
文件编码：ISCCC-SV-001:2010

信息安全服务资质认证实施规则

2010-4-15 发布

2010-4-15 实施

中国信息安全认证中心

目 录

1.	适用范围	2
2.	认证标准	2
3.	认证模式	2
4.	认证的基本环节	2
5.	认证实施	3
5.1.	认证时限	3
5.2.	认证申请及受理	4
5.3.	文档审核	5
5.4.	现场审核	6
5.5.	认证决定	6
5.6.	证后监督	7
5.7.	再认证	8
5.8.	认证变更	8
6.	认证证书	9
6.1.	认证证书有效期	9
6.2.	认证证书的管理	9
7.	收费	10

1. 适用范围

信息安全服务资质认证是依据国家法律法规、国家标准、行业标准和技术规范，按照认证基本规范及认证规则，对提供信息安全服务提供方的安全服务资质进行评价的合格评定活动。中国信息安全认证中心根据《中华人民共和国认证认可条例》及相关规定制定本规则。

本规则适用于中国信息安全认证中心开展的信息安全服务资质认证工作，信息安全服务类别可包括信息安全应急处理、风险评估、灾难恢复、系统测评、安全运维、安全咨询、安全培训、安全审计、安全监理等多种。

本规则规定了实施信息安全服务资质认证管理与实施的基本要求。

2. 认证模式

现场检查+ 特定服务检查 + 获证后监督

3. 认证的基本环节

(1) 认证申请及受理

(2) 文档审核

(3) 现场审核

(4) 认证决定

(5) 获证后监督

(6) 再认证

4. 认证标准

信息安全服务资质认证所依据的标准包括相关国家标准、行业标准和认证技术规范，涵盖了对信息安全服务提供方的基本资格、基本能力、管理能力、技术能力等方面的要求。目前，信息安全服务资质认证采用的标

准主要分为两大类：

(1) 通用基础标准：

CNCA/CTS 0052-2007 《信息安全服务资质认证技术规范》

YD/T 1621-2007 《网络与信息安全服务资质评估准则》

(2) 特定评价标准：针对特定类型的信息安全服务的评价要求。

可作为认证评价的所依据或参考的标准包括相关国家或行业标准、技术规范及管理指南，如：

YD/T 1799-2008 《网络与信息安全应急处理服务资质评估方法》

GB/T 20984-2007 《信息安全技术 信息安全风险评估规范》

GB/Z 20985-2007 《信息技术 安全技术 信息安全事件管理指南》

GB/Z 20986-2007 《信息安全技术 信息安全事件分类分级指南》

GB/T 20988-2007 《信息安全技术 信息系统灾难恢复规范》

GB/T 22081-2008 《信息技术 安全技术 信息安全管理实用规则》

特定类型服务的资质认证要求可通过相关标准、规范或实施规则另行规定。

5. 认证实施

5.1. 认证时限

认证时限是指自申请被正式受理之日起至颁发认证证书时止所实际发生的时间，其中包括认证受理、文档审核、现场审核、认证决定以及证书颁发。

认证受理不超过2个工作日（因申请材料不齐全，补充材料时间不计算在内）。在认证受理提交后3个工作日内由项目管理人员安排审核组进行文

档审核，文档审核不超过5个工作日（因申请材料不满足标准要求，补充材料时间不计算在内）。文档审核完成后在10个工作日内进行现场审核（因申请方原因延误的时间不计算在内）。现场审核时间由认证机构根据申请方的申请级别和其所承担的风险等确定。一般情况下，申请某一类别的信息安全服务资质认证现场审核时间为2到4人日；同时申请两种以上（含两种）服务类别的资质认证，适当增加审核时间。现场审核报告在现场审核完成后10个工作日内由审核组长完成，并由被审核单位签字或盖章（对于存在不符合项报告的情况，整改要求在一个月之内完成，整改后由审核组确认纠正/预防措施的有效性）。现场审核报告完成后在5个工作日内进行认证决定，3个工作日内制作、颁发证书并予以公告。

信息安全服务提供方如果已获得信息安全服务资质认证，再申请其他类别的信息安全服务资质认证，认证周期可适当缩短。

5.2. 认证申请及受理

5.2.1 申请方按照要求自愿向认证机构提交信息安全服务资质认证申请。

申请方须满足以下基本条件：

- （1）应是一个独立的实体，具有独立法人资格；
- （2）应遵守国家现行法律、法规的规定；
- （3）应有一支稳定的信息安全服务团队；
- （4）应完成一定数量的信息安全服务项目，且通过验收；
- （5）应建立符合标准要求的质量管理与项目管理体系；
- （6）从事涉及国家秘密的服务提供方必须获得国家保密机关的资质认证；

- (7) 应与信息安全服务人员签订保密协议，并对服务人员进行保密教育；
- (8) 信息安全服务提供方应具备安全保密的工作环境，主要体现在：指派专人负责将信息安全服务的资料进行单独保管；准备独立且不联网的计算机以存放有保密要求的电子文档。

5.2.2 申请方应提交的文件

- (1) 信息安全服务资质认证申请书；
- (2) 独立法人资格证明材料；
- (3) 从事信息安全服务的相关资质证明；
- (4) 工作保密制度及相应组织监管体系已建立的证明材料；
- (5) 与信息安全服务人员签订的保密协议复印件；
- (6) 人员构成与素质证明材料；
- (7) 规模与资产证明材料；
- (8) 公司组织结构证明材料；
- (9) 具备固定办公场所的证明材料；
- (10) 项目管理制度文档；
- (11) 信息安全服务质量管理文件；
- (12) 项目案例及业绩证明材料；
- (13) 信息安全服务能力证明材料等。

