版本/版次	修订内容	修订日期	修订人
B/2	合理化修订	2024.11.20	田斌斌

文件批准发布

批准		日期	
审核		日期	
制订	田斌斌	日期	2024.11.20

1、 引言

1.1 信息安全管理体系（ISMS）认证是独立于供求双方并具有认证审核资格的机构可颁发信息安全管理体系认证证书，证明企业的信息安全管理体系符合 ISO/IEC 27001:2022《信息安全管理体系要求》标准要求的活动。

（广汇联合（北京）认证服务有限公司,以下简称 GH）

1.2 向 GH 申请 ISMS 认证的企业必须具备以下条件：

1.2.1 中国企业持有工商行政管理部门颁发的《企业法人营业执照》，或等效的文件；外国企业持有有关机构的登记注册证明。

1.2.2 企业已按 ISO/IEC 27001:2022《信息安全管理体系要求》标准建立了 ISMS 体系并运行 3 个月以上。

1.2.3 认真贯彻执行我国有关信息安全管理和产品的法律、法规和标准。

1.2.4 特殊行业许可证（如生产许可证、卫生许可证、安全生产许可证、特种行业资质证、特种设备安检报告、行业入网证、强制性产品认证证书等）

1.2.5 过去一年中未发生过重大信息安全事故。

1.2.6 企业已经进行了内部审核和管理评审。

1.2.7 没有被执法监管部门责令停业整顿，未列入国家信用信息严重失信主体相关名录。

2、 范围

本程序适用于广汇联合（北京）认证服务有限公司（以下简称 GH）有效认证业务范围内开展信息安全体系认证工作。

本程序适用于在 GH 审核授权下开展 ISMS 的认证审核活动；不得超越 GH 审核授权，开展其他认证品牌、业务范围的认证业务的关键活动。

3、 职责

认证审核部是本文件的归口管理部门，其他部门协助。

4.1 认证的申请

4.1.1 市场营销部应主动向申请方提供的有关信息：

✧ GH 基本资质；

✧ 《认证申请表》；

✧ 《认证合同书》；

✧ 其他有关说明。

申请方可通过电话、信函或面谈向 GH 询问了解 ISMS 认证的程序、认证收费及有关情况。

4.1.1.1 申请方/受审核方应填写《认证申请书》及《认证合同书》。只有当 GH 收到以下文件才能决定是否进行受理评审：

a)说明申请人的简况，如组织的特征、名称、地址、法律地位、有关的人力和技术资源；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所处的关系，包含保密性或敏感性信息而不能提供给审核组核查的任何文件或记录；

