信息安全服务资质认证实施规则

ISCCC-ISV-R01:2017

2017-08-01 发布 **2017-09-01 实施**

中国信息安全认证中心

目 录

1 适用范围

本规则用于规范中国信息安全认证中心（简称中心）开展信息安全服务资质认证活动。

2 认证依据

以ISCCC-ISV-C01：2017《信息安全服务 规范》为认证依据。

3 术语与定义

3.1 信息安全服务

由供应商、组织机构或人员执行的一个安全过程或任务。（ISO/IEC TR 15443-1:2005《信息技术安全技术 信息技术安全保障框架 第一部分：总揽和框架》）

3.2 自评价

申请方根据认证依据对自身的服务过程进行符合性评价，并进行评价证据的收集和分析，以确定组织满足认证依据的程度。

3.3 现场审核

中心指派审核组到受审核方或获证组织所在办公地点进行的审核活动。

3.4 非现场审核

中心指派的审核组在受审核方或获证组织所在办公地点以外进行的审核活动，通常以远程审核工具、电话、视频、邮件等远程审核方式进行。

3.5 现场见证

现场见证是针对受审核方或获证组织为满足相关方利益诉求、实现组织业务目标和处置组织风险而实施的关键活动进行的，是对关键活动的执行过程进行跟踪见证。

3.6 特殊审核

特殊审核分扩大认证范围、提前较短时间通知的审核两种。

4 审核人员及审核组要求

审核人员必须取得服务审查员的注册资格，并得到中心的专业能力评价，以确定其能够胜任所安排的审核任务。

审核组应由能够胜任所安排的审核任务的审查员组成。必要时可以补充技术专家以增强审核组的技术能力。

具有与服务资质类别相关的管理和法规等方面特定知识的技术专家可以成为审核组成员。技术专家应在审查员的监督下进行工作，可就受审核方或获证组织服务过程中技术充分性事宜为审查员提供建议，但技术专家不能作为审查员。

5 认证信息公开

中心应向申请认证的社会组织(以下称申请方)至少公开以下信息：

1) 认证服务项目；

2) 认证工作程序；

3) 认证依据；

4) 证书有效期；

5) 认证收费标准。

6 认证程序

6.1 初次认证

6.1.1 认证申请

中心应要求申请方的授权代表至少提供以下必要的信息：

1) 认证申请书，包括但不限于以下内容：

   a. 申请方基本信息，包括业务活动、组织架构、联系人信息、物理位置、服务和申请级别等基本内容；

   b. 法律地位资格证明(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，组织代码证和税务登记证（如果有）)；

   c. 业务运行的时间；

   d. 取得相关法规规定的行政许可文件(适用时)。

2) 自评价表，包括但不限于：

   a. 组织根据认证依据所进行的符合性评价；

   b. 评价结论所需要的证据材料。

6.1.2 申请评审

中心应根据认证依据、程序等要求，对申请方提交的认证申请书、自评价信息及其相关资料进行评审并保存评审记录，做出评审结论，以确定：

1) 所需要的基本信息都得到提供（特别指自评价信息的完整性）；

2) 申请方的行业类别和与之相对应服务的过程特性和管理要求；

3) 对应行业的管理要求；

4) 中心与申请方之间任何已知的理解差异得到消除；

5) 中心有能力并能够实施所申请的认证活动；

6) 申请的认证范围、申请方的运作场所、完成审核需要的时间和任何其他影响认证活动的因

素；

7) 核算并确定审核人日。

6.1.3 建立审核方案

在申请评审后，中心应针对申请方建立审核方案（申请方变更为受审核方），并由专职人员负责管理审核方案。审核方案范围与程度的确定应基于受审核方的规模和性质，以及受审核服务和服务管理的性质、功能、复杂程度以及成熟度。

中心应建立审核人日确定准则，根据申请方的规模、特性、业务复杂程度、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。确定的人日数记录在审核方案记录中。

审核方案应包括在规定的期限内有效和高效地组织和实施审核所需的信息和资源，应包括以下内容：

1) 审核的范围与程度、数量、类型、持续时间、地点、日程安排；

2) 审核准则；

3) 审核方式；

依据企业提供的信息和认证资信，由项目管理人员决定采取具体的审核方式实施审核，目前可选择的审核方式如表 1 。

表 1. 审核方式分类表：

审核方式	一级	二级	三级	备注
非现场审核	√	√	√	
现场审核	√	√	√	
现场见证	√	√	√	仅适用于安全运维、工控安全
注： 1、三级初次认证宜采取非现场审核，获证后6个月内实施现场监督审核； 2、一、二级初次认证宜采取非现场审核与现场审核相结合；必要时，实施现场见证； 3、监督审核依据获证方的自评价，先实施非现场审核，必要时实施现场审核和（或）现场见证。				

