**中鸿认证（江苏）有限公司**

# 云服务信息安全管理体系认证实施规则

规则编号：ZHCC-R-06-A

文件版本：C/2

受控状态：受控文件

编写人员：技术部

审核人员：韩自鹤

批准人员：丁泽林

发布日期：2023年4月12日

修订日期：2026年4月20日

实施日期：2026年4月20日

# 目录

## 1.适用范围

1.1 本规则用于规范中鸿认证（江苏）有限公司（简称中鸿认证）开展云服务信息安全管理体系（CSISMS）认证活动。

1.2 本规则是依据认证认可相关法律法规及认可规范，对（CSISMS）认证实施过程作出具体规定，强化 ZHCC 对认证过程的管理和责任。

1.3 本规则是对 ZHCC 从事 CSISMS 认证活动的基本要求，ZHCC 从事该项认证活动应当遵守本规则。

1.4《国家认监委关于加强认证规则管理的公告》（2025 年第 9 号）

## 2.对认证机构的基本要求

2.1 ZHCC应获得国家认监委备案后方可开展云服务信息安全管理体系认证。

2.2 建立可满足 GB/T 27021《合格评定 管理体系审核认证机构的要求》的内部管理体系，以使从事的 CSISMS 认证活动符合法律法规及技术规范的规定。

2.3 建立内部制约、监督和责任机制，实现受理、培训（包括相关增值服务）、审核和作出认证决定等环节的相互分开。

2.4 鼓励 ZHCC 通过认可机构的认可，证明其从事的 CSISMS 认证能力符合要求。

## 3.认证人员的基本要求

3.1 审核人员应当具有 CCAA 注册的信息安全管理体系审核员注册资格。

3.2 云服务信息安全审核员专业评定要求如下：通过公司组织的云服务信息安全管理体系标准知识及相关内容的培训考试，可获得云服务信息安全管理体系相关技术领域专业。

3.3 云服务信息安全管理体系审核组长应具备审核组长资格。

3.4 认证规则、认证方案制定人员和合同评审人员、认证决定人员、人员能力评价人员、审核方案管理人员应经评价确认满足 ZHCC 人员能力的要求，应具备项目管理人员资格。

3.4.1 如认证规则、认证方案制定人员和认证决定人员、人员能力评价人员同时为审核员时，

对其审核员资格的评价可替代其认证管理人员的能力评价。

3.5 云服务信息安全管理体系技术专家应具备大专学历以上；3 年以上与云服务信息安全管理相关的全职工作经历；技术专家专业能力评定至各技术领域。

认证人员应当遵守与从业相关的法律法规，对认证活动及作出的认证审核报告和认证结论的真实性承担相应的法律责任。

## 4.认证依据

4.1 ISO/IEC 27017:2015 《信息技术-安全技术-基于ISO/IEC 27002 云服务的信息安全控制规范》

## 5.初次认证程序

### 5.1.初次认证

5.1.1. 受理认证申请

ZHCC 市场部应向申请认证的组织（以下简称申请组织）进行信息公开，信息公开可采用公司官网进行公开，也可以在客户进行合同洽谈的时机，通过钉钉、微信、邮箱等单一方式或者多种方式相结合，公开的信息至少包含以下信息：

（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）ZHCC 的授予、保持、扩大、更新、缩小、暂停或撤销认证及其证书等环节的制度规定。

（4）认证证书样式。

（5）对认证决定的申诉程序。

（6）认证流程及公开文件。

5.1.2 ZHCC 市场部应当要求申请组织提交以下资料：

（1）认证申请书，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。

（2）法律地位的证明文件（包括：企业营业执照、事业单位法人证书、社会团体登记证书、非企业法人登记证书、党政机关设立文件等）的复印件。CSISMS 覆盖多场所活动时，应提交每个场所的法律地位证明文件的复印件（适用时）。

（3）CSISMS 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）CSISMS 管理体系手册。

（5）必要的程序文件及证明公司符合本标准中各项要求适当的记录等。

（6）CSISMS 已有效运行 3 个月以上的证明材料。

（7）其他与认证审核有关的必要文件。

5.1.3 认证申请的审核确认

ZHCC 审核部申请评审人员应对申请组织提交的申请资料进行审核，并确认：

（1）申请资料齐全，认证委托人应取得合法主体资质，并处于有效期内。

（2）申请组织从事的活动符合相关法律法规的规定，取得相关法律法规规定的行政许可。

（3）申请的认证范围、申请组织的运作场所和任何其他影响认证活动的因素已经得到识别和确认。

5.1.4 根据申请组织申请的认证范围、生产经营场所、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国家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。

