



计算机信息系统安全服务机构等级 认证实施规则

控制状态： 受控有效

编 制： 李丽娟

审 核： 成玲范

批 准： 

文件编号： WAL-RZGZ-001

版本号： 2.0

网安联认证中心有限公司

发布时间：2021年02月16日

更新时间：2025年06月12日

实施时间：2021年03月16日

目 录

1	适用范围	4
2	认证依据	4
3	认证模式	4
4	认证级别	4
5	认证单元划分	4
6	审查人员基本要求	4
7	初次认证程序	4
7.1	认证申请	4
7.2	认证申请评审	5
7.3	认证合同签订	5
7.4	审核策划	5
7.5	初次认证审核	6
7.6	现场审核活动实施	6
7.7	审核报告	7
7.8	复核	7
7.9	认证决定	7
8	监督审核程序	8
9	再认证程序	9
10	特殊审核	9
10.1	扩大、缩小认证范围审核	9
10.2	提前较短时间通知的审核	9
11	认证证书和认证标识要求	9
11.1	认证证书内容	9
11.2	认证证书管理	10
11.3	认证标志	11
12	认证记录管理	11
13	保密	12
14	申诉/投诉、争议及处理	12
15	费用	12
16	公告	12
17	其他	12

1 适用范围

本规则用于规范网安联认证中心有限公司（以下简称“网安联”）依据DB44/T1920-2016《计算机信息系统安全服务机构等级评定规范》在中国境内开展的服务认证活动。

2 认证依据

DB44/T 1920-2016《计算机信息系统安全服务机构等级评定规范》为认证依据。

3 认证模式

文件审核+现场审核+获证后监督

4 认证级别

计算机信息系统安全服务机构等级认证级别分为一级、二级、三级、四级，其中一级为最高级别。

5 认证单元划分

不同的网络安全服务提供者、网络安全服务类别应划分为不同的认证单元。

采用不同工程原理和方法来构建和维护安全的网络安全服务类别应划分为不同的认证单元。

6 审查人员基本要求

认证人员应当取得中国认证认可协会的服务认证审查员注册资格，并得到网安联内部能力评价，确定能够胜任审核的人员；应当遵守与从业相关的法律法规，对认证审核活动及相关认证审核记录和认证审核报告的真实性承担相应的法律责任。

7 初次认证程序

7.1 认证申请

7.1.1 网安联将向申请组织至少公开以下信息：

- (1) 可开展认证业务的范围，以及获得认可的情况；
- (2) 本规则的完整内容；
- (3) 认证证书样式；
- (4) 对认证过程的申诉规定；
- (5) 收费标准。

7.1.2 初次认证申请，申请组织至少提供以下必要的资料：

- (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)，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。
- (3) 申请组织应满足以下条件：
 - a) 具有中华人民共和国境内注册的独立法人资格。如果申请组织是独立法人组织的一部分，无独立法人资格，则应提供独立法人组织的授权证明；

- b) 近三年内，未发生网络安全事故或被执法监管部门责令停业整顿或在全国企业信用信息公示系统中被列入“严重违法企业名单”或违反国家相关法规。

7.1.3 网安联对申请组织提交的申请资料进行评审，根据申请认证的范围、级别及场所、完成审核所需时间和其他影响认证活动的因素，综合确定是否有能力受理认证申请。

7.1.4 对被执法监管部门责令停业整顿或在全国企业信用信息公示系统中被列入“严重违法企业名单”的申请组织，网安联不受理其认证申请。

7.1.5 对符合7.1.2、7.1.3要求的，网安联可决定受理认证申请；对不符合上述要求的，网安联认证中心将通知申请组织补充和完善，或者不受理认证申请。

7.2 认证申请评审

网安联应根据认证依据、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) 认证过程所需要的基本信息及自评信息都得到提供；
- (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) 网安联与申请组织之间任何已知的理解上的分歧已得到解决；
- (5) 网安联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。

