附件 4

《信息安全管理体系认证规则》释义

【规则条款】

1　适用范围

1.1 为规范信息安全管理体系（以下简称 ISMS）认证活动，根据《中华人民共和国认证认可条例》和《认证机构管理办法》等法律法规，结合相关技术标准制定本规则。

1.2 本规则规定了认证机构实施 ISMS 认证的程序与管理的基本要求，是认证机构从事 ISMS 认证活动的基本依据。

1.3 在中华人民共和国境内从事 ISMS 认证活动应遵守《中华人民共和国认证认可条例》《认证机构管理办法》及本规则。

1.4 认证机构遵守本规则的规定，并不意味着可免除其所承担的法律责任。

【要点与释义】

1.本规则是认证机构从事 ISMS 认证活动的基本依据和底线要求，认证机构可在此规则的基础上制定更加详细的 ISMS 认证管理制度、程序文件等。

2.本规则适用于认证机构在中国境内开展的 ISMS 认证活动，认证机构在境外开展的 ISMS 认证活动不适用本规则。

3.认证依据包含《网络安全技术 信息安全管理体系 要求》（GB/T 22080）和/或《Information security, cybersecurity and privacy protection—Information security management systems—Requirements》（ISO/IEC 27001）的 ISMS 认证活动，需要符合本规则的要求。

4.特定领域的信息安全管理体系认证活动（如 ISO 27701 隐私信息管理体系认证等），认证依据不包含《信息安全管理体系 要求》（GB/T 22080）或《Information security, cybersecurity and privacy protection—Information security management systems-Requirements》（ISO/IEC 27001）的，其认证活动需要符合本规则的 3.9、3.10、4.2 和 5.12.1 等条款。

5.认证机构作为经营主体，应对开展的认证活动及其他行为负责。认证机构即使遵守本规则，但若存在其他违反法律法规的行为，仍需承担相应法律责任。

【规则条款】

2 **认证依据**

《网络安全技术 信息安全管理体系 要求》（GB/T 22080）/《Information security, cybersecurity and privacy protection—Information security management systems—Requirements》（ISO/IEC 27001）

【要点与释义】

1.认证依据规定了管理体系应满足的要求。认证机构开展信息安全管理体系认证活动，需持有有效版本的信息安全管理体系认证依据标准。

2.认证依据需要在管理体系认证证书中列明。认证机构发放的管理体系认证证书应列明现行有效的标准名称及标准号。如，信息安全管理体系认证所依据的现行标准为《网络安全技术 信息安全管理体系 要求》/《Information security, cybersecurity and privacy protection —Information security management systems—Requirements》，现行有效的标准号为GB/T 22080-2025/ISO/IEC 27001:2022。

【规则条款】

3 对认证机构的基本要求

3.1 获得国家认证认可监督管理委员会（以下简称国家认监委）批准、取得 ISMS 认证领域资质。

3.2 开展 ISMS 认证活动，应当围绕国家经济和社会发展目标，重点服务于经济社会高质量发展，不得影响国家安全和社会公共利益，不得违背社会公序良俗。

3.3 内部管理和认证活动符合 GB/T 27021.1/ISO/IEC 17021—1《合格评定 管理体系审核认证机构要求 第 1 部分：要求》和 GB/T 25067/ISO/IEC 27006—1，确保持续满足开展 ISMS

认证的基本要求。

3.4 建立风险防范机制，对从事ISMS认证活动可能引发的风险和责任采取合理有效措施。认证机构应能证明其已对ISMS认证活动引发的风险进行了评估，对引发的责任作出了充分安排（如保险或储备金）。

3.5 建立认证人员管理制度，明确认证人员的能力准则、选择条件、聘用和评价程序，以及能力提升机制。确保从事ISMS认证的人员持续具备相应职业素养和能力。

3.6 在拟开展的ISMS认证业务范围（认证业务范围分类见附录A表A），具备2名（含）以上ISMS专业领域审核员。认证机构应结合认证业务范围识别相关专业的学历和专业信息安全工作经历。相应认证业务范围的专业领域审核员，应具备如下条件之一：

（1）具有本科（含）以上学历：在中风险认证业务范围具有至少2年（含）以上该专业的信息安全工作经历或具有该专业的中级（含）以上技术职称；在高风险认证业务范围具有至少3年（含）以上该专业的信息安全工作经历或具有该专业高级技术职称；

注1：信息安全工作包括信息安全管理、信息安全技术研究与开发及服务、信息安全相关测评、信息安全教学等。

注2：认证机构应参照附录A表A确定ISMS认证业务范围的风险级别。

（2）取得ISMS正式审核员注册资格后，参加该认证业务

范围信息安全专业技术培训且考核合格，并且在ISMS专业领域审核员或技术专家的指导下完成一定数量的ISMS专业审核活动：中风险认证业务范围不少于4次10个现场审核人日，高风险认证业务范围不少于6次20个现场审核人日；

（3）作为项目主要参加人，在该专业完成一定数量的信息安全标准的制定、科研项目（应用于相应行业/过程的信息安全）和设计开发等信息安全专业技术工作。其中，高风险认证业务范围至少为2项，中风险认证业务范围至少为1项；

（4）低风险的认证业务范围，具有ISMS正式审核员注册资格。

3.7 应对其认证活动的公正性负责，不允许商业、财务或其他压力损害公正性。如：不得将申请认证的组织（以下称认证委托人）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。

3.8 对认证活动中所知悉的国家秘密、商业秘密负有保密义务。应通过在法律上具有强制实施力的协议，确保认证活动中所获得的信息在未经认证委托人书面同意的情况下，不向第三方透漏，认证行政监管有要求的除外。

3.9 应对 ISMS 认证活动的真实性、有效性负责，加强认证人员的管理及素质、能力提升，合理安排审核员的工作量。每个审核员参加包括 ISMS 在内的管理体系现场审核时间的总和不应超过 180 天/周期年。

3.10 认证机构拥有的ISMS有效认证证书的数量应与该机构ISMS审核员数量相匹配，人均每个审核员匹配的包括ISMS在内的管理体系有效认证证书总数不应超过50张/周期年。

3.11 不得委派未取得ISMS注册资格的审核员开展ISMS认证审核活动。

3.12 不得以“认证证书在国家认监委网站可查”或近似表述进行广告宣传。

【要点与释义】

1.认证活动应围绕我国经济社会发展目标，重点服务于经济社会高质量发展（如，推动制造业转型升级、实施乡村振兴战略、推进生态文明建设、发展现代服务业、促进消费升级等）。认证机构不得擅自开展涉及国家安全、政治组织、社会民俗、民族宗教等领域的认证业务。

2.认证机构应当建立健全风险防范机制，选择以储备金形式应对潜在风险的，需制定专门的储备金管理制度，明确储备金的计提标准、管理要求（包括专户存储、独立核算等）以及使用规范（包括使用条件、审批程序、补充机制等）。

3.认证机构应确保参与ISMS认证活动的人员能力满足认证机构资质审批的相关要求。同时，认证申请评审人员、认证审核人员、认证决定或复核人员需要具备GB/T 27021.1和GB/T 25067中列明的相应知识和技能，以确保ISMS认证的有效性。

4.在拟开展的ISMS认证业务范围，需要具备至少2名专业

领域审核员（专、兼职均可），专业领域审核员不能为ISMS实习审核员，ISMS实习审核员不评定专业领域。在拟开展的ISMS认证业务范围，专业领域审核员低于2人的，则不能开展该认证业务范围的ISMS认证活动。如，某认证机构拟在03.02电子商务业务范围开展ISMS认证，需要具备至少2名03.02电子商务领域的专业领域审核员。

5.认证机构应当基于本规则附录A，适用时可细分认证业务范围及其风险级别，并依据本规则3.6条款列明的条件，建立基于风险的认证业务范围专业领域审核员的能力评定准则，评估审核员和技术专家的专业领域。审核员的专业领域可通过以下5种方式评定：

（1）基于专业工作经历。通过此方式获得专业能力的，需要一定时间的全职专业信息安全工作经历。

（2）基于专业技术职称。对于中风险认证业务范围，以04.08信息与通信技术行业为例，如具有信息安全/网络空间安全中级及以上职称，可被评定为“04.08信息与通信技术”认证业务范围的专业领域审核员。

（3）基于专业审核经历。专业审核经历是指针对相应认证业务范围类别内的专业过程所实施ISMS认证审核的经历，如信息安全风险评估过程、信息安全风险处置过程、信息安全技术控制过程、数据中心物理安全控制过程、项目管理中的信息安全控制过程等。专业审核经历需要在取得ISMS正式审核员注册资格后在本认证机构内获得。专业审核经历需要在每次认证审核中，从首次会议到末次会议期间全程与专业领域审核员或技术专家

在同一组进行实习，同时，专业实习的ISMS审核员按ISMS实习审核员管理，其审核人日不计入该次ISMS认证审核的审核时间，但计入其周期年内的现场审核天数。审核人日数以该次现场审核专业过程的审核人日数计算。专业审核经历的次数，以参与全程的初次认证审核第二阶段审核、监督审核和再认证审核计算，不包括初次认证审核第一阶段审核和特殊审核。参加该认证业务范围的信息安全专业技术培训和考核时，培训可由认证机构自行组织，但须考核合格，培训情况和考核结果需要留有证据。

（4）基于专业技术工作。作为主要起草人参与制定信息安全标准的，所制定的信息安全相关标准应为国家标准或行业标准，所承担的角色应为主要起草人（前5名）；参与市厅级和高校以上（含）级别科研项目的，所承担的角色应至少为技术骨干。

（5）基于ISMS审核员注册应掌握的知识和技术，可以认定ISMS正式审核员（不含实习）具备了低风险级别认证业务范围的专业领域审核员能力。

6.对于不能满足本规则3.6条款专业领域条件，但在本规则发布前已被认证机构评定为专业领域审核员的（留存有证据材料），同时满足以下条件的可以维持专业领域审核员资格：

（1）本规则发布前，近5年在本机构作为专业领域审核员参与不少于10次专业审核经历；

（2）本规则发布后经专业领域审核员重新见证评审。见证评审是见证人在初次认证第二阶段审核、监督审核或再认证审核中与被见证人同组，见证其对专业过程的审核能力。见证人应为

经认证机构确认满足3.6条款要求的ISMS专业领域审核员，在被见证人能力不足时见证人应接管审核任务。见证人的见证时间不计入审核人日，但计入见证人和被见证人周期年内的现场审核天数。

7.通过认可的认证机构可采用认可机构认可的方式扩展ISMS认证审核员的认证业务范围专业领域，但未经认可的认证业务范围应按3.6列明的条件开展相应认证业务范围的审核员专业领域评定。

8.认证机构对认证活动中了解到的认证委托人/获证组织的保密信息，未经认证委托人/获证组织书面同意不得向第三方透露（包括无意透露），尤其是涉及国家秘密和商业秘密的信息。认证机构应制定认证活动保密制度，要求认证人员和技术专家签署保密协议。除认证委托人/获证组织自行公开或其与认证机构商定公开的信息外，所有信息均视为保密信息。

在认证审核前，认证机构应要求认证委托人识别并向认证机构告知其ISMS 范围内的哪些信息资产不允许认证机构接触，或者认证机构在接触相关信息资产时应满足哪些要求，包括法律要求、相关方的要求和认证委托人自身的要求。认证机构应满足所有这些要求，否则不应在认证活动中接触认证委托人的相关信息资产。