b)产品生产工艺流程，产品信息安全安全方面的法律法规名称及标准代码、名称。

✧ 有关信息安全管理体系及其覆盖的活动的一般信息，包括申请认证的范围，组织的名称、 物理场所的地址、人数、过程和运作的重要方面以及任何相关的法律义务；

✧ 对拟认证体系和每个体系所适用的标准或其他规范性文件的说明，申请组织采用的所有影响符合性的外包过程的信息；申请组织寻求认证的标准或其他要求；

✧ 是否存在不能提供的包含保密性或敏感性信息的记录及其对认证审核有效性的影响。

✧ 接受与管理体系有关的咨询的情况。

c) 申请方/受审核方应做出以下承诺：

✧ 遵守认证的有关规定

✧ 为进行认证审核做出全部必要的安排，包括为进行审核、监督、复评和解决投诉，而准备待审查文件，开放所有区域，提供记录（包括内审报告）和准备相应的人员：

✧ 应就获准认证的范围做宣传。

✧ 在宣传认证结果时不得损害我司的声誉，不得做使我司认为误导的或未授权声明。

✧ 当认证被暂停或撤销后，（不论如何解决的）应立即停止涉及认证内容的广告、宣传，并按我司要求交回所有的认证文件。

✧ 认证只能用来证明其 ISMS 符合了特定标准或其他规范性文件，不能用认证来暗示其产品或服务得到了我司的批准。

✧ 确保不采取误导的方式使用认证文件，标志和报告或其中任何部分。

✧ 在传播媒体中（例如文件、小册子或广告）对认证引用，应符合我司的要求。

d) 当申请的认证范围涉及某一特定认证项目时，应向申请人做出必要的解释。

e) 当申请方提出要求时，我司应向其提供更详细的信息。

4.1.2 申请前期资料

组织应在正式合同签订前填写认证申请书及认证合同书初案，并按 4.1.1 b）提供审核所需的必要信息和下列文件。

✧ 信息安全手册、适用性声明和要求时的相关文件。

✧ 内审、管理评审报告。

GH 应为从申请文件到现场审核前收集的信息保密，如果 GH 接受了认证范围之外的业务范围的申请，应按照扩大、缩小认证范围实施。

4.2 审核准备、申请评审

4.2.1 申请评审（合同评审）

GH 申请评审人员应对认证的申请进行评审，评审内容如下：

✧ 申请认证的领域；

✧ 组织是否已建立了文件化的 ISMS，体系是否已有效运行三个月以上，并进行了至少一次完整的内审及管理评审；

✧ 组织是否基本具备申请认证的条件，未发生过重大质量事故，未被执法监管部门责令停业整顿，未列入国家信用信息严重失信主体相关名录；

✧ 是否遵守公正性、转机构合规性等商务规则；

✧ 组织申请的认证范围是在 GH 的认证范围内；

✧ 受审核方使用的语言及口头和书面交流所用的语言；

✧ 支持远程审核的条件是否能有效保证远程审核实施；

✧ 政府部门信息技术外包服务机构是否经过安全审查程序审核（工信部联协【2010】394号通知要求）

✧ GH 应组织有专业能力的人员在正式签订合同进行前期评审，评审的内容包括：

a)界定申请人拟接受审核的现场活动和过程的性质、风险/复杂程度；

b)识别个人技术能力要求相一致的方式，识别审核组要求具备的能力；

c)评价可能影响信息安全体系的任何法定的许可或注册要求；

d)确认是否具备所需能力；

e)根据认证范围覆盖的人数及其它相关因素确定项目需要投入的审核时间；

信息安全管理体系认证覆盖人数应包括如下几类人员：

✧ 信息安全管理体系管理层；

✧ 信息技术人员；

✧ 与信息安全/管理有关的部门主管人员；

✧ 涉及信息安全管理设备的责任人及主要使用人（主要信息涉密人员）；

✧ 其它与信息安全管理体系的建立、实施、维护与改进的主要人员。

f)对于多场所，尽可能识别出各现场的差异、确定抽样充分程度；

g)临时场所，但不满足多场所的定义，也宜进行抽样审核，但需考虑在路途中所花费的时间；

h)是否存在不能提供的包含保密性或敏感性信息的记录及其对认证审核有效性的影响；

i)关于对认证机构的资质、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最新法律法规要求。

评审的结果应记录在《认证申请受理评审表》或《合同评审表中》中，以确保：

a） 申请组织及其管理体系的信息充分，可以进行审核；

b） 认证的各项要求已明确形成文件并得到申请方理解；

c） 本公司和申请方在理解上的差异已得到解决；

d） 拟认证组织申请认证领域内审核范围及其风险得到充分识别；

e）本公司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、保密控制……等；

f）支持远程审核的基础设施等条件应清晰明确，可以据此判断能否实施远程审核；

g）企业如原来已经通过认证的，需办理证书转换的，应查核企业认证证书是否仍在有效期内，应办理转机构备案手续，失效、暂停或撤销证书不得转换；若申请因业务需要接受多重认证，按初次认证申请的，不受前述限制；

i）政府部门信息技术外包服务机构已经过安全审查程序审核（工信部联协【2010】394号通知要求）；

j）对认证机构的资质、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最新法律法规要求。

根据上述评审，GH 应确定审核组及进行认证决定需要具备的能力，是否具备对该客户实施认证活动的资格和条件。在评审后，应确定是否接受或拒绝组织的认证申请。当基于评审结果拒绝认证申请时，应记录拒绝申请的原因并告知企业。

