神州（天津）认证服务有限公司

云服务信息安全管理体系
认证实施规则

规则编号：SCS-CSISMS-2025　　编写人员：技质部

版 本 号：A版　　审核人员：周相荣

修 订 号：0.0　　批准人员：韩璐璐

2025-5-20 发布　　2025-5-20 实施

修改记录

无特殊说明时，一般修改均由修改日起开始实施。

修订号	修订日期	修改内容	修改人	审核人	批准人

目 录

云服务信息安全管理体系认证实施规则

1 适用范围

1.1 本规则适用于神州（天津）认证服务有限公司(以下简称：SCS)开展云服务信息安全管理体系（简称 CSISMS）认证活动。

1.2 本规则依据认证认可相关法律法规，结合相关技术标准，对规范云服务信息安全管理体系认证过程做出具体规定，明确云服务信息安全管理体系认证过程的相关责任，保证认证活动的规范有效。

2 基本要求

2.1 获得国家认监委批准或备案、取得从事云服务信息安全管理体系认证的资质或能力。

2.2 建立可满足 GB/T 27021.1《合格评定 管理体系审核认证机构要求》的内部管理体系，以使从事的云服务信息安全管理体系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。

3 认证依据

SCS 对申请 CSISMS 认证的组织按照标准 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施规程》开展认证活动。

4 对认证人员的要求

4.1 认证管理人员

4.1.1 包括机构主要业务主管负责人、认证规则和认证方案制定人员、认证申请评审人员、认证审核方案管理人员、认证决定或复核人员、认证人员能力的审核人员、计划调度人员、证书制作人员等；

4.1.2 认证人员应当符合《SCS-I-03M 认证管理人员、管理职能人员专业相关资格及能力评定工作细则》的要求。

4.1.3 认证人员需经过系统的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施规程》的学习和本机构本认证实施规则的培训和学习，通过考核，具备能力，从事相应的工作岗位。

4.2 认证审核人员

4.2.1 审核人员应具有 CCAA 注册（含实习）ISMS或ITSMS管理体系审核员资格，并具

备相应专业技术能力，以及熟悉云服务信息安全管理体系相关专业知识。

4.2.2 审核人员应当经过ISO / IEC 27017：2015 和本机构本认证实施规则的培训，综合评价考核，取得SCS任命的云服务信息安全管理体系认证审核员资格。

4.2.3 审核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。

4.3 认证决定或复核人员

具有与认证领域相关的专业知识；熟悉认证认可相关标准及认证审核原则、实践和技巧；了解认证机构认证管理过程要求。

5 认证程序和要求

认证的基本环节包括：

a) 认证申请和受理；

b) 第一阶段审核（含文件审核）；

c) 第二阶段审核；

d) 认证决定与批准；

e) 获证后的监督。

5.1 认证申请和受理

5.1.1 SCS 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，也可以在客户进行认证咨询、合同洽谈的时机，通过 QQ、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）SCS 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。

（3）认证证书样式。

（4）对认证决定的申诉程序。

5.1.2 申请组织应具备以下条件：

(1)应具有明确的法律地位；

(2)应取得相关法规规定的行政许可文件(适用时)；

(3)已经按照标准建立文件化的管理体系（包括质量手册、程序文件、内审资料、管理评审资料以及程序文件要求的其它相关表单）；

(4) 认证申请前，受审核方的管理体系原则上至少有效运行三个月并进行了一次完整的内部审核和管理评审。

(5) 认证申请前，已通过 ISO 27001 认证。

5.1.3 认证委托人申请认证时需向SCS 提交以下文件资料,并对其提供的文件真实性负责：

(1)组织简介(包括组织名称、注册地址、注册资金；经营场所名称、地址、从业人员、主要设施设备的配置、从事的业务等基本情况介绍)；

(2)组织机构图(可放入云服务信息安全管理体系文件中，如管理手册)；

(3)法律地位的证明文件(如企业营业执照、事业单位法人代码证书、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。若拟申请认证覆盖多场所活动，应提供每个场所的法律地位证明文件的复印件(适用时)；

(4)与拟申请认证范围有关法律法规要求的许可证明（适用时）；

(5)拟申请认证的范围和内容说明，包括主要的经营过程描述、涉及的国家或行业的相关标准、规范，以及为其提供支持的主要设施；

(6)ISMS 证书复印件；

(7)信息安全适用性声明（SOA）；

(8)保密协议、信息安全敏感区域的声明；

(9)影响主要经营过程绩效的任何外包过程的信息；

(10)云服务信息安全管理体系文件，如管理手册、程序文件；

(11)支持 CSISMS 的规程和控制措施、风险评估方法的描述、风险评估报告、风险处置计划、组织为确保其信息安全过程的有效规范/运行和控制以及描述如何测量控制措施的有效性的文件。