5.3. 文档审核

认证机构应根据认证依据、程序等要求，及时对申请方提交的申请文件和资料进行审核并保存审核记录，以确保：

- (1) 认证要求规定明确、形成文件并得到理解；
- (2) 认证机构和申请方之间在理解上的差异得到解决；
- (3) 对于申请的认证范围、工作场所和任何特殊要求，认证机构均有能力开展认证服务。

文档审核内容包括：

- (1) 文件的符合性、适宜性和充分性；
- (2) 适用法律、法规的识别情况及在相关文件中落实的情况。

5.4. 现场审核

认证机构应组成审核组，依据相关标准和审核要求，对申请方进行现场审核。现场审核的内容主要包括：

- (1) 通过检查、观察、访谈，对申请方的信息安全服务技术能力进行验证；
- (2) 通过检查、观察、访谈，对申请方的信息安全服务管理能力进行验证；
- (3) 观察服务模拟演示或见证现场服务。

5.5. 认证决定

认证评价及认证决定是由认证决定委员会执行。认证决定委员会至少由3名以上（含3名）奇数认证决定人员组成。

5.5.1 认证决定

认证决定人员依据认证标准、信息安全服务资质认证程序与实施规则的要求及相关标准，结合审核过程中收集的信息（对于存在不符合项的情况，必须通过整改并由审核组验证通过），对审核结果进行综合评价，做出

“通过认证”或“不通过认证”的决定。必要时，认证机构应对申请方满足认证依据的情况进行风险评估，以做出是否授予认证的决定。

对于符合认证要求的申请方，认证机构应颁发认证证书并在相关媒体上予以公告。

对于不符合认证要求的申请方，认证机构应以书面的形式明示其不能获得认证的原因。

5.5.2 对认证决定的申诉

申请人如对认证决定结果有异议，可在10个工作日内向认证机构申诉，认证机构自收到申诉之日起，应在一个月内进行处理，并将处理结果书面通知申请方。

5.6. 证后监督

5.6.1 证后监督频次和方式

认证机构应根据信息安全服务的特点以及所承担的认证风险，合理确定监督审核的时间间隔和方式。一般情况下，每年度进行一次监督审核，由项目管理人员提前两个月通知获证方。监督审核的方式可采用文档审核或现场审核的方式。

当信息安全服务提供方的信息安全服务发生重大事故、客户投诉，或组织结构、人员等方面发生重大变更等时，认证机构视情况可增加现场监督审核的频次。

5.6.2 监督审核应包括，但不限于以下内容：

(1) 新实施的服务案例；

(2) 顾客投诉情况；

(3) 涉及变化的范围（例如：人员变化、实验环境变化、项目管理、质量管理体系变化）；

(4) 上次审核提出的不符合项所采取纠正/预防措施、观察项的实施情况。

5.6.3 监督结果评价

对于监督审核合格的信息安全服务提供方，认证机构应做出保持其认证资格的决定；否则，应暂停、撤销其认证资格。

5.6.4 信息通报制度

为确保信息安全服务提供方的信息安全服务能力持续有效，认证机构应要求服务提供方建立信息通报制度，及时向认证机构通报以下信息：

- (1) 有关组织机构变化信息；
- (2) 消费者投诉等信息；
- (3) 其他重要信息。

5.6.5 信息分析

认证机构应对上述信息进行分析，视情况采取相应措施，包括增加监督审核频次、暂停或撤销认证资格。

5.7. 再认证

在认证证书有效期满的前三个月内，服务提供方可申请再认证。再认证程序与初次认证程序相同。

5.8. 认证变更

- (1) 如果认证变更只涉及到注册地址、资金或法定代表人的变更，申请方须递交变更申请，经书面审核批准后，认证机构仅对证书更新并

收回原证书；

(2)信息安全服务提供方的组织机构发生重大调整、人员变动较大、拟变更业务范围时，应向认证机构提出变更申请，并提交相关材料。

认证机构策划并实施适宜的审核活动，并按照要求做出认证决定。

审核活动可单独进行，也可与信息安全服务监督或再认证同时进行。

6. 认证证书

6.1. 认证证书有效期

信息安全服务资质认证证书有效期为 3 年。

6.2. 认证证书的管理

6.2.1 暂停认证证书

信息安全服务提供方有下列情形之一的，认证机构应当暂停认证证书。

- (1) 未按照规定及时接受监督审核或申请再认证；
- (2) 信息安全服务提供方未按规定使用认证证书；
- (3) 监督结果证明信息安全服务提供方的信息安全服务能力不符合认证要求，但不需要立即撤销认证证书。

暂停期限一般为三个月。在三个月内，申请方可提出恢复证书的申请，认证机构经审核、批准后，方可使用该证书。在认证证书暂停期间，申请方不得继续使用证书。

6.2.2 撤销认证证书

信息安全服务提供方有下列情形之一，认证机构应当撤销其认证证书。

- (1) 监督结果证明信息安全服务提供方的信息安全服务能力不符合认证要求，应撤销证书的；

- (2) 认证证书暂停使用期间，信息安全服务提供方未采取有效纠正措施；
- (3) 信息安全服务提供方出现严重责任事故，影响其继续有效提供服务的；
- (4) 信息安全服务提供方不接受认证机构对其实施的监督审核或未申请再认证的。

6.2.3 注销认证证书

信息安全服务提供方因为自身原因申请注销认证证书，认证机构应当给予注销。

认证证书注销和撤销后，认证机构应收回认证证书，并在相关媒体上予以公告。

7. 收费

认证机构参考国家有关规定制定收费标准，如国家计委、国家质量技术监督局、计价格 [1999] 1610 号文等收费要求。