4.2.2　认证范围确定

4.2.2.1 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。

4.2.2.2 认证范围应涉及受审核方在特定场所和具体活动的管理控制下：

a）应在资质允许的范围内，确定信息安全管理体系覆盖的产品范围；

b）应涵盖过程和覆盖的场所；

c）必须为已生产/服务、并且审核得到的产品/服务；

d)应考虑法律要求范围（注册要求，公告要求，经营者的证书、许可证、行业规定的资质等）。

4.2.2.3 应明确界定认证所涉及的活动场所：常设场所、临时场所、多场所组织、中心职能、虚拟场所。

注：常设场所、临时场所、多场所组织、中心职能、虚拟场所详见如下定义：

a）常设场所：组织持续进行工作或提供服务的场所（有形或虚拟）

b）临时场所：组织为在有限时期内进行特定工作或提供服务而设立的场所（有形或虚拟），该场所不准备作为常设场所。

注：客户组织为完成特定的服务所处的地点属于临时服务点，属于客户组织的服务对象设立的组织场所，而不是客户组织设立的临时场所。

c）多场所组织：某单一管理体系覆盖的一个组织，其构成包括经识别的中心职能以及多个场所，中心职能（并不必须是组织的总部）对某些过程、活动进行策划和控制，在多个场所（常设的、临时的或虚拟的）中这些过程、活动得到全部或部分实施。

说明：证书可以包括多场所。但该范围覆盖的每一场所要满足以下之一：

✧ 已全部经过审核；

✧ 或按抽样原则进行了抽样审核，抽样原则详见审核方案策划。

d）中心职能：对管理体系负责并对管理体系集中控制的职能。

e）虚拟场所：指组织完成工作或提供服务所用到的，允许处理不同物理地点的人员执行过程的在线环境。

注 1：当某过程必须在某一有形环境实现时不能将其考虑为虚拟场所，如：仓储、物理检测试实验、安装或维修有形产品等。

注 2：这类虚拟场所的一个例子是，一个设计开发组织的所有员工在远程位置开展工作，在云环境中工作。

注 3：一个虚拟场所（如：一个组织的内部网络）被当作一个独立场所来计算审核时间。

注 4：更进一步信息见 CNAS-CC14(IAF MD4)《信息和通信技术（ICT）在审核中应用》。

f）使用远程审核方式进行审核时，应给审核员充分的时间来进行所有与审核或复评有关的活动，该时间的分配宜根据组织的规模，场所的数量（包括临时场所）实施 ISMS 的各种不同的组成部分时所使用的技术（如文件和/或过程控制，纠正/预防措施的控制等），已经证实的 ISMS 的绩效，以及认证用的标准等因素。

体系覆盖范围（产品、活动、过程和场所）最终在第一、二阶段审核时予以确认。

4.2.3 申请评审结果为可以受理的认证项目，经由市场营销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。

4.2.4 认证合同

4.2.4.1 本公司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。此外，对于公司可能的后续发展，如若有分布于各地分公司、办事处或客户有多个场所等情形，则全部由总部与所有场所之间签订在法律上具有强制实施力的书面合同。

4.2.4.2 认证合同应至少包含如下内容：

（1）申请组织获得认证后持续有效运行管理体系的承诺。

（2）申请组织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。

（3）申请组织承诺获得认证后发生以下情况时，应及时向认证机构通报：

① 客户及相关方有重大投诉。

② 产品或服务被监管部门认定不合格。

③ 发生信息安全事故。

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；取得的行政许可资格、强制性认证或其他资质证书变更；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；管理体系覆盖的活动范围变更；管理体系或重要过程的重大变更；技术特点的变更等。

⑤出现影响管理体系运行的其他重要情况。

（4）申请组织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或服务通过认证。

（5）拟认证的管理体系覆盖的生产或服务的活动范围。

（6）在认证审核实施过程及认证证书有效期内，认证机构和申请组织各自应当承担的责任、权利和义务。

（7）认证服务的费用、付费方式及违约条款。

4.2.4.3 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。

4.3 审核方案策划

4.3.1 实施内容

技术研发部负责按照《审核方案策划程序要求》，认证审核部、市场营销部协助实施审核方案的策划，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》。