通过评审的申请组织，网安联向其出具受理通知书。

7.3 认证合同签订

凡网安联确认受理认证申请的机构均应与网安联签订服务认证合同，确定认证费用、双方责任和义务等内容。如申请机构对合同内容及认证费用无异议，应在网安联实施现场核查前完成认证合同的签订工作。合同书有效期为三年，如果认证范围没有变更，年度监督认证审核不再另签合同书

7.4 审核策划

7.4.1 建立审核方案

在申请评审后，网安联应针对申请方建立审核方案（申请方即为受审核方），并由专职人员负责管理审核方案。审核方案范围内容包括但不限于：申请方名称、审核地址、审核准则、审核依据、审核范围、审核类别、审核人天数等，网安联根据《服务认证人日计算表》确定审核人日。

7.4.2 确定审核组

7.4.2.1 网安联根据服务覆盖的活动的专业技术领域选择具备相应能力的审核员组成审核组，必要时可以选择技术专家参加审核组。审核组中的审核员承担审核任务和责任。

7.4.2.2 技术专家主要负责提供认证审核的技术支持，不作为审核员实施审核，不计入审核时间，其在审核过程中的活动由审核组中的审核员承担责任。

7.4.2.3 审核组可以有实习审核员，其要在审核员的指导下参与审核，不计入审核时间，不单独出具记录等审核文件，其在审核过程中的活动由审核组中的审核员承担责任。

7.4.3 审核时间

网安联根据《服务认证人日计算表》确定审核人天数。

7.4.4 审核计划

- 7.4.4.1 网安联为每次审核制定书面的审核计划（第一阶段审核不要求正式的审核计划）。审核计划至少包括以下内容：审核目的，审核准则，审核范围、级别，现场审核的日期和场所，审核组成员（包括姓名、组内职务、注册级别、通信方式、CCAA注册号等）。
- 7.4.4.2 在审核活动开始前，审核组将审核计划交申请组织确认，遇特殊情况临时变更计划时，应及时将变更情况通知申请组织，并协商一致。

7.5 初次认证审核

初次认证审核，分为第一阶段和第二阶段实施审核。

7.5.1 第一阶段审核为文件审核，申请机构根据评定要求先确定需要申请的等级，提交符合相应等级要求的材料，提交的证明材料应包含但不限于：

- (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。

7.5.2 第二阶段审核为现场审核，审核组应将第一阶段审核情况形成书面文件告知申请组织，对文件审核不合格的申请组织，按规定的时间并提交纠正和纠正措施，经审核组确认有效方可进行第二阶段现场审核。

7.5.3 第二阶段审核需在申请组织现场进行，包含申请组织所有办公现场及其服务实施现场（必要时）。在文件审核通过后，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) 对受审核方的法律地位、财务资信、办公场所、人员能力等多个方面进行现场验证；
- (2) 对受审核方的服务管理执行情况进行现场验证；
- (3) 对受审核方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（必要时）等。

7.5.4 不符合项的纠正和纠正措施及其结果的验证。

对审核中发现的不符合项，网安联要求申请组织分析原因，按规定的时间并提交纠正和纠正措施。由审核组对纠正和纠正措施及其结果的有效性进行验证。如果未能在规定期限内对整改完毕，网安联将不予以认证通过决定。

7.5.5 发生以下情况时，审核组应向网安联副总经理报告，经同意后终止审核。

- (1) 受审核方对审核活动不予配合，审核活动无法进行；
- (2) 受审核方实际情况与申请材料有重大不一致；
- (3) 其他导致审核程序无法完成的情况。

7.6 现场审核活动实施

现场审核包含受审核方所有认证范围内办公现场及其服务实施现场（必要时）。现场审核活动包括：

- (1) 召开首次会议。审核组长主持召开首次会议。审核组与受审核方相关负责人及成员确认现场审核目的、范围和准则，确认现场审核日程计划安排，确认审查方法和程序，确认审查期间沟通渠道、资源、设施，明确公正性、保密性承诺及申诉、投诉渠道。
- (2) 现场评价。审核组按照审核计划中日程安排实施审查，通过查阅受审核方的文件和记录、与过程和活动相关岗位人员面谈、座谈，观察活动、测评系统等适当方法，抽样收集并验证有关的信息，形成审核发现，确认不符合情况。

