不同性质和不同行业的客户，其ISMS认证所覆盖的范围，可视客户要求的表达方式、产品/服务类型、活动场所、组织界限等因素予以描述；

h)保存决定实施审核的理由的记录。

注1：员工人数是仅指在认证覆盖的物理边界及业务管理边界直接相关人员的数量，不一定是组织的所有员工数量，不在认证覆盖的边界范围内的人员，不记入员工人数。

注2:认证覆盖人数仅指在认证覆盖的物理边界及业务管理边界范围内与对要认证项目管理活动直接相关的人员数量，不一定是组织的员工人数。计算方法见“CNAS-CC170：2024《信息安全管理体系认证机构要求》，附录C（规范性附录）：审核时间，C.3.4 确定初始人数”部分。

5.2.3 申请评审人员根据上述评定的认证范围及专业类别、认证覆盖人数、场所、审核方式、审核时间以及客户的特定要求等，确定中标通审核组及进行认证决定需要具备的能力通用能力和特定技术领域的专业能力以及审核日程的可行性，确保审核组及进行认证决定需要具备的能力符合对应的管理体系认证人员能力准则要求，以确保中标通有能力在拟认证的范围、运作场所、活动场所实施认证并能满足申请方的其他特殊要求，如审核时间、审核方式等方面要求，确保中标通有能力客观、公正地做出决定前的复核评审和认证决定。

5.2.4 满足以下条件的，认证机构可以受理申请认证：

a）认证委托人已具备《信息通报与处理管理程序》的附录A:《拟认证组织须知》之A 3.1所要求的条件；

b）认证机构具备实施认证的能力；

c）双方就认证事宜达成一致。

5.2.5 申请评审结果为可以受理的认证项目，由运营部以《认证申请受理通知书》通知申请方，并与其沟通协商最终的合同方案。评审发现的问题经过客户整改直到满足要求，保留评审记录。申请评审未通过的，运营部须通知认证申请人在规定时间内补充、完善，或拒绝受理认证申请，拒绝受理时，运营部需告知客户拒绝理由，并使客户清楚拒绝的原因。

5.3 合同签署

5.3.1 总体要求

对申请评审通过的认证项目，中标通须与每个客户之间签订在法律上具有强制实施力的提供认证服务的书面《认证合同书》，明确认证服务提供的基本事项双方的责任和义务。客户有多个场所时须在合同中体现，具体多场所信息可以多场所清单的方式单独列出。

5.3.2 合同内容

5.3.2.1认证合同要至少包含以下内容：

a）客户获得认证后持续有效运行管理体系的承诺；

b）客户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；

c）客户承诺获得认证后发生以下情况时，要及时向中标通通报：

1）相关方有重大投诉；

2）管理体系或信息安全被信息安全监管或市场监管部门认定不合格；

3）发生管理体系相关的重大事故；

4）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；取得的行政许可资质、强制性认证或其它资质变更；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；活动边界、产品工艺、生产规模变更；认证评价覆盖的活动范围变更；相关管理系统或重要过程（适用的法律法规、过程方式等）变更等重大变更；

5）出现影响管理体系运行的其他重要情况。

d）客户承诺获得认证后正确使用认证证书、认证标志和有关信息，不利用管理体系认证证书和相关文字、符号误导公众认为其产品/服务通过认证；正确宣传认证结果，不损害认证机构的声誉；

e）拟认证的管理体系覆盖的生产/服务的活动范围；

f）在认证审核实施过程及认证证书有效期内，中标通和客户各自要承担的责任、权利和义务，包括暂停、撤销相关处理的责任、权利和义务；

g）认证服务的费用、付费方式及违约条款；认证费用应由认证委托人向认证机构直接支付；

h）客户隐瞒真实信息的责任；

i）因认证机构批准资质注销或被撤销导致获证组织认证证书无法有效保持的责任和经济赔偿。

5.3.2.2 认证合同还必须就控制审核和认证活动引发的客户信息安全风险做出规定，包括明确中标通和客户及其有关人员的责任与义务。例如：接受认证机构的信息安全和数据保护措施和规则，事先向审核组说明与认证审核相关必要的信息管理系统基本知识及特定的网络和信息安全知识，遵守信息安全管理相关要求等。

5.3.3 签署生效

5.3.3.1中标通总经理或授权人员负责与申请方负责人或其授权人共同签字、盖章，生成具有法律效力的《认证合同书》。合同编号按《记录控制程序》中的合同编号原则进行合同编号,合同原件由行政部保管。

5.3.3.2运营部负责将合同签定信息传递给行政部，由行政部落实有关收费管理，并将客户认证申请和认证合同资料以复印件或电子档传递给运营部，以便安排审核工作。

5.4　审核方案策划

5.4.1 认证周期内的审核方案策划

5.4.1.1 总则

运营部按照《审核方案策划管理规定》的要求，对整个认证周期制定审核方案，以识别初次认证审核、认证决定之后的第一年与第二年的监督审核和第三年在认证到期前进行的再认证审核等整个认证周期内各阶段所需的审核活动以及时间间隔要求，确定信息安全管理体系的审核时间、多场所抽样、多管理体系标准审核等活动要求，以证实客户的管理体系符合ISO/27001标准及客户所确定的信息安全控制要求。认证周期的审核方案须覆盖全部的管理体系要求及客户所确定的信息安全控制要求。

注：客户所有确定的信息安全控制来自于 ISO/IEC 27001 附录 A，和/或其他适用的标准，和/或由组织自行设计，具体根据客户组织提交的《信息安全适用性声明》确定。中标通可以采用 ISO/IEC 27007 给出的有关审核的进一步指南对客户的 ISMS 实施审核。

5.4.1.2 初次认证审核方案须包括两阶段初次审核、认证决定之后的第一年与第二年的监督审核和第三年在认证到期前进行的再认证审核，各阶段审核时间间隔及审核活动要求具体详见《审核方案策划管理规定》的相关要求。

5.4.1.3 特殊情况或虚拟场所需要远程审核时，运营部须按照《基于信息和通信息技术（ICT）

的远程审核管理规定》的要求，先进行远程审核风险分析，再策划实施远程审核。

5.4.1.4 审核方案的策划需考虑客户为初次审核做的总体准备情况。运营部先确认客户提交的所必须的资料情况，尤其内部审核报告及信息安全独立评审报告（管理评审报告）的提交情况，若客户没有提交或提交不全，应通过电话、微信或其他适宜的方式要求客户提交相应的准备资料，至少要提交内部审核报告、信息安全独立评审报告（管理评审报告），以便为审核做好充分的准备。

5.4.1.5 信息安全管理体系审核方案策划须策划审查期间。运营部通过对客户提供的 ISMS 内部审核、管理评审资料确认，有充分的证据证实客户覆盖认证范围的内审和管理评审已实施，并且 ISMS 体系充分、适宜、有效，并能持续运行，才能在此期间对客户的 ISMS 认证。

5.4.1.6 信息安全管理体系审核方案策划须确定认证范围。运营部通过对客户的业务证据、管理手册、信息安全适用性声明、信息安全策略、信息安全风险评估等与认证范围相关的文件的评审来确定客户的 ISMS 认证范围，认证范围的确定须满足如下条件：

a）确保客户的 ISMS 满足了 ISO/IEC 27001 中 4.3 的要求；

b)确保审核组须根据所有适用的认证要求对在确定范围内的客户 ISMS 进行审核；

c)客户的信息安全风险评估和风险处置准确地体现了认证范围所界定的活动并延伸到活动的边界，并在客户的 ISMS 范围和适用性声明中得到了体现（须验证每个认证范围至少有一个适用性声明）；

d）确保与不完全包含在 ISMS 范围内的服务或活动的接口（例如：与其他机构共享 IT 系统、数据库、通讯系统或外包业务职能）已在寻求认证的 ISMS 中得到说明，并已包括在客户的信息安全风险评估中。

5.4.2 确定审核时间

审核方案策划人员须以 CNAS-CC170（ISO/IEC 27006，IDT）之 9.1.4.2、附录 C 等部分的审核时间确定准则来确定审核时间，以确保审核的充分性和有效性。确定审核时间时须考虑认证覆盖的有效人数，客户管理体系复杂程度，与组织的产品、过程或活动相关联的风险，场所的数量和分布，是否结合审核或一体化审核，技术和法规环境，以前审核的结果，管理体系范围内活动的分包情况等因素。审核时间确定的具体要求详见《管理体系审核时间管理规定》。

5.4.3 多场所的抽样

当客户的信息安全管理体系包含在多个地点（固定或临时地点）进行的相同活动时，可以按照抽样规则对多场所实施抽样审核，以确保对该管理体系的正确审核。抽样审核的策划与实施要求具体详见《多现场审核管理规定》。抽样审核策划的合理性须记录到《审核方案策划及管控表》。