信息安全管理体系的审核准则包括：

1）ISO 27001:2022；

2）受审核方信息安全管理体系文件；

3）适用于受审核方的信息安全管理相关的法律法规及其他要求。

ISMS 审核不应预先假定 ISMS 实施的特殊方式或文件和记录的特殊格式，应将重点放在确定客户的 ISMS 满足 ISO/IEC 27001 的要求和客户的策略与目标。

广汇检测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必要的安排。在认证审核的第一阶段，客户应至少提供以下信息：

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。

如果一个 ISMS 没有至少实施过一次覆盖认证范围的管理评审和内部审核，不应对该 ISMS 实施认证。

4.3.2 基本要求

4.3.2.1 初次认证审核方式

信息安全管理体系的初次认证审核应分两个阶段实施：第一阶段和第二阶段。审核组代表 GH 对申请组织实施文件审查和现场审核，相关的技术专家可作为顾问参加 GH 派出的审核组，技术专家可以不是审核员。

第一阶段审核应到客户现场实施审核。

4.3.2.2 确定审核人日数应按照《管理体系审核时间管理规定》，考虑(但不限于)以下方面：

a) 相关管理体系标准的要求；

b) 规模和复杂程度；

c）技术和法规环境；

d）管理体系范围内活动的分包情况；

e）以前审核的结果；

f）场所的数量和对多场所的考虑。

g）与组织的产品、过程或活动相关联的风险；

h）是否是结合审核、联合审核或一体化审核。

非审核策划阶段，在审核过程才发现因认证覆盖人数变更、多场所变更、审核复杂程度变更等因素导致审核时间增加，可通过增加工作日的工作时数以增加审核时间，以保证审核时间的充分性。

4.3.2.3 当受审核方管理体系包含在多个地点进行的相同活动时，如果使用多场所抽样，则按《多现场审核规定》针对每个受审核方将抽样计划的合理性形成文件，以确保正确审核。

4.3.2.4 审核组构成

4.3.2.4.1 认证机构应根据实现审核目的所需的能力以及公正性要求来选择、确定审核组长及审核员，审核组应是在 GH 唯一机构执业。多领域认证的结合审核的组长原则上应具备两个以上领域的审核资格和综合领导能力。否则，可以设立分组长以满足每一个管理体系认证对组长的要求，并负责做出结合审核组长没有能力作出的那部分。如果仅有一名审核员，该审核员应有能力履行适用于该审核的审核组长职责。

4.3.2.4.2 决定审核组的规模和组成时，认证审核部应考虑下列因素：

a）审核目的、范围、准则和预计的审核时间；

b）是否是结合、一体化或联合审核；

c）实现审核目的所需的审核组整体能力（允许具有不同注册资格和能力的审核成员结合审核时同组同时对某一部门在其资格范围内的认证领域条款进行审核）；

d）认证要求（包括任何适用的法律、法规或合同要求）；

e）语言和文化；

f）审核组成员以前是否审核过该组织的管理体系。

注：结合审核或一体化审核的审核组长应至少对一个标准有深入的知识，并了解该审核所使用的其他标准。

4.3.2.4.3 下列情况必须充分考虑审核组专业能力：

a）审核的专业有特殊要求；

b）受审核方信息安全管理复杂且容易导致信息安全事故。

c）审核电子化 ISMS 的审核员能力和信息安全。

d）考虑配置必要的资源，如计算机及计算机辅助的审核技术，可能包括诸如电视电话会议，网络会议，网络交流，远程电子方式获得 ISMS 文档和/或 ISMS 过程等，并注意审核有效性和效率审核过程的完整性。

4.3.2.4.4 审核组长和审核员所需的知识和技能可以通过技术专家和翻译人员补充。技术专家和翻译人员不能单独审核，应在审核员的指导下工作，其在审核过程中的活动由审核组中的审核员承担责任。使用翻译人员时，翻译人员的选择要避免他们对审核产生不正当影响。技术专家的选择准则根据每次审核的审核组和审核范围的需要为基础确定。

4.3.2.4.5 审核组成员的任务分工与所具备的专业能力相适应，专业人员应负责审核专业要素和部门，并保证审核组中非相应专业的成员通过在审核前技术专家的讲解或专业管理人员的培训或对作业指导书的学习，了解承担分配任务所需的专业知识。审核组工作的分配应当考虑审核员的独立性和能力的需要、资源的有效利用以及审核员、实习审核员和技术专家的不同作用和职责。在已为特定的认证方案确定了特定的准则时，这些特定准则应得到采用。

