上海英格尔认证有限公司

信息安全管理体系
认证管理程序

编 制 Compiling	审 核 Auditing	批 准 Approving	发布日期 Issuing date	版 本 Edition
编制小组	管理者代表	杨宏奇	2015.12.15	C版
修 订 说 明 Revision note		修订页数 Revision page	修订日期 Revision date	批 准 Approval
根据ISMS认证标准换版修订			2016.10.20	杨宏奇
全文修订		/	2023.02.10	王珍
根据ISO/IEC 27006-1:2024要求修订		P4、P15、P19	2025.03.21	王珍

1 目的

本文件用于指导上海英格尔认证有限公司（以下简称ICAS）开展信息安全管理体系（以下简称ISMS）认证活动，以保证与认证有关的活动具有一致性、连续性和可追溯性。

2 范围

本文件适用于ICAS信息安全管理体系业务范围内的认证活动管理。

3 职责

- 市场部负责认证申请的处理、信息的提供、报价、客户满意度调查及其它必要的协调工作；
- 审核部负责合同评审、审核方案策划、审核组委派、审核行程的安排，审核任务书的发放及审核计划的确认；
- 审核组长负责审核过程的执行；
- 注册部负责认证决定、证书的制作、发放和管理；
- 技术资源部负责对参与管理和实施审核与认证人员进行专业能力评定、专业能力发展策划（如见证的安排、专业能力持续监督）；
- 品管部-技术岗负责ISMS认证业务运转过程中必要的技术文件的编制；
- 品管部负责认证用文件的更新及认证过程的监督。

4 认证基本流程

① 认证申请

② 申请评审

③ 合同评审

④审核方案策划

⑤现场审核的准备

⑥ 初次认证

⑦ 认证决定

⑧发放证书

⑨获证后的监督

⑩再认证

5 认证依据

信息安全管理体系认证以ISO 27001:2022《信息安全、网络安全和隐私保护-信息安全管理体系-要求》为认证依据，并按照《信息安全管理体系认证技术领域及分类表》（ICASP12 附件17）所列范围开展认证业务。

6 认证程序

6.1 认证申请

6.1.1 申请认证组织应按ICAS要求，提供以下申请信息或资料：

(1)法人资格证明(工商营业执照、事业单位法人证书或社会团体法人登记证书)；

(2)取得相关法规规定的行政许可文件(适用时)；

(3)从事的业务活动符合中华人民共和国相关法律、法规、信息安全标准和有关规范的要求；

(4)对信息安全管理体系认证范围涉及的业务活动的描述；

(5)已按认证依据ISO/IEC 27001和其他的认证相关要求建立和实施了文件化的信息安全管理体系；

(6) 体系有效运行3个月以上，并且已完成内部审核和管理评审。

(7)组织依据ISO/IEC 27001 标准所制定的适用性声明，以及是否删减了控制集及删减理由。

6.1.2 申请认证组织提供的信息应包括以下：

(1)申请组织的行业类别；

(2)申请认证的范围；

(3)申请组织的一般特征，包括其名称、物理场所的地址；是否有在虚拟场所通过远程方式从事相关活动的情况；

(4)申请组织与申请认证的领域相关的一般信息，包括其活动，人力与技术资源，以及适用时，其在一个较大实体中的职能和关系；

(5)申请组织采用的所有影响符合性的外包过程的信息；

(6)接受与信息安全管理体系有关的咨询的情况；

(7)特定认证方案所要求的申请组织的相关详细情况，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；

(8)申请组织采用的所有影响符合性的外包过程；

(9)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；

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

适当时，可要求客户向其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，以便可以判断ICAS是否具备对该客户实施认证活动的资格或条件。

6.1.3 市场部收到认证申请时，须对认证申请及补充信息进行评审确认，以确保：

1) 申请资料齐全，申请组织从事的活动符合相关法律法规的规定，信息充分，可以进行审核；

2) 解决了ICAS与申请组织之间任何已知的理解差异；

3) ICAS有能力并能够实施认证活动；

4) 考虑了申请的认证范围、申请组织的运作场所、完成审核需要的时间和任何其他影响认证活动的因素（语言、安全条件、对公正性的威胁等）；

5) 至少实施过一次覆盖认证范围的管理评审和内部审核；否则不对该ISMS实施认证

6) 保持了决定实施审核的理由的记录。

7) 认可业务范围的正确实施。

- 如果申请属于认可的业务范围，则继续6.1.3及之后的步骤；
- 如果申请不属于认可的业务范围，但属于由ICAS顾问委员会批准的业务能力范围内，则应于当天或最迟于第二个工作日通知申请方，征求申请方是否接受没有认可标志的证书；如果客户接受，继续6.1.3的步骤；
- 如果申请不属于认可的业务范围，也不属于由英格尔的业务能力范围内，则应于当天或最迟第二个工作日通知客户，终止进一步的步骤。

6.1.4 市场部在收到申请的当天或最迟不超过第二个工作日内，分别根据《ISMS 审核人天表及收费标准》等对认证活动进行报价；申请人为多场址时，应请客户填写《多场所多现场、在建项目清单》（MFP0350）。《认证合同》（MAP0312）应跟报价单同时传真给客户。

6.1.5 市场部收到报价确认后，将《认证合同》（MAP0312）原件一式两份以适当的方式提供给申请方。

6.1.6 市场部收到报价确认后，应于当天或最迟不超过第二个工作日内将《认证申请表》(MFP0388)转交审核部。

6.1.7 市场部确定审核意向后，应及时向审核申请方要求提交信息安全管理手册、程序文件。以确认申请组织为达到信息安全目标而建立了文件化的管理体系。

6.1.8 认证申请的受理

对符合6.1 要求的，市场部可决定受理认证申请；对不符合上述要求的，市场部应通知申请组织补充和完善，或者不受理认证申请。

市场部应完整保存认证申请的审查确认工作记录。

6.2 合同评审

6.2.1 审核部合同评审人员进行合同评审，必要时，项目经理应协助合同评审人员完成合同评审。合同评审人员在进行合同评审时不可在合同评审阶段将高风险的风险等级降低、应待一阶段完成后才可根据现场实际情况进行降级处理。评审人员在综合各方面的因素后确定审核所需人天及认证专业范围。任何等级降低或提高、人天减少或增加的理由均应给予记录。按《信息安全管理体系（ISMS）认证审核人日计算方法》（D27）确定审核所需人日数及认证专业范围。合同评审时，要考虑以下项目：

