编号：WJBZ-JS-019

信息安全管理体系认证规则

(修订状态：A/3)

2022-11-15 发布 **2025-08-12 修订**

万佳标准认证（湖北）有限公司发布

目　录

信息安全管理体系认证规则

1. 适用范围

1.1 为规范信息安全管理体系（以下简称ISMS）认证工作，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。

2. 认证依据

《Information security, cybersecurityand privacy protection—Informationsecurity management systems—Requirements》（ISO/IEC 27001）

3. 对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 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CNAS-CC170-2024《信息安全管理体系认证机构要求》，以确保机构持续满足开展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。认证机构应能证明已对其开展的ISMS认证活动可能引发的风险进行了评估，对可能引发的责任做出了充分安排，建立风险储备金制度，按照有效证书数量的20倍数作为风险储备金。比如有效证书是5000张，风险储备金为5000*20=10万元人民币。

3.5 建立认证人员管理制度，包括认证人员的能力要求准则，选择、评价和聘用程序，以及能力提升机制。确保从事ISMS认证的人员持续具备相应素质和能力。

3.6 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（以下简称“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。

3.7 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，确保在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（监管有要求的除外）。

3.8 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。

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承担相应责任。

4.2 认证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 不得发生影响认证公正性的行为，应主动告知认证机构他们所了解的任何可能使其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性认证结果的，认证人员应当负有连带责任（如承担因此造成的经济损失）。

4.4 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。

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）可开展认证业务的范围，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或其他规范性要求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）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；

（9）其他需要公开的信息。

5.1.2 提出认证申请时，认证委托人应具备以下条件：

（1）取得法人资格（或其组成部分）；

（2）取得相关法规规定的行政许可（适用时）；

（3）已按认证标准建立 ISMS 体系，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、撤销认证证书已满一年（适用时）；

（5）原 ISMS 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）未被行政监管部门责令停业整顿；

（7）未被列入国家企业信用信息公示系统和“信用中国”发布的严重违法失信名单；

（8）一年内未发生行政监管部门责令停产整顿的重大质量事故；

（9）一年内未发生产品质量国家监督抽查（以下简称“国抽”）

不合格，或发生国抽不合格但已按相关规定整改合格；

（10）其他应具备的条件。

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、认证标准、申请的认证范围、认证范围内组织人员数量及影响体系有效性的外包过程；

（2）法律地位的证明性文件，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性文件；

（3）申请认证范围所涉及的质量法律法规要求的行政许可文件、资质证书、强制性产品认证证书等；

（4）组织机构及职责；

（5）工艺流程/服务流程及生产和（或）服务的班次及轮班情况；

（6）ISMS体系运行满足三个月的证据；

（7）三年内所发生的质量事故、与质量相关的行政处罚、国抽不合格，一年内所发生的其他质量抽查不合格的情况以及整改情况；

（8）其他需要提供的文件。

5.2 申请评审

5.2.1 认证机构应建立相应程序，对认证委托人提交的申请文件和资料实施申请评审，以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，认证机构应按照初次认证开展认证活动，无论其是否持有其他认证机构颁发的ISMS有效证书。

5.2.4 认证机构应将申请评审的结果告知认证委托人。

5.3 认证合同

5.3.1 通过申请评审的，认证机构应与认证委托人签订具有法律效力的认证合同，以明确认证委托人和认证机构的责任。

5.3.2 认证机构的责任至少包括：

（1）及时向符合认证要求并已缴纳认证费用的组织颁发认证证书，通过其网站或者其他形式向社会公布获证信息；

（2）对获证组织ISMS体系运行情况进行有效监督，发现获证组织的ISMS不能持续符合认证要求的，应及时暂停或者撤销其认证证书；

（3）因认证机构原因（如机构或其ISMS认证资质被注销或撤销）导致获证组织ISMS证书无法有效保持的，需及时告知获证组织并做出妥善处理，并承担由此导致的获证组织的经济损失。