如果认证委托人事先没有禁止认证机构接触某一信息和相关资产，或未告知认证机构应满足的要求，但认证机构在认证过

程中发现自己并不具备接触该信息资产的资格和条件，应立即向认证委托人提出。审核组成员不宜在审核过程中以任何方式记录认证委托人的保密或敏感信息。审核组在离开认证委托人现场前，宜请认证委托人检查和确认审核组携带的文件、资料和设备中未夹带认证委托人的任何保密或敏感信息。

9.认证机构应对认证活动的真实性负责。为确保认证有效性，认证机构应合理安排审核员的工作量，给审核员留出充足时间开展审核策划、审核准备、审核报告编制，以及对不符合的整改措施进行审查、验证，并有充足时间接受继续教育、培训，保持和提升能力。

10.每个 ISMS 审核员（包括实习审核员）在 1 个周期年内（从 2026 年 3 月 1 日之后的任意起始日期开始计算，连续满 12 个月为一个周期年。例如，从 2026 年 3 月 16 日开始的周期年，截止日为 2027 年 3 月 15 日），参加包括 ISMS 在内的管理体系现场审核时间的总和不应超过 180 天。现场审核时间是审核时间的一部分，包括从首次会议到末次会议之间实施审核活动的所有时间。管理体系认证审核员超出 180 天参加的管理体系认证审核的认证结果，不具有证明作用。认证机构应对审核安排是否符合本规则 3.9 条款的情况进行持续监督，管理体系现场审核时间总和超过 180 天的审核员仍作为审核组成员参与现场审核的，该次现场审核无效，认证机构应重新组建符合本规则要求的审核组，在该次无效现场审核结束后 1 个月内完成对该认证项目的再次现场审核。通过再次现场审核的，该认证项目的认证证书才能持续有效，证书有效期与原证书相同。

对于违反本规则3.9条款规定的，市场监管部门将按照减少遗漏认证规则规定的程序进行处理，对相关认证机构、审核员从严处理，包括但不限于暂停认证机构在“认证认可业务信息统一上报平台”上传管理体系认证证书信息，以及在“全国认证认可信息公共服务平台”（认e云）展示其颁发的管理体系认证证书信息的权限。

11.管理体系认证审核员，如果同时拥有产品认证检查员或服务认证审查员注册资质，开展产品认证和服务认证的现场审核时间不计算在管理体系现场审核时间180天内。

12.ISMS认证审核员需要在同时满足以下情况并经本机构批准后，可被评定为本机构其他相应管理体系领域认证业务范围专业领域的技术专家：

（1）经本机构管理体系认证业务范围专业领域技术专家能力评定，符合管理体系认证业务范围专业领域技术专家的能力要求。

（2）未在相应管理体系认证领域注册为认证审核员或实习审核员。

例如，某审核员为“04.08信息与通信技术”认证业务范围的ISMS专业领域审核员，其没有ITSMS审核员资格，在其具备能力并经认证机构评定的前提下，可作为ITSMS相关专业领域的技术专家，但其不能再被评为ISMS“04.08信息与通信技术”专业领域的技术专家。其作为审核员身份和技术专家身份每年参与管理体系现场审核时间的总和不得超过180天。

13.人均每个审核员匹配的包括ISMS在内的管理体系有效认证证书总数不应超过50张/周期年。

（1）每个周期年内，认证机构持有的ISMS有效证书的数量不应超过ISMS认证审核员人数×50张。

（2）每个周期年内，认证机构持有的管理体系有效认证证书数量总计不应超过管理体系认证审核员人数×50张。

（3）上述ISMS认证审核员数量、管理体系认证审核员数量取本机构3月31日、6月30日、9月30日和12月31日注册的ISMS认证审核员、管理体系认证审核员数量的平均值；新规则正式实施前，管理体系认证审核员人均证书数大于50张的认证机构，应采取相应措施，确保在新规则正式施行后的一年内（2027年2月28日前），其管理体系认证审核员人数与证书数的匹配情况满足新规则的要求。

（4）管理体系认证审核员包括专职审核员和兼职审核员，不包括实习审核员。

（5）有效认证证书数包括子证书数，即所有带证书编号的认证证书数量总和；1张主认证证书附带N张子认证证书的，证书数量记为1+N张。

（6）有效认证证书数包括统计时点下的认证证书状态为“有效”和“暂停”的证书数量。

14.认证机构委派开展ISMS认证审核的所有审核员，均应取得ISMS审核员注册资格；对于不满足此条件并颁发认证证书的，应撤销相应认证证书，已委派的，应立即终止认证审核活动。

15.认证机构不得在其网站、宣传册、广告等相关材料以及市场推广等活动中，宣传其认证证书可在国家认监委相关网站查询。

【规则条款】

4　对认证人员的基本要求

4.1 遵守认证认可相关法律法规、部门规章及规范性文件的要求，具有从事认证工作的基本职业操守，对认证活动及其结果的真实性和有效性承担相应责任。

4.2 审核员应取得国家认监委确定的认证人员注册机构批准的 ISMS 审核员注册资格。

4.3 审核员不得接受超出其注册资格的认证审核任务。

4.4 不得发生影响认证公正性的行为，应主动告知认证机构其所了解的任何可能使本人或认证机构陷入利益冲突的情况。因认证人员未履行告知义务而导致非公正认证结果的，认证人员应当负有连带责任（如承担因此造成的经济损失）。

4.5 按要求接受人员注册/保持注册所要求的继续教育培训，以及认证机构要求的能力（包括知识和技能）提升活动，以持续具备从事 ISMS 认证工作相适宜的能力。

【要点与释义】

1.认证人员作为认证活动的实施者，应遵守认证认可相关的法律法规和政策要求，如《中华人民共和国认证认可条例》《认证机构管理办法》《信息安全管理体系认证规则》以及市场监管总局（国家认监委）发布的规范管理认证活动相关的公告、通知等文件。

2.认证人员应具有诚实、正直、客观、公正等职业操守，不得在认证活动中弄虚作假、减少遗漏认证程序，并对作出的记录、出具的结论负责。

3.“国家认监委确定的认证人员注册机构”目前指中国认证认可协会（简称 CCAA）。开展 ISMS 认证的审核员，应取得 CCAA 颁发的 ISMS 审核员注册证书。ISMS 审核员在实施审核时，其 ISMS 审核员注册证书应在有效期内且注册状态有效，注册执业机构应为安排认证审核任务的认证机构。

4.审核员在接到认证审核任务后，应确认注册资格与认证审核任务是否匹配。若注册资格与认证审核任务不匹配，应及时与认证机构沟通，不得接受该项审核任务。1 个周期年内管理体系现场审核时间总和超过 180 天的审核员，该周期年内不得再接受管理体系审核任务。

5.ISMS 实习审核员，不得接受独自开展 ISMS 审核活动的审核任务；非 ISMS 专业领域审核员，不得接受对 ISMS 专业过程的审核任务。

6.认证机构应公正开展认证活动，并对认证活动的公正性负责，不受商业、财务或其他方面的影响和干预。认证活动涉及的所有人员（无论专职还是兼职，审核员还是技术专家），应恪守公正，不得接受任何商业贿赂，不得损害认证活动的公正性。认证机构应建立相关机制确保认证活动涉及的所有人员，理解认证的公正性并保留相应证据，如签署公正性及保密声明等。

7.审核员在注册证书有效期内，为持续具备从事 ISMS 认证工作相适宜的能力，应满足 CCAA《管理体系审核员注册准则》关于继续教育的要求。

【规则条款】

5　认证程序

5.1 认证申请

5.1.1 认证机构应向认证委托人至少公开以下信息:

（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 ISMS 认证活动所依据的认证标准以及相关的认证方案、认证流程;

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

（4）拟向认证委托人获取的信息以及保密规定;

（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）对认证过程和结果的申诉、投诉规定;

（8）认证标准换版的规定（适用时）;

（9）“提前较短时间通知的审核”的情形;

（10）其他需要公开的信息。

【要点与释义】

1.认证机构应结合自身管理要求，规定其信息公开的途径/方式。认证机构应确保其公开的信息准确、真实。认证机构应适时评审公开信息的有效性，必要时予以更新。

2.认证机构应按照本规则 5.1.1 条款列明的内容进行信息公开，确保认证委托人在选择认证机构或签订认证合同前能够准确理解有关的认证要求，了解其所拥有的权利和义务以及应承担的责任。

3.认证机构应通过其网站或者其他形式公布相关信息，对相关信息的真实性、有效性负责，并保证以不同形式公布的信息具有一致性和可追溯性。

4.认证标准换版的规定可在认证标准换版时单独编制和公开。

【规则条款】

5.1.2 提出认证申请时，认证委托人应具备以下条件:

（1）取得合法主体资格，并处于有效期内;

（2）取得相关法律法规规定的行政许可（适用时），并处于有效期内;

（3）已按认证标准建立 ISMS，且运行满三个月;

（4）因获证组织自身原因被原发证机构暂停、注销或撤销 ISMS 认证证书已满一年（适用时）;

（5）原 ISMS 认证证书发证机构被国家认监委撤销 ISMS 认证资质已满三个月（适用时）;

（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;

（8）一年内未发生重大及以上级别的网络安全事件;

注：网络安全事件级别依据GB/T 20986判定。

（9）其他应具备的条件。

【要点与释义】

1.认证委托人应取得合法主体资格，合法主体资格包括企业法人、合伙企业、个人独资企业及其分支机构，以及机关、事业单位、社会团体、民办非企业单位等。

2.无合法主体资格的单位（如无营业执照的内设部门）申请认证，应以合法主体资格证照上载明的主体作为认证委托人。认证委托人申请签发子证书的场所，也应取得合法主体资格。

3.因获证组织自身原因，ISMS 认证证书被暂停、撤销、注销满一年后，原获证组织方可向认证机构（包括原认证机构）重新申请认证。ISMS 认证证书暂停期满后被撤销的，按 ISMS 认证证书被暂停的日期起算满一年。ISMS 认证证书暂停后未办理恢复，认证证书有效截止日期后失效的，在其认证证书暂停满一年后方可向认证机构（包括原认证机构）重新提出 ISMS 认证申请。

4.认证委托人被行政监管部门责令停产停业整顿的，应积极整改违法违规行为，消除相应后果。提出认证申请时，认证委托人应处于正常开展生产经营活动状态，且在 1 年内未发生重大及以上级别的网络安全事件。

【规则条款】

5.1.3 认证机构应要求认证委托人提供以下信息和文件资料:

（1）认证申请，包括认证委托人的名称、地址、认证依据的标准、申请的认证范围、认证范围内人员数量及影响体系有效性的外包过程;

（2）法律地位的证明文件，当 ISMS 覆盖多个法律实体时，应提供每个法律实体的法律地位证明文件;

（3）申请认证范围所涉及的网络安全法律法规要求的行政许可文件、资质证书等（适用时）;

（4）组织机构及职责;

（5）生产/服务的流程、班次及轮班情况;

（6）ISMS 运行满三个月的证据;

（7）一年内所发生的与网络安全相关的行政处罚以及整改情况（适用时）;

（8）其他需要提供的文件。

【要点与释义】

1.生产/服务的流程、班次及轮班情况，包括：生产流程图、服务流程图，轮班的班次、人数、各班次的工作内容和工作时间信息等。

2.ISMS 运行时间的认定应基于多维度证据，包括但不限于：体系文件发布实施时间、体系文件实施记录、内部审核报告、管理评审记录、过程运行数据等。ISMS 有效运行满足 3 个月的证据可以是不同形式，由认证机构自行确定可接受的证据形式，但至少需要满足GB/T 22080/ISO/IEC 27001 要求的文件化制度实施已满3个月。