(12)与企业云服务信息安全管理体系认证有关的法律、法规清单及服务规范执行的标准清单(可现场提供)；

(13)云服务信息安全管理体系内部审核和管理评审记录；

(14)申请组织自我声明(承诺遵守相关法律法规、未被列入国家信用信息严重失信主体名录，以及拟申请认证前未发生质量、安全、环境及卫生等事故或顾客重大投诉等情况)；

(15) 登录全国企业信用信息公示系统（http://gsxt.gdgs.gov.cn/）查询“严重

违法企业名单”，提供查询截图；

(16)适用时，任何特殊要求(如特殊的语言、环境、安全、保密要求等)。

(17)申请受理提出的其他所需信息。

5.1.4 认证申请的审核确认

SCS 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，组织及其云服务信息安全管理体系的信息充分。

（2）申请组织从事的活动符合相关法律法规的规定。

（3）申请的认证范围、申请组织的运营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 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，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，SCS 可决定受理认证申请；对不符合上述要求的，SCS 应通知申请组织补充和完善，或者不受理认证申请。

5.1.6 SCS 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，SCS 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云服务信息安全管理体系的承诺。

（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 SCS 通报：

① 相关方有重大投诉。

② 有严重云服务信息安全事件。

③ 组织的体系文件和业务重大变化；

④ 出现影响云服务信息安全管理体系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；不擅自利用云服务信息安全管理体系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）拟认证的云服务信息安全管理体系覆盖的范围。

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

（7）认证服务的费用、付费方式及违约条款。

5.2 审核策划

5.2.1 审核方式及审核方案

（1）SCS 结合 SCS 相关文件要求，根据企业的规模、企业类型、信息安全适用性声明、信息安全策略集、信息安全风险准则、云服务信息安全管理体系及其他因素对认证全过程进行策划，制定审核方案(包括多场所的抽样计划)。并通过每次审核结束后的反馈信息和审核前再次获取的变化信息，对原有审核方案及时调整，以实现动态的管理。

（2）SCS 按照确定的认证标准或技术规范，对申请组织进行审核，云服务信息安全管理体系通常采用文件审核结合现场检查的方式，旨在证实其持续符合认证标准或认证技术规范要求的能力。

（3）为确保认证审核的完整有效，SCS 依据申请组织申请认证覆盖的类别、特性、运行复杂程度及覆盖范围内的有效人数和实施场所数量等情况，核算并拟定完成认证审核工作需要的时间。特殊情况下，可以合理的增加或减少审核时间。具体审核时间核算按照附录 A 的规定执行。

5.2.2 审核准备

5.2.2.1 确定审核目的、范围和准则

SCS 按照《管理体系认证审核控制程序》的要求，在充分掌握受审核组织基本信息的基础上，确定审核目的、审核范围和审核准则，审核准则包括适用的审核标准或认证技术规范、相关法律法规和受审核组织建立并有效运行的体系文件。

5.2.2.2 选择和指派审核组

（1）审核组应具备实施云服务信息安全管理体系认证审核的能力。审核组中应指定一名有能力的审核员担任审核组长，审核组内至少有一名熟悉信息安全相关专业知识的人员，在必要时可配备相关行业的技术专家，以保证审核组的整体能力覆盖组织的云服务信息安全管理体系范围所需的专业审核能力要求。

（2）必要时，可选择技术专家参加审核组。审核组的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同组审核员承担责任。

5.2.2.3 审核通知

确定审核时间和审核组后，拟定审核通知，发给受审核方，经受审核方确认后，发给审核组。

5.2.2.4 审核计划

SCS 委派的审核组组长负责根据规定的要求，结合收集的受审核组织信息编制审核计划，以便为有关各方就认证审核活动的安排和实施达成一致提供依据。

审核组组长提前与受审核组织就认证审核活动安排进行沟通，达成一致意见。为使现场审核活动能够观察到认证覆盖范围内的所有活动情况，现场审核应安排在认证范围覆盖的过程活动正常实施时进行。