- (3) 得出总体审核结论。审核组对审核过程中收集的信息和证据进行汇总分析，就审核结果达成一致，做出综合性的评价结果。并就审核情况、结论与受审核方的管理层进行沟通，就审核结论、不符合事实与受审核方取得共识。
- (4) 召开末次会议。审核组长主持召开末次会议，向受审核方相关负责人及成员汇报审核报告、不符合项及建议报告，并就结果与受审核方达成一致

7.7 审核报告

7.7.1 审核组应对审核活动形成书面审核报告，由审核组组长签字。审核报告应准确、简明和清晰地描述审核活动的主要内容，至少包括以下内容：

- (1) 申请组织的名称和地址；
- (2) 申请组织认证范围、级别；
- (3) 审核的类型、准则和目的；
- (4) 审核组组长、审核组成员及其个人注册信息；
- (5) 审核活动的实施日期和地点，包括固定现场和临时现场；对偏离审核计划情况的说明等；
- (6) 审核发现和审核结论；
- (7) 识别出的不符合项；
- (8) 审核组对是否通过认证的意见建议。

7.7.2 网安联会保留用于证实审核报告中相关信息的证据。

7.7.3 网安联会在作出认证决定后10个工作日内将审核报告提交申请组织。

7.7.4 对终止审核的项目，审核组应将已开展的工作情况形成报告，网安联应将此报告及终止审核的原因提交给申请组织，并保留签收或提交的证据。

7.8 复核

网安联对申请组织所有资料、审核报告、不符合项的纠正和纠正措施及其结果进行综合评审、复核后作出认证决定。

7.9 认证决定

7.9.1 由网安联指定的认证决定人员对申请组织所有资料、审核报告、不符合项的纠正和纠正措施、复核结果及其结果以及其他信息进行综合评价的基础上，作出认证决定。认证决定人员应为网安联管理控制下的人员，审核组成员不得参与对审核项目的认证决定。

7.9.2 网安联在作出最终的认证决定前，应确认如下情况：

- (1) 提交认证决定的材料是否齐全；
- (2) 认证申请评审记录是否考虑影响认证活动的所有因素；
- (3) 审核过程是否合规；
- (4) 审核人员的能力和资格是否胜任；
- (5) 本次审核是否达到审核目的、覆盖认证范围；
- (6) 审核计划编写是否目标明确、分工合理；
- (7) 首末次会议签到记录是否完整；
- (8) 审核发现是否表述清晰，若存在不符合是否进行分级；
- (9) 不符合项的纠正和纠正措施是否已被验证有效；
- (10) 审核报告是否客观反映了审核发现、内容完整、结论明确；
- (11) 客户信息是否完整、清晰、正确表述；
- (12) 若机构转换情况，申请组织转机构资料是否齐全（包括最近一个认证周期的审核报告、不符合项报告等信息）。

7.9.3 在满足7.9.2条要求的基础上，网安联有充分的客观证据证明申请组织满足下列要求的，评定该申请组织符合认证要求，向其颁发认证证书。

- (1) 申请组织的服务活动符合标准要求且运行有效。
- (2) 认证范围覆盖的产品和服务符合相关法律法规要求。
- (3) 申请组织按照认证合同规定履行了相关义务。

7.9.4 申请组织不能满足上述要求或者存在以下情况的，评定该申请组织不符合认证要求，以书面形式告知申请组织并说明其未通过认证的原因。

- (1) 受审核方的服务活动有重大缺陷，不符合DB44/T 1920-2016《计算机信息系统安全服务机构等级评定规范》标准的要求；
- (2) 发现受审核方存在重大安全问题或有其他与服务质量相关严重违法违规行为。

7.9.5 网安联在颁发认证证书后，将在30个工作日内按照规定的要求将认证结果相关信息报送国家认监委。

8 监督审核程序

8.1 网安联将定期对获证组织进行监督审核，以确认获证组织的服务持续满足认证要求，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。

