信息安全管理体系认证规则

（B/1 版）

2023-4-11 发布 · 实施

信息安全管理体系认证规则

目　录

1. 适用范围 3
2. 对认证机构的基本要求 3
3. 对认证审核人员的基本要求 4
4. 初次认证程序 4
5. 监督审核程序 16
6. 再认证程序 19
7. 暂停或撤销认证证书 21
8. 认证证书要求 23
9. 与其他管理体系的结合审核 25
10. 受理转机构认证证书 25
11. 受理组织的申诉和投诉 26
12. 认证记录的管理 26
13. 其他 27
附录 A　信息安全管理体系认证审核时间要求 28

1. 适用范围

1.1 本规则用于规范依据 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》标准在中国境内开展的信息安全管理体系认证活动。

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，对信息安全管理体系认证实施过程作出具体规定，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 本规则是认证机构在信息安全管理体系认证活动中的基本要求，相关部门、分公司、人员在该项认证活动中应当遵守本规则。

2. 对认证机构的基本要求

2.1 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。

2.2 认证能力、内部管理和工作体系符合 GB/T 27021-1/ISO/IEC 17021.1《合格评定　管理体系审核认证机构要求》和 CNAS-CC170《信息安全管理体系认证机构要求》。

2.3 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。

2.4 条件成熟时，认证机构通过国家认监委指定或承认的认可机构的认可，证明认证能力、内部管理和工作体系符合 GB/T 27021-1/

ISO/IEC 17021.1《合格评定　管理体系审核认证机构要求》和CNAS-CC170《信息安全管理体系认证机构要求》。

2.5 不得将受审核组织是否通过认证与认证审核的审核员及其他工作人员的薪酬挂钩。

3. 对认证审核人员的基本要求

3.1 认证审核员应当取得国家认监委承认的认证人员注册机构颁发的信息安全管理体系审核员注册资格。

3.2 认证人员应当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. 初次认证程序

4.1 受理认证申请

4.1.1 认证机构应向申请组织至少公开以下信息：

（1）可开展认证业务的范围，以及获得认可的情况。

（2）本规则的完整内容。

（3）认证证书样式。

（4）对认证过程的申诉、投诉处理规定。

4.1.2 认证机构应当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。

（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）信息安全管理体系成文信息（适用时）。

4.1.3 认证机构应对申请组织提交的申请资料进行评审，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，综合确定是否有能力受理认证申请。

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”的申请组织，认证机构不应受理其认证申请。

4.1.4 对符合 4.1.2、4.1.3 要求的，认证机构可决定受理认证申请；对不符合上述要求的，认证机构应通知申请组织补充和完善，或者不受理认证申请。

4.1.5 签订认证合同

在实施认证审核前，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政府主管部门认定不合格。

③发生产品和服务的信息安全安全事故。

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。

4.2 审核策划

4.2.1 审核时间

4.2.1.1 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。在特殊情况下，可以减少审核时间，但减少的时间不得超过附录 A 所规定的审核时间的 30%。

4.2.1.2 整个审核时间中，现场审核时间不应少于总审核时间的 80%。

4.2.2 审核组

4.2.2.1 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。

4.2.2.2 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。

4.2.2.3 审核组可以有实习审核员，实习审核员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。

4.2.3 审核计划

4.2.3.1 认证机构应为每次审核制定书面的审核计划（非现场第一阶段审核不要求正式的审核计划）。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：审核员应标明认证人员注册号；技术专家应标明专业代码、工作单位及专业技术职称）。

4.2.3.2 如果信息安全管理体系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，认证机构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，应当逐一到各现场进行审核。

4.2.3.3 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。

4.2.3.4 在审核活动开始前，审核组应将审核计划交受审核组织和认证机构确认，遇特殊情况临时变更计划时，应及时将变更情况通知受审核组织和认证机构，并协商一致。

4.3 实施审核

4.3.1 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。

4.3.2 审核组应当会同受审核组织按照程序顺序召开首、末次会议，受审核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。

4.3.3 审核过程及环节

4.3.3.1 初次认证审核，分为第一、二阶段审核。

4.3.3.2 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描述的一致性，特别是体系成文信息中描述的产品和服务、部门设置和职责与权限、生产或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《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。