4) 审核组的选择（审核组成员应具有相对应的服务审核方向）；

5) 所需的资源，包括交通和食宿；

6) 处理保密性、信息安全、健康和安全，以及其它类似事宜。

6.1.4 确定审核组

中心应根据受审核方的行业、规模和业务复杂程度和审核方案组建审核组，指派审核组长。审核组组建原则见第4章。

6.1.5 非现场审核

依据项目管理人员的安排，审核组对申请方实施非现场审核。非现场审核时，审核组通过对受审核方提交的自评价信息进行评审，获取需要的信息，对于无法从自评价信息中获取的信息，审核组通过远程审核工具进行信息获取，以确保完成非现场审核。

6.1.5.1 非现场审核计划

审核组长应结合受审核方的申请书/自评价信息、审核方案对非现场审核的策划做出具体安排，包括但不限于具体的时间安排、审核组成员对受审核方按岗位、活动和评价方式的安排。审核组长应至少在实施审核前与受审核方就审核计划进行充分沟通，确保双方在理解上没有歧义。

6.1.5.2 实施非现场审核

审核组长依据认证依据和审核要求，对申请方递交的资料进行审核，必要时辅以电话、视频、邮件等远程审核，并出具非现场审核报告。

非现场审核应对以下几个方面进行关注：

1） 受审核方的人员管理情况；

2） 受审核方的工具管理情况；

3） 受审核方的保密管理情况；

4） 受审核方的组织管理情况；

5） 受审核方的服务项目管理情况；

6） 受审核方对服务过程中资源的管理情况；

7） 受审核方对服务过程中风险（包括安全风险）的管理情况；

8） 受审核方已完成的项目及验收的结果；

9) 是否进行现场审核；

10) 现场审核时是否进行现场见证；

11）其他审核组员认为需要关注的方面等。

6.1.5.3 非现场审核结论

审核组应该对非现场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。

如果非现场审核发现不符合项和观察项应开具不符合项报告和观察项，且获得受审核方认同。

非现场审核结束，审核组可以根据非现场审核的结果对受审核方的服务是否满足所有适用的认证依据的要求进行评价，并判断是否需要：

a)进行现场审核、

b)服务项目现场见证，

c)推荐认证注册等。

非现场审核结束后，审核组长完成审核报告。如果非现场审核结束后，审核组认为有必要进行现场审核，需在审核报告中进行说明，并向项目管理人员提出申请，由项目管理人员进行分析后确定。

6.1.6 现场审核

依据项目管理的安排，审核组对申请方实施现场审核。

6.1.6.1 现场审核计划

审核组应结合受审核方的申请书/自评价信息、非现场审核发现、审核方案对现场审核的策划对现场审核做出具体安排，包括但不限于具体的时间安排、审核组成员对受审核方按岗位、活动和评价方式进行证据收集、人员沟通和会议安排。审核组长应至少在实施现场审核5个工作日之前，与受审核方就审核计划进行充分沟通，确保双方在理解上没有歧义。

必要时，在制定现场审核计划时应考虑对受审核方执行服务项目的现场见证。

6.1.6.2 现场审核实施

审核组长依据认证依据和审核要求，到受审核方现场进行审核，并出具现场审核报告。

现场审核应对以下几个方面进行关注：

1) 受审核方的现场环境、实验环境；

2) 受审核方的资源管理情况；

3) 受审核方的文档管理情况；

4) 受审核方的服务管理情况；

5) 受审核方的服务项目管理过程；

6） 受审核方已完成的项目及验收证明；

7） 审核组认为非现场审核发现需要关注的方面；

审核组通过现场审核，应实现以下目的：

1） 确定受审核方有能力策划并实施合同约定的服务项目；

2） 确定受审核方有能力确保所有的服务项目都按照既定的要求执行；

3） 确定受审核方的项目管理和执行过程满足认证依据的通用评价要求和专业评价要求。

6.1.6.3 现场审核结论

审核组应该对非现场审核和现场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。

如果现场审核发现不符合项和观察项应开具不符合项报告和观察项，且获得受审核方认同。

现场审核结束，审核组可以根据非现场审核结果和现场审核的结果对受审核方的服务是否满足所有适用的认证依据的要求进行评价，并判断是否需要增加非现场审核、是否推荐认证注册。

现场审核结束后，3个工作日内，审核组长完成审核报告。

6.1.7 现场见证（必要时）

依据项目管理的安排，审核组对受审核方实施现场见证。

6.1.7.1 现场见证计划

审核组应结合受审核方的申请书/自评价信息、审核方案对现场见证做出具体安排，包括但不限于具体的时间安排、审核组成员、具体的见证客户及见证内容。审核组长在制定见证计划前，与受审核方就时间安排进行充分沟通，确保双方达成一致。