5.2.3 审核时间的确定

（1）为确保认证审核的完整有效，SCS 根据申请组织云服务信息安全管理体系覆盖的活动范围、环境背景和风险、组织规模等情况，核算并拟定完成审核工作需要的时间。附录 A 给出了确定审核时间的指南。

（2）若申请组织已通过信息安全管理体系认证，并证书有效，则可适当减少审核时间，现场审核时间不应少于总人日数的 80%，最低不能少于一个人日。

5.3 实施审核

5.3.1 总要求

云服务信息安全管理体系认证审核分为初审、监督审核（第一次、第二次）、再认证审核类型，审核组将按照审核计划的安排完成审核工作。现场审核中的“现场”指认证范围内的各类活动完成的主要场所，一般情况下，是组织人员集中的地方。

5.3.2 初审

初次认证审核，分为第一、二阶段实施审核。

5.3.3 第一阶段审核

5.3.3.1 第一阶段审核活动包括文件审核，并通常包括现场访问。有下列情况之一时，第一阶段可以不在申请组织现场进行：

——客户已获 SCS 颁发的其他认证证书，已对云服务信息安全管理体系有充分了解。

——客户有充足的理由证明其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。

——客户获得过其他经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核 可以达到第一阶段审核的目的和要求。

除以上情况以外，第一阶段应在受审核方的生产或服务场所进行。

5.3.3.2 文件审核。

（1）文件审核将在现场审核实施前进行，SCS 依据审核标准或认证技术规范及相关的法律法规，对受审核组织的云服务信息安全管理体系运行文件进行适宜性和充分性的评审。当文件审核过程中发现文件存在不符合而影响体系的有效运行时，SCS 将告知受审核组织进行及时的纠正和纠正措施，审核组组长对其文件修改内容进行确认。在文件审核通过后方可实施现场审核。

(2)审核组按审核计划进第一阶段现场审核，至少应包含以下内容：

a. 审核申请组织的 CSISMS 管理体系文件，了解体系建立情况；

b. 评价申请组织的运作场所和现场的具体情况，并与申请组织的人员进行讨论，以确定第二阶段审核的准备情况；

c. 审核申请组织理解和实施 CSISMS 标准要求的情况，特别是对关键绩效、风险等级、关键云服务信息安全、过程、目标和管理体系的运行方面。收集和确定必要的信息资料，包括管理体系的范围（含边界），过程，场所（含虚拟场所），以及相关的法律和法规合规性；

d. 审核申请组织是否系统而充分地识别与 CSISMS 相关的法律法规和其他要求及其遵守情况；

e. 审核第二阶段审核所需资源的配置情况，并与申请组织商定第二阶段审核的细节；

f. 结合申请组织 CSISMS 方针和目标，了解其审核准备状态，为策划第二阶段的审核提供重点；

g. 评价申请组织是否策划和实施了内部审核与管理评审，以及 CSISMS 实施程度能否证明其已为第二阶段审核做好准备。

h. 确定认证活动引发的客户信息安全风险（包含保密性或敏感性信息），以及控制措施。

5.3.3.2 第一阶段审核结束后，审核组应将第一阶段审核发现及一阶段审核结论形成文件并告知申请组织，包括任何应引起关注的、在第二阶段审核中可能被判定为不符合的问题。

5.3.4 第二阶段现场审核

SCS 委派审核组按照本规则的要求和确定的审核标准或规范，对受审核组织的云服务信息安全管理体系实施现场审核，包括查阅文件和记录、询问工作人员、观察现场、现场试验等。

5.3.4.1 召开首次会议

审核组与受审核组织的管理层(适用时,还包括拟审核职能或过程的负责人员)召开正式的首次会议，并形成记录。首次会议通常由审核组组长主持，会议目的是简要解释将如何进行审核活动。受审核方要求时，审核组成员应向申请组织出示身份证明文件。

5.3.4.2 现场审核

（1）审核时采用查阅文件和记录、询问工作人员、观察现场、现场试验等方式，充分搜集与申请组织云服务信息安全管理体系相关的信息。按照 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施规程》及相关法律法规和需求对申请组织进行审核。