4.3.3.3 在下列情况，第一阶段审核可以不在受审核组织现场进行（即非现场审核），但认证机构应记录和批准非现场审核的原因（至少具备以下情形之一）：

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

（2）认证机构有充足的理由证明受审核组织的生产经营或服务的技术特征明显、过程简单，通过对其提交文件和资料的审查可以达到第一阶段审核的目的和要求；

（3）受审核组织获得了其他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组织的生产经营或服务现场进行。

4.3.3.4 远程审核属于现场审核中的特例，当同时具备下列情形时，第一阶段审核可以远程审核（完全远程审核、或部分远程审核、或现场远程审核）：

（1）认证机构有充足的理由证明受审核组织的拟认证范围属于中、低风险（或二、三级复杂程度）；

（2）拟审核期间，认证机构及相关审核员所在地、或受审核组织所在地发生了疾病流行、或战乱、或恐怖活动、或重大自然灾害、或交通管制限制出行等。

4.3.3.5 审核组应将第一阶段审核情况形成书面文件告知受审核组织和申请组织（当申请方、受审核方不是同一组织时）。对在第二阶段审核中可能被判定为不符合项的重要关键点，要及时提醒受审核组织特别关注。

4.3.3.6 第二阶段审核应当在受审核组织现场进行。重点是审核信息安全管理体系符合 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》标准要求和有效运行情况，应至少覆盖以下内容：

（1）在第一阶段审核中识别的重要审核点的过程控制的有效性。

（2）为实现信息安全方针而在相关职能、层次和过程上建立信息安全目标是否具体适用、可测量并得到沟通、监视。

（3）对信息安全管理体系覆盖的过程和活动的管理及控制情况。

（4）受审核组织实际工作记录是否真实。对于审核发现的真实性存疑的证据应予以记录并在做出审核结论及认证决定时予以考虑。

（5）受审核组织的内部审核和管理评审是否有效。

4.3.3.7 远程审核属于现场审核中的特例，当同时具备下列情形时，第二阶段审核可以部分远程审核：

（1）认证机构有充足的理由证明受审核组织的拟认证范围属于中、低风险（或二、三级复杂程度），或信息安全管理体系的非专业要素部分；

（2）拟审核期间，认证机构及相关审核员所在地、或受审核方所在地发生了疾病流行、或战乱、或恐怖活动、或重大自然灾害、或交通管制限制出行等。

4.3.4 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。

4.4 审核报告

4.4.1 审核组应对审核活动形成书面审核报告，由审核组组长签字。审核报告应准确、简明和清晰地描述审核活动的主要内容，至少包括以下内容：

（1）受审核组织的名称和地址。

（2）受审核组织活动范围和场所。

（3）审核的类型、准则和目的。

（4）审核组组长、审核组成员及其个人注册信息。

（5）审核活动的实施日期和地点，包括固定现场和临时现场；对偏离审核计划情况的说明，包括对审核风险及影响审核结论的不确定性的客观陈述。

（6）叙述从 4.3 条列明的程序及各项要求的审核工作情况，其中：对 4.3.3.6 条的各项审核要求应逐项描述或引用审核证据、审核发现和审核结论；对信息安全目标和过程及信息安全绩效实现情况进行评价。

（7）识别出的不符合项。

（8）审核组对是否通过认证的意见建议。

4.4.2 认证机构应保留用于证实审核报告中相关信息的证据。

4.4.3 认证机构应在作出认证决定后 30 个工作日内，将认证机构批准的审核报告提交受审核组织和申请组织（当申请方、受审核方不是同一组织时），并由认证机构保留签收或提交的证据。

4.4.4 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，认证机构应将此报告及终止审核的原因提交给受审核组织和申请组织（当申请方、受审核方不是同一组织时），并由认证机构保留签收或提交的证据。

4.5 不符合项的纠正和纠正措施及其结果的验证

4.5.1 对审核中发现的不符合项，审核组应要求受审核组织分析原因，并由受审核组织提出和实施纠正和纠正措施。对于一般不符合，审核组应要求受审核组织在最多不超过 1 个月期限内（法定节日可以顺延几天）采取纠正和纠正措施。对于严重不符合，审核组应要求受审核组织在最多不超过 6 个月期限内（日历天数）采取纠正和纠正措施。认证机构或审核组长/组员（必要时，由技术专家支持）应对受审核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最长 6 个月内（日历天数）验证对严重不符合实施的纠正和纠正措施，则应按 4.6.5 条进行终止处理，或者按照 4.3.3.5 条重新实施第二阶段审核。

