云服务信息安全管理体系
认证实施规则

编制：张晓丹

审核：邵海梅

批准：张艳红

发布日期：2021/5/1　　修订日期：2025/5/26　　实施日期：2025/5/26

目　录

1 适用范围

1.1 本规则用于 RLAC 在中国境内开展的云服务信息安全管理体系认证活动。

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，对云服务信息安全管理体系认证实施过程作出具体规定，明确 RLAC 对认证过程的管理责任，保证云服务信息安全管理体系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认证以国际标准 ISO/IEC 27017《信息技术--安全技术--基于 ISO/IEC27002 的云服务信息安全控制的实用规则》为认证依据。

3 对认证审核人员的基本要求

3.1 具备 CCAA 注册的信息安全管理体系资格；

3.2 从事与信息安全管理体系认证相关活动的人员应具备必要的教育、工作经历，具备与信息安全管理体系相关工作的经验或接受相关内容的培训，并具有与云服务信息安全管理体系等方面的专业知识。

3.3 参加公司或认可的外部组织的 ISO/IEC 27017 标准培训，培训不少于 8 学时。

3.4 应当遵守《中华人民共和国认证认可条例》等与从业相关的法律法规，对认证活动及作出的认证评价报告和认证结论的真实性承担相应的法律责任。

4. 初次认证

4.1 受理认证申请

申请组织的授权代表至少提供以下必要的信息：

(1)法人资格证明(工商营业执照、事业单位法人证书或社会团体法人登记证书)；

(2)取得相关法规规定的行政许可文件(适用时)；

(3)从事的业务活动符合中华人民共和国相关法律、法规、云服务信息安全标准和有关规范的要求；

(4)已按认证依据和相关要求建立和实施了文件化的云服务信息安全管理体系；

(5)已取得有效的 ISMS 证书且证书在有效期内或与 CSSMS 结合审核；

(6)体系有效运行 3 个月以上，并且已完成内部审核和管理评审。

4.2 申请评审

RALC 应根据认证依据、程序等要求，及时对申请组织提交的申请文件和资料进行评审并保存评审记录，以确保：

(1) 申请组织及其 CSSMS 的信息充分，可以进行审核；

(2)认证要求已有明确说明并形成文件，且已提供给申请组织；

(3)考虑了申请的认证范围、申请组织的运作场所、完成审核需要的时间和任何其他影响认证活动的因素；

(4)保持了决定实施审核的理由的记录。

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，RLAC 不受理其认证申请。

4.3 签订认证合同

在实施认证审核前，RLAC 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。

（2）申请组织应及时向 RLAC 提供真实有效信息，包括但不限于：

① 申请认证的组织名称、注册地址、经营地址、通讯地址、联系人、职务、联系方式；

② 认证类型；

③ 认证依据；

④ 体系覆盖的人数；

⑤ 根据业务、组织、位置、资产和技术等方面的特性所确定的 CSSMS 的范围和边界，包括对任何范围、删减的详细说明和正当性理由；

⑥ 经营场所、分场所、临时场所以及各场所从事的活动等；

⑦ 服务器数量、终端数量、用户的数量；

⑧ 适用性声明、资产列表；

⑨ 保密协议、信息安全敏感区域的声明；

⑩ 申请组织对 RLAC 的资质、诚信守法记录或认证人员身份背影的要求以及适用的、最新的与保守国家秘密或维护国家安全有的法律法规要求，以便 RLAC 判断是否具备为申请组织实施认证活动的资格或条件；

⑪ 关于认证活动的限制条件(如出于安全和/或保密等原因，存在时)。

⑫ 在认证审核之前，RLAC 应要求客户组织报告是否存在因包含保密性或敏感性信息而导致不能提供给审核组核查的 CSSMS 相关信息(例如 CSSMS 记录或关于控制的设计与有效性的信息)。RLAC 应确定 CSSMS 是否能在缺少这些信息的情况下得到充分审核。如果 RLAC 的结论是若不核查已识别的保密性或敏感性信息就不能对 CSSMS 进行充分的审核，那么 RLAC 将会告知客户只有在适当的访问安排获得许可后才能进行认证审核。

