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）、合理化修订	2025.03.18	黄　云

批准_____

审核_____

制订____黄 云____

发布日期	修订日期	实施日期
2020.10.27	2025.03.18	2025.03.18

1 目的

为规范信息安全管理体系认证服务的过程管理，确保认证服务过程规范有效，特制定本程序。

2 范围

本程序适用于中标通国际认证（深圳）有限公司（以下简称中标通）信息安全管理体系的认证申请受理、申请评审、审核方案的策划、审核组的选派、审核实施、认证决定、证书颁发、证后审核及认证状态管理。

3 引用文件

3.1 CNAS-CC01《管理体系认证机构要求》

3.2 CNAS-CC170《信息安全管理体系认证机构要求》

4、 职责

4.1 运营部负责认证申请的受理、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、再认证审核的实施；

4.2 技术部负责认证决定、证书颁发、以及证书状态的管理。

5、 程序

5.1 认证前的活动

5.1.1 认证申请受理

5.1.1.1 运营部按照《询价管理和申请评审管理程序》的认证申请受理要求向认证申请组织公开与认证申请项目相关的公开信息，明确申请组织应具备的条件，要求申请组织填写并提交认证申请资料，初步核实申请组织是否具备相应的条件。

5.1.1.2 运营部按照《询价管理和申请评审管理程序》的申请评审要求对申请组织的提交资料进行申请评审，做出是否受理的评审结论，确定体系覆盖范围、体系覆盖人数， 认证机构应确定审核组及进行认证决定需要具备的能力。ISMS 认证覆盖人数的应按照 CNAS-CC170:2024《信息安全管理体系认证机构要求》附录 C 的 C3.4 部分的要求确定。对于不同性质和不同行业的申请组织，其 ISMS 认证所覆盖的范围，可视申请组织要求的表达方式、产品/服务类型、

活动场所、组织界限等因素予以描述。申请评审结果为可以受理的认证项目，经由运营部与申请方沟通协商，达成最终合同方案，并签订认证合同，如果不受理认证申请则说明拒绝的理由。

5.1.2 认证合同

5.1.2.1 中标通按照《询价管理和申请评审》中合同签置管理要求，与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合同。

5.1.2.2 认证合同应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，包括明确认证机构和客户及其有关人员的责任与义务。

5.1.3　审核方案策划

5.1.3.1 运营部按照《审核方案策划程序要求》通用实施审核方案的基础策划，确定认证类型、认证标准、认证范围及专业、周期方案、抽样方案、审核组的构成、审核人日、审核方式、所确定的信息安全控制等方案要求，并形成《审核方案策划与管控表》。信息安全管理体系审核方案策划还应满足如下 5.2.3~

5.1.3.2 ISMS 审核的审核方案应考虑所确定的信息安全控制。

注 1：信息安全控制能来自于 ISO/IEC 27001 附录 A，和/或其他适用的标准，和/或由组织自行设计。

注 2：ISO/IEC 27007 给出了有关审核的进一步指南。

5.1.3.3 总体考虑

ISMS 审核的审核方案应考虑所确定的信息安全控制：

a）ISMS 和其所覆盖活动的一般信息；

b）ISO/IEC 27001 所规定的、必要的 ISMS 文件的副本，及必要的相关文件。

5.1.3.4 远程审核

实施远程审核活动时中标通应规定程序，以确定在审核客户 ISMS 时应用远程审核活动（“远程审核”）的程度。程序应包括分析对客户使用远程审核的相关风险，风险分析时应考虑以下因素：

a）认证机构和客户的可用基础设施；

b）客户所在的行业；

c）从初次审核到再认证审核的认证周期内的审核类型；

d）认证机构和客户参与远程审核的人员的能力；

e）以往已证实的、对客户实施远程审核的绩效；

f）认证范围。

应在远程审核实施前进行分析。认证周期内使用远程审核的风险分析和理由应予以记录。

审核计划和审核报告应清楚地说明是否实施了远程审核活动。

如果风险评估发现对审核过程的有效性存在不可接受的风险，则不应使用远程审核。

风险评估应在认证周期内进行审查，以确保其持续适用性。

注：如果客户使用虚拟场所（即：组织利用网络环境完成工作或提供服务的地点，相关人员通过网络环境执行流程，不受其所在物理位置的影响。），远程审核技术是审核计划的一个相关部分。