4.6 认证决定

4.6.1 认证机构应该在对审核报告、不符合项的纠正和纠正措施及其结果进行综合评价基础上，作出认证决定。

4.6.2 认证决定人员应为认证机构管理控制下的人员（具备能力的工作人员或审核员），审核组成员不得对自己参与审核项目的认证决定。

4.6.3 认证机构在作出认证决定前应确认如下情形：

（1）审核报告符合本规则第 4.4 条要求，审核组提供的审核报告及其他信息能够满足作出认证决定所需要的信息。

（2）反映以下问题的不符合项，认证机构已评审、接受并验证了纠正和纠正措施的有效性。

①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。

②制定的信息安全目标不可测量、或测量方法不明确。

③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。

④其他严重不符合项。

（3）认证机构对其他一般不符合项已评审，并接受了受审核组织计划采取的纠正和纠正措施。

4.6.4 在满足 4.6.3 条要求的基础上，认证机构有充分的客观证据证明受审核组织满足下列要求的，评定该受审核组织符合认证要求，向其颁发认证证书。

（1）受审核组织的信息安全管理体系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）受审核组织和申请组织（当申请方、受审核方不是同一组织时）按照认证合同规定履行了相关义务。

4.6.5 受审核组织不能满足上述要求或者存在以下情况的，评定该受审核组织不符合认证要求，以书面形式告知受审核组织和申请组织（当申请方、受审核方不是同一组织时）并说明其未通过认证的原因。

（1）受审核组织的信息安全管理体系有重大缺陷，不符合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》标准的要求。

（2）发现受审核组织存在重大信息安全安全问题或有其他与产品和服务信息安全相关严重违法违规行为。

4.6.6 认证机构在颁发认证证书后，当月的认证证书不得迟于次月 10 日前（法定节假日不得顺延）按照规定的要求将认证结果相关信息报送国家认监委。

5. 监督审核程序

5.1 认证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并符合认证要求。

5.2 为确保达到 5.1 条要求，认证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。

5.2.1 作为最低要求，初次认证后的第一次监督审核应在认证决定之日（与认证证书签发日相同）起 12 个月内（日历天）进行。此后，监督审核应至少每个日历年（应进行再认证的年份除外）进行一次，且两次监督审核的时间间隔不得超过 15 个月。

5.2.2 超过期限而未能实施监督审核的，应按 7.2 或 7.3 条处理。

5.2.3 获证组织的产品及生产服务过程在国家监督抽查中被查出信息安全不合格时，自国家相关部门发出通报起 30 日内，认证机构应对该组织实施加密监督审核。

5.3 监督审核的时间，应不少于按 4.2.1 条计算审核时间人日数的 1/3。

5.4 监督审核的审核组，应符合 4.2.2 条和 4.3.1 条的要求。

5.5 监督审核应在获证组织现场进行，且应满足第 4.2.3.3 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。

