江西腾标认证有限公司

信息安全管理体系认证规则

受控状态：（ 受控 ）

文件编号：TB-GZ-041

版本号：B/0

编制：技术部

审核：张辉根

批准：周春阳

发布日期：20260115　　生效日期：20260209

目录

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，签字确认与原件一致。

本公司可开展标准及相关技术标准的宣贯培训，促使组织全体员工正确理解和执行本标准。

1. 适用范围

1.1. 本规则用于规范依据 GB/T 22080-2025/ISO /IEC 27001:2022网络安全技术 信息安全管理体系 要求 标准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，明确江西腾标认证有限公司（以下简称：TB）对认证过程的管理责任，保证通过认证企业信息安全管理体系认证活动的规范有效。

1.3. 本规则是TB与申请获证组织在企业信息安全管理体系认证活动中的基本要求，TB在该项认证活动中应当遵守本规则。

2. 规则性引用文件

GB/T 22080-2025/ISO /IEC 27001:2022网络安全技术 信息安全管理体系 要求

注：本规则内容引用的文件提及的标准时，均指认证活动发生时该标准、规则规范的有效版本。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。

3. 术语和定义

采用上述规范性引用文件提出的术语和定义。

4. 对认证人员的要求

4.1. 认证审核员

应取得信息安全管理体系审核员注册证书，并通过了GB/T 22080-2025/ISO /IEC 27001:2022网络安全技术 信息安全管理体系 要求 相关标准培训，且考试合格，方可以实施云服务信息安全管理体系的认证审核。

4.2. 合同评审与审核策划人员

应取得任意一个管理体系审核策划和合同评审人员资格，并且通过 GB/T 22080-2025/ISO /IEC 27001:2022网络安全技术 信息安全管理体系 要求 考试合格，可以实施信息安全管理体系审核策划和合同评审。

4.3. 认证决定人员

应取得任意一个管理体系的认定决定资格，并且通过 GB/T 22080-2025/ISO /IEC 27001:2022网络安全技术 信息安全管理体系 要求 考试合格，方可实施认定决定。

注：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做出的认证审核报告、认证结论的真实性承担相应的法律责任。

5. 初次认证程序

5.1.受理认证申请

5.1.1. TB应向受审方至少公开以下信息：

(1) 可开展认证业务的范围，以及获得认可的（如有）情况。

(2) 本规则的完整内容。

(3) 认证证书样式。

(4) 对认证过程的申投诉规定。

5.1.2. TB应当要求受审方至少提交以下资料：

(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）。

(5) 依据 GB/T 22080-2025/ISO /IEC 27001:2022网络安全技术 信息安全管理体系 要求建立的信息安全管理体系成文信息。

(6) 当前未被行政监管部门责令停产停业整顿。

(7) 当前未列入“国家企业信用信息公示系统”和“信用中国”发布的严重违法失信名单。

5.2.申请评审

5.2.1.TB申请评审人员，应当对受审方的认证申请资料是否齐全进行确认，并对其有效性进行审查。

5.2.2.申请评审人员对申请方的认证申请进行评审并保持记录，以证明TB能够对拟实施认证的申请方完成以下工作：

（1） 明确申请的认证范围；

（2） 界定信息安全管理体系所覆盖的范围；

（3） 确定实施审核所需的能力；

（4） 考虑受审方申请的认证范围、场所及活动的复杂性，确定完成审核需要的审核时间。

（5） 体系运行三个月以上。

5.2.3.对符合5.1.2至5.1.4要求的，TB可决定受理认证申请；对不符合上述要求的，TB将通知申请方补充和完善，或者不受理认证申请。审核部应自申请之日起30日内通知申请人，说明理由并退回申请资料。对被执法监管部门责令停业整顿或被列入“国家企业信用信

息公示系统”和“信用中国”发布的严重失信主体相关名录的受审方，TB不受理其认证申请。

5.3.签订认证合同及相关责任

5.3.1. 认证合同

5.3.1.1.在实施认证审核前，TB审核部将对申请材料进行评审，审查确认受理认证申请后，由TB总经理或具有法人代表授权资格的人员签署与申请认证组织订立具有法律效力的书面认证合同《管理体系认证合同》，并签署。合同应至少包含以下内容：

(1) 获证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) 获证组织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) 获证组织承诺获得认证后发生以下情况时，应及时向TB通报。

① 获证组织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 发生产品和服务的质量安全事故；

④ 相关情况发生变更，包括但不限于：

a. 法律地位、生产经营状况、组织状态或所有权变更；

b. 取得的行政许可资格、强制性认证或其他资质证书变更；

c. 法定代表人、最高管理者变更；

d. 生产经营或服务的工作场所变更；

e. 信息安全管理体系覆盖的活动范围变更；

f. 信息安全管理体系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) 获证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，使其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活动范围。

(6) 在认证审核实施过程及认证证书有效期内，TB和获证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。

5.3.1.2.合同一经签字生效，双方必须认真执行。如签订合同的一方不能履行合同，提出后协商解决；若终止合同，则所产生的经济损失由责任方承担。

5.3.1.3.对签订的合同内容的任何变更，审核部应与申请组织签订补充协议。对变更申请进行评审通过后，将其作为合同附件由TB存档。该申请与原合同具有同等的法律效力。

5.3.2. 认证活动相关责任：

5.3.2.1.认证过程、活动引发的责任及处理由总经理负责做出安排。

(1) 属TB的责任

a.审核活动不符合认证标准和公司管理体系认证文件要求；

b.审核活动中发生违反科学性、公正性现象；

c.审核活动中审核人员违反审核纪律、发生泄密行为；

d.审核结论与事实不符；

e.违反认证合同的双方约定。

(2) 属于申请人（客户）的责任

a.申请的管理体系覆盖产品、过程范围、体系覆盖人数与现场提供的审核范围不符；

b.管理体系建立和运行未按认证标准要求和管理体系文件规定实施；

c.违反认证证书和认证标志的使用规定；

d.对认证审核中发生的不符合项不能按规定采取纠正和预防措施，使其满足认证要求；

e.违反认证合同书和双方约定。

5.3.2.2.TB和申请人（客户）关系、活动均应以双方签订的合同书为依据，涉及合同书范围以外的活动，须经双方商定，发生责任问题以书面文件为准，对确属公司的责任，由总经理做出具体安排，组织有关部门分析原因，制定纠正和纠正措施，并与申请人（客户）协商妥善解决。