5.4.4 多管理体系审核标准

5.4.4.1 依据多个管理体系标准进行认证时，须根据拟结合认证的其他管理体系类型及客户提交结合管理体系文件，先识别是否有清楚的接口，只要能够清楚地识别 ISMS 以及 ISMS 与其他管理体系的适当接口，中标通可以接受多个管理体系（例如，信息安全、质量、健康与安全、环境）文件组合在一起的文件，若没有清晰的接口文件则按不能接受。

5.4.4.2 有清晰的接口的文件，如果能证实审核满足了 ISMS 认证的所有要求，ISMS 可以则按照《结合审核管理规定》的要求策划结合审核，ISMS 的所有重要要素须清晰地在审核报告中体现并易于识别，确保审核的质量不应因结合审核而受到负面影响。

5.5 策划审核

5.5.1 确定审核目的、范围和准则

审核方案策划人员按照《审核方案策划管理规定》中确定审核目的、范围和准则的相关规定要求，确定不同审核阶段的审核目的、范围和准则。

5.5.2 选择和指派审核组

审核方案策划人员要求根据《审核方案策划管理规定》的审核组选择与指派规定，确定审核组的专业能力要求、特定能力要求及公正性要求，相应要求记入《审核方案策划及管控表》中。计划调度人员根据审核方案策划确定的能力和公正性要求，结合法规要求、客户需求、任务均衡、成本控制等因素，指派合适的审核组成员，并以《审核任务书及派出令》的方式通知到对应的审核人员。选派任用的审核员和审核组长须具备通用的审核知识与技能以及特定中类的技术领域审核所需的知识与技能，以实现和证实有效审核。选派任用的审核员和审核组长不得违反《认证公正性及认证风险管理程序》中确定的公正性管理原则及其相关的措施要求。

至少 1 名实施第一阶段审核的审核员须参加第二阶段审核，每个审核组须包括：

（1）审核组长：中标通须建立并实施审核组长的选择、培训以及任用的管理制度；审核组长应当具有管理和领导审核组达成审核目标的知识和技能，其能力应至少满足 GB/T 19011《管理体系审核指南》中对审核组长的通用要求；

（2 ）至少 1 名与申请所属认证业务范围相匹配的 ISMS 专业人员（专业领域审核员或技术专家）。ISMS 和其他管理体系实施结合审核的，审核组还须包括其他管理体系的专业人员，确保专业人员的能力覆盖实施结合审核的全部管理体系；

（3）至少 1 名专职审核员，并确保专职审核员全程参与 ISMS 审核过程。

5.5.3 审核计划

5.5.3.1 总则

5.5.3.1.1 审核组长接到《审核任务书及派出令》后，至少在每次审核的正式审核前编制《审核计划》，并传送给拟审核的客户组织（受审核方）、审核组内其他成员、审核方案策划人员确认，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。有关方对审核计划有异议时，审核组长须负责协商解决分歧，必要时可反馈给计划调度、业务跟单或部门负责人协调解决。审核计划必须考虑客户所确定的信息安全控制措施。为确保能最佳地证明受审核方全部范围的审核时间，可采用与受审核方商定的方式确定审核时间，商定审核时间时可考虑季度、月份、日期和班次。

5.5.3.1.2 远程审核技术的目标是提高审核的有效性和效率，并支持审核过程的完整性。涉及远程审核，审核计划中须识别审核中所使用的网络支持的审核技术，以便分析确定能否达到审核目标。

5.5.3.1.3 第一阶段不要求正式的审核计划，但必须让有关各方明确当次审核的审核目的、审核准则、审核范围、拟实施现场审核活动的日期和场所、预计的现场审核活动持续时间、审核组成员及审核组同行的人员的角色或职责。

5.5.3.2 编制审核计划

5.5.3.2.1 审核组长基于客户组织提交的申请资料、申请评审及审核方案策划信息、审核任务指令信息、以及与拟受审核方沟通结果等方面的信息，分析确定审核计划编制相关的组织结构及职能分配、场所分布、生产/服务活动过程、信息资产及控制措施、ICT 设施（拟 ICT 审核适用）、保密要求、交通路线等情况，在充分考虑审核有效性、可行性的基础上制定编制审核计

划，将具体的过程、职能、场所、区域或活动的审核职责分配给审核组每位成员（包括技术专家），确保审核计划与审核目的和范围相适应。审核计划包括或引用如下内容：

a）受审核方基本情况，包括受审核方名称、地址、联系方式等；

b）审核类型/目的，审核目的须与审核方案确定的各阶段的审核目的相一致；

c）审核依据（准则），包括：ISO/IEC 27001 标准，客户的 ISMS 体系文件（如信息安全方针、程序文件、作业指导书等）；与 ISMS 相关的法律法规（如《网络安全法》《数据安全法》）和合同要求等；

d）审核范围，包括识别拟审核的体系覆盖的活动范围；

e）审核日期，当次审核开始的日期到审核结束的日期；

f）审核组成员信息，包括姓名、性别、组内编号、审核职务、审核员注册证书号或技术专家编号、专业代码、联系电话等信息；

g）审核日程具体安排，包括拟审核的职能单元、重点审核活动及其对应的管理体系要求条款编号或信息安全控制标准对应的条款编号、审核日期、审核持续时间（开始到结束时间）、审核组成员任务分配等内容；

i）特别注意事项：包括审核组声明、会议要求、审核支持、 更改联络、必审内容、条款调整、不适用条款确认、意见反馈、审核使用语言等内容。

5.5.3.2.2 审核计划编制后，审核组长至少在正式审核前发给客户组织、同组成员确认，并要求客户按照《信息安全与保密管理程序》报告因保密或敏感而不能提供审核组审查的信息。客户组织须确认审核计划并提前做好应对审核的准备，客户若提出异议或不同意见，审核组长须确认异议或不同意见，并采取措施解决分歧。同组成员须确认与自己的相关审核任务，并提前做好审核准备工作，必要时与审核组长沟通。客户报告有因保密或敏感而不能提供审核组审查的信息时，审核组长负责组织讨论因此审核的充分性，如果讨论的结论是若不审查已识别的保密信息或敏感信息就不能对 ISMS 进行充分地审核，审核组长负责告知客户只有在适当的访问安排获得许可后才能进行认证审核，并及时反馈计划调度人员，以便调整审核日程安排。有客户报审核过程中如需调整计划须与客户商定后再调整。

5.5.3.2.3 审核方案策划在认证周期内需要对轮班作业抽样审核的，须计划对轮班作业审核。

5.5.3.3 审核组任务的沟通

计划调度人员结合能力和公正性要求、法规要求、客户需求、任务均衡、成本控制等因素考量，正式任命审核组并为其提供与 ISMS 审核相关的资料，包括企业的 ISMS 资料、企业的资质文件（营业执照及必要的许可文件）、经营地址证明文件（产权证明或租赁合同）、有效人数清单、多场所信息（如有）、申请评审文件、审核方案策划资料等审核所需的工作资料，并以《审核任务书及派出令》的方式规定审核组的任务，要求审核组实施：

a）检查和验证客户组织与管理体系相关的结构、方针、过程、程序、记录及相关文件；

b）确定上述方面满足与拟认证范围相关的所有要求；

c）确定客户组织有效地建立、实施并保持了管理体系过程和程序，以便为建立对客户管理体系的信任提供基础；

d）告知客户其方针、目标及指标(与相关管理体系标准或其它规范性文件的期望一致）与结果之间的任何不一致，以使其采取措施。

5.5.3.4 审核计划的沟通

计划调度人员先基于法律法规要求、客户需求、合理化等因素考量，预排审核日期，然后由业务跟单人员与客户沟通预排结果，同时告知客户在审核日期内须做好包括但不限于：ISMS 体系资料完整、有认证覆盖范围内的生产/经营活动、有信息安全管理活动及控制措施、管理层及关键部门负责人应受审核现场、有专门的审核应对人员等方面的准备。客户分析判定后同意预排结果，则可将预排的审核日期做为商定的审核日期，若客户不同意预排审核日期，业务跟单应及时向计划调度人员反馈，计划调度人员须重新预排审核日期，再次给客户确认，直至客户同意，形成最佳的审核时间。商定审核时间时可考虑季度、月份、日期和班次。

5.5.3.5 审核组成员信息的通报

业务跟单人员向客户提供预排的审核组每位成员的姓名，客户若请求了解每位成员的背景情况时，还须向其提供每位成员的背景情况，并留出足够的时间，让客户组织对每位成员的背景进行充分的了解，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。若客户组织对任命提出反对，业务跟单人员须先确认反对是否合理有效，若反对合理有效，必须反馈给计度调度人员以重组审核组；若反对无效，须给客户合理的解释，以消除分岐或争议。一旦与客户确定了审核组，运营部要正式发出《审核任务书及派出令》，以及适当的工作文件，并在认