⑬ 认证协议应就控制审核和认证活动引发的客户信息安全风险做出规定，包括明确认证机构和客户及其有关人员的责任与义务。

⑭ 出现影响管理体系运行的其他重要情况。

（3）拟认证的管理体系覆盖的信息安全的活动范围。

（4）在认证审核实施过程及认证证书有效期内，认证机构和申请组织各自应当承担的责任；

（5）认证服务的费用、付费方式及违约条款。

4.4 审核策划

4.4.1 审核时间

4.4.1.1 为确保认证审核的完整有效，RLAC 以附录 B 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系覆盖的活动范围、特性、技术复杂程度、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。考虑文审、前期策划等原因，可以减少审核时间，减少的时间不得超过附录 B 所规定的审核时间的 30%；

4.4.1.2 依据申请组织的体系成熟度、业务过程的风险程度等因素，可以减少 20-30%的审核时间。

4.4.1.3 与信息安全管理体系、隐私信息安全管理体系等结合审核时，可以减少 20%的审核时间。

4.4.2 审核组

4.4.2.1 审核组应由取得 ISMS 认证注册资格且经机构认可 CSSMS 的的审核员组成。必要时可以补充技术专家以增强审核组的技术能力。

4.4.2.2 具有 CSSMS 及相关法规等方面的特定知识的技术专家可以成为审核组成员。技术专家应在审核员的监督下进行工作，可就受审核方 CSSMS 中技术充分性事宜为审核员提供建议，但技术专家不能作为审核员。

4.5 实施审核

初次认证审核，分为第一、二阶段实施审核。

4.5.1 第一阶段审核

4.5.1.1 第一阶段审核宜采取现场审核的方式进行。如遇不可抗力，可以考虑远程审核的方式进行。审核内容包括：

(1)审核申请组织的 CSSMS 文件；

(2)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；

(3)审查申请组织理解和实施 CSSMS 标准要求的情况；

(4)审查申请组织是否系统而充分地识别与 CSSMS 相关的法律法规和其他要求及其遵守情况；

(5)审查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；

(6)结合申请组织 CSSMS 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；

(7)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 CSSMS 实施程度能否证明其已为第二阶段审核做好准备。

4.5.1.2RALC 应将第一阶段审核发现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。

4.5.2 第二阶段审核

第二阶段审核宜采取现场审核的方式进行。如遇不可抗力，宜采取远程的方式进行。

第二阶段审核的目的是评价申请组织的 CSSMS 是否满足所有适用的认证依据的要求，并判断是否推荐认证注册。

RALC 应要求申请组织证实其已依据 ISO/IEC 27017《信息技术--安全技术--基于 ISO/IEC27002 的云服务信息安全控制的实用规则》及相关法律法规和需求对云服务信息安全管理体系进行了相应的策划、实施、监视和改进，应至少包括：

（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 CSSMS 方针而在相关职能、层次和过程上建立 CSSMS 目标是否具体适用、可测量并得到沟通、监视。

（3）对 CSSMS 管理体系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） 申请组织的内部审核和管理评审是否有效。

4.5.3 发生以下情况时，审核组应向 RLAC 报告，经 RLAC 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。

4.6 审核报告

4.6.1 审核组应对审核活动形成书面审核报告。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、审核组成员信息。

（5）审核活动的实施日期和地点；

（6）识别出的不符合项。

（7）审核组对是否通过认证的意见建议。

4.6.2 RLAC 应保留用于证实审核报告中相关信息的证据。

4.6.3 认证机构应在作出认证决定后 30 个工作日内将审核报告提交申请组织；

4.6.4 对终止审核的项目，审核组形成终止审核报告。

4.7 不符合项的纠正和纠正措施及其结果的验证

对审核中发现的不符合项，RLAC 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。RLAC 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，则应不予通过，或者重新实施第二阶段审核。

4.8 认证决定

4.8.1 认证机构应该在对审核报告、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。

4.8.2 认证决定人员应为认证机构管理控制下的人员，审核组成员不得参与对审核项目的认证决定。

4.8.3 RLAC 应为符合标准要求且运行有效的申请组织颁发认证证书。若申请组织不符合认证要求，以书面形式告知并说明其未通过认证的原因。

5 监督审核

5.1 监督审核策划

5.1.1 依据相关管理体系审核要求和获证组织的 CSSMS 特点及风险，合理设计监督审核的时间和频次。当获证组织 CSSMS 发生重大变更，或发生重大问题、信息安全事故、客户投诉等情况时，RALC 可视情况增加监督的频次。