5.4.审核方案和审核策划

5.4.1. 认证周期

TB依据 GB/T 19011《管理体系审核指南》等文件，根据风险和复杂程度策划整个认证周期：

5.4.1.1.初次审核

5.4.1.2.一监：认证决定后第一年的监督审核

5.4.1.3.二监：认证决定后第二年的监督审核

5.4.1.4.再认证：认证决定后第三年在认证到期前进行的再认证审核

5.4.1.5.特殊审核：包括已认可的认证转换审核、扩大认证范围审核、调查投诉审核、组织变更审核、认证要求变更审核等审核方案，以清晰地识别所需的审核活动。

5.4.2. 审核方案

审核方案的确定和任何后续调整应考虑受审方组织的规模，其管理体系、产品和过程的范围与复杂程度，以及经过证实的管理体系有效性水平和以前审核的结果。

5.4.2.1.审核方案应包括为审核的有效实施进行适当的策划、提供资源和制定程序。

5.4.2.2.审核方案应确定对受审方的多场所及临时场所的抽样计划（必要时）。

5.4.2.3.对于审核方案的确定和任何后续的调整贯穿于认证审核的全过程。

5.4.3. 审核时间

信息安全管理体系认证审核时间要求详见附录A。

5.4.4. 审核范围

5.4.4.1.TB根据受审方拟申请的或已获得认证的范围以及其审核时所提供的临时场所的业务范围，并结合组织行业或行政许可的范围如营业执照、行业资质证书的范围进行确定，通过现场审核活动进一步加以确认。

5.4.4.2.TB根据信息安全管理体系认证的特点，按照CNAS-TRC-012:2017《管理体系认证机构认证业务范围分类指南》的要求对认证业务范围进行分类管理。

5.4.5. 多场所抽样方案

原则上，认证的初次审核及后续的监督和再认证审核宜在组织认证范围内的每个场所进行。

5.4.5.1.通常情况下，组织总部在初次认证审核及后续的监督审核和再认证审核中都应接受审核。

5.4.5.2.分支机构（区域公司或分公司）

① 对于在组织总部的授权和控制之下、以相似的方式在不同的场所进行认证所覆盖的活动的分支机构，其抽样数量基于 CNAS-CC11《多场所组织的管理体系认证与审核》的规定。

② 对于开展不同业务活动或专业性质差异较大的业务活动的分支机构，宜根据组织的认证范围及其所涉及的不同业务活动和类别，分别对这类分支机构进行抽样审核。

5.4.5.3.临时场所

考虑一般风险活动的情况，本文件给出了每次审核至少抽取的临时场所数量。

① 初次认证审核：一般样本量应当为场所数量的平方根（$y=\sqrt{n}$），n 上入成整数。

② 监督审核：监督审核抽样量至少为 $0.6\times\sqrt{n}$，上入成整数；

③ 再认证审核：再认证审核抽样量至少为 $0.8\times\sqrt{n}$，上入成整数；n= 临时场所的数量。

5.4.5.4.值得注意的是，对于初次认证审核和再认证审核，基于上述方法抽取的临时场所的样本总量，应能完整覆盖组织管理体系下认证范围内所涉及的全部业务范围。对于监督审核而言，则宜根据组织的业务状况，在一个合理的时间内（如一个认证周期内）覆盖组织管理体系下认证范围内所涉及的全部业务范围。

5.4.6. 组建审核组

5.4.6.1.TB选择具备相关资格、能力和经验的审核员组成审核组，确保审核组具备与拟执行的审核任务相适宜的能力。

5.4.6.2.审核实施前，审核组应获得以下应用文件：

① 审核实施规范

② 审核方案策划文件

③ 审核任务书
④ 审核文件包
⑤ 受审方的体系文件
⑥ 获得指导审核实施的三级作业文件（必要时）
⑦ 法律法规的清单（必要时）

5.4.7. 审核计划

5.4.7.1.TB依据 GB/T 22080-2025/ISO /IEC 27001:2022网络安全技术 信息安全管理体系 要求 要求，对申请获证组织的信息安全管理体系实施审核。

5.4.7.2.TB为每次审核制定书面的审核计划。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：审核员标明认证人员注册号；技术专家标明专业代码、工作单位及专业技术职称）。

5.4.7.3.在审核活动开始前，审核组应将审核计划交受审方确认，审核组成员中如有受审方认为可能与其利益发生冲突的人员时，有权要求更换。遇特殊情况临时变更计划时，应及时将变更情况通知受审方，并协商一致。

5.5.实施审核

5.5.1. TB分两阶段实施管理体系审核：第一阶段和第二阶段。

5.5.2. 文件评审

① 文件评审的目的是评价受审方的管理体系文件是否满足标准要求、过程识别是否充分、方针和目标是否符合受审方的实际等。
② 审核组长应获得受审方文件（手册、程序文件等成文信息）及相关清单。当文件审核不能足以了解受审方管理体系运行的基本情况时，应对有关的作业文件进行审核。
③ 由审核组长或经组长委托的专业审核员对组织的体系文件进行书面审核，审核组长需在文件审查报告上签字，其审查结果《文件审核报告》应发给受审方进行确认。

5.6.初次认证审核

5.6.1. 第一阶段审核

5.6.1.1.第一阶段审核至少覆盖以下内容：

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信息安全管理体系的情况，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管理体系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。

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

② 本机构有充足的理由证明申请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 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生产经营或服务现场进行。