证认可业务信息统一上报平台上报审核计划。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。

5.6 初次认证

5.6.1 初次认证审核

5.6.1.1 总则

信息安全管理体系的初次认证审核要实行两个阶段审核，第一阶段审核、第二阶段审核。

5.6.1.2 第一阶段

5.6.1.2.1 第一阶段审核的策划须确保第一阶段的目的能够实现，须告知客户组织第一阶段需实施的任何现场活动。第一阶段审核不要求正式的审核计划。

5.6.1.2.2 第一阶段审核的目的须与 CNAS-CC01《管理体系认证机构要求》第 9.3.1.2.2 条中规定的目的一致，具体见《审核方案策划管理规定》中“第一阶段的审核目的及覆盖内容”部分。

5.6.1.2.3 第一阶段审核方式和要求

5.6.1.2.3.1 初次认证审核的第一阶段审核须在客户现场实施审核。在现场审核前，须先对客户组的管理体系进行系统化的文审，并形成《文审报告》。当第一阶段满足如下条件时，可以不在客户现场实施审核：

a)客户已获中标通颁发的其他管理体系认证领域的有效认证证书，中标通已对客户 ISMS 有充分了解；

b)客户获得了经认可机构认可的其他认证机构颁发的有效的 ISMS 认证证书,通过对其文件和资料的审核可以达到第一阶段审核的目的和要求。

中标通应记录未在现场进行第一阶段审核的理由。

5.6.1.2.3.2 第一阶段审核须获取有关 ISMS 设计的文件，包括 ISO/IEC 27001 所要求的文件，客户须至少提供 ISMS 和其所覆盖活动的一般信息，以及 ISO/IEC 27001 要求的 ISMS 文件的副本，以及需要时，其他相关文件。第一阶段审核须在客户的组织设置、风险评估与风险处置（包括所确定的控制）、信息安全方针和信息安全目标的背景下充分了解 ISMS 设计，特别是须充分了解客户的审核准备情况。所了解的信息须用于策划第二阶段。

5.6.1.2.3.3 第一阶段对于多场所的审核重点须放在总部，以全面了解情况，并为第二阶段审核确定抽样方案，总部时间须充分；第一阶段对于分场所审核的样本数不做统一的规定，可根据审核组长文审以及对受审核方活动、产品、生产工艺的熟悉程度、信息资产、信息管理流程、信息安全风险等方面确定分场所审核的样本数确定；分场所的选择须首先选择风险较大的分场所；一般风险的客户，可只考虑总部所在地的分场所。

5.6.1.2.3.4 第一阶段审核须形成书面的《管理体系认证一阶段审核报告》，为第二阶段审核提供关注点，包括识别任何引起关注的、提出第二阶段审核所需资源（人日数、专业能力要求、审核路线）的必要建议，在第二阶段可能被判定不符合的问题，做出是否达到第一阶段的审核目的，是否具备/不具备实施第二阶段审核条件，可否实施第二阶段审核的结论，并书面告知客户。第一阶段须让客户知晓第二阶段可能需要详细检查的、更多类型的信息和记录。

5.6.1.2.3.5 审核组长须在审核结束后，将第一阶段的审核报告以及能否进行第二阶段审核的结论通过邮件或其他适宜的方式反馈到计划调度人员及审核方案策划人员。审核方案策划人员须在进行第二阶段审核之前审查第一阶段的审核报告，并确定是否可以进行第二阶段审核，以及第二阶具备审核组成员所具备的能力。如果第一阶段的审核组长具备能力且适宜时，可由其来实施该审查。

5.6.1.2.3.6 计划调度人员基于审核方案策划人员是否进行第二阶段审核以及第二阶段审组的能力需求，确定是否调整计划、重派审核组。若审核方案策划人员的结论是不能继续进行第二阶段审核或第二阶段审核组能力需要调整，则须调整审核计划、重编审核组，重做审核任务安排；若审核方案策划人员的结论是可以继续进行第二阶段审核、第二阶段审核组能力无须调整时，则无须修订原审核计划，也无须重新安排审核任务。

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

5.6.1.2.3.8 第一阶段有采取远程审核方式的，须在审核报告中加以说明。

5.6.1.2.3.9 初次认证审核的第一阶段审核须合理分配审核时间,并在审核计划中加以明确的区分记录，且必须对客户的管理手册、程序文件、工作文件等文件化管理体系信息进行充分审核，形成专门的文件审核记录。

5.6.1.3 第二阶段审核

5.6.1.3.1 第二阶段的目的是评价客户信息安全管理体系的实施情况，包括有效性，须在受审核方的现场进行，审核组须现场审核除了访问物理场所(如工厂)外，“现场”还可以包括远程访问，包含管理体系审核相关信息的电子站点，现场审核须按审核计划实施，并至少覆盖以下内容：

a)与适用的管理体系标准或其他规范性文件的所有要求的符合情况及证据；

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

c)客户管理体系的能力以及在符合适用法律法规要求和合同要求方面的绩效；

d)客户过程的运作控制；

e)内部审核和管理评审；

f)针对客户方针的管理职责。

5.6.1.3.2 信息安全管理体系审核第二阶段的目的除了评价 ISMS 的其有效实施外，还包括确认客户是否有效遵守自身的方针、策略和规程，是否有违反方针、策略和规程的情况，第二阶段的审核计划须根据第一阶段的审核报告中的审核发现制定，审核须重点关注以下内容：

a）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；

b）ISO/IEC 27001 中所列的文件要求；

c）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；

d）基于风险评估和风险处置过程，确定控制；

e）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；

f）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；

g）控制的实现（见 ISO/IEC 27006 附录 D），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；

h）针对客户方针的管理职责；

i）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。

5.6.1.3.3 初次认证的审核结论

审核组长在末次会议前，组织审核组成员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分析，以评审审核发现并就审核结论达成一致。为使技术部有效的做出认证决定，审核组至少须向技术部提供以下信息：

a)第一、第二阶段审核报告，以及文审报告；

b)对不符合的处理意见，适用时，还包括对受审核方采取的纠正和纠正措施的意见；

c)对提供给中标通用于申请评审的信息的确认；

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。

5.7　实施审核

5.7.1 总则

5.7.1.1 审核组须按照本程序的要求实施现场审核，实施审核的过程包括审核开始时的首次会议和审核结束时的末次会议。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管理体系审核相关信息的电子化场所。当审核的任何部分以电子手段实施时，或拟审核的场所为虚拟场所时，须确保实施电子化审核的人员具有信息技术应用及在线沟通能力。电子化审核活动中获取的证据须包括文件、视频、图片、在线沟通记录等充分有效的证据，足以让审核员对相关要求的符合性做出有根据的决定。

5.7.1.2 审核组须要求客户提供信息资产、信息资产风险评估及控制措施、残余风险评估等相关的证据，用以证实对信息安全相关风险的评估与 ISMS 范围内的 ISMS 运行是相关的和充分的。审核组须确定客户识别、检查和评价信息安全相关风险的管理程序、以及控制程序要求实施的结果是否与客户的方针、目标和指标一致，要确定用于风险评估的规程是否健全并得到正确实施，是否有明显的漏项、缺项或明显不合理的地方。

5.7.2 召开首次会议

在召开首次会议时，中标通要求审核组需要按以下要求执行：

a）会议组织与主持：每次审核都要与客户的管理层（若适用，还需包括拟审核职能或过程的负责人员）召开正式的首次会议， 通常由审核组长主持会议。会议目的是简要解释将如何进行审核活动。详略程度可与客户对审核过程的熟悉程度相一致。

b）介绍参会人员：介绍包括审核组成员、客户方人员等，并简要说明每个人在审核中的角色，比如审核组长负责整体审核把控、审核组员负责具体领域审核等。

c）确认认证范围：与客户再次明确本次审核所涉及的认证范围，如具体是哪些业务部门、业务流程等在认证范围内，避免出现理解偏差。

d）确认审核计划：向客户确认审核计划，包括审核的类型（初次审核、监督审核等）、范围、目的和准则 ，以及审核计划是否有任何变化。同时，与客户确认末次会议的日期和时间，以及审核期间审核组与客户管理层会议的日期和时间等相关安排。

e)确认审核组与客户之间的正式沟通渠道:与客户确认审核组和客户之间正式的沟通渠道，如指定的联络人、沟通方式（电话、邮件等）， 确保审核期间信息能够及时、准确传达。

f）确认审核组可获得所需的资源和设施：和客户确认审核组在审核过程中可获得所需的资源和设施，例如办公场地、文件查阅权限、必要的办公设备等。

g）确认与保密有关的事宜：与客户明确保密相关的事宜，如审核组会对客户提供的信息严格保密，同时也要求客户对审核过程中涉及的中标通相关信息进行保密。

h）确认适用于审核组的相关的工作安全、应急和安保程序：向客户了解并确认适用于审核组的工作安全、应急和安保程序，如办公场所的安全规定、紧急疏散流程等，确保审核人员的人身安全和审核工作顺利进行。

