

中部国际认证有限公司

云服务信息安全管理体系认证实施规则



文件编号： **CTS ZICC-GZ-YIS-53**

发布日期： **2025 年 07 月 04 日**

实施日期： **2025 年 07 月 04 日**

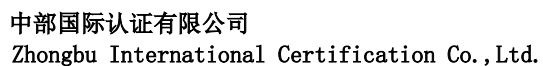
修订日期： **2025 年 08 月 19 日**

版 本： **B/0**

编 制： 技术部

审 核： 郭魁娜

批 准： 王 华



修改记录

CTS ZICC-GZ-YS-14-B/1





目录

1. 目的和适用范围	4
2. 认证依据	4
3. 对认证审核人员的基本要求	4
4. 认证程序	4
5. 初次认证程序	4
5.1. 认证申请与评审	4
5.2. 审核方案和审核策划	6
5.3. 实施审核	8
5.4. 审核报告	9
5.5. 不符合项的纠正和纠正措施及其结果的验证	10
5.6. 复核与认证决定	10
6. 监督审核	11
7. 特殊审核	12
8. 再认证审核	13
9. 认证资格的暂停、恢复、撤销	14
9.1. 认证资格的暂停	14
9.2. 认证资格的恢复	15
9.3. 认证资格的撤销	15
10. 认证证书及认证标志要求	16
11. 与其他管理体系的结合审核	18
12. 受理组织的申诉	18
13. 认证记录的管理	18
14. 其他	18
附录 A	19
附录 B	19



云服务信息安全管理体系统认证实施规则

1. 目的和适用范围

1.1. 本规则适用于规范依据ISO/IEC 27017:2015《信息技术- 安全技术-基于ISO/IEC 27002的云服务信息安全控制实践准则》标准在中国境内开展的云服务信息安全管理体系统认证活动。

1.2. 中部国际认证有限公司（简称：ZICC）依据认证认可相关法律法规，结合相关技术标准，对云服务信息安全管理体系统认证实施过程作出具体规定，明确ZICC对认证过程的管理责任，保证云服务信息安全管理体系统认证活动的规范有效。

2. 认证依据

云服务信息安全管理体系统认证依据ISO/IEC 27017:2015《信息技术- 安全技术-基于ISO/IEC 27002的云服务信息安全控制实践准则》标准。

3. 对认证审核人员的基本要求

3.1. 认证审核员应当取得中国认证认可协会颁发的信息安全或信息技术任一管理体系审核员注册资格，经过云服务信息安全管理体系统相关标准的培训，并考试合格。

3.2. 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。

4. 认证程序

- （1）认证申请与评审
- （2）签订认证合同
- （3）审核方案和审核策划
- （4）初次认证审核，（适用时）不符合纠正和纠正措施及其结果的验证
- （5）复核与认证决定
- （6）监督审核
- （7）变更审核、扩大认证范围、提前较短时间通知的审核等特殊审核
- （8）再认证审核
- （9）认证资格的暂停、恢复、撤销

5. 初次认证程序

5.1. 认证申请与评审

5.1.1. 认证申请



5.1.1.1. 申请认证的条件

- (1) 具有法律地位；
- (2) 从业条件中，有行政许可要求的，已取得行政许可并在有效期内；
- (3) 产品及过程符合国家相关法律法规和标准要求；
- (4) 已建立文件化的管理体系；
- (5) 本年度无重大质量事故，未因发生重大质量事故被行政主管部门责令停业整顿；
- (6) 未被“国家企业信用信息公示系统”（www.gsxt.gov.cn）列入“严重违法失信企业名单”；
- (7) “信用中国”（www.creditchina.gov.cn）中没有“严重失信”记录；

符合上述条件的组织可以随时提出认证申请。已获得其他认证机构颁发的认证证书愿意转换ZICC认证证书且符合中国认证认可协会（CCAA）《认证证书转换实施指南》要求的认证组织，可以随时提出认证申请。