1) 申请方的管理体系是否主要以电子化（“e-based”）过程和文件为主；
2) 是否结合审核、联合审核或一体化审核；
3) 管理体系范围内活动的分包情况；
4) 以前审核的结果；
5) 对于多场所或含有临时场所或在虚拟场所办公的组织，应考虑：
   - 是否具有利用计算机辅助审核技术进行远程审核；
   - 多场所运做组织应确定组织总部作为其实施认证的合同方；
   - 检查组织在每个各案场所在何种程度上按照相同的程序和方法生产或提供本质上同类的服务，只有在肯定全部场所符合多场所运作准则后，抽样才能用于各个场所；
   - 一个服务性组织中实施认证所覆盖的活动的全部场所，没有准备好同时进行认证时，应要求组织确定包含在认证书中的场所。

6.2.2 合同评审的结果应能够确保：

(1)识别申请组织的行业类别和与之相应的信息安全提供过程的特性和服务要求；

(2)掌握国家对相应行业的信息安全管理体系认证的管理要求；

(3)申请组织及其管理体系的信息充分，可以进行审核；

(4)认证要求已有明确说明并形成文件，且已提供给申请组织；

(5)解决了ICAS与申请组织之间任何已知的理解差异；

(6)ICAS有能力并能够实施认证活动；

(7)考虑了申请的认证范围、申请组织的运作场所、完成审核需要的时间和任何其他影响认证活动的因素；

(8)保持了决定实施审核的理由的记录。

6.3 审核方案

6.3.1 审核部负责识别审核方案开发、实施、管理和改进审核活动所必需的资源；

6.3.2 审核方案策划

由审核部负责，以清晰地识别这些审核活动。这些审核活动用以证实客户的管理体系满足依据所选标准或其他规范文件的认证的要求。

策划时，应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。

审核方案应包括两阶段初次审核，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。审核方案的确定和任何后续调整应考虑客户的组织规模、其管理体系，服务过程的范围与复杂程度，以及经证实的管理体系有效性水平和以前审核的结果。

第一阶段，客户应至少提供以下信息：1）ISMS和其所覆盖活动的一般信息；2）ISO/IEC 27001中所规定的、必要的ISMS文件的副本，以及必要的相关文件。

确定认证范围的时候，审核方案策划人员应确保：1）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。ICAS应确认这在客户的 ISMS 范围和适用性声明中得到了体现。ICAS应验证每个认证范围至少有一个适用性声明。2）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。3）客户 ISMS接受审核的准则应是标准ISO/IEC 27001与所实施的业务相关的其他文件，可以作为认证要求。4）及时获取客户方对ISMS 适用法律法规的重大变更的信息。

如果ICAS计划进行远程审核活动，要确定可应用于审核客户 ISMS 的远程审核活动（“远程审核”）的级别。包括对与客户使用远程审核相关的风险进行分析，且在执行任何远程审核之前进行分析，其中应考虑以下因素：1）ICAS和客户可用的基础设施；2）客户经营所在的行业；3）认证周期中从初次审核到再认证审核的审核类型；4）参与远程审核的认证机构和客户人员的能力；5）先前为客户展示的远程审核表现；6）认证范围。

如果风险评估发现审核过程的有效性存在不可接受的风险，则不得使用远程审核。

现场审核应安排在认证范围覆盖的服务活动正常运行时进行。

如果受审核方体系包含多个现场或多个临时场所，且这些场所都处于该申请组织授权和控制时，根据客户填写的《多场所多现场、在建项目清单》（MFP0350），制定合理的抽样方案以确保对各场所管理体系的正确审核。该抽样方案应考虑到不同场所的活动是否存在可能对信息安全管理产生显著影响的区域性因素，如果是，则不能进行抽样。

6.3.3 审核目标应由公司审核部负责确认。审核范围和准则包括任何更改应由审核部在市场部的协助下与申请认证客户商讨后确定。

如果客户事先没有禁止ICAS接触某一信息资产，或未告知ICAS应满足的要求，但ICAS在认证过程中发现自己并不具备接触该信息资产的资格和条件，应立即向客户提出。

6.4 确定审核人日

ICAS根据申请组织提交的信息，梳理清其规模、特性、业务复杂程度、信息安全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，审核人日数的确定见《信息安全管理体系（ISMS）认证

审核人日计算方法》（D27）。

确定审核人日时，充分考虑与审核相关的所有活动，包括报告审核情况所需的时间。

6.5 多场所的抽样

6.5.1 当客户拥有满足以下a)至c)的多个场所时，ICAS将使用基于抽样的方法进行多场所认证审核：

a） 所有的场所在同一个 ISMS 下运行且该 ISMS 实行集中统一的管理、审核和管理评审；

b） 所有的场所都包含在客户的 ISMS 内部审核方案中；

c） 所有的场所都包含在客户的 ISMS 管理评审方案中。

6.5.2 多场所的抽样程序

ICAS 使用基于抽样的方法时，抽样程序应确保：

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

b） 结合以下因素，ICAS 抽取具有代表性的场所：

1) 总部及其他场所的内部审核的结果；
2) 管理评审的结果；
3) 场所规模的差异；
4) 各场所业务目的的差异；
5) 不同场所的信息系统的复杂程度；
6) 工作实践的差异；
7) 所实施的活动的差异；
8) 控制的设计与运行的差异；
9) 与关键的信息系统或处理敏感信息的信息系统之间的潜在交互；
10) 任何不同的法律要求；
11) 地域因素和文化因素；
12) 场所的风险状况；

c） 发生在特定场所的信息安全事件。

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

e） 在授予认证之前，ICAS 审核了 ISMS 中每个具有重大风险的场所；

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

g) 无论是在总部还是在单个场所发现不符合，纠正措施程序的实施适用于证书所覆盖的总部和所有场所。

6.6 管理体系结合审核

6.6.1 信息安全管理体系文件与其他管理体系文件的整合

ICAS可以仅提供信息安全管理体系认证服务，或结合信息安全管理体系认证提供其他管理体系认证服务。ICAS应有程序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。

只要信息安全管理体系以及与其他管理体系的适当接口能够清楚地被识别，可以允许申请组织将信息安全管理体系文件与其他管理体系文件(例如，质量管理体系、环境管理体系，职业健康安全管理体系等)相结合。

6.6.2 结合审核原则

信息安全管理体系的审核和其他管理体系的审核相结合，必须以审核活动满足信息安全管理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，应清晰体现所有与信息安全管理体系有关的重要要素的描述并易于识别。