i）确认可得到向导和观察员及其角色和身份：确认是否有向导和观察员参与审核，以及他们的角色和身份，明确他们在审核过程中的职责和权限。

j）说明报告方法,包括审核发现的任何分级：向客户说明审核报告的方法，包括审核发现如何分级（如严重不符合、一般不符合等），以及报告的提交时间和方式等。

k）说明可能提前终止审核的条件：告知客户可能提前终止审核的条件，如客户故意隐瞒关键信息、不配合审核工作等情况，让客户清楚审核的严肃性和规则。

l）确认审核责任及控制审核计划的执行：确认审核组长和审核组代表认证机构（中标通）对审核负责，并且会严格控制审核计划的执行，包括审核活动的开展和审核路径的安排。

m）确认以往评审情况（若适用）：如果客户以往有相关评审或审核，需要与客户确认以往评审或审核发现的状态，比如是否已经完成整改等。

n）说明抽样审核方法和程序：向客户说明基于抽样实施审核的方法和程序，让客户了解审核并非全面检查，而是通过抽样来评估整体的符合性。

o）确认审核中使用的语言：与客户确认审核过程中使用的语言，若存在语言沟通障碍，提前安排好翻译等相关事宜。

p）确认审核进程及任何关注点：告知客户在审核中将及时告知其审核进程以及发现的任何关注点，让客户能够及时了解审核动态。

q）提供提问机会：给客户提供提问的机会，让客户对审核相关的内容提出疑问，审核组及时进行解答，确保双方对审核工作达成共识。

5.7.3　审核中的沟通

5.7.3.1 审核组负责通过双向交流、内部会议等方式定期评估审核的进程，并沟通审核进程信息，以便按计划有效实施审核。审核组长负责审核进程和进度进行分析预估，必要时审核组成员之间重新进行工作分配。审核组负责定期将审核进程及任何关注告知客户。

5.7.3.2 可获得的受审核方资料信息、经营场所范围、认证覆盖的活动类型、有效人数、ISMS管理活动、信息安全控制措施、受审核方环境、审核过程进度等方面的证据显示无法实现审核目的，或显示存在紧急和重大的风险（例如安全风险）时，审核组长向客户（如果可能还向中标通）报告这一情况，审核组长（必要时与运营部负责人一起）根据影响审核目的实现或风险类型性质确定采取行动，包括重新确认或修改审核计划，改变审核目的或审核范围，或者终止审核。重新确认或修改审核计划，改变审核目的时，审核组长以《审核现场技术问题申报处理单》的方式向运营部报告所采取行动的结果。发生以下情况时，审核组长负责向中标通报告，经中标通同意后终止审核，向客户发出《终止审核现场审核决定书》。

a）受审核方对审核活动不予配合，审核活动无法进行。

b）受审核方实际情况与申请材料有重大不一致。

c）其他导致审核程序无法完成的情况。

5.7.3.3 如果在现场审核活动的进行中发现需要改变审核范围，审核组长须与客户审查该需要，并以《审核现场技术问题申报处理单》的方式报告中标通审核方案管理人等。

5.7.3.4 观察员和向导

5.7.3.4.1 观察员

观察员可以是客户组织的成员、咨询人员、实施见证的认可机构人员、监管人员或其他有合理理由的人员。非客户组织的成员做为观察员，运营部与客户须在实施审核前就审核活动中观察员的到场及理由达成一致。审核组须确保观察员不影响或不干预审核过程或审核结果。

5.7.3.4.2 向导

每个审核员须由一名向导陪同，除非审核组长与客户另行达成一致。为审核组配备向导是为了方便审核。审核组须确保向导不影响或不干预审核过程或审核结果。向导的职责可以包括：

a）为面谈建立联系或安排时间；

b）安排对现场或组织的特定部分的访问；

c）确保审核组成员知道并遵守关于现场安全和安保程序的规则；

d）代表客户观察审核；

e）应审核员请求提供澄清或信息。

5.7.4　收集和验证信息

5.7.4.1 对于初次审核的组织，审核组尽量安排简短的现场巡视或 ICT 巡视，再依据审核计划，分组按规定的审核路线、审核方法到各部门及生产/服务场所进行现场审核。现场审核要覆盖管理体系覆盖的产品范围和主要的活动和场所。在审核过程中，审核组须通过适当的抽样方式来收集与审核目的、范围和准则相关的信息，这些信息包括与职能、活动和过程之间的接口有关的内容，并对收集到的信息进行验证，确保其能成为有效的审核证据，以便形成审核发现和审核结论。

注：适当的抽样方式见附录 C：《现场审核取证抽样方法》。

5.7.4.2 信息获取方法须包括（但不限于）：

a)面谈。与被审核方的相关人员（如管理人员、工作人员等）进行交流，了解相关情况，获取信息，例如，与信息安全管理负责人面谈，了解企业信息安全方针的制定与传达情况。

b)对过程和活动进行观察。到现场观察被审核方的实际过程和活动开展情况，比如，观察企业数据中心的运维操作过程，查看是否符合信息安全管理体系中关于机房管理的要求。

c)审查文件和记录。查阅被审核方的各类文件（如信息安全管理手册、程序文件、作业指导书等）和记录（如风险评估记录、内部审核记录、事件处理记录等），验证文件的符合性和记录的真实性、完整性。

5.7.5 确定和记录审核发现

5.7.5.1 审核组确定审核发现。审核发现要简述符合性，详细描述不符合以及为其提供支持的审核证据，审核发现要进行分级（符合、不符合、观察），并予以记录和报告，以便为认证决定或保持认证提供充分的信息。

5.7.5.2 审核组可以识别和记录信息安全管理相关的改进机会，但认证方案要求禁止或出于信息安全保密的需要禁止的不得识别和记录。属于不符合的审核发现不得作为改进机会予以记录。

5.7.5.3 关于不符合的审核发现要对照审核准则的具体要求予以记录，包含对不符合的清晰陈述，并详细标识不符合所基于的客观证据。要与客户讨论不符合，以确保证据准确且不符合得到理解。但是，审核员要避免提示不符合的原因或解决方法。

a)下列情况之一者判为严重不符合项：

✧ 受审核方 ISMS 的某一个要素/要求缺少或出现严重问题，导致不能满足法律法规要求；

✧ 受审核方 ISMS 的某一活动/过程要求出现多项(根据规模大小、复杂程度掌握 3—5 项)轻微不符合项，导致出现系统性和/或区域性的不符合；

✧ 严重的相关方投诉，无法及时采取适宜措施进行整改，从而影响其 ISMS 满足要求的信心；

✧ 严重违反相关法律法规或其他要求；

✧ 严重的欺骗行为。

b)下列情况之一者判为轻微不符合项：

✧ 对照审核准则，出现的不符合对 ISMS 没有产生严重的影响；

✧ 对于受审核区域、过程的管理现状而言，是偶尔发生的、个别的问题。

c) 改进机会

✧ 对于不能界定为不符合，但是可能对受审核方的 ISMS 有帮助之处，由审核组以改进机会的形式向受审核方提出。

d)在证后监督、再认证时不符合项还包括：

✧ 错误使用认证标识和证书，若属明知故犯恶意违规、造成严重后果的，要判定为严重不符合项；其情节及后果并不严重的，要被判定为轻微不符合项。要该注意的是，凡属此类不符合项要当即要求受审核方进行整改。

✧ 前次审核发现的不符合项的现场整改情况不佳的,将视其情节及后果的严重程度形成轻微/严重不符合项。

✧ 没有足够的措施、证据证明其 ISMS 具备持续改进能力、取得持续改进绩效的，也将判定为不符合项。

5.7.5.4 审核组长负责尝试解决审核组与客户之间关于审核证据或审核发现的任何分歧意见，未解决的分歧点要予以记录。

5.7.5.5 审核组须：

a）要求客户提供在 ISMS 范围内，信息安全风险评估与 ISMS 运行是相关的和充分的证据，包括但不限于信息资产识别，信息安全风险识别、分析、评价、风险控制措施、残余风险分析，风险评估报告等相关的证据，以便验证其信息安全风险管理充分性、有效性；

b）确定客户识别、检查和评价信息安全风险的程序及其按程序实施的结果是否与客户的信息安全方针、目标和指标相一致。

5.7.5.6 中标通还须确定客户风险评估的规程（方法）是否符合行业标准或最佳实践（如 ISO 27005、NIST SP 800-30），是否覆盖了组织的业务环境和风险场景，组织是否实际按照规程执行了风险评估（而非仅停留在纸面），结果是否可信且用于指导 ISMS 控制措施的选择。

5.7.6 准备审核结论

在末次会议前，由审核组长负责做审核结论的准备工作，包括：

a) 审查审核发现与信息并分级不符合项:

审核组长对照审核目的(如判定客户 ISMS 是否符合 ISO/IEC 27001 标准)和审核准则(如 ISO/IEC 27001 标准、客户体系文件等），对审核过程中发现的问题以及获取的其他适用信息进行全面审查。按照 5.7.5.3 条的不符合等级区分标准对不符合项进行分级。

b）考虑不确定性并达成审核结论：

充分考虑审核过程中存在的内在不确定性（如抽样审核可能存在的偏差等），审核组内部就审核结论进行讨论并达成一致，确定客户的管理体系是否符合审核准则等结论。

c）确定必要的跟踪活动：

审核组就任何必要的跟踪活动（如对不符合项整改情况的验证活动）进行讨论并达成一致，明确跟踪的方式、时间等要求。

d）确认审核方案的适宜性并识别改进点：

确认当前审核方案（包括认证范围、审核时间、监督频次、审核组能力等方面）的适宜性。若发现存在不适宜之处，识别出为未来审核所需进行的修改内容，以优化后续审核工作。

5.7.7　召开末次会议

5.7.7.1 审核组要与客户的管理层（适用时，还包括所审核的职能或过程的负责人员）召开正式的末次会议，并记录参加人员。末次会议通常要由审核组长主持，会议目的是提出审核结论，包括关于认证的推荐性意见。

5.7.7.2 末次会议还要包括下列要素。详略程度要与客户对审核过程的熟悉程度一致，会议内容包括但不限如下方面：

a）感谢致辞/签到；

b）重申审核目的、范围、依据及审核原则、方法，审核发现的分类及对审核结论的影响；

c）重申“公正性声明及保密声明”及审核的局限性（如抽样，但要强调审核组通过控制抽样的典型性和代表性已使此种风险降至最低限度，从而确保审核结论能尽可能反映受审核方 ISMS 的客观情况）；

d）向客户说明所收集的审核证据基于对信息的抽样，因而会有一定的不确定性；

e）审核员宣读“不符合报告”，必要时宣读观察项；不符合项要取得企业管理者代表或其它负责人的确认。不符合要以使其被理解的方式提出，并要就回应的时间表达成一致。“被理解”不一定意味着客户已经接受了不符合。

f）征询受审核方对不符合事实是否仍存在异议；

g）中标通处理不符合（包括与组织认证状态有关的任何结果）的过程说明，包括：

✧ 强调不能仅采取就事论事的“补救”措施，须按如下步骤制定并实施纠正/纠正措施：

✧ 纠正（如不符合项为孤立事件，则无需下述措施）；

✧ 检查类似的问题是否存在；

✧ 分析产生原因，制订并实施纠正措施。

✧ 纠正/纠正措施方案经受审核方管理者代表审批后实施，验证合格后，交审核组长确认；

✧ 纠正/纠正措施期限根据不符合项性质及严重程度决定，一般为 30 个工作日至 3 个月内。

h）客户为审核中发现的任何不符合的纠正和纠正措施提出计划的时间表（纠正/纠正措施要求）；

i）中标通在审核后的活动（包括证后要求，认证证书和标志的使用）；

j）审核综述（从以下方面总结受审核方 ISMS 的符合性及有效性）：

✧ 文件评审结果；

✧ 现场审核观察综述；

✧ ISMS 运行过程的符合性、有效性；（ISMS 的活动、产品、服务过程中遵守有关法律、法规的情况；信息安全事故、相关方投诉；资源配置；职责权限；员工特别是管理者的信息安全意识；培训管理评审、内审、纠正、预防措施等要素的实施有效性；信息安全方针、目标、指标的实现及监测情况；信息资产、风险评估及控制措施；严重不符合项情况；不符合项的数量及分布……）

k）审核结论：

✧ 现场审核通过：审核小组建议中标通对客户的 ISMS 给予注册；

✧ 改善后通过：审核小组建议，申请单位要对审核小组提出的不符合项采取纠正措施并经审核小组成员评审或验证后，符合批准认证注册条件的，审核小组才推荐中标通对申请单位的 ISMS 给予注册；

✧ 现场审核不通过：审核小组建议中标通不对申请单位的 ISMS 给予注册，建议申请单位在条件成熟后重新申请认证；

l)说明投诉处理过程和申诉过程；

m)受审核方管理者简短讲话（受审核方意见，包括提出问题）；

n)以致谢结束会议。

5.7.7.3　审核组要给客户机会提出问题。审核组与客户之间关于审核发现或结论的任何分歧意见要得到讨论并尽可能获得解决。任何未解决的分歧意见要予以记录并提交中标通。

5.7.8 审核报告

5.7.8.1 审核组要为每次审核提供书面报告，这是审核工作的重要成果体现。审核组可以在报告中识别出客户的改进机会，为客户后续优化管理体系提供方向，但不能提出具体解决办法的建议，确保审核的核心是评估符合性，而非直接参与问题解决。中标通享有对审核报告的所有权，涉及到报告的管理、使用和分发等权限。

5.7.8.2 审核组长负责编制并向中标通提交审核报告，并对审核报告的内容负责。审核报告须提供对审核的准确、简明和清晰的记录，以便为认证决定提供充分的信息，并应包括或引用下列内容：

a) 认证机构（中标通）的名称；

b) 客户的名称和地址及其管理者代表；

c) 审核的类型（例如初次、监督或再认证审核）；

d) 结合、联合或一体化审核情况（适用时）；

e) 审核准则（如 ISO/IEC 27001 标准等）；

f) 审核目的及其是否达到的确认；

g) 审核范围，特别是标识出所审核的组织或职能单元或过程，以及审核时间；

h) 审核组长、审核组成员及任何与审核组同行的人员；

i) 审核活动（永久或临时场所）的实施日期和地点；

j) 与审核类型的要求一致的审核证据(或审核证据的引用）、审核发现和审核结论；

k) 已识别出的任何未解决的问题（如有）；

l) 审核的说明，其中包括了文件评审的摘要；

m) 与审核计划的偏离（例如：在某一预定的活动上花费更多或更少的时间）；

n) 任何影响审核方案的重要事项；

o）对客户信息安全风险分析进行认证审核的说明，说明对客户信息安全风险识别、评估、处置等方面的审核发现；

p）客户在实施 ISO/IEC 27001:2022　6.1.3 c)所要求的比较时，所使用的任何信息安全控制集；

q）所采用的主要审核路线和所使用的审核方法,阐述所采用的主要审核路线和使用的审核方法，让报告使用者了解审核的开展逻辑和方式；

r）所引用的适用性声明版本，以及适用时，与客户以往认证审核结果的任何有用的比较。

s)支持性文件纳入：完成的问卷、检查清单、评论意见、日志或审核员笔记等可作为审核报告的组成部分，若使用了这些方法，需将这些文件作为支持认证决定的证据提供。同时，有关审核中所评价样本的信息，要包含在审核报告或其他认证资料中。

t）关于 ISMS 要求和信息安全控制的实现与有效性的最重要评论意见，包括正面和负面的，为认证决定提供全面的参考。

u）客户的 ISMS 是否获得认证的建议，以及支持建议的信息。

v)如果使用了远程审核方法，审核报告须说明远程审核涉及的场所、管理要求条款或信息安全控制条款、使用的方法工具，是否达到有效审核的目的。当组织的活动不是在明确的物理位置实施的，而是其所有活动都是远程实施的时候，审核报告须说明组织所有活动都是远程实施的。

w)客户所采用的内部组织和规程的充分性，以便对其 ISMS 建立信心。

5.7.8.3 审核报告还须包含如下内容

a)ISMS 管理体系符合性与有效性声明以及对下列方面相关证据的总结：

1）管理体系符合相关标准、法规要求的证据总结，管理体系实现预期结果的能力的总结；

2）内部审核和管理评审实施过程的总结。

b)认证范围适宜性结论：对认证范围是否适宜做出明确结论，判断其是否与受审核方的实际业务、管理体系覆盖范围相匹配。

c)审核目的达成情况确认：确认审核是否达到了预先设定的目的，如是否达到评估管理体系的符合性、有效性等的目的。

d)与网络安全相关的行政处罚，及相关原因分析和整改措施的有效性（适用时）；

e)上次审核后发生的影响客户 ISMS 的重要变更（适用时）；

f)获证组织对认证证书和认证标志使用的控制情况（适用时）；

g)对以前不符合采取的纠正措施有效性的验证情况（适用时）。

5.7.9 不符合原因分析

当在审核过程中发现不符合项时，中标通要求审核组要在现场就向客户提出要求，让客户在规定的期限内对不符合的原因进行分析，并且详细说明为了消除该不符合，已经采取或者打算采取的具体纠正（用于消除已发现的不符合）和纠正措施（用于消除不符合的原因，防止不符合再次发生）。

