文件编码：DSCC-SC-003

个人信息安全规范

认证规则

发布日期：2025 年 6 月 12 日

生效日期：2025 年 6 月 12 日

实施日期：2025 年 6 月 12 日

数据安全认证（贵州）有限公司

目　录

1 目的

为规范数据安全认证（贵州）有限公司（以下简称“本机构”）的个人信息安全规范认证工作，符合国家认证认可监督管理委员会规定的有关要求，保障认证工作的质量及符合性，特制定本规则。

2 适用范围

本规则适用于本机构开展个人信息安全规范认证工作，包含初次认证、认证保持和复审（再认证）所需的评价活动。

3 认证依据

GB／T 35273《信息安全技术 个人信息安全规范》。

4 认证模式

认证模式为：服务管理审核+服务能力确认或验证+获证后监督。

5 领域划分

单一领域:个人信息安全规范认证。

6 人员能力

6.1 审查组人员能力要求

1）具备国家承认的大学本科（含）以上学历，信息安全、密码学、计算机科学与技术、计算机应用、电子信息科学与技术、电子信息技术应用、人工智能、计算数学与应用数学、自动化、通信、电气等相关专业或从事个人信息保护领域相关工作三年以上；

2）熟悉 GB／T 35273《信息安全技术 个人信息安全规范》国家标准，具备相应的知识和技能；

3)具有人信息保护相应领域的专业知识和工作经验；

4)熟悉 GB／T 35273《信息安全技术 个人信息安全规范》认证依据标准；

5)熟悉人信息保护适用的有关法律、法规、技术标准及其他要求；

6)了解认证客户的业务/产品/过程/组织结构的相关知识；

7）具有 CCAA 注册的服务认证审查员资质；

8）审查组人员和观察员（适用时）需要符合 DSCC-QP14《认证工作人员管理及培训办法》的相关要求，并定期或不定期接受本机构对其能力的评估，达标才能从相关工作；

9）对同一申请组织的同一认证申请，不能连续 3 年以上（含 3 年）委派同一审查人员实施审查工作。

6.2 认证决定人员要求

由具备相应资质和能力的人员组成，具体要求如下：

1）应具有相关专业教育和工作经历；

2）需熟悉 GB／T 35273《信息安全技术 个人信息安全规范》国家标准，具备相关的专业知识；

3）需要符合《认证工作人员管理及培训办法》的相关要求，并定期或不定期接受本机构对其能力的评估，达标才能从事相关工作。

7 认证工作流程

7.1 认证申请

7.1.1 受理条件

1)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；

2)近三年内，未发生个人信息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；

3）从事行业有资质、资格要求的，应具备相关法定资质、资格。

7.1.2 申请材料

1)个人信息安全规范认证申请书；

2)其他需要的文件。

认证机构对申请资料进行评审后作出受理或不予受理决定，并向认证申请方反馈。若决定受理，认证机构根据认证申请资料确定认证方案，并通知认证申请方。

7.2 认证评价

本机构应实施服务管理审核和服务能力确认或验证，依据 GB／T 35273《信息安全技术 个人信息安全规范》开展，并出具报告。

7.2.1 制定计划

1）制定书面的审查计划，明确审查目的、审查范围、审查依据、审查时间及具体安排。

2）充分考虑审查所涉及的人员能力、专业能力和公正性要求，确定审查组成员，除不可预见的特殊情况外，不得随意更换审查计划确定的人员。

3）审查组应提前将审查计划告知申请组织，如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。

4）审查组在现场审查前应提前告知审查组成员信息，以便双方再次确认和解决可能存在的异议。

7.2.2 审查准备

1）审查组长应负责组织前期准备工作，包括计划沟通、角色的指定、任务分配、资源的申请。

2）审查组长应确保成员了解审查的方法、计划、申请组织的情况、审查中适用的工具等。

3）审查组成员根据分配的任务制定检查表。

4）审查组全体成员签订《认证审查组公正性、保密性承诺》（两份），分别由申请组织和本机构存档。

7.2.3 首次会议

审查组到达现场后，会同申请组织按照认证程序召开首次会议，申请组织的管理层（或其委托的管理者代表）和涉及个人信息安全管理相关的各职能部门人员应参加会议。参会人员均应签到，审查组保留首次会议签到表，首次会议至少包含以下内容：

