北京国标联合认证有限公司

信息安全管理体系认证实施规则

文件编号：ISC-GZ-37

发布日期：2025 年 11 月 05 日

实施日期：2025 年 11 月 20 日

修改日期：

版　　次：A/0

人 本　　责 任

精 进　　协 同

公司名称：北京国标联合认证有限公司

官　　网：www.china-isc.org.cn

邮　　箱：service@china-isc.org.cn

目 录

信息安全管理体系认证实施规则

1 适用范围

本认证实施规则适用于北京国标联合认证有限公司（以下简称：ISC）实施信息安全管理体系认证，满足第三方认证制度要求，作为提供认证服务的规范。必要时，在认证合同中补充相关的技术要求。

本规则规定了本认证机构进行认证的实施细则和工作程序。

1.1 本规则用于规范北京国标联合认证有限公司（以下简称：ISC）开展信息安全管理体系(ISMS) 认证活动。

1.2 本规则依据认证认可相关法律法规，结合相关技术标准，对企业信息安全管理体系认证实施过程做出具体规定，明确认证机构对认证过程的管理责任，保证信息安全管理体系认证活动的规范有效。

1.3 本规则是本机构在信息安全管理体系认证活动中的基本要求，相关机构在该项认证活动中应当遵守本规则。

2 认证依据

ISO/IEC 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》。

3 对本认证机构的基本要求

3.1 获得国家认监委批准、取得从事信息安全管理体系认证的资质。

3.2 认证能力、内部管理和工作体系符合GB/T 27021/ISO/IEC 17021-1《合格评定管理体系审核认证机构要求》。

3.3 建立内部制约、监督和责任机制，实现培训（包括相关增值服务）、审核和作出认证决定等工作环节相互分开，符合认证公正性要求。

3.4 不将申请认证的组织（以下简称申请组织）是否获得认证与参与认证审核的审核员及其他人员的薪酬挂钩。

3.5 建立风险防范机制，对其从事信息安全管理体系认证活动可能引发的风险和责任，采取合理有效措施。能证明已对其开展的信息安全管理体系认证活动引发的风险进行了评估，并对各个活动领域和运作地域的业务引发的责任做了充分安排（如保险或储备金）。

3.6 获证组织发生重大事故或引发重大舆情，应及时采取措施，迅速进行调查、处理，并将信息及时报送市场监管部门。

4 对认证人员的条件和要求

4.1 本认证机构应建立认证人员管理制度，对认证人员的选择条件、评价准则、聘用程序、培养机制等做出明确规定，确保从事信息安全管理体系认证的人员持续具备相应素质和能力。

4.2 认证审核人员及审核组要求

4.2.1 认证审核员应当取得CCAA 信息安全管理体系认证审核员注册资格证书。

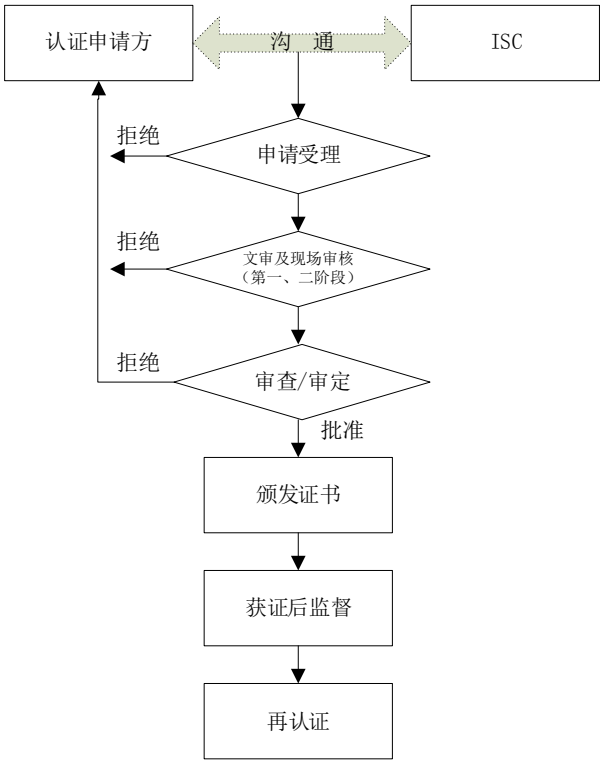
4.2.2 认证人员应遵守与从业相关的法律法规，对认证审核活动及相关认证审核记录和认证审核报告的真实性承担相应的法律责任。

4.2.3 认证人员应具备与其所从事认证工作相适宜的能力，且为保证自身能力持续满足认证相关要求，应持续学习，并定期参加本机构组织或要求的各类培训。

4.2.4 认证人员不得发生影响认证公正性和有效性的行为；不得参与近两年内其咨询过的组织的认证活动；不得接受认证委托人及其相关利益方的礼金、礼品或其他不当利益；未经允许不得私自到获证组织报销食宿交通等票据。

4.2.5 具有与管理体系相关的管理和法规等方面特定知识的技术专家可以成为审核组成员。技术专家应在审核员的监督下进行工作，可就受审核方或获证组织管理体系中技术充分性事宜为审核员提供建议，但技术专家不能作为审核员独立实施审核活动。

5 认证过程流程图



6 初次认证程序

6.1 受理认证申请

6.1.1 信息公开

本认证机构应向申请组织至少公开以下信息：

（1）可开展的认证业务范围，获得认可的情况，以及分包境外认证机构业务的情况；

（2）开展认证活动所依据的认证标准及认证流程；

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

（4）拟向组织获取的信息，以及对相关信息的保密规定；

（5）认证收费标准

（6）认证证书、认证标志及相关的使用规定；

（7）对认证过程的申诉、投诉规定；

（8）认证依据用标准转版的规定（适用时）。

（9） “提前较短时间通知的审核”的情形；

（10）相关的认证方案、认证程序；

6.1.2 受理认证申请的基本条件

1）认证客户具有明确的法律地位,客户具有企业营业执照、事业单位法人证书、社会团体登记证书、非企业法人登记证书等，可独立申请认证。其他类型的客户，应由具备资格的单位代为申请；

2）国家、地方或行业有要求时，认证客户具有规定的行政许可文件,其申请认证范围应在法律地位文件和行政许可文件核准的范围内；

3）认证客户按相关的管理体系标准建立了文件化的管理体系。初次认证现场审核前已至少持续稳定运行了3个月，至少已实施一次完整的内审和管理评审或已编制实施计划，并承诺在证书有效期内，持续有效运行管理体系；

4）认证客户承诺遵守国家的法律、法规及其他要求,承诺始终遵守认证的有关规定，承担与认证有关的法律责任，并有义务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；且客户符合工信部联协[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/监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）后，公司方可安排现场审核。

5）认证客户未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”或发生违反国家相关法规，虚报、瞒报获证所需信息的情况；

6）认证客户承诺获得ISC认证后，按规定使用认证证书和认证标志和有关信息，不得擅自利用管理体系认证证书的文字、符号误导公众认为其产品或服务通过认证；

7）按合同支付认证费用，并按规定接受监督；

8）认证客户承诺获得 ISC 认证后，按照 ISC 要求向 ISC 通报管理体系变更的信息和其他可能影响管理体系持续满足认证标准要求的能力的事宜的信息，一般包括：客户及相关方有重大投诉；发生重大事故；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、强制性认证或其他资质证书变更；法定代表人、最高管理者、管理者代表发生变更；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；管理体系和重要过程的重大变更等）；出现影响管理体系运行的其他重要情况；