5.1.3.5 初次审核的总体准备

中标通要求客户为调阅内部审核报告和信息安全独立评审报告做出所有的必要安排。

5.1.3.6 审查周期

只有充分的证据证实覆盖认证范围的管理评审和 ISMS 内部审核的安排已经实施、是有效的并将得到保持，认证机构才能认证客户的 ISMS。

5.1.3.7 认证范围

审核组应根据所有适用的认证要求，对包含在确定范围内的客户 ISMS 进行审核。 中标通应确认客户在其 ISMS 范围内满足了 ISO/IEC 27001 中 4.3 的要求。

中标通应确保：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扩展到活动的边界。应确认这在客户的 ISMS 范围和适用性声明中得到了体现。中标通应验证每个认证范围至少有一个适用性声明。

中标通应确保：与不完全包含在 ISMS 范围内的服务或活动的接口，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。与其他机构共享设施（如：IT

系统、数据库和通讯系统或外包一项业务职能），是这类情形的一个示例。

5.1.4　审核时间

审核方案策划人员应根据《审核方案策划程序》、以及《管理体系审核时间管理规定》中 ISMS 审核时间确定的管理要求，策划确定审核时间。

5.1.5 多场所的抽样

审核方案策划人员应《审核方案策划程序》、《多现场审核规定》中的多场所的抽样要求，策划确定多场所抽样方案。

5.1.6 多管理体系标准

审核方案策划人员应《审核方案策划程序》、《结合审核的管理规定》的要求，策划确定多管理体系标准审核方案。

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文件相结合的文件（例如，对信息技术服务、信息安全）。

只要能够证实审核满足了 ISMS 认证的所有要求，ISMS 审核可以和其他管理体系审核相结合。在审核报告中，所有对 ISMS 重要的要素应清晰地体现并易于识别。审核的质量不应因结合审核而受到负面影响。

5.2 策划审核

5.2.1 确定审核目的、范围和准则

审核方案策划人员应根据《审核方案策划程序》中确定审核目的、范围和准则的管理要求，确定审核目的、范围和准则。ISMS 的审核目的还应包括：

a）确定管理体系的有效性；

b）确保客户根据风险评估识别了必要控制；

c）确定实现了客户所建立的信息安全目标。

5.2.2 选择和指派审核组

5.2.2.1 审核方案策划人员应根据《审核方案策划程序》、《审核组组成及管理规定》等关于选择和指派审核组的要求，选择和指派审核组。审核组可以有技术专家，应在实施审核前与客

户就技术专家在审核活动中的作用达成一致。技术专家不担任审核组中的审核员。技术专家由审核员陪同。实习审核员可以参与审核，此时要指派一名审核员作为评价人员。评价人员应有能力接管实习审核员的任务，并对实习审核员的活动和审核发现最终负责。 、

5.2.3　审核计划

5.2.3.1 总则

运营部确保为审核方案中确定的每次审核编制审核计划，以便为有关各方就审核活动的日程安排和实施达成一致提供依据。

注：第一阶段不要求正式的审核计划。

信息安全管理体的审核计划应考虑所确定的信息安全控制措施。

适宜时，审核计划中应识别中审核中所使用的网络支持的审核技术。

注：良好的实践是中标通与接受审核的组织商定一个能最佳地证实其组织全部范围的审核时间。适当时，可考虑季度、月份、日期和班次。

5.2.3.2 编制审核计划

审核计划应与审核目的和范围相适应。审核计划至少应包括或引用：

a）审核目的；

b）审核准则；

c）审核范围，包括识别拟审核的组织和职能单元或过程；

d）拟实施现场审核活动（适用时，包括对临时场所的访问和远程审核活动）的日期和场所；

e）预计的现场审核活动持续时间；

f）审核组成员及与审核组同行的人员（例如观察员或翻译）的角色和职责。

注：审核计划的信息可以包含在一个以上的文件中。

远程审核技术的目标宜是提高审核的有效性和效率，并支持审核过程的完整性。

审核计划应说明用于协助远程审核的工具。

5.2.3.3 审核组任务的沟通

运营部应根据与客商定的审核日期及审核组选派要求，正式任命审核组并为其提供相应的工作文件，以《审核任务书及派出令》的方式明确规定审核组的任务并要求审核组实施：

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；

e）审核组全员完成审核计划的全部工作。

第一、第二阶段的《审核任务书及派出令》可根据预定日程同时发送给审核组，若第一阶段审核组审核结论是不能继续进行第二阶段审核时，应通过审核报告及及时反馈到计划调度人员，计划调度人员及时修订原第二阶段原审核日期，重新进行审核任务安排，若第一阶段审核组审核结论可以继续进行第二阶段审核时，无须修订原审核日期，也无须重新安排审核任务。

