编号：SEC/GZ-01-ISMS-2025

信息安全管理体系
认证实施规则

第 2.1 版

2022 年 1 月 28 日发布　　2025 年 8 月 8 日第 1 次修订　　2025 年 8 月 8 日实施

目录

前　　言

为了保证东南标准认证中心信息安全管理体系认证工作顺利开展，确保认证各项工作符合相关文件要求，以及中心质量手册、程序文件汇编等的要求，使各项认证活动得以规范有序进行，制定本实施规则。

2025 年 8 月 8 日修订以下内容：增加认证资格恢复要求、直接明示引用文件内容。

制定单位：　福建东南标准认证中心有限公司

修订人员：肖宇航

批准人员：李东山

1. 适用范围及认证依据

本规则用于规范福建东南标准认证中心有限公司（简称中心或本中心）的信息安全管理体系认证活动。

认证依据是以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》为认证依据。

注：认证依据以国家或国际标准的现行有效版本为准。

2 对认证审核人员的基本要求

2.1 认证审核员应当取得国家认监委确定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。

2.2 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。

3. 术语和定义

3.1. 现场审核

中心指派审核组到受审核组织所在地点进行的审核活动。

3.2. 远程审核

应用信息和通信技术(ICT)，在受审核活动的实际场所以外任何地点实施的审核。

注1:ICT是应用技术来收集、存储、检索、处理、分析和发送信息，它包括软件和硬件，例如:智能手机、手持设备、笔记本电脑、台式电脑、无人机、摄像机、可穿戴技术、人工智能及其他。

注2:远程审核可以是审核人员在受审核方某一场所对其他场所的人员、活动或过程进行的审核，也可以是审核人员不在受审核方场所对受审核方的人员、活动或过程进行的审核。

3.3. 特殊审核

扩大认证范围或提前较短时间通知的审核。

4. 审核类别和审核方式

审核类别分为初次认证审核（包括一阶段和二阶段审核）、监督审核、再认证审核和特殊审核。

审核方式分为现场审核、远程审核。

5. 技术专家、审核组要求

技术专家必须得到中心的专业能力评价，以确定其能够胜任所安排的技术支持工作。

审核组应由能够胜任所安排的审核任务的审核员组成。必要时可以补充技术专家以增强审核组的技术能力，技术专家应在审核员的监督下进行工作，可就受审核组织管理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. 认证信息公开

中心应向申请认证的社会组织(以下称申请组织)至少公开以下信息：

1) 认证服务项目；

2) 认证工作程序；

3) 认证依据；

4) 证书有效期；

5) 认证收费标准等。

7. 认证程序

7.1. 初次认证

7.1.1. 认证申请

中心应要求申请组织的授权代表至少提供以下必要的信息：

1) 认证申请书，包括但不限于以下内容：

a.组织基本信息，包括业务活动、组织架构、联系人信息、物理位置和体系范围等基本内容；

b.法律地位资格证明(营业执照、事业单位法人证书或社会团体法人登记证书）；

c.申请认证的范围；

d.涉及的管理体系过程；

e.管理体系正式运行的时间、内审时间、管理评审时间；

f.取得相关法规规定的行政许可文件、相关法律法规要求的其他证明文件(适用时)。

7.1.2. 申请评审

中心应根据认证依据、程序等要求，在三个工作日内对申请组织提交的认证申请书及其相关资料进行评审并保存评审记录，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业务过程特性和要求；

3) 国家对相应行业的管理要求；

4) 申请组织管理体系运行时间满三个月，已完成内部审核和管理评审；

5) 中心与申请组织之间任何已知的理解差异得到消除；

6）中心有能力并能够实施所申请的认证活动；

7）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）核算并确定审核人日；

9）根据申请认证的活动范围及场所、从事活动的影响、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，不予受理其认证申请。

中心应建立审核人日确定准则，根据受审核组织的规模、特性、业务复杂程度、管理涵盖的范围、认证要求和其承担的风险以及采取审核方式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。确定的人日数记录在审核方案记录中。