结合审核时，按照《一体化管理体系审核的实施和管理程序》实施。

6.7 审核的策划

6.7.1 确定审核目的、范围和准则

审核目的应包括确定管理体系的有效性，以确保客户已根据风险评估实施了适用的控制并实现了所设立的信息安全目标。

审核范围和准则，客户提出申请后，通过合同评审及审核方案策划予以确定，确定的信息体现在审核任务派遣信息中。

6.7.2 确定审核组

6.7.2.1 ICAS指定的认证审核人员必须具备信息安全管理体系认证注册资格。

6.7.2.2 审核组可以由一个人组成，前提为其满足相关的全部技术能力准则要求则。也可以有多人组成，其中至少有一名专职审核员。必要时可以补充技术专家以增强审核组的技术能力。具有信息安全、信息安全法规等方面的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。

6.7.2.3 ICAS通过发出审核任务派遣通知书，明确所任命的审核组；并由审核部通过认证信息管理系统，为审核组发送工作文件。

6.7.2.4 审核部应将审核组派遣通知书在文件审核之前同时发放给客户及审核组，征求客户及审核组成员的意见，以避免利益冲突。如果客户反对审核组或审核组成员，声明有利益冲突， 应立即调整审核组成员。

6.7.2.5 对于监督和特殊审核活动，仅那些与所安排的监督活动和特殊审核活动相关的要求适用。

当为特定认证审核选择审核组时，ICAS应确保每次委派时审核组的能力是适宜的。审核组应：1）对拟认证ISMS范围内的特定活动具备适当的技术知识，以及相关时，对这些活动的相关规程和其潜在信息安全风险具备适当的技术知识（技术专家可以履行此项职责）；2）理解客户，足以基于客户 ISMS 范围和组织环境对ISMS（该体系管理着客户活动、产品和服务的信息安全） 进行可靠的认证审核；3）适当地理解适用于客户ISMS的法律法规要求。

6.7.3 审核计划

6.7.3.1审核组在编制ISMS审核计划时，应考虑所确定的信息安全控制措施。

6.7.3.2 审核组长在安排审核计划时应参照客户管理体系文件的描述及相关的职能分配表（客户有提供时）和《审核组派遣通知书》（MFP0308）合理安排审核时间和人员。审核组长或其指定的人员与审核组成员协商，对具体的过程、职能、或活动等的审核工作分配给审核组成员。审核工作的分配应考虑充分利用资源和时间，任务分配后，审核组长或其指定人员应对计划进行审核，审核计划应具有一定的灵活性，以允许更改，随着现场审核活动的进展，审核范围的更改可能是必要的，并注意以下事宜：

a) 审核计划应体现过程审核方式；
b) 实习审核员不可单独审核；
c) 观察员不可执行审核；
d) 技术专家必须分配作关键区域的审核员的陪同；为审核员提供技术咨询并对审核记录签字确认。不能把技术专家当审核员。为严肃保密性，技术专家陪同过程中个人记录应交审核员留存，并归档；

e) 见证审核员可以作为审核组成员，作为审核员见证时,不可同时审核,但作为审核组长见证时，可作为审核组成员同时参加审核；

f) 审核时间每天每人8小时；

g) 审核时间应与《任务书》中一致；

h) 审核计划必须由审核组长或审核组长指定的人员完成。若由于种种原因无法由审核组长或审核组长指定的人员完成，由公司指定的其他人员完成时，审核组长应于现场审核前或现场时确认，必要时于现场进行适当调整，并于现场在审核计划上签字确认。调整不得违反上述要求，否则为审核组长的责任；

i) 新进审核员初试见证为现场见证，且见证审核员与被见证审核员至少有1小时以上针对部分条款分在同组审核，审核计划发给客户前应交给审核部确认。

审核计划应包括：

●审核目的

●审核准则

●审核范围

●拟审核的组织和职能单元或过程

●现场审核活动的日期和地点；

●现场审核活动预期的时间和期限，包括于受审核方管理层的会议及审核组会议；

●审核组成员和向导的作用和职责；

●为审核的关键区域配置适当的资源；适当时，审核计划还应包括：

●明确受审核方的代表；

●审核所使用的语言；

●审核报告的主题；

●后勤安排（交通、现场设施等）；

●保密事宜；

●审核后续活动。

●如果进行了远程审核审核活动，其明确的说明。

除上述事宜外，如适宜，审核计划还应识别审核中将使用的网络审核技术。网络支持的审核技术可包括：例如，电话会议、网络会议、基于网络的交互式通信和远程电子访问ISMS文件和（或）ISMS过程。

6.7.3.3 编制审核计划时，审核组和受审核方就审核时间的选择应能达成一致意见，且保证所选择的的审核时间能最有效地证实其整个ISMS范围。是当时可考虑季度、月份、日期和班次。

6.7.3.4 现场审核活动开始前，审核计划应当经审核委托方评审和接受，并提交受审核方。受审核方的任何异议应在审核组长、受审核方和审核委托方之间予以解决。任何经修改的审核计划应在继续审核前征得各方的同意。

6.8 初次认证

初次审核分两阶段实施：第一阶段和第二阶段。第一阶段审核和第二阶段审核应有一定时间的间隔。审核组长应根据一阶段审核的结果，向审核部报告建议二阶段的审核时间，以便受审核方有足够的时间针对一阶段审核发现的问题采取纠正措施。

第一阶段审核可以不制定正式的审核计划:第一阶段审核可以不安排正式的首末次会议(此时以非正式方式如初步沟通、审核总结进行)。

6.8.1 第一阶段

6.8.1.1 第一阶段的审核所需要的时间应考虑组织在业务活动中可能发生的信息安全风险情况、相应控制措施的复杂程度及文件的复杂程度，通常不超过总人天的三分之一。

6.8.1.2 文件审核

a) 文件审核应有专业审核员或技术专家的参与。由审核组长签名确认。

b) 文件审核时，依据ISO27001，以确认组织的文件中是否涵盖了标准的要求并满足标准的要求。

c) 就文件审核中所发现的描述与实际情况或申请范围不完全符合时，应作为文件审核问题给予描述，并要求客户给予书面的澄清。

d) 文件审核后应完成文件审核报告。文审中所发现的问题或需书面澄清的问题应记录在MFP0374《管理体系文审、一阶段审核结论及问题清单》中，在一个工作日内提交给客户，限期整改文件审核发现的不符合宜在第二阶段现场审核前完成；

e) 文审人员在关闭文审问题时，应在MFP0374《管理体系文审、一阶段审核结论及问题清单》中纠正措施引用文件一栏中注明针对文审问题所纠正的手册及程序文件的条款号，并签字确认，应保留符合性证据；