5.6 远程审核属于现场审核中的特例，当同时具备下列情形时，监督审核可以远程审核（完全远程审核、部分远程审核、现场远程审核）：

（1）上次审核（上次可能是初审 2 阶段，可能是监督，可能是再认证审核等）采用的是完全现场审核或部分远程审核；

（2）认证机构有充足的理由证明受审核组织的拟认证范围属于中、低风险（或二、三级复杂程度），或信息安全管理体系的非专业要素部分；

（3）拟审核期间，认证机构及相关审核员所在地、或受审核方所在地发生了疾病流行、或战乱、或恐怖活动、或重大自然灾害、或交通管制限制出行等。

5.7 监督审核时至少应审核以下内容：

（1）上次审核以来信息安全管理体系覆盖的活动及影响体系的重要变更及运行体系的资源是否有变更。

（2）按 4.3.3.2（4）条要求已识别的重要关键点是否按信息安全管理体系的要求在正常和有效运行。

（3）对上次审核中确定的不符合项采取的纠正和纠正措施是否继续有效。

（4）信息安全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。

（5）信息安全目标及信息安全绩效是否达到信息安全管理体系确定值。如果没有达到，获证组织是否运行内审机制识别了原因、是否运行管理评审机制确定并实施了改进措施。

（6）获证组织对认证标志的使用或对认证资格的引用是否符合《认证认可条例》及其他相关规定。

（7）内部审核和管理评审是否规范和有效。

（8）是否及时接受和处理投诉。

（9）针对体系运行中发现的问题或投诉，及时制定并实施了有效的改进措施。

5.8 在监督审核中发现的不符合项，审核组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。

5.9 审核组应对监督审核活动形成书面审核报告，由审核组组长签字。监督审核的审核报告，应按 5.7 条列明的审核要求逐项描述或引用审核证据、审核发现和审核结论。

5.10 认证机构根据监督审核报告及其他相关信息，作出继续保持或暂停、撤销认证证书的决定。

5.11 对于描述为信息安全管理体系持续有效，且没有开具不符合项报告的监督审核报告，认证机构可以免于评审，直接决定予以保持，并发出保持通知书和保持标识贴花。

5.12 对于描述为信息安全管理体系持续有效，但又开具不符合项报告的监督审核报告，认证机构应由认证决定人员（应为认证机构管理控制下的人员）（具备能力的工作人员或审核员）进行评审，审核组成员不得对自己参与审核项目的评审。

6. 再认证程序

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

6.2 认证机构应按 4.2.2 条和 4.3.1 条要求组成审核组。按照 4.2.3 条要求并结合历次监督审核情况，审核组长制定再认证审核计划交审核组实施。

在信息安全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按 4.2.1 条计算人日数的 2/3。

6.3 当发生下列情况之一时，再认证前应进行一阶段审核：

（1）获证组织的生产工艺发生重大变化；

（2）获证组织的组织架构、管理体系文件发生重大变化；

（3）启动再认证工作时间不当，已经明显可以预料不能在原认证证书到期前完成全部再认证工作（包括完成对纠正与纠正措施的验证、颁发出新的证书）。

6.4 对再认证审核中发现的不符合项，认证机构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。

6.5 认证机构按照 4.6 条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。

6.6 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，否则应至少再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。

7. 暂停或撤销认证证书

7.1 认证机构应制定暂停、撤销认证证书或缩小认证范围的规定和文件化的管理制度，规定和管理制度应满足本规则相关要求。认证机构对认证证书的暂停和撤销处理应符合其管理制度，不得随意暂停或撤销认证证书。

7.2 暂停证书

7.2.1 获证组织有以下情形之一的，认证机构应在调查核实后的 5 个工作日内暂停其认证证书。

（1）信息安全管理体系持续或严重不满足认证要求。

（2）不承担、履行认证合同约定的责任和义务的。

（3）被有关执法监管部门责令停业整顿的。

（4）持有的与信息安全管理体系范围有关的行政许可证明、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的。

（5）主动请求暂停的。

（6）其他应当暂停认证证书的。

7.2.2 认证证书暂停期不得超过 6 个月。但属于 7.2.1 第（4）项情形的暂停期可至相关单位作出许可决定之日。

7.2.3 认证机构应以适当方式公开暂停认证证书的信息，明确暂停的起始日期和暂停期限，并声明在暂停期间获证组织不得以任何方式使用认证证书、认证标识或引用认证信息。

7.3 撤销证书

7.3.1 获证组织有以下情形之一的，认证机构应在获得相关信息并调查核实后 5 个工作日内撤销其认证证书。

（1）被注销或撤销法律地位证明文件的。

（2）被国家市场监督管理总局列入严重失信企业名单

（3）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的。

（4）拒绝接受国家行政监督抽查的。

（5）出现重大信息安全安全事故，经执法监管部门确认是获证组织违规造成的。

（6）有其他严重违反法律法规行为的。

（7）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的（包括持有的与信息安全管理体系范围有关的行政许可证明、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）。

（8）没有运行信息安全管理体系或者已不具备运行条件的。

（9）不按相关规定正确引用和宣传获得的认证信息（如：获得信息安全管理体系认证的组织，宣传其获得了产品认证、服务认证、CCC 认证），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 个月仍未纠正的。