5.1.1.2. 认证组织应向ZICC提交以下资料：

- (1) 认证申请书，包括申请认证的范围与申请组织的生产经营或服务活动等情况说明。
- (2) 法律地位的证明文件的复印件。若管理体系覆盖多场所活动，将附每个场所的法律地位证明文件的复印件(适用时)。
- (3) 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) 多场所活动、活动分包情况。
- (5) 对于不适用标准的某些条款的理由说明。
- (6) 相关管理体系文件化信息，如《云服务信息安全手册》、《程序文件》或《管理制度》。
- (7) 工艺流程/服务流程及生产和（或）服务的班次及轮班情况；。
- (8) 其他与认证审核有关的必要文件。

5.1.2. 认证申请评审

5.1.2.1. ZICC对申请组织提交的申请资料进行评审。

5.1.2.2. ZICC将根据申请组织提交的材料，根据申请认证的活动范围及场所、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；对符合要求的，ZICC可决定受理认证申请；对不符合要求的，ZICC将通知申请组织补充和完善，或者不受理认证申请。



5.1.2.3. 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，ZICC不应受理其认证申请。

5.1.3. 签订认证合同

5.1.3.1. 评审通过后，ZICC将与申请组织签订具有法律效力的书面认证合同，合同将至少包含以下内容：

（1）申请组织获得认证后持续有效运行云服务信息安全管理体的承诺。

（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，将及时向ZICC通报：

①客户及相关方有重大投诉；

②生产的产品和服务被执法监管部门认定不符合法定要求；

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：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、最高管理者变更；生产经营或服务的工作场所变更；云服务信息安全管理体覆盖的活动范围变更；云服务信息安全管理体和重要过程的重大变更等；

⑤出现影响云服务信息安全管理体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，不利用云服务信息安全管理体认证证书和相关文字、符号误导公众认为其产品和服务通过认证。

（5）在认证审核实施过程及认证证书有效期内，ZICC和申请组织各自应当承担的责任、权利和义务。

（6）认证服务的费用、付费方式及违约条款。

5.2. 审核方案和审核策划

5.2.1. 审核方案

审核方案包括整个认证周期的初次认证审核、认证决定后的第一年与第二年的监督审核、特殊审核方案（适用时）和第三年在认证到期前进行的再认证审核。特殊审核方案包括变更审核（如认证要求变更等）、扩大认证范围审核、提前较短时间通知的审核方案。初次认证后的第一次监督审核应在认证决定日期起12个月内进行，之后每次监督应在上一次监督审核末次会议（审核结束）日期后12个月内进行，两次监督审核的时间间隔不得超过15个月。



5.2.2. 审核时间

5.2.2.1. 为确保认证审核的完整有效, ZICC将以附录A所规定的审核时间为基础, 根据申请组织云服务信息安全管理体覆盖的活动范围、特性、技术复杂程度、风险程度、认证要求和体系覆盖范围内的有效人数等情况, 核算并拟定完成审核工作需要的时间。在特殊情况下, 可以减少审核时间, 但减少的时间不得超过附录A所规定的审核时间的 30%。

5.2.2.2. 整个审核时间中, 包括编写审核计划、审核报告、不符合项验证以及认证决定等时间, 管理体系认证审核时间, 不宜少于审核时间的 80%。

5.2.3. 审核组

5.2.3.1. ZICC将根据云服务信息安全管理体覆盖的活动的专业技术领域选择具备相关能力的审核员组成审核组, 必要时可以选择技术专家参加审核组。审核组中的审核员承担审核任务和责任。实施云服务信息安全管理体认证业务范围分类与分级按附录B执行。

5.2.3.2. 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。

5.2.3.3. 审核组可以有实习审核员, 其要在审核员的指导下参与审核, 不计入审核时间, 不单独出具记录等审核文件, 其在审核过程中的活动由审核组中的审核员承担责任。

5.2.4. 审核计划

5.2.4.1. ZICC将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, 审核组成员(其中: 审核员将标明认证人员注册号; 技术专家将标明专业代码、工作单位及专业技术职称)。

5.2.4.2. 如果云服务信息安全管理体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, ZICC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云服务信息安全管理体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云服务信息安全管理体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。但应确保所抽样的现场可以覆盖其申请的认证范围, 对已竣工的项目将按照一定的比例进行抽样确保审核证据的完整性和充分性。