f) 文件审核报告应归入该客户的审核档案。

6.8.1.3第一阶段审核应在申请组织的现场进行，审核内容包括：

(1) 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。在此基础上确定如何实施第二阶段的策划；

(2) 评价申请组织的运作场所和现场的具体情况，并与申请组织的人员进行讨论，以确定第二阶段审核的准备情况；

(3) 审查申请组织理解和实施信息安全管理体系标准要求的情况；

(4) 审查申请组织是否系统而充分地识别与所提供的服务相关的法律法规和其他要求及其遵守情况；

(5)审查第二阶段审核所需资源的配置情况，并与申请组织商定第二阶段审核的细节；

(6)结合申请组织信息安全管理体系方针和目标，了解其审核准备状态，为策划第二阶段的审核提供重点；

(7)评价申请组织是否策划和实施了内部审核与管理评审，以及信息安全管理体系的实施程度能否证明其已为第二阶段审核做好准备。

6.8.1.4 ISMS初次认证审核的第一阶段审核时间宜合理分配，并予以记录。ICAS应在一阶段前或一阶段审核期间，对客户的文件化管理体系信息进行充分审核。ICAS应将第一阶段的结果形成书面报告并告知申请组织，包括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。在进行第二阶段之前，ICAS应审查第一阶段的审核报告，以便为第二阶段选择具备所需能力的审核组成员。如果第一阶段的审核组长具备能力且适宜时，宜由其来实施该二阶段审核。

6.8.2 第二阶段审核

审核组应在具备实施认证审核的条件下在申请组织的场所实施第二阶段审核。

如果第一阶段审核提出影响实施第二阶段审核的问题，这些问题应在第二阶段审核前得到解决。第二阶段审核的目的是通过在申请组织的现场进行系统、完整地审核，确认客户遵守自身的方针、目标和规程，评价申请组织的信息安全管理体系是否满足所有适用的认证依据的要求，并判断是否推荐认证注册。应重点关注申请组织是否充分识别了信息安全管理过程的重要性，并证实与申请组织的信息安全活动是相适应的，除此之外，审核组还应重点关注：

a） 最高管理层对信息安全方针和信息安全目标的领导和承诺；

b） 对与信息安全有关的风险的评估，以及在重复评估时可产生一致的、有效的和可比较的结果；基于风险评估和风险处置过程所确定的控制目标和控制；

c） 根据信息安全目标对其实施了评价的信息安全绩效和 ISMS 有效性；

d） 所确定的控制、适用性声明和风险评估与风险处置过程的结果，与信息安全方针和目标之间的一致性；

e） 控制的实现，考虑了外部环境、内部环境、相关的风险，以及组织为确定控制是否得以实现、有效且达到其所规定的信息安全目标而对信息安全过程和控制进行的监视、测量与分析；

f） 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、信息安全方针和信息安全目标。

6.8.2.1 首次会议

会议由审核组长主持，审核组成员、受审核方管理层、受审核的职能或过程负责人参加，参会所有人员（包括审核组成员）应在《签到表》（MFP0312）上签到由审核组长保存记录。审核组长负责召开首次会议，会议的主要目的是简要解释将如何进行审核活动，并让受审核方有提问的机会同时应包括下列要素。详细程度可与受审核方对审核过程的熟悉程序相一致：

- 双方介绍与会者；包括简要介绍其角色；
- 介绍审核性质、审核目的、审核依据；与客户确认认证范围，并向客户解释审核将根据确认的范围进行抽样；与客户确认审核范围内是否有法律所禁止的产品；
- 与客户确认审核场所，如果有多现场或临时场所，且被审核方在申请时未向机构申报，应请客户填写《多场所多现场、在建项目清单》（MFP0350），并报请审核部进行审核方案的复核和调整；
  与客户确认各现场/场所的真实性和合法性，特别要确认该场所是否确实属于被审核方，以避免被审核方借用他人场所获取认证；
- 与客户确认客户名称的合法性；
- 确认审核计划；
- 确认审核组和客户之间的沟通渠道；
- 与受审核方确认其他相关的安排，例如，末次会议的时间、地点、参加人员，审核组和受审核方管理层之间的临时会议以及任何新的变动；
- 简要介绍审核活动如何实施；
- 说明审核所用的抽样方法；
- 介绍审核程序；
- 说明现场审核结论是推荐性结论；说明严重不符合项、轻微不符合项和观察项的定义及处理方法，以及对现场审核的影响程度
- 宣布保密承诺和确认有关保密事宜；
- 宣布公正性声明；
- 确认审核所使用的语言（必要时）；
- 确认审核组所需的资源和设施（临时办公、通讯、交通工具、劳动保护）；
- 确认审核和工作的安全事项、应急和安全程序（存在时）；
- 介绍陪同人员的作用并安排落实（向导、见证、联络）；
- 关于审核过程发生争议时的处理程序；
- 是否有需要澄清的事项；

- 安排受审核方领导讲话；
- 将表单《专业交底记录》(MFP0348) 交技术专家填写（适用时）；
- 说明可能终止审核的条件。
- 确认以往评审或审核的发现的状态（适用时）；
- 确认在审核中将告知客户审核进程及任何关注点；

6.8.2.2 审核中的沟通

1）根据客户的审核范围及复杂程度，审核组长应安排必要的沟通渠道及沟通方式；

2）审核时间超过一天以上时，审核组长应每天组织审核组内部进行一次简短的会议，以便：

a) 交换信息；

b) 评定审核进展情况；

c) 必要时，重新分配审核组成员的工作。

3）视组织规模及其复杂程度，审核组长应定期向客户通报审核进展情况及相关情况。

4）审核组成员在审核中发现重大不符合时，应及时报告审核组长，并由组长与客户沟通。

5）审核组成员如发现超过范围之外的引起关注的问题时，应当指出并向审核组长报告，必要时，应通报客户。

6）当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事件、事故，例如安全风险等情况时，审核组长应与审核部取得联系,并同客户商量确定补救措施或终止审核。补救措施可以考虑以下方式：

a) 重新安排审核时间及审核计划；

b) 修改审核计划，对存在重大不符合项的相关区域另外安排时间跟踪审核；

c) 改变审核目的及审核范围。

7）当现场审核时,出现客户人数、名称、地址或/及审核范围变更，审核组长负责与ICAS审核部取得联系并填写《变更申请》（MFP0360），由客户方签字确认后传回给公司审核部进行评审。 审核部审核方案管理人员负责变更的评审，对于认证业务范围的变更或/及客户人数的变更应确定下述事宜后决定应采取的措施：

a) 认证业务范围的变更

- 评估审核组成员的业务能力；
- 评估认可的业务范围；
- 征求客户的意见。

b) 客户人数的变更

- 审核人天的变更
- 审核计划的调整
- 征求客户的意见

8）任何审核组成员如发现其所审部门实际没有分配给其要素活动，应随时通知审核组长，由审核组长进行调整以避免审核结束后遗漏要素，对审核计划的调整务必符合要求。

9）审核组长应召集审核组成员对审核过程中的发现在末次会议前进行讨论并综合评价，确定构成不符合项时，应经审核组长确认同意后，方可向受审核方提出，当审核员与审核组长就不符合项产生争议时，审核员现场应服从审核组长的安排。事后可将该争议提报ICAS认证技术委员会裁定。