8.2 超过期限而未能实施监督审核的，应按11.2.3或11.2.6条处理。

8.3 获证企业的服务被国家监督抽查中被查出不合格时，自抽查部门发出通报起30日内，网安联认证中心应对该企业实施监督审核。

8.4 监督审核的审核组，应符合第6条款的要求。

8.5 监督审核时申请组织至少提供以下资料：

- (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；
 - d) 上次审核中确定的不符合所采取的措施和效果，以及观察项整改的效果。
- (2) 自评信息，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。

8.6 在监督审核中发现的不符合项，网安联要求获证组织分析原因，规定时限提供纠正和纠正措施有效性的证据，网安联认证中心将采用适宜的方式及时验证获证组织对不符合项进行处置的效果。若申请组织没有按时关闭不符合，将可能导致认证证书的暂停或撤销。

8.7 网安联认证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。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。

8.8 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。

8.9 监督审核的审核报告，应按8.5条列明的审核要求逐项描述或引用审核证据、审核发现和审核结论。

8.10 网安联认证中心根据监督审核报告及其他相关信息，作出继续保持或暂停、撤销认证证书的决定。

9 再认证程序

9.1 认证证书期满前三个月内，若获证组织申请继续持有认证证书，网安联认证中心应当实施再认证审核，并决定是否延续认证证书。

9.2 网安联认证中心应按第6条要求组成审核组。按照7.5条要求并结合历次监督审核情况，制定再认证审核计划交审核组实施。

9.3 对再认证审核中发现的不符合项，获证组织应在规定时限内（与初次认证相同）实施纠正与纠正措施，网安联认证中心将在原认证证书到期前完成对纠正与纠正措施的验证。

9.4 网安联认证中心按照7.9条要求作出再认证决定。获证组织继续满足认证要求并履行认证合同义务的，向其换发认证证书。

9.5 如果在当前认证证书的终止日期前完成了再认证活动并决定换发证书，新认证证书的终止日期可以基于当前认证证书的终止日期计算。新认证证书上的颁证日期应不早于再认证决定日期。

9.6 如果在当前认证证书终止日期前，网安联未能完成再认证审核或对不符合项实施的纠正和纠正措施未能进行验证，则不应予以再认证，也不应延长原认证证书的有效期。

9.7 在当前认证证书到期后，如果网安联认证中心能够在6个月内完成未尽的再认证活动，则可以恢复认证，否则应至少进行一次第二阶段审核才能恢复认证。认证证书的生效日期应不早于再认证决定日期，终止日期应基于上一个认证周期计算。

10 特殊审核

10.1 扩大、缩小认证范围审核

10.1.1 针对已获证的客户，网安联对扩大、缩小认证范围的变更申请进行评审，确定能否予以扩大、缩小的决定所需的审核活动，这一工作可与监督审核同时进行。

10.2 提前较短时间通知的审核

10.2.1 为调查投诉、对变更做出回应或对被暂停的获证客户进行追踪，需要在提前较短时间通知获证客户后对其进行的审核。

10.2.2 获证客户的产品和服务被国家行政主管部门在监督抽查中被查出不合格时，网安联认证中心将对获证客户实施特殊审核。如获证客户不接受特殊审核，认证证书将被暂停。

11 认证证书和认证标识要求

11.1 认证证书内容

认证证书内容应至少包含以下信息：

- (1) 认证证书名称，即计算机信息系统安全服务机构等级认证证书；
- (2) 证书编号；

- (3) 获证组织名称、注册地址、认证地址；
- (4) 认证依据；
- (5) 通过认证的服务类别、级别；
- (6) 初始颁证日期、颁证日期以及证书有效期的起止年月日；
- (7) 网安联的名称及其标志。
- (8) 网安联的印章和法定代表人或其授权人的签字；
- (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)
- (10) 证书查询方式。

正式的认证证书应仅在下列事项完成之后颁发：

- (1) 批准或扩大认证范围的决定已经做出；
- (2) 认证合同规定内容已经完成。

11.2 认证证书管理

11.2.1 认证证书的保持

本方案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。

网安联保存获证组织的信息，至少包括：

- (1) 认证证书识别信息；
- (2) 证用的标准和其他规范性文件；
- (3) 获证组织识别信息。

11.2.2 认证证书的变更

获证组织证书内容变更时，应向网安联认证中提出变更申请，并按照规定提交相关材料。

- (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，网安联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。