5.1.5 对符合5.1.3、5.1.4要求的，ZHCC可决定受理认证申请；对不符合上述要求的，ZHCC市场部应通知申请组织补充和完善，或者不受理认证申请。

5.1.6 ZHCC应完整保存认证申请的审核确认工作记录。

5.1.7 签订认证合同

在实施认证审核前，ZHCC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CSISMS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ZHCC通报：

① 相关方有重大CSISMS有关方面的投诉。

② CSISMS范围内业务活动或行为被执法监管部门认定不符合法定要求。

③ 有严重与CSISMS相关事故的信息；

④ 组织的体系文件和业务重大变化；

⑤ 出现影响CSISMS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；不擅自利用CSISMS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CSISMS覆盖的企业活动、产品和服务范围。

（6）在认证审核及认证证书有效期内各次监督审核中，ZHCC和申请组织各自应当承担的责任、权利和义务。

（7）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。

## 5.2 建立审核方案

5.2.1 审核时间

5.2.1.1 为确保认证审核的完整有效，ZHCC 市场部申请评审人员应以附录 A 所规定的审核时间为基础，根据申请组织 CSISMS 覆盖的活动范围、特性、技术复杂程度、认证要求和员工人数等情况，核算并拟定完成审核工作需要的时间。

5.2.1.2 整个审核时间中，现场审核时间不应少于 70％。

5.2.2 审核组

5.2.2.1 ZHCC 审核部审核计调人员应当根据 CSISMS 覆盖的活动的专业技术领域选择具备相关能力的审核员和技术专家组成审核组。审核组中的审核员应承担审核责任。

5.2.2.2 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。

5.2.2.3 审核组应至少有 1 名专职审核员全程参与审核过程。

5.2.2.4 实习审核员不能独立组成审核组，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。

5.2.3 审核计划

5.2.3.1 ZHCC 应制定书面的审核计划交审核组实施。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）。

5.2.3.2 如果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环境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。

对多个相似场所可进行抽样审核，抽样数量不少于按以下方法计算的结果：

①初审：一般样本量应当为场所数量的平方根（$Y=\sqrt{X}$）。

②监督审核：每年度的样本量为场所数量的平方根乘以系数 0.6($Y=0.6\sqrt{X}$）。

③再认证审核：样本数量应与初审相同，如证明管理体系在认证周期中有效，

则样本的数量可最低为 0.8（$Y=0.8\sqrt{X}$）。

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。

5.2.3.3 为使现场审核活动能够观察到企业活动、产品和服务情况对 CSISMS 的影响，现场审核应安排在认证范围覆盖的企业活动、产品和服务正常运行时进行。

5.2.3.4 在审核活动开始前，审核组应将书面审核计划交申请组织确认。遇特殊情况临时变更计划时，应及时将变更情况书面通知受审核的申请组织，并协商一致。

**5.3 实施审核**

5.3.1 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（技术专家和实习审核员除外）。

5.3.2 审核组应当会同申请组织按照程序顺序召开首、末次会议。审核组应当提供首、末次会议签到表，参会人员应签到。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。

5.3.3 审核时应采用文件调查和现场调查的方式，包括查阅文件和记录、询问工作人员、观察现场、访问顾客和利益相关方、诚信行为调查等。

5.3.4 审核过程及环节

5.3.4.1 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 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。

5.3.4.2 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，审核申请组织有关人员理解和实施标准要求的情况，评价管理体系运行过程中是否实施了内部审核与管理评审，确认管理体系是否已有效运行并且超过3个月；

（3）确认申请组织建立的管理体系覆盖的活动内容和范围、申请组织的员工人数、活动过程和场所，遵守相关法律法规及技术标准的情况；

（4）结合管理体系覆盖活动的特点识别对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。

在第一阶段审核中，如发现组织存在违反审核依据的情况， 审核组将以《一阶段问题点清

单》指出，不开具《不符合报告》。在《一阶段问题点清单》中问题没有得到有效处理前，不会进行第二阶段审核。现场审核结束前，审核组将与受审核方进行沟通，通报第一阶段审核结论，出具第一阶段《审核报告》。

5.3.4.3 在下列情况，第一阶段审核可以不在申请组织现场进行：

（1）申请组织已获本 ZHCC 颁发的其他管理体系认证证书，ZHCC 已对申请组织 CSISMS 有充分了解。

（2）ZHCC 有充足的理由证明申请组织的业务简单，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）申请组织获得过其他经认可或备案的认证机构颁发的有效的 CSISMS 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，第一阶段审核应在申请组织的生产经营或服务现场进行。