10）现场审核发现人数严重失实导致审核无法按计划完成时，应首先填写《变更申请》（MFP0360），由客户签字确认，传回审核部以便审核部重新进行审核人天的确认，审核组长负责与客户协调补救措施。

11）当与客户就不符合项发生分歧时，审核组应首先虚心听取客户的解释，决不可武断或以自己以往的经验要求客户，应努力以适当的、富有建设性、专业的方式解决与客户之间的分歧；如客户的解释合理，应取消发生争议的不符合项。如争议无法解决，应向客户解释ICAS有关《申诉、投诉、争议程序》（ICASP06）对争议的处理方法。

12）若审核组内部或与受审核方之间发生无法处理或协调的异常/突发事件，审核组长应立即上报总经理。

6.8.2.3 信息的搜集和验证和记录

6.8.2.3.1 ICAS应要求申请组织证实其对信息安全管理过程的分析和组织运作实施了适当的控制措施，以便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；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、目标和指标相一致。用于风险评估的规程健全并得到正确实施。相关搜集的信息和证据包括：

a) 信息安全策略；
b) 信息安全组织；
c) 人力资源的安全；
d) 资产管理；
e) 访问控制；
f) 密码控制；
g) 物理和环境安全；
h) 操作安全；
i) 通讯安全；
j) 系统的获取、开发和维护；
k) 供应商关系；
l) 信息安全事故管理；
m) 业务连续性管理的信息安全方面；
n) 符合性。

6.8.2.3.2 审核组成员应在其承担的审核工作内，根据审核计划、用抽样的方式进行信息的收集，信息的来源可以是：

a) 与员工和其他人员的交谈与员工和其他人员的交谈,当非被审核人员(如顾问)代替被审核人员不断回答问题时，相关审核组员应给予适当的制止；
b) 对活动、周围工作环境和条件的观察；
c) 文件，如：方针、目标、计划、程序、标准、指导书、规范、图样、合同、营业执照、许可证、产品强制性检验报告、订单等；
d) 数据的汇总、分析、和业绩指标；
e) 客户抽样方案的信息、抽样和测量过程的信息；
f) 其他方面的报告，如：客户抱怨、反馈等；
g) 计算机数据库和网站；
h) 记录；

6.8.2.3.3 审核记录

所有记录包括从申请、合同评审、任务书、文件审核报告、审核计划等所有与审核相关的记录和文件，审

核部均应将原件以电子档案或书面形式予以保留在公司，审核组或任何其它人员不可将原件带离公司。
采用计算机技术进行远程审核时，要详细记录以下信息：

a) 采用何种计算机辅助技术进行的远程审核；
b) 远程审核项目、远程地址；
c) 对方参加远程审核参加人员；
d) 调用的文件和记录名称；
e) 通过视频或电话等审核的人员名称和职务；
f) 符合/或不符合的关键证据。

记录中应避免涂改液或其它方式覆盖原始记录，必须纠正时，可以以划改的方式修正，并由原记录人签字。

审核记录使用的文字为中文，特殊情况下，经批准可使用外文。审核记录应体现审核证据， 证据可以是人证、物证、质量记录等。如：具有可追溯的抽样（产品名称和批号等），面谈的人员姓名和见证人等。

应当记录具体的不符合和支持的审核证据；符合要求和支持的审核证据的记录应简明扼要，具有唯一可追溯性。

6.8.2.3.4 审核组长在审核过程中应随时检查审核组成员是否按照ICAS程序要求使用文件。

6.8.2.3.5 实习审核员指导对实习审核员的记录负责。

6.8.2.4 形成审核发现

6.8.2.4.1 审核组成员利用依据审核准则对审核记录的完整性进行确认,以确保审核充分性和完整性，并评价审核证据，形成审核发现，记录符合与不符合的审核发现。

6.8.2.4.2 审核组成员应分别将所发现的不符合项记录于《不符合项报告》（MFP0314）中，并对不符合项分级。关于不符合的审核发现应对照具体要求予以记录，包含对不符合的清晰陈述（详细标识不符合所基于的客观证据）

6.8.2.5 审核组应就不符合项与客户沟通，确认审核证据的准确性，并使客户理解并接受。

a) 针对审核目的,评审审核发现及审核过程中所发现的其它信息；
b) 考虑审核过程中不确定的因素,对审核结论达成一致；
c) 根据管理评审、内部评审的适宜性及本次审核发现，及确保审核的连续性，对下次监督审核的需关注的部门和要素、过程提出建议；
d) 确定任何必要的跟踪活动；
e) 确认审核方案的适宜性，或识别任何需要的修改（例如范围、审核时间或日期、监督能力）

6.8.2.6 审核结论

审核组通过内部讨论及与客户方的沟通，形成审核结论，审核结论应包含以下内容：

a) 管理体系与审核准则的符合程度；
b) 管理体系的实施、保持和改进的有效程度；
c) 内审、管理评审的适宜性、充分性、有效性和改进方面的能力；
d) 有关ISMS管理体系实施中最重要的正面和负面的总结；
e) 审核组的结论。
f) 必要时，提出建议。

审核结论以几种形式得出：

b) 推荐注册/ 维持证书：当审核发现的不符合项都已采取纠正措施并经验证后，初次认证和再认证时，推

荐注册，监审时，推荐保持注册；

c) 推荐证书暂停：监督审核时，轻微不符合未能在1个月内关闭，严重不符合项未能在3个月内关闭，则暂停证书；

d) 推荐撤销证书，证书暂停后的3个月内仍未对重大不符合项采取有效的纠正措施。

e) 推荐变更注册：

6.8.2.7 末次会议

审核组全体人员、受审核方有关领导及人员参加，由审核组长主持，并以受审核方能够理解和认同的方式提出审核发现和结论，审核组长可使用《结束会议查检表》（MFP0316）以免遗漏有关的事项。必要时，可以解释审核发现和对审核标准的理解。

末次会议主要内容：

- 请与会者填写《签到表》(MFP0312）：
- 审核情况报告：主要是确认本次审核的范围、确认不符合报告、管理体系的综合评价、确认审核结论、审核报告的分发等；
- 重申抽样方法；
- 审核组审核结论的说明以及客户针对不符合项制定纠正措施、实施及自行验证关闭、审核组长验证关闭、ICAS 注册部评定、ICAS 总经理批准、发证（初审）/资格保持（监督）过程的说明；
- 解释不符合项及纠正措施的要求（如进行再认证应规定在认证终止前实施纠正与纠正措施的时限，从而使新的认证周期在上一个认证周期结束前已经生效）；
- 监督审核要求；
- 认证证书和标志的使用要求；
- 重申公正性声明、保密承诺；
- 受审核方信息沟通的要求；
- ICAS 有关服务的说明；
- 需要澄清的问题；
- 说明投诉处理过程和申诉过程

