国家信息安全测评

信息安全服务资质申请与维持指南

（信息系统审计类一级）

CNITSEC

2025 年 5 月

目　录

引　言

中国信息安全测评中心（以下简称测评中心）是中央批准成立的国家信息安全权威测评机构，以“为信息技术安全性提供测评服务”为宗旨。

依据中央授权，测评中心的主要职能是：

1. 开展信息安全漏洞分析与风险评估；
2. 开展信息技术产品、系统和工程建设的安全性测试与评估；
3. 开展信息安全服务和信息安全专业人员的能力评估与资质审核；
4. 开展信息安全技术咨询、工程监理与开发服务；
5. 从事信息安全测试评估的理论研究、技术研发、标准研制；
6. 出版《中国信息安全》杂志等。

“信息安全服务资质认定”是对信息安全服务提供者的技术、资源、法律、管理等方面的资质、能力和稳定性、可靠性进行评估，依据公开的标准和程序，对其安全服务保障能力进行评定和确认。为我国信息安全服务行业的发展和政府主管部门的信息安全管理以及全社会选择信息安全服务提供一种独立、公正的评判依据。

欢迎关注国家信息安全服务资质官方微信号

一、 认定依据

信息安全服务（信息系统审计类）资质认定是对信息系统审计服务提供者的资格状况、技术实力和服务实施过程质量保证能力等方面的具体衡量和评价。

信息安全服务（信息系统审计类）资质级别的认定，是依据《信息安全服务资质评估准则》和对应级别的信息安全服务（信息系统审计类）资质具体要求，在对申请单位基本资格、技术实力、信息系统审计服务能力以及信息系统审计项目的组织管理水平等方面进行综合评定后，由测评中心给予相应的资质级别认定。

二、 级别划分

信息安全服务（信息系统审计类）资质认定是对信息系统审计服务提供者的综合实力的客观评价和确认，信息安全服务（信息系统审计类）资质级别反映了信息系统审计服务提供者从事信息系统审计服务保障能力的成熟程度。

信息安全服务资质依照国家标准 GB/T 20261-2020《信息安全技术 系统安全工程能力成熟度模型》的能力等级，设为五个级别，一级到五级能力递增，五级为最高级别。

一级：基本执行级

二级：计划跟踪级

三级：充分定义级

四级：量化控制级

五级：持续改进级

三、 一级资质要求

申请单位需要在基本资格和基本能力、信息系统审计服务过程能力和项目与组织过程能力等几个方面符合《信息安全服务资质具体要求（信息系统审计类一级）》的规定。

3.1 基本资格要求

申请信息安全服务（信息系统审计类一级）资质的单位必须是一个独立的实体，具有独立法人资格，遵守国家法律法规。

3.2 基本能力要求

3.2.1 组织与管理要求

申请单位应拥有健全的组织和管理体系，为持续的信息系统审计服务提供保障，并有利于提高审计活动的可信任度。应建立和确定对以下工作负责的最高管理层，最高管理层可以是委员会、小组或个人：

1. 制定信息系统审计单位运作的方针；
2. 信息系统审计服务和制度的开发；
3. 监督其方针和制度的实施；
4. 监督信息系统审计单位的财务；
5. 评价投诉解决的成效；
6. 批准审计报告；
7. 需要时，授权委员会或个人代表最高管理层开展规定的活动；
8. 为认证活动提供充分的，合格的资源等。

3.2.2 技术能力要求

申请单位应建设和储备相应的技术条件，以满足信息系统现场审计和非现场审计的需要：

1. 了解信息技术应用现状和发展趋势，以及新兴技术的发展和应用现状；
2. 具有较全面的信息系统控制相关领域的专业知识；
3. 具有不断的审计和信息系统等相关领域的技术更新能力；
4. 掌握影响信息系统安全性、有效性、可靠性等的风险因素，并具备相应的风险评估的能力；