【规则条款】

5.2 申请评审

5.2.1 认证机构应建立并实施相应程序，对认证委托人提交的申请信息和文件资料实施申请评审，仔细鉴别申请信息和文件资料的真伪，确定是否受理认证申请，并保存相应评审记录。

5.2.2 满足以下条件的，认证机构可以受理认证申请:

（1）认证委托人已具备受理条件（见 5.1.2）;

（2）认证机构具备实施认证的能力;

（3）双方就认证事宜达成一致。

5.2.3 对于新的认证委托人，仅在同时满足下列情况的前提下，认证机构可实施认证转换，否则应按照初次认证开展认证活动:

（1）认证机构具有认证委托人申请认证的 ISMS 认证范围的认可资格;

（2）认证委托人持有其他被认可的认证机构（原认证机构）颁发的带认可标识的 ISMS 认证证书（原认证证书）;

（3）原认证证书处于有效期内，未被原认证机构实施暂停或撤销;

（4）原认证机构认证业务正常运行，不存在认可资格到期、被暂停或撤销的问题;

（5）认证机构应获得认证委托人初次认证审核报告或最近一次的再认证审核报告、监督审核报告、审核中发现的不符合及其纠正措施。

5.2.4 认证机构应将申请评审的结果告知认证委托人。

【要点与释义】

1.申请评审时，认证机构应评估自身是否具备实施认证的能力，包括获批的认证业务范围、现有审核员能力、认证决定人员及其他认证人员能力、满足认证委托人其他要求的能力等。

2.其他被认可的认证机构，是指已取得认可机构授予的ISMS认可资格的认证机构。本释义所述认可机构为全球认可合作组织多边互认协议（GLOBAC MRA）签约成员，或国际认可论坛多边互认协议（IAF MLA）签约成员（2029年1月1日之前有效），且签署ISMS认证机构认可互认协议。

3.认证转换时，认证机构应收集认证委托人最近一个认证周期内的认证资料，包括初次认证或最近一次的再认证审核报告及最近一次的监督审核报告，所有在这些审核中发现的不符合及其纠正措施。

【规则条款】

5.3 认证合同及相关责任

5.3.1 通过申请评审的，认证机构应与每个认证委托人签订具有法律效力的认证合同，明确认证服务的费用、付费方式和违约条款，及认证委托人、认证机构和获证组织的责任。认证费用应由认证委托人向认证机构直接支付。

5.3.2 认证机构应及时向符合认证要求的认证委托人颁发认证证书，对获证组织 ISMS 运行情况进行有效监督，通过其网站或者其他形式向社会公布认证证书信息；因认证机构批准资质注销或被撤销导致获证组织 ISMS 认证证书无法有效保持的，需及时告知获证组织并作出妥善处理，并承担由此导致的获证组织在合同上约定或法律认定的经济损失。

5.3.3 认证委托人应遵守认证程序要求，如实提供相关材料和信息，配合认证行政监管部门的监督检查和认证机构对投诉的调查，及时向认证机构通报 ISMS 及 5.1.2 中条件的变更情况，承担选择的认证机构资质被撤销而带来的认证活动终止、认证证书无法使用的风险。

5.3.4 获证组织应遵守认证程序要求，如实提供相关材料和信息，通过ISMS认证后持续有效运行ISMS，配合认证行政监管部门的监督检查和认证机构对投诉的调查，在广告、宣传等活动中正确使用认证证书、认证标志和有关信息，及时向认证机构通报ISMS及5.1.2中条件的变更情况，承担选择的认证机构资质被撤

销而带来的认证证书无法使用的风险。

【要点与释义】

1.认证机构在2026年2月28日前已签订的认证合同可继续执行，但2026年3月1日（含）后开展的认证活动应符合本规则的要求。2026年3月1日（含）后新签订的认证合同应满足本规则5.3的要求。

2.认证委托人应向认证机构直接支付认证费用，不得通过第三方支付。认证委托人的上级单位（如认证委托人所属的集团公司、事业单位、社会团体或机关）或下级单位向认证机构支付费用是可接受的形式。个体工商户作为认证委托人时，可以由经营者向认证机构支付认证费用，其他类型的认证委托人的认证费用不得由个人支付。

3.2026年2月28日前已签订的认证合同中约定的付款方式不满足新版规则要求的，认证机构应与认证委托人及时签署补充协议或重新签署认证合同，明确2026年3月1日后认证费用由认证委托人直接支付给认证机构。

4.认证机构应在合同中约定认证委托人隐瞒真实信息的责任，以及因认证机构批准资质注销或被撤销导致获证组织ISMS认证证书无法有效保持的责任和经济赔偿。

【规则条款】

5.4 审核方案和审核策划

5.4.1 审核方案

5.4.1.1 认证机构应针对每一认证委托人建立认证周期内的审核方案，以清晰地识别所需的审核活动。

5.4.1.2 初次认证的审核方案应包括两阶段初次认证审核、获证后的监督审核和认证到期前的再认证审核。再认证的审核方案应包括再认证审核、获证后的监督审核和认证到期前的再认证审核。

5.4.1.3 初次认证审核和再认证审核是对认证委托人完整体系的审核，应覆盖 GB/T 22080/ISO/IEC 27001 所有要求，以及认证范围内的主要信息安全风险及所涉及的典型过程/活动、产品和服务。认证证书有效期内的监督审核累计应覆盖 GB/T 22080/ISO/IEC 27001 所有要求。

5.4.1.4 初次认证及再认证后的第一次监督审核应在认证证书签发之日起 12 个月内进行。此后，监督审核间隔不应超过 12 个月。

5.4.1.5 认证机构应考虑认证委托人不同班次完成的过程，以及其所证实的对每个班次的 ISMS 控制水平来策划对不同班次实施的审核程度，以确保审核的有效性:

（1）每次审核应至少对其中一个班次的生产或服务活动现场进行审核;

（2）未审核其他班次生产或服务活动现场的，应记录未审

核的理由。

【要点与释义】

1.一个认证周期内的审核方案中，应包括至少两次监督审核。监督审核的安排应同时满足以下要求：

（1）第一次监督审核应在证书签发之日起 12 个月内进行，第二次监督审核应在认证证书签发之日起 24 个月内进行；

（2）两次监督审核的时间间隔不应超过 12 个月，即本次监督审核的开始日期距上一次监督审核的结束日期不超过 12 个月；

（3）除再认证的年份外，监督审核每个日历年需要进行 1 次。

2.在具体实施认证审核过程中，认证机构可根据认证委托人 ISMS 的实际情况对审核方案进行必要的调整。

3.认证范围内的主要信息安全风险所涉及的典型过程/活动、产品和服务是指该过程/活动、产品和服务的实现过程涉及的主要信息安全风险，同时也能涵盖认证范围内的其他过程/活动、产品和服务的实现过程涉及的主要信息安全风险，认证机构应记录确定典型过程/活动、产品和服务的理由。原则上，至少应在同一认证业务范围分类内选取典型过程/活动、产品和服务，选取的典型过程/活动、产品和服务应具有代表性。

4.认证委托人存在多班次生产/服务情况的，认证机构应根据各班次的生产/服务内容，以及认证委托人对各班次的控制水平，策划对不同班次的审核。

5.不同班次的生产/服务的内容、过程相似的，每次的ISMS审核应审核至少一个班次的生产/服务活动现场;不同班次的生产/服务的内容、过程不相似的,每次审核应覆盖生产/服务实现的不同内容、过程的各班次。

【规则条款】

5.4.2 审核时间

5.4.2.1 审核时间包括在认证委托人现场的审核时间以及在现场审核以外实施策划、文件审核和编写审核报告等活动的时间。审核时间以人日计，1人日为8小时，不应通过增加工作日的工作小时数以减少审核人日数。

如果认证委托人工作日的实际工作时间不足8小时，则应延长现场审核天数以满足审核时间要求。

5.4.2.2 认证机构应以附录B所规定的审核时间为基础,考虑认证委托人有效人数、ISMS风险级别等因素，建立文件化的不同审核类型审核时间（包括现场审核时间）的确定方法。不同业务范围ISMS风险级别见附录A表A。

5.4.2.3 每次审核的审核时间确定过程应形成记录,尤其是减少审核时间的理由，减少的审核时间不得超过附录B所规定的审核时间的30％，现场审核时间不得少于所确定的审核时间的70%。如果审核人日计算后结果包括小数，应将其调整为最接近的半人日数。

5.4.2.4 认证机构应建立文件化的结合审核时间确定方法，ISMS 和其他管理体系实施结合审核的，结合审核的总审核时间不得少于多个单独体系所需审核时间之和的 80%。

【要点与释义】

1.对于市场监管总局（国家认监委）或认可机构未明确审核时间要求的管理体系，信息安全管理体系不能与其实施结合审核，也不能通过结合审核的方式减少审核时间。

2.现场审核时间的人日数计算最终结果含有小数的，应调整为就近的半人日数。如 5.3 人日应调整为 5.5 人日，5.2 人日应调整为 5 人日。

【规则条款】

5.4.3 多场所抽样方案

5.4.3.1 认证机构应建立并实施文件化的多场所组织认证抽样的规则，策划并保留多场所组织的抽样及审核时间确定的记录。

5.4.3.2 多场所抽样应基于与认证委托人活动或过程性质相关的 ISMS 风险的评价。

5.4.3.3 对涵盖相同活动、过程及 ISMS 风险级别的多个相似场所 ISMS 可进行抽样审核，抽样数量应不少于按以下方法计算的结果:

（1）初次认证审核：$Y=\sqrt{X}$;

（2）监督审核：$Y=0.6\sqrt{X}$;

（3）再认证审核：$Y=0.8\sqrt{X}$。

注：其中 Y 为抽样的数量，结果向上取整；X 为相似场所的总体数量。

5.4.3.4 对多个非相似场所，则不应抽样，初审和再认证审核应当逐一到各场所进行审核。监督审核应抽取不少于 30%的场所进行审核，且每次审核均应包括中心职能部门。第二次监督审核选取的场所通常不同于第一次监督审核所选取的场所。

5.4.3.5 确定多场所组织的现场审核时间时，可依据附录 B 计算出总的现场审核人日，将总的现场审核人日分配到不同的场所；分场所审核人日的计算方法也可参见 5.4.2，且现场审核时间不得少于依据附录 B 所确定的现场审核时间的 50%。

【要点与释义】

1.认证机构建立的多场所组织认证抽样规则，应包括多场所抽样的应用条件。可应用抽样的多场所，抽样数量计算结果出现小数点均应进位，如可抽样多场所数量为 3，按要求监督审核的抽样量计算结果为 1.04，抽样量应为 2。

2.认证机构根据各场所有效人数、ISMS 风险级别以及审核时间增减条件等，计算出总的现场审核人日，将总的现场审核人日分配到不同的场所；分场所审核人日的计算方法也可参见 5.4.2，采用此方法计算时现场审核时间不得少于依据附录 B 所确定的现场审核时间的 50%。

【规则条款】

5.4.4 组建审核组

5.4.4.1 认证机构应根据实现审核目的所需的能力和公正性要求组建审核组，至少 1 名实施第一阶段审核的审核员应参加第二阶段审核，每个审核组应包括:

（1）审核组长：认证机构应建立并实施审核组长的选择、培训以及任用的管理制度；审核组长应当具有管理和领导审核组达成审核目标的知识和技能，其能力应至少满足 GB/T 19011《管理体系审核指南》中对审核组长的通用要求;

（2）至少 1 名与认证委托人所属认证业务范围相匹配的 ISMS 专业人员（专业领域审核员或技术专家）。ISMS 和其他管理体系实施结合审核的，审核组还应包括其他管理体系的专业人员，确保专业人员的能力覆盖实施结合审核的全部管理体系;

（3）至少 1 名认证机构的专职审核员，并确保专职审核员全程参与 ISMS 审核过程。

5.4.4.2 技术专家主要负责为审核组提供技术支持，不作为审核员实施审核，不计入审核时间。

5.4.4.3 实习审核员应在正式审核员的指导下参加审核，不计入审核时间，其在审核过程中的活动由负责指导的正式审核员承担责任。审核组中实习审核员的数量不得超过正式审核员的数量。

5.4.4.4 审核组成员不得与认证委托人存在利益关系。

【要点与释义】

1.审核组成员是指组成审核组的审核员、实习审核员和技术专家，不包括可能一同进入认证委托人现场的观察员、翻译或其他外部人员。审核组中的审核员应承担审核任务和责任。

2.当认证委托人所属的认证业务范围包括不同分类的，ISMS 专业人员的专业能力应覆盖该认证委托人的全部认证业务范围分类。

3.每次审核均应有专职审核员全程参加，包括初次认证审核的第一阶段。当发生突发情况或不可抗力时，认证机构可更换专职审核员，但应确保审核过程全程有专职管理体系审核员参加。

4.ISMS 单体系审核时，审核组中应至少有 1 名 ISMS 专职审核员参与全程审核。ISMS 和其他管理体系结合审核的，审核组应至少有 1 名结合审核涉及的管理体系领域的专职审核员参与全程审核。例如，ISMS 与 ITSMS 结合审核的，审核组应至少有一名 ITSMS 或 ISMS 专职审核员。

5.专业实习的 ISMS 审核员在积攒专业审核经历时，与 ISMS 专业领域审核员全程同组的，其在审核中的活动和审核发现由 ISMS 专业领域审核员负责；与技术专家全程同组的，需要在审核组内指派一名 ISMS 审核员对其在审核中的活动和审核发现负责。

6.对于多场所的审核活动，不要求专职审核员参与每一个场所的现场审核。颁发子证书的场所的现场审核活动，应有专职审核员全程参加。

【规则条款】

5.4.5 审核计划

5.4.5.1 认证机构应依据审核方案制定每次现场审核的审核计划。审核计划至少包括：审核目的、审核准则、审核范围、现场审核的日期、时间安排和场所、审核组成员及审核任务安排。其中，审核员应注明 ISMS 审核员注册号，专业领域审核员和技术专家应标明专业代码，兼职审核员和技术专家应注明工作单位。

5.4.5.2 现场审核应安排在认证委托人的生产或服务处于正常运行时进行。

5.4.5.3 现场审核开始前，应将审核计划提交给认证委托人并经其确认。如需要临时调整审核计划，应经双方协商一致后实施。

【要点与释义】

1.生产或服务处于正常运行，是指产品或服务实现过程的主要环节正常进行。认证机构应在编制审核计划前，与认证委托人确认审核期间拟实施审核的生产或服务是否处于正常运行，现场审核不应安排在无生产/服务现场活动的时间段。

2.审核计划应注明兼职审核员和技术专家的工作单位。兼职审核员以及技术专家暂无工作单位的，可依据社保缴纳单位填写，如果未缴纳社保的，填写无。兼职审核员以及技术专家退休的，填写退休单位并注明已退休。

3.认证机构与认证委托人确认审核计划的方式，可包括邮件

或其他沟通途径，认证机构应留存沟通记录。

【规则条款】

5.5 实施审核

5.5.1 ISMS 认证审核应在认证委托人的现场实施，包括初次认证审核以及认证周期内的每年度的监督审核、再认证审核和特殊审核。

5.5.2 审核组应按照审核计划实施审核，并采用中文记录审核过程，可补充使用图片/音像作为记录。

5.5.3 审核组应会同认证委托人召开首、末次会议，认证委托人的最高管理者、ISMS 相关职能部门负责人应参加首、末次会议，认证机构应保留首末次会议签到记录、图片/音像证明材料。认证委托人的最高管理者不能参加首、末次会议的，应由获得书面授权的其他高级管理层成员参会，审核组应记录最高管理者缺席理由。

5.5.4 审核组应通过面对面访谈等形式，对认证委托人的最高管理者在 ISMS 中发挥领导作用的情况进行重点审核，并保留现场图片/音像、审核记录等证明材料。最高管理者不熟悉组织自身的信息安全方针、信息安全目标，未亲自参与并推动 ISMS 实施的，认证审核应不予通过。

5.5.5 发生下列情况的，审核组应向认证机构报告后终止审核：

（1）认证委托人对审核活动不予配合，审核活动无法进行；

（2）认证委托人的最高管理者或经授权的高级管理层成员缺席首、末次会议；

（3）认证委托人实际情况与申请材料有重大不一致；

（4）其他导致审核程序无法完成的情况。

【要点与释义】

1.审核组应以中文记录审核过程，图片/音像只能作为记录的补充。

2.认证委托人的最高管理者，是指认证委托人申请认证范围活动的主要负责人或决策者，可以是一个人或一组人。认证委托人仅对其某个组成部分申请认证的，最高管理者可以是该组成部分的负责人。

3.认证委托人对审核活动不予配合的情形，是指由于认证委托人的原因导致审核组无法按计划开展审核活动，或无法获取有效审核证据。

4.认证委托人实际情况与申请材料有重大不一致，是指认证委托人实际情况（如认证委托人的组织机构、场所、活动、认证范围内人员数量、产品和服务类型、管理体系运行时间等）与本规则 5.1.3 条款要求的申请材料不一致，对审核方案有重大影响，导致审核组无法按原来的策划开展审核活动。

5.如果认证机构因为未获得认证委托人的允许或无法满足适用的要求而不能接触相关信息资产，那么认证机构应对审核和认

证所受到的影响进行评估并采取相应的措施（例如终止审核、缩小审核和认证的范围等）。

【规则条款】

5.6 初次认证审核

5.6.1 总则

初次认证审核应分为两个阶段实施：第一阶段审核和第二阶段审核。两个阶段审核时间间隔最短不应少于5日，最长不应超过6个月。如需要更长的时间间隔，应重新实施第一阶段审核。

5.6.2 第一阶段审核

5.6.2.1 第一阶段审核的目的是通过了解认证委托人的ISMS和其对第二阶段的准备情况，确定其是否具备接受第二阶段审核的条件并策划第二阶段审核的关注点。第一阶段审核的内容包括但不限于以下方面：

（1）了解认证委托人的情况，包括其产品和服务、信息资产、支持性设施、生产/服务流程、现场运作、主要信息安全风险、适用的信息安全标准；

（2）评审认证委托人ISMS体系文件（含适用性声明），确认其与认证委托人产品和服务实现过程的信息安全管理相吻合；

（3）确认认证委托人申请信息和文件资料的真实性；

（4）审核认证委托人理解和实施GB/T 22080/ISO/IEC 27001标准的情况，特别是对信息安全风险、ISMS关键绩效、过程、信

息安全目标和运作的识别情况;

（5）确认认证委托人是否为第二阶段审核做好准备，已实施了内部审核和管理评审;

（6）确认认证委托人ISMS认证范围、体系覆盖范围内有效人数和场所;

（7）认证委托人的产品和服务实现过程的信息安全管理符合网络安全法律法规的情况。

5.6.2.2 为达到第一阶段审核的目的和要求，除下列情况外，第一阶段审核应在认证委托人现场实施:

（1）认证委托人已获本认证机构颁发的其他管理体系认证领域的有效认证证书，认证机构已对认证委托人ISMS有充分了解;

（2）认证委托人获得了经认可机构认可的其他认证机构颁发的有效的ISMS认证证书，通过对其文件和资料的审核可以达到第一阶段审核的目的和要求。

认证机构应记录未在现场进行第一阶段审核的理由。

5.6.2.3 认证机构应将认证委托人是否具备第二阶段审核条件的结论书面告知认证委托人，包括所识别的需引起关注的、在第二阶段可能被判定为不符合的问题。

5.6.2.4 认证机构通过第一阶段审核发现相关申请信息和文件资料存在虚假情况的，应终止认证活动。

5.6.3 第二阶段审核

5.6.3.1 第二阶段审核的目的是评价认证委托人ISMS的实施情况，包括对GB/T 22080/ISO/IEC 27001标准要求的符合性和体系的有效性。

5.6.3.2 第二阶段审核应在认证委托人的现场实施，至少覆盖以下内容:

（1）认证委托人ISMS与GB/T 22080/ISO/IEC 27001标准的符合情况及证据;

（2）依据ISMS关键绩效目标和指标，对绩效进行的监视、测量、报告和评审;

（3）认证委托人实施ISMS的能力以及在符合适用法律法规要求方面的绩效;

（4）认证委托人信息安全管理过程的运作控制;

（5）认证委托人的内部审核和管理评审;

（6）针对认证委托人ISMS方针的管理职责。

【要点与释义】

1.初次认证审核分为两个阶段审核，认证机构应在第一阶段审核结论的基础上策划安排第二阶段现场审核。

2.认证委托人获得了经认可机构认可的其他认证机构颁发的有效ISMS认证证书，是指认证委托人持有其他认证机构颁发的带认可标识的ISMS认证证书，该认证证书处于有效状态，且本次申请的认证范围不超出带认可标识的ISMS认证证书上的认证范围。

3.未进行第一阶段现场审核的，审核组应在第二阶段现场审

核时关注认证委托人申请信息和文件资料的真实性，发现存在认证委托人实际情况与申请材料有重大不一致的虚假情况的，应终止审核，认证机构确认申请信息和文件资料存在虚假情况的，应终止认证活动。

4.审核组应汇总第一阶段和第二阶段收集的审核证据，综合审核组所有成员的审核发现，做出初次认证的审核结论。

【规则条款】

5.7 监督审核

5.7.1 认证机构应对获证组织进行有效跟踪，依据审核方案对获证组织开展监督审核，并要求获证组织的最高管理者参与审核访谈，以确认获证组织 ISMS 与 GB/T 22080/ISO/IEC 27001 标准的持续符合性和运行的有效性。

5.7.2 每次监督审核应尽可能覆盖认证范围内的主要信息安全风险及所涉及的典型过程/活动、产品和服务，并确保在认证证书有效期内的监督审核覆盖认证范围内的主要信息安全风险及所涉及的所有典型过程/活动、产品和服务。

5.7.3 监督审核应重点关注获证组织的变更以及 ISMS 绩效的持续改进，监督审核的内容至少包括:

（1）内部审核和管理评审;

（2）对上次审核确定的不符合采取的纠正措施及效果;

（3）ISMS在实现获证组织目标和ISMS预期结果方面的有效

性;

（4）为持续改进而策划的活动的进展;

（5）持续的运作控制;

（6）任何变更;

（7）认证证书、认证标志的使用和（或）任何其他对认证信息的引用;

（8）ISMS 相关投诉的处理;