9）认证审核期间，认证客户能够提供与拟认证范围相关的活动或过程。

6.1.3 本认证机构应要求申请组织至少提交以下资料：

1）认证申请书，申请书应包括申请认证的生产、经营或服务活动范围及活动情况的说明。提供申请的范围，ISMS范围内开展的业务类型，分包方情况，ISMS覆盖的场所数量和灾难恢复场所数量，ISMS复杂性（信息安全保密要求的、关键资产的数量、以及涉及的过程和服务的数量等）

2）法律地位的证明文件的复印件。若信息安全管理体系覆盖多场所活动，应附每个场所的法律地位证明文件的复印件（适用时）。

3）信息安全管理体系覆盖的活动所涉及法律法规要求的行政许可证明、资质证书、强制性认证证书等的复印件。

4）受控的管理文件；体系运行三个月的证明；

5）申请组织多场所清单（适用时）；

6）服务流程图；

7）保密的相关事项（哪些信息不允许认证机构接触，或者认证机构在接触相关信息时应满足哪些要求）；

8）召开内部审核和管理评审的时间；

9）适用的法律法规、标准及其他要求清单；

10）适用性声明（适用于ISMS）；

11）体系覆盖的范围。

6.2 申请受理评审

6.2.1 确认评审申请方的基本信息，核对申请资料的完整性。

1）依据企业认证申请，核对申请书填写的完整性，申请材料的齐全性；

2）依据申请书及申请资料，核对管理系统客户信息录入的准确性，包括：企业名称、注册资本、地址场所信息、法人代表、联系方式等全部内容，保证申请信息与管理系统的一致性。

6.2.2 核对申请方是否具有合法的法人地位：

1）营业执照需在有效期内；

2）营业执照即将过期的，要求提供原营业执照复印件和正在办理换证的有效证明或说明，在评审表的资料齐全性中予以记录，供审核部及技术部后续关注。

3）新成立的企业营业执照的批准时间至现场审核的时间应同时满足上述要求,存在变更营业执照的情况，以首次取得营业执照时间为准；

4）无法人地位的组织，应提供相关证明材料，如社会团体等级证书、非企业法人登记证书的复印件；

6.2.3 根据申请认证的活动范围及场所、员工人数、完成审核所需时间和其他影响认证活动的因素，综合评审，保存评审记录，做出评审结论，以确定:

1) 所需要的基本信息都得到提供;

2) 申请组织的行业类别和与之相对应的管理体系所管理的过程特性和管理要求;

3) 国家对相应行业的管理要求;

4) 机构与申请组织之间任何已知的理解差异得到消除;

5) 机构有能力并能够实施认证活动;

6) 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;

7) 机构应建立关于审核人日的确定准则，根据受审核方ISMS的复杂性、ISMS范围内开展业务的类型、客户规模以及分包方信息开发程度、以及ISMS涉及的场所及灾难恢复场所的数量等因素核算并确定审核人日,以确保审核的充分性和有效性。将确定后的人日数记录在审核方案中，审核人日的确定规则参考**附录A**。

6.2.4 对符合 6.1.2/6.2.3 要求的，本机构可决定受理认证申请;对不符合上述要求的，本机构应通知申请组织补充和完善，或者不受理认证申请。

6.3 认证合同的签署

在实施认证审核前，本认证机构应与申请组织订立具有法律效力的书面认证合同，合同应至少包含以下内容：

1）申请组织获得认证后持续有效运行信息安全管理体系认证的承诺;

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 生产、销售的产品或提供的服务被质量或市场监管部门认定不合格。

③ 发生严重信息安全事故。

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；信息安全量管理体系覆盖的活动范围变更；信息安全管理体系和重要过程的重大变更等。

⑤ 出现影响信息安全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，不利用信息安全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）拟认证的信息安全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。

6.4 策划审核

6.4.1 建立审核方案

6.4.1.1 本认证机构审核方案范围与程度的确定应基于受审核组织的规模和性质，以及受审核管理体系的性质、功能、复杂程度以及成熟度水平。对于ISMS主要考虑组织所确定的信息安全控制：ISMS覆盖的场所数量和灾难恢复场所数量，ISMS复杂性（信息安全保密要求的、关键资产的数量、以及涉及的过程和服务的数量等）。针对每一认证客户建立认证周期内的审核方案，包括初次认证（初次认证审核分两个阶段实施：第一阶段和第二阶段）、认证决定之后的监督审核和认证到期前进行的再认证审核。

审核方案应包括在规定的期限内有效和高效地组织和实施审核所需的信息和资源，应包括以下内容:

1) 审核方案的目标;

2) 审核的范围与程度、数量、类型、持续时间、地点、日程安排;

3) 审核准则;

4)审核方法;

5)审核组的选择;

6)所需的资源；

7)处理保密性、信息安全、健康和安全，以及其它类似事宜。

6.4.1.2 公司目前主要在以下场合应用计算机辅助审核技术

（1）公司本部各部门及审核组长远程方式获取客户电子文档、管理体系过程或其他信息。如申请评审、审核组派遣、认证决定中问题的交流等；

（2）第一阶现场审核时，审核组远程方式获得的电子文档资料及必要的信息；

（3）审核组在认证客户应用电视电话、网络技术或远程方式审核认证客户偏远的、交通不便的电子化场所（分场所或临时项目）；

6.4.1.3 审核组运用计算机辅助技术审核认证客户电子化分场所时应：

（1）在审核计划中说明；

（2）总部、典型的重要场所、不能进行抽样的场所（即至少有同类场所两个以上）不允许进行电子化审核；

（3）远程审核活动占所策划的现场审核时间要在30％以下；

（4）做好记录，并对确保有效性做出解释。

6.4.2 审核时间

为确保认证审核的完整有效,认证机构应以**附录A**所规定的审核时间为基础,根据申请组织信息安全管理体系覆盖的活动范围、特性、技术复杂程度、信息安全风险程度、认证要求和体系覆盖范围内的有效人数等情况，核算并拟定完成审核工作需要的时间。

6.4.3 多场所

6.4.3.1适用于抽样审核的多场所组织

当认证客户拥有满足以下条件的多个场所时，可以考虑使用基于抽样的方法进行多场所抽样审核：

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。

6.4.3.2 抽样的考虑

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，抽取具有代表性的场所：

1)总部（适宜时）及各场所的内部审核结果；

2)管理评审的结果；

3)场所规模的差异；

4)场所业务范围的差异；

5)不同场所信息系统的复杂程度；

6)工作实践的差异；

7)所开展活动的差异；

8)控制的设计与运行的差异；

9)与关键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；

13) 特定场所发生的信息安全事件。

c）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中所列因素以及随机因素作出判断；

f）在单个场所发现不符合时，纠正措施程序的实施适用于证书所覆盖的所有场所。确定所有场所的活动都在同一管理体系之下，该管理体系确实覆盖了所有场所。

6.4.3.3 抽样方法

（1）若分场所拟在认证证书中显示:x代表生产/服务场所数量，初次认证的服务场所抽样量为$\sqrt{x}$，监督审核的抽样量为$0.6\sqrt{x}$，再认证的抽样量为 $0.8\sqrt{x}$ ；

（2）若分场所为临时场所，则一般不在认证证书中列明，每次审核(含初次认证、监督或再认证)抽样的生产/服务场所数量均不低于1，且应确保认证周期内所抽样场所的生产/服务范围覆盖认证范围(或拟认证的范围)。

6.4.3.4 下列可视为单一场所，一般不采用多场所抽样的方式审核:

（1）不在同一地点的办公场所和生产/服务场所，其中生产/服务场所是唯一的,且办公场所不提供认证范围所涉及的产品和服务;

（2）彼此靠近的多个场所，比如:位于同一栋建筑的不同楼层，或同一园区/片区的不同楼栋。

6.4.3.5不适用于抽样审核的多场所组织

（1）所有场所实施的过程、活动与管理体系的范围有关且存在显著差别;

（2）多个场所没有涵盖相同的活动、过程及管理风险;

（3）客户要求对每个场所审核;

（4）有专门的方案或法规要求规定了系统性地对每个场所审核。

6.4.3 审核组

6.4.3.1 认证机构应当根据信息安全管理体系覆盖的活动的专业技术领域选择具备相关能力的审核员组成审核组，必要时可以选择技术专家参加审核组。审核组中的审核员承担审核任务和责任。

6.4.3.2 技术专家主要负责提供认证审核的技术支持，不作为审核员实施审核，不计入审核时间，其在审核过程中的活动由审核组中的审核员承担责任。

6.4.3.3 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。

6.4.4 审核计划

6.4.4.1 本机构应为每次审核指定审核组长，并给组长下达书面的审核计划(通知书)，审核组长收到审核计划(通知书)后应及时编制审核计划，审核计划至少包括以下内容:审核目的、审核准则、审核范围、现场审核的日期和场所、现场审核持续时间，审核组成员(其中:审核员应注明证书号)。当使用了远程审核方法和工具，要在审核计划里加以识别。

6.4.4.2 如果信息安全管理体系认证覆盖范围包括在多个场所进行相同或相近的活动，且这些场所都处于申请组织授权和控制下，本机构审核组可以在审核中对这些场所进行抽样，但应根据相关要求实施抽样以确保对所抽样本进行的审核对信息安全管理体系认证包含的所有场所具有代表性，如果不同场所的活动存在明显差异、或不同场所间存在可能对信息安全管理体系能力有显著影响的区域性因素，则不能采用抽样审核的方法，应当逐到各现场进行审核。

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

6.4.4.4在审核活动开始前，审核组应将审核计划交申请组织确认，遇特殊情况临时变更计划时，应及时将变更情况通知申请组织，并协商一致。

6.5 实施审核

6.5.1 审核组应当按照审核计划的安排完成审核工作。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。

6.5.2 审核组应当会同申请组织按照程序顺序召开首、末次会议，申请组织的最高管理者及与信息安全管理体系相关的职能部门负责人员应该参加会议。参会人员应签到，审核组应当保留首、末次会议签到表。申请组织要求时，审核组成员应向申请组织出示身份证明文件。

6.5.3 审核过程及环节

6.5.3.1 初次认证审核，分为第一、二阶段实施审核。

6.5.3.2 第一阶段审核应至少覆盖以下内容:

（1）结合现场情况，确认申请组织实际情况与信息安全管理体系成文信息（ISMS 和其所覆盖活动的一般信息；ISO/IEC 27001:2022 要求的 ISMS 文件的副本等）描述的一致性，特别是体系成文信息中描述的客户的组织设置、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、服务过程等是否与申请组织的实际情况相一致。

（2）结合现场情况，审核申请组织理解和实施ISO/IEC 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》标准要求的情况，评价信息安全管理体系运行过程中是否实施了内部审核与管理评审，确认信息安全管理体系是否已运行并且超过 3 个月。

（3）确认申请组织建立的信息安全管理体系覆盖的活动内容和范围、体系覆盖范围内有效人数、过程和场所，遵守适用的法律法规及强制性标准的情况。

（4）结合信息安全管理体系覆盖产品和服务的特点识别对信息安全目标的实现具有重要影响的关键点，并结合其他因素，科学确定重要审核点。

（5）与申请组织讨论确定第二阶段审核安排。对信息安全管理体系成文信息不符合现场实际、相关体系运行尚未超过3个月或者无法证明超过3个月的，以及其他不具备二阶段审核条件的，不应实施二阶段审核。

如果发生任何将影响管理体系的重要变更，ISC可能将重复整个或部分第一阶段审核。第一阶段审核的结果可能导致推迟或取消第二阶段。

6.5.3.3 在下列情况，第一阶段审核可以不在申请组织现场进行，但应记录未在现场进行的原因:

（1）申请组织已获本认证机构颁发的其他有效认证证书，认证机构已对申请组织信息安全管理体系有充分了解。

（2）申请组织获得了其他经认可机构认可的认证机构颁发的有效的信息安全管理体系认证证书，通过对其文件和资料的审查可以达到第一阶段审核的目的和要求。

除以上情况之外，第一阶段审核应在受审核方的生产经营或服务现场进行。

注：如一阶段采用非现场审核，不报审核计划，但不可与审核组成员的日程和路程时间冲突。此时所有现场审核人日计入二阶段审核。

6.5.3.4 审核组应将第一阶段审核情况形成书面文件告知申请组织，对在第二阶段审核中可能的重要关键点，要及时提醒申请组织特别关注。

6.5.3.5第二阶段审核

第二阶段审核应当在申请组织现场进行审核，现场审核应考虑一阶段审核结果，对受审核方的管理过程和控制措施的运行情况进行评价，对一阶段审核提出的问题改进情况进行验证。审核应重点关注客户的以下方面：

（1）最高管理层对信息安全目标的领导和承诺；

（2）信息安全风险评估，包括确保在重复实施风险评估时能产生一致的、有效的和可比较的结 果；

（3）根据信息安全风险评估和风险处置过程来确定控制；

（4）信息安全绩效和 ISMS 有效性，包括根据信息安全目标对其实施评价；

（5）所确定的控制、适用性声明、信息安全风险评估结果、风险处置过程与信息安全方针和信 息安全目标之间的对应关系；

（6）控制的实现（见附录 E-审核控制的示例）：审核应考虑外部环境、内部环境、相关风险以 及组织对信息安全过程和控制的监视、测量与分析过程，并确定待实现的控制是否已经实 现且在整体上是有效的；

（7）方案、过程、规程、记录、内部审核和对 ISMS 有效性的评审，且这些都能追溯到最高管理 层的决定、信息安全方针和信息安全目标。

如果认证客户不能在初次认证第二阶段结束后的规定时间内按要求关闭不符合，ISC将再实施一次第二阶段审核或不批准认证。

6.5.3.6 发生以下情况时，审核组应向本机构报告，经本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。

6.6 审核报告的编制和分发

6.6.1审核报告的编制

审核组长应根据审核方案程序报告审核结果。审核报告应提供完整、准确、简明和清晰的审核记录，并包括或引用以下内容：

1）审核目标；

2）审核范围，尤其是应明确受审核的组织单元和职能单元或过程；

3）明确审核委托方；

4）明确审核组和受审核方在审核中的参与人员；

5）进行审核活动的日期和地点；

6）审核准则；

7）审核发现和相关证据；

8）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；

9）关于对审核准则遵守程度的陈述。

10)审核的说明，其中包括文件评审摘要;

11)对客户信息安全风险分析进行认证审核的说明;

12)与审核计划的偏离(适用时);

13)所采用的主要审核路线和所使用的审核方法

14)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)

15)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。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审议人员。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。

16)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:

适当时，审核报告还可以包括或引用以下内容

——包括日程安排的审核计划；

——审核过程综述，包括遇到可能降低审核结论可靠性的障碍；

——确认在审核范围内，已按审核计划达到审核目标；

——尽管在审核范围内，但没有覆盖到的区域；

——审核结论综述及支持审核结论的主要审核发现；

——审核组和受审核方之间没有解决的分歧意见；

——改进的机会(如果审核计划有规定）；

——识别的良好实践；

——商定的后续行动计划（如果有）；

——关于内容保密性质的声明；

——对审核方案或后续审核的影响；

——审核报告的分发清单。

审核报告可以在末次会议之前编制。

6.6.2审核报告的分发

本机构应在做出认证决定后30个工作日内将审核报告提交申请组织，申请组织可以通过本认证机构官网www.chin-isc.org.cn登陆查看和下载。如果延迟，应向受审核方和审核方案管理人员通告原因。审核报告应按审核方案程序的规定注明日期。

6.6.3 对终止审核的项目，审核组应将已开展的工作情况形成报告，本机构应将此报告及终止审核的原因提交给申请组织。

6.7不符合项的纠正和纠正措施及其结果的验证

6.7.1 根据审核目标，审核结论可以表明采取纠正、纠正措施和预防措施或改进措施的需要。此类措施通常由受审核方确定并在商定的期限内实施。适当时，受审核方应将这些措施的实施状况告知审核方案管理人员和审核组。审核组应对措施的完成情况及有效性进行验证，验证可以是后续审核活动的一部分。

审核组对给企业开出的不符合项的纠正措施进行确认，无法当次审核过程中关闭的不符合，采取纠正措施验证有效后在下一年监督审核时进行确认验证关闭。

6.7.2 对审核中发现的不符合项，认证机构应要求申请组织分析原因，并提出纠正和纠正措施。对于严重不符合，应要求申请组织在最多不超过 6 个月期限内采取纠正和纠正措施。认证机构应对申请组织所采取的纠正和纠正措施及其结果的有效性进行验证。如果未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，则应按照重新认证申请或重新实施一次二阶段审核。

6.8 认证决定

6.8.1 本认证机构应在对审核报告、不符合项的纠正和纠正措施及其结果以及其他信息进行综合评价的基础上，作出认证决定。认证决定人员应为本认证机构管理控制下的人员，并不得为审核组成员。

6.8.2 经评定，本认证机构有充分的证据确认受审核方满足下列条件时，可做出授予认证的决定：

1）具备应有的法定资格、资质；

2）认证范围覆盖的活动、产品和服务符合相关法律法规要求，未发生重大事故和严重违法行为；

3）对于严重不符合项，已评审、接受并验证了纠正和纠正措施的有效性；对于轻微不符合项，已评审、接受了受审核方的纠正和纠正措施或计划采取的纠正和纠正措施；

4）受审核方的信息安全管理体系总体符合标准要求且运行有效；

5)有充分的证据证实管理评审和 ISMS 内部审核的安排已实、是有效的并将得到保持。

6.8.3 授予组织的认证范围应基于组织的法律地位文件及审核范围，不得大于其营业执照范围和行政许可范围以及审核范围。

6.8.4 认证决定给予注册批准后，颁发认证证书后在 30 个工作日内按照规定的要求将认证结果相关信息报送国家认监委。

7 监督审核程序

7.1 本机构应对持有其颁发的信息安全管理体系认证证书的组织(以下称获证组织)进行有效跟踪，监督获证组织持续运行信息安全管理体系认证并符合认证要求。

7.2 为确保达到7.1条要求，本机构应根据获证组织的产品和服务的信息安全风险程度或其他特性，确定对获证组织的监督审核的频次。

7.2.1 作为最低要求，初次认证后的第一次监督审核应在认证证书签发日起 12 个月内进行。此后，监督审核的时间间隔不得超过12个月。

7.2.2 超过期限而未能实施监督审核的，认证证书将被暂停或撤销处理。

7.2.3 获证企业的产品在地方政府监管部门抽查中被查出不合格时，自行政部门发出通报起 30 日内，认证机构应对该企业实施监督审核。

7.3 监督审核的时间应与初次认证审核(第1阶段+第2阶段)的时间成比例，约为初审时间的 1/3。在策划每次监督审核时，应获得与客户管理体系有关的更新信息所策划的监督审核时间应考虑到客户的体系成熟度等变化情况，对策划的监督审核时间进行确认审查，审查的结果(包括对审核时间的调整)应在审核方案策划中予以记录。

7.4 监督审核的审核组，应符合6.4.3条的要求。

7.5 监督审核应在获证组织现场进行，且应满足第6.1.2 条确定的条件。由于市场、季节性等原因，在每次监督审核时难以覆盖所有产品和服务的，在认证证书有效期内的监督审核需覆盖认证范围内的所有产品和服务。

7.6 监督审核时至少应审核以下内容：

1）ISMS 在实现客户信息安全方针的目标方面的有效性；

2）相关信息安全法律法规合规性的定期评价和审查规程的运行情况；

3）所确定的控制的变更，及其引起的适用性声明变更；

4）审核方案中所述控制的实现和有效性。

3）内部审核和管理评审；

4）投诉的处理；

5）管理体系实施的有效性；

6）认证范围相关的产品/服务/活动现场情况；

7）为持续改进而策划的活动的进展；

8）以往审核的结果，特别是对上次审核中确定的不符合采取的措施；

9）证书和标志的使用和（或）任何其他对认证资格的引用；

10)对体系有影响的有关投诉的处理,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。

7.7 在监督审核中发现的不符合项，认证机构应要求获证组织分析原因，规定时限要求获证组织完成纠正和纠正措施并提供纠正和纠正措施有效性的证据。认证机构应采用适宜的方式及时验证获证组织对不符合

项进行处置的效果。

7.8 监督审核的审核报告，应包括有关消除以往发现的不符合、适用性声明的版本和上次审核后发生的重大变更的信息。监督审核报告应至少覆盖监督审核方案要求的内容和7.6的全部要求。

7.9 根据监督审核报告及其他相关信息，作出继续保持、暂停、暂停恢复、撤销认证证书等决定。

7.10 若发生下述情况则需增加监督频次，或安排提前较短时间通知的审核：

1) 获证客户对管理体系进行了重大更改；

2) 有足够信息表明获证客户发生了组织机构、服务过程的变化，包括：服务交付过程、关系过程、控制过程、主要相关方的变化等影响到其认证基础的更改；

3) 获证客户出现服务质量事故、服务协议违约或用户提出对相关管理体系运行效果的投诉未得到处理时；

4) 获证客户的产品和服务被国家行政主管部门在监督抽查中被查出不合格时；

5) 其他需要考虑的情况。

8 再认证程序

8.1 认证证书期满前，若获证组织申请继续持有认证证书，认证机构应当完成再认证审核，并决定是否延续认证证书。

8.2 认证机构应按要求组成审核组。按照历次监督审核情况，制定再认证审核计划交审核组实施。

8.3 再认证审核时间的确定应考虑客户管理体系的变化和体系成熟度的变化情况和绩效评价结果等因素，而不是简单按初次认证审核时确定的结果计算，依据客户更新的信息(再认证申请及资料)确认组织实施初次认证审核(第1阶段+第2阶段)的审核时间。ISMS年度再认证时间应与初次认证审核(第1阶段+第2阶段)的时间成比例，再认证审核时间不低于初次审核时间的2/3。

8.4 再认证时通常可不进行一阶段审核，但当获证客户的管理体系和获证客户的内外部运作环境有重大变化时，再认证审核活动可能需要有第一阶段审核。

8.3 对于审核组开具的轻微不符合在规定的时间内按要求关闭，否则，因认证客户的原因导致ISC不能在原认证证书到期后6个月内作出认证决定的，再认证审核失效。对再认证审核中发现的严重不符合项，应规定时限要求获证组织实施纠正与纠正措施，并在原认证证书到期前完成对纠正与纠正措施的验证。实施纠正措施的时限，应与不符合的严重程度和相关的信息安全风险相一致。