7.1.3. 建立审核方案

在申请评审后，中心应针对申请组织建立审核方案（申请组织变更为受审核组织），并由审核管理部负责管理审核方案。审核方案的范围与程度应基于受审核组织的规模和性质，以及受审核方服务的性质、功能、复杂程度以及成熟度水平。

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，确定审核范围应考虑如下要求：

a.初次认证、再认证审核内容为认证依据的全部条款；

b.监督审核采取抽样的方式进行，两次监督审核必须覆盖标准所有适用条款。

3）审核准则；

4）审核方式；

5）审核组的选择；

6）所需的资源，包括交通和食宿；

7）确定的审核人日；

8）处理保密性、信息安全、健康和安全，以及其它类似事宜。

7.1.4. 初次认证审核

7.1.4.1. 确定审核组

审核管理部应依据第5章中的审核组组建原则，根据受审核组织的行业、规模和业

务复杂程度组建审核组，指派审核组长。

7.1.4.2. 制定审核计划

审核组结合受审核组织的申请材料、审核方案对审核的策划以及上一次审核（如果有）的结果，对审核做出具体安排，包括但不限于审核的目的、内容、具体的时间安排、审核组成员对受审核组织按岗位和活动以何种方式进行审核的安排、高层沟通的安排和会议的安排。审核组长应至少在开展审核3个工作日之前，与受审核组织就审核计划进行充分沟通，确保双方没有异议。

7.1.4.3. 一阶段审核

审核组应对受审核组织开展一阶段审核，以确定：

1) 受审核组织的管理体系得到策划和实施；

2) 受审核组织的管理体系已运行，并有足够的证据证明其运行情况；

3) 受审核组织对运行的管理体系进行了监视、测量、分析和评价，并有充分的证据；

4) 受审核组织对管理体系进行了有效的持续改进；

5) 受审核组织是否识别并遵守了相关的法律法规；

6) 受审核组织有充足的资源保障二阶段审核的进行；

7) 收集关于客户的管理范围、过程和场所的必要信息，包括：

a.客户的场所；

b.使用的过程和设备；

c.所建立的控制的水平（特别是客户为多场所时）。

审核组按照审核计划实施一阶段审核，以获取审核需要的信息。

如果一阶段审核发现问题，审核组应开具一阶段审核问题清单，且获得受审核组织确认，并要求受审核组织按整改要求针对发现的问题进行整改并提供整改证据。

审核组长对整改材料进行验证，并确认整改结果。必要时与客户沟通调整二阶段审核计划。

审核组长将第一阶段审核发现开成审核报告并告知申请组织，并与申请组织进行沟通，确保双方对报告没有异议。

对于风险等级是三级风险的或曾经取得过ISMS证书、在中心做过其它管理体系的认证客户，其一阶段可采取非现场审核方式进行。

7.1.4.4. 二阶段审核

审核组按照审核计划的安排对受审核组织进行审核，审核应考虑一阶段审核结果，

对受审核组织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。

第二阶段的目的是评价受审核组织管理体系的实施情况，包括有效性。第二阶段覆盖标准的全部条款，包括但不限于以下方面：

a）与适用的管理体系标准或其他规范性文件的要求的符合情况及证据；

b）依据关键绩效目标和指标（与适用的管理体系标准或其他规范性文件的期望一致），对绩效进行的监视、测量、报告和评审；

c）受审核组织管理体系的能力以及在符合适用法律法规要求和合同要求方面的绩效；

d）受审核组织管理过程的运作控制；

e）内部审核和管理评审；

f）针对受审核组织管理方针的管理职责。

7.1.5.不符合项的纠正和纠正措施及其结果的验证

对审核中发现的不符合项，中心将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 3 个月期限内采取纠正和纠正措施。中心将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 3 个月内验证对严重不符合实施的纠正和纠正措施，则应按 7.1.7 条处理，或者按照 7.1.4 条重新实施审核。