4.3.2.4.6 技术专家在审核中的职责和权利：

a）参加审核组的活动，在专业及技术上给审核员提供咨询意见或建议；

b）服从审核组安排，协助审核员一起完成审核任务；

c）参加审核组有关会议，发表自己的意见和看法。

d）技术专家不能出具不符合报告。

技术专家的选择准则根据每次审核的审核组和审核范围的需要为基础确定。

4.3.2.4.7 审核组可以有实习审核员，其要在审核员的指导下参与审核，不计入审核时间，不单独出具记录等审核文件，其在审核过程中的活动由审核组中的审核员承担责任。

4.3.2.4.8 未被指派为审核员的审核组成员（即技术专家、翻译人员、观察员和实习审核员）所花费的时间不应计入上面所确定的审核时间。使用翻译人员可能需要额外增加审核时间。

4.3.2.4.9 审核组成员（包括技术专家）的所有审核记录都应当交给审核组长，由 GH 集中妥善保管，特别是涉及保密或知识产权信息的工作文件/记录。

4.3.2.5 审核范围应说明审核的内容和界限，例如拟审核的实际位置、组织单元、活动及过程。当初次认证或再认证过程包含一次以上审核（例如覆盖不同位置的审核）时，单次审核的范围可能并不覆盖整个认证范围，但整个审核所覆盖的范围应与认证文件中的范围一致。

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或服务活动正常运行时进行。

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。 GH 应确认客户在其 ISMS 范围内满足了 ISO/IEC27001 中 4.3 的要求。

GH 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。认证机构应确认这在客户的 ISMS 范围和适用性声明中得到了体现。本公司应验证每个认证范围至少有一个适用性声明。

本公司应确保：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。

4.3.2.6 审核准则应被用作确定符合性的依据，并应包括：

——所确定的管理体系规范性文件的要求；

——所确定的由客户制定的管理体系的过程和文件；

——所履行的职能相关的其他文件，可以作为认证要求。

4.3.2.7 审核目的应明确，包括：

a）确定客户管理体系或其部分与审核准则的符合性；

b）评价管理体系确保客户组织满足适用的法律、法规及合同要求的能力；

c）评价管理体系确保客户组织持续实现其规定目标的有效性；

d）适用时，识别管理体系的潜在改进区域。

4.3.2.8　远程审核的策划

4.3.2.8.1 第一阶段审核、监督审核、特殊审核、第二阶段或再认证的局部场所或虚拟场所审核经评估符合远程审核条件的，可以实施远程审核。评估流程方法详见《基于信息和通信技术（ICT）的远程审核管理规定》。

4.3.2.8.2 使用远程审核方式进行审核时，应给审核员充分的时间来进行所有与审核或复评有关的活动，该时间的分配宜根据组织的规模，场所的数量（包括临时场所）实施 ISMS 的各种不同的组成部分时所使用的技术（如文件和/或过程控制，纠正/预防措施的控制等），已经证实的 ISMS 的绩效，以及认证用的标准等因素。

4.3.2.8.3 审核计划中应识别出审核中将使用的远程审核技术。

4.3.2.8.4 远程审核不应将审核时减少到低于各管理体系基础审核时间并考虑了适当调整之后所计算出的审核时间。

4.3.2.8.5 如果在制定的审核计划中，远程审核时间活动所占时间超过了所策划的现场审核时间的 30%，应将相应理由形成文件。

4.4　审核组选派

4.4.1　审核组拟定与确认

认证审核部根据 4.3.2.4 审核组构成要求及审核员的注册资格、专业能力、任务进度、实习需求等因素，选择拟定相应的审核组成员，经有专业能力的方案策划人员确认，以确保：

a）审核组中相应的现场审核能力及专业技术能力；

b）进行文件审查和制订审核计划的复检人员应具有相应的专业能力；

c）当审核一个以电子化过程和文件为主的 ISMS 时，应考虑审核组运用这种审核方法所需要的能力；

d）审核组长制定《审核计划》，并与审核组充分协商，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）。

4.4.2　审核任务通知

公司应提前与客户就审核计划进行沟通，并商定审核日期，由计划调度人员以《审核任务书及派出令》的方式通知审核组成员，并要求审核组：

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）审核组应当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》可根据预定的审核计划同时发送给审核组成员，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计划，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，无须修订原审核计划，也无须重新安排审核任务。