5.3.3 获证组织的责任至少包括：

（1）遵守认证程序要求，认证过程如实提供相关材料和信

息，通过ISMS认证后持续有效运行ISMS；

（2）配合认证监管部门的监督检查，配合认证机构对投诉的调查；

（3）应当在广告、宣传等活动中正确使用认证证书、认证标志和有关信息，认证证书注销或被暂停、撤销的，不得继续使用该证书和相关认证标志、信息；

（4）发生如下情况，应及时向认证机构通报：发生重大质量事故、受到市场监管部门行政处罚、被市场监管部门公布存在质量不符合、被媒体曝光存在质量问题、ISMS不能正常运行或发生重大变更，以及其他应通报的情况等；

（5）承担选择认证机构的风险，如：因认证机构资质被撤销而带来的认证证书无法使用的风险。

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审核、获证后的监督审核和认证到期前进行的再认证审核。

注：一个认证周期通常为3年，从初次认证（或再认证）决定算起，至认证的有效期截止。

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ISO/IEC27001所有要求，以及认证范围内的典

型产品和服务。认证证书有效期内的监督审核应覆盖ISO/IEC27001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证书签发起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15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的一个班次的生产或服务的活动现场进行审核；

（2）对于未审核的班次，应记录不对其审核的理由。

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的实施策划、文件审核和编写审核报告等活动的时间。审核时间以人天计，1 人天为 8 小时。如果每天的实际工作时间不足 8 小时，则应延长审核天数以满足人天要求。

5.4.2.2 认证机构应以CNAS-CC170《信息安全管理体系认证机构要求》所规定的审核时间为基础，考虑认证委托人有效人数、ISMS风险类型等因素，建立文件化的不同类型审核的审核时间（包括现场审核时间）的确定方法。不同行业ISMS风险类型示例见CNAS-SC170《信息安全管理体系认证机构认可方案》。

5.4.2.3 每次审核的审核时间的确定过程应形成记录，尤其是减少审核时间的理由，减少的时间不得超过CNAS-CC170《信息安全管理体系认证机构要求》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80%。

5.4.2.4 认证机构应建立结合审核时间的确定方法，ISMS和其他管理体系实施结合审核时，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%。

5.4.3 多场所抽样方案

5.4.3.1 认证机构应建立并实施多场所组织认证抽样的规则并遵照执行，策划并保留多场所组织的抽样及确定审核时间的记录。

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，如果多个场所未涵盖相同的活动、过程及ISMS风险类型，则不应抽样，应当逐一到各场所进行审核。对多个相似场所可进行抽样审核，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。

5.4.4 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，每个审核组应包括：

（1）审核组长，认证机构应建立审核组长的选择、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》标准中对审核组长的通用要求；

（2）至少一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；

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。

5.4.5 远程审核方法

5.4.5.1 ISMS认证审核应在认证委托人的现场实施，初次认证以及认证周期内的每年度的监督审核和再认证审核活动，应包括访问认证委托人现场的现场审核。

5.4.5.2 因安全因素的考虑，审核组可在认证委托人的现场采用远程审核方法对认证委托人的某个过程的运作情况实施审核。

5.4.5.3 审核中采用远程审核方法的，远程审核时间不得超过现场审核时间的30%，并应在审核计划、审核记录及审核报告中予以注明。

5.4.6 审核计划

5.4.6.1 认证机构应依据审核方案为每次现场审核制定审核计划。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，专业审核员和技术专家应标明专业代码，在职技术专家应注明工作单位。

5.4.6.2 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。

5.4.6.3 现场审核开始之前，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。

5.5 实施审核

5.5.1 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，可使用图片、音像等作为补充材料。

5.5.2 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（因特殊原因不能参加的，应授权高级管理层其他成员）、ISMS相关职能部门负责人应参加会议，缺席应记录理由。审核组应保留首、末次会议签到记录。审核组应按国家认监委的要求完成首、末次会议现场审核的网络签到。

5.5.3 发生下列情况时，审核组应向认证机构报告，经同意后终止审核：

（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 初次认证

5.6.1 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个工作日，最长不应超过6个月。如果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，包括其活动、产品和服务、设施设备、工艺流程、现场运作以及适用的质量标准；

（2）评审认证委托人ISMS体系文件，确认其与组织业务活动及产品和服务相吻合；

（3）审核认证委托人理解和实施ISO/IEC27001标准的情况，特别是对ISMS关键绩效、过程和运行及质量目标识别情况；

（4）认证委托人是否为第二阶段审核做好准备，已实施了

内审和管理评审；

（5）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；

（6）认证委托人的产品和服务符合质量相关法律法规及强制性标准的情况。

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，第一阶段审核活动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）认证机构有充足的理由证明认证委托人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核可以达到第一阶段审核的目的和要求；