5.6.1.3.审核组应将第一阶段审核情况形成书面文件，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，要及时提醒客户特别关注。

5.6.1.4.对客户管理体系文件不符合现场实际、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，审核组应及时通知审核部，经审核部认可后终止审核，并将审核材料、证明材料予以上交。

5.6.2. 第二阶段现场审核

5.6.2.1.现场审核以判定受审方的管理体系能否通过认证为目的，确认受审方遵守了管理体系方针、目标和程序；确认受审方的管理体系符合标准的所有要求，并且正在实现管理方针与目标，关注体系的运行有效性。

5.6.2.2.审核组长要保证审核组成员了解认证合同和受审方情况，明确他们的分工，并按分工编制各自的现场审核检查清单。

5.6.2.3.审核组应按期到受审方现场实施审核，重点是审核管理体系符合认证标准要求和有效运行情况，应至少覆盖以下内容：

① 识别管理过程（特别是重要过程）的合理性，重要审核点的过程控制的有效性；

② 针对方针的管理职责，为实现方针而在相关职能、层次和过程目标是否具体适用、是否得到贯彻；

③ 提供的资源能否实现目标；

④ 对管理体系覆盖的过程和活动的管理及控制情况，包括信息的交流和管理措施的落实；

⑤ 承诺和评价机制的建立和实施的有效性；

⑥ 建立和持续改进信息安全管理体系改进机制的有效性，以及改进时是否保持了体系的完整性。

⑦ 受审方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；

5.6.2.4.通过了解受审方的基本情况、现场分布、信息安全管理体系过程等情况，确认审核范围。

5.6.3. 审核过程及环节

审核组应当全员完成审核计划的全部工作。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（技术专家除外）。

5.6.3.1.首次会议：

审核组全体成员、受审方的最高管理者及管理体系相关部门负责人参加会议，受审方有要求时，审核组应向受审方出示身份证明文件，会议由审核组长主持，填写现场审核首次会议签到表。首次会议内容包括：

① 介绍审核组成员和受审方管理者代表介绍参会的成员；

② 说明审核类型、目的、范围和审核依据；

③ 适用时，确认以往评审或审核发现的状态；

④ 简要说明基于抽样审核方法、程序；

⑤ 明确审核发现的方法、审核结论分级的三种情况和审核结论的依据；

⑥ 确认审核计划的各项安排；确认在审核中将告知受审方审核进程及任何关注点；

⑦ 确认审核组与受审方之间的正式沟通渠道，确定审核陪同人员；

⑧ 介绍由于审核组成员的到场对组织可能形成的风险的管理方法，落实审核组必要的工作条件和支持；

⑨ 说明保密承诺；

⑩ 询问限制条件；说明审核可能被终止的条件的信息；

⑪ 确认审核组可获得所需的资源和设施，以及适用于审核组工作安全事项、应急和安保程序；

⑫ 说明审核纪律、审核员规范声明、介绍对审核发现、审核结论（包括抱怨和申诉、投诉）的反馈渠道的信息；

⑬ 其他需要澄清的问题；

⑭ 让受审方提问的机会；

⑮ 对受审方选择 TB 认证和接待表示感谢。

5.6.3.2.审核中的沟通

① 审核组进行现场审核时，每天用于核算工作量的审核时间不宜少于 8 小时，其中应保证有充足的时间用于收集客观证据。

② 在审核实施过程中，审核组长应定期向受审方通报审核进展及相关情况。当现场审核中发现的，如：人数、审核范围等与审核任务书上不一致或获得的审核证据表明不能达到审核目的时，审核组长应及时与受审方核查需要并向审核部报告，以确定采取适当的行动。

5.6.3.3.终止审核的条件：

审核过程中发生以下情况，审核组应向TB审核部报告，经TB研究同意后终止审核。

① 受审方对审核活动不配合，审核活动无法进行；

② 受审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。

5.6.3.4.信息的收集和验证

① 审核组成员由陪同人员引导到各部门、过程进行审核，各部门应指定代表和有关人员参加；

② 审核组成员通过面谈、查阅文件、记录、现场观察等方式来收集客观证据；

③ 审核组成员采用适当的抽样对收集的信息进行验证，并与审核准则相比较，只有当收集的信息得到证实时方可作为审核证据；

④ 审核组在审核中，应注意调阅受审方内部和外部质量信息的记录，特别是受审方反馈的质量信息，以确认受审方针对这些信息制定纠正措施及实施结果能否达到改进质量和达到受审方满意的程度。现场审核应填写审核记录并满足审核计划对审核过程的要求。

5.6.3.5.形成审核发现

① 审核组对照审核准则评价审核证据（在审核过程中所收集的任何其他适当的信息）的符合性。

② 现场审核发现的不符合事实应开具书面不符合项报告，对不符合事实的描述应准确并具有可追溯性，判定不符合的性质以及违反了标准、组织的体系文件、法律法规的哪些条款准则的要求。对于不符合项，应依据认证标准判定，并在现场审核不符合项报告中明确标准的对应条款。

③ 不符合报告经审核员签字，审核组长复核后提交受审方的管理者代表签字确认。

④ 审核组长应尝试解决审核组与受审方之间关于审核证据或审核发现的任何分歧意见。对于未解决的分歧点，应予以记录。

5.6.3.6.审核组内部决定规则

首先对不符合性质进行判断分级，然后对管理体系的适宜性、有效性和充分性做出整体评价，以便为认证决定或保持认证提供充分的信息。

① 凡属下列之一，可判为严重不合格：

a.建立实施的管理体系与标准要求不符；

b.管理体系过程、活动有系统性或区域性的缺陷或严重失效；

c.产品、过程发生严重质量事故，受审方反映强烈；

d.造成严重的环境危害；

e.发生严重安全事故，相关方反映强烈；

f.严重违反质量手册和程序有关规定。

② 凡属下列情况之一，可判为一般不合格：

a.孤立的人为错误，对体系要素或体系文件的要求而言是个别的、偶然的、孤立的、性质轻微的问题；

b.文件偶尔未被遵守，未造成严重后果；

c.对系统不会产生重要影响的不合格等。

③ 考虑审核过程中固有的不确定因素，对审核结论达成一致；

④ 就任何必要的跟踪活动达成一致；

⑤ 其他未尽事宜说明

5.6.3.7.管理体系整体评价

根据审核获取的证据，根据审核组的内部沟通结果，得出管理体系整体评价结论，在审核报告中体现。

5.6.3.8.审核结论

① 符合要求，有能力满足 GB/T 22080-2025/ISO /IEC 27001:2022 网络安全技术 信息安全管理体系 要求 和适用法律、法规要求，同意推荐；