审核组应明确要求申请认证客户在规定的期限内分析原因，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。

6.8.3 现场审核结束前审核信息及审核文件的收集

审核组长负责以上审核信息的收集及并根据《ICAS审核记录查检表》（MFP0309）对以下审核文件的收集及确认：

- 初次认证审核，请受审核方签字确认“客户信息确认表”；
- 审核计划和审核经历表（必要时）请受审核方盖章；
- 技术专家完成的《专业交底记录》(MFP0348)，并请所有审核组成员在受训栏中签字（适用时）；
- 签字后的《技术专家须知》（MFP0344）（适用时）；
- 签到表；
- 签字后的公正性声明；
- 审核记录；
- 审核报告；

- 客户签字后的合同；
- 其它所收集的必要信息。

6.8.4 不符合项的原因分析、处理及验证的方式

机构指定人员负责对审核档案及审核组所开出不符合项的合理性于审核员沟通并进行确认。

审核组长或审核组长指定的开出不符合项的审核员或机构指定人员负责跟踪不符合项的关闭，确保不符合项在规定的时间内的有效整改(机构指定人员可以通过审查客户提供的文件，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，不符合的解决提供支持的证据应予以记录，对不符合的解决进行审查和验证的证据应予以记录，有必要时请审核员确认。应将审查和验证的结果告知客户)。

不符合的分类：严重不符合项、轻微不符合项、观察项

严重不符合项的验证方式：

受审核方应在现场审核后的2周内提交ICAS整改计划，并在3个月内提交ICAS有关的整改措施实施有效性的证据，由要求亲自进行书面验证的提出不符合项的审核员或审核组长或由机构指定人员对其首先进行书面验证，并需机构在必要时指定审核员于现场对纠正措施的有效性进行验证。由机构指定人员对其首先进行书面验证，并需机构在必要时指定审核员于现场对纠正措施的有效性进行验证。三个月后未提交纠正措施及实施效果的证明材料，已认证客户作撤销证书处理，初次认证客户作不发证决定。

轻微不符合项的验证方式：

初次认证和再认证时，受审核方应在30天内提交ICAS纠正措施及实施效果的证明材料，再认证不符合项实施纠正和纠正措施的时限应在认证证书有效期终止前，由机构指定人员完成不符合项关闭的书面确认，并在必要时指定审核员于现场对纠正措施的有效性进行现场确认。就无法在短期内完成的纠正措施，由机构指定人员与审核员沟通后决定，其实施的有效性是否可在下次年度审核时确认。凡30天内未提交纠正措施及实施效果的证明材料，已认证客户作暂停证书处理，三个月后仍未提交纠正措施及实施效果的证明材料，已认证客户作撤销证书处理，初次认证客户作不发证决定。监督审核时，受审核方应在30天内提交纠正措施计划，其有效性可在下次监督审核/复评时现场验证。

审核组长或其指定的人员获悉已收到受审核方的整改资料后，审核组长或其委托的人员应在 2 个工作日内对纠正措施实施的有效性和符合性进行确认关闭。纠正措施不满足要求时应于当天立即联系客户向客户说明要求，并跟踪直至关闭为止。审核组长应采取适宜的方法对关闭的不符项确认。

6.8.5 发生以下情况时，审核组应终止审核，并通过填写《终止审核流转单》方式，及时向ICAS报告：

（1）申请组织对审核活动不予配合，审核活动无法进行。

（2）申请组织的管理体系有重大缺陷，不符合GB/T 24405.1-2009标准的要求。

（3）发现申请组织存在重大质量安全问题或有其他严重违法违规行为。

（4）其他导致审核程序无法完成的情况。

6.8.6 审核报告

审核结案时，审核组长负责提交审核报告，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。报告内容包括或引用以下内容：

a) 标识出ICAS；
b) 申请认证客户及其管理者代表的名称/名称和地址；
c) 审核类型；
d) 审核准则；

e) 审核目的；
f) 审核日期
g) 标识出审核组长、审核组成员及其个人注册信息；
h) 如已识别出任何未解决的问题；
i) （现场或非现场）审核活动的实施地点和日期；
j) 受审核的所有场所的名称和地址及管理者代表；如果客户的活动都不在物理场所，是远程进行的，应包含“组织的所有活动都是远程进行的”说明。
k) 是否采用远程审核方式；如果采用远程审核，其审核方法的程度及其在实现审核目标方面的有效性的说明；
l) 已审核的认证范围或涉及范围，包括依据的适用的标准和（或）其他规范性文件包括版次和（或）修订号；；
m) 审核的说明，其中包括文件评审摘要；
n) 对客户信息安全风险分析进行认证审核的说明；
o) 与审核计划的偏离；
p) 所采用的主要审核路线和所使用的审核方法；
q) 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）；
r) 对客户的ISMS符合认证要求的评价意见和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；
s) 关于 ISMS 要求和信息安全控制的实现与有效性的、最重要的观察（正面的和负面的）的摘要；
t) 与审核要求一致的审核证据、审核发现和审核结论，
u) 解释与末次会议上提供给供方的信息的差异
v) 已识别出的任何未解决的问题；
w) 审核组关于客户的ISMS是否获得认证的建议，以及支持该建议的信息；
x) 内部审核的可信任程度；
y) 有关ISMS的实施中最重要的正面和负面的观察总结;监督及复评时应与以往对顾客评审结果作有用的比较；
z) 审核组的结论；

根据审核的实际特点，完成的问卷、检查清单、观察结果、日志或审核员审核记录都可以构成完整的审核报告的一部分。当这种情况发生是，这些资料应和审核报告一起，由审核组长整体提交注册部评审。

6.9 认证决定

6.9.1 原则

6.9.1.1 参加审核的人员不能再作为认证决定人员实施认证决定。

6.9.1.2 认证决定基于审核报告中审核组对客户ISMS是否通过认证的建议；而且应该以认证过程中收集的信息和其他相关信息为基础，以充分的证据证实申请组织建立信息安全管理体系的管理评审和内部审核的方案已经得到有效实施并且将得到保持，才可决定申请组织通过认证。通常情况下，对认证决定人员不宜推翻审核组的负面建议。如果发生这种情况，ICAS应记录其做出推翻建议的决定的依据，并说明其合理性。