5.2.3.4 审核计划的沟通

中标通应提前与客户就审核计划进行沟通，并商定审核日期。

5.2.3.5 审核组成员信息的通报

中标通应向客户提供审核组每位成员的姓名、审核日程，并在客户请求时使其能够了解每位成员的背景情况，应留出时间，以使客户组织能够对某一审核员或技术专家的任命表示反对，并在反对有效时使运营部能够重组审核组。一旦与申请组织确定了审核组，运营部应正式发出《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监管理计划。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（技术专家和实习审核员除外）。

5.3 初次认证

5.3.1 初次认证审核

5.3.1.1 总则

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

5.3.1.2 **第一阶段**

5.3.1.2.1 策划应确保第一阶段的目的能够实现，应告知第一阶段需实施的任何现场活动。

注：第一阶段不要求正式的审核计划。

5.3.1.2.2　第一阶段审核应：

a）审核客户的文件化的管理体系信息；

b）评价客户现场的具体情况，并与客户的人员进行讨论，以确定第二阶段的准备情况；

c）审查客户理解和实施标准要求的情况，特别是对管理体系的关键绩效或重要的因素、过程、目标和运作的识别情况；

d）收集关于客户的管理体系范围的必要信息，包括：

- 客户的场所
- 使用的过程和设备
- 所建立的控制的水平（特别是客户为多场所时）
- 适用的法律法规要求；

e）审查第二阶段所需资源的配置情况，并与客户商定第二阶段的细节；

f）结合管理体系标准或其他规范性文件充分了解客户的管理体系和现场运作，以便为策划第二阶段提供关注点；

g）评价客户是否策划和实施了内部审核与管理评审，以及管理体系的实施程度能否证明客户已为第二阶段做好准备。

在第一阶段，应获取有关 ISMS 设计的文件，其中包括 ISO/IEC 27001 所要求的文件。

在第一阶段，应充分了解在组织环境下所进行的 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，以及特别是客户的审核准备情况。在此基础上，才能进行第二阶段的策划。

5.3.1.2.3　第一阶段审核要求

5.3.1.2.3.1 初次认证审核的第一阶段审核应在客户现场实施审核。

5.3.1.2.3.2 现场审核（含远程审核）时间一般按第一阶段不低于不低于 0.5 个审核人日。当客户由于信息安全的原因在申请评审阶段不能提供给认证机构足够的信息时，认证机构应通过

第一阶段审核在客户的现场补充对上述信息的确认，并完成申请评审任务。这种情况下，认证机构应增加第一阶段现场审核时间。

5.3.1.2.3.3 第一阶段对于多场所的审核重点应放在总部，以全面了解情况，并为第二阶段审核确定抽样方案，总部时间应充分；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；分场所的选择应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。审核组长编制的审核计划应提前传递给受审核方，并予以确认。现场审核过程中如需调整审核计划必须与运营部沟通，经同意后审核组长可在审核计划中补充说明或调整审核计划。

5.3.1.2.3.4 第一阶段现场审核须使用《检查表》，做相应的审核记录。

5.3.1.2.3.5 第一阶段审核，应形成书面的《管理体系第一阶段审核报告》，明确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，做出第一阶段审核结论，判断具备/不具备实施第二阶段审核条件，可否实施二阶段审核，并告知客户。第一阶段应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。

5.3.1.2.3.6 认证机构在确定第一阶段和第二阶段的间隔时间时，应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。认证机构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，认证机构应考虑是否有必要重复整个或部分第一阶段。认证机构应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。