5.7.10　纠正和纠正措施评审与验证

审核组按照以下要求评估验证纠正和纠正措施的有效性：

a)审查客户提交的材料：审核组要对客户提交的纠正措施、所确定的不符合原因以及纠正措施进行审查，判断这些内容是否可以被接受。

b)验证纠正和纠正措施的有效性：审核组对客户所采取的任何纠正（用于消除已发现的不符合）和纠正措施（用于消除不符合原因，防止再次发生）的有效性进行验证。可以通过审查客户提供的文件化信息（如整改报告、相关记录等），或者在必要时实施现场验证的方式来进行验证。

c)告知客户结果：审核组要将审查和验证的结果告知客户。

d)记录支持证据：为不符合的解决提供支持的证据必须加以记录，以便后续追溯和管理。

e)特殊情况告知：如果为了验证纠正和纠正措施的有效性，需要补充一次全面的或有限的审核，或者需要文件化的证据（需要在未来的审核中确认），中标通必须告知客户。

初次认证的严重不符合应在第二阶段严重审核结束后 6 个月内完成纠正和纠正措施并验证有效，否则则须重新进行一次第二阶段审核。

5.8　认证决定

5.8.1 技术部按照《认证决定管理程序》的要求确定认证决定及认证复核人员，确保做出授予或拒绝认证、扩大或缩小认证范围、暂停或恢复认证、撤销认证或更新认证的决定及认证复核的人员或委员会不是实施审核的人员，并经评价具有相应的能力，确保不违反公正性管理要求。

5.8.2 认证复核人员基于认证过程中收集到的证据信息及审核报告中审核组对客户 ISMS 是否通过认证的建议等方面的评审和确认，以及不符合纠正和纠正措施有效性验证结果，做出同意或不同意注册或保持注册的推荐性意见，认证决定人结合认证复核人的推荐性意见，根据《认证决定管理程序》做出认证决定,同意注册或保持注册后，技术部负责制定并向客户颁发证书,并在出的次月 10 前按照《信息通报与处理管理程序》要求上报认证证书信息。

5.8.3 只有符合《认证决定管理程序》中的授予初次证条件，且有充分的证据证实管理评审和 ISMS 内部审核的安排已实施、是有效的并将得到保持，才能向客户授予 ISMS 认证。

5.9 保持认证

5.9.1 总则

运营部按照审核方案策划的监督审核时间间隔及审核活动要求，在每年的监审到期前组织对获证客户实施监督审核、认证复核及认证决定，在证实获证客户持续满足管理体系标准要求后保持对客户的认证。当满足下列前提条件时，可以根据审核组长的肯定性结论保持对客户的认证，而无需再进行独立复核和决定：

a)对于任何严重不符合或其他可能导致暂停或撤销认证的情况，由审核组长向中标通报告，由具备认证决定或认证复核人员能力且未实施该审核的人员进行复核，以确定能否保持认证；

b)由具备认证决定或认证复核人员能力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，以确认认证活动在有效地运作。

5.9.2 监督活动

5.9.2.1 总则

5.9.2.1.1 监督审核程序作为客户 ISMS 认证审核程序的子集，目的是验证已被认证的 ISMS 得到持续实施、考虑客户变化所引起的管理体系的变化的影响并确认与认证要求的持续符合。运营部按照审核方案策划的监督审核时间间隔及审核活动要求，在每次监审到期前 3 个月组织对获证客户实施监督审核，对管理体系范围内有代表性的区域和职能进行监视，并考虑获证客户及其管理体系的变更情况。因季节性生产、客观环境、或其他特定情况需要延期监督审核时，客户需要提出延期申请，经运营部评审确认后才可延期监审，否则须按照《认证决定管理程序》及《认证证书及注册状态管理程序》的暂停、撤销管理要求做暂停、撤销处理。在制定监督审核方案时，考虑到内部审核方案及其可信度，至少包括：

a)ISMS 维护要素，如信息安全风险评估与控制的维护、ISMS 内部审核、管理评审和纠正措施；

b)根据 ISMS 标准 ISO/IEC 27001 的与来自外部各方沟通，以及认证所需的其他文件的要求；

5.9.2.1.2 监督活动包括对获证客户信息安全管理体系满足认证标准规定要求情况的现场审核。监督活动还可以包括：

a)中标通就认证的有关方面询问获证客户；

b)审查获证客户对其运作的说明（如宣传材料、网页）；

c)要求获证客户提供文件化信息（纸质或电子介质）；

d)其他监视获证客户绩效的方法。

5.9.2.1.3 监督审核时间间隔要至少在认证决定后的 12 个月内进行，两次监督审核间的时间间隔不超过 12 个月，一般第三次监督转为再认证。每次监督审核的内容只是 ISMS 的一部分。

5.9.2.1.4 如果有其它组织对持证者的 ISMS 有重大投诉时，中标通有权给持证企业通知后在短期内进行非例行监督。

5.9.2.2 监督审核

5.9.2.2.1 技术部通常在监审到期前 3 个月内（最早 6 个月内、最晚 1 个月内）将要监审的证书信息通知运营部，由业务人员将《 监督审核/变更审核(含转版)事项安排确认表》发给获证客户确认，并洽谈监督事项。若客户确认不愿意监督审核保持证书，则按照暂停、撤销管理要求到期做暂停、撤销处理（见 5.9.2.1.1），若客户确认愿意监督审核保持证书，业务人员跟踪办理监审手续，并收集获证客户自上次审核以来体系持续有效运行的情况、变更信息、转版需求信息，转交给审核方案策划人员。获证客户自上次审核以来若有体系覆盖范围、场所、组织结构等影响体系有效运行的重大变更，客户组织填写《认证信息变更申请表》。审核方案策划人员根据收集信息评审监督审核方案，必要时变更初审时监审核策划，以反映与风险相关的信息安全问题及其对客户的影响，并说明监督方案的合理性，并记录到《审核方案策划及管控表》。监督审核可以与其他管理体系审核相结合，但报告须清晰地指出与每个管理体系相关的方面。

5.9.2.2.2 计划调度人员根据客户提交的监审材料、最新的《审核方案策划及管控表》，拟定监督审核日程及审核组人员，然后由业务人员与客户沟通确定后，以《审核任务书及派出令》的方式通知相应的审核组，确保其知晓并接受审核安排。审核组的选派要求详见 5.5.2。

5.9.2.2.3 审核组长接到监督审核任务后，须做好监审前的准备，包括获取并确认初审记录、制定审核计划、与客户沟通、与其他相关人员沟通等事项。制定并沟通审核计划要求详见 5.5.3。

5.9.2.2.4 现场审核

5.9.2.2.4.1 监督审核是现场审核，按照初次认证第二阶段审核的流程步骤实施审核，但不一定是对整个体系的审核，但两次监督审核必须覆盖整个体系的管理要求，以使中标通能对获证客户管理体系在认证周期内持续满足要求保持信任。每次监督审核要包括对以下方面的审查：

a)内部审核和管理评审和纠正措施；

b)对上次审核中确定的不符合采取的措施；

c)申诉、投诉的处理查阅申诉、投诉与争议记录，并确认当出现有不符合或不能满足认证要求的情况时，还须检查客户是否对其自身的 ISMS 和规程进行了调查并采取了适当的纠正措施。

d)管理体系在实现获证客户目标和各管理体系的预期结果方面的有效性；

e)为持续改进而策划的活动的进展；

f)持续的运行控制；

g)任何变更；

h)认证证书、认证标志的使用和(或)任何其他对认证信息的使用。

i)ISMS 在实现客户信息安全方针的目标方面的有效性；

j)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；

k)所确定的控制变更，以及其引起的适用性声明的变更；

l)控制的实施和有效性。

5.9.2.2.4.2 监督报告须包括有关消除以往出现的不符合、适用性声明的版本和从上次审核之后发生的重大变更的信息。监督审核报告须至少完全覆盖本文件 5.7.8 的全部要求。监督审核可以与其它管理体系审核相结合，监督审核以结合审核的方式进行时，每个管理体系可形成单独的审核报告，也可形成结合审核报告，但报告要清晰地指出与每个管理体系相关的方面。

5.9.2.2.4.3 监督审核不符合原因分析及纠正和纠正措施评审与验证须符合本文件 5.7.9、5.7.10 的要求。

注：监督审核的严重不符合在 3 个月内未完成验证的，表明获证组织 ISMS 运行有效性存在问题，认证机构应暂停或撤销认证证书；

5.9.2.2.4.4 技术部根据本文第 5.8 条相关要求，结合监督审核结果做出同意或不同意保持注册的认证决定。

5.9.3 再认证

5.9.3.1 再认证审核的策划

5.9.3.1.1 再认证审核程序是客户 ISMS 认证审核程序的子集,目的是验证组织的信息安全管理体系作为一个整体的持续符合与有效性，以及与认证范围的持续相关性和适宜性。通常情况下，在证书有效期到期前 3 个月由技术部将需要再认证的证书信息传递给运营部，运营部策划并实施再认证审核,以评价获证客户是否持续满足相关管理体系标准或其他规范性文件的所有要求，技术部根据再认证审核结果做出认证复核及认证决定。再认证先由业务人员与获证客户洽谈再认证事宜，若客户不同意再认证保持证书的则按照到期失效处理，中标通做好到期前的维护，若客户同意再认证保持证书，业务人员跟踪办理再认证手续，督促企业提交认证申请资料、受理再认证申请。再认证申请及申请受理流程和要求同初次认证申请及申请受理。