② 存在不符合项，同意不符合项采取纠正措施并验证后推荐；根据不符合情况，由审核部确定现场关闭或书面关闭不符合项。对于现场关闭验证的，由审核组长或由审核部委派审核人员到现场验证对不符合项进行关闭以后，写出不符合项现场验证报告，并按程序进行认证审批。

③ 有严重不符合项，且短期内不可能进行纠正，则总体评价为不合格，不推荐认证注册。

5.6.3.9.向受审方通报情况

在审核组内部决定会议（如遇延期或不予通过现场审核必须向TB领导报告）后，应向受审方管理层报告审核情况，并提供书面的关于受审方的管理体系是否符合规定的认证要求的说明，包括不符合项和审核结论，并充分听取受审方意见。

5.6.3.10. 末次会议

① 参加会议人员一般同首次会议，会议签到应填写现场审核末次会议签到表。

② 末次会议程序，会议由审核组长主持其内容：

a.重申审核目的、范围、依据；说明审核情况，向受审方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；提出不合格报告，包括：审核发现的任何分级；

b.对受审方管理体系建立、运行的适宜性、有效性和充分性进行总体评价；请受审方提出问题。审核组与受审方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记录并提交TB。

c.宣布审核结论和纠正措施验证要求等后续事宜；

d.说明认证证书的使用要求；

e.说明监督审核要求的有关内容；

f.再次重申保密承诺、审核员规范声明；说明投诉的处理、申诉过程；

g.对受审方给予审核组工作的支持、配合与接待表示感谢；

h.末次会议记录应予以保存。

5.6.3.11. 有关认证审核信息反馈事宜

① 《认证证书信息确认表》作为印制认证证书的凭据，应由受审方填写（如受审方对中英文对照填写有困难，可只填写中文部分，英文可委托 TB 翻译，但应签署免责声明），并经审核组长审查确认（中文部分）签字，受审方需加盖公章确认。

② 审核员需要填写审核经历表时，受审方给予证实并盖章。

③ 《审核人员工作质量反馈表》请受审方填写评价意见，盖章后传真或直接寄 TB 审核部，以便其对审核人员的工作质量进行评价和管理。

5.6.3.12. 审核记录

作为编制审核报告和为认证决定提供支持性客观证据的基础，审核记录宜突出对选取的样本中那些对于判断组织管理体系与审核准则符合程度（符合与不符合）是至关重要的、必不可少的关键信息。

5.6.4. 不符合项的纠正和纠正措施及其结果的验证

① 不符合项的情况，包括不符合项的明确说明、性质，受审方应改进的主要方面， 适用时，对以前不符合采取的纠正措施有效性的验证情况。不符合项的表述，应基于客观证据和审核依据，用写实的方法准确、具体、清晰描述，易于被受审方理解。不应用概念化的、不确定的、含糊的语言表述不符合项；

② 对审核中发现的不符合项，审核组应要求受审方分析原因，并要求受审方在规定期限内采取措施进行纠正。如果为了验证纠正和纠正措施的有效性，将需要补充一次全面的或有限的审核，或者需要文件化的证据（需要在未来的审核中确认），则 TB 应告知受审方。

③ 由审核组长或其他级别审核人员，对受审方不符合项分析原因采取纠正措施的实施结果的书面证实材料进行验证，满足要求后在纠正措施验证栏内签署意见进行关闭。

④ 对于需到现场进行验证的，审核部需下达经批准的《审核任务书》，原则上由原审核组长或审核组成员进行现场验证。审核部也可另派审核人员进行现场验证，证实其满足要求后签署意见，对不符合项进行关闭，并提交现场验证情况记录。

⑤ 当所有书面不符合项进行验证关闭后，由审核组长填写《管理体系认证决定审批表》。

5.6.5. 审核报告

① 根据现场审核情况，审核组长应编写审核报告，对受审方的管理体系建立、运行的适宜性、有效性、充分性进行总体评价，并征求全体审核组成员的意见后得出审核结论。审核组长对审核结论负责，并在审核报告上签字确认。审核报告应准确、简明和清晰地描述审核活动的主要内容。

② 审核报告内容及编写要求：

a. 组织名称及代表、地址、审核日期、审核目的、审核依据（准则）、审核类型、审核组成员及其个人注册信息、审核活动（现场或非现场，永久或临时场所）；

b. 审核计划的完成及审核目的实现情况，任何偏离审核计划的理由说明；

c. 现场审核情况的描述，包括审核覆盖的区域（认证要求、地点、部门、过程）；

d. 管理体系文件与申请认证标准要求的符合性评价；

e. 受审方管理体系的评价，具体内容在《管理体系认证审核报告》中描述。

f. 任何对审核方案有显著影响的问题；

g. 对不符合项纠正措施的要求和验证方式；

h. 审核组对是否通过认证的推荐意见。当经最终决定的审核结论与现场审核结论有差异时，TB将书面通知受审方相关事宜。

③ 注意事项

a. 如果受审方有多个不在同一地址的现场，应在报告中说明；

b. 如果受审方对报告持不同意见，如某些问题双方无法统一，可记入检查结果，记录应予以保存，并随审核资料一起提交TB。

④ 审核报告一式两份，受审方一份，TB 一份。审核组应保留签收和提交的证据，并随审核资料一同上交。

⑤ 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。

⑥ 综合部负责将审核报告提交或邮寄给受审方，并保留签收或提交的证据。

5.6.5.1. 发生以下情况时，审核组应向TB报告，经TB同意后终止审核。

① 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。

5.6.6. 认证决定

5.6.6.1. TB建立并实施《认证评定管理规定》，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的基础上，作出认证决定。

5.6.6.2.认证决定人员为TB聘用的人员，与TB签订在法律上具有强制实施力的协议。审核组成员不得参与对审核项目的认证决定。TB负责做出认证决定的人员以及参与决定的技术专家，需经专业能力评价后使用。