7.1.6.审核报告

7.1.6.1 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）申请组织的名称和地址。

（2）申请组织活动的范围和场所。

（3）认证的类型、准则和目的。

（4）审核组组长、审核组成员及其他个人信息，如技术专家。

（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 7.1.4 条列明的程序及各项要求的审核工作情况，其中：对 7.1.4 条的各项认证要求应逐项描述或引用审核证据、审核发现和审核结论，并对实现情况进行审核。

（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。

7.1.6.2 中心将保留用于证实审核报告中相关信息的证据。

7.1.6.3 中心将在作出认证决定后 7 个工作日内将审核报告提交申请组织，并保留签收或提交的证据。

7.1.6.4 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，中心将此报告及终止审核的原因提交给申请组织，并保留签收或提交的证据。

7.1.7. 认证决定

中心应指派认证决定人员，对受审核组织的认证申请实施认证决定，以决定：

1）同意认证注册，颁发认证证书；

2）补充认证决定所需的信息，包括但不限于申请材料、审核材料，再行决定；

3）不同意认证注册，通知受审核组织不同意的理由。

认证决定人员实施认证决定时应以认证过程中收集的信息和其他相关信息为基础，以充分的证据证实受审核组织的管理体系得到了建立、实施、运行、监视、评审、保持和改进做出决定。

注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。

注2：受审核组织获得认证注册资格后变更为获证组织。

7.1.8. 证书发放

技术审定部负责制作证书，将证书、审核报告发放给获证组织。

7.1.9. 审核方案记录与变更

审核方案管理人员应收集审核和认证决定的信息，特别是形成的结论和变化的信息，记录到审核方案中，并确定审核方案是否需要进行变更，如需要则更新相应项目内容。

7.2. 监督审核

7.2.1. 监督频次

审核管理部应在满足认可要求的基础上，根据获证组织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。当获证组织管理体系发生重大变更，或发生重大问题、业务中断事故、客户投诉等情况时，中心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。

必要情况下，中心可采取事先不通知的方式对获证组织进行飞行检查。

7.2.2. 监督审核通知

审核管理部应提前向获证组织发出监督审核通知，受审核组织按要求填写监督审核通知的回执等相关信息。

7.2.3. 信息收集

在进行监督审核之前，审核管理部需要收集获证组织的管理体系相关信息，以确定获证组织的管理体系相关信息是否发生变化。需要客户提供的信息包括以下几个方面：

1）信息确认文件，包括但不限于：

a.基本信息，包括组织名称、地址、联系人等信息的变化情况；

b.组织信息：包括组织范围、组织架构、人员数量等信息的变化情况；

c.管理体系相关信息，关键文件化信息的变化情况。

7.2.4. 信息评审与审核方案维护

项目管理人员应对获证组织的信息确认文件进行评审，以确定：

1）获证组织的管理体系变化情况，尤其是管理范围的变化；

2）是否需要修订审核方案，需要时对审核方案进行维护。

7.2.5. 监督审核实施

7.2.5.1. 确定审核组

同7.1.4.1。

7.2.5.2. 制定审核计划

审核组应结合获证组织的信息确认文件、审核方案对监督审核的策划和前一次审核的结果对监督审核做出具体安排，包括但不限于具体的时间安排、审核组各成员按岗位和活动以何种方式对获证组织进行审核的安排、高层沟通的安排和会议的安排。审核组长应至少在实施审核三个工作日之前，与获证组织就审核计划进行充分沟通，确保双方没有异议。