5.9.3.1.2 再认证申请受理后，运营部先按照本文件第 5.2 条要求进行申请评审及第 5.3 条要求签署再认证合同，然后由审核方案策划人员对再认证审核方案进行策划并记录。再认证审核需要重点关注管理体系在最近一个认证周期（通常为 3 年）内的运行绩效，包括调阅以往的监督审核报告（即每年的例行审核记录），以综合评估体系的持续符合性和有效性。再认证审核可以与其他管理体系审核相结合，但报告须清晰地指出与每个管理体系相关的方面。

5.9.3.1.3 再认证审核通常不需要第一阶段审核，但当获证客户的 ISMS 管理体系、信息安全控制措施、组织或管理体系的运作环境（如法律的变更）有重大变更时，再认证审核活动可能需有第一阶段。

注：此类变更可能在认证周期中的任何时间发生，认证机构可能需要实施特殊审核（见 5.9.4），该特殊审核可能需要或不需要两阶段审核。

5.9.3.1.4 通常情况下，再认证审核时间不低于初审的 2/3 审核时间。

5.9.3.1.5 计划调度人员根据客户提交的再认证申请材料、最新的《审核方案策划及管控表》，拟定再认证审核日程及审核组人员，然后由业务人员与客户沟通确定后，以《审核任务书及派出令》的方式通知相应的审核组，确保其知晓并接受审核安排。审核组的选派要求详见 5.5.2。

5.9.3.1.6 审核组长接到再审核任务后，须做好再认证审核前的准备，包括获取并确认初审记录、制定审核计划、与客户沟通、与其他相关人员沟通等事项。制定并沟通审核计划要求详见 5.5.3.

5.9.3.2 再认证审核

5.9.3.2.1 再认证审核是现场审核，须覆盖 ISO/IEC 27001 管理要求的全部条款要求及信息安全控制措施的实施情况，包括针对下列方面的现场审核：

a）结合内部和外部变更来看的整个管理体系的有效性，以及认证范围的持续相关性和适宜性；

b）经证实的对保持管理体系有效性并改进管理体系，以提高整体绩效的承诺；

c）管理体系在实现获证客户目标和管理体系预期结果方面的有效性。再认证审核策划时应考虑获证组织最近一个认证周期内的 ISMS 绩效，包括调阅以往的监督审核报告。

5.9.3.2.2 再认证审核报告须包括有关消除以往出现的不符合、适用性声明的版本和从上次审核之后发生的重大变更的信息。再认证审核报告须至少完全覆盖本文件 5.7.8 的全部要求。再认证审核以结合审核的方式进行时，每个管理体系可形成单独的审核报告，也可形成结合审核报告。但报告要清晰地指出与每个管理体系相关的方面。

5.9.3.2.3 在再认证审核中发现不符合时，不符合原因分析及纠正和纠正措施评审与验证与初次认证要求相同，须根据不符合的严重程度和相关的信息安全风险相一致，规定实施纠正和纠正措施的期限，并且这些措施须在认证到期前得到实验和验证。

注：再认证审核的严重不符合未在认证证书到期前完成验证的，认证证书到期自动失效。获证组织再次申请认证的，中标通应按初次认证开展认证活动，满足 5.6.1.2.3.1 的情况下第一阶段审核可不在客户的现场实施。

5.9.3.2.4 技术部根据本文第 5.8 条相关要求，结合再认证审核结果做出同意或不同意再注册的认证决定。

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

5.9.3.2.6 如果在认证终止日期前，中标通未能完成再认证审核或不能验证对严重不符合实验的纠正和纠正措施，则不应推荐再认证，也不应延长认证的效力。中标通须告知客户并解释后果。

5.9.3.2.7 在认证到期后，如果中标通能够在 6 个月内完成未尽的再认证活动，则可以恢复认证，否则须至少进行一次第二阶段才能恢复认证。证书的生效日期应不早于再认证决定日期，终止日期须基于上一个认证周期。

5.9.4 特殊审核

5.9.4.1 扩大认证范围

获证组织生产/经营的产品/服务类别增加、经营场所增加时，须按照《认证合同书》的协议要求，向中标通业务人员通报变更情况，业务人员收到通报后与获证客户沟通，指导客户办理扩大认证业务范围申请，指导客户填写《认证认息变更申请表》，并提交扩大认证范围所需要的信息和资料：

—要求扩大认证范围的有关产品或服务的资料；

—修改管理手册、程序文件。

业务人员收到客户的扩大认证业务范围申请信息资料后，将信息录入 ERP 系统，然后由运营部组织相关认证职能人员实施申请评审、审核方案策划、现场审核(可结合监督审核同时进行)及审核档案提交，并经技术部做出认证决定，认证决定可以换发新认证证书时，证书制作人员负责制作新的证书。扩大认证范围审核时间可视扩大范围的复杂程度、即往审核的结果等因素确定审核时间。审核时间的确定通常按照每扩展 1～3 个产品、服务、或活动类型安排 0.5 人.天，每扩展 4～6 个产品、服务、或活动类型安排 1.0 人.天，依此类推；增加经营场所时审核时间按照每个临时服务现场加不少于 0.25 人.天，每个多场所加审核基础审核时间的 50%（基础审核时间为多场所认证覆盖人数对应的信息安全管理体系基础审核时间）。扩大认证范围可以和监督审核同时进行，单独进行扩大认证范围审核至少需要 1.0 人天。

5.9.4.2 提前较短时间通知的审核

为调查投诉、重大及以上级别的网络安全事件，对变更做出回应或对被暂停的客户进行追踪等，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。针对提前较短时间通知的审核，中标通须：

a）说明并使获证客户提前了解在如下条件将进行此种审核：

1）客户相关方有较多投诉，或反映其有隐瞒事实真相；

2）出现重大及以上级别的网络安全事件；

3）信息安全管理系统发生重大变化，影响到体系运行的有效性；

4）监督审核出现严重不符合或较多一般不符合项，审核组建议增加监督审核；

5）获证组织对认证证书、标志有较严重的不正确宣传或误导的。

b）由于客户缺乏对审核组成员的任命表示反对的机会，要在指派审核组时给予更多关注。如公正性、专业能力、审核员合规性与资质核验、审核组指派过程形成的记录及便于追溯性等方面的关注。

c)审核组可结合具体的审核任务，开展审核活动，形成审核报告，并提交中标通审查。

d)提前较短时间的审核要视审核的目的、审核涉及的范围等因素确定审核时间。

5.9.5 变更管理

5.9.5.1 认证范围的变更

5.9.5.1.1 认证范围的变更包括获证组织的名称变化，地址的增加、减少或变化，认证覆盖的产品、服务、活动类型的扩大、缩小、变化等方影响证书载明信息的变更。

5.9.5.1.2 获证组织生产/经营地址变更

a）增加或变更生产/经营地址的，按照本文“5.9.4.1 扩大认证范围”要求组织安排认证审核及其他相关的认证活动，直至并换发证书。

b）缩小生产/经营地址的，可依据其书面申请，由技术部评定直接办理换证。

5.9.5.1.3 获证组织注册地址变更

获证组织变更注册地址（注册地址为非生产/经营现场）的，在取得了地址变更后的营业执照或事业单位登记证明、相应资质证书（必要时）等文件后，向中标通提出注册地址变更申请，中标通在收到申请后经认证决定人员评审，评审通过后直接换发认证证书。

5.9.5.1.4 产品、服务 、活动类型变更

a）增加或变更产品、服务、活动类型的，按照本文“5.9.4.1 扩大认证范围”要求组织安排认证审核及其他相关的认证活动，直至并换发证书。

b）缩小产品、服务、活动类型的，可依据其书面申请，由技术部评定直接办理换证。

5.9.5.1.5 获证组织名称变化

获证组织变更名称的，在取得了名称变更后的营业执照或事业单位登记证明、相应资质证书（必要时）等文件后，向中标通提出名称变更申请，中标通在收到申请后经认证决定人员评审，评审通过后可直接换发认证证书。

5.9.5.2 认证要求的变更

5.9.5.2.1 认证要求的变更包括认证标准发生变更或重大修改。

5.9.5.2.2 在考虑各相关方的意见后，中标通确定一个过渡时期的转换要求。

5.9.5.2.3 中标通须预先通知获证组织，与其协商确定变更的方式和验证时机（在监督审核时变更、再认证审核时变更或独立审核变更）。

5.9.5.2.4 在规定的认证转换时期内，中标通按照新标准的要求组织进行审核，确保审核到所有与新范围有关的区域和活动。

5.9.6 暂停、撤销或缩小认证范围

当客户的获证 ISMS 出现暂停、恢复、撤销情况时，技术部按照《认证决定管理程序》要求做出暂停、恢复、撤销的决定，并按照《认证证书及注册状态管理程序》要求做好注册证书状态变更管理以及与之相关的信息报送与信息公开管理。当客户的获证 ISMS 出现缩小认证范围情况时，技术部按照《认证决定管理程序》要求做出缩小认证范围的决定，制定相应的通知书或证书给获证客户，并做好信息报送管理。

