信息安全管理体系认证实施规则

编制：申金怡

审核：邵海梅

审批：张艳红

发布日期：2021 年 5 月 10 日　　更新日期：2025 年 7 月 11 日　　实施日期：2021 年 5 月 10 日

目　录

1 适用范围

本规则用于规范认证机构在中国境内开展信息安全管理体系认证活动。

2 认证依据

信息安全管理体系认证以 ISO/IEC27001:2022 标准为认证依据。

3 认证程序

3.1 认证申请

认证机构应要求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；

(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、信息安全标准和有关规范的要求；

(4)对信息安全管理体系认证范围涉及的业务活动的描述；

(5)已按认证依据和相关要求建立和实施了文件化的信息安全管理体系；

(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。

3.2 申请评审

认证机构应根据认证依据、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)掌握国家对相应行业的信息安全管理体系认证的管理要求；

(2)申请组织及其管理体系的信息充分，可以进行审核；

(3)认证要求已有明确说明并形成文件，且已提供给申请组织；

(4)解决了认证机构与申请组织之间任何已知的理解差异；

(5)认证机构有能力并能够实施认证活动；

(6)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；

(7)保持了决定实施审核的理由的记录。

3.3 现场审核的准备

3.3.1 确定审核组

3.3.1.1 认证审核人员必须取得 CCAA 批准的信息安全管理体系认证注册资格。

3.3.1.2 审核组应由取得信息安全管理体系认证注册资格的审核员组成，必要时可以补充技术专家以增强审核组的技术能力。

3.3.1.3 具有信息安全、信息安全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，可就受审核方管理体系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。

3.3.2 确定审核人日

RLAC 根据申请组织的规模、特性、业务复杂程度、信息安全服务管理体系涵盖的范围、认证要求和其承担的风险等因素核算并确定审核人日，以确保审核的充分性和有效性。具体执行 CC170《信息安全管理体系认证机构要求》的相关规定，

3.4 初次认证审核

3.4.1 初次认证审核分第一阶段和第二阶段进行。第一阶段与第二阶段现场审核应有时间间隔。

3.4.2 第一阶段审核应在申请组织的现场进行，审核内容包括：

(1)审核申请组织的信息安全管理体系文件；

(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信息安全管理体系标准要求的情况；

(4)审查申请组织是否系统而充分地识别与所提供的服务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)结合申请组织信息安全管理体系方针和目标，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，以及信息安全管理体系的实施程度能否证明其已为第二阶段审核做好准备。

3.4.3 RLAC 应将第一阶段审核发现形成文件并告知申请组织，包括识别任何引起关注的、在第二阶段审核中可能被判定为不符合的问题。

3.4.4 第二阶段审核

第二阶段审核应在具备实施认证审核的条件下在申请组织的场所进行。如果第一阶段审核提出影响实施第二阶段审核的问题，这些问题应在第二阶段审核前得到解决。第二阶段审核的目的是通过在申请组织的现场进行系统、完整地审核，评价申请组织的信息安全管理体系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。应重点关注申请组织是否充分识别了信息安全管理过程的重要性，并证实与申请组织的信息安全活动是相适应的。

申请组织证实其对信息安全管理过程的分析和组织运作实施了适当的控制措施，应包括:

(1) ）信息安全有关的风险的评估的结果；

(2) ）基于风险评估与风险处置过程所选择的控制目标与控制措施的适宜性、有效性；

(3) 标准及附录 A 中要求形成控制策略的过程，是否考虑了外部环境、内部环境与相关的风险，以及组织对信息安全过程和控制的监视、测量与分析，以确定控制是否得以实施、有效并达到其所规定的目标；

(4) 所选择和实施的控制措施、适用性声明（(SoA)及风险评估和风险处置过程的结果相互之间的一致性），以及它们与信息安全方针和目标之间的一致性；

(5) 客户对信息安全绩效和信息安全体系有效性的评审等

3.4.5 信息安全管理体系文件与其他管理体系文件的整合

只要信息安全管理体系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信息安全管理体系文件与其他管理体系文件(例如，质量管理体系、环境管理体系，职业健康安全管理体系等)相结合。

3.4.6 管理体系结合审核

3.4.6.1 RLAC 可以仅提供信息安全管理体系认证服务，或结合信息技术服务管理体系认证或结合其他管理体系，提供管理体系认证服务。

3.4.6.2 可以把信息安全管理体系的审核和其他管理体系的审核相结合，但是这种结合必须以审核活动满足信息安全管理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，应清晰体现所有与信息安全管理体系有关的重要要素的描述并易于识别。

3.4.7 初次认证的审核结论

审核组应该对第一阶段和第二阶段审核中收集的所有信息和证据进行汇总分析，评价审核发现并就审核结论达成一致。

3.5 认证决定

3.5.1 原则

3.5.1.1 参加审核的人员不能再作为认证决定人员实施认证决定。

3.5.1.2 应该以认证过程中收集的信息和其他相关信息为基础，以充分的证据证实申请组织建立信息安全管理体系的管理评审和内部审核的方案已经得到有效实施并且将得到保持，才可决定申请组织通过认证。