（3）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、在二阶段可能被判定为不符合项的问题。

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 ISO/IEC27001 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ISO/IEC27001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）认证委托人过程的运作控制；

（5）认证委托人的内部审核和管理评审是否有效；

（6）针对认证委托人ISMS方针的管理职责。

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，包括依据审核方案对获证组织开展的监督审核，以确认获证组织ISMS与ISO/IEC27001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有代表性的生产/服务过程、行业类别的典型产品/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所有代表性的生产/服务过程、行业类别的典型产品/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是否规范和有效；

（2）对上次审核中确定的不符合项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。

5.7.4 监督审核的时间应根据获证组织当前情况（有效人数和ISMS风险类型）确定，不少于CNAS-CC170《信息安全管理体系认证机构要求》所规定的初次认证审核时间的1/3。

5.8 再认证

5.8.1 获证组织拟继续持有认证证书的，应至少在认证证书到期前3个月向认证机构提出再认证申请，逾期则按初次认证申请处理。

5.8.2 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ISO/IEC27001持续符合性和运行的有效性。

5.8.3 再认证审核应在获证组织现场进行，并至少应在认证证书到期前1个月完成。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。

5.8.4 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。

5.8.5 再认证审核的审核时间应按5.4.2的要求，根据获证组织当前情况（有效人数和ISMS风险类型）来确定，不少于CNAS-CC170《信息安全管理体系认证机构要求》所规定的审核时间所确定的初次认证审核时间的2/3。

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，以做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、质量事故、对变更做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：

（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；

（3）获证组织的产品在产品质量国家监督抽查中被查出不合格时，自市场监管部门发出通报起30日内，认证机构应对该组织实施监督审核。

5.10 不符合项及其验证

5.10.1 对审核中发现的不符合项，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项制定纠正措施计划，由认证机构在下次审核时验证。

5.10.3 严重不符合项的验证时限应满足以下要求：

（1）初次认证：在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：在审核结束之日起 1 个月内完成。

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项所采取措施的情况，认证机构不应做出授予认证、保持认证或更新认证的决定。

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ISO/IEC27001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（例如初次、监督、再认证或其他类型审核);

（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）应描述与审核类型的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产品和服务提供过程与控制情况、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质量目标之间存在的差距和改进机会;

（13）行政监管部门在质量方面抽查的不合格情况，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）认证委托人对认证证书和认证标志的使用进行着有效的控制（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证据。

5.11.5 认证机构应将审核报告提交认证委托人。

5.11.6 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。

5.12 认证决定

5.12.1 认证机构应在对审核报告、不符合项的纠正措施及验证情况和其他信息进行综合评价的基础上，做出认证决定。认证决定人员应为认证机构管理控制下的专职认证人员，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做出。

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

（1）5.1.2 中的认证条件；

（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 总体符合 ISO/IEC27001 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应在上一认证周期认证证书到期前完成，否则应在推荐认证注册前再实施一次第二阶段审核。

5.12.5 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并说明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项及其他可能导致认证资格暂停、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。

6. 认证证书和认证标志

6.1 总则

6.1.1 认证机构应制定相应管理制度，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》中相关规定。

6.1.2 获证组织可以在认证有效期内使用ISMS认证标志，并接受认证机构的监督管理。

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，不得在产品上标注 ISMS 认证标志，只有在注明获证组织通过 ISMS 认证的情况下方可在产品的包装上标注 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。

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，认证证书的签发日期不应早于做出认证决定日期。

6.2.2 ISMS认证证书的有效期最长为3年，初次认证证书有效期的起算日期为认证决定日期，再认证证书有效期的起算日期不

得晚于最近一次有效认证证书的截止日期。

6.2.3 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。

6.2.4 认证证书在中华人民共和国境内使用的，证书使用的语言至少应包括中文。

6.2.5 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，当在认证证书上展示临时场所时，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ISO/IEC27001所采用的当时有效版本的完整标准号；

（4）证书签发日期和有效截止日期，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。

（5）证书编号（或唯一的识别代码）；

（6）认证机构名称、地址；

（7）认证标志、相关的认可标识及认可注册号（适用时）；

（8）证书信息及证书状态的查询途径。

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，不得与国家推行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。