11.2.3 认证证书的暂停

获证组织有下列情形之一，网安联应暂停其认证证书：

- (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且不能在规定期限内整改完成的；
- (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，网安联将证书信息报送国家认监委，并予以公示，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。若企业在3个月暂停期到期前，想延长暂停期，需向网安联认证中心申请并填写《延期认证证书暂停期申请书》，经网安联评定、批准后上报全国认证认可信息公共服务平台，暂停期最长不超过6个月。

11.2.4 认证证书的恢复

暂停证书时，网安联将向获证组织说明为结束暂停和恢复认证，获证组织所需采取的措施。

在证书暂停期间，获证组织可提出恢复证书的申请，经网安联审核、批准，并予以公告后，通知获证组织使用证书。认证证书的恢复可结合监督审核进行审核。

11.2.5 认证证书的注销

获证组织因自身原因申请注销认证证书，网安联应予以注销。认证证书注销后，网安联予以公示。

11.2.6 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3-6个月未按规定进行监督审核的(按企业暂停的时间做出撤销决定，暂停时间一般为3个月，最长不超过6个月)；
- (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) 他需要撤销证书的情况。

认证证书撤销后，网安联将证书信息报送国家认监委，并予以公示。

11.3 认证标志

11.3.1 认证标志样式



11.3.2 CNAS标识(与认证标志一起使用的示例)



11.3.3 认证证书和认证标志的使用

获证客户应建立认证证书和认证标志的使用方案，获证后按照《WAL-IP-21服务认证证书和认证标志认可标志使用规则》正确使用认证证书和认证标志。

11.3.4 认证证书和认证标志的误用

获证客户误用认证证书和认证标志，可能导致认证资格的暂停或撤销。误用认证证书和标志的类型及对误用认证证书和标志的处理见《WAL-IP-21服务认证证书和认证标志认可标志使用规则》中规定。获证客户一旦发现误用认证证书或认证标志，应立即采取纠正措施，并报告网安联认证中心审核管理部门。

11.4 网安联将采取有效措施避免各类无效的认证证书和认证标志被继续使用。

12 认证记录管理

12.1 网安有建立认证记录保持制度，记录认证活动全过程并妥善保存。

12.2 记录将真实准确以证实认证活动得到有效实施。记录资料使用中文，保存时间至少应当与认证证书有效期一致。

12.3 以电子文档方式保存记录的，采用不可编辑的电子文档格式。

12.4 所有具有相关人员签字的书面记录，可以制作成电子文档保存使用，保存时间至少应当与认证证书有效期一致。

13 保密

13.1 网安联承诺为申请组织/受审核方/获证组织保密（提前告知获证组织的需公开信息除外）。对申请组织/受审核方/获证组织的保密信息如需公开或向第三方提供时，网安联将拟提供的信息提前通知申请组织/受审核方/获证组织（法律限制除外）。

13.2 如有证据表明，网安联因认证接触申请组织/受审核方/获证组织的商业、技术秘密，而泄露给第三者（法律规定除外），承担相应法律责任。

14 申诉/投诉、争议及处理

对网安联有关人员违反国家认证法律、法规、认可机构有关规定、缺乏公正性及对认证的评价结果等有异议时，可以向网安联认证中心提出申诉、投诉。

网安联将在30日内答复处理情况。

对网安联申诉/投诉和争议的处理有异议时可向中国合格评定国家认可委员会、中国国家认证认可监督管理委员会等有关部门进一步申诉/投诉。

15 费用

实施本方案的费用，按文件《服务认证收费管理规则》执行。

16 公告

对获得认证、暂停、恢复或撤销的认证客户，在网安联公众号上公布。

17 其他

本规则内容提及DB44/T 1920-2016《计算机信息系统安全服务机构等级评定规范》时均指认证活动时该标准的有效版本。认证活动及认证证书中描述该标准号时，应采用当时有效版本的完整标准号。