（10）其他应当撤销认证证书的。

7.3.2 撤销认证证书后，认证机构应及时收回撤销的认证证书。若无法收回，认证机构应及时在相关媒体和网站上公布或声明撤销决定。

7.4 认证机构暂停或撤销认证证书应当在认证机构的公开网站上公布相关信息，同时按规定程序和要求报国家认监委。

7.5 认证机构应采取有效措施避免各类无效的认证证书和认证标志被继续使用。

8. 认证证书要求

8.1 认证证书应至少包含以下信息：

（1）获证组织名称、注册地址和统一社会信用代码。该信息应与其法律地位证明文件的信息一致。

（2）信息安全管理体系覆盖的生产经营或服务的地址和业务范围。若认证的信息安全管理体系覆盖多场所，表述覆盖的相关场所的名称和地址信息。

（3）信息安全管理体系符合 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》标准的表述。

（4）证书编号。

（5）认证机构名称。

（6）有效期的起止年月日。

证书应注明：获证组织必须定期接受监督审核并经审核合格此证书方继续有效的提示信息。

（7）相关的认可标识及认可注册号（适用时）。

（8）证书查询方式。认证机构除公布认证证书在本机构网站上的查询方式外，还应当在证书上注明：“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”，以便于社会监督。

8.2 初次认证的信息安全管理体系认证证书有效期最长为 3 年。再认证的认证证书有效期不超过最近一次有效认证证书截止期再加 3 年。

8.3 认证机构应当建立证书信息披露制度。除向获证组织、申请组织、认证监管部门等执法监管部门提供认证证书信息外，还应当根据社会相关方的请求向其提供证书信息，接受社会监督。

9. 与其他管理体系的结合审核

9.1 对信息安全管理体系和其他管理体系实施结合审核时，通用或共性要求应满足本规则要求，审核报告中应清晰地体现 4.4 条要求，并易于识别。

9.2 结合审核的审核时间人日数，不得少于多个单独体系所需审核时间之和的 80%。

10. 受理转机构认证证书

10.1 认证机构应当履行社会责任，严禁以牟利为目的受理不符合 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》标准、不能有效执行信息安全管理体系的组织的认证证书的转换。

10.2 认证机构受理组织申请转换为本机构的认证证书，应该详细了解申请转换的原因，并报认证认可业务信息统一上报平台同意后，认证机构通过文件评审决定换发证书，必要时进行现场审核后决定换发证书。

10.3 转换仅限于现行有效的信息安全管理体系认证证书。被暂停或正在接受暂停、撤销处理的认证证书以及已失效的认证证书，不得接受转换申请。

10.4 被发证的认证机构撤销证书的，除非该组织进行彻底整改，导致暂停或撤销认证证书的情形已消除，否则不应受理其认证申请。

11. 受理组织的申诉和投诉

申请组织、受审核组织或获证组织对认证决定有异议时，认证机构应接受申诉并且及时进行处理，在 60 个工作日内将处理结果形成书面通知送交申诉人。

书面通知应当告知申诉人，若认为认证机构未遵守认证相关法律法规或本规则并导致自身合法权益受到严重侵害的，可以直接向所在地认证监管部门或国家认监委投诉，也可以向相关认可机构投诉。

申请组织、受审核组织或获证组织对认证及其相关人员不满，认证机构应接受投诉并且及时进行处理，在 60 工作日内将处理结果形成书面通知送交投诉人。

当认证机构收到政府监管部门转办的投诉时，应及时开展调查、或配合调查，及时进行处理，并在政府监管部门要求的时限内将处理结果形成书面通知送交投诉人及政府监管部门。

12. 认证记录的管理

12.1 认证机构应当建立认证记录保持制度，记录认证活动全过程并妥善保存。

12.2 记录应当真实准确以证实认证活动得到有效实施。记录资料应当使用中文（必要时，中外文字对照），持续有效证书的认证记录的保存时间一般为当前认证周期和上一个认证周期。

12.3 以电子文档方式保存记录的，应采用不可编辑的电子文档格式存档（不能保留 Word、excel、PPT 文档作为认证档案）。

12.4 所有具有相关人员签字的书面记录，可以制作成电子文档保存使用，但是原件必须妥善保存，持续有效证书的认证资料签字记录的保存时间一般为当前认证周期和上一个认证周期。

13. 其他

13.1 本规则内容提及 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》标准时，均指认证活动发生时该标准的有效版本。认证活动及认证证书中描述该标准号时，应采用当时有效版本的完整标准号。

13.2 本规则所提及的各类证明文件的复印件应是在原件上复印的，并必须经审核员签字确认与原件一致。

13.3 认证机构可开展信息安全管理体系及相关技术标准的宣贯培训，促使组织的全体员工正确理解和执行信息安全管理体系标准。

附录 A

信息安全管理体系认证审核时间要求

表 B.1 给出了初次审核天数平均值的起点（在此处及后面的内容中，这个数值包括一次初次审核（第一阶段和第二阶段）的天数）。经验表明，对于一个覆盖了给定数量的、在组织控制下工作的人员的 ISMS 范围来说，这一数值是适当的。经验还表明，对于相似规模的 ISMS 范围，有些需要多的审核时间，有些需要少的审核时间。