8.4 认证机构按照要求作出再认证决定。获证组织继续满足认证要求并履行认证合同义务的，向其换发认证证书。

8.5 如果在当前认证证书的终止日期前完成了再认证活动并决定换发证证书，新认证证书的终止日期可以基于当前认证证书的终止日期。新认证证书上的颁证日期应不早于再认证决定日期。

如果在当前认证证书终止日期前，认证机构未能完成再认证审核或对严重不符合项实施的纠正和纠正措施未能进行验证，则不应予以再认证，也不应延长原认证证书的有效期。

在当前认证证书到期后，如果认证机构能够在6个月内完成未尽的再认证活动，则可以恢复认证，否则应至少进行一次第二阶段审核才能恢复认证。认证证书的生效日期应不早于再认证决定日期，终止日期应基于上一个认证周期。

9 特殊审核

9.1 扩大认证范围审核

针对已获证的客户，ISC 对扩大认证范围的申请进行评审，确定能否予以扩大的决定所需的审核活动，这一工作可与监督审核同时进行。

9.2 提前较短时间通知的审核

为调查投诉、对变更做出回应或对被暂停的获证客户进行追踪，需要在提前较短时间通知获证客户后对其进行的审核。获证客户的产品和服务被国家行政主管部门在监督抽查中被查出不合格时，ISC将对获证客户实施特殊审核。如获证客户不接受特殊审核，认证证书将被暂停。

10认证的批准、拒绝、保持、扩大、缩小、变更、暂停、恢复和撤/注销的程序

10.1 批准认证范围的程序

1) ISC 向认证客户提供认证有关信息的公开文件，使其知悉并理解；

2) 认证客户向 ISC 正式提交认证申请书和相关附件；

3) ISC 根据客户申请信息进行申请评审，并已确认受理认证申请；

4) 满足批准认证资格的条件，经ISC审定，认为认证客户在认证范围内已满足批准认证资格的条件，同意批准认证；

5) ISC 向认证客户颁发认证证书，要求获证方按规定使用认证标志。

10.2 拒绝认证注册的程序

1) 不满足满足批准认证资格的条件，经ISC评审为不予受理认证或认证客户的管理体系不满足批准认证资格条件；

2) ISC 向认证客户发出《不予认证注册通知》。

10.3 保持认证资格的程序

1) 满足保持认证资格的条件，监督审核后，经 ISC 派出的审核组长确认和 ISC 审查后认为获证客户在认证范围内能持续满足保持认证资格的条件，同意保持认证资格，由ISC签发确认证书并向获证客户发放；

2) 在认证证书有效期内如有认证要求变更，获证客户接受变更的认证要求，并经ISC验证在认证范围内管理体系满足变更的要求，可保持认证资格。

10.4 扩大认证范围程序

1) ISC向获证客户提供与扩大认证范围有关信息的公开文件，获证客户知悉并理解；

2) 获证客户向ISC正式提交扩大认证范围的申请和相关附件；

3) 需要时，获证客户与ISC补充签署或修订认证合同，并按照规定补充缴纳认证费用；

4) 满足扩大认证范围的条件，经ISC审核、审定，认为获证客户在申请扩大认证范围内已满足批准认证资格的条件，同意批准扩大认证范围，认证证书的注册号和有效期保持不变；

5) ISC向获证客户送交新认证证书，同时收回原证书。

10.5 缩小认证范围的程序

1）获证客户向ISC正式提交缩小认证范围的申请，或ISC提出缩小获证客户认证范围的建议，并提供理由和证据。ISC的审定意见和日常监督结果也可作为认证范围缩小的信息来源和理由，经认证双方沟通后达成一致意见；

2）需要时，获证客户应与ISC修订认证合同；

3）经ISC审定，认为获证客户在申请缩小认证范围不会对仍保持的认证范围产生影响，同意批准缩小认证范围，收回原认证证书，换发认证证书或附件，认证证书的注册号和有效期保持不变。

10.6 变更认证信息的程序

1）获证客户向 ISC 正式提交变更认证信息的申请和相关文件资料；

2）需要时，获证客户应接受 ISC 的审核；

3）经 ISC 审定，认为获证客户满足认证信息变更的条件，同意批准认证信息变更；

4）ISC 收回原认证证书，换发认证证书或附件，认证证书的有效期保持不变。

10.7 暂停认证资格的程序

1） 符合下列条件之一的获证组织的认证将被暂停：

--获证组织管理及服务体系持续或严重不满足认证要求，包括对体系运行的有效性要求；

--获证组织不承担、履行认证合同约定的责任和义务；

--获证组织在证书有效期间受到相关执法监管部门处罚；

--获证组织被地方认证监管部门发现体系运行存在问题；

--获证组织持有的行政许可证明、资质证书、强制性认证证书等过期失效，重新提交的申请已被受理但尚未换证；

--获证组织主动请求暂停；

--获证组织发生了与信息安全管理等有关的重大事故，反映出组织的体系建立及运行存在重大缺陷；

--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等。

2）ISC提出对获证客户暂停全部或部分认证范围内认证资格的建议，并提供理由和证据,或由获证客户向ISC提出暂停认证资格的申请；

3）必要时，ISC与获证客户沟通，核实证据；

4）经 ISC 审定，认为获证客户在认证范围内全部或部分不再持续满足认证要求，但仍然有可能在短期内采取纠正措施的，同意批准暂停全部或部分认证范围的认证资格，并确定暂停期限，向获证客户颁发《认证证书暂停通知书》并公告；

e）获证客户按照《认证证书和标志的使用要求》停止使用认证证书和认证标志,在暂停期间，客户的管理体系认证暂时无效。

10.8 恢复认证资格的程序

1）获证组织已针对暂停认证资格的原因采取了有效的纠正措施，产生原因已经消除，认证资格的恢复符合相关的认证要求，同时已证实在暂停期间内没有使用、引用认证资格（如广告宣传）和使用认证标志；

2) 在确定的认证资格暂停限期结束前，根据暂停原因，获证客户在规定期限内向ISC提出恢复认证资格的《恢复使用认证证书和认证标志的申请书》；

3) 需要时，获证客户应提交相关纠正措施和有效性验证材料；

4) 经 ISC 审定，确认获证客户在暂停认证资格的认证范围内已恢复符合相关的认证要求，作出同意恢复认证资格的结论，颁发《恢复使用认证证书和标志的通知》并公告。

10.9 撤/注销认证资格的程序

符合下列条件之一的获证组织的认证将被撤/注销：

1) 获证组织审核未通过；

2) 获证组织被注销或撤销法律地位证明文件；

3) 获证组织拒绝配合认证监管部门实施的监督检查，或者对有关事项的询问和调查提供了虚假材料或信息；

4) 获证组织出现重大的与信息安全管理等有关重大事故等，经执法监管部门确认是获证组织违规造成；

5) 获证组织在证书有效期间有其他严重违反法律法规行为，受到相关执法监管部门处罚；

6) 获证组织暂停认证证书的期限已满但导致暂停的问题未得到解决或纠正

（包括持有的行政许可证明、资质证书、强制性认证证书等已经过期失效但申请未获批准）；

7) 获证组织没有运行管理体系或者已不具备运行条件；

8) 获证组织不按相关规定正确引用和宣传获得的认证信息，造成严重影响或后果，或者认证机构已要求其纠正但超过2个月仍未纠正；

9) 获证组织不承担、履行认证合同约定的责任和义务；

10) 获证组织申请注销认证证书；

11) 认证证书有效期届满，未申请延续使用；

12) 因换发新证书而注销旧证书；

13) 其他原因需要撤/注销证书。

经 ISC 核实与审定，确认获证客户在认证范围内的管理体系不再满足认证要求，作出撤/注销认证资格的结论，发放《认证证书注/撤销通知书》并公告，收回认证证书，认证客户不得再使用认证证书和认证标志。