5.3.4.4 审核组应将第一阶段审核情况形成书面文件告知申请组织。对在第二阶段审核中可能被判定为不符合项的重要关键因素，要及时提醒申请组织特别关注。

5.3.4.5 第一阶段审核和第二阶段审核应安排适宜的间隔时间，使申请组织有充分的时间解决第一阶段中发现的问题。

5.3.4.6 第二阶段审核应当在申请组织现场进行，重点是审核 CSISMS 符合 ISO/IEC 27017:2015 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监视、测量、报告和评审记录的充分性和有效性。

（2）为实现总目标而建立的各层级目标是否具体、有针对性、可测量并且可实现。

（3）现场审核应对最高管理者发挥对管理体系领导作用的情况进行面对面审核。

（4）对管理体系覆盖的过程和活动的管理及控制情况。

（5）申请组织实际工作记录是否真实。

（6）申请组织的内部审核和管理评审是否有效。

5.3.5 发生一些问题时，审核组应终止审核，并向 ZHCC 审核部报告，等待审核部确认且向认监委办理了终止审核计划后，方可终止审核，离开现场，可终止审核计划的情况包含：

（1）申请组织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）申请组织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。

（4）申请组织的 CSISMS 有重大缺陷，不符合 ISO/IEC 27017:2015 标准的要求。

（5）发现申请组织已经或可能严重损害国家安全、社会秩序、公共利益或获证客户及其相关方的合法权益；

（6）其他导致审核程序无法完成的情况。

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申请组织。

**5.4 审核报告**

5.4.1 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）认证机构名称；

（2）申请组织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申请组织管理体系的重要变更（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。

5.4.2 审核报告应随附必要的用于证明相关事实的证据或记录，包括文字或照片摄像等音像资料。

5.4.3 ZHCC 应将审核报告提交申请组织，并保留签收或提交的证据。

5.4.4 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，ZHCC 应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。

**5.5 不符合项的纠正和纠正措施及其结果的验证**

5.5.1 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。

5.5.2 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。

5.5.3 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。

**5.6 认证决定**

5.6.1 ZHCC 技术部应该在对审核报告、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。

5.6.2 审核组成员不得参与对审核项目的认证决定。

5.6.3 认证机构应有充分的证据确认认证委托人满足下列条件的，做出授予、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）认证委托人建立的管理体系符合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。

5.6.4 ZHCC 技术部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 5.4 条要求，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，ZHCC 已评审、接受并验证了纠正和纠正措施及其结果的有效性。

① 未能满足 CSISMS 标准的要求。

② 制定的目标不可测量或测量方法不明确。

③ 对实现目标具有重要影响的要素的监视和测量未有效运行，或者对这些要素的报告或评审记录不完整或无效。

④ 其他严重不符合项。

（3）ZHCC 对其他不符合项已评审，并接受了申请组织计划采取的纠正和纠正措施。

5.6.5 在满足 5.6.3 条要求的基础上，ZHCC 有充分的客观证据证明申请组织满足下列要求的，评定该申请组织符合认证要求，向其颁发认证证书。

（1）申请组织的 CSISMS 符合标准要求且得到有效实施与保持。

（2）认证范围覆盖的企业活动、产品和服务符合相关法律法规要求。

（3）申请组织按照认证合同规定履行了相关义务。

5.6.6 申请组织不能满足上述要求的，评定该申请组织不符合认证要求，以书面形式告知申请组织并说明其未通过认证的原因。

5.6.7 ZHCC 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。国家认监委在其网站（www.cnca.gov.cn）开设专栏向社会公开各 ZHCC 上报的认证证书等信息。

5.6.8 ZHCC 不得将申请组织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。

**6.监督审核程序**

6.1 ZHCC 应对持有其颁发的 CSISMS 认证证书的组织（以下称获证组织）进行有效跟踪，监督获证组织通过认证的 CSISMS 持续符合要求。

6.2 为确保达到 5.1 条要求，ZHCC 应根据获证组织的产品或服务的风险程度或其他特性，确定对获证组织的监督审核的频次。

6.2.1 作为最低要求，在初次认证的第二阶段审核后至少 12 个月内应进行一次监督审核。每次监督审核间隔不应超过 12 个月且每个日历年至少有一次监督审核（再认证的年份除）。