5.3.1.2.3.7 第一阶段采用非现场审核或远程审核方式的，应在报审核报告中加以说明。

5.3.1.2.3.8 第一阶段审核结束后，审核组长负责形成第一队段审核报告，并通过邮件或其他适宜的方式将能否进行第二阶段审核的结论、审核报告反馈到认证机构。

5.3.1.2.3.9 认证机构应基于第一阶段的输出和反馈，确认第二阶段所需的能力及审核安排。同时策划第一、二阶段审核日程、发放《审核任务书及派出令》的，若第一阶段审核组结论是不能继续进行第二阶段审核时，应重新审核任务安排，若第一阶段审核组审核结论可以继续进行第二阶段审核时，无须修订原审核计划，也无须重新安排审核任务。

5.3.1.3　第二阶段审核

第二阶段审核的目的是评价受审核方管理体系的实施情况(包括有效性)，确认客户遵守自身的方针、策略和规程情况。第二阶段审核应在受审核方的现场进行，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。

鉴于第二阶段的目的是评价客户 ISMS 的实施情况及其有效性，评价客户遵守自身的方针、策路和规程情况，因此，第二阶段的审核应重点关注：

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，确定控制目标和控制；

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；

f）针对客户方针的管理职责；

h）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。

5.3.1.4　初次认证的审核结论

审核组应对在第一阶段和第二阶段审核中收集的所有信息和证据进行分析，以评审审核发现并就审核结论达成一致。

为使中标通做出认证决定，审核组至少应向中标通提供以下信息：

a)　审核报告；

b)　对不符合的意见，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。

中标通在评价审核发现和结论及任何其他相关信息(如公共信息、受审核方对审核报告的意见)的基础上，进入本程序“5.5　认证决定”阶段。

5.4　实施审核

5.4.1 总则

审核组应按中标通确定的程序实施现场审核，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。

审核组应要求客户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，应确定客户识别、检查和评价信息安全相关风险的规程及其实施结果是否与客户的方针、目标和指标一致，应确定用于风险评估的规种是否健全并得到正确实施。

5.4.2　召开首次会议

审核组应与客户的管理层（适用时，还包括拟审核职能或过程的负责人员）召开正式的首次会议，并记录参加人员。首次会议通常应由审核组长主持，会议目的是简要解释将如何进行审核活动，并应包括下列要素。详略程度可与客户对审核过程的熟悉程度相一致：

a）介绍参会人员，包括简要介绍其角色；

b）确认认证范围；

c）确认审核计划（包括审核的类型、范围、目的和准则）及其任何变化，以及与客户其他相关安排，例如末次会议的日期和时间，审核期间审核组与客户管理层的会议的日期和时间；

d）确认审核组与客户之间的正式沟通渠道；

e）确认审核组可获得所需的资源和设施；

f）确认与保密有关的事宜；

g）确认适用于审核组的相关的工作安全、应急和安保程序；

h）确认可得到向导和观察员及其角色和身份；

i）报告的方法，包括审核发现的任何分级；

j）说明可能提前终止审核的条件；

k）确认审核组长和审核组代表中标通对审核负责，并应控制审核计划（包括审核活动和审核路径）的执行；

l）适用时，确认以往评审或审核的发现的状态；

m）基于抽样实施审核的方法和程序；

n）确认审核中使用的语言；

o）确认在审核中将告知客户审核进程及任何关注点；

p）让客户提问的机会。

5.4.3　审核中的沟通

5.4.3.1 在审核中，审核组应定期评估审核的进程，并沟通信息。审核组长应在需要时在审核组成员之间重新分配工作，并定期将审核进程及任何关注告知客户。

5.4.3.2 当可获得的审核证据显示审核目的无法实现，或显示存在紧急和重大的风险（例如安全风险）时，审核组长应向客户（如果可能还应向运营部）报告这一情况，以确定适当的行动。该行动可以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。审核组长应向运营部报告所采取行动的结果。

5.4.3.3 如果在现场审核活动的进行中发现需要改变审核范围，审核组长应与客户审查该需要，并报告运营部。

5.4.3.4 终止审核

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。

5.4.5　收集和验证信息

5.4.5.1 在审核中应通过适当的抽样来收集与审核目的、范围和准则相关的信息（包括与职能、活动和过程之间的接口有关的信息），并对这些信息进行验证，使之成为审核证据。

5.4.5.2 信息收集方法应包括（但不限于）：

a）　面谈；

b)　对过程和活动进行观察；

c)　审查文件和记录。

5.4.5 确定和记录审核发现

5.4.5.1　审核发现应简述符合性，详细描述不符合以及为其提供支持的审核证据，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。