5.6.6.3.TB在做出认证决定前应确认如下情形：

5.6.6.4.审核组提供的审核报告及其他信息能够满足做出认证决定所需要的信息。

5.6.6.5.反映以下问题的不符合项，TB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，对实现信息安全管理体系目标有重大疑问。

② 制定的信息安全管理体系目标不可测量或测量方法不明确。

③ 对实现信息安全管理体系目标具有重要影响的关键过程的监视和测量未有效运行，或者对这些关键过程的报告或评审记录不完整或无效。

④ 其他严重不符合项。

5.6.6.6.对于所有轻微不符合，TB已审查和接受了受审方对纠正和纠正措施的计划。

5.6.6.7.在满足以上条件要求的基础上，TB有充分的客观证据证明受审方满足下列要求的，评定该受审方符合认证要求，向其颁发认证证书。

① 受审方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 受审方按照认证合同规定履行了相关义务。

TB 及其认证人员应当及时做出认证结论，保证其客观、真实并承担相应法律责任。TB 及其认证人员不得出具虚假或者严重失实的认证结论。

5.6.6.8.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方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 GB/T 22080-2025/ISO /IEC 27001:2022 网络安全技术 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质量安全问题或有其他与产品、服务质量和信息安全管理体系相关严重违法违规行为。

5.6.7. 认证决定与批准

① 认证决定的方式为认证决定人员审定，审定时需在《管理体系认证决定审批表》上签字。

② 如认证决定中存在重大问题时，提交 TB 技术部进行决定，并做出处理。

③ 当受审方不能满足要求或者存在重大缺陷，不符合认证标准的要求或存在重大质量安全问题或与产品和服务质量有关的严重违规违法行为，评定结果为不符合认证要求，以书面形式告知受审方未通过认证的原因。

④ 当出现影响批准认证的事宜时，信息获取部门应及时向技术部传递信息，以保证认证决定的有效性。

⑤ 如果认证审议审定结果与审核组提交的报告存在差异时，技术部要及时通知审核员，由审核员与受审方沟通、说明原因，并由技术部向受审方发送书面通知。

⑥ 总经理根据认证决定人员签字的《管理体系认证决定审批表》附有关资料批准认证注册。

⑦ 《管理体系认证决定审批表》需经总经理批准/法人代表签字方能制作证书。

⑧ TB 将记录每项认证决定，包括从审核组或其他来源获得的任何补充信息或澄清。

5.6.7.1.如果审核组不能在现场审核结束后6个月内验证对严重不符合实施的纠正和纠正措施，则应在推荐认证前再实施一次现场审核。

5.6.7.2.TB在颁发认证证书后，应当在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。对于认证标志、认证证书的管理执行《认证证书和认证、认可标识及国际认证证书和互认标识使用控制程序》。

5.6.8. 认证活动引发的责任

认证过程、活动引发的责任及处理由总经理负责做出安排。

5.6.8.1.属TB的责任

① 审核活动不符合认证标准和 TB 管理体系认证文件要求；

② 审核活动中发生违反科学性、公正性现象；

③ 审核活动中审核人员违反审核纪律、发生泄密行为；

④ 审核结论与事实不符；

⑤ 违反认证合同的双方约定。

5.6.8.2.属于申请人（受审方）的责任

① 申请的管理体系覆盖产品、过程范围、体系覆盖人数与现场提供的审核范围不符；

② 管理体系建立和运行未按认证标准要求和管理体系文件规定实施；

③ 违反认证证书和认证标志的使用规定；

④ 对认证审核中发生的不符合项不能按规定采取纠正和预防措施，满足认证要求；

⑤ 违反认证合同书和双方约定。

TB和申请人（受审方）关系、活动均应以双方签订的合同书为依据，涉及合同书范围以外的活动，须经双方商定，发生责任问题以书面文件为准，对确属TB的责任，由总经理做出具体安排，组织有关部门分析原因，制定纠正和纠正措施，并与申请人（受审方）协商妥善解决。

5.6.9. 认证要求的更改

根据国际标准化组织（ISO）对认证标准和认证规则的更改，并将这些更改信息和更改的实施部署要求，TB以公开文件的形式及时通知受审方，使他们能在规定的时限内调整管理体系文件并实施，并对满足新的要求情况进行验证。

首先由获证受审方书面申请，并提供与认证标准相适应的成文信息，由审核部审查决定是

否受理，然后在确定审核组组成后，由专人进行文件审查和现场审核。现场审核中重点审核认证标准或认证规则变更的要求、过程、活动及相关部门。审核程序按本文件对现场审核实施的要求进行。审核结束后，由技术部审定，总经理批准，给予认证证书的更换。如新的申请人或获证组织不愿意或不能确保符合新的要求时，TB将按规定做出适宜处理，包括中止合同或撤销认证注册资格。

6. 监督审核程序

6.1.总体要求

TB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。

6.2.监督审核频次与实施

为确保达到6.1条要求，TB应根据获证组织的质量信息安全管理体系程度或其他特性，确定对获证组织的监督审核的频次。

6.2.1.在认证证书三年有效期内，对获证组织管理体系运行情况每年按计划进行监督审核。初次认证后的第一次监督审核应在认证证书签发日起9—12个月内进行。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12个月。