5.10 申诉/投诉与争议处理

当客户或其他相关方对中标通的认证活动有申诉、投诉或争议时，各部门收到申诉、投诉或争议后统一转交给技术部，由技术负部责按照《申诉/投诉和争议处理管理程序》实施处理，并记录处理结果。

ISMS 认证投诉意味着一个替在的事件，表明可能存在不符合。

5.11 客户的记录管理

5.11.1 中标通确保对所有客户（包括提交申请的组织、接受审核的组织和获得认证或被暂停或撤销认证的组织)保持从认证申请、申请受理、合同签署、审核方案策划、策划审核、实施审核、认证决定、申投诉或争议处理、暂停撤销处理、缩小认证范围处理、认证人员能力评价等活动过程和结果的相关记录。

5.11.2 获证客户记录包括但不限于以下内容：

a)申请资料及初次认证、监督和再认证的审核报告；

b)认证协议/合同；

c)适用时，多场所抽样方法的理由；

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

d) 确定审核时间的理由；

e) 纠正与纠正措施的验证；

f) 投诉和申诉及任何后续纠正或纠正措施的记录；

g) 适用时，委员会的审议和决定；

h) 认证决定的文件；

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

j) 建立认证的可信度所需的相关记录，如审核员和技术专家能力的证据；

k) 审核方案。

5.11.3 从认证申请到认证审核结束后案卷提交等过程的活动记录由运营部填写、标识、收集，然后整理纸质档案和电子档案传递给技术部使用及保管。认证决定，申投诉或争议处理，暂停、撤销或撤销认证范围等过程活动的记录由技术部填写、标识、收集，认证人员能力评价活动的记录由行政部填写、标识、收集。除认证人员能能力评价记录最终由行政部保存外，其他认证审核活动的记录由技术部负责保存。所有客户的记录须按照《记录控制程序》、《信息安全与保密管理程序》的要求填写、标识、收集、传输、编目、归档、存贮、保管及处理，确保记录的完整性和保密性。

5.11.4 记录保存期要为当前认证周期加上一个完整的认证周期。法规有要求时，记录需按法律规定保存更长的时间。

6、相关文件

6.1《信息通报与处理管理程序》

6.2《记录控制程序》

6.3《申诉/投诉和争议处理管理程序》

6.4《认证证书及注册状态管理程序》

6.5《认证决定管理程序》

6.6《审核方案策划管理规定》

6.7《审核组长指引》

6.8《基于信息和通信息技术（ICT）的远程审核管理规定》

7、相关记录

7.1《认证申请表》

7.2《认证合同书》

7.3《信息安全管理体系调查表》

7.4《拟认证组织声明承诺》

7.5《认证覆盖有效人数评估单》

7.6《固定/临时多场所/临时服务点清单》

7.7《信息安全适用性声明》

7.8《体系覆盖人员花名册》

7.9《认证申请受理通知书》

7.10《认证申请受理评审表》

7.11《合同评审表》

7.12《审核方案策划及管控表》

7.13《审核任务书及派出令》

7.11《 监督审核/变更审核(含转版)事项安排确认表》

7.15《认证信息变更申请表》

7.16《补充合同》

7.17《不符合项及纠正措施报告》

7.18《审核计划》

7.19《首/末次会议签到表》

7.20《文审报告》

7.21《管理体系审核报告》

7.22《审核现场技术问题申报处理单》

7.23《终止审核现场审核决定书》

7.24《认证审核结果通知书》

7.25《认证证书暂停通知书》

7.26《认证证书撤销通知书》

7.27《认证证书恢复通知书》

8、附录

附录 A：商务行为守则

附录 B：认证收费标准

附录 C：现场审核取证抽样方法

附录 A：

商务行为守则

任何个人（包括委托或受托于他人、专/兼职/临时）在任何场合从事中标通认证业务营销活动中，均应承诺并无条件执行以下守则：

A.1．声明：中标通决不从事有损公正性的活动，不直接或间接提供：

a)认证对象所提供的服务；

b)为获得或保持认证的咨询服务；

c)设计实施或保持管理体系的服务。

A.2．不得以任何方式推销咨询业务，暗示或宣称如果使用了某一特定的咨询或培训服务，认证会更简单，更容易或更经济，以防造成中标通的认证与咨询活动有联系的印象。

A.3．不得将合同预存放或交由他人特别是咨询机构人员代为签署，以防事实上授予对方中标通业务代表的身份和权利，造成认证和咨询活动有联系的事实。

A.4．禁止在合同明确约定的甲乙方之间直接结算（认证费用）之外，声称或实际接受任何形式的间接结算特别是和咨询机构之间的任何结算。

A.5．禁止承揽：

a)体系覆盖常年平均规模人数严重编差（按实事求是的原则依据劳动生产率、特定产品初始投资规模起点、特定工序要求的最少工位配置、资质要求等判断和确认）或存疑未排除的合同；

b)体系运行时间不足三个月而要求审核的合同；

c)超认证范围的合同；

d)不具备法律法规要求的资质（准产）条件的合同；

e)他机构中止审核或判为严重不符合后（不足三个月）转移委托的合同；

f)不具备生产稳定合格产品所需的起码的生产手段，工艺装备、环境条件的合同；

g)明显低于本公司最低收费标准（含年度费用）的合同。

A.6．不接受或不提交：

a)份数不足的合同；阴阳合同；要约栏目空缺未填的合同；未经许可添加任何内容的合同；涂改处未加盖确认章的合同；

b)《认证申请表》及其附报文件资料种类不全、填列内容不全不实、无法联络的合同。

附录 B：

认证收费标准

序号	收费项目	收费标准 【单位：元（人民币）】	备注
1	认证申请费用	4000 x n	1）n 为认证领域数； 2）人日数按国家规定或备案认证规则执行； 3）证书副本及子证书每张收费 100 元； 4）补发证书每张收费 100 元； 5）年金每年交纳 1 次。
2	审定与注册费用（含证书费）	2000 x n	
3	初次认证审核费用	1000～10000 x 人日数	
4	监督审核费用	1000～10000 x 人日数	
5	再认证审核费用	1000～10000 x 人日数	
6	特殊审核费用	1000～10000 x 人日数	
7	年金（含标志使用）	2000 x n	
8	证书副本费用	100 元/ 张	

注 1:人日数是指认证审核所需的工作人天数(即审核员人数 x 工作天数)；

注 2:具体认证项目收费根据服务工作内容在合同中约定；

注 3:上述收费不含差旅食宿费用，按实际发生额结算，由申请方承担。

附录 C：

现场审核取证抽样方法

C.1 审核组应安排合理的时间针对生产/服务场所审核，通过观察、查阅文件和有关记录、与基层人员的交谈和提问，必要时实际测定等调查方法，抽取一定的样本，获取客观证据。

C.2 抽样只适用于体系中同类过程（或活动）。凡是与认证审核的管理体系所覆盖的产品和管理要素中的活动所涉及到的部门和地区均应列在审核范围之内。

C.3 审核组应使用抽样的方法开展审核，在抽样时，必须注意样本应有一定数量，适当均衡。但不必绝对平均，不同的产品/服务，不同的生产/服务场所，不同的过程采用不同的抽样方法。为突出重点，抓住关键，对关键过程或特殊过程可以适当加大样本量，而一般过程只需抽取少量样本，以示区别。

C.4 样本策划的科学合理性:

C.4.1 明确抽样的对象和总体，要保证一定数量，通常抽取的样本为 1 个到 12 个之间，具体数量据审核对象的规模大小和审核时间而定；

C.4.2 注意分层抽样，可按产品/服务、设备、生产线、岗位、记录和标识等分层；

C.4.3 适度均衡，不要集中在某部门或某段时间内；

C.4.4 独立抽样应坚持审核员亲自选取样本；

C.4.5 对管理绩效影响较大的重点产品、服务、过程、场所应重点抽样,例如：

a)重点信息资产、重大信息安全风险分布场所或单位应重点抽样，重点关注控制措施；

b)关键信息技术服务活动应重点抽样；

c)顾客投诉率较高的产品，关键产品，生产工艺复杂的产品，应关注首件生产、末件生产，停产复工，新品投产，新材料新技术的应用；

d)重要环境因素、重大危险源分布场所或单位应重点抽样，重点关注其控制措施；

e)关键服务接触活动应重点抽样；

f)重点用能设施、设备、过程及系统应重点抽样；

C.4.6 当首次抽样超过可接受的水平时，应加大抽样量审核。