表 B.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识别审核时间的起点，然后根据适用于所审核的 ISMS 范围的重要因素来调整它，并对每一个因素赋予增、减权重以修正基数。使用表 B.1 时应考虑促成因素和最大偏移的限制（见 B.3.4 和 B.3.5）。B.2 解释了表 B.1 中所使用的术语，附录 C 提供了如何计算审核时间的示例。

表 B.1 审核时间表

在组织控制下工作的人员的数量	QMS 初次审核审核时间（审核人日）	EMS 初次审核审核时间（审核人日）	ISMS 初次审核审核时间（审核人日）	增加或减少的因素	总审核时间
1 ~ 10	1.5-2	2.5-3	5	见本附录 B.3.4	
11 ~ 15	2.5	3.5	6	见本附录 B.3.4	
16 ~ 25	3	4.5	7	见本附录 B.3.4	
26 ~ 45	4	5.5	8.5	见本附录 B.3.4	
46 ~ 65	5	6	10	见本附录 B.3.4	
66 ~ 85	6	7	11	见本附录 B.3.4	
86 ~ 125	7	8	12	见本附录 B.3.4	
126 ~ 175	8	9	13	见本附录 B.3.4	
176 ~ 275	9	10	14	见本附录 B.3.4	
276 ~ 425	10	11	15	见本附录 B.3.4	
426 ~ 625	11	12	16.5	见本附录 B.3.4	
626 ~ 875	12	13	17.5	见本附录 B.3.4	

876 ~ 1175	13	15	18.5	见本附录 B.3.4	
1176 ~ 1550	14	16	19.5	见本附录 B.3.4	
1551 ~ 2025	15	17	21	见本附录 B.3.4	
2026 ~ 2675	16	18	22	见本附录 B.3.4	
2676 ~ 3450	17	19	23	见本附录 B.3.4	
3451 ~ 4350	18	20	24	见本附录 B.3.4	
4351 ~ 5450	19	21	25	见本附录 B.3.4	
5451 ~ 6800	20	23	26	见本附录 B.3.4	
6801 ~ 8500	21	25	27	见本附录 B.3.4	
8501 ~ 10700	22	27	28	见本附录 B.3.4	
＞ 10700	沿用 以上规律		沿用 以上规律	见本附录 B.3.4	

B.3.4 调整审核时间的因素

不能孤立地使用表 B.1。所安排的时间，还应考虑以下因素。这些因素与 ISMS 复杂程度相关，并因此与 ISMS 审核工作量相关。

a）ISMS 的复杂程度（例如，信息的关键程度、ISMS 的风险状况）；

b）ISMS 范围内所开展的业务的类型；

c）以往已证实的 ISMS 绩效；

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]；

e）ISMS 范围内所使用的外包和第三方安排的程度；

f）信息系统开发的程度；

g）场所的数量和灾难恢复场所的数量；

h）对于监督或再认证审核：符合 CNAS-CC01 8.5.3 条款的、与 ISMS 相关的变更的数量和程度。

附录 C 提供了在计算审核时间时如何考虑这些不同因素的示例。

需要增加审核时间的其他因素，例如：

a） 复杂的后勤，在 ISMS 范围中涉及不止一处建筑物或地点；

b) 员工所说的语言超过一种（需要翻译或审核员个人无法独立工作），提供的文件使用了一种以上的语言；

c) 为了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；

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产品/过程；

b) 过程只涉及单一的常规活动（例如，只有服务）；

c) 在组织控制下工作的雇员大部分是从事相同的任务；

d) 对组织已经有些了解（例如，如果组织获得了同一个认证机构的、另一个标准的认证）；

e) 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）；

f) 高度成熟的管理体系。

在认证客户或被获证组织在临时场所提供其产品或服务时，将对这类场所的评价纳入到认证审核和监督方案中是十分重要的。

宜考虑上述因素，并根据这些因素对审核时间做出调整。这些因素可证实一次有效审核所需更多或更少的审核时间的合理性。增加时间的因素可被减少时间的因素冲抵。在任何情况下，对审核时间表中的时间的调整，应保持足够的证据和记录来证实其变化的合理性。