6.2.2.如果受审方对其管理体系进行了重大的更改，或者发生了影响到其认证基础的变更时，可根据获证组织的具体情况及管理体系成熟度在认证审核方案中考虑和调整增加监督审核频次。

6.2.3.获证企业的产品在产品质量国家监督抽查中被查出不合格时，自国家市场监督管理总局发出通报起30日内，TB应对该企业实施监督审核。

6.2.4.监督审核应在获证组织现场进行，且现场审核应安排在认证范围覆盖信息安全管理体系活动正常运行时进行。由于产品生产的季节性原因，在每次监督审核时难以覆盖信息安全管理体系所有产品和服务的，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。

6.2.5.超过期限而未能实施监督审核的，按8.1或8.3条处理。

6.3.监督审核实施程序

6.3.1.审核部负责提前3个月与监审的获证组织联系，制定监督审核方案，其中包括：确定审核时机、多场所抽样方案等。

6.3.2.每次监督审核的人日数应依据认证获证组织的具体情况确定，监审人日数不得低于初审

时总人日数的30%，任何人日数的增减情况及原因说明予以记录。

6.3.3.审核部负责组建满足专业要求的审核组，并基于运行环节与企业沟通的结果、审核组专业能力配备等情况及时调整审核方案，经审核部部长审查批准，签发《审核任务书》。

6.3.4.审核组长负责依据审核方案策划结果、审核任务书，编制审核实施计划，对审核活动进行具体安排。在编制实施计划时，应关注下列要素、过程和活动的审查：

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 按要求对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 管理体系在实现组织方针、目标方面的有效性，质量目标及质量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规定要求。

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，及时建立并实施了有效的改进措施。

审核组长在现场审核中发现的，如：人数与审核任务书上不一致、审核范围的扩大等情况，需与审核部联系，以便能及时采取措施。

6.3.5.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，审核组长应向技术部报告，技术部组织具备适宜能力且未实施该审核的人员进行复核，以确定能否保持认证。

6.3.6.认证资格保持的条件

① 管理体系能持续满足认证标准要求；

② 产品质量稳定，服务及时，履行承诺，获证组织满意；

③ 管理体系持续有效运行，保持自我改进和自我完善的机制；

④ 再认证审议结论时，还应考虑和评价获证组织在认证有效期内管理体系整体的持续有效性。

6.3.7.审核组应编制审核报告，对报告中的要求应逐项描述，并做出建议TB给予继续保持、暂停、撤销认证资格的推荐性结论。如果发现不合格，获证组织应在规定的时间内采取有效纠正措施，并经审核组长验证合格后提交技术部。

6.3.8.技术部根据监督审核报告及其他相关信息，做出继续保持或暂停、撤销认证证书的决定。

6.4.建立通报制度和不定期的监督

6.4.1.通报内容：在认证证书有效期内，获证组织应明确职能部门和责任人员，如发生下列情

况应及时主动地向TB通报情况，必要时TB将要求获证组织提供有关投诉记录和采取纠正措施的记录。管理体系发生相关变更包括：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、管理者代表变更；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。

6.4.2.不定期的监督：根据6.4.1条发生的影响管理体系认证基础的更改或运行的重大变化，不能满足认证标准和获证组织要求时，可决定立即实施不定期的监督审核，并根据监督结果，视情节做出处理决定。

7. 再认证程序:

7.1. 总体要求：

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

7.2. 再认证目的与审核安排：

再认证的目的是确认管理体系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，在证书到期前安排更新认证。在认证周期届满前三个月，审核部应与获证组织联系再认证事宜，并安排再认证审核。现场审核时间应安排在证书到期前。审核策划人员应在审核任务书中明示证书的到期时间，提醒审核员在认证证书到期前，提交经验证后的审核资料，以便技术部在认证证书到期前有充足的时间做出认证决定。

7.3. 审核组合安排：

再认证审核可以和暂停恢复的现场审核同时安排。

7.4. 审核重点与内容：

再认证审核前，应由审核组长对获证组织获证以来，管理体系的总体变化趋势进行评价，对薄弱环节应作为再认证的审核重点，并包括体系文件审查和现场审核。再认证至少应包括针对下列方面的现场审核

7.4.1.结合内部和外部变更（如组织、产品、法规、标准、流程、场所、获证组织等方面发生的重大变化以及因改进而发生的变更），通过绩效数据的分析、内审、管理评审等提供的信息的评价，了解组织保持体系完整性的措施，管理体系在经历了各种变更影响下的有效性保持，以及认证范围的持续相关性和适宜性；

7.4.2.经证实的对保持管理体系有效性并改进管理体系，以提高整体绩效的承诺；

7.4.3.获证管理体系的运行是否促进了组织方针和目标的实现，管理体系在实现获证组织的目标和管理体系的预期结果方面的有效性；

7.4.4.在经历各种变更下，管理体系是否还能支持认证范围所覆盖的对象。认证范围是否需要做必要的调整。

7.5. 超期申请的处理

对获证组织超出认证证书有效期提出的再认证申请，审核部应按照初审对待。

7.6. 未完成审核的后果

如果在认证终止日期前，未能完成再认证审核或不能验证对严重不符合实施的纠正和纠正措施，则不应推荐再认证，也不应延长认证的有效期。TB应告知获证组织并解释（说明）后果。

7.7. 认证有效期与颁证日期：

如果在当前认证的终止日期前成功完成了再认证活动，新认证的终止日期可以基于当前认证的终止日期，新证书上的颁证日期应不早于再认证决定日期。

7.8. 认证终止后的恢复：

在认证终止后，如果TB能够在6个月内完成未尽的再认证活动，则可以恢复（复活）认证，否则应至少进行现场审核才能恢复（复活）认证。证书的生效日期应不早于再认证决定日期，到期日期应基于上一个认证周期。