- 介绍审查组成员及其职责；
- 阐明审查的目的和准则；
- 确定审查日程安排；
- 介绍审查方法和程序；
- 确认审查组陪同人员、所需资源和设施；
- 说明审查结果的提交方法和可能存在的审查结论。

7.2.4 现场审查

审查组按照《认证审查计划表》安排实施审查，采取提问、交谈、查阅文件资料、现场观察等方法，取得确切的证据，记录审查情况，对申请组织的个人信息安全管理进行有效性评价。

在审查期间，受审查方应予以协助、配合，并保证：

1） 审查组能够查阅和个人信息安全管理的有关文件资料和相关记录，包括原始记录；

2） 审查组能够进入与个人信息安全规范认证审查有关的场所(若受审查方认为某些场所为本单位的机密场所，应在首次会议上说明，双方协商解决)；

3） 审核组能够访问与个人信息安全管理有关的人员；

4） 审核组能够访问与个人信息安全管理有关的人员。

7.2.5 报告编写

1） 审查组长负责编写《认证审查报告》初稿，给出初步结论；

2） 审查组长组织报告内容讨论，形成报告终稿；

3） 《认证审查报告》需要经由审查组长和受审查方代表共同确认。

7.2.6 末次会议

审查组会同申请组织按照认证程序召开末次会议，申请组织的管理层（或其委托的管理者代表）的各职能部门人员应参加会议。参会人员均应签到，审查组保留末次会议签到表，末次会议至少包含以下内容：

- 告知审查结论；
- 告知审核后续事项和发证流程；
- 告知如获得证书后，到期换证、变更及年度监督审查的要求；
- 告知投诉、申诉程序。

1） 如受审查方对审核结论有不同看法，与审查组不能达成一致意见时，应记录在审查报告中。

2） 审查组就现场审查发现的不符合项（经确认的）与受审查方商定在一个适当的时间内采取纠正措施。对一般不符合项采取纠正措施的时间要求一般不超过一个月，严重不符合项一般不超过三个月。

3） 不符合项通常分为严重不符合项和一般不符合项，对存在严重不符合项的情况，将导致受审查方的个人信息安全规范认证不能给予注册或推迟给予注册，出现下列情形之一的，即为严重不符合：

- 体系运行出现系统性失效。如认证依据标准的某一或多个重要过程要求要素没有覆盖、没有得到实施，或多个一般不符合同时存在导致审查员认为认证依据标准的一个或多个要素未能被覆盖或实施即多次重复发生不符合现象，而又未能采取有效的纠正措施加以消除，形成系统性失效。
- 体系运行出现区域性失效。如某一部门适用安全管理要求的全面失效现象。
- 所发现不符合事项严重影响个人信息安全管理业绩。
- 组织个人信息安全行为严重违反法律法规或其它要求。

出现下列情况为一般不符合项：

- 对满足个人信息安全管理要求或体系文件的要求而言，是个别的、偶然的、孤立的、性质轻微的不合格。或者说，对审查范围覆盖的体系而言，是个次要的问题。

● 在个人信息安全规范认证活动中，审查员/实习审查员/评估师所识别组织违反法律法规要求， 且未予评价并采取措施的审查发现，将构成不符合。对有意不遵守法律法规（如决定交纳罚款后继续违规操作，而不寻找导致不符合的原因并制订措施）的组织，将不能通过认证或保持认证资格。对存在严重违反法律法规要求的组织，需经确认已采取措施恢复法律法规符合性后，方可获得或保持认证资格。