5.1.2 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。

5.1.3 由于获证组织业务运作的时间(季节)特点及其内部审核安排等原因，可以合理选取和安排监督周期及时机，在认证证书有效期内的监督审核必须覆盖 CSSMS 认证范围内的所有业务活动。

5.2 监督审核应包括，但不限于以下内容：

(1)体系保持和变化情况；

(2)顾客投诉情况；

(3)涉及变更的范围；

(4)内部审核与管理评审；

(5)CSSMS 的响应事件及处理结果是否达到了目标；

(6)对上次审核时提出的不符合所采取纠正措施的审查；

(7)标志的使用和（或）任何其他对认证资格的引用；

(8)适当时，其它选定的范围。

5.3 对于监督审核合格的获证组织，应作出保持其云服务信息安全管理体系认证资格的决定；否则，应暂停、撤销或注销相应的认证资格。

5.4 监督审核的时间，应不少于初次审核时间人日数的 1/3。

5.5 在监督审核中发现的不符合项，认证机构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。

5.6 监督审核的审核报告，应有相应的描述或引用审核证据、审核发现和审核结论。

5.7 认证机构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。

6 再认证审核

6.1 再认证审核

再认证认证证书有效期满前，根据获证组织的申请对获证组织实施再认证，以保证 CSSMS 认证证书持续有效。

6.1 再认证审核的策划

6.1.1 应策划和实施再认证审核，以评价获证组织是否持续满足 CSSMS 标准和相关的认证规范性文件的所有要求。

6.1.2 再认证审核应考虑 CSSMS 在认证周期内的绩效，包括调阅以前的监督审核报告。

6.1.3 当获证组织、获证组织的 CSSMS 或其运作环境有重大变更时，RALC 应有程序确保对再认证审核活动可能需要进行的第一阶段审核实施管理。

6.1.4 对于多场所认证或依据多个管理体系标准进行的认证，再认证审核的策划应确保现场审核具有足够的覆盖范围，以提供对 CSSMS 认证的信任。

6.1.5 再认证审核时间应不少初审认证计算人日数的 2/3。

6.2 对再认证审核中发现的不符合项，认证机构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。

6.3 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。

6.4 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。

7 暂停或撤销认证证书

7.1 对于体系运行不能持续满足要求，或在体系运行期间，获证组织严重不满足认证要

求，RLAC 将对申请组织的证书进行暂停或者撤销等处理。

7.2 暂停证书

7.2.1 获证组织有以下情形之一的，RLAC 应在调查核实后的 5 个工作日内暂停其认证证书。

（1）获证组织不允许按要求的频次实施监督或再认证审核；

（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）主动请求暂停的。

（5）其他应当暂停认证证书的。

7.2.2 认证证书暂停期不得超过 6 个月。

7.2.3 RLAC 及时上报暂停证书信息，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。

7.3 撤销证书

7.3.1 获证组织有以下情形之一的，RLAC 应撤销其认证证书。

（1）被注销或撤销法律地位证明文件的。

（2）被列入信用严重失信企业名单或者被列入异常经营企业名单；

（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）拒绝接受国家产品质量监督抽查的。

（5）出现重大的产品和服务等质量安全事故，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（包括持有的与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）没有运行管理体系或者已不具备运行条件的。

（9）其他应当撤销认证证书的。

7.3.2 撤销认证证书后，RLAC 应及时上报撤销的认证证书信息。

7.4 RLAC 暂停或撤销认证证书信息及时上报国家认监委相关信息平台。

8 认证证书要求

8.1 证书内容

认证证书内容应以中文书写，至少包括以下方面：

(1)认证证书名称，即“云服务信息安全管理体系认证证书”；

(2) 获证组织名称、注册地址、受审核地址；

(3)认证覆盖的范围；

(4)颁证日期、换证日期以及证书有效期的起止年月日。

(5)RLAC 的名称及其标志；

(6)RLAC 法定代表人代表或其授权人的签字；

如果认证所覆盖产品(或服务)的类别及其所涉及的过程和覆盖的场所较多，需在证书附

件上加以注明。

8.2 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。

8.3 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，RLAC 还在官网上提供认证证书信息，接受社会监督。