7.9. 认证更新决定：

TB应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。

8. 暂停或撤销认证证书

TB制定保持认证管理要求，规定对认证证书的暂停和撤销的管理要求，不得随意暂停或撤销认证证书。

8.1. 暂停证书

8.1.1. 获证组织有以下情形之一的，TB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， 包括对信息安全管理体系运行有效性要求的。

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。

8.1.2. 认证证书暂停期不得超过6个月。但如果获证组织正在向相关行政许可或监管部门申请办理与保持认证资格相关的必要许可、资质或批准，且此状态已正式告知TB，则暂停期可延长至该许可决定作出之日。

8.1.3. TB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。

8.1.4.暂停的办理：

① 对证书暂停由审核部提出，认证决定阶段提出暂停由技术部提出，暂停应经提出部门主管领导审批。综合部负责统一变更办公系统内的相应信息及上报 CCAA。综合部负责制作和发放“暂停认证证书和标志通知书”。

② “暂停认证证书和标志通知书”中应有暂停具体原因、暂停的起始日期和暂停期限，应明确并声明在暂停期间客户不得以任何方式使用认证证书、认证标识或引用认证信息。

8.2.恢复

8.2.1.针对暂停的不同原因，客户如采取有效的纠正措施并经验证有效后，可对其认证资格进行恢复 （包括恢复使用证书和标志），如果客户未能在公司规定的时限内解决造成暂停的问题，公司将撤销或缩小其认证范围。

8.2.2.恢复的办理：

8.2.2.1.根据不同的暂停原因，本着“谁办理谁跟踪”的原则，恢复应由暂停提出部门办理。

① 由技术部提出暂停的，其恢复由技术部提出，由审核部策划特殊审核中的“提前较短时间通知的审核”，并通知客户和审核组长。待现场审核资料交回后，技术部认证决定通过，由管理者代表审批，予以恢复。

② 对因欠费暂停的，获证组织在规定的时间内缴费的，由审核部直接办理恢复手续；

③ 对因持有的与信息安全管理体系范围有关的安全生产许可证、资质证书等过期失效，重新提交的申请已被受理但尚未换证原因暂停的，获证组织上交有效资质后，由审核部直接办理恢复手续；

④ 除以上的①②③点外，由审核部安排审核组长现场确认是否具备恢复条件。如具备，由审核组长告知审核部，由审核部办理恢复手续。综合部负责制作和发放“恢复认证证书和标志通知书”。

8.2.2.2.公司有关部门要与认证暂停客户保持信息沟通、联系，了解该客户采取纠正措施进展的动态情况，以便对暂停的恢复做出及时安排。

8.2.3.恢复的现场审核

8.2.3.1.恢复审核的主要内容有：

① 针对暂停原因，受审核方采取了纠正措施和预防措施，对其纠正措施和预防措施的适宜性和实施的有效性进行审核，并收集相关证据予以证实。

② 了解暂停期间受审核方是否按规定停止使用认证证书和认证标志。

③ 了解暂停期间受审核方管理体系是否正常运行，评价管理体系运行的有效性。

④ 审核员应根据上述审核内容，评价受审核方的暂停能否恢复，给予是否推荐恢复注册资格的结论。审核记录和审核报告中需对审核过程中了解的情况和结论予以明确记录。

8.2.3.2.“恢复+监审”的审核要求

① 审核部在策划“恢复+监审”的审核时，应提前与客户充分沟通，了解其针对暂停是否已完成整改和验收，必要时需客户提供相关证实材料。

② 当本次审核的审核目的是“恢复+监审”时，审核员应先进行恢复审核。只有当审核组通过现场审核确认受审核方具备恢复认证资格后，方能进行正常的监督审核；如不具备恢复条件时，审核组应及时向审核部报告。

8.3.撤销证书

8.3.1.获证组织有以下情形之一的，TB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 被执法监管部门责令停业整顿或被列入国家信用信息严重失信主体相关名录

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 拒绝接受国家产品质量监督抽查的。

⑤ 出现重大的产品和服务等质量安全事故，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，造成严重影响或后果，或者 TB 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。

8.3.2.撤销的办理：

8.3.2.1.在规定的期限内未解决造成暂停原因的，撤销的办理本着“谁暂停谁撤销”的原则，分别由审核部/技术部办理撤销手续。

8.3.2.2.管理体系认证证书一经撤销，即表明公司不再证明获证客户管理体系符合其特定的标准，终止了双方的认证关系，由综合部收回认证证书。

8.4.证书的管理与责任

8.4.1.对获证客户暂停、恢复、撤销等有关审批材料由办理部门负责存档。对于暂停、恢复、撤销认证证书和标志通知书随审核资料归档。

8.4.2.管理体系认证证书状态的任何变更，综合部均上报CNCA、CNAS备案（CNAS备案需认可后）。

8.4.3.公司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。

9. 特殊审核

9.1. 体系认证范围的扩大

由获证组织提出书面申请，提出与扩大认证范围相适应的相关证据（含质量/管理手册），由审核部审查是否受理，并签订扩大认证范围的合同补充协议。审核部在确定审核组组成后，由专人针对扩大范围的内容进行文件审查，并进行必要的审核活动，以做出是否可以扩大的决定。

9.2. 体系认证范围的缩小

当获证组织的某些已认证的范围不能持续满足标准要求时，获证组织须提前一个月向本TB提出缩小认证范围的变更通报，由TB更换所发的认证合格证书。有下列情况之一者，本TB将缩小获证组织认证范围：