通过认证并取得认证证书的企业，可以在宣传等方面使用，具体要求《认证证书和认证标志管理办法》。

7. 认证资格的暂停、撤销和注销

7.1 总则

认证机构应制定认证资格暂停、撤销和注销的文件化的管理制度，并遵照执行，不得随意暂停、撤销和注销认证资格。

7.2 认证资格的暂停

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的5个工作日内暂停其认证资格，并保留相应证据：

（1）ISMS 持续或严重不满足认证要求的；

（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）受到与质量相关的行政处罚；

（4）发生较大或重大质量事故，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范围有关的行政许可文件、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审核的；

（8）未按相关规定正确引用和宣传获得的认证资格和有关信息，包括认证证书和认证标志的使用，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）被有关行政监管部门责令停业整顿的；

（11）发生与质量相关的重大舆情；

（12）主动请求暂停的；

（13）其他应暂停认证资格的。

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，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资格，并保留相应证据。

7.3 认证资格的撤销

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确认后5个工作日内撤销其认证资格，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）认证资格的暂停期限已满，但导致暂停的问题未得到解决或有效纠正的；

（4）因获证组织违规造成重大产品和服务等质量安全事故的；

（5）有其他严重违反 ISMS 相关法律法规行为，受到相关行政监管部门处罚的；

（6）ISMS 没有运行或者已不具备运行条件的；

（7）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 1 个月仍未纠正的；

（8）其他应撤销认证资格的。

7.4 认证资格的注销

获证组织主动申请不再保持认证资格时，认证机构应注销其认证资格，并保留相应证据。

8. 申诉（投诉）处理

8.1 认证机构应建立文件化的申诉（投诉）处理制度，并遵照执行。

认证委托人或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）事项无关的人员做出，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）。

8.4 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，可以直接向认证机构所在地市场监管部门或国家认监委投诉。

9. 信息公开与报告

9.1 认证机构应建立文件化的认证信息报告制度，并遵照执行。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 认证机构应至少在审核实施前3天，将审核计划上报国家认监委相关网站，并应在上报认证证书信息的同时，上报管理体系审核结果信息。

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。

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，按规定程序和要求报国家认监委。

9.5 获证组织发生重大质量事故的，认证机构应在事故发生之日起2个工作日内，将该组织的认证情况及最近一个认证周期的认证材料报送获证组织所在地市场监管部门。

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，归档留存时间为认证证书有效期届满或者被注销、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；

（5）审核计划；

（6）首、末次会议签到表；

（7）现场审核记录；

（8）不符合项报告及验证记录；

（9）审核报告；

（10）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纸质版原件。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）不符合项报告及验证记录。

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

11. 其他

11.1 认证标准换版

认证机构应按照国家市场监管部门统一制订发布的

ISO/IEC27001标准的换版工作要求，执行落实标准的换版工作，确保组织能够及时获得新版标准认证。

11.2 内部审核

认证机构应建立文件化的内部审核程序并遵照执行，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证监管部门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认证活动中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

认证机构可为组织提供ISMS技术服务。为确保没有利益冲突，参与了对某组织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。未经安全评估和网信等相关部门批准，认证机构不得向境外传输、提供、公开存储于中华人民共和国境内的数据。法律、行政法规

另有规定的，依照其规定。

12. **附则**

12.1 本规则包含的术语具有如下含义：

12.1.1 认证委托人：申请认证并接受认证审核的组织。

12.1.2 ISMS 认证业务范围：以 ISMS 相关过程及预期结果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。

12.1.3 专职认证人员：是指满足以下条件之一的认证人员：

（1）与认证机构建立劳动关系并签订劳动合同的工作人员；

（2）认证机构返聘的具有认证人员注册资格的退休人员和企事业单位内退人员；

（3）认证机构的出资方为事业单位时，由出资方任命在认证机构任职的事业编制人员。

12.1.4 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。

12.1.5 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。

12.1.6 远程审核方法：利用信息和通信技术（ICT）在认证委托人所在地以外的任何地方实施审核活动所采用的方法。

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或者产品或服务能否满足规定要求存在严重的怀疑。

—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 市场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 本规则由万佳标准认证（湖北）有限公司负责解释。