5.2.4.3. 为使现场审核活动能够观察到产品生产或服务活动情况, 现场审核应安排在认证范围覆盖的产品生产或服务活动正常运行时进行。

5.2.4.4. 在审核活动开始前, 审核组应将审核计划交申请组织确认, 遇特殊情况临时变更计划时, 应及时将变更情况通知申请组织, 并协商一致。



5.3. 实施审核

5.3.1. 审核组应按照审核计划的安排完成审核工作。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。

5.3.2. 审核组应会同申请组织按照程序顺序召开首、末次会议，申请组织的最高管理者及与云服务信息安全管理体系相关的职能部门负责人员应该参加会议。参会人员应签到，审核组应当保留首、末次会议签到表。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. 审核过程及环节

5.3.3.1. 初次认证审核，分为第一、二阶段实施审核。

5.3.3.2. 第一阶段审核将至少覆盖以下内容：

(1) 结合现场情况，确认申请组织实际情况与云服务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 ISO/IEC 27017:2015标准要求的情况，确认云服务信息安全管理体系是否已运行并且超过6个月。

(3) 确认申请组织建立的云服务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) 结合云服务信息安全管理体系覆盖产品和服务的特点识别对云服务信息安全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。对云服务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6个月或者无法证明超过6个月的，以及其他不具备第二阶段审核条件的，不应实施第二阶段审核。

5.3.3.3. 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ZICC颁发的其他有效认证证书，ZICC已对申请组织云服务信息安全管理体系有充分了解。

(2) 认证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云服务信息安全管理体系认证证书，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，第一阶段审核将在受审核方的生产经营或服务现场进行。

5.3.3.4. 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点，要及时提醒申请组织特别关注。

5.3.3.5. 第二阶段审核应在申请组织现场进行。重点是审核云服务信息安全管理符合ISO/IEC 27017:2015标准要求和有效运行情况，将至少覆盖以下内容：

(1) 在第一阶段审核中识别的重要审核点的过程控制的有效性。

(2) 为实现云服务信息安全方针而在相关职能、层次和过程上建立云服务信息安全目标是否具体适用、可测量并得到沟通、监视。

(3) 对云服务信息安全管理覆盖的过程和活动的管理及控制情况。

(4) 申请组织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。

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

(1) 受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。

5.4. 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) 申请组织的名称和地址。

(2) 申请组织活动范围和场所。

(3) 审核的类型、准则和目的。

(4) 审核组组长、审核组成员及其个人注册信息。

(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) 叙述各项要求的审核工作情况，其中：对各项审核要求应逐项描述或引用审核证据、审核发现和审核结论；对云服务信息安全目标和过程及绩效实现情况进行评价。

(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。

5.4.2. ZICC将保留用于证实审核报告中相关信息的证据。

5.4.3. ZICC将在作出认证决定后30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。

5.4.4. 对终止审核的项目，审核组应提供终止审核的情况说明提交给申请组织，并保留证据。

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项，ZICC应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6个月期限内采取纠正和纠正措施。ZICC应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6个月内验证对严重不符合实施的纠正和纠正措施，则将按5.6.5条处理，或者重新实施第二阶段审核。

5.6. 复核与认证决定

5.6.1. ZICC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，作出认证决定和复核。

5.6.2. 认证决定人员应为ZICC管理控制下的人员，审核组成员不得参与对审核项目的认证决定和复核。

5.6.3. ZICC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，审核组提供的审核报告及其他信息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，ZICC已评审、接受并验证了纠正和纠正措施的有效性。

①在持续改进云服务信息安全管理体系的有效性方面存在缺陷，实现云服务信息安全目标有重大疑问。

②制定的云服务信息安全目标不可测量、或测量方法不明确。

③对实现云服务信息安全目标具有重要影响的关键点的监视和测量未有效运行，或者对这些关键点的报告或评审记录不完整或无效。

④其他严重不符合项。

(3) ZICC对其他一般不符合项已评审，并接受了申请组织计划采取的纠正和纠正措施。

5.6.4. 在满足5.6.3条要求的基础上，ZICC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) 申请组织的云服务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) 申请组织按照认证合同规定履行了相关义务。