6.9.2 决定

6.9.2.1 对于通过认证的申请组织，向其颁发信息安全管理体系认证证书。ISMS认证证书宜从客户的业务、组织

结构、位置和技术特点等方面清晰地界定认证所覆盖的ISMS范围。如果由于客户的信息安全的原因不能在认证证书上明示上述全部与客户ISMS范围相关的信息时，通过在认证证书上引用客户的适用性声明的方式是一种可以采取的间接方式。

6.9.2.2 对于未通过认证的申请组织，应以书面的形式明示其不能通过认证的原因。

6.9.2.3 认证决定的流程和管理规定，见《认证决定程序》ICASP10。

6.10 监督活动

监督审核程序，应与CNAS CC17中有关客户ISMS的认证审核的要求和指南保持一致。

6.10.1 监督目的

监督的目的是验证已被认证的ISMS得到持续实施、考虑由客户运作变化所引起的管理体系变化的影响并确认与认证要求的持续符合。

6.10.2 监督频次

ICAS应在满足认可要求的基础上，根据获证组织信息安全管理体系覆盖的业务活动的特点以及所承担的风险，合理设计和确定监督审核的时间间隔和频次。当获证组织信息安全管理体系发生重大变更，或发生重大问题、服务质量事故、客户投诉等情况时，ICAS视情况可增加监督的频次。

监督审核的最长时间间隔不超过12个月。由于获证组织业务运作的时间(季节)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。

6.10.3 监督审核方案

审核方案策划人员收集之前审核的信息，以保证能够针对与风险相关的信息安全问题及其对客户的影响来调整监督方案，并说明监督方案的合理性。

监督审核的方案应包括，但不限于以下内容：

a） 管理体系的保持要素，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 和认证所需的其他文件的要求，与来自外部各方沟通；

6.10.4 监督审核内容

每一次监督应至少审查：

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） 所确定的控制的变更，及其引起的适用性声明的变更；

d） 控制的实现和有效性（根据审核方案来审查）；

e） 客户提交给 ICAS 的申诉和投诉记录，并且在发现任何不符合或不满足认证要求时，还应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。

6.10.5 监督审核报告

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。此外，监督审核报告应至少完全覆盖 6.8.6 的要求。

6.10.6 监督审核结果评价

对于监督审核合格的获证组织，ICAS应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、撤销或注销相应的认证资格。

监督审核可能有以下结果，有关条件参见《批准、保持、扩大、缩小、暂停以及撤销程序》（ICASP11）。

- 证书的保持；
- 证书范围扩大或缩小；
- 证书暂停或撤销。
  - 管理体系覆盖的活动涉及法律法规规定的，是否持续符合相关规定；是否发生过重大信息安全事故，如发生是如何处理的；对相关方投诉所采取的措施；
  - 总目标及各层级目标是否实现。目标没有实现的，获证组织在内部管理评审时是否及时调查并采取了改进措施。
  - 证书和标志使用或对认证资格的引用是否符合国家及 ICAS 相关的规定等。

6.11 再认证

再认证审核程序，应与本程序中有关客户ISMS的初次认证审核的要求保持一致。允许采取纠正措施的时间，应与不符合的严重程度和相关的信息安全风险相一致。

6.11.1 再认证审核的策划

6.11.1.1 ICAS应策划和实施再认证审核，以评价获证组织是否持续满足信息安全管理体系标准和相关的认证规范性文件的所有要求。

审核部负责采取适宜和有效的方法确保再认证每三年进行一次，应在认证证书有效期终止前三个月内进行。

6.11.1.2 审核部应在再认证前至少三个月，通知市场部。

6.11.1.3 市场部接到通知后，通知客户。并为下一个认证周期报价格。

6.11.1.4 再认证审核应考虑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。

6.11.1.5 当获证组织、获证组织的信息安全管理体系或其运作环境有重大变更时，ICAS应有程序确保对再认证审核活动可能需要进行的第一阶段审核实施管理。当管理体系及获证组织的内部和外部环境无重大变更时，再认证审核可省略第一阶段审核，但审核时间应不少于初审计算人日数的70％。

6.11.2 再认证审核的要求和方法与6.8.2第二阶段审核相同。

6.11.3 ICAS应根据再认证审核报告的结果，以及认证周期内的体系评价结果和认证使用方的投诉，作出是否更新认证的决定。

6.12 特殊审核

6.12.1 扩大认证范围

对于已授予的认证，ICAS应对获证组织扩大认证范围的申请进行评审，策划并实施必要的审核活动，并在该审核活动中验证获证组织的信息安全管理体系的适宜性和有效性，以作出是否可予扩大的决定。扩大认证范围的审核活动可单独进行，也可和对获证组织的监督审核或再认证一起进行。

6.12.2 ICAS为调查投诉、对变更做出回应或对被暂停认证资格的获证组织进行追踪，可能需要在提前较短时间通知获证组织后对其进行审核。此时：

(1)应向获证组织说明并使其提前了解将在何种条件下进行此类审核；

(2)由于获证组织缺乏对审核组成员的任命表示反对的机会，ICAS应在指派审核组时给予更多的关注。

6.13 暂停、撤销认证或缩小认证范围

6.13.1 ICAS编制有《认证授予、拒绝、保持、变更、暂停、恢复、撤销程序》，对暂停、撤销认证或缩小信息安全管理体系认证范围的流程和所采取的措施作出规定。

6.13.2 发生以下情况(但不限于)时，ICAS应暂停获证组织的信息安全管理体系认证资格：

(1)获证组织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；

(2)获证组织不允许按要求的频次实施监督或再认证审核；

(3)获证组织不接受或不配合认证认可监督管理部门的监督管理；

(4)获证组织主动请求暂停。

6.13.3 认证资格暂停期最长不超过6个月。

6.13.4 在暂停认证期间，获证组织的信息安全管理体系认证证书暂时无效。ICAS应做出具有强制实施力的安排，以确保暂停认证期间避免获证组织继续宣传信息安全管理体系认证资格。ICAS应使认证证书的暂停信息可公开获取，并采取其认为适当的任何其他措施。

6.13.5 如果获证组织未能在ICAS规定的时限内解决造成暂停认证的问题，ICAS应撤销其信息安全管理体系认证或缩小其相应的认证范围。

6.13.6 如果获证组织在认证范围的某些部分持续地或严重地不满足认证要求，ICAS应缩小其信息安全管理体系认证范围，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。