（2）审核内容

现场审核组至少对下列活动进行审核确认：

a. 云服务信息安全管理体系建立和运行与 ISO / IEC 27017：2015《云服务信息安全管理体系要求》的符合性、适宜性、充分性和有效性；

b. 在第一阶段审核中确定的重要审核点的监视、测量和控制措施的充分性和有效性；

c. CSISMS 与法律合规性；

d. 建立并实施云服务信息安全政策；

e. 申请组织的内部审核和管理评审是否有效。

f. 云服务信息安全管理体系的自我改进及完善机制的持续性和有效性。

(3)在现场审核中发现的任何应引起关注的、或可能被判定为不符合项的问题，审核组将选用的适当方式告知受审核组织。

(4)确定和记录审核发现

a. 审核组依据认证依据及受审核组织的云服务信息安全管理体系运行情况,结合现场审核的客观证据逐项进行审核并记录。

b. 审核组在现场确定审核发现,简述符合性并详细描述不符合以及为其提供支

持的审核证据，以便为认证决定或保持认证提供充分的信息。

c. 关于不符合项的审核发现需对照审核准则的具体要求予以记录，包含对不符合事实的清晰陈述及其客观证据。审核员初步确定不符合项并填写相关记录文件。

(5)当审核组发现受审核组织的名称、地址、受审核组织人数、认证范围(扩大、缩小、变更)等内容与审核委派不一致时，审核组组长应在发现变化时，及时将了解到的变化信息报告 SCS。

5.3.4.3 末次会议

现场审核结束前，审核组与受审核组织的管理层(适用时，还包括审核职能或过程的负责人员)召开正式的末次会议并形成记录。末次会议通常由审核组组长主持，会议目的是提出审核结论，包括关于审核的推荐性意见。并就不符合项纠正措施实施时限和有效性验证方式达成一致。

5.3.5 审核报告

(1)现场审核结束后，由审核组组长负责编制审核报告，报告应包括但不限于以下内容：

a. 首页：

——标题、项目编号；

——受审核方/委托单位及地址、委托方代表及联系方式；

——审核单位、审核组成员及联系方式、报告编制日期；

——审核单位声明。

b. 正文：

——审核目的；

——审核准则；

——审核类型；

——审核范围；

——审核方案；

——审核结果；

——与有关认证要求符合性的陈述；

——报告覆盖的时间段；

——不符合项的情况；

——审核结论。

c. 附件（需要时）：

——审核参考资料、原始记录；

——企业声明等。

(2)在现场审核结束后(适用时，不符合纠正措施验证有效后)，审核组及时将交本次审核的报告及与审核项目有关且符合标准的全部案卷资料提交 SCS，用以支持 SCS 评审委员会做出认证决定。

(3)SCS 享有对审核报告的所有权。经 SCS 批准后，向受审核组织提供审核报告。如果对本报告如有异议，受审核组织应在报告发出之日起 10 个工作日内提出。

(4)受审核组织应妥善保管审核报告、审核计划等文件化信息，以便证实认证活动的真实性。

5.4 不符合项的纠正和纠正措施及其结果的验证

（1）对审核中发现的不符合项，SCS 应要求申请组织分析原因，并要求申请组织在规定期限内采取措施进行纠正。

（2）SCS 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。

5.5 认证决定

5.5.1 SCS 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审核基础上，作出认证决定。

5.5.2 审核组成员不得参与对审核项目的认证决定。

5.5.3 SCS 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 5.3 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，本机构已评审、接受并验证了纠正和纠正措施及结果的有效性。

a. 未能满足云服务信息安全管理体系标准的要求。

b. 制定的管理目标不可测量、或测量方法不明确。

c. 对实现管理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。

d. 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，实现管理目标有重大疑问。

(3) SCS 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。

5.5.4 在满足 5.5.3 条要求的基础上，SCS 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。

a.申请组织的云服务信息安全管理体系认证符合标准要求且运行有效。

b.认证范围覆盖的产品或服务符合相关法律法规要求。

c.申请组织按照认证合同规定履行了相关义务。

5.5.5 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。

5.5.6 SCS 在颁发认证证书后，应当在 30 个工作日内按照规定的要求将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本机构上报的认证证书信息。

5.5.7 SCS 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 监督审核的频次

（1）为确保获证组织持续满足认证要求，在认证证书有效期内，SCS 安排在初次认证决定(认证证书的发证日期)后的 12 月内实施第一次监督审核；在第一次监督审核结束后的 12 个月内完成第二次监督审核。