5.6.5. 申请组织不能满足上述要求或者存在以下情况的，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。

(1) 受审核方的云服务信息安全管理体有重大缺陷，不符合ISO/IEC 27017:2015标准的要求。

(2) 发现受审核方存在重大质量、信息安全问题或有其他与产品和服务质量相关严重违法违规行为。

5.6.6. ZICC在颁发认证证书后，按照《认证机构管理体系认证、服务认证信息报告规范》规定的要求将认证结果相关信息报送国家认监委。

6. 监督审核

6.1. ZICC应对持有其颁发的云服务信息安全管理体认证证书的组织（以下称获证组织）进行有效跟踪，监督获证组织持续运行云服务信息安全管理体并符合认证要求。

6.2. 为确保达到6.1条要求，ZICC应根据获证组织的产品和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，初次认证后的第一次监督审核应在认证证书签发日起12个月内进行。此后，监督审核将至少每个日历年（将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。

6.2.2. 超过期限而未能实施监督审核的，将按9.1或9.3条处理。

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，自国家发出通报起30日内，ZICC应对该企业实施监督/特殊审核。

6.3. 监督审核的时间，将不少于初次审核时间人日数的1/3。

6.4. 监督审核的审核组，应和初次审核的审核组要求一致。

6.5. 监督审核应在获证组织现场进行，且应满足第5.2.4.3条确定的条件。由于市场、季节性等原因，在每次监督审核时难以覆盖所有产品和服务的，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和服务。

6.6. 监督审核时至少审核以下内容：

(1) 上次审核以来云服务信息安全管理体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) 已识别的重要关键点是否按云服务信息安全管理体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) 云服务信息安全管理体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) 云服务信息安全目标及绩效是否达到云服务信息安全管理体系确定值。

(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《认证认可条例》及其他相关规定。

(7) 是否及时接受和处理投诉。

(1) 针对体系运行中发现的问题或投诉，及时制定并实施了有效的改进措施。

6.7. 在监督审核中发现的不符合项，ZICC应要求获证组织分析原因，规定时限要求获证组织完成纠正和纠正措施并提供纠正和纠正措施有效性的证据。

6.8. ZICC应采用适宜的方式及时验证获证组织对不符合项进行处置的效果。

6.9. 监督审核的审核报告，应按审核要求逐项描述或引用审核证据、审核发现和审核结论。

6.10. ZICC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. 特殊审核

7.1. 特殊审核的目的是为确保获证客户的管理体系因非常规的事件而持续有效，在对变更（包括认证要求的变更）、扩大认证范围、提前较短时间通知等情况进行评估、验证，对变更、扩大认证范围等的管理体系持续运行进行评价，确认体系的持续符合性和有效性。

7.2. 获证组织在认证证书有效期内出现以下情况时，公司应进行特殊审核（包括提前较短时间通知的审核）：

(1) 获证客户发生重大变更，管理体系发生重大变化，可能影响组织的活动与运行（例如：组织的所有权、组织机构、人员或设备的改变、场所的变迁）及体系运行的有效性；

(2) 认证要求的更改，如认证标准变更，认证、认可标志变更；

(3) 认证范围扩大或缩小；

(4) 对暂停的客户进行追踪，包括对导致暂停认证资格的不符合纠正措施有效性的追踪；

(5) 相关方严重投诉或较多投诉，或其他来自相关的信息的分析，表明已获证的组织不再满足认证机构的要求，或反映其有隐瞒事实真相，需要进行调查核实；

(6) 国家和地方有关部门对产品质量的监督检查不合格，环保/职业健康安全主管部门执法检查不符合，市场监督管理部门监督检查产品和食品安全生产规范体系检查不符合；

(7) 发生信息安全、投诉等重大事故，或违规行为受到公开通报的；



(8) 获证组织对认证证书、标志有较严重的不正确宣传或误导的；

(9) 根据认证认可监管机构要求，安排的专项检查。

7.3. ZICC选择具备相关能力的审核员组成审核组，必要时可以选择技术专家参加审核组。审核组中的审核员承担审核任务和责任。审核组实施审核，形成审核报告，并提交ZICC审查。必要时，审核组长应对客户变更部分的文件进行审核，文件审核报告应提交ZICC。