（9）上次审核后发生的重大及以上级别网络安全事件的调查与处理。

5.7.4 监督审核的时间应根据获证组织当前有效人数和ISMS风险级别确定，不少于依据附录 B 所确定的初次认证审核时间的1/3。

【要点与释义】

1.获证组织认证范围覆盖多个活动、产品和服务涉及的主要信息安全风险的，在一个认证周期内的监督审核应覆盖所有主要信息安全风险所涉及的典型过程/活动、产品和服务。

2.获证组织的认证范围包括季节性生产/服务活动的，监督审核策划时应考虑其季节性生产/服务情况，必要时应分多次进行监督审核。

【规则条款】

5.8 再认证审核

5.8.1 认证证书期满前，获证组织申请继续持有认证证书的，

认证机构应依据审核方案实施再认证审核，以判断获证组织的ISMS 作为一个整体与 GB/T 22080/ISO/IEC 27001 的持续符合性和运行的有效性。

5.8.2 再认证审核应在获证组织现场进行，并应在认证证书到期前完成。再认证审核的内容至少应包括:

（1）结合其内部环境和外部环境的变化情况，确认获证组织ISMS有效性及认证范围的持续相关性和适宜性;

（2）ISMS绩效持续改进的证实;

（3）ISMS在实现获证组织目标和ISMS预期结果方面的有效性。

5.8.3 再认证审核策划时应考虑获证组织最近一个认证周期内的 ISMS 绩效，包括调阅以往的监督审核报告。

5.8.4 再认证审核的审核时间应按 5.4.2 的要求，根据获证组织当前有效人数和 ISMS 风险级别来确定，不少于依据附录 B 所确定的初次认证审核时间的 2/3。

【要点与释义】

认证机构应关注获证组织的认证证书到期时间，提前进行再认证审核的策划安排，确保留有足够的时间在认证证书到期前完成再认证现场审核。不能在认证证书到期前完成现场审核的，认证机构应按初次认证开展认证活动，满足 5.6.2.2 的情况下第一阶段审核可不在认证委托人现场实施。

【规则条款】

5.9 特殊审核

5.9.1 扩大认证范围

对于已授予的认证，认证机构应对扩大认证范围的申请进行评审，并确定任何必要的审核活动，以作出是否可予扩大的决定。这类审核活动可以结合监督审核同时进行。

5.9.2 提前较短时间通知的审核

为调查投诉、重大及以上级别的网络安全事件，对变更作出回应或对被暂停的客户进行追踪，可能需要在提前较短时间或不通知获证组织的情况下进行审核，此时:

（1）认证机构应说明并使获证组织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，认证机构应在指派审核组时给予更多的关注。

【要点与释义】

1.认证机构应明确扩大认证范围的必要审核活动，包括文件审核和现场审核（适用时）。扩大认证范围审核活动的范围和深度，取决于申请评审和审核方案策划的结果。

2.特殊审核与监督审核同时进行的，应注意审核结论与审核目的的对应关系，同时保证特殊审核的充分性和监督审核的完整性。

3.发生涉及获证组织 ISMS 认证范围的投诉、重大及以上级别的网络安全事件、变更或有需要跟踪被暂停的认证证书的，认

证机构在评估认证有效性可能遇到的威胁后，可安排提前较短时间通知的审核。

【规则条款】

5.10 不符合项及其验证

5.10.1 对审核中发现的不符合，认证机构应要求认证委托人在规定的时限内进行原因分析，采取相应的纠正措施。

5.10.2 认证机构应对认证委托人所采取的纠正措施的有效性进行验证。认证委托人可以针对轻微不符合制定纠正措施计划，由认证机构在下次审核时验证。

5.10.3 严重不符合的验证时限应满足以下要求:

（1）初次认证：在第二阶段审核结束之日起6个月内完成;

（2）监督审核：在审核结束之日起3个月内完成;

（3）再认证：在原认证证书到期前完成。

5.10.4 对于认证委托人未能在规定的时限内完成对不符合所采取措施的情况，认证机构不应作出授予认证、保持认证或更新认证的决定。

【要点与释义】

1.对于轻微不符合，认证机构可要求认证委托人在规定的时限内进行原因分析并完成整改，也可要求认证委托人制定整改计划，并结合下一次现场审核进行验证，认证机构的处理方式应符合其自行制定的管理要求。

2.关于严重不符合的验证时限，应满足以下要求：

（1）初次认证审核的严重不符合在6个月内未完成验证的，认证机构应在验证期限截止后30日内重新实施一次第二阶段审核；

（2）监督审核的严重不符合在3个月内未完成验证的，表明获证组织ISMS运行有效性存在问题，认证机构应暂停或撤销认证证书；

（3）再认证审核的严重不符合未在认证证书到期前完成验证的，认证证书到期自动失效。获证组织再次申请认证的，认证机构应按初次认证开展认证活动，满足5.6.2.2的情况下第一阶段审核可不在认证委托人现场实施。

【规则条款】

5.11 审核报告

5.11.1 认证机构应就每次审核向认证委托人提供书面的审核报告。审核组长应对审核报告的内容负责。

5.11.2 审核报告的内容应准确、简明和清晰，反映认证委托人ISMS的真实状况，描述对照GB/T 22080/ISO/IEC 27001标准的符合性和有效性的客观证据信息，及对认证结论的推荐意见。

5.11.3 审核报告至少应包括或引用以下内容:

（1）认证机构名称;

（2）认证委托人的名称和地址及其代表;

（3）审核类型（如初次认证、监督、再认证或其他类型）；

（4）结合、联合或一体化审核情况（适用时）；

（5）审核准则；

（6）审核目的及其是否达到的确认；

（7）审核范围，特别是标识出所审核的组织、职能单元或过程，以及审核时间；

（8）任何偏离审核计划的情况及其理由；

（9）任何影响审核方案的重要事项；

（10）审核组成员姓名、身份及任何与审核组同行的人员；

（11）审核活动（现场或非现场，永久或临时场所）的实施日期和地点；

（12）应描述与审核类型要求一致的审核发现、审核证据（或审核证据的引用）以及审核结论，重点反映认证委托人主要信息安全风险识别和控制情况、内部审核和管理评审的过程、所取得的绩效，认证委托人实际情况与其预期信息安全目标之间存在的差距和改进机会；

（13）与网络安全相关的行政处罚，及相关原因分析和整改措施的有效性（适用时）；

（14）上次审核后发生的影响认证委托人 ISMS 的重要变更（适用时）；

（15）获证组织对认证证书和认证标志使用的控制情况（适用时）；

（16）对以前不符合采取的纠正措施有效性的验证情况（适用时）；

（17）已识别出的任何未解决的问题；

（18）说明审核基于对可获得信息的抽样过程的免责声明；

（19）审核组的推荐意见以及对申请的认证范围适宜性的结论。

5.11.4 认证机构应保留用于证实审核报告中相关信息的审核证据。

5.11.5 对终止审核的项目，审核组应将终止审核的原因以及已开展的工作情况形成报告，认证机构应将此报告提交给认证委托人。

【要点与释义】

1.初次认证审核第一阶段、初次认证审核第二阶段、监督审核、再认证审核、特殊审核结束后，认证机构均应向认证委托人提供书面审核报告。第一阶段的审核报告可不包括本规则第5.11.3 条款中的全部内容。

2.“应描述与审核类型要求一致的审核发现、审核证据（或审核证据的引用）以及审核结论”是指：

（1）初次认证审核第一阶段的审核报告，应覆盖本规则5.6.2.1 条款要求内容；

（2）初次认证审核第二阶段的审核报告，应覆盖本规则5.6.3.2 条款要求内容；

（3）监督审核的审核报告，应覆盖本规则 5.7.3 条款要求内容；

（4）再认证审核的审核报告，应覆盖本规则 5.8.2 条款要求内容；

（5）扩大认证范围审核的审核报告，应覆盖拟扩大的 ISMS 认证范围（包括增加的过程/活动、产品、服务、场所及有效人数）以及获证组织 ISMS 实施情况；扩大认证范围与监督审核结合实施的，还应满足本条释义（3）的要求；

（6）提前较短时间通知审核的审核报告应与审核目的要求一致。

3.审核组长对审核报告所有内容的真实性、准确性承担责任。

4.认证审核报告应描述认证委托人（或获证组织）受到的与网络安全相关的行政处罚情况，及相关原因分析和整改措施的有效性。不同审核类型描述的信息所覆盖的时期不同：

（1）初次认证审核：审核前一年内的；

（2）监督审核：自上次审核结束至本次审核之间的；

（3）再认证审核：认证证书有效期内的。

5.除审核报告外，认证机构应妥善保存在认证审核过程中收集的、用于证实审核报告所陈述信息，特别是审核发现和结论的证据，如审核记录等。

【规则条款】

5.12 认证决定

5.12.1 认证机构应在对审核报告、不符合的纠正措施及验证情况和其他信息进行复核、综合评价的基础上，作出认证决定。认证决定人员应为认证机构的专职认证人员，并不得为审核组成员，能力应满足关于认证机构资质审批的相关要求。认证决定过程不得外包，认证决定须由中华人民共和国境内的工作人员作出。

5.12.2 认证机构有充分的证据确认认证委托人满足下列条件的，应作出授予、更新、扩大认证范围的决定:

（1）5.1.2 中的条件;

（2）对于严重不符合，已评审、接受并验证了纠正措施的有效性；对于轻微不符合，已评审、接受了认证委托人的纠正措施或计划采取的纠正措施;

（3）认证委托人的 ISMS 符合 GB/T 22080/ISO/IEC 27001 标准要求且运行有效;

（4）认证委托人按照认证合同规定履行了相关义务。

5.12.3 初次认证审核的认证决定应在现场审核后 6 个月内完成。否则应在推荐认证注册前再实施一次第二阶段审核。

5.12.4 再认证审核的认证决定宜在上一认证周期认证证书到期前完成，最迟应在认证证书到期之日起 6 个月内完成。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。

5.12.5 认证委托人不能满足 5.12.2 要求的，认证机构应以书面形式告知其未通过认证的原因。

5.12.6 对于监督审核，认证机构在满足下列条件时，可根据审核组长的肯定性结论保持对获证组织的认证，无需再进行独立的认证决定:

（1）监督审核未发现严重不符合及其他可能导致认证证书暂停、撤销的情况;

（2）获证组织认证信息未发生变更，不存在扩大、缩小认证范围的情况;

（3）认证机构建立了监督审核的监视机制并予以实施，可确保监督审核活动的有效性。

【要点与释义】

1.在中华人民共和国境内开展的所有类型的 ISMS 认证，认证决定过程必须在中华人民共和国境内实施，且必须由中华人民共和国境内的工作人员做出。

2.认证决定过程包括对审核报告等认证记录的复核，并做出认证决定，该过程可由一个人或一组人完成；如果是一组人，其中做出最终认证决定的人员应为认证机构的专职认证人员；认证机构可选择兼职技术专家为认证决定提供技术支持。

3.授予、更新、扩大认证范围的决定，必须基于对审核的发现、不符合及其验证结果等信息的综合评价，并有充分证据证明

已满足本规则第 5.12.2 条款的所有要求。

4.认证机构宜在获证组织的认证证书到期前完成再认证审核的认证决定，使再认证证书与原证书无缝连接；在获证组织的认证证书到期前未完成再认证决定的，认证机构应注意后续认证活动的时效性。重点关注以下情形：