（2）如果发生以下情形时，SCS 在正常例行监督审核的间隔期间可考虑增加审核频次或专项审核：

a. 获证组织发生影响产品和服务质量的重大事故、媒体曝光或顾客投诉，经查实为获证组织责任的；

b. 获证组织发生重大变更时，包括法人、运行场所、组织机构、有关职能、资源、产品或服务提供流程等变更，以及影响体系运行符合性的相关变更；

c. 认证依据发生变化时；

d. 获证组织发生质量、安全、环境和卫生事故及发生重大失信事件或客户多次投诉；

e. 对被暂停认证资格的获证组织进行追踪；

f. 发生其他影响符合认证要求的特殊情况时。

6.2 监督审核的方式

（1）SCS 的监督审核通常为现场审核。

（2）监督审核至少包括以下内容：

a. 上次审核以来云服务信息安全管理体系覆盖的活动及运行体系的资源是否有变更。

b. 重要关键点是否按云服务信息安全管理体系的要求在正常和有效运行。

c. 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。

d. 云服务信息安全管理体系覆盖的活动涉及法律法规规定的，是否持续符合相关规定。

e.云服务信息安全相关的事件及处理结果是否达到了目标。适用时，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、分析原因并采取了改进措施。

f. 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。

g. 适用时，内部审核和管理评审是否规范和有效。

h. 是否及时接受和处理投诉。

i. 适用时，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。

j.认证证书、标志的使用和(或)任何其他对认证结果信息的引用。

6.3 监督审核结果审定

SCS 对监督审核的结果进行审定，审定为合格者，SCS 将批准其继续保持认证资格、使用认证标志。并以书面形式告知获证组织。审定不合格者，将暂停其认证资格、使用认证证书和标志,并通知获证组织在两个月内限期整改。审核员对其纠正措施进行验证，验证通过的，恢复其认证资格、使用认证证书和标志；验证不通过的，撤销其认证证书，并对外公告。

7 再认证审核

7.1 认证证书有效期为三年，若获证组织需要延续认证有效期，应在认证证书有效期截止日期前 3 个月，向 SCS 提出再认证审核申请，并提交相关资料。

7.2 当获证组织的云服务信息安全管理体系及内部和外部环境未发生重大变化时，再认证审核可省略文件审核过程，可直接进行现场审核。但现场审核时间不应少于初始现场审核人日的 70%。特殊情况下，可适时合理增加人日数，增加理由应充分。当获证组织

的云服务信息安全管理体系或组织管理机构的运行环境有重大变更时，再认证审核应该安排文件审核。

7.3 对于再认证审核组提出的不符合，受审核组织要在规定的时限内实施纠正和纠正措施，并确保在认证证书有效期截止日期前得到审核组和 SCS 对实施有效的验证。

7.4 当 SCS 做出同意再认证的决定并换发认证证书。新认证证书发证日期为再认证决定日期，有效期 3 年。对在 SCS 初次认证以来未中断过的再认证证书，可注明 SCS 初次认证证书的发证日期。

8 认证的变更

8.1 变更的申请

证书上的内容发生变化时，持证人应向 SCS 提出申请。

8.2. 变更和批准

SCS 根据变更的内容和提供的资料进行评审，确定是否允许变更。如果需要进行审核的，则 SCS 组织审核合格后方能变更。

对符合要求的，批准变更。换发新证书的，新证书的编号、批准有效日期保持不变，并注明换证日期。

8.3 特殊审核与补充审核

必要时，为调查投诉、主管部门监督抽查不合格、社会曝光情况等做出回应或对被暂停的客户进行追踪，需进行特殊审核；为需要进行全面或部分的补充，或需要形成文件的证据（在将来的监督审核中予以确认），以验证纠正和纠正措施的有效性，需进行补充审核。

9 暂停或撤销认证证书

9.1 SCS 应制定暂停、撤销认证证书或缩小认证范围的规定，并形成文件化的管理制度。

9.2 暂停证书

9.2.1 获证组织有以下情形之一的，SCS 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）被地方认证监管部门发现云服务信息安全管理体系运行存在问题，需要暂停

证书的。

（5）持有的与云服务信息安全管理体系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。

（6）主动请求暂停的。

（7）其他应当暂停认证证书的。

9.2.2 认证证书暂停期不得超过 6 个月。但属于 9.2.1 第（5）项情形的暂停期可至相关单位作出认证决定之日。

9.2.3 SCS 暂停认证证书的信息，应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。

9.3 撤销证书

9.3.1 获证组织有以下情形之一的，SCS 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）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。

（4）有其他严重违反法律法规行为的。

（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（包括持有的与云服务信息安全管理体系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）。