9. CSSMS 文件与其他管理体系文件的整合

只要 CSSMS 以及与其他管理体系的适当接口能够清楚地被识别，可以允许申请组织将 CSSMS 文件与其他管理体系文件(如：质量管理体系、信息技术服务管理体系、信息安全管理体系等)相整合。

9.1 管理体系结合审核

9.1.1 RALC 可以仅提供 CSSMS 认证服务，或结合其他管理体系提供认证服务。但是这种结合必须以审核活动满足 CSSMS 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。

9.1.2 RALC 应有程序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的管理。在结合审核报告中，应清晰体现所有与 CSSMS 有关的重要要素的描述并易于识别。

10 对获证组织的信息沟通和要求

10.1 信息沟通

为确保获证组织的 CSSMS 认证持续有效，RALC 应要求获证组织建立信息通报制度，及时向 RALC 通报以下信息：

(1)业务、地点、组织机构变化等情况的信息(及时通报)；

(2)顾客投诉的相关信息；

(3)组织的体系文件、产品和服务信息的变化；

(4)有严重 CSSMS 事故的信息(及时通报)；

(5)其他重要信息(视情况)。

10.2 响应要求

RALC 应对上述信息以及收集到的相关公共信息进行分析，视情况采取相应措施，包括增加监督审核频次在内的措施和暂停或撤销认证资格的措施。在发生重大客户投诉等严重情况时，需立即采取措施。

附录 A CSSMS 认证业务范围分类表

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	一	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	一	医疗服务	
	02.06	三	教育	
	02.07	二	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	二	旅游 、宾馆 、饭店	
	03.06	三	其他	
04		**产品的生产**		
	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	
	04.04/ 1	一	农药	
	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	04.11/ 1	二	药品	
	04.12	三	农 、林 、牧 、 副、 渔业	
	04.13	三	其他	
	04.13/ 1	三	制造业	
	04.13/ 2	三	建设工程施工	
	04.13/ 3	三	测绘服务	

注：CSSMS 是 ISMS 的扩展，业务范围管理基于 ISMS 的划分实施。

附录B 认证审核时间要求

有效人数	审核时间 第一阶段+第二阶段 （天）	有效人数	审核时间 第一阶段+第二阶段 （天）
1 ~ 10	5	876 ~ 1175	18.5
11 ~ 15	6	1176 ~ 1550	19.5
16 ~ 25	7	1551 ~ 2025	21
26 ~ 45	8.5	2026 ~ 2675	22
46 ~ 65	10	2676 ~ 3450	23
66 ~ 85	11	2451 ~ 4350	24
86 ~ 125	12	4351 ~ 5450	25
126 ~ 175	13	5451 ~ 6800	26
176 ~ 275	14	6801 ~ 8500	27
276 ~ 425	15	8501 ~ 10700	28
426 ~ 625	16.5	> 10700	沿用以上规律
626 ~ 875	17.5		

注 1：CSSMS 是基于 ISMS 扩展的管理体系，CSSMS 这对 ISMS 附录 A 扩展的要求有三个方面：一是在原有的 ISMS 标准的附录 A 中控制条款延展了 40-50%的要求，并且分为云服务客户、云服务提供方和两者组成的供应链三种情况，相当于延伸了 280%-300%，将控制要求更具体化；二是在 ISMS 标准附录 A 中的控制条款基础上，增加了 7 个（为云服务客户、云服务提供方和两者组成的供应链三种，相当于增加了 14 个）CSSMS 特定的云服务控制条款。虽然 CSSMS 标准没有涉及 ISMS 的正文条款，为使审核具备完整性，CSSMS 审核要兼顾 ISMS 正文要求；三是审核的时候面对的审核样本巨大，且偏向于技术审核。

注2：监督审核人天不低于初次认证审核总时间的1/3；再认证审核人天不低于初次认证审核总时间的2/3；