11认证证书和认证标志

11.1 认证证书和认证标志

11.1.1 认证证书包含以下信息

（1）证书名称；

（2）认证注册号（即证书编号）；

（3）获证客户的名称、地址（多场所认证包括总部和所有场所的地址信息）、邮政编码、统一社会信用代码/组织机构代码。该信息应与其法律地位证明文件的信息一致；

（4）认证所覆盖的范围，适用时，包括每个场所相应的认证范围；

（5）授予认证、扩大或缩小认证范围、更新认证的生效日期，生效日期不应早于相关认证决定的日期；

（6）认证有效期；

（7）审核获证客户对所用的管理体系标准,适用时，包括明示不适用的标准条款。

（8）认证用标准和（或）其他规范性文件所要求的任何其他信息（例如专项技术要求）；

（9）公司的名称、地址和认证标识；

（10）公司的印章和公司总经理的签字；

（11）为便于社会监督，在证书上应注明：“本证书信息可在国家认证认可监督管理委员会官方网站（www.cnca.gov.cn）上查询”。

（12）当组织不是在明确的物理位置实施其认证范围内的任何活动时，认证证书应说明组织所有的活动是远程实施的。

11.2 认证证书和认证标志的使用

获证客户应建立认证证书和认证标志的使用方案，获证后按照《认证证书和标志的使用要求》正确使用认证证书和认证标志。

11.3 认证证书和认证标志的误用

11.3.1 获证后，按照下述规定正确使用认证证书、认证标志和认可标识,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。正确引用认证资格的广告宣传，并承担由于私自篡改认证证书、错误使用认证标志、错误引用认证状态所引发的全部法律责任：

① 在传播媒介（如互联网、宣传册或广告）或其他文件中引用认证状态时，应符合乙方文件要求；

② 不得对其认证资格做出误导性说明；

③ 不得以误导性方式使用认证证书或其任何部分；

④ 认证资格被撤销或到期失效后，立即停止使用所有引用认证资格的广告材料；

⑤ 认证范围被缩小后，修改所有的广告材料；

⑥ 不得在引用认证资格时，暗示认证机构对其产品（服务）或过程进行了认证；

⑦ 不得暗示认证适用于认证范围以外的活动和场所；

⑧ 在使用认证资格时，不得使认证机构和认证制度的声誉受损，失去公众信任；

⑨ 被暂停认证资格期间不得使用认证证书；

11.3.2 管理体系认证证书只能由获证组织在证书有效期内和获准认证范围内使用，不准以任何方式转让、出售或借用、冒用。

11.3.3 获得公司认证的组织，可以在其公开出版物、宣传品、网页等载体上展示认证证书，但应保证其清晰可辨。

11.3.4 认证证书有效期为为五年，在有效期内，经公司监督审核被确认保持注册资格后，获证组织方可继续使用管理体系认证证书。

11.3.5 因不符合认证要求，可能导致被暂停、撤销认证资格时，应停止使用认证证书。

11.3.6 获证客户一旦发现误用认证证书或认证标志，应立即采取纠正措施，并报告国标联合审核管理部门。

11.4 获证客户的信息通报

获证客户应建立向国标联合通报最新信息的程序，并及时通报其重大投诉、国家监督检查结果、重大事故及获证客户变更的各种信息等。变更信息包括（但不限于）以下：

1) 组织名称，组织法人，隶属关系；

2) 联系人，联系方式(包括：电话、传真、手机)；

3) 组织地址(包括：注册地址、认证地址)；

4) 体系覆盖人数；

5) 认证范围变化；

6) 组织机构和职能分配；

7) 证书表述的组织认证场所/生产场所；

8) 管理体系文件。

当上述信息发生变更时，获证客户应填写《认证证书变更申请书》，并及时反馈给ISC。

12 认证要求变更的条件和程序

12.1 认证要求变更的条件

1) 获证客户保持认证资格有效；

2) 认证要求变更应在规定的时间前完成；

3) 申请认证要求变更的获证客户应提交认证要求变更需求申请，并提交按新的认证要求进行体系调整的证据；

4) 获证客户的管理体系已满足新的认证要求,且已正常运行。

12.2 认证要求变更的程序

1) 在认证要求变更转换期结束前，获证客户向ISC提出认证要求变更申请；提出申请日期宜在转换期截止前至少90天；

2) ISC 通过对获证客户实施年度监督审核或再认证审核，或应获证客户要求安排的认证要求变更的专项审核，评审调整后的管理体系对认证要求的符合性、适宜性和有效性；

3) 经 ISC 审定，认为获证客户已满足批准认证资格的条件，同意批准认证范围，换发认证证书或附件，收回原证书，认证证书的注册号和有效期保持不变。

13 受理转换认证证书

本机构履行社会责任，严禁以牟利为目的受理不达到 ISO/IEC 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》标准和本认证规则要求、不能有效执行信息安全管理体系认证要求的组织申请认证证书的转换。当监管部门有要求时，按照监管部门要求进行证书转换，暂时无转换要求的，按初次认证进行受理。

14 与获证组织间的信息交换

14.1 当获证组织发生以下情况时，应向本机构及时通报：

(1)可能影响管理体系持续满足认证标准要求能力的事宜及变更通知本机构包括(但不限于)与下列方面有关的变更：

a)法律地位、经营状况、组织状态或所有权；

b)组织和管理层(如关键的管理、决策或技术人员)；

c)联系地址和场所；

d)获证管理体系覆盖的运作范围：

e)管理体系和过程的重大变更

(2)发生任何重大事故；

(3)发生任何违法行为；

(4)产品/服务严重不合格或被监管部门认定不符合法定要求：

(5)被列入信用信息严重失信名单；

(6)行政许可资格、强制性认证或其他资质变更或失效。

14.2 当管理标准或相关认证认可规范、法规的要求发生变化并涉及到获证组织时，ISC将采取网站公告、电话、邮件、信函等方式及时通知获证客户，需要时在合同中做出安排并验证获证组织是否符合新的要求。

15 保密

ISC 承诺为认证客户保密（提前告知认证客户的需公开信息除外）。对认证客户的保密信息如需公开或向第三方提供时，将拟提供的信息提前通知认证客户（法律限制除外）。

如有证据表明，ISC因认证接触受审核方的商业、技术秘密，而泄露给第三者（法律规定除外），承担相应法律责任。

在认证审核之前，ISC要求客户报告是否存在因包含保密信息或敏感信息而导致不能提供给审核组审查的 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）。ISC会确定是否能在缺少这些信息的情况下对 ISMS 进行充分审核。如果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，ISC会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。

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

ISC审核组成员不在审核过程中以任何方式记录客户的保密或敏感信息；审核组在离开客户前，接受或主动请客户检查和确认审核组携带的文件、资料和设备中未夹带客户的任何保密或敏感信息。