9.2.1.如果获证组织认证范围内的部分信息安全管理体系过程不再继续符合认证标准和其他附加要求、不再进行信息安全管理体系过程或不愿再继续保持认证资格；

9.2.2.如果获证组织被暂停，未能在规定的时限内解决造成暂停的问题，TB将根据实际情况撤销或缩小其认证范围。

9.3. 认证范围扩大与缩小的条件

9.3.1.扩大（缩小）体系覆盖信息安全管理体系范围，其体系应符合申请标准要求；

9.3.2.产品/服务质量符合相关法规/标准要求，获证组织满意；

9.3.3.管理体系有效运行，并具有满足规定的管理目标的能力。

9.3.3.1.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，TB将缩小其认证范围，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。在办理缩小其认证范围时，应经认证决定人员做出认证决定，经总经理或管理者代表批准后，由综合部制作并发放经认证范围缩小的认证证书。

9.3.3.2.对缩小其认证范围的获证组织，按其职责划分，TB相应部门应与获证组织进行沟通，正确说明缩小认证范围的情况。

9.4. 基于特定事由的紧急审核

9.4.1.机构在接到投诉后应即刻启动调查程序，如需现场取证追踪，则需至少提前24小时书面通知客户进行现场核实；通知中应明确投诉内容、对象、调查人员等信息；

9.4.2.如因客户进行变更、对被暂停的客户进行追踪而需要提前较短时间进行通知审核的，则

应至少提前24小时书面通知客户，应让客户了解：对整个审核过程的详细说明，包括：审核原因、认证依据、产生的费用、审核人员、客户需提供资源的要求、投诉和申诉处理过程的信息等；

9.4.3.不通知获证客户的审核：一般为机构内部的随机抽查，相关监督部门的飞行检查，和随机检查等；机构在对客户的合同中已经明确了规定，客户需无条件进行配合；

9.4.4.提前较短时间通知获证客户进行的审核，由于客户缺乏对审核组成员的任命表示反对的机会，所以无特殊情况下一般安排前一任组长或组员担任组长；如因处理投诉而进行的调查，则应提前与客户沟通调查组成员的情况。

10.认证证书与认证标识的要求

10.1. 认证证书内容要求

认证证书应至少包含以下信息：

① 获证组织名称、地址（包括获证组织总部的名称和地址，以及认证证书所涉及的所有分支机构的清单）和统一社会信用代码。该信息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经营地址和业务范围。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（不包括生产现场）。如果分支机构的认证范围只是整个组织认证范围的一部分，认证证书应明确说明每个分支机构的适用范围。

③ 信息安全管理体系符合 GB/T 22080-2025/ISO /IEC 27001:2022 网络安全技术 信息安全管理体系 要求 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。

⑦ 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。

⑧ 相关的认可标识及认可注册号（适用时）。

⑨ 证书查询方式。TB 除公布认证证书在 TB 网站上的查询方式外，还应当在证书上注明：“本证书信息可在本 TB 网站（http://www.jxtengbiao.com/）查询，亦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。

10.2. 证书有效期

10.2.1. 初次认证证书有效期最长为3年

10.2.2. 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。

10.3. 证书信息通报与社会监督

TB 建立《信息通报管理规定》，规定除向获证组织、认证监管部门等执法监管部门提供认证证书信息外，还根据社会相关方的请求向其提供证书信息，接受社会监督。

11. 与其他管理体系的结合审核

11.1. 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信息安全管理体系专项的要求，并易于识别。

11.2. 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％。

12. 受理组织的申投诉

12.1. TB制定了《申诉投诉管理程序》，以便正确、及时地处理来自受审核方或其它各方对本TB的申诉、投诉，维护管理体系认证的公正性和严肃性。获证组织或获证组织对认证决定有异议时，TB应接受申诉并及时进行处理，在 60日内将处理结果形成书面通知送交申诉人。

12.2. 书面通知应当告知申诉人，若认为TB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。

13. 认证记录

13.1. 公司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。

13.2. 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。

13.3. 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。

13.4. 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，保存时间至少应当与认证证书有效期一致。

14. 受理转换认证证书

信息安全管理体系无需转换

15. 相关文件

- TB-GZ-01《项目受理管理规定》
- TB-GZ-02《申请评审、受理和审核人日确定办法》
- TB-GZ-03《审核方案管理规定》
- TB-GZ-04《审核方案策划实施管理规定》

- TB-CX-10《管理体系认证初次审核实施与控制程序》
- TB-CX-12《保持认证管理程序》
- TB-CX-19《认证证书和认证、认可标识及国际认证证书和互认标识使用控制程序》
- TB-CX-13《申诉投诉管理程序》
- TB-GZ-18《信息通报管理规定》
- TB-GZ-17《多场所认证实施管理规定》

附录 A 认证审核时间要求

信息安全管理体系认证审核时间要求

有效人数	审核时间（人天数） 第1阶段+第2阶段	有效人数	审核时间（人天数） 第1阶段+第2阶段
1-10	1.5	876-1175	9
11-15	1.5	1176-1550	10
16-25	2	1551-2025	11
26-45	2	2026-2675	12
46-65	3	2676-3450	13
66-85	3	3451-4350	14
86-125	4	4351-5450	15
126-175	4	5451-6800	16
176-275	5	6801-8500	17
276-425	6	8501-10700	18
426-625	7	>10701	遵循上述递进规律
626-875	8		

注：

1. 确定有效人数：在认证范围内的、处于组织控制下工作的、所有班次的人员的总数，是确定审核时间的起点。当人员中达到50%从事某些相同的活动时，允许在计算审核时间前进行人员数量的折减。按照对实施每项相同活动的人数开平方根的方式，得到用于计算审核时间的有效人数。该数值是允许折减到的最小值。
2. 从事某项被认定为重复活动/工作的示例包括：
   ① 履行职责时对信息只有读取访问权限的人员；
   ② 不能使用组织ISMS范围内的信息处理设施的人员；
   ③ 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人员；
   ④ 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。
3. 组织正常工作期间（如轮班制组织）安排的审核时间可以计入有效的管理体系认证审核时间，但往返多审核场所之间所花费的时间不计入有效的管理体系认证审核时间。
4. 监督人日为初审的 1/3；再认证人日为初审的 2/3；计算结果若不为整数，则以0.5人天为最小单位进行修约取整。