需要抽样时，抽样原则为：

1）两次监督审核必须覆盖标准所有适用条款和所有部门；

2）标准中对管理体系过程有决定作用的条款和部门每次监督审核都需要抽到；

3）获证组织前一次审核问题较多的部门在本次监督审核中需要抽到；

4）审核组认为需关注的条款应考虑进行抽样。

每次监督审核的内容应包括但不限于以下方面：

1）内部审核；

2）管理评审；

3）上次审核中发现的不符合项整改的有效性；

4）上次审核中发现的观察项进行跟踪；

5）投诉的处理；

6）ISMS在实现客户信息安全方针的目标方面的有效性；

7）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珠运行情况；

8）所确定的控制的变更，及其引起的SoA的变更；

9）控制的实施和有效性；

10）证书的使用和（或）任何其他对认证资格的引用。

7.2.5.3. 监督审核实施

审核组按照审核计划对获证组织进行审核，如审核过程中获证组织的认证范围与策划不一致，应对不一致的部分特别关注，必要时重新确认审核范围、变更审核计划，发生变更时，需向项目管理人员报告说明情况，由项目管理人员会商技术主管确定是否调整审核计划。

如果监督审核发现不符合项和观察项，经沟通获得受审核组织确认，开具不符合项报告和观察项报告。要求受审核组织按整改要求针对发现的问题进行整改并提供整改证据。审核组负责对整改情况进行验证。具体要求见7.1.5。

7.2.6. 监督审核结论

审核组应对收集的所有信息和证据进行汇总分析，评价审核发现并就审核结论达成一致。

审核组应根据监督审核的结果对获证组织的管理体系是否满足适用的认证依据的要求进行评价，并判断是否推荐保持认证注册。

监督审核结束后审核组长完成审核报告编制工作，并与获证组织进行沟通，确保双方对报告没有异议，并确保报告准确性。

7.2.7. 认证决定

中心应指派认证决定人员，对获证组织的认证申请实施认证决定，以决定：

1）同意保持认证注册；

2）补充认证决定所需的信息，包括但不限于申请材料、审核材料，再行决定；

3）不同意保持认证注册，做出暂停或撤销的决定，通知获证组织不同意保持的理由。

认证决定人员实施认证决定时应以认证过程中收集的信息和其他相关信息为基础，

以充分的证据证实获证组织管理体系得到了建立、实施、运行、监视、评审、保持和改进。

7.2.8. 证书发放

技术审定部负责制作证书（如需要），将证书、审核报告发放给获证组织。

7.2.9. 审核方案记录与变更

同7.1.9。

7.3. 再认证

7.3.1. 再认证频次

再认证周期为三年，认证证书有效期满前3个月，中心根据获证组织的申请对获证组织实施再认证审核，以保证管理体系认证证书持续有效。

7.3.2. 再认证审核通知

中心应提前向获证组织发出再认证审核通知，受审核组织按要求填写再认证审核通知的回执等相关信息。

7.3.3. 信息收集

同7.2.3。

7.3.4. 信息评审与审核方案维护

项目管理人员应对收集的获证组织信息和确认文件进行评审，以确定获证组织的管理变化情况，尤其是管理体系范围的变化，如果获证组织的认证范围信息有变化，应对变化的方面进行关注，必要时重新确认审核范围。

项目管理人员根据信息评审的结果维护审核方案，维护审核方案时应考虑管理体系在最近一个认证周期内的绩效。其它内容参考7.1.3。

7.3.5. 再认证审核

7.3.5.1. 确定审核组

同7.1.4.1。

7.3.5.2. 制定审核计划

审核组应结合获证组织的信息确认文件、审核方案对再认证审核的策划和上一周期审核的结果对审核做出具体安排，包括但不限于具体的时间安排、审核组各成员按岗位和活动以何种方式对获证组织进行审核的安排、高层沟通的安排、审核日程安排和会议的安排。审核组长应至少在实施审核三个工作日之前，与获证组织就审核计划进行充分沟通，确保双方没有异议。

再认证审核的内容应包括但不限于以下方面：

1）内部审核；

2）管理评审；

3）上一认证周期审核中发现的不符合项整改的有效性；

4）上次审核中发现的观察项进行跟踪；

5）投诉的处理；

6）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）管理体系在实现获证客户目标和各管理体系的预期结果方面的有效性；