4） 现场审查全部结束后，审查组将现场审查报告及全套审查文件及记录交本机构存档。

7.3 认证决定

1） 审查组长提交审查报告、审查记录到本机构；

2） 认证决定人员依据 GB／T 35273《信息安全技术 个人信息安全规范》的要求，对审查报告、审查记录等进行综合评价的基础上，作出认证决定。同时，认证决定人员为本机构管理控制下的人员，审查组成员不得参与对审查项目的认证决定；

3） 对于不符合认证要求的申请方，本机构以书面的形式明示其不能获得认证的原因；

4） 申请人如对认证决定结果有异议，可在 30 个工作日内向本机构提出书面投诉，本机构按照《投诉、申诉和争议处理程序》处理投诉事件，并将处理结果书面通知投诉方。

7.4 证书的制作和发放

1） 申请方确认《认证证书内容确认书》后，本机构完成证书制作和发放；

2） 本机构在颁发认证证书后，应在 30 个工作日内按照规定要求将认证结果相关信息报送国家认证认可监督管理委员会。

7.5 监督审核

7.5.1 监督审核周期

1）在认证证书有效期内，对获证组织进行持续监督，年度监督审核至少每个日历年进行一次,初次认证后的第一次监督审核在认证证书签发日起 12 个月

内进行；

2）若超过期限未能实施监督审核的，应按照《认证证书和标志的管理程序》和《认证授予、保持、更新、暂停、恢复、扩大、缩小、注销、撤销程序》对其进行管理；

3）当本机构收到关于获证组织发生重大个人信息安全事故或组织结构、人员等方面发生重大变更等信息或投诉，并认为需要核实的，本机构可增加现场监督审核的频次。

7.5.2 监督审核决定

监督审核完成后，本机构根据监督审核情况和审核报告，作出保持、暂停或者撤销认证证书的决定。涉及证书状态变化的，需向证书持有者发出《认证证书状态变化通知单》，通知被注销或撤销认证证书资格的组织，应于接到通知单的 5 个工作日内将证书交还至本机构，同时，在本机构网站上公布年度监督审核结果。

7.6 复审（再认证）

1）认证证书期满前，若获证组织申请继续持有认证证书，应当至少在认证证书有效期结束前 3 个月向本机构提出申请，由本机构按照认证程序，实施认证审核，并决定是否延续认证证书；

2）获证组织的获证服务未发生重大变化时，本机构可适当简化申请受理和资料审查程序；

3）对超过 3 个月仍不能复审的获证组织，应按初次认证进行实施；

4）因不可抗力或重大自然灾害的原因，不能在认证证书有效期内复审的，获证组织应在证书有效期内向本机构提出书面申请说明原因。经本机构确认，复审可在认证证书有效期后的 3 个月内实施，但不得超过 3 个月，在此期间本机构将暂停并收回已颁发的证书，同时获证组织也不得使用该认证证书。

8 申诉/投诉、争议及处理

参照《投诉、申诉和争议的处理程序》进行管理。

9 认证证书

9.1 证书的保持

1）个人信息安全规范认证证书有效期为 3 年；

2）获证组织应在证书有效期满前三个月向 DSCC 提出复审（再认证）申请，原认证证书复印件以及补充或变更的申请材料提交至本机构。

9.2 证书的更新

本机构通过复审（再认证）的方式对获证组织证书到期时进行认证资格的更新。复审的目的是确认个人信息安全规范水平作为一个整体的持续符合性和有效性，以及于认证范围的持续相关性和适宜性，从而确定能否推荐更新（换发）证书，执行复审申请和审查程序。

9.3 认证的暂停、撤销和注销

当获证组织不再符合认证要求时，本机构对认证证书予以暂停直至撤销。认证申请方在认证证书有效期内可申请暂停或注销认证证书。本机构采用适当方式对外公布被暂停、注销和撤销的认证证书。