5.4.5.2 可以识别和记录改进机会，除非某一管理体系认证方案的要求禁止这样做。但是属于不符合的审核发现不应作为改进机会予以记录。

5.4.5.3 关于不符合的审核发现应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。应与客户讨论不符合，以确保证据准确且不符合得到理解。但是，审核员应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：

✧ 错误使用认证标记和证书，若属明知故犯恶意违规、造成严重后果的，应判定为严重不符合项；其情节及后果并不严重的，应被判定为轻微不符合项。应该注意的是，凡属此类不符合项应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。

5.4.5.4 审核组长应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，未解决的分歧点应予以记录。

5.4.6 准备审核结论

在末次会议前，审核组应：

a）对照审核目的审查审核发现和审核中收集的任何其他适用的信息；

b）考虑审核过程中内在的不确定性，就审核结论达成一致；

c）确定任何必要的跟踪活动；

d）确认审核方案的适宜性，或识别任何所需要的修改（例如范围、审核时间或日期、监督频次、能力）。

5.4.7　召开末次会议

5.4.7.1　审核组应与客户的管理层（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。末次会议通常应由审核组长主持，会议目的是提出审核结论，包括关于认证的推荐性意见。不符合应以使其被理解的方式提出，并应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。

5.4.7.2　末次会议还应包括下列要素。详略程度应与客户对审核过程的熟悉程度一致：由组长主持，受审核方各部门主要负责人参加。议程如下：

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，但应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“不符合通知单”，必要时宣读观察项；不符合项应取得企业管理者代表或其它负责人的确认。

f）征询受审核方对不符合事实是否仍存在异议；

g）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……）

h）审核结论

现场审核通过：审核小组建议中标通对申请组织的 ISMS 给予注册；

改善后通过：审核小组建议，申请单位应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。

审核小组应给申请组织提供针对审核结果和说明提出质疑的机会，包括：

a）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；

b）中标通在审核后的活动；

c）说明投诉处理过程和申诉过程；

d）纠正/纠正措施要求。

强调不能仅采取就事论事的“补救”措施，应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。

5.4.7.3 客户应有机会提出问题。审核组与客户之间关于审核发现或结论的任何分歧意见应得到讨论并尽可能获得解决。任何未解决的分歧意见应予以记录并提交中标通。

5.4.8 审核报告

5.4.8.1 审核组应为每次审核提供书面报告。审核组可以识别改进机会，但不应提出具体解决办法的建议。中标通应享有对审核报告的所有权。

5.4.8.2 在现场审核的末次会议上，审核组应口头说明申请组织是否符合规定的认证要求，以及审核小组的结论。审核组长一周内应向审核部提交书面的审核报告，并应对审核报告的内容负责。审核报告应提供对审核的准确、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）本机构名称；

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）审核准则；

e）审核目的；

f）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；

g）审核组长、审核组成员及任何与审核组同行的人员；

h）（现场或非现场）审核活动的实施日期和地点；

i）与审核类型的要求一致的审核证据、审核发现和审核结论；

j）已识别出的任何未解决的问题；

k) 审核的说明，其中包括了文件评审的摘要；

l) 对客户信息安全风险分析进行认证审核的说明；

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) ISMS 范围；

o)所采用的主要审核路线和所使用的审核方法；

p)形成的观察结果，包括正面的(例如，值得注意的特征)和负面的（例如:潜在的不符合）；

q)对客户 ISMS 与认证要求的符合性的评价意见、对不符合的清楚说明、所引用的适用性声明的版本，以及适用时，与客户以往认证审核结果的任何有用的对照；

注：完成的问卷、检查清单、观察结果、日志或审核员笔记可以构成完整的审核报告的一部分。如果使用这些方法，这些文件应作为支持认证决定的证据提供给认证机构。在审核过程中，有关被评价的样本的信息应包含在审核报告或其他认证资料中；