4.4.3　审核组成员信息的通报

公司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，并在反对有效时使认证审核部能够重组审核组。一旦与申请组织确定了审核组，认证审核部应正式发出《审核任务书及派出令》【《审核任务书及派出令》至少包括审核范围、准则、目的和任务、日程、审核组成员信息】，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）。

4.5　审核计划制定与沟通

4.5.1 总则

GH 任命的每一次审核组应编制《审核计划》，经审核组沟通后在审核前发给受审核方确认，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。

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 1：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。对这些技术的关注，将提高审核的有效性和效率，并支持审核过程的完整性。

4.5.2　确定审核目的、范围和准则

审核组长应根据《审核任务书及派出令》的要求，确定或引用审核目的、范围和准则，对于审核目的、范围和准则及其它任何更改，应在与客户商讨后确定。

4.5.3　编制审核组任务计划

公司宜与拟审核的组织就选择一个能最有效地证实其整个 ISMS 范围的审核时间达成一致意见。适当时，可考虑季度、月份、日期和班次。

审核组编制的任务计划（日程安排）应与《审核任务书及派出令》相一致，包括但不限于

a）审核日程；

b）审核范围，包括识别拟审核的客户和职能单元或过程；

c）审核准则（条款）；

d）拟实施现场审核活动（适用时，包括对临时场所的访问）日期；

e）现场审核活动预期的时间和持续时间；

f）审核组成员及与审核组同行人员的角色和职责。

4.5.4 审核计划的沟通

审核组长制定了明确分工的《审核计划》后，给各小组成员，以便做好如下审核准备：

a）文件审核/复检，以及前期资料审查，只有文件基本符合标准的情况下才能进行审核；

b）确保审核及审核计划由具备相应专业能力的审核员进行或复检；

c）根据审核计划的分工编写或补充“检查表”；

d）组织审核组成员，做好审核准备和专业引导，明确审核的实施策略及注意事项，做好专业引导培训。

4.6 初次审核

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。

4.6.1　第一阶段审核

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。

4.6.1.1　第一阶段审核目的：

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。

4.6.1.2　第一阶段审核方式

4.6.1.2.1 初次认证审核的第一阶段审核应在客户现场实施审核。

4.6.1.2.2 现场审核（含远程审核）时间一般按第一阶段不低于 1 个审核人日确定，但对认证覆盖人数较少或组织结构相对简单、风险程度较低的企业，也可以按照第一阶段不低于 0.5

个审核人日确定。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。

4.6.1.2.3 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认证审核部沟通，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。

4.6.1.3 第一阶段现场审核须使用《检查表》，做相应的审核记录。

4.6.1.4 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。

4.6.1.5 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。

4.6.1.6 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。

4.6.1.7 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。

4.6.1.8 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。

4.6.2 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。

4.6.3 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 GH 做出认证决定，审核组至少应向 GH 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 GH 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。

GH 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 认证决定”阶段。

4.7 实施现场审核

4.7.1 总则

审核组应按 GH 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。

4.7.2 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 GH 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。

4.7.3　审核中的沟通

4.7.3.1 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。

4.7.3.2 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（如果可能还应向认证审核部）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。审核组长应向认证审核部报告所采取行动的结果。

4.7.3.3　如果在现场审核活动的进行中发现需要改变审核范围，审核组长应与客户审查该需要，并报告认证审核部。

4.7.4　观察员和向导

4.7.4.1　观察员

认证审核部与客户应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。审核组应确保观察员不影响或不干预审核过程或审核结果。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。

4.7.4.2　向导

每个审核员应由一名向导陪同，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。审核组应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。

4.7.5　收集和验证信息

4.7.5.1　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。

4.7.5.2　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。

4.7.6　确定和记录审核发现

4.7.6.1　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。

4.7.6.2　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。

4.7.6.3　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。

4.7.6.4 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。

4.7.7 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）。

4.7.8　召开末次会议

4.7.8.1　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。

4.7.8.2　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 GH 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 GH 对申请单位的 ISMS 给予注册。