6.13.7 ICAS应与获证组织就撤销信息安全管理体系认证时的要求做出具有强制实施力的安排，以确保获证组织接到撤销认证的通知时，立即停止使用任何引用信息安全管理体系认证资格的广告材料。

6.13.8 在任何组织提出请求时，ICAS应正确说明获证组织的信息安全管理体系认证被暂停、撤销或缩小的情况。

7 审核档案及客户记录

7.1 审核组成员必须将审核形成记录，在审核结束时交审核组长。 审核组长负责检查所有审核记录的完整性，妥善保管于审核档案中，并在审核结束后、不符合项整改措施验证关闭后的2个工作日内提交至ICAS注册部。

7.2 获证客户记录应包括：

1) 申请资料及初次认证、监督和再认证的审核报告；
2) 认证协议；
3) 审核方案，其中包括抽样方法的理由、 确定审核时间的理由；
4) 纠正与纠正措施的验证；
5) 投诉和申诉及任何后续纠正或纠正措施的记录；
6) 技术委员会的审议和决定（适用时）；
7) 认证决定的文件；
8) 认证文件，包括与产品（包括服务）、过程相关的认证范围，管理绩效统计情况，适用时，包括每个场所相应的认证范围；
9) 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。

认证协议由市场部负责保管，认证可信度所需的相关记录由技术资源管理部负责保管，其余的客户记录由注册部负责保管并扫描成电子档放置ICAS内部服务器上。

7.4 档案管理人员根据程序《记录控制程序》（ICASP05）对记录进行控制。

8. 其他要求

8.1 ICAS在信息安全管理体系认证领域内，为避免被认为是做咨询或具有潜在的利益冲突，应按下列要求从事相关工作：

- 安排培训课程并作为讲师参与讲授。如果这些课程涉及信息安全管理、相关的管理体系或审核，ICAS仅限于提供可公开获取的通用信息和建议

- 根据请求，提供或发布ICAS对认证审核标准要求的解释性信息；
- 仅以确定认证审核是否就绪为目的的审核前活动，但是这些活动不应导致提供违反本条款的建议和意见；
- 根据没有包含在认可范围内的标准或法规，实施第二方或第三方审核；
- 在认证审核和监督访问过程中的增值活动，例如，在审核过程中，当改进机会明显时，识别改进机会但不推荐具体的解决方案。
- 不为寻求认证的客户的ISMS提供内部信息安全评审；ICAS及ICAS人员不为其提供ISMS内部审核。

8.2 认证协议

ICAS与客户方签订的ISMS协议中，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ICAS以及客户及其有关人员的责任与义务。

8.3 保密要求

8.3.1 在认证审核前，ICAS应要求客户识别并向认证机构告知其ISMS范围内的哪些信息资产不允许认证机构接触，或者ICAS在接触相关信息资产时应满足哪些要求，包括法律要求、相关方的要求和客户自身的要求。ICAS应满足所有这些要求，否则不应在认证活动中接触客户的相关信息资产。

如果ICAS因为未获得客户的允许或无法满足适用的要求而不能接触相关信息资产，那么认证机构应对审核和认证所受到的影响进行评估并采取相应的措施（例如终止审核、缩小审核和认证的范围等）。

如果客户事先没有禁止认证机构接触某一信息资产，或未告知ICAS应满足的要求，但ICAS在认证过程中发现自己并不具备接触该信息资产的资格和条件，应立即向客户提出。

8.3.2 ICAS应与其ISMS认证相关人员签订在法律上具有保密协议，以确保认证相关人员对审核和认证过程中接触到的客户的保密或敏感信息予以保密。ICAS宜要求直接接触客户信息的认证人员（例如审核组成员）按照客户的保密要求与客户签署保密协议，或向客户做出保密承诺。

8.3.3 ICAS不定期对ISMS认证人员进行保密意识教育，并进行保密方面的法律法规、标准、规章制度、知识技能的培训。

8.3.4 审核组成员不宜在审核过程中以任何方式记录受审核客户的保密或敏感信息。审核组在离开受审核客户前，宜请受审核客户检查和确认审核组携带的文件、资料和设备中未夹带受审核客户的任何保密或敏感信息。

8.3.5在认证审核之前，ICAS应要求客户报告是否存在因包含保密性或敏感性信息而导致不能提供给审核组核查的ISMS相关信息（例如ISMS记录或关于控制的设计与有效性的信息）。ICAS应确定ISMS是否能在缺少这些信息的情况下得到充分审核。当结论是若不核查已识别的保密性或敏感性信息就不能对ISMS进行充分地审核，那么ICAS将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。

8.3.6 ICAS编制《保密管理程序》，为包含客户保密或敏感信息的文件、资料和其他物品的制作、收发、传递、使用、复制、摘抄、保存和销毁制定管理措施。

8.4 与客户间的信息交换

ICAS有权要求客户即时报告其业务、组织结构、位置和技术特点等方面可能导致其 ISMS 范围和边界变化的情况，以及与其 ISMS 相关的法律法规的变化情况。

8.5 认证文件

8.5.1 认证文件应由总经理签署。认证文件应包括适用性声明的版本。如果适用性声明的变更没有改变认证范围中控制的覆盖范围，则不要求更新认证证书。

8.5.2 认证文件可以引用那些作为组织适用性声明中控制集来源的国家标准和国际标准，前提是：1）组织已将其所有必要的控制与参考控制源中的控制进行比较，已确定其没有根据ISO/IEC 27001:2022,6.1.3 c)无意中遗漏

任何此类参考控制；2）认证文件中应说明：适用性声明中的控制集仅用于提及在ISMS中选择和删减控制的相关性，而不是用于合格评定。

8.5.3如果组织在认证范围内没有在规定的地理地点进行任何活动，则认证文件应声明组织的所有活动都是远程进行的。

9 纠正措施

在日常运作中发现的不符合，由管理者代表责成相关部门负责人在规定的期限内进行纠正，并由管理者代表负责验证纠正措施的有效性。

10 相关程序

《认证授予、拒绝、保持、变更、暂停、恢复、撤销程序》（ICASP11）
《记录控制程序》（ICASP05）
《申诉、投诉、争议处理程序》（ICASP06）

11 相关记录

a) 执行本文件应产生下列记录：
b) 申请表（MFP1488）
c) 报价单（MFP0306）
d) 认证合同（MAP0312）
e) 合同评审表（MFP0363）
f) 审核组派遣通知书（MFP0308）
g) 审核计划（MFP0311）
h) 签到表（MFP0312）
i) 首次会议查检表（MFP0313）
j) 不符合项报告（MFP0314）
k) 管理体系一阶段审核检查表及报告（MFP0373）
l) 信息安全管理体系审核报告（MFP0315）
m) 结束会议查检表（MFP0316）
n) 客户信息确认表（MFP0318）
o) 审核查检表（MFP0309）
p) 《ISMS认证审核人天表及收费标准》