报告应考虑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；

r）关于 ISMS 要求和信息安全控制的实施与有效性、最重要的观察（正面的和负面的）的接要；

s）客户的 ISMS 是否获得认证的建议，以及支持建议的信息。

5.4.8.3 审核报告还应包含：

a)关于管理体系符合性与有效性的声明以及对下列方面相关证据的总结：

-- 管理体系满足适用要求和实现预期结果的能力；

-- 内部审核和管理评审的过程；

b)对认证范围适宜性的结论；

c)确认是否达到审核目的。

审核报告打印一式两份，一份寄给客户，一份本中标通存档。

5.4.9 不符合原因分析

对于审核中发现的不符合，审核组应要求客户在规定期限内分析原因，并说明为消除不符合已采取或拟采取的具体纠正和纠正措施。

5.4.10　纠正和纠正措施评审与验证

审核组应评审和/或验证客户提交的纠正和纠正措施及相应的整改证据的可接受性及有效性，并将审查和验证的结果告知客户。

不符合评审或验证可通过审查客户提供的文件不实现，或在必要时实施现场验证来验证纠正和纠正措施的有效性。

5.5　认证决定

5.5.1 总则

5.5.1.1 认证决定由技术部组织专业技术人员对审核报告及认证过程中收集到的信息进行评审，评审合格或问题改善后，然后由相关人员做出同意或不同意注册或保持注册的认证决定。做出认证决定的人员不应是参加此次审核的人员，被指定进行认证决定的人员须经过能力评价具有适宜的能力。 认证决定人员（不包括委员会成员）应为中标通的雇员，或者是中标通控制下的实体的雇员；或者与中标通或中标通控制的实体具有在法律上有强制实施力的安排。中标通的组织控制应为下列情况之一：

a）中标通拥有另一实体的全部或多数所有权；

b）中标通在另一实体的董事会中占多数；

c）在一个通过所有权或董事会控制联结而成的法律实体网络中（中标通处于其中），中标通对另一实体有形成文件的权力。

5.5.1.2 认证决定人员应在评价审核发现和结论及任何其他相关信息(如公共信息、受审核方对审核报告的意见)的基础上做出认证决定，必要时由认证决定人发起，组织技术委员会做出同意或不同意注册或保持注册复核决定。

认证决定人员对前而的推荐意见具有否决权。

通常情况下，对授予认证做出决定的人员或委员会不宜推翻审核组的负面建议。如果发生这种情况，认证机构应记录其做出推翻建议的决定的依据，并说明其合理性。

5.5.1.3 应记录每项认证决定，包括从审核组或其他来源获得的任何补充信息或澄清。

5.5.2 认证决定人在做出决定前应确认：

a)审核组提供的信息足以确定认证要求的满足情况和认证范围；

b)对于所有反映以下问题不符合，中标通已评审、接受并证实了纠正和纠正措施的有效性：

- ✧ 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。
- ✧ 制定的信息安全目标不可测量、或测量方法不明确。
- ✧ 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。
- ✧ 其他严重不符合项。

c)其他一般不符合，中标通已评审并接受了受审核方计划采取的纠正和纠正措施。

5.5.3 颁发认证证书

5.5.3.1 在满足 5.5.2 条要求的基础上，认证机构有充分的客观证据证明申请组织满足下列要求的，评定该申请组织符合认证要求，向其颁发认证证书。

（1)申请组织信息安全管理体系管理评审和内审安排已实施，符合标准要求且运行有效。

（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。

5.5.3.2 为使中标通做出认证决定，审核组按规定至少向中标通提供以下信息：

a)审核报告；

b)对不符合的意见，适用时，还包括对客户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（见 9.1.2）的信息的确认；

d)对是否达到审核目的的确认；

e)对是否授予认证的推荐性意见及附带的任何条件或评论。

5.5.3.3　如果中标通不能在第二阶段结束后 6 个月内验证对严重不符合实施的纠正和纠正措施，则须在推荐认证前再实施一次第二阶段。

5.5.3.4 技术部须按照《认证后审核及管理程序》实施证书转换。确保当认证从别的认证机构转换到中标通时，确保有过程在充分获取信息的基础上再做出认证决定。

5.5.3.5 技术部按照《证后审核及管理程序》，规定授予再认证的要求。根据再认证审核的结果，以及认证周期内的体系评价结果和认证使用方的投诉，做出是否更新认证的决定。