5. 具备提出信息系统风险处置建议的能力；
6. 具备跟踪、了解、掌握、应用国际、国家和行业标准的能力。

3.2.3 人员构成与素质要求

申请单位应确保其人员具有与审计活动和被审计方业务领域相关的知识、技能和经验：

1. 有足够的人员从事直接与信息系统审计服务相关的活动，对直接参与审计活动的人员，具有至少 4 名注册信息系统审计师或注册信息安全专业人员；
2. 识别不同被审计业务领域的信息系统审计所需的人员资格和能力要求；
3. 识别单位内直接参与审计活动以外的岗位如管理、营销、质量保证等人员的知识和能力要求；
4. 识别培训要求，具有获取必要的技术知识和技能的渠道和制度安排，以确保其人员持续满足所需的资格和能力要求；
5. 应建立选择、培训、正式授权和监督信息系统审计师以及技术专家的制度，对信息系统审计师的初始能力评价，应包括现场见证审计师的活动；
6. 应确保信息系统审计师和技术专家熟悉审计活动、审计方法、审计工具和其它相关要求；
7. 应保存参与信息系统审计活动的工作人员的相关资格、培训、经历、社会关系、职业状态和能力的最新记录。

3.2.4 设备、设施与环境要求

申请单位应具有与其开展审计服务相适应的设备、设施与工作环境，包括：

1. 具有固定的工作场所，满足工作要求的适宜的工作环境；
2. 逐步建设和维护信息系统审计工具库，包括但不限于数据审计、代码审计、流量审计、日志审计、配置审计、常用技术控制措施审计、关键信息基础设施审计等工具；
3. 逐步建设信息系统审计实验环境，建设常见被审计信息系统的仿真模拟环境，培养使用工具开展审计的能力。

3.2.5 规模与资产要求

申请单位应具备满足业务运作和承担审计风险所需的财力：

1. 具备与其业务规模相适应的注册资本金和流动资金；
2. 应能证明已对审计活动引发的风险进行了评价并做出了安排（如商业保险或储备基金），安排能覆盖其因审计活动所产生的责任；
3. 应评价其财务状况和收入来源，并向申请单位证实来自商业、财务和其它方面的压力不会损害其公正性。
4. 有足够的人员从事直接与信息安全服务相关的活动。

3.2.6 业绩要求

申请单位应具有与其申请资质等级相适应的从业经历，主要包括：

1. 从业时间；
2. 信息系统审计项目数量和规模；
3. 联合审计项目参与程度；
4. 项目完成结果评价。

3.3 信息系统审计服务过程能力要求

信息系统审计服务过程能力是评价信息系统审计服务专业水平高低的标志。申请单位应能实施以下 7 个信息系统审计过程域：

1. 编制信息系统审计计划；
2. 启动信息系统审计；
3. 信息系统审计活动的准备；
4. 实施信息系统审计活动；
5. 编制和交付信息系统审计报告；
6. 结束信息系统审计活动；
7. 信息系统审计的后续活动。

3.4 项目和组织过程能力要求

项目和组织过程能力是评价信息系统审计服务规范性和质量保证成熟度标志。

申请单位应能实施以下 6 个项目和组织过程域：

1. 审计活动的质量保证；
2. 审计活动的风险管理；
3. 审计活动的监控；
4. 信息系统审计知识和技能的提升；
5. 信息系统审计机构原则；
6. 信息系统审计人员职业道德。

四、 申请准备

申请单位需要到测评中心网站（https://www.itsec.gov.cn）查看并下载《信息安全服务资质评估准则》《信息安全服务资质申请与维持指南（信息系统审计类一级）》和《信息安全服务资质申请书（信息系统审计类一级）》及有关附件，认真阅读上述文档，了解资质认定的流程及相关情况，确定本单位满足一级资质的基本资格和基本能力要求。