同时，尽量与现场审核的时间安排保持一致。

6.1.7.2 现场见证实施

必要时，对申请认证的组织，审核组长/或组员依据认证依据和审核要求，对受审核方正在实施的服务项目现场进行见证，并出具现场见证报告。

现场见证应对以下几个方面进行关注：

1） 受审核方服务现场的安全管理情况；

2） 受审核方的现场服务过程的规范性；

3） 服务人员的技术能力；

4） 服务人员对工具的规范操作能力；

5） 受审核方服务技术要求的满足程度。

6.1.8 认证决定

审核完成后，项目管理人员应指派认证决定人员，对受审核方的认证申请实施认证决定，以决定：

a) 同意认证注册，颁发认证证书；或不同意认证注册。

b) 并给出下次监督审核方式的建议。

注1：参加审核的人员不能作为认证决定人员实施认证决定。

注2：受审核方获得认证注册资格后变更为获证组织。

6.1.9 证书颁发

对于符合认证要求的获证组织，颁发认证证书。

6.2 监督审核

6.2.1 频次和方式

对获证组织实施监督审核，每年度（不超过12个月）进行一次监督审核。对于三级获证组织，需要在半年内进行初次监督审核，第二次监督审核在获证后的第12个月进行。

对于信誉良好的获证组织，信任度级别高，可以根据实际情况延长监督的频次和灵活运用监督的方式。

当获证组织发生重大变更、事故、信任度级别低以下或客户投诉时，可增加现场监督评估的频次。

监督的方式包括非现场监督审核和现场监督审核两种方式。

6.2.2 信息收集

在进行监督审核之前，中心需要收集获证组织的安全服务管理与安全服务能力的相关信息，以确定获证组织的安全服务管理与安全服务能力相关信息是否发生变化。需要客户提供的信息包括以下几个方面：

1) 信息确认文件，包括但不限于：

a. 基本信息，包括组织名称、地址、联系人、法人等信息的变化情况；

b. 组织信息：包括范围、组织架构、人员数量等信息的变化情况；

c. 服务管理体系相关信息，关键文件化信息的变化情况。

2) 自评价信息：包括但不限于：

a. 安全服务管理运行情况，包括运行说明和运行证据；

b. 安全服务管理监视、测量、分析和评价的结果和证据；

c. 安全服务管理运行的持续改进情况，包括改进说明和证据；

d. 满足法律法规的情况说明；

e. 对安全服务管理符合性的自我评价。

6.2.3 信息评审与审核方案维护

项目管理人员对收集的信息的完整性进行评审，必要时，对审核方案进行维护。

6.2.4 制定审核计划

审核组应结合获证组织的信息确认文件、自评价信息、审核方案对监督审核的策划和前一次审核的结果对现场审核做出具体安排，包括但不限于具体的时间安排、审核组成员对获证组织按岗位和活动以何种方式进行评价的安排、高层沟通的安排、现场见证和会议的安排。审核组长应至少在实施审核3个工作日之前，与获证组织就审核计划进行充分沟通，确保双方没有歧义。

监督审核并不覆盖认证依据所有条款，监督审核的抽样采取抽样的方式进行， 抽样准则为：

1) 两次监督审核必须覆盖标准所有条款和所有部门；

2) 标准中对服务管理过程有决定作用的条款和部门每次监督审核都需要抽到；

3) 获证组织前一次审核问题较多的条款在本次监督审核中需要抽到；

4) 审核组认为重要的条款应考虑进行抽样。

每次监督审核的内容应包括对以下方面：

1) 非现场审核；

2) 对上次审核中确定的不符合采取的措施；

3) 投诉的处理；

4) 安全服务管理与安全服务能力在实现获证客户目标的有效性；

5) 为持续改进而策划的活动的进展；

6) 持续的运作控制；

7) 任何变更；

8) 标志的使用和（或）任何其他对认证资格的引用。

6.2.5 审核实施

审核组按照审核计划的安排对获证组织进行审核，由于监督审核并不要求覆盖安全服务管理和安全服务能力的所有方面，在监督审核的策划过程中，如果获证组织的认证范围信息有变化，应对变化的方面进行关注，必要时重新确认审核范围。

监督审核原则上采取非现场审核的方式进行，非现场审核结束后，审核组根据审核结果确定是否需要进行现场审核和（或）现场见证，如果需要，审核组需向项目管理人员进行申请，项目管理人员根据获证组织的相关信息确定是否进行现场审核和（或）现场见证并进行相关活动的安排。