5.5.4 中标通不把批准、保持、扩大、暂停和撤销认证的权力委任给外部人员和机构。

5.5.5 获准认证注册的企业将得到认证结果通知单及中标通认证证书等文件。这些文件应表明认证所覆盖的供方及其每个场所的：

a) 每个获证组织的名称和地理位置(或多场所认证范围内总部和所有场所的地理位置)；

b) 授予、扩大或更新认证的日期；

c) 认证有效期或与认证周期一致的应进行再认证的日期；

d) 唯一的识别代码，即证书编号；

e) 对获证组织的审核所用的标准和(或）其他规范性文件，包括版次和(或）修订号；

f) 认证范围(述及每个场所的相关产品(包括服务)、过程等)；

g) 中标通的名称、地址和认证标志，签发人签名。

h) 认证用标准和(或)其他规范性文件所要求的任何其他信息；

i) 在颁发经过修改的认证文件时，区分新文件与任何已作废文件的方法。

5.5.6 认证证书的有效期为三年。

5.6 保持认证

5.6.1 总则

证书的保持应确保在证实获证客户持续满足管理体系标准要求后才能保持对客户的认证。当中标通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，中标通有制度要求审核组长向中标通报告需由具备适宜能力（见 7.2.8）且未实施该审核的人员进行复核，以确定能否保持认证；

b)由具备能力的中标通人员如质量稽查员等对中标通的监督活动进行监视，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。

5.6.2 监督活动

5.6.2.1 总则

5.6.2.1.1ISMS 监督的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。监督审核方案应至少包括：

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；

5.6.2.1.2 监督活动包括对获证客户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。

5.6.2.1.3 监督审核时间间隔应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 15 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。

5.6.2.1.4 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。

5.6.2.2 监督审核

每次监督审核至少要审核的内容详见《证后审核与管理程序》相关内空要求，ISMS 每次监督审核还至少要审核如下内容：

a) ISMS 在实现客户信息安全方针的目标方面的有效性；

b) 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；

c) 所确定的控制变更，以及其引起的适用性声明的变更；

d) 控制的实施和有效性（根据审核方案来审查）。

在监督审核过程中，中标通须检查客户提交给认证机构的申诉和投诉记录。在发现任何不符合或不满足认证要求时，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。特别是，监督报告应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。监督审核报告应至少完全覆盖 5.6.2.2 的全部要求。

5.6.3 再认证

再认证审核的目的是确认 ISMS 作为一个整体的持续符合性与有效性，以及与认证范围的持续相关性和适宜性。按照《认证后审核及管理程序》实施，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。证书持有者应在证书有效期期满前三个月向中标通提出再认证的申请，中标通根据再认证的结果决定是否重新发放注册证书。

5.6.4 特殊审核

5.6.4.1 扩大认证范围

对于已授予的认证，应按照《认证后审核及管理程序》中扩大认证范围审核的要求实施。

5.6.4.2 提前较短时间通知的审核

中标通为调查投诉、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。提前较时间通知的审核按照《认证后审核及管理程序》中提前较时间通知的审核要求实施。

5.6.5 变更管理

证书持有者的注册组织名称、地址变更，产品/服务（地域边界）范围的扩大/缩小，生产工艺、产品类型/规格等发生变化时，应按照《认证后审核及管理程序》中“认证范围的变更”要求实施变更管理。

颁证后发生认证要求的变更的，应按照《认证后审核及管理程序》中“认证要求的变更”实施变更管理。

5.6.6 证书状态管理

当客户的获证 ISMS 出现暂停、撤销、或缩小认证范围情况时，技术部按照《批准、保持、更新、扩大、缩小、暂停、撤销和恢复认证程序》的相关规定，对相关证书实施暂停、撤销或缩小认证范围的管理。

5.7 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，技术负责按照《申诉/投诉和争议处理程序》实施处理，并记录处理结果。

5.8 客户的记录管理

5.8.1 技术部应按照《记录控制程序》、《认证项目档案管理规定》的要求，对所有客户(包括所有提交申请的组织、接受审核的组织和获得认证或被暂停或撤销认证的组织)保持审核及其他认证活动的记录。保证申请组织和客户记录的安全，以确保满足保密要求。运送、传输或传递记录的方式应确保保密。记录保存期应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。

7、 相关程序文件

7.1 《证后审核及管理程序》

7.2 《审核方案策划程序》

7.3 《认证业务范围管理程序》

8、 相关工作文件

8.1 《管理体系审核时间管理规定》

8.2 《结合审核的管理规定》

8.3 《审核组组成及管理规定》

8.4 《拟认证组织须知》

8.5 《多现场审核规定》

8.6《认证项目档案管理规定》

9、 相关表格/记录

9.1 审核用表格文件包