申请单位根据《信息安全服务资质申请书（信息系统审计类一级）》的要求填写申请书、加盖公章并装订后，将申请书及所要求的相关资料刻光盘，将纸版、电子版资料一起以快递方式提交给测评中心。在正式递交前，申请单位须逐项检查所填报的材料的完整性和正确性。

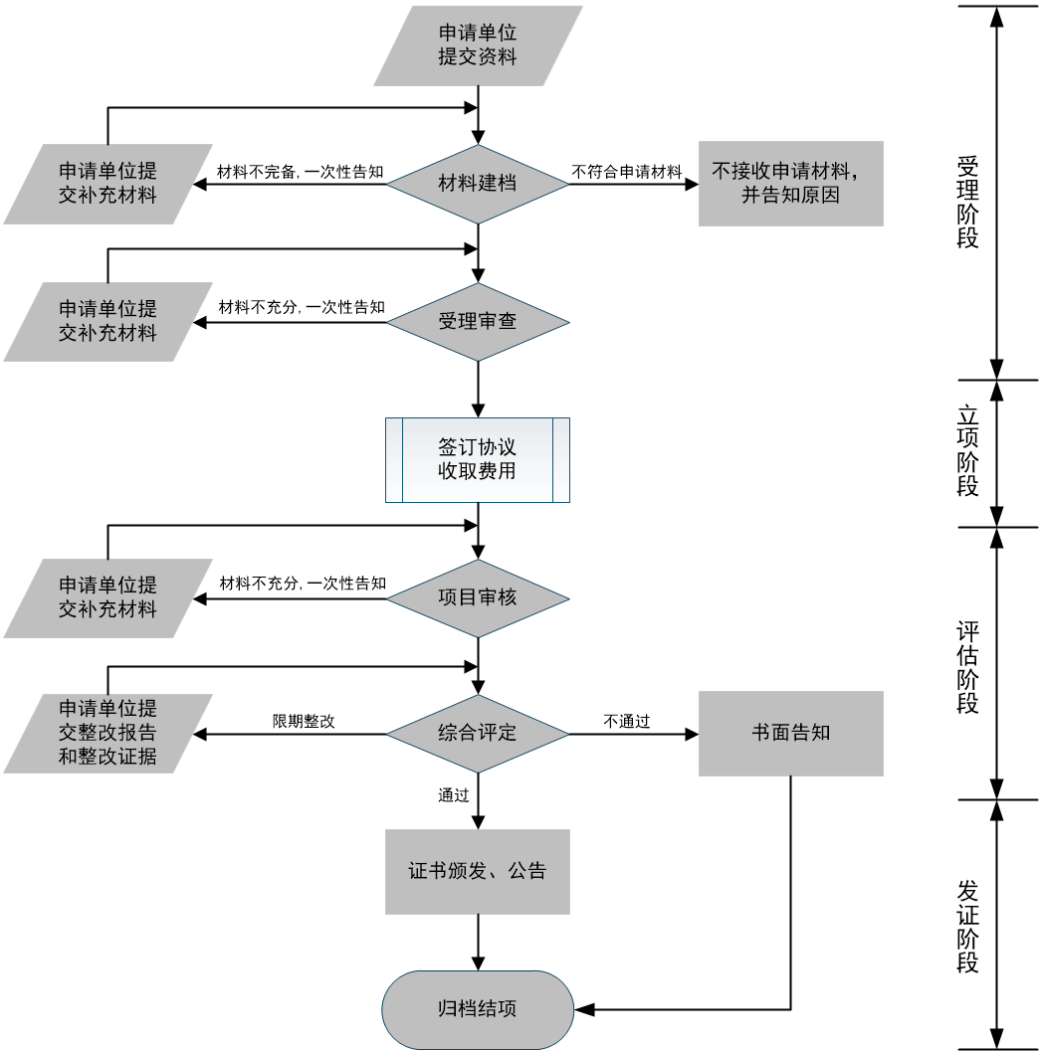
如申请单位已获得该类别服务资质证书，至少需要在证书有效期届满前六个月，提交该类型资质维持原有级别的申请，以确保资质有效。证书有效期届满六个月后提交维持申请，视作初次申请。维持申请需要提交近三年的资料信息。维持申请流程与首次申请流程一致。