（1）再认证审核开具轻微不符合的，轻微不符合的关闭（对纠正措施计划的评审和接受）和认证决定，可在原认证证书到期后 6 个月内完成。

（2）再认证审核开具严重不符合的，严重不符合的关闭（对纠正措施有效性的验证）需要在证书到期前完成，认证决定应在原认证证书到期后 6 个月内完成。

（3）在原认证证书到期后 6 个月内仍未完成认证决定的，获证组织应重新申请认证。重新申请认证时，认证机构应按初次认证审核开展认证活动。

5.对于监督审核，如满足本规定第 5.12.6 条款的要求，可以不单独进行“保持认证的认证决定”，可根据审核组提供的监督审核报告及其中“建议保持认证”的审核结论，保持对获证组织的认证。

6.对监督审核不单独进行“保持认证的认证决定”的前提是，认证机构建立了文件化的监督审核的监视机制，并保留实施了监视的证据。

7.监督审核的发现可能导致认证证书暂停或撤销时，认证机

构应按本规则 5.12 条款的要求进行认证决定。监督审核的结论涉及认证证书变更的（如扩大认证范围、变更证书信息等），认证机构也应按本规则 5.12 条款的要求进行认证决定。

【规则条款】

6　认证证书和认证标志

6.1 总则

6.1.1 认证机构应制定文件化的管理制度，要求获证组织正确使用 ISMS 认证证书和认证标志，以满足《认证证书和认证标志管理办法》相关规定。

6.1.2 获证组织可以在认证证书有效时使用 ISMS 认证证书和认证标志，并接受认证机构的监督管理。认证证书处于暂停期间、被撤销或注销后，不得继续使用认证证书和认证标志。

6.1.3 获证组织应当在广告等有关宣传中正确使用 ISMS 认证标志，不得在产品上仅标注 ISMS 认证标志，只有在注明获证组织通过 ISMS 认证及认证机构名称的情况下，方可在产品包装上标注 ISMS 认证标志。

6.1.4 认证机构发现获证组织未正确使用认证证书和认证标志的，应当要求获证组织立即采取有效纠正措施，并跟踪监督纠正情况。

【要点与释义】

1.认证机构应建立文件化的认证证书和认证标志管理制度，

且该制度应符合国家认监委关于认证证书和认证标志管理的相关要求，如《认证证书和认证标志管理办法》等，避免误导公众或侵犯公共利益。

2.认证机构应结合监督审核和再认证审核，现场查看获证组织对认证证书和认证标志的使用情况。同时，认证机构应根据掌握的获证组织的认证证书状态变化情况，对获证组织正确使用认证证书和认证标志履行告知和监督义务。

3.获证组织仅可在认证证书处于有效状态的情况下使用该认证证书，如认证证书处于暂停期间、被撤销或注销后，认证机构应要求获证组织不得使用认证证书和认证标志；认证证书被暂停、撤销或注销的，获证组织应及时对正在使用的认证证书和认证标志进行处理，如包装或宣传材料等不可再继续使用认证证书和认证标志的信息，原印制有认证证书和认证标志信息的包装或宣传材料等应妥善处理。

4.信息安全管理体系认证标志和证书信息，仅可在产品可以分割的包装（指包装可以从产品上移除且不会导致产品分解、碎裂或损坏）上使用，需使用中文注明获证组织通过信息安全管理体系认证及认证机构名称，以免与产品和服务认证标志混淆而误导公众。

【规则条款】

6.2 认证证书

6.2.1 认证机构应及时向认证决定符合要求的组织出具认证证书，认证证书的有效期最长为3年。

6.2.2 认证证书有效期的起算日期为认证证书签发日期，认证证书的签发日期不应早于作出认证决定的日期。

6.2.3 对于未能在原认证证书到期前完成再认证决定的，获证组织的 ISMS 认证证书到期后自动失效，直至获得新签发的再认证证书，新签发的再认证证书的终止日期不超过上一认证周期终止日期再加 3 年。

6.2.4 对每张 ISMS 认证证书应赋予一个认证证书编号，认证证书编号应遵循一定的规律，具体详见附录 C。

6.2.5 认证证书在中华人民共和国境内使用的，认证证书应使用中文。

6.2.6 认证证书的信息应真实、准确，不产生误导，并至少包含以下内容:

（1）获证组织名称、统一社会信用代码、注册地址、认证范围所覆盖的经营地址。若认证的 ISMS 覆盖多场所，应表述认证所覆盖的所有场所的地址信息;

注：认证证书中可不包括临时场所，在认证证书上展示临时场所的，应注明这些场所为临时场所。

（2）获证组织 ISMS 所覆盖的产品、活动、服务的范围；包括每个场所相应的认证范围，且没有误导或歧义（适用时）；

（3）认证依据的认证标准 GB/T 22080/ISO/IEC 27001 所采用的当时有效版本的完整标准号;

（4）认证证书应包括适用性声明的版本;

注：如果适用性声明的变更没有改变认证范围中控制的覆盖范围，则不要求更新认证证书。

（5）认证证书签发日期和有效截止日期，认证证书应注明: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;

（6）认证证书编号（或唯一的识别代码）;

（7）认证机构名称、地址;

（8）认证标志、相关的认可标识及认可注册号（适用时）;

（9）认证证书信息及认证证书状态的查询途径。

【要点与释义】

1.本规则实施前签发的有效期超过 3 年的再认证证书，可以继续使用至该认证证书到期；本规则实施后，新签发的再认证证书有效期不得超过 3 年。

2.存在以下情况的，认证机构不能按照再认证签发认证证书:

（1）原证书到期前未完成再认证现场审核的;

（2）原证书到期前未完成严重不符合的整改和验证的;

（3）原证书到期后 6 个月内未完成再认证审核的认证决定的。

3.本规则实施后，认证机构颁发的 ISMS 认证证书，证书编号应遵循本规则附录 C 的编号规则,且该证书编号应具有唯一性。

4.本规则实施前颁发的认证证书，证书编号不符合本规则附录C编号规则的，认证机构可结合监督审核和再认证审核更换认证证书，换证时须按本规则附录C的编号规则对认证证书重新编号。

5.认证机构应在2029年3月1日前完成所有不符合本规则附录C的编号规则认证证书的换证工作。

6.认证证书上载明的获证组织名称、统一社会信用代码和注册地址应与其合法主体资格证明文件载明信息保持一致；ISMS认证范围应在其合法主体资格证明文件载明的业务范围内。

7.认证机构应在认证证书上注明认证证书状态的查询方式，确保利益相关方和社会公众能查询到该认证证书状态的有效信息。

【规则条款】

6.3 认证标志

认证机构自行制定的认证标志的式样、文字和名称，不得违反法律、行政法规的规定，不得与国家统一的自愿性认证标志或其他认证机构自行制定并公布的认证标志相同或者近似，不得妨碍社会管理，不得有损社会道德风尚。

【要点与释义】

1.认证机构可根据需要，确定是否制定本机构信息安全管理体系认证标志。自行制定管理体系认证标志的，应建立管理体系认证标志的管理制度，明确认证标志式样、使用要求等。

2.认证机构自行制定的信息安全管理体系认证标志，须确保

其合法性，应符合本规则第 6.1 条款的相关要求。

【规则条款】

7　认证证书的暂停、撤销和注销

7.1 总则

认证机构应建立并实施认证证书暂停、撤销和注销的文件化的管理制度，不得随意暂停、撤销和注销认证证书。

【要点与释义】

1.认证机构应建立文件化的认证证书暂停、撤销和注销管理制度或程序文件，制度或程序文件应包括获证组织认证证书暂停、撤销和注销的适用情形及处理流程，适用情形应包括本规则第 7.2.1 条款、第 7.3 条款和第 7.4 条款中列明的情形。

2.认证机构不得随意暂停、撤销和注销获证组织的认证证书。认证机构应按本规则规定的暂停、撤销和注销情形以及认证机构的管理制度，执行认证证书的暂停、撤销和注销，并保留暂停、撤销和注销相关记录性资料。

【规则条款】

7.2 认证证书的暂停

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5日内暂停其认证证书，并保留相应证据:

（1）ISMS 持续或严重不满足认证要求的，包括 ISMS 文件

与实际业务运作严重脱离;

（2）不满足 ISMS 适用的法律法规要求，且未采取有效纠正措施的;

（3）受到与网络安全相关的行政处罚，且尚未完成整改的;

（4）发生重大及以上级别网络安全事件，反映获证组织 ISMS 运行存在重大缺陷的;

（5）拒绝配合市场监管部门的认证执法监督检查，或者提供虚假材料或信息的;

（6）持有的与 ISMS 认证范围有关的行政许可文件、资质证书等过期失效的;

（7）不能按照规定的时间间隔接受监督审核的;

（8）未按相关规定正确引用和宣传获得的认证证书和有关信息，包括认证证书和认证标志的使用;

（9）不承担、履行认证合同约定的责任和义务的;

（10）被有关行政监管部门责令停产停业整顿的;

（11）发生与网络安全相关重大舆情的;

（12）主动请求暂停的;

（13）监督审核时发现的严重不符合的纠正措施未能在 3 个月内完成验证的;

（14）其他应暂停认证证书的。

7.2.2 认证机构可根据暂停的原因和性质确定暂停期限，暂停期限最长不得超过 6 个月。

7.2.3 暂停期间，ISMS 认证证书暂时无效。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，认证机构应恢复其认证证书，并保留相应证据。

【要点与释义】

1.认证机构应对获证组织的行政许可文件、资质证书等持续有效情况开展调查核实，并在合同中约定获证组织应及时通报的相关变化情况。

2.对适用暂停认证证书的情形，认证机构应在调查核实后的 5 日内暂停认证证书。若认证机构在作出暂停决定前，已确认该暂停情形在调查核实后 5 日内彻底消除且无再发生风险，可不予暂停；若暂停决定已作出，则须认证机构正式验证并确认暂停原因已消除后，方可恢复认证证书。

3.第一次监督审核未能在认证证书签发后 12 个月内开展的，以及第二次监督审核未能在第一次监督审核按期结束后 12 个月开展的，认证机构应暂停认证证书。认证证书因不能按期接受第一次监督审核被暂停，在暂停期间认证证书状态恢复，第二次监督审核未能在认证证书签发之日起 24 个月内开展的，认证机构应暂停认证证书。

4.获证组织可根据自身需求与认证机构协商一致，提前进行再认证审核。获证组织选择提前再认证的，认证机构应确保在认证周期内的每个日历年有一次监督审核或再认证审核，且提前再认证审核时间距离上一次监督审核不应超过 12 个月，否则应暂

停认证证书。

5.认证证书被暂停后，认证证书状态应由有效变更为暂停。认证机构应公开认证证书的暂停起止日期，通知并要求获证组织暂停期间不得使用认证证书和认证标志。

6.认证机构应根据暂停的原因和实际情况确定暂停期限，暂停期限最长不得超过6个月,暂停截止日期不应超过证书有效期。

7.暂停期内，认证机构确认暂停原因已消除的，应恢复获证组织的认证证书，证书状态由暂停变更为有效，并告知其可以恢复使用认证证书和认证标志。暂停期限已满，暂停原因仍未消除的，应按照本规则第7.3条款的规定撤销认证证书。

【规则条款】

7.3 认证证书的撤销

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日内撤销其认证证书，并保留相应证据:

（1）被注销或撤销法律地位证明文件的;

（2）被“国家企业信用信息公示系统”和“信用中国”列入严重违法失信名单的;

（3）认证证书的暂停期限已满，但导致暂停的问题未得到解决或有效纠正的;