（6）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。

（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 SCS 已要求其纠正但超过 6 个月仍未纠正的。

（8）其他应当撤销认证证书的。

9.3.2 撤销认证证书后，SCS 应及时收回撤销的认证证书。若无法收回，SCS 应及时在相关媒体和网站上公布或声明撤销决定。

9.4 SCS 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。

9.5 SCS 有义务和责任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。

10 认证证书要求

10.1 认证证书应至少包含以下信息：

(1)SCS 的名称、地址和认证标志；

(2)获证组织的名称、地址及其服务提供场所的地址；

(3)认证范围；

(4)审核所依据的认证标准、认证技术规范或其他规范性文件；

(5)与云服务信息安全管理体系有关认证要求符合性的陈述；

(6)发证日期(即生效日期)和认证有效期或终止日期；

(7)认证证书名称和证书编号；

(8)SCS 的印章和证书签发人的签字；

(9)证书查询方式:SCS 除公布认证证书在 SCS 的查询方式外,还应当在证书上注明:“可在国家认证认可监督管理委员会网站 www.cnca.gov.cn 查询”，以便于社会监督。

(10)适用时，其他需要标注的内容。

10.2 认证证书有效期最长为 3 年。

10.3 SCS 应当建立证书信息披露制度。除向申请组织、认证监管部门等执法监管部门提供认证证书信息外,还应当根据社会相关方的请求向其提供证书信息,接受社会监督。

11 与其他服务、管理体系的结合审核

11.1 对云服务信息安全管理体系认证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，审核报告中应清晰地体现 5.3 条要求，并易于识别。

11.2 结合审核时，应按公司《审核时间确定程序》核算结合审核的审核人日数。

12 受理转换认证证书

12.1 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、不能有效执行云服务信息安全管理体系要求的组织申请认证证书的转换。

12.2 SCS 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。

12.3 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。

12.4 被发证的认证机构撤销证书的，除非该组织进行彻底整改，导致暂停或撤销认证

证书的情形已消除，否则不应受理其认证申请。

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，SCS 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。

13.2 书面通知应当告知申诉人，若认为 SCS 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，保存时间至少应当与认证证书有效期一致。

14.3 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。

14.4 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，保存时间至少应当与认证证书有效期一致。

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。

15.2 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，并经审核员签字确认与原件一致。

14.3 SCS 可开展云服务信息安全管理体系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

审核时间计算说明

云服务信息安全管理体系的审核时间与信息安全管理体系的审核时间相同。

若申请方已获得 GB/T 22080(ISO/IEC 27001,IDT)有效认证证书:并且范围覆盖了云服务信息安全管理体系认证申请范围,则云服务信息安全管理体系的审核时间数按照信息安全管理体系的审核时间的 0.5 倍+1 天进行计算(向上取整至 0.5 人天)；当 GB/T22080(ISO/IEC27001,IDT) 证书由 SCS 颁发时,则云服务信息安全管理体系的审核时间数按照信息安全管理体系的审核时间的 0.5 倍进行计算(向上取整至 0.5 人天);云服务信息安全管理体系与信息安全管理体系结合审核时,审核时间按照信息安全管理体系的审核时间的 0.4 倍进行计算(向上取整至 0.5 人天)

附录 A 证书模板

云服务信息安全管理体系认证证书

注册号：XXXXXXXX

兹证明

XXXXXXXXXXX

统一社会信用代码：xxxxxxxxxxxxxxxxxx

注册地址：xxxxxxxxxxxxxxxxxxxxxx 邮编：xxxxxx

经营地址：xxxxxxxxxxxxxxxxxxxxxx 邮编：xxxxxx

云服务信息安全管理体系符合标准：

ISO/IEC 27017：2015 通过认证的范围如下：

XXXXXXXXXXXXXXXXXXX

认证范围涉及法律法规要求的行政许可、资质许可、强制性认证的，证书与资质共同使用有效。

首次发证日期:xxxxxxxx
本次发证日期:xxxxxxxx
证书有效期至:xxxxxxxx

签发人：

注：在证书有效期内，获证组织必须定期接受监督审核并经评定合格后证书方可保持有效。本证书有效性可扫描下方二维码获取，同时可在国家认证认可监督管理委员会网站 www.cnca.gov.cn 查询。

二维码

神州（天津）认证服务有限公司

Shenzhou(Tianjin) Certification Service Co., Ltd.

地址：天津市河东区八纬路 20 号院内副楼三层-301 300012

网址：http://www.shenzhourz.com

电话：022-84220001