信息安全服务资质认证实施规则

CCRC-ISV-R01:2021

2021-10-15 发布 **2021-10-15 实施**

中国网络安全审查技术与认证中心

目 录

1 适用范围

本规则用于规范中国网络安全审查技术与认证中心（简称中心）开展信息安全服务认证活动。

2 认证依据

CCRC-ISV-C01《信息安全服务规范》

3 认证模式

初次认证+获证后监督

4 认证级别

信息安全服务认证级别分为一级、二级、三级，其中一级为最高级别。

5 认证基本环节

1) 认证申请及受理
2) 文件审核
3) 现场审核
4) 结果评价与决定
5) 获证后监督

6 认证程序

6.1 认证申请及受理

6.1.1 认证申请

初次认证（含增项、升降级等）申请，申请组织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) 申请组织基本信息，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(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）)；独立法人实体的一部分，经法人批准成立，法人实体能为申请人开展的活动承担相关的法律责任；
   c) 业务运行时间的证明材料；
   d) 取得相关法规规定的行政许可文件(适用时)。
2) 自评估表，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

中心根据认证依据、程序等要求，对申请组织提交的认证申请书、自评估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) 所需要的基本信息及自评估信息都得到提供；
2) 申请组织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) 中心与申请组织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。

6.1.3 方案建立

在申请评审通过后，中心针对申请组织建立审核方案。审核方案应明确所涉及的文件审核、现场审核等各阶段的活动安排，并根据中心的人日计算标准确定审核人日。

6.2 初次认证

6.2.1 文件审核

文件审核应根据申请组织提交的申请材料及自评估表进行评审，确保满足认证依据的要求。

文件审核应确认申请组织是否针对所涉及的所有认证规范条款进行了自我评价并提供了充足的证据证明其满足认证规范的要求，内容包括但不限于：

1) 提供的基本信息，包括法律地位、财务、办公场所、人员能力、业绩等；
2) 服务管理制度文件的发布时间，确认是否满足运行时间；
3) 服务管理制度文件的内容是否满足认证规范的要求；
4) 服务管理制度文件的覆盖范围是否与申请的范围保持一致；
5) 提供的制度文件执行证据是否充分；
6) 提供的证据是否能够证明其技术能力。

6.2.2 现场审核

现场审核包含申请组织办公现场及其服务实施现场。一级和二级项目在文件审核通过后，实施现场审核。三级项目根据文件审核结论经中心复核后，必要时实施现场审核。

现场审核应根据文件审核的结果，对文件审核中查阅的证据材料进行现场验证，必要时重新抽样，现场审核内容包括但不限于：

1) 对客户的法律地位、财务资信、办公场所、人员能力等多个方面进行现场验证；

2) 对客户的服务管理执行情况进行现场验证；

3) 对客户的服务技术能力进行跟踪验证，包括已结束项目的和正在执行项目。验证方式包括但不限于：文件和记录查阅、人员访谈、现场核查等。

6.2.3 结果评价与决定

审核完成后，中心对审核结果及相关资料进行综合评价，做出认证决定，符合认证要求的颁发认证证书，不符合认证要求的认证终止。

6.3 获证后监督

6.3.1 频次和方式

自获证后12-18个月内至少进行1次监督审核。监督审核对象为获证组织。当获证组织持有多张证书时，应以最早的获证日期发起监督审核，其他证书合并审核。获证后监督活动可采取以下方式进行：

1) 文件审核；

2) 现场审核；

3) 其他监督获证组织的方法。

若获证组织在证书有效期内出现以下情况之一，中心应视情况增加监督频次：

1) 获证组织发生重大变更，例如组织架构、关键办公场所、服务管理过程等发生变更；

2) 针对获证组织的投诉；

3) 获证组织出现重大服务质量事故或风险隐患等。

必要情况下，中心可采取事先不通知的方式对获证组织进行飞行检查。

6.3.2 信息收集

获证组织应于监督审核前3个月，提交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。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) 自评估信息，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。

6.3.3 方案维护

中心结合获证组织的实际情况，对审核方案进行维护调整，包括：监督审核的频次和覆盖范围、监督审核方式、审核人日等，并确定相关活动的安排。应重点关注获证组织的多方向的服务实施现场，并结合实际情况，确保在一个认证周期内应覆盖全部的服务方向。

6.3.4 监督审核实施

认证周期内的监督审核应覆盖认证依据所有条款，监督审核采取抽样的方式进行，抽样准则为：

1) 一个认证周期内的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以下方面：

1) 对上次审核中确定的不符合及观察项采取的措施；
2) 投诉的处理；
3) 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；
4) 任何变更。

6.3.5 获证后监督结果的评价

监督审核完成后，中心对审核结果及相关资料进行综合评价。评价通过的，认证证书持续有效，评价不通过的，按照本规则第7章的暂停、注销及撤销的相关规定处理。

7 认证证书

7.1 证书内容

认证证书内容至少包括以下方面：

1) 认证证书名称，例如：信息安全服务资质认证证书；
2) 证书编号；
3) 获证组织名称、注册地址、办公地址；
4) 符合本规则第2章的认证依据；
5) 通过认证的服务类别；
6) 首次颁证日期、换证日期以及证书有效期的起止年月日；
7) 中心的名称及其标志；
8) 中心的印章和法定代表人代表或其授权人的签字；
9) 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)。

7.2 认证证书管理

7.2.1 认证证书的保持

本规则覆盖服务的认证证书有效期为 3 年。证书有效性通过获证后监督维持。

获证组织应在证书有效期届满前至少 3 个月提交换证申请。认证证书有效期内且最后一次监督审核结果合格的，换发新证书；获证组织在证书有效期届满时未提出换证申请的，其证书到期后失效。

7.2.2 认证证书的变更

获证组织证书内容变更时，应向中心提出变更申请，并按照要求提交相关材料。

1) 如果认证变更只涉及到获证组织名称、注册地址的变更，获证组织须递交变更申请及工商变更证明材料等，经认证决定后，中心换发新证书并收回原证书；
2) 如果获证组织受审核地址变更时，可与监督审核合并进行，审核通过后换发新证书并收回原证书。

7.2.3 认证证书的暂停

获证组织有下列情形之一，认证机构应暂停其认证证书：

1) 获证组织的服务管理持续地或严重地不满足认证要求；

2) 逾期未按规定进行监督审核；

3) 违规使用认证证书，且未造成不良影响；

4) 监督审核有严重不符合项；

5) 获证组织主动请求暂停；

6) 其他需要暂停证书的情况。

在暂停认证期间，获证组织的服务认证证书暂时无效，中心应使认证证书的暂停信息可公开获取。

证书暂停时间一般为3个月，最长不超过6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。

7.2.4 认证证书的注销

获证组织因自身原因申请注销认证证书，中心予以注销。认证证书注销后，中心予以公示。

7.2.5 认证证书的撤销

获证组织有下列情形之一，应撤销其认证证书：

1) 逾期6个月未按规定进行监督审核的；

2) 证书暂停期间，未在规定时间内完成整改并通过验证；

3) 违规使用认证证书，造成不良影响；

4) 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；

5) 其他需要撤销证书的情况。

认证证书撤销后，中心予以公示。