7.4. ZICC为调查投诉、对变更做出回应或对被暂停的获证客户进行追踪，可能需要在提前较短时间通知获证获证客户后对其进行审核。ZICC审核方案策划/管理人员根据上一次审核的结果、认证客户的最新信息、对认证客户日常管理的情况，以及当前的的问题，确定此次审核目标、准则和范围，策划审核方案。当需要在提前较短时间内通知或不通知获证客户就对其进行审核时，指派审核组应在公正性上给予更多关注。审核组应保证公正性和保密性，不得向无关人员或受审核方提前泄露审核事项。

7.5. 扩大认证范围审核和变更审核通常需要文审。ZICC审核方案策划/管理人员根据上一次审核的结果、认证客户的最新信息、对认证客户日常管理的情况，以及评审结果，策划特殊审核方案。

7.6. 审核组应在受审核方现场完成以下方面：

(1) 向受审核方说明审核目的（不通知获证客户就对其进行审核时）；

(2) 按审核方案实施现场审核；

(3) 在审核过程中完成有关问题的调查、取证工作；

(4) 在现场审核记录表中如实记录现场审核发现的缺陷、问题及判定依据，并与受审核方确认；

(5) 做出审核结论，并将结论告之受审核方，完成审核报告。

7.7. ZICC对审核组提交的审核报告进行审议和复核，作出认证决定，包括采取相应的措施，以书面形式或适当的形式通知客户。

8. 再认证审核

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

8.2. ZICC应按要求组成审核组。并结合历次监督审核情况，制定再认证审核计划交审核组实施。

8.3. 在云服务信息安全管理体系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，但审核时间将不少于按初次审核人日数的2/3。



8.4. 对再认证审核中发现的严重不符合项，ZICC应规定时限要求获证组织实施纠正与纠正措施，并在原认证证书到期前完成对纠正与纠正措施的验证。

8.5. ZICC按照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。

8.6. 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，ZICC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，则不将予以再认证，也不将延长原认证证书的有效期。

在当前认证证书到期后，如果ZICC能够在6个月内完成未尽的再认证活动，则可以恢复认证，否则将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，终止日期将基于上一个认证周期。

9. 认证资格的暂停、恢复、撤销

ZICC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，规定和管理制度将满足本规则相关要求。ZICC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。

9.1. 认证资格的暂停

9.1.1. 发生以下情况（不仅限于此）时，ZICC应在确认情况后5日内，暂停获证客户的认证资格：

- (1) 客户的获证管理体系持续或严重不满足认证要求，包括对体系运行有效性要求；
- (2) 获证客户不承担、不履行认证合同约定的责任和义务，包括获证客户不允许按要求的频次实施监督或再认证审核、未按时缴纳认证费用；
- (3) 被有关执法监管部门责令停业整顿的，尚不需立即撤销认证证书的；
- (4) 被地方认证监管部门发现体系运行存在问题，需要暂停证书的；
- (5) 持有的行政许可证明、强制性资质证书、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；
- (6) 因第5)条该情况被暂停认证资格，暂停期6个月到期后获证客户仍未提供有效证据的，应根据实际情况评审是否可将暂停期延期至相关单位做出许可结论之日，经公司批准后暂停期限可延长至相关单位做出结论之日，保存审批记录，并根据证书信息上报要求将暂停信息进行上报更新；



(7) 获证客户发生质量相关的重大事故，获证客户质量监督或行业主管部门抽查不合格等情况，反映出组织的体系建立及运行存在重大缺陷的，尚不需立即撤销认证证书的；

(8) 获证组织未按ZICC规定使用认证证书、认证标志的；

(9) 获证组织未按要求对信息进行通报的；

(10) 获证客户主动请求暂停；

(11) 其他应当暂停认证证书的。

9.1.2. 多数情况下，暂停将不超过6个月。在暂停期间，客户的管理体系认证暂时无效。

9.1.3. ZICC在公司网站与认证认可监督管理委员会认证认可信息公共服务平台公开查询暂停认证证书的信息，并以书面形式或适当的形式通知客户暂停的起始日期和暂停期限，以及在暂停期间，客户应停止引用认证资格和使用认证证书、标志，不得以任何方式使用认证证书、认证标识或引用认证信息。