8）持续的运行控制；

9）持续改进活动；

10）任何变更；

11）标志的使用和（或）任何其他对认证资格的引用。

7.3.5.3. 审核实施

审核组按照审核计划对获证组织进行审核，如审核过程中获证组织的认证范围与策划不一致，应对不一致的部分特别关注，必要时重新确认审核范围、变更审核计划，发生变更时，需向项目管理人员报告说明情况，由项目管理人员会商技术主管确定是否调整审核计划。

对于管理体系审核，如发现获证组织或其管理体系的运行环境（如法律的变更等）有重大变更时，再认证审核活动需要有单独的第一阶段审核。如果单独实施一阶段审核，再认证审核的方式与初次认证一、二阶段审核方式一致。

如果再认证审核发现不符合项和观察项，经沟通获得受审核组织确认，开具不符合项报告和观察项报告，要求受审核组织按整改要求针对发现的问题进行整改，并提供整改证据。审核组负责对整改情况进行验证。具体要求见7.1.5。

7.3.6. 再认证审核结论

审核组应对收集的所有信息和证据进行汇总分析，评价审核发现并就审核结论达成一致。

再认证审核结束，审核组应根据再认证审核结果对获证组织的管理体系管理是否满足所有适用的认证依据的要求进行评价，并判断是否推荐换发证书。

再认证审核结束，审核组长完成审核报告编制工作，并与获证组织进行沟通，确保双方对报告没有异议，并确保报告准确性。

7.3.7. 认证决定

中心应指派认证决定人员，对获证组织的认证申请实施认证决定，以决定：

1）同意换发认证证书；

2）补充认证决定所需的信息，包括但不限于申请材料、审核材料，再行决定；

3）不同意换发认证证书，通知获证组织不同意换发的理由。

认证决定人员实施认证决定时应以认证过程中收集的信息和其他相关信息为基础，以充分的证据证实获证组织管理体系得到了建立、实施、运行、监视、评审、保持和改进。

7.3.8. 证书发放

中心负责制作证书，将证书、审核报告发放给获证组织。

7.3.9. 审核方案记录与变更

同7.1.9。

7.4. 特殊审核

7.4.1. 变更或扩大认证范围

获证组织申请变更或扩大认证范围时，中心应对获证组织变更或扩大的认证范围进行全部适用条款的审核，最终形成是否同意变更或扩大认证注册范围的决定。变更或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，审核方式与监督审核或再认证审核方式一致。

7.4.2. 提前较短时间通知的审核

中心为调查投诉、对变更做出快速回应或对被暂停认证资格的获证组织进行追踪时，应指派审核组在提前较短时间通知获证组织后对其进行特殊审核。特殊审核原则上以现场审核方式进行，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，中心应在指派审核组时给予更多的关注；