（4）经行政监管部门确认因获证组织违规而造成重大及以上级别网络安全事件的;

（5）ISMS 没有运行或者已不具备运行条件的；

（6）其他应撤销认证证书的。

【要点与释义】

1.对于适用撤销认证证书的情形，认证机构应在获得相关信息并调查核实后 5 日内撤销认证证书，认证证书状态由有效（或暂停）变更为撤销，通知并要求获证组织停止使用认证证书和认证标志。

2.撤销的认证证书失效，且不可恢复。

【规则条款】

7.4 认证证书的注销

获证组织主动申请不再保持认证证书时，认证机构应确认不存在暂停或撤销情形后注销其认证证书，并保留相应证据。

【要点与释义】

1.获证组织主动申请不再保持认证证书时，认证机构应确认该认证证书是否存在暂停或撤销情形。存在暂停或撤销情形的，应撤销其认证证书，证书状态由有效变更为撤销；不存在暂停或撤销情形的，应注销其认证证书，证书状态应由有效变更为注销。认证机构应通知并要求获证组织停止使用该认证证书和认证标志。

2.注销的认证证书失效，且不可恢复。

【规则条款】

8　申诉（投诉）处理

8.1 认证机构应建立并实施文件化的申诉（投诉）处理制度。认证委托人对认证决定有异议的，可以向认证机构提出申诉。任何组织和个人对认证过程和认证决定有异议的，可以向认证机构提出投诉。

8.2 申诉（投诉）的提交、调查和决定不应造成针对申诉人/投诉人的歧视。认证机构对申诉人（投诉人）、申诉（投诉）事项的信息应予以保密。

8.3 认证机构应及时、公正、有效地处理申诉（投诉），采取必要的纠正措施。对申诉（投诉）的处理决定，应由与申诉（投诉）事项无关的人员作出，或经其审核和批准，并应在 60 日内将处理结果书面告知申诉人（投诉人）。

【要点与释义】

1.认证机构应建立文件化的申诉（投诉）处理制度或程序文件，规定申诉（投诉）提交渠道、受理条件、调查处理程序、审核和批准程序、时限要求及结果告知方式等，并指定专人负责处理。认证机构应通过其网站或者其他形式公开申诉（投诉）渠道（如受理邮箱、电话等）。

2.认证机构处理申诉（投诉）时，不得存在歧视、区别对待等情形。认证机构须对申诉（投诉）人和申诉（投诉）事项的相关信息严格保密，申诉（投诉）处理人员应签署保密承诺书等。

【规则条款】

9 信息公开与报告

9.1 认证机构应建立并实施文件化的认证信息报告制度。按照国家认监委关于认证信息上报的要求，按时上报认证相关信息，至少包括:

（1）上一年度工作报告;

（2）社会责任报告;

（3）认证计划及认证结果;

（4）认证证书的状态;

（5）其他应报告的信息。

9.2 认证机构应至少在现场审核实施前 3 日，将审核计划上报国家认监委。

9.3 认证机构在颁发认证证书后，应在次月 10 日前将认证结果相关信息报送国家认监委。

认证机构应通过其网站或者其他形式，向公众提供查询认证证书有效性的方式，不得仅提供“国家认监委”或“全国认证认可信息公共服务平台（认 e 云）”查询路径。

9.4 认证机构应通过其网站或者其他方式公开暂停、撤销、注销认证证书的信息。暂停认证证书的，还应明确暂停的起始日期和暂停期限。认证机构应在暂停、撤销、注销认证证书之日起 2 个工作日内，按规定程序和要求将相关信息报送国家认监委。

9.5 获证组织发生重大及以上级别网络安全事件的，认证机构应对该组织的认证过程进行自查，并按照认证行政监管部门的要求，在规定的时间内提供相关认证材料。

【要点与释义】

1.认证机构应履行公开认证证书信息的主体责任，公布认证证书信息的自有查询方式。公开的认证证书信息应包括：获证组织名称及统一社会信用代码、认证范围、认证依据、证书编号、签发日期和有效截止日期、是否被认可及认可机构名称等。认证证书暂停的，还应公开暂停起止日期；认证证书撤销、注销的，还需公开撤销、注销日期。

2.认证机构的自有查询方式，不得仅链接跳转至国家认监委官方查询平台，如“全国认证认可信息公共服务平台（认e云）”等；否则，不能认为是认证机构的自有查询方式。

【规则条款】

10　认证记录

10.1 认证机构应建立文件化的认证记录、认证资料归档留存制度，记录认证活动全过程并妥善保存。归档留存期限为认证证书有效期届满之日起2年以上，或被注销、撤销之日起2年以上。

10.2 认证记录应真实、准确、完整，以证实认证活动得到有效实施。认证记录包括但不限于:

（1）认证申请书;

（2）认证申请评审记录;

（3）认证合同;

（4）审核方案，包括多场所抽样方法（适用时）;

（5）确定审核时间的理由（计算过程）;

（6）审核计划;

（7）首、末次会议签到表;

（8）现场审核记录;

（9）不符合报告及验证记录;

（10）审核报告;

（11）认证决定记录。

10.3 在认证证书有效期内，认证活动参与各方签字或者盖章的认证记录、资料等，应保存具有法律效力的原件，可以纸质文件或符合《电子签名法》规定的电子文件形式保存。签字或盖章的认证记录至少包括:

（1）认证申请书;

（2）认证合同;

（3）审核计划;

（4）首、末次会议签到表;

（5）不符合报告;

（6）认证决定的结论。

10.4 认证记录应使用中文，以电子文档形式保存认证记录的，应采用不可编辑的方式。

10.5 为了证实认证活动的实施，除了认证机构要保持上述认证记录外，获证组织应留存认证证书有效期内相应的认证记录，至少包括:

（1）认证合同;

（2）审核计划;

（3）首、末次会议签到表;

（4）不符合报告及原因分析和纠正措施;

（5）审核报告;

（6）暂停、撤销通知（适用时）。

【要点与释义】

1.认证机构应制定文件化的认证记录、认证资料归档留存制度或程序文件，对认证全流程（包括认证申请、申请评审、方案策划、现场审核、认证复核与决定、认证证书签批及监督审核、再认证等环节）形成的记录、报告等资料进行归档，确保认证全过程可追溯。

2.认证证书有效期正常届满的，认证记录、认证资料归档留存时间为有效期届满之日起2年以上；认证证书在其有效期内被注销或撤销的，认证记录归档留存时间为认证证书被注销或撤销之日起2年以上。归档留存期间需采取有效的防损毁、防篡改等措施，以满足监督检查、法律纠纷举证及认证有效性追溯等需求。

3.认证记录的真实性要求认证记录内容必须与认证活动实际开展情况一致，杜绝虚假或误导性信息；准确性要求数据、时间、人员、结论等关键信息精准无错误；完整性要求认证记录覆盖认证全流程，所记录的信息完整无遗漏。认证记录包括但不限于本规则第10.2条款列明的11项内容。

4.根据《认证机构管理办法》，在认证证书有效期内，认证活动参与各方盖章或者签字的认证记录、认证资料等，应当保存具有法律效力的原件。本规则 10.3 条明确了签字、盖章的记录至少包括所列明的 6 项内容。

5.认证机构采用电子化认证记录的，建议根据《电子签名法》等法律法规的规定，委托电子认证服务提供者为其电子签名、数据电文（如电子化认证记录、认证资料）的真实性、可靠性进行验证，并提供电子认证证明。经电子认证的电子签名、数据电文，视为具有法律效力的原件。

6.认证记录应使用中文，使用其他语言的认证记录应附中文译文，认证机构对译文的准确性负责。

7.以电子文档形式保存认证记录的，应采用不可编辑的方式，确保记录一旦生成即无法被修改；能被修改的电子文档形式不能视为不可编辑的方式。

8.认证机构应要求获证组织留存认证证书有效期内相应的认证记录，包括本规则第 10.5 条款列明的 6 项内容，可以纸质文件或电子文档形式保存，以电子文档形式保存的，应采用不可编辑的方式。

【规则条款】

11　其他

11.1 认证标准换版

认证机构应按照国家认监委发布的管理体系认证标准换版

工作要求，落实标准的换版工作，确保认证委托人能够及时获得新版标准认证。

11.2 内部审核

认证机构应建立并实施文件化的内部审核程序，确保至少每年对 ISMS 认证开展情况实施内部审核。内部审核应包括对本规则执行情况的自查，并保持相应记录和报告。

11.3 同行评议

认证机构应积极配合国家认监委组织安排的对本机构实施的同行评议活动，并在要求的时间内对同行评议中发现的 ISMS 认证活动存在的问题采取有效的纠正措施，以持续符合本规则的要求。

11.4 ISMS技术服务

11.4.1 认证机构可为组织提供 GB/T 22080/ISO/IEC 27001 贯标服务，但不得代替组织编制 ISMS 文件、开展内部审核和管理评审，严禁协助组织编造虚假管理体系文件、体系运行记录等。

11.4.2 为确保没有利益冲突，参与对某组织 ISMS 技术服务的人员，2 年内不应被认证机构安排针对该组织的审核或其他认证活动。

11.5 认证数据安全

认证机构应严格落实《中华人民共和国数据安全法》和《中华人民共和国网络安全法》等法律法规要求，在中华人民共和国境内开展 ISMS 认证活动中收集和产生的重要信息和数据应当在

境内存储，确保信息和数据处于有效保护和合法利用的状态。

【要点与释义】

1.信息安全管理体系认证标准换版，认证机构应按照国家认监委后续发布的认证标准换版工作要求执行。

2.认证机构应建立文件化的内部审核程序，确保每年至少开展一次针对 ISMS 认证活动的内部审核。内部审核应覆盖 ISMS 认证活动的所有环节，包括本规则的执行情况，完整保留内部审核记录并形成报告。

3.认证机构应配合国家认监委组织开展的同行评议工作。认证机构在接受同行评议时，需保持开放协作态度，确保评议流程顺利推进；针对评议过程中发现的不合规认证活动，须在规定时限内制定整改方案并落实纠正措施，通过持续改进机制维持认证活动的规范性和有效性。

4.认证机构可为组织提供《网络安全技术 信息安全管理体系要求》等标准的宣贯、实施指导等技术服务，但须严格遵循“指导而非替代”原则，禁止直接参与组织内部管理体系文件编制、内审、管理评审等核心管理环节，尤其严禁通过编造虚假记录等帮助组织通过认证。

5.参与某组织 ISMS 技术服务的人员（如咨询顾问、培训讲师等），在服务结束后 2 年内不得参与对该组织的 ISMS 认证审核或其他认证活动。

6.在中华人民共和国境内开展 ISMS 认证活动的认证机构，须严格履行数据安全与网络安全法律责任，依据《数据安全法》和《网络安全法》等法律法规的规定，对认证活动中收集、生成的信息和数据在境内实施本地化存储管理。