暂停期限为 6 个月。暂停期限内，获证组织可提出恢复认证证书的申请，经本机构评价、批准后，方可使用该证书。在暂停认证期间，获证组织不得继续使用认证证书。暂停期满仍未恢复认证资格的，认证证书自动撤销。

当获证组织主动申请不再保持认证资格时，经本机构评价、批准后予以注销。

10 保密处置

在现场审查中，涉及到保密要求的项目或活动，为获得必要的证据，也需对保密要求的项目或活动进行审查。但审查过程中应：

1） 必要时，可与被审查方签订相应的保密承诺书；

2） 在被审查方规定的场所内查看涉及到保密要求工作内容的原件。

11 公正性承诺

本机构郑重承诺：在本机构认证的业务范围内，科学、公正地为申请人提供认证服务。

1） 本机构是独立的第三方认证机构，具有独立开展业务的权利。其中个

人信息安全规范认证是围绕认证工作而开展的活动，不受上级主管部门和其职能部门行政的、经济的和任何其他方面的干预。本机构的财务收入来自认证活动，财务实行独立核算，有稳定的财务状况和良好的财务监督机制。

2） 本机构在公布的认证业务范围内向所有申请者开放。不附加过分的财务或其他条件；不以申请者的规模、是否为某一协会/团体的成员，以及已颁发证书的数目等作为是否受理申请的限制条件。不以不公正的做法，加快或拖延对认证申请的受理。严格按照国家有关法律、法规和认可要求开展认证工作。

3） 本机构确保负有执行职责的管理者和全体人员均不受任何有可能影响认证结果公正性的、来自商业、财务和其他方面的压力。

4） 本机构严格遵守保密制度，对申请者提供的管理和技术资料，在未经申请者同意时保证不向任何第三方提供。

5） 本机构及所属各业务部门：

- 均不主动或被动地为本机构的客户提供对获证或拟认证的咨询；
- 如果需要对申请人的获认证服务进行评价时，均不对申请人提供获认证服务的咨询或内审。

12 权利与义务

12.1 权利

1） 申请组织有权要求本机构按认证合同约定的内容开展认证活动，履行合同义务；

2） 申请组织自主选择咨询单位，本机构不提供咨询服务；

3） 申请组织有权要求本机构向其提供公开性文件资料；

4） 申请组织或持证组织有权要求本机构为认证活动所接触的各种商业机密保密；

5） 对参加评估审核的人员、审核日期安全有意义时，与本机构协商解决；

6） 持证组织有权按照规定使用认证证书和认证标志；

7） 申请组织或持证组织有权就与认证活动有关的工作提出申诉、投诉和争议。

12.2 义务

1） 申请组织对所提供的信息的真实性、准确性负责；

2） 始终遵守国家和本机构关于个人信息安全规范认证的要求，包括：支付认证所需的申请及其他有关费用，妥善保管报告、认证变更确认等认证资料，按要求及时进行变更或复审；

3） 为认证评价做出必要的安排，包括：审查文件和记录、进入相关区域或场所、开展测试验证、访问相关人员和分包方、配合对投诉的调查等。适用时，允许观察员的参与；

4） 在使用个人信息安全规范认证结果时，不得损害本机构的声誉，不做出本机构认为可能误导或未经授权的有关声明；

5） 当认证被暂停或撤销时，应及时停止使用认证证书，采取本机构要求的措施（如交回所有认证文件），以及其他需要的措施；

6） 若需将认证证书的副本提供给他人使用，请提供完整的证书及证书附件；

7） 在文件、宣传册或广告等传播媒体中引用个人信息安全规范认证内容时，应符合本机构的要求；

8） 遵守国家和本机构关于认证标志使用的要求；

9） 保存已知的与认证要求符合性有关的所有投诉记录，在本机构要求时能够提供。

13 其他

1） 本规则内容提及 GB／T 35273《信息安全技术 个人信息安全规范》标准时均指认证活动发生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；

2） 本认证规则由数据安全认证（贵州）有限公司负责解释。