16 申诉/投诉、争议及处理

对 ISC 或审核人员违反国家认证法律、法规、认可机构有关规定、缺乏公正性及对认证的评价结果等有异议时，可以向ISC提出申诉、投诉。

ISC 将在30日内答复处理情况。

对ISC申诉/投诉和争议的处理有异议时可向中国合格评定国家认可委员会、中国国家认证认可监督管理委员会等有关部门进一步申诉/投诉。

17 公告

对获得认证、暂停、恢复或撤销的认证客户，在ISC网站上公布可查询。

附录 A:信息安全管理体系审核时间的要求

A.1 确定初次认证审核时间

A.1.1 确定远程审核

如果使用了远程审核技术（例如：基于网络的交互式协作、网络会议、电话议和/或电子验证组织的过程）与客户组织接触，可以考虑将其作为现场审核时间的一部分。应在审核计划中加以识别。

A.1.2 确定初始人数

审核方案管理岗根据客户提供与大量人员从事某些相同活动有关的信息（包括：从事该活动的人数；活动或过程的类型），确定初始人日数。因人员从事某些相同活动而减少作为审核时间计算基础的人数的示例包括:

——履行职责时对信息只有读取访问权限的人员；

——不能使用组织 ISMS 范围内的信息处理设施的人员；

——对组织 ISMS 范围内的信息处理设施具有明确且可证实的受限访问权限的人员；

——在有严格限制以防信息泄露的场所工作的人员，例如采取措施禁止个人物品和设备进入工作区域。

审核方案管理岗应根据与工作任务相关的活动的风险来减少从事相同活动的人数。对实施每项相同活动的人数 开平方根，然后将其四舍五入取整，得到用于计算审核时间的有效人数。该数值是允许减少到的最小值。工作任务的性质、法规要求以及组织人员可访问信息的重要性能限制这种减少。经由本过程确定的人数是表1 中确定审核时间的起点。

A.1.3 ISMS审核基准人日数

ISC按照CNAS-CC170要求，制定了信息安全管理体系的基础人日(见表1)。审核方案管理岗依据A.2确定的初始人数，参照 表1 对每一申请ISMS认证项目（包括：初次认证、监督审核和再认证）所需的审核时间进行核算。

表 1--信息安全管理体系员工有效人数与审核时间的关系

在组织控制下工作的人员的数量	审核时间				在组织控制下工作的人员的数量	审核时间		
	初次认证	监督审核	再认证			初次认证	监督审核	再认证
1～10	5	2	3.5		876～1175	18.5	6.5	12.5
11～15	6	2	4		1176～1550	19.5	6.5	13
16～25	7	2.5	5		1551～2025	21	7	14
26～45	8.5	3	6		2026～2675	22	7.5	15
46～65	10	3.5	7		2676～3450	23	8	15.5
66～85	11	4	7.5		3451～4350	24	8	16
86～125	12	4	8		4351～5450	25	8.5	17
126～175	13	4.5	9		5451～6800	26	9	17.5
176～275	14	5	9.5		6801～8500	27	9	18

在组织控制下工作的人员的数量	审核时间		
	初次认证	监督审核	再认证
276～425	15	5	10
426～625	16.5	5.5	11
626～875	17.5	6	12

在组织控制下工作的人员的数量	审核时间		
	初次认证	监督审核	再认证
8501～10700	28	9.5	19
＞10700	延用以上规律		

A.1.4 审核时间调整因素

审核方案管理岗根据ISMS的复杂性、ISMS范围内开展业务的类型、客户规模以及分包方信息开发程度、以及ISMS涉及的场所及灾难恢复场所的数量等信息对审核时间进行调整。

所安排的审核时间考虑以下与ISMS复杂程度和ISMS审核工作量相关的因素：

一与 ISMS 的复杂程度有关因素(如开发项目的数量和规模，远程工作的范围，ISMS 的风险状况等)；

一在 ISMS 范围内开展的业务类型；

一以往已证实的 ISMS 绩效；

一在 ISMS 各部分的实施过程中，所应用的技术的水平和多样性（例如，不同 IT 平台的数量、 隔离网络的数量；

一ISMS范围内所使用的外包和第三方安排的程度；

一信息系统开发的程度；

一场所的数量和灾难恢复场所的数量；

一第一阶段之后，认证机构将考虑控制的数量和复杂性；

一对于监督或再认证审核:符合CNAS-CC018.5.3条款的、与 ISMS 相关的变更的数量和程度；

需要增加审核时间的因素，例如：

a) 复杂的过程和后勤，ISMS 范围内涉及不止一处建筑物或地点；

b) 员工的语言不止一种（需要口译员或审核员个人无法独立工作），或提供的文件使用了多种 语言；

c) 为确认管理体系认证范围内永久场所的活动，需要访问临时场所的活动；（见下一列表之后 的段落）

d) 适用于 ISMS 的标准和法规数量很多。

允许减少审核时间的因素，例如：

a) 没有风险或者低风险的过程；

b) 过程只涉及单一的常规活动（例如，只有服务）；

c) 对组织已经有所了解（例如，如果组织获得了同一认证机构授予的另一个标准的认证）；

d) 客户的认证准备情况较好（例如，已经获得了另一个第三方认证方案的认证或承认）；

e) 高度成熟的管理体系。

f)在临时场所提供其产品或服务的情况。

A.1.5 对偏离审核时间的限制

为了确保能够实施有效的审核并确保可靠和可比较的结果，减少的时间不得超过**附录A中表1**所规定的审核时间的30%。任何经评审确定的审核人日及其增加或减少的理由应记录在《审核方案策划表》中。

A.1.6 现场审核时间

对于初次审核，其现场审核时间应不少于总审核时间的70%。

根据拟认证客户情况来确定第一阶段的审核人日，第一阶段的现场审核时间不低于1审核人日。

A.2 监督审核时间

原则上，监督审核的时间为初次审核时间的1/3。审核ISMS的变更（例如，审核新的或发生变更的信息安全控制、过程和服务），应增加监督审核时间。

A.3 再认证审核的时间

原则上，再认证审核的时间是同一组织初次认证审核时间的2/3。

A.4 多场所的审核时间

具体参见《多场所组织认证管理》文件。

A.5 扩大认证范围的审核时间

扩大 ISMS 范围所需的审核时间应考虑以下因素:

a) 扩大的类型;

b) 当前的认证活动;

c) 开展活动的地点的数量;

d) 与活动相关的信息安全风险;

e) 与所扩范围相关的控制的数量;

f) 所扩范围内、在组织控制下工作的人数;

g) 审查将所扩范围整合到 ISMS 时所需时间。

对于所扩范围的初次审核，审核时间应根据在当前认证范围内增加的人员和场地的数量。扩大 ISMS 范围所需的审核时间，应增加到审查客户获证 ISMS 所需的审核时间中。当扩大范围 审核是结合监督审核或再认证审核进行时，应至少增加为 0.5 天(审核人日)；当扩大范围审核是单独进行时，相应的时间应至少为 1.0 天(审核人日)。

A.6 结合审核

如结合其他管理体系实施一体化审核时，结合审核总人日数不宜少于每一个单一管理体系相加的总人日数的80%。

A.7 审核时间计算方法

表 1 提供了审核策划应使用的框架。该表基于在组织控制下工作的、所有班次的人员的总数 来确定审核时间的起点。根据适用于待审核 ISMS 范围的重要因素来调整审核人日数：通过对每个因 素赋予增减权重来修改基数。