申请单位可在测评中心网站或“国家信息安全服务资质”公众号上阅读《信息安全服务资质申请常见问题解答》了解更多信息。

联系方式详见第十章。

五、 资质认定

5.1 项目实施流程图



5.2 受理阶段

申请单位资料建档立项应满足以下三个条件：（一）申请单位必须是一个独立的实体，具有独立法人资格；（二）申请书加盖申请单位公章且装订成册；（三）随附电子版资料。

项目负责人对申请资料的形式规范度、申请单位的基本资格、基本能力、专项技术过程能力和组织管理能力进行受理审查，判定证据的充分性，并以电子邮件形式反馈受理审查意见，申请单位需在收到邮件后一个月内提交补充资料。

5.3 立项阶段

项目负责人按照测评中心合同管理要求起草制式委托协议，依据收费标准确定委托测评费用，电子邮箱发送协议及附件模板至申请单位指定电子邮箱，邮件中说明协议和附件的准备要求。

委托协议生效，且申请单位支付委托测评费用后，项目进入评估阶段。

5.4 评估阶段

项目组与申请单位充分沟通，确保可获得执行评估必须的所有信息和（或）文件，拟定审核计划，进行评估准备。

项目组按照审核计划，开展评估活动。评估方式包括但不限于文档审查、人员访谈、实际操作等。

a) 文档审查。通过审查申请单位相关管理机制，核验执行信息系统审计服务过程产生的工作产品，例如：所有记录、报告、数据、制品等，掌握信息系统审计服务活动的执行情况；

b) 人员访谈。通过访谈的方式与申请单位进行交流和讨论，获取信息系统审计服务有关活动信息，掌握具体执行过程；

c) 实际操作。通过演示和操作信息系统审计服务活动所必须的工具、平台及测试环境等，掌握申请单位的技术管理执行效率。

项目组根据采集的证据，进行申请单位信息系统审计服务能力符合程度的评估，并给出项目审核结论。

专家组对该项目证据的充分性，审核结论的合理性，进行综合评定，形成专家评审结论。评审结论为通过的项目进入发证阶段。

5.5 发证阶段

制证工作人员依照测评中心证书发放及公告的审批流程，按批次制作证书并及时发放，申请单位获证信息在测评中心网站、《中国信息安全》杂志、“国家信息安全服务资质”公众号上予以公告。

六、 处置

申请单位存在违规行为时，测评中心有权视申请单位违规情节轻重予以以下处置：警告、限期整改、暂停证书、取消证书。

七、 争议、投诉与申诉

申请单位对测评中心所作评审结论有异议时，可向测评中心提出书面申诉。测评中心监督部门负责进行调查，并给出调查结论。

申请单位应妥善处理因自身行为而发生的投诉，保留记录并采取措施防止问题的再发生。测评中心监督部门将在必要时查阅申请单位的投诉或申诉记录。

八、 申请单位档案

申请单位的项目档案归档保存六年。

九、 费用及周期

1. 首次获得一级资质证书费用：

   21000（审核费用）+15000（三年年金）＝36000 元

2. 维持一级资质证书费用：

   21000（审核费用）+15000（三年年金）＝36000 元

3. 项目实施周期原则上为三个月，最长不超过六个月。周期时间不包含申请单位补充资料、协议审批生效及支付费用等时间。

十、 联系方式

名　称：中国信息安全测评中心 资质评估处

地　址：中国北京市海淀区上地西路 8 号院 1 号楼（邮编：100085）

咨询电话：010－82341582 或 82341551

测评中心网站：https://www.itsec.gov.cn

服务资质公众号：国家信息安全服务资质

欢迎关注国家信息安全服务资质官方微信号