6.2.2 在达到监督审核期限而有证据表明获证组织暂不具备实施监督审核的条件时，可以适当延长监督审核期限，但最长间隔不能超过 15 个月。

6.2.3 超过期限而未能实施监督审核的，应按 6.6 条款处理。

6.3 监督审核的时间，按照附录 A。

6.4 监督审核的审核组，应符合 5.2.2 条和 5.3.1 条的要求。

6.5 监督审核应在获证组织现场进行，且应满足第 5.2.3.3 条确定的条件。由于生产经营活动的季节性原因，在每次监督审核时难以覆盖所有生产经营活动的，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活动。

6.6 监督审核时至少应审核以下内容：

（1）上次审核以来 CSISMS 覆盖的活动及运行体系的资源是否有变更。

（2）已识别的重要关键因素是否按 CSISMS 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）CSISMS 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）方针、目标是否实现。目标没有实现的，获证组织在内部管理评审时是否及时调查并采取了改进措施。

（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相关的规定。

（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）针对内审发现的问题或投诉的问题，及时制定并实施了有效的持续改进。

6.7 监督审核的审核报告，应按 6.6 条列明的审核要求逐项描述审核证据、审核发现和审核结论。审核组应提出是否继续保持认证证书的意见建议。

6.8 ZHCC 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。

**7.再认证程序**

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，确认获证组织管理体系有效性及认证范围的持续相关性和适宜性；

（2）管理绩效持续改进的证实；

（3）管理体系在实现获证组织目标和管理体系预期结果方面的有效性。

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

7.2 ZHCC 应按 5.2.2 条要求组成审核组。按照 5.2.3 条要求并结合历次监督审核情况，制定再认证计划并交审核组实施。审核组按照要求开展再认证审核。

在 CSISMS 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 5.2.1 条计算人日数的 2/3。

7.3 对再认证审核中发现的不符合项，应按 5.5 条要求实施纠正和纠正措施并进行验证，验证应在原证书有效期满前完成。

7.4 ZHCC 参照 5.6 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。

7.5 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认证证书，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。

**8.认证证书状态管理要求（暂停、撤销、注销、恢复、失效）**

8.1 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。执行本机构的《认证授予、拒绝、保持、变更、暂停、恢复、撤销程序》。

8.2 暂停证书

8.2.1 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）云服务信息安全管理体系持续或严重不满足认证要求，包括对云服务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）持有的与云服务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。

8.2.2 认证证书暂停期不得超过 6 个月。但属于 8.2.1 第（4）项情形的暂停期可至相关单位作出许可决定之日。

8.2.3 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。

8.3 撤销证书

8.3.1 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）被国家行政机关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）拒绝接受国家监督抽查的。

（5）出现重大的云服务信息安全管理事故，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（包括持有的云服务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）没有运行云服务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。

8.3.2 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。

8.4 认证机构暂停或撤销认证证书应当在其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。

8.5 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。

8.6 注销认证证书

获证组织主动申请不再保持认证资格时，本机构会注销其认证资格，并保留 相应证据。在机构与客户沟通确认后，向获证客户发送注销通知，要求停止认证 证书、认证标志使用和一切

宣传活动，并要求获证客户立即寄回认证证书。同时，注销信息上网公示。

8.7 认证证书的恢复

8.7.1 证书恢复的条件

获证客户对存在问题采取整改措施并在规定的时限内，解决了造成暂停的问题，认证资格的恢复符合相关的认证要求，同时在暂停期内没有使用、引用认证证书（如广告宣传）和使用认证标志。

8.7.2 证书恢复的程序

获证客户在规定时限内解决了造成暂停的问题后，向公司提出恢复使用认证证书申请并提供证明资料，可分两种情况：一种可立即办理恢复手续，经确认后办理恢复手续；另一种要经现场评审确认后办理恢复手续，根据暂停的原因，经评定后做出证书恢复／现场评审确认的评定意见确认后办理恢复手续。

8.7.3 在机构确认原因消除后，按流程进行恢复，机构将恢复信息上网公示，并向获证客户发送恢复通知，通知获证客户恢复认证证书和认证标志使用和宣传。

8.8 证书失效

8.8.1 认证证书有效期为三年，到期自动失效；

8.8.2 认证标准发生变更时，旧版使用期限到期，证书自动失效；

8.8.3 证书失效不需要向客户发送失效通知书。

**9.认证证书要求**

9.1 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。

9.2 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做出认证决定的日期。

9.3 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 CSISMS 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。

9.4 对每张 CSISMS 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。

9.5 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。

9.6 认证证书应至少包含以下信息：

（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

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 CSISMS 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/IEC 27017《信息技术-安全技术-基于 ISO/IEC 27002 云服务的信息安全控制规范》所采用的当时有效版本的完整标准号。