9.2. 认证资格的恢复

9.2.1. 如果客户造成暂停的问题已解决，根据暂停的原因，通过ZICC文件审核或现场审核的结果，重新满足规定的要求和条件，经过ZICC审批后，恢复被暂停的认证资格，规定如下：

9.2.1.1. 对于认证资格被暂停的获证组织，通过对获证组织提供的申请恢复认证资格的文件材料，经ZICC技术部文件审核，确认其在规定期限内已采取有效的纠正措施重新满足相关要求，作出恢复认证资格的决定，经ZICC审批通过后，恢复被暂停的认证资格，以书面形式或适当的形式通知客户。

9.2.1.2. 对于认证资格被暂停的获证组织，通过现场审核的方式，评价暂停原因是否有效消除，审核组确定是否推荐恢复认证资格，ZICC在对审核报告等进行综合评价和复核，做出认证决定，经审批后，作出恢复认证资格的决定，以书面形式或适当的形式通知客户。

9.2.2. 如果客户未能在ZICC规定的时限内解决造成暂停的问题，或未通过ZICC文件审核或现场审核，或ZICC经审议做出不予恢复认证的决定，ZICC应根据审核结果及相关情况，采取缩小认证范围或撤销认证的措施，并以书面形式或适当的形式通知客户。

9.3. 认证资格的撤销

9.3.1. 获证组织有以下情形之一的，ZICC应在获得相关信息并调查核实后5个工作日内，撤销获证客户的认证资格：

(1) 被注销或撤销法律地位证明文件的；

(2) 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；



- (3) 出现重大的产品或质量等严重事件，经执法监管部门确认是获证客户违规造成的；
- (4) 有其他严重违法法律法规行为的；
- (5) 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换证或延期未获批准）；
- (6) 没有运行管理体系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，不按相关规定正确使用认证证书和认证标志，造成严重影响或后果，或者ZICC已要求其纠正但超过ZICC要求期限仍未纠正的；
- (8) 获证客户提供虚假资料或信息，虚报、瞒报获证所需信息，需要撤销撤销认证证书的；
- (9) 获证客户发生相关方重大投诉，但未能采取有效处理措施的，需要撤销撤销认证证书的；
- (10) 其他应当撤销认证证书的情形。

9.3.2. 经审查确认获证客户发生应被撤销认证资格的情况后，经ZICC审批，做出撤销认证的决定，以书面形式或适当的形式通知客户，收回撤销的认证证书，并告知客户停止引用认证资格和使用认证证书、标志，不得以任何方式使用认证证书、认证标识或引用认证信息。

10. 认证证书及认证标志要求

10.1. 认证证书应至少包含以下信息：

- (1) 获证组织名称、地址和统一社会信用代码（或组织机构代码）。该信息将与其法律地位证明文件的信息一致。
- (2) 云服务信息安全管理体系覆盖的生产经营或服务的地址和业务范围。若认证的云服务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。
- (3) 云服务信息安全管理体系符合ISO/IEC 27017:2015标准的表述。
- (4) 证书编号。
- (5) ZICC名称。
- (6) 有效期的起止年月日。
- (7) 证书将注明：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。ZICC除公布认证证书在本机构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站（www.cnca.gov.cn）上查



询”，以便于社会监督。

10.2. 初次认证认证证书有效期最长为3年。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. 认证资格引用、认证证书和认证标志或徽标使用规定

10.3.1. ZICC拥有其徽标的所有权和使用权，不授予其他任何机构和个人使用。

10.3.2. 获证组织在引用认证资格和使用ZICC认证证书、认证标志时，应遵守以下：

（1）获证组织应在认证范围和认证有效期内持续保持认证资格有效状态下，在传播媒介（如：互联网、宣传册或广告）或其他文件中展示认证证书、认证标志或引用认证资格，但应保证其清晰可辨，不可篡改。