A.7.1 审核时间计算因数的分类

表2中列举了主要的审核时间计算因数的分级示例，用作审核时间计算的基础。

表2 审核时间计算因数的分级

对工作量的影响 / 因数	减少工作量	正常工作量	增加工作量
a）ISMS的复杂性： 信息安全要求[保密性、完整性和可用性，（CIA）] 关键资产的数量 过程和服务的数量	只有少量的敏感信息或保密信息，可用性要求低； 很少的关键资产（根据CIA）； 只有一个关键业务过程，该过程的接口和涉及的业务单元很少。	较高的可用性要求或若干敏感/保密信息； 若干关键资产； 2-3个简单的业务过程，这些过程的接口和涉及的业务单元很少。	比较多的保密信息或敏感信息（例如，健康、个人可识别信息、保险、银行），或可用性要求高； 很多关键资产 超过2个复杂的过程，这些过程的接口和涉及的业务单元很多。
b）ISMS范围内所开展的业务的类型	低风险的业务，没有法规要求	法规要求高	高风险的业务，有（仅有）有限的法规要求
c）以往已证实的ISMS绩效	最近刚获得认证； 没有获得认证，但ISMS已充分实施了多个审核与改进周期，包括文件化的内部审核，管理评审和有效的持续改进体系。	最近刚通过监督审核； 没有获得认证，但部分实施了ISMS：获得并实施了一些管理体系工具，一些持续改进过程是适宜的但未全部文件化。	未获得认证且最近未接受审核； ISMS是新的且没有完全建立（例如：缺少管理体系的特定控制机制，不成熟的持续改进过程，特别的过程执行）。
d）在ISMS各部分的实施过程中，所应用的技术的水平和多样性（例如，不同IT平台的数量、隔离网络的数量）	高标准化、低多样性的环境（很少的IT平台、服务器、操作系统、数据库、网络等）。	标准化且多样性的IT平台、服务器、操作系统、数据库和网络。	高多样性或复杂的IT环境（例如，很多不同的网段、服务器或数据库的类型、关键应用的数量）
e）ISMS范围内所使用的外包和第三方安排的程度	没有外包且对供应商的依赖较小； 对外包协议进行了明确的规定、良好的管理与监视； 外包方获得了ISMS认证； 可获得相关的独立担保报告。	多个管理不充分的外包协议。	高度依赖外包或供应商，它们对重要业务活动有很大影响； 对外部的数量或程度不清楚； 多个未得到管理的外包协议。
f）信息系统开发的程度	没有内部的系统开发； 使用标准化的软件平台	使用标准化的、具有复杂配置/参数化的平台； （高度）定制软件； 若干开发活动（内部的或外包的）。	大量的内部软件开发活动，有若干正在实施的、针对重大业务目的的项目。
g）场所的数量和灾难恢复场所的数量	较低的可用性要求，且没有或有一个可选的灾难恢复场所。	中等或高的可用性要求，且没有或有一个可选的灾难恢复场所。	高可用性要求，例如7×24服务； 若干个可选的灾难恢复场所； 若干个数据中心。
h）控制的数量和复杂性	控制数量比平常的少，不包括一些常见的控制域。例如，没有系统开发控制或没有物理控制。	控制数量和复杂性是平常的。	数量比平常的多且详细和复杂的控制，例如，许多与网络协议或密码相关的控制。
i）对于监督或再认证审核：符合CNAS-CC01-2017 8.5.3条款中所述的ISMS相关变更的数量和程度。	自上次再认证审核后未发生变化。	ISMS的范围或适用性声明有微小的变化，例如，一些策略、文件发生变化； 以上因素有微小变化；	ISMS的范围或适用性声明有重大变化，例如，新的过程，新的业务单元、区域、风险评估管理方法、策略，文件、风险处置。 以上因素有重大变化。

A.7.2 审核时间计算的方法与示例

第一步：确定与业务和组织相关的（非IT）因数（见表3）。识别表3中每个类别的适宜分值，并对结果求和；

第二步：确定与IT环境相关的因数（见表4）。识别表4中每个类别的适宜分值，并对结果求和；

第三步：基于以上第一步和第二步的结果，通过选择表表5中的适宜条目，识别这些因数对审核时间的影响；

第四步：最终计算。将由审核时间表1所确定审核人天数乘以第三步中得出的系数。当使用多场所抽样时，要将实施多场所抽样计划所需的工作量增加所计算出的审核人天。

这个结果是最终需要调整的审核人天数。

表3 与业务和组织（非IT）相关的因数

类别	分值
业务类型和法规要求	1） 组织所处的是一个非关键业务领域，且不受管制的领域； 2） 组织的客户处于关键业务领域； 3） 组织处于关键业务领域。
过程与任务	1） 标准过程，标准任务，很少的产品或服务； 2） 标准的但不重复的过程，涉及大量的产品或服务； 3）复杂的过程，大量的产品和服务，许多业务单元包含在认证范围内（ISMS 有复杂性高的过程，或相对较多的独特活动）。
管理体系的建立水平	1） 已经很好地建立了 ISMS，和（或）存在其他管理体系； 2） 其他管理体系的要素，有些已经实施，有些没有实施； 3） 根本没有实施其他管理体系，ISMS 是新的且尚未建立。

注：关键业务领域是能影响关键公共服务的领域，这些公共服务将引起健康、安全、经济、信誉和政府履职能力的风险，从而可能对国家造成非常重大的负面影响。

表4与IT环境相关的因数

类别	分值
IT 基础设施的复杂程度	1）很少的或高度标准化的 IT 平台、服务器、操作系统、数据库、网络等； 2）多个不同的 IT 平台，服务器、操作系统、数据库、网络； 3）很多不同的 IT 平台、服务器、操作系统、数据库、网络。
对外包和供应商（包括云服务）的依赖程度	1） 很少或不依赖外包或供应商； 2)有些依赖外包或供应商，这些外包或供应商与某些重要业务活动相关，但不是与所有的重要业务活动相关； 3）高度依赖外包或供应商，外包或供应商对重要业务活动有着很大影响。
信息系统开发	1）没有或非常有限的内部系统/应用开发； 2）有一些服务于某些重要业务目的的、内部的或外包的系统/应用开发； 3）有大量服务于重要业务目的的、内部的或外包的系统/应用开发。

表 5 因数对审核时间的影响

IT 复杂性 业务复杂性	低 （3～4）	中 （5～6）	高 （7～9）
高 （7～9）	+5%～+20%	+10%～+50%	+20%～+100%
中 （5～6）	-5%～-10%	0%	+10%～+50%
低 （3～4）	-10%～-30%	-5%～-10%	+5%～+20%

示例 1：

受审核的组织有 700 人，因此根据表-1，其初次认证审核需要 17.5 人天。该组织不属于关键业务领域，从事高度标准化和重复性的任务且刚建立 ISMS。根据表-3，得出与业务和组织相关的因数为 1+1+3=5。该组织具有非常 少的 IT 平台和数据库，但大量地使用外包。该组织没有内部的或外包的开发活动。根据表-4，得出与 IT 环境相关 的因数为 1+3+1=5。利用表-5，可以得出该审核时间无需调整。

示例 2： 还是示例 1 中的这个组织，但其已有多个管理体系且已较好地建立了 ISMS。根据表-3，与业务和组织相关的 因数将变为：1+1+1=3。根据表-5，将得出需要减少 5%∽10%的审核时间，即：审核时间将减少 1 到 1.5 人天，变 为 16 到 16.5 人天。

附 件

文件更改记录

序号	版次	更改内容	编制/修改人	审批人	批准日期
1	A/0	全文发布	技术部	刘达军	2025-11-20