（4）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；

（5）认证证书编号（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）认证证书信息及认证证书状态的查询途径。ZHCC 除公布认证证书在 ZHCC 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（www.cnca.gov.cn）上查询”，以便于社会监督。

**10.与其他管理体系的结合审核**

10.1 当申请组织在运行云服务信息安全管理体系的同时还运行了其他管理体系，若其他管理体系在中鸿认证的认证业务范围内，中鸿认证可以根据申请组织的需求对管理体系进行单独的审核，或者对多个管理体系进行结合审核，但中鸿认证需确保在结合审核的情形下，对诸如审核范围的界定、审核时间的确定、审核方案的策划等进行有效地管理。

10.2 对于结合审核，必须以审核活动满足体系认证所有要求为前提，并且审核的质量不应由于结合审核而受到负面影响。在审核报告中，应清晰体现所有与管理体系有关的重要因素的描述并易于识别。

**11.受理转换认证证书**

11.1 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 27017:2015 标准、不能有效执行 CSISMS 的组织申请认证证书的转换。

11.2 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，必要时进行现场审核。

11.3 转换仅限于现行有效认证证书。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。

**12.证书的更换**

获证组织需更改获准认证/注册的企业云服务信息安全管理体系时，应及时将更改情况报本公司市场部。 在管理体系认证证书有效期内，当证书覆盖的范围、认证依据的标准、证书持有者、注册地址等发生变更时，应重新换证。

**13.受理组织的申诉**

13.1 申请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。

13.2 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。

**14.认证记录的管理**

14.1 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。

14.2 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，保存时间证书失效后至少再保存3年。

**15.其他**

15.1 本规则内容提及 ISO/IEC 27017:2015 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。

## 附录 A：云服务信息安全管理体系认证审核时间要求

下表为CSISMS初次认证的审核人日基数，具体审核时间需要考虑受审核方的规模、特性、业务复杂程度、CSISMS涵盖的范围、认证要求和其承担的风险等因素。根据受审核方的特点在项目方案制定过程中可以在人日基数上进行增减。

审核人日包括一阶段审核、现场审核、现场见证以及报告编写的时间。

当CSISMS与其他管理体系结合审核时，CSISMS的审核时间可根据结合审核的其他管理体系的特点进行减少。

监督审核的人日数为初次认证人日数的三分之一，再认证的人日数为初次认证人日数的三分之二，上述原则仅限于获证组织的认证范围和组织规模未发生变化的情况。

基本人日数计算表

| 有效人数 | 审核时间<br>第 1 阶段+第 2 阶段（天） | 有效人数 | 审核时间<br>第 1 阶段+第 2 阶段（天） |
|---|---|---|---|
| ≤15 | 2.5 | 876-1175 | 13 |
| 16-25 | 3 | 1176-1550 | 14 |
| 26-45 | 4 | 1551-2025 | 15 |
| 46-65 | 5 | 2026-2675 | 16 |
| 66-85 | 6 | 2676-3450 | 17 |
| 86-125 | 7 | 3451-4350 | 18 |
| 126-175 | 8 | 4351-5450 | 19 |
| 176-275 | 9 | 5451-6800 | 20 |
| 276-425 | 10 | 6801-8500 | 21 |
| 426-625 | 11 | 8501-10700 | 22 |
| 626-875 | 12 | >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全职人员，原则上以组织的社会保险登记证所附名册等信息为准。

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核定，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.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.云服务信息安全管理体系监督审核的人日数 为初次认证人日数的 1/3（不得少于1人日），再认证的人日数为初次认证审核人日数的 2/3。

# 附录 B：云服务信息安全管理体系认证业务范围分类

| 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，

# 修订记录

| 发布日期 | 实施日期 | 版本 | 修订内容概要 | 拟制 | 审核 | 批准 |
|---|---|---|---|---|---|---|
| 2023.04.12 | 2023.04.12 | A/0 | 新版发行 | 韩自鹤 | 张凯 | 张凯 |
| 2025.06.15 | 2025.06.15 | C/0 | 增加证书更换、认证资格变更内容 | 孙敬 | 韩自鹤 | 丁泽林 |
| 2025.8.25 | 2025.8.25 | C/1 | 依据《国家认监委关于加强认证规则管理的公告 2025 年第 9 号》进行修订 | 孙敬 | 韩自鹤 | 丁泽林 |
| 2026.04.20 | 2026.04.20 | C/2 | 根据认监委规则备案整改 | 孙敬 | 韩自鹤 | 丁泽林 |