（2）认证证书有效期为三年，在有效期内，获证组织应按期接受监督审核，经ZICC监督审核被确认保持认证注册资格后，发放《监督审核结论通知书》，获证组织方可继续使用认证证书。认证证书应与《监督审核结论通知书》同时使用。

（3）获证组织在向ZICC通报备案后，方可使用ZICC认证标志。只能使用与ZICC所提供色调一致、排列方式一致的标志，使用时应在ZICC认证标志下方添加证书编号，必须保证整体使用，不允许分割认证标志仅使用其中的某一部分，可以按比例放大或缩小，但不得使其变形。

（4）获证组织只能使用与所持有的认证证书完全相同的认证标志，不得使用所持认证证书上没有的其他认证标志或标志。

（5）不得利用产品、服务认证证书、认证标志和相关文字、符号，误导公众认为其管理体系已通过认证。

（6）不得利用管理体系认证证书、认证标志和相关文字、符号，误导公众认为其产品、服务已通过认证，也不得有对其认证资格做出误导性说明。

（7）不得暗示认证适用于认证范围以外的活动或场所，仅就获得认证的范围方面（包括获得认证的场所）进行有关认证声明。

（8）不得将ZICC认证标志用于产品、产品包装上或附带信息中，也不允许用于实验室检测、校准或检验的报告或证书上。获证组织如要在产品外包装上使用认证标识时，应同时附有明确的声明：“如本组织通过云服务信息安全管理体认证”的情况下，方可将ZICC认证标志标注在运输产品的大包装上但应当保证此包装不会到达最终用户手中，不得以此来暗示产品、服务已被认证，或以任何方式作为产品合格的说明。

（9）在被暂停认证资格期间，获证组织应立即停止认证证书和认证标志的使用，以及认



证资格的宣传。

(10) 当认证资格被撤销或认证证书到期失效后，获证组织应立即停止使用认证证书和认证标志，立即停止引用认证资格的宣传，并应向ZICC寄回持有的认证证书。

(11) 认证范围被缩小后，获证组织应修改所有的广告材料。

(12) 不允许获证组织以任何形式转让、出售、借用或冒用ZICC认证证书、认证标志；

(13) 获证组织规定正确使用认证证书和认证标志，正确宣传认证结果，不得使认证机构和（或）认证制度声誉受损，失去公众信任。

11. 与其他管理体系的结合审核

11.1. 对云服务信息安全管理体系统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，并在审核报告中清晰地体现，且易于识别。

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. 受理组织的申诉

申请组织或获证组织对认证决定有异议时，ZICC应接受申诉并且及时进行处理，在60日内将处理结果形成书面通知送交申诉人。

书面通知应当告知申诉人，若认为ZICC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. 认证记录的管理

13.1. ZICC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。记录资料将当使用中文，保存时间至少将当与认证证书有效期一致。

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，保存时间至少将当与认证证书有效期一致。

14. 其他

14.1. 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。

14.2. 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，并经审核组长加盖组织公章确认与原件一致。

14.3. ZICC可开展云服务信息安全管理体系统及相关技术标准的宣贯培训，促使组织的全体员



工正确理解和执行云服务信息安全管理体系标准。

附录 A

认证审核时间要求

有效人数	初次审核审核时间（审核人日）	有效人数	初次审核审核时间（审核人日）
1~25	2.5	201 ~ 300	5.5
26 ~ 50	3	301 ~ 400	6
51 ~ 75	3.5	401 ~ 600	7
76 ~ 100	4	601 ~ 800	8
101 ~ 150	4.5	801 ~ 1000	9
151 ~ 200	5	> 1000	沿用 以上规律

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）。覆盖于认证范围内的非固定人员（如：承包商人员）和兼职人员也将包括在有效人数内。

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. 监督审核的人日数不少于初次认证人日数的三分之一，再认证的人日数不少于初次认证人日数的三分之二。

附录 B

云服务信息安全管理体系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
			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	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）
			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	03.03	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	
			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	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	