现场审核不通过：审核小组建议 GH 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）GH 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。

4.7.8.3 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 GH。

4.7.9 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。

4.8　审核报告

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。GH 应享有对审核报告的所有权。

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。

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 GH 存档。

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。

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。

4.11 补充审核

如果需要进行全面或部分的补充审核，或需要形成文件的证据（在将来的监督审核中予以确认），以验证纠正和纠正措施的有效性，则审核组应告知受审核的组织。

4.12 结合审核

ISMS 可以和其他管理体系如信息技术服务管理体系、环境管理体系、职业健康安全管理体系结合审核，结合审核时体系文件应是整合文件，并能清晰的识别出客户的 ISMS。

a）ISMS 文件亦能详细描述该体系，并清晰界定与组织内运行的其他相关体系的关系，或其他管理体系对拟认证的 ISMS 的影响。只要 ISMS 及其与其他体系适宜的接口可以清晰地界定，可以将 ISMS 文件与其他体系文件（如信息安全和环境）合在一起。

b）GH 应给审核员安排足够时间的完成与审核相关的所有活动，详见《管理体系审核时间管理规定》,GH 应有能力证实和判断任何初评，监督和复评所需的人日合适的。

c）结合审核应满足 ISMS 体系的所有要求，且不能受到结合审核的负面影响。

d）结合审核或依次进行时，对于共有要素，在确定审核员能力时，主要原则是保持每个体系审核的完整性，所以应配备适当的能力，详见《结合审核的管理规定》。

5、 认证决定

5.1 GH 由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）。

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。

5.2 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，GH 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，GH 已评审并接受了受审核方计划采取的纠正和纠正措施。

5.3 颁发认证证书

在满足 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。

注：符合颁证的条件另见 “GH-QP-025” 程序文件相关内容。

5.4 GH 不应把批准、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 获准认证注册的企业将得到认证结果通知单及 GH 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) GH 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。

5.6 认证证书的有效期为三年。

6、 认证后的监督和管理

认证后的监督和管理参照《证后审核及管理程序》执行.

6.1 监督审核时间间隔应至少在认证决定后的 12 个月内进行，两次监督审核之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，详见《证后审核及管理程序》。

6.2 每三年必须进行一次完整的复评，持证者应在有效期期满前三个月向 GH 提出复评的申请，GH 根据复评的结果决定是否重新发放注册证书。

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

6.4 获证组织信息安全管理文件的修改

6.4.1 对本证组织信息安全手册的重大修改，必须加以记录，并交给 GH 审核并备案。

6.4.2 GH 在收到重大修改的通知后应及时地将其手册进行更新。

6.4.3 审核组长收到文件更改的通知时将对有关的重大更改加以审查。对确已影响到信息安全管理体系的修改，应进行一次全面的“文件审查”或附加的现场审查，有时二者兼有。（持证企业须承担所有这些额外的文件审查和现场审核的费用）。

6.4.4 如 GH 对于某组织的 ISMS 在一段时期内持续表明有效的组织，GH 经与该组织协商一致的，可按照监督和复评程序对其设计一个个性化的监督和复评方案，实施监督或复评，但必须事前向认可委报告。

6.5 GH 的《认证业务范围管理程序》规定了我司对已获证组织认证范围进行更改的评定活动。

6.6 申请组织和客户的档案

6.6.1 GH 建立认证档案，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。

6.6.2 认证档案卷宗内至少包括以下内容：

a） 申请资料及初次认证、监督和再认证的审核报告；

b） 认证合同、管理体系认证申请及信息调查表；

c） 抽样方法的理由，包括评审特定管理体系和(或)选取多场所评审中对场所的选择；

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） 技术委员会的审议和决定；

h） 认证证书复印件；

i） 认证文件，包括认证范围(述及相关产品(包括服务）或过程）；

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。

6.6.3 GH 建立和保持《认证项目档案管理规定》，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。

6.6.4 GH《认证项目档案管理规定》对认证档案保存做出了规定，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