3）审核组应制订审核计划，形成审核结论；

4）中心应根据审核结论作出认证决定。

7.4.3. 审核方案记录与变更

同7.1.9。

7.5 暂停、恢复、注销及撤销认证证书

7.5.1 总则

7.5.1.1 本中心制定暂停、恢复、撤销、注销认证证书的管理规定，并遵照执行，不得随意暂停、撤销、注销和恢复认证。

7.5.1.2 本中心在暂停、撤销、注销或恢复认证决定生效后，按国家认监委的要求及时上报信息。

7.5.2 认证证书的暂停、恢复

7.5.2.1 获证组织有以下情形之一的，本中心在调查核实后的 5 日内暂停其认证证书：

（1）管理体系持续或严重不满足认证要求的；

（2）故意的或持续的不满足管理体系适用的法律法规要求的；

（3）被有关执法监管部门责令停业整顿的；

（4）发生重大事故/事件的；

（5）拒绝配合执法监管部门的监督检查，或者提供虚假材料或信 息的；

（6）持有的与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的；

（7）不能按照规定的时间间隔接受监督的；

（8）未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的；

（9）不承担、履行认证合同约定的责任和义务的；

（10）主动请求暂停的；

（11）其他应当暂停认证证书的。

7.5.2.2 恢复

本中心可以根据暂停的原因和性质规定暂停的期限，但暂停期限最长不得超过 6 个月。暂停到期后，将恢复或撤销（含注销）认证证书。

7.5.2.3 本中心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、认证标志或引用认证信息。

7.5.2.4 暂停期间，如获证组织采取有效的纠正措施，造成暂停的原因已消除的，中心将恢复其认证资格，并保留相应证据。

7.5.3 认证证书的撤销

获证组织有以下情形之一的，本中心在获得相关信息并调查核实后 5 日内撤销其认证证书：

（1）注销或被撤销法律地位证明文件的；

（2 被执法监管部门认定存在严重违法失信行为的；

（3）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有效纠正的；

（4）其他应当撤销认证证书的。

7.5.4 认证证书的注销

获证组织主动申请不再保持认证资格时，中心应注销其认证资格，并保留相应证据。

8. 认证证书及认证标志要求

8.1. 证书有效期

管理体系认证证书有效期为三年，每年通过监督审核维持证书的有效性。

8.2. 证书内容

认证证书内容至少包括以下方面：

1）认证证书名称，例如：信息安全管理体系认证证书；

2）证书编号；

3）获证组织名称、统一社会信用代码、注册地址、受审核地址；

4）认证依据，可以包括所使用的行业特定标准；

5）通过认证的业务范围；

6）列明《适用性声明》文件的适用版本， 例如：XX.0版本；

7）颁证日期、换证日期和证书有效期。如发证日期：2022年4月30日，有效期至：2025年4月29日，首次发证日期：2022年4月30日；

8）中心的名称及其标志；

9）中心的印章和法定代表人或其授权人的签字；

10）认可标识及认可注册号(适用通过认可的体系)等。

如果认证所覆盖业务(或服务)及其所涉及的过程和覆盖的场所较多，需在证书附件上加以注明。

8.3. 证书编号

证书编号规则由中心进行明确规定。

同一个组织的认证范围覆盖多个场所并需要颁发子证书时，在子认证证书编号后加上“-”和序号，如-1(-2，-3，…)。

有效期内换发证书，认证证书编号和认证的有效期保持不变。

撤销证书后，原认证证书编号废止，不得再次使用。

8.4. 对获证组织正确宣传认证结果的控制

中心应采取授权使用标识的方式来要求获证组织在认证结果的宣传和使用中采用本规则确定的认证依据，同时注明通过认证的业务范围和认证证书编号。在认证证书被暂停期间或撤销后，应收回相应的授权。

不应授权获证组织在产品上使用上述标识，或以表示产品合格的方式使用上述标识。

8.5 认证标志的使用

本管理体系未使用认证标志。

9.对获证组织的信息通报要求及响应

为确保获证组织的管理体系持续有效，中心应要求获证组织建立信息通报制度，及时向中心通报以下信息：

1) 业务、地点、组织机构变化等情况的信息；

2) 顾客重大投诉的相关信息；

3) 组织的体系文件和业务重大变化时进行通报；

4) 有严重管理体系相关事故的信息，如：发生重大信息安全事件；

5) 其他重要信息(视情况)。

中心应对上述信息以及收集到的相关公共信息进行分析，视情况采取相应措施，包括增加监督审核频次在内的措施和暂停或撤销认证资格的措施。在发生重大客户投诉等严重情况时，中心需立即采取措施。