3.5.2 决定

3.5.2.1 对于通过认证的申请组织，向其颁发信息安全管理体系认证证书。

3.5.1.2 对于未通过认证的申请组织，应以书面的形式明示其不能通过认证的原因。

3.6 监督审核

3.6.1 监督频次

RLAC 根据获证组织信息安全管理体系覆盖的业务活动的特点以及所承担的风险，合理设计和确定监督审核的时间间隔和频次。当获证组织信息安全管理体系发生重大变更，或发生重大问题、服务质量事故、客户投诉等情况时，RLAC 视情况可增加监督的频次。

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。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信息安全管理体系认证范围内的所有业务活动。

3.6.2 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)信息安全有关的风险变化情况；

(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等。

3.6.3 监督审核结果评价

对于监督审核合格的获证组织，RLAC 应作出保持其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。

3.7 再认证

认证证书有效期满前，RLAC 根据获证组织的申请对获证组织实施再认证，以保证信息安全管理体系认证证书持续有效。

3.7.1 再认证审核的策划

3.7.1.1 RLAC 应策划和实施再认证审核，以评价获证组织是否持续满足信息安全管理体系标准和相关的认证规范性文件的所有要求。

3.7.1.2 再认证审核应考虑信息安全管理体系在认证周期内的绩效，包括调阅以前的监督审核报告。

3.7.1.3 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，以提供对信息安全管理体系认证的信任。

3.7.2 再认证程序应与信息安全管理体系认证审核的要求和指南保持一致。

3.7.3 RLAC 应根据再认证审核的结果，以及认证周期内的体系评价结果和认证使用方的投诉，作出是否更新认证的决定。

3.8 特殊审核

3.8.1 扩大认证范围

对于已授予的认证，RLAC 应对获证组织扩大认证范围的申请进行评审，策划并实施必要的审核活动，并在该审核活动中验证获证组织的信息安全管理体系的适宜性和有效性，以作出是否可予扩大的决定。扩大认证范围的审核活动可单独进行，也可和对获证组织的监督审核或再认证一起进行。

3.9 远程审核

3.9.1 因不可抗力（疫情、恶劣天气等）因素导致无法实施现场审核时，RLAC 考虑实施远程审核。远程审核时应包括分析对客户使用远程审核的相关风险，风险分析时应考虑以下因素：

a） 机构和客户的可用基础设施；

b） 客户所在的行业；

c） 从初次审核到再认证审核的认证周期内的审核类型；

d） 机构和客户参与远程审核的人员的能力；

e） 以往已证实的、对客户实施远程审核的绩效；

f） 认证范围。

3.9.2 应在远程审核实施前进行分析。认证周期内使用远程审核的风险分析和理由应予以记录。

3.9.3 审核计划和审核报告应清楚地说明是否实施了远程审核活动。

3.9.4 如果风险评估发现对审核过程的有效性存在不可接受的风险，则不应使用远程审核。

3.9.5 风险评估应在认证周期内进行审查，以确保其持续适用性。

注：如果客户使用虚拟场所（即：组织利用网络环境完成工作或提供服务的地点，相关人员通过网络环境执行流程，不受其所在物理位置的影响。），远程审核技术是审核计划的一个相关部分。

3.10 暂停、撤消认证或缩小认证范围

3.10.1 发生以下情况(但不限于)时，RLAC 应暂停获证组织的信息安全管理体系认证资格：

(1)获证组织的信息安全管理体系持续地或严重地不满足认证要求，包括对信息安全管理体系有效性的要求；

(2)获证组织不允许按要求的频次实施监督或再认证审核；

(3)获证组织不接受或不配合认证认可监督管理部门的监督管理；

(4)获证组织主动请求暂停。

3.10.2 认证资格暂停期最长不超过 6 个月。

3.10.3 在暂停认证期间，获证组织的信息安全管理体系认证证书暂时无效。RLAC 将暂停信息上报认证认可业务信息统一上报平台，并采取其认为适当的任何其他措施。

3.10.4 如果获证组织未能在 RLAC 规定的时限内解决造成暂停认证的问题，RLAC 应撤消其信息安全管理体系认证或缩小其相应的认证范围。RLAC 将撤销信息上报认证认可业务信息统一上报平台，并采取其认为适当的任何其他措施。

3.10.5 如果获证组织在认证范围的某些部分持续地或严重地不满足认证要求，RLAC 应缩小其信息安全管理体系认证范围，以排除不满足要求的部分。

4 认证证书

4.1 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，即信息安全管理体系认证证书；

(2) 证书编号；

(3)获证组织名称、注册地址、受审核地址和邮政编码；

(4)认证依据；

(5) 颁证日期、换证日期以及证书有效期的起止年月日。

(6)认证机构的名称及其标志；

(7)认证机构的印章和法定代表人代表或其授权人的签字等

4.2 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。

5 对获证组织的信息通报要求及响应

5.1 为确保获证组织的信息安全管理体系持续有效，RLAC 要求获证组织建立信息通报制度，及时 RLAC 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)组织的体系文件的变化；

(4)有严重信息安全事故的信息(及时通报)

(5)其他重要信息。

5.2 RLAC 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，RLAC 需立即采取措施。

附录 A 信息安全管理体系审核人日表

有效人数	审核时间 第1阶段＋第2阶段（天）	有效人数	审核时间 第1阶段＋第2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	3451-4350	**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	遵循上述递进规律
626-875	**17.5**		