12 附则

12.1 术语及释义

12.1.1 认证人员：指从事认证活动的人员，及认证机构的业务管理人员。

12.1.2 认证委托人：申请认证并接受认证审核的组织。

12.1.3 ISMS 认证业务范围：以与 ISMS 预期结果有关的过程的共性为特征的领域。

注：认证业务范围类别与信息安全管理体系范围内的产品、过程和服务有关，认证业务范围也被称作“技术领域”“行业”等。

12.1.4 认证转换：一个已获认可的认证机构为了颁发自己的认证证书，而承认另一个已获认可的认证机构颁发的现行有效的管理体系认证证书。

12.1.5 审核时间：策划并完成一次完整有效的管理体系审核所需要的时间。

12.1.6 现场审核时间：审核时间的一部分，包括从首次会议到末次会议之间实施审核活动的所有时间。

12.1.7 严重不符合：影响管理体系实现预期结果的能力的不

符合。

注：严重不符合可能是下列情况：

—对过程控制是否有效存在严重的怀疑。

—多项轻微不符合都与同一要求或问题有关，可能表明存在系统性失效，从而构成一项严重不符合。

12.1.8 轻微不符合：不影响管理体系实现预期结果的能力的不符合。

12.2 认证行政监管部门可以依照本规则的规定对管理体系认证活动实施监督管理，发现违法违规行为，应依法依规处理。

12.3 本规则由国家认监委负责解释。

附录 A

信息安全管理体系
认证业务范围分类与风险级别

ISMS 认证业务范围共划分为 30 个中类，详见表 A。

表 A　ISMS 认证业务范围分类与风险级别

大类	中类	风险级别	中类名称	分类内容
01	政务			
	01.01	高	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	高	税务机关	
	01.03	高	海关	
	01.04	中	其他	如政党，政协，社会团体等
02	公共			
	02.01	高	通信、广播电视	
	02.02	高	新闻出版	包括互联网内容的提供
	02.03	中	科研	涉及特别重大项目的应提升为高
	02.04	中	社会保障	如社会保险基金管理、慈善团体等。包括医疗保险
	02.05	高	医疗服务	
	02.06	低	教育	
	02.07	中	其他	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)

大类	中类	风险级别	中类名称	分类内容
03	商务			
	03.01	高	金融	如银行、证券、期货、保险、资产管理等
	03.02	高	电子商务	以在线交易为主要特点，含网络游戏
	03.03	高	物流	包括邮政
	03.04	低	咨询中介	如法律、会计、审计、公证等
	03.05	中	旅游、宾馆、饭店	
	03.06	低	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	高	电力	包括发电和输、变、配电等
	04.02	高	铁路	
	04.03	高	民航	
	04.04	高	化工	
	04.05	高	航空航天	
	04.06	高	水利	
	04.07	中	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	中	信息与通信技术	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	中	冶金	
	04.10	中	采矿	含石油、天然气开采
	04.11	中	食品、药品、烟草	
	04.12	低	农、林、牧、副、渔业	

大类	中类	风险级别	中类名称	分类内容
	04.13	低	其他	

注:

1.认证机构应基于表 A 开展 ISMS 认证活动，可在表 A 基础上对认证业务范围进一步细分。

2.高风险、中风险、低风险也可表述为一级、二级、三级。

【要点与释义】

1.本规则将 ISMS 认证业务范围划分 30 个中类，认证机构应基于表 A 开展 ISMS 认证活动，适用时认证机构可在表 A 的基础上，对认证业务范围进行特征分析与风险级别划分，确定细分的认证业务范围类别及其风险。无论何种理由，均不能将表 A 中的高风险认证业务范围调整为低风险。

2.认证机构应建立认证业务范围及风险划分的文件化的管理制度或程序，并留存认证业务范围类别及风险划分的记录及结果。

附录 B

信息安全管理体系认证审核时间要求

有效人数	审核时间 第 1 阶段 + 第 2 阶段 （人日）	有效人数	审核时间 第 1 阶段 + 第 2 阶段 （人日）
≤15	6	876 - 1175	18.5
16 - 25	7	1176 - 1550	19.5
26 - 45	8.5	1551 - 2025	21
46 - 65	10	2026 - 2675	22
66 - 85	11	2676 - 3450	23
86 - 125	12	3451 - 4350	24
126 - 175	13	4351 - 5450	25
176 - 275	14	5451 - 6800	26
276 - 425	15	6801 - 8500	27
426 - 625	16.5	8501 - 10700	28
626 - 875	17.5	> 10700	遵循上述递进规律

注：

1.有效人数包括认证范围内涉及的所有人员（含每个班次的人员）。认证范围内覆盖的非固定人员（包括季节性人员、临时人员和分包商人员）和兼职人员也应包括在有效人数内。

2.对非固定人员（包括季节性人员、临时人员和分包商人员）和兼职人员的有效人数确定，可根据其实际工作小时数予以适当减少或换算成等效的全职人员数。

3.认证委托人正常工作期间（包括轮班）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路途时间不计入有效的管理体系认证审核时间。

4.审核时间的计算：低风险认证业务范围可在按照附录 B 计算所得审

核时间的基础上，最多减少 10%；中风险认证业务范围应按照附录 B 计算审核时间；高风险认证业务范围应在按照附录 B 计算所得审核时间的基础上，至少增加 10%。

【要点与释义】

1.对于中风险认证业务范围，附录 B 明确了认证审核活动的审核时间；对于低风险认证业务范围，审核时间可在此基础上适当减少，但减少量不能多于附录 B 所列审核时间的 10%，认证范围如有其他减少审核时间的理由，可以适当减少审核时间，但总的减少审核时间不得超过附录 B 所规定审核时间的 30%；对于高风险认证业务范围，审核时间需要在此基础上增加，增加量不能少于附录 B 所列审核时间的 10%。

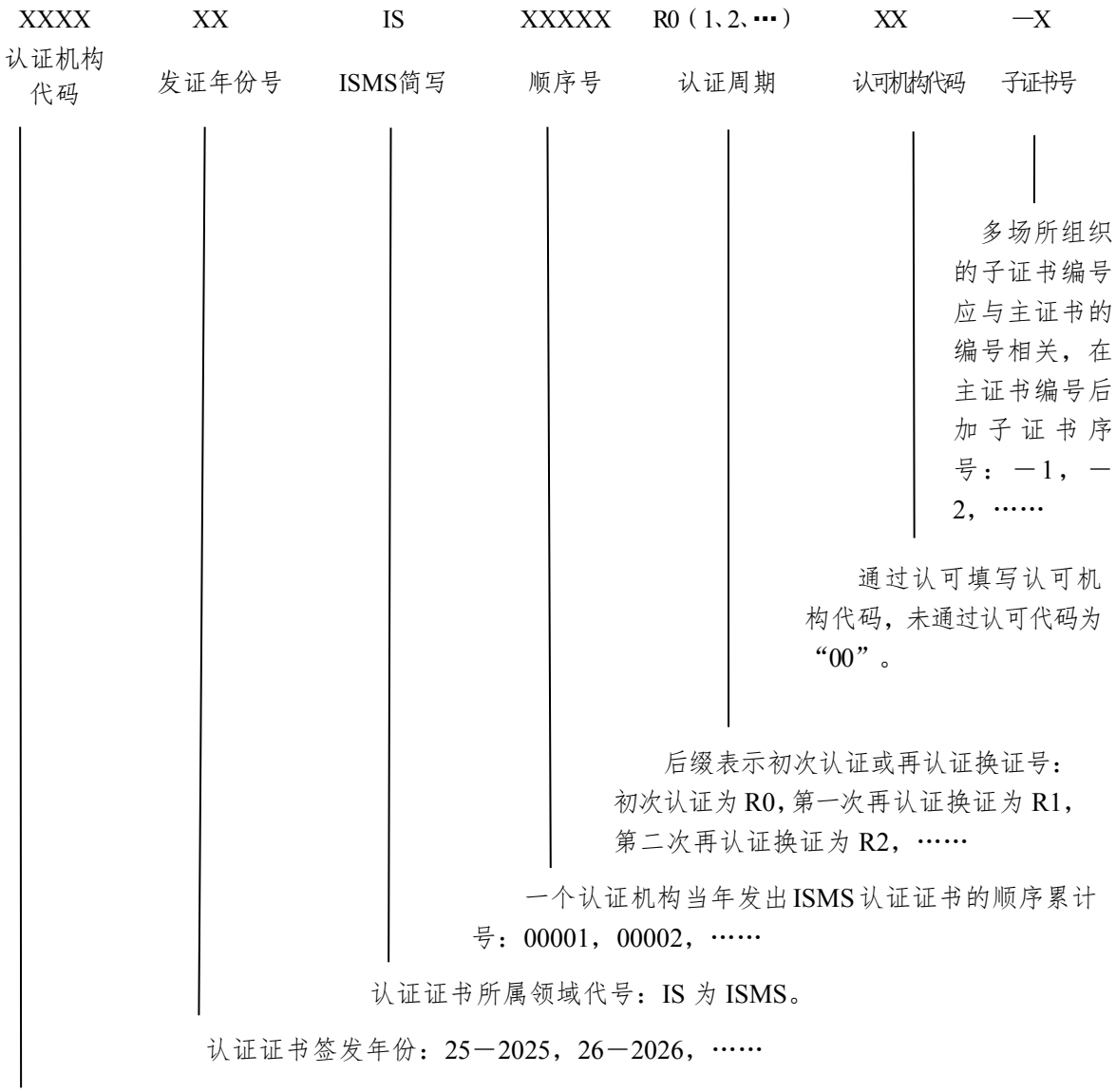
2.有效人数可以不同于社保缴纳的人数，计算认证审核时间时，认证机构应先确定认证委托人的有效人数。

3.认证机构应建立文件化的有效人数确定方法。确定有效人数时，应考虑认证委托人 ISMS 认证范围内涉及的所有人员，相似或重复过程以及雇佣大量非熟练人员的情况，减少人数应符合 ISO/IEC 27006-1 的相关规定。认证委托人 ISMS 认证范围内涉及的所有人员，包括兼职人员和部分处于认证范围内的雇员，以及倒班工作、行政工作和全部类别的办公室职员。如果是季节性运营的情况（如收获活动、度假村或度假旅馆等），计算有效人数应以高峰期的人员为计算基础。认证机构应留存确定有效人数的记录。

附录 C

ISMS认证证书编号规则

C.1 ISMS 认证证书编号由认证机构代码、发证年份号、ISMS 简写、顺序号、认证周期、认可机构代码和子证书号构成，格式如下:



注：认证机构批准号的编号格式为“CNCA—R/RF—年份—流水号”，

其中R表示内资认证机构，RF表示外资认证机构，年份为4位阿拉伯数字，流水号是内资、外资认证机构分别流水编号。内资认证机构代码为：该认证机构批准号的3位或4位阿拉伯数字批准流水号；外资认证机构代码为：F+认证机构批准号的后3位阿拉伯数字批准流水号，不足3位的，首位以0补位。

C.2 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，子证书编号为在主认证证书编号后加上“—”和序号，如—1（—2，—3，…）。

C.3 有效期内换发认证证书，认证证书编号中的认证机构批准号、年份号、顺序号和认证证书的有效期保持不变，应注明换证日期。

C.4 再认证完成后换发认证证书，按C.1规定重新赋予认证证书编号，初次认证为“R0”，第一次再认证为“R1”，第二次再认证为“R2”，依此类推。

C.5 撤销认证证书后，原认证证书编号废止，不再使用。

【要点与释义】

1.认证证书标号需要满足本规则附录C编号要求。认证机构确需保留其原认证证书编号的，可在认证证书上同时体现原认证证书编号。

2.认证机构批准号流水号为1000以下的内资认证机构，编号规则中的认证机构代码为认证机构批准号后三位数字批准流水号；认证机构批准号流水号为1000（含）以上的内资认证机构，编号规则中的认证机构代码为认证机构批准号后四位数字批准流水号。

3.按照5.2.3的要求实施认证转换的，新认证证书的编号可延续原认证证书的认证周期。