6.2.6 监督审核结论

审核组应该对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。

如果审核发现不符合项和观察项应开具不符合项报告，且获得获证组织认同。

审核结束，审核组应形成是否推荐保持认证注册的结论；。

审核结束后3个工作日内审核组长完成审核报告。

6.2.7 认证决定

中心应指派认证决定人员，对获证组织的认证申请实施认证决定，以决定：

1) 同意保持认证注册，颁发认证标志；

2) 补充认证决定所需的信息，包括但不限于申请材料、审核材料，再进行认证决定；

3) 不同意保持认证注册，做出暂停或撤销的决定，通知获证组织不同意保持的理由。

认证决定人员实施认证决定时应以认证过程中收集的信息和其他相关信息为基础，以充分的证据证实获证组织符合服务资质规范的要求。

6.2.8 审核方案记录与变更

审核方案管理人员应收集特殊审核的信息，特别是形成的结论和变化的信息，记录到审核方案中，并确定审核方案是否需要进行变更，如需要则更新相应项目内容。

6. 3 特殊审核

6.3.1 变更或扩大认证范围

获证组织申请级别变更时，中心应按初次认证的过程对获证组织进行特殊审核，最终形成是否同意级别变更的决定。级别变更的审核活动可单独进行，也可和对获证组织的监督审核一起进行。

中心为调查投诉、对变更做出回应或对被暂停认证资格的获证组织进行追踪时，应指派审核组在提前较短时间通知获证组织后对其进行特殊审核。特殊审核以现场审核方式进行，此时：

1) 应向获证组织说明并使其提前了解将在何种条件下进行此类审核；

2) 给予获证组织对审核组成员的任命表示反对的机会，中心应在指派审核组时给予更多的关注；

3) 审核组应制订审核计划，形成审核结论；

4) 中心应根据审核结论作出认证决定。

6.3.2 审核方案记录与变更

审核方案管理人员应收集特殊审核的信息，特别是形成的结论和变化的信息，记录到审核方案中，并确定审核方案是否需要进行变更，如需要则更新相应项目内容。

7 信息通报

为确保获证组织的安全服务能力持续有效，获证组织应建立信息通报规范，及时向认证机构报告以下信息：

1) 组织机构变更信息；

2) 安全事故、客户投诉信息；

3) 其他重要信息。

8 认证证书管理

8.1 证书内容

认证证书内容应分别以中、英文书写，至少包括以下方面：

a) 认证证书名称，例如：信息安全服务资质认证证书；

b) 获证组织名称、注册地址、审核地址；

c) 符合本规则第 2 章的认证依据；

d) 通过认证的服务类别；

e) 首次颁证日期、换证日期以及证书有效期的起止年月日；

f) 中心的名称及其标志；

g) 中心的印章和法定代表人代表或其授权人的签字；

h) 认可标识及认可注册号(应为国家认监委确定的认可机构的标识，以申请认可为目的发出的证书可没有此内容)。

8.2 证书编号

a) 证书编号规则由中心进行明确规定。

b) 有效期内换发证书，认证证书编号中的机构注册号、年份号、顺序号和认证的有效期保持不变，应注明换证日期。

c) 撤销证书后，原认证证书编号废止，不再它用。

d） 认证证书上的中心名称应与相应的中心批准书上的名称一致。

8.3 证书有效期

获证组织应通过年度监督审核，保持证书有效，证书每年更新一次。

8.4 暂停认证证书

获证组织有下列情形之一，认证机构应暂停其认证证书：

a） 获证组织的服务管理持续地或严重地不满足认证要求，

b） 逾期未按规定接受监督审核；

c） 违规使用认证证书，且未造成不良影响；

d） 监督审核有严重不符合项；

e） 获证组织主动请求暂停；

f） 其他需要暂停证书的情况。

在暂停认证期间，获证组织的服务资质认证证书暂时无效。中心应做出具有强制实施力的安排，避免暂停认证期间获证组织继续宣传并使用服务资质认证证书。中心应使认证证书的暂停信息可公开获取。

证书暂停时间一般不超过六个月。在证书暂停期间，组织可提出恢复证书的申请，并经认证机构审核、批准后方可使用证书。

在任何组织提出请求时，中心应正确说明获证组织的服务资质认证被暂停的情况。

8.5 撤销认证证书

获证组织有下列情形之一，应撤销其认证证书：

a） 逾期6个月未按规定接受监督审核的；

b） 证书暂停期间，未在规定时间内完成整改并通过验证；

c） 违规使用认证证书，造成不良影响；

d） 获证组织出现严重责任事故、被投诉且经核实，影响其继续有效提供服务；

e） 获证组织因自身原因不再维持证书，可提出撤销认证证书的申请；

f） 其他需要撤销证书的情况。

认证证书撤销后，获证组织应交回认证证书，中心予以公示。

8.6 证书变更

证书变更如只涉及地址、资金或法定代表人的变更，获证组织需递交变更申请，经书面审核批准后，中心可更换其证书并收回原证书。

如获证组织发生除以上的重大调整，应向中心提出变更申请，并提供相关材料。中心组织审核组需进行现场审核，并做出认证决定。