附录 1 ISMS 认证机构认证业务范围分类与分级

大类	中类	级别	描述	备注
01			政务	
	01.01	一	国家机构	包括人大、政府、法院、检察院等， 不含税务 机关和海关
	01.02	一	税务机关	
	01.03	一	海关	
	01.04	二	其他	例如政党，政协，社会团体等
02			公共	
	02.01	一	通信、广播电视	
	02.02	一	新闻出版	包括互联网内容的提供
	02.03	二	科研	涉及特别重大项目的应提升为一级
	02.04	二	社会保障	例如社会保险基金管理、慈善团体等。包括医疗保险
	02.05	二	医疗服务	
	02.06	三	教育	
	02.07	三	其他	例如市政公用事业（水的生产和供应、污水处理、燃气生产和供应、热力生产和供应、 城 市 水 陆 交 通 设 施 的 维 护 管 理 等 ）
03			商务	
	03.01	一	金融	例如银行、证券、期货、保险、资产管理等
	03.02	一	电子商务	以在线交易为主要特点，含网络游戏
	03.03	一	物流	包括邮政
	03.04	三	咨询中介	例如法律、会计、审计、公证等
	03.05	三	旅游、宾馆、饭店	
	03.06	三	其他	
04			产品的生产	产品包括软件、硬件、流程性材料和服务
	04.01	一	电力	包括发电和输、变、配电等
	04.02	一	铁路	
	04.03	一	民航	
	04.04	一	化工	
	04.05	一	航空航天	
	04.06	一	水利	
	04.07	二	交通运输	包括公路、水路、城市公共客运交通等， 不含 航空和铁路
	04.08	二	信息与通信技术	例如软、硬件生产及其服务， 系统集成及其服务，数字版权保护等
	04.09	二	冶金	
	04.10	二	采矿	含石油、天然气开采
	04.11	二	食品、药品、烟草	
	04.12	三	农、林、牧、副、渔业	
	04.13	三	其他	

注 1： CNAS 提出 ISMS 认证机构认证业务范围分类是为了在规范的框架下对认证机构的能力实施评审，并相应地限定其认可范围，以促使 ISMS 认证活动规范、有序地发展，控制认可风险；同 时给各认证机构开展能力分析和评价提供一致的框架。 该分类并不意味着 CNAS 批准认证机构可 以对每个类别中的任何组织实施认证活动。

注 2： CNAS 考虑到 ISMS 相关技术和知识与组织的业务活动具有相关性， 组织相关方和业内专家，

通过讨论和划分 ISMS认证组织业务活动的类型，提出了认证业务范围分类。该分类基于我国 ISMS 认证和认可活动当前的实践和经验， 注意涵盖了我国信息安全等级保护的重点领域， 例如：广播 电视网、通信网、金融银行、电力、铁路、民航、石油化工等，同时兼顾了其他行业领域。

注 3：由于 ISMS认证在世界范围内仍处于发展阶段，我国 ISMS认证的数量以及涉及的业务活动 类型都还有限,所以认证业务范围中组织业务活动类型的划分方式仍需随着我国 ISMS 认证的发 展和经验的增加不断改进。因此认证机构不宜直接将认证业务范围分类作为业务应用技术领域分 类，而需要以其为框架进一步分析和确定业务应用技术领域。

注 4： 认证业务范围分级是为了使CNAS在确定认证业务范围的评审方式时考虑相关的风险，从而 对认证机构业务活动的扩展进行控制， 降低认可风险。这里的风险是指CNAS认可的风险， 即 CNAS 认可的 ISMS认证机构所认证的组织的信息安全发生问题时， 连带使CNAS声誉受损或承担责任的 风险。每个中类的级别主要考虑了在该中类信息安全对于国家安全、社会秩序、公共利益、组织 及其相关方合法权益的重要性的典型情况。

附录 2　审核时间的确定

本附录为中心制定信息安全管理体系审核时间的程序，合同评审人员应针对每一个客户及其被认证的 ISMS，识别初次认证、监督审核和再认证审核所需花费的审核时间。

信息安全管理体系（ISMS）审核时间的确定原则:

一、初次审核（一阶+二阶）

（一）基准审核时间（按表 1 确定）

表 1　ISMS 审核时间表

在组织控制下工作的人员的数量	ISMS 初次审核审核时间（审核人日）	在组织控制下工作的人员的数量	SMS 初次审核审核时间（审核人日）
1-10	3	626-875	13
11-15	3.5	876-1175	14
16-25	4	1176-1550	15
26-45	5	1551-2025	16
46-65	6	2026-2675	17
66-85	7	2676-3450	18
86-125	8	3451-4350	19
126-175	9	4351-5450	20
176-275	10	5451-6800	21
276-425	11	6801-8500	22
426-625	12	8501-10700	23
＞10700	沿用以上规律		

（二）调整审核时间

根据受审核方的分布状态和体系的复杂程度，在基准审核时间的基础上对人日数进行调整。调整时应考虑以下因素（不限于这些因素）。

1、增加审核时间的因素

a）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），增加 5%审核时间；

b）需要访问临时场所，以确认拟认证管理体系中的常设场所的活动。每增加一个临时场所，增加 5%的审核时间，如有多个临时场所，并符合“多场所”的定义，则按多场所处理；多场所抽样及审核的要求详见 CNAS-CC11。

c）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 涉及复杂性高的过程，或数量相对较大的活动，或独特的活动），增加 5%的审核时间；

d）法规要求高，在《ISMS 认证机构认证业务范围分类与分级》中是一级风险，视具体情况增加 10%-20%审核时间；

e）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，过程中同时包括硬件、软件、过程和服务，增加 5%审核时间；

f）员工使用多于一种的语言（需要翻译或妨碍单个审核员独立工作）,该因素应增加 5%审核时间；

g）对外包和供应商（包括云服务）的依赖程度高，外包或供应商对重要业务活动有着很大影响的，该因素应增加 5%审核时间.

2、减少审核时间的因素

a）《ISMS 认证机构认证业务范围分类与分级》中为三级风险，该因素减少 10-20%审核时间；

b）客户组织保持了本机构其他管理体系认证的，该因素减少 30%审核时间；

c）客户组织管理体系成熟的或通过其他认证机构 ISMS 认证的， 该因素减少 20%审核时间；

d）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）,该因素减少 5%审核时间；

e）没有或非常有限的内部系统/应用开发,使用标准化的软件平台, 该因素减少 5%审核时间；

f）一般的过程，涉及一般的且重复性的任务；大量在组织控制下工作的人员从事相同的任务；很少的产品或服务， 该因素减少 30%审核时间；

g）很少或不依赖外包或供应商， 该因素减少 5%审核时间

二、监督审核审核时间的确定原则

每年监督审核的审核时间约为初审认证审核时间的 1/3。在策划监督审核时，应获得客户与认证有关的更新信息，并对审核时间进行审查并记录。

三、再认证审核审核时间的确定原则

再认证审核时间应考虑更新的客户信息。如企业信息有更新，则应基于更新的信息重新计算出组织初次认证审核时间，再认证审核时间应不少于初次审核所需时间的 70%；如再认证时组织的情况与初次认证审核时相同，则再认证审核时间大约为初次认证审核时间的 70%。审核时间应考虑管理体系绩效的评价结果。

注：1.增加审核时间的因素和减少审核时间的因素可以互相抵消；

2.在对表 1 所列审核时间进行调整时，减少量不应超过 30%。

3.根据以上得出的审核时间包含了一、二阶段审核时间，包含了在客户现场的审核时间及用于策划与准备以及编写报告的审核时间。这些用于非现场组合活动的时间，不宜使现场总审核时间少于上文计算出的 70%。

4.一、二阶段审核时间的分配一般按 1:2 进行分配；现场审核时间不得少于上文中计算出的 70%，这适用于初审、监督审核和再认证审核；

5. 监督与再认证审核时间不能少于 1 个审核人日，否则可能影响审核有效性。

6.确定审核时间的相关证据，包括人日数调整及其它例外情况均应予以记录。