文件编码：DSCC-SC-001/04

数据安全能力成熟度
服务认证规则

发布日期：2025 年 9 月 2 日

生效日期：2025 年 9 月 2 日

实施日期：2025 年 9 月 2 日

数据安全认证（贵州）有限公司

前 言

本认证规则由数据安全认证（贵州）有限公司制订并发布，版权归数据安全认证（贵州）有限公司所有，任何组织及个人未经数据安全认证（贵州）有限公司许可，不得以任何形式全部或部分使用。本规则的最终解释权归数据安全认证（贵州）有限公司所有。

（1）本规则首次发布实施日期：2021 年 2 月 9 日。

（2）第 1 次修订，V2，2021 年 6 月 30 日发布并实施；变更内容：受理条件和工作流程细化；

（3）第 2 次修订，V3,2025 年 6 月 12 日发布并实施；变更内容：按国家认监委关于加强认证规则管理的公告 2025 年第 9 号要求修订；

（4）第 3 次修订，V4，2025 年 9 月 2 日发布并实施，变更内容：按备案整改要求修订。

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）的数据安全能力成熟度服务认证工作，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

本规则规定了对组织开展数据安全能力成熟度服务认证的基本原则和要求，包含初次认证、认证保持和复审（再认证）。

本规则的认证对象为申请方申请的业务过程或系统的数据处理活动。

3 认证依据

GB/T 37988-2019《信息安全技术 数据安全能力成熟度模型》（现行有效）。

4 术语说明

（1）为便于实施，本规则引用了认证依据 GB/T 37988-2019 的以下术语：

PA：过程域（process area）的简称，实现同一安全目标的相关数据安全基本实践的集合，一个过程域中包含多个基本实践。

BP：基本实践（base practice）的简称，实现某一安全目标的数据安全相关活动。

能力成熟度：对一个组织有条理的持续改进能力以及实现特定过程的连续性、可持续性、有效性和可信度的水平。

（2）根据认证过程的变化，本规则对申请认证组织使用了不同的称呼：

申请方：认证审核之前。

受审查方：审核过程中及获证前。

获证组织：获得管理体系认证证书后。

5 认证领域

SC12 电信服务；信息检索和提供服务。

6 认证模式

基于 GB/T 27207-2020《合格评定 服务认证模式选择与应用导则》可选服务认证的模式包括 A-I:

（1）公开的服务特性的检验，简称模式 A；

（2）神秘顾客（暗访）的服务特性的检验，简称模式 B；

（3）公开的服务特性的检测，简称模式 C；

（4）神秘顾客（暗访）的服务特性的检测，简称模式 D；

（5）顾客调查（功能感知），简称模式 E；

（6）既往服务足迹检测（验证感知），简称模式 F；

（7）服务能力的确定和验证，简称模式 G；

（8）服务设计审核，简称模式 H；

（9）服务管理审核，简称模式 I。

6.1 初次服务认证模式及其组合

本机构对初次认证选择的服务认证模式及其组合为：模式 A（公开的服务特性的检验）+模式 I（服务管理审核）。

6.2 监督和再认证模式及其组合

（1）认证保持（或监督）：可根据上一次的评价结果，调整或交替使用服务特性的检验和服务管理审核模式。

（2）再认证：可基于上一个认证周期的综合评价结果，采用初次认证确定的服务认证模式及其组合，或予以简化，包括其样本量的变化。

7 抽样

7.1 人员类

抽样基数为受审查方涉及认证范围的各部门代表，及承担数据安全职责的人员，按“核心角色－支持角色”分类统计总数；采用分层随机抽样的方法，核心角色抽样率≥80%，支持角色抽样率≥50%。

7.2 活动场所类

以受审查方涉及认证范围的相关物理场地总数为基数；初次认证覆盖主体涉及认证范围的所有相关场地，监督审核周期内覆盖主体下所有相关场地。

8 服务特性评价要求

数据安全能力成熟度服务认证的服务特性评价要求依据《信息安全技术 数据安全能力成熟度模型》（GB/T 37988-2019）的具体条款，对申请方数据处理活动的数据安全能力开展服务特性评价，具体内容如下：

8.1 数据安全能力维度

组织建设：评估申请方的数据安全组织架构对组织业务的适用性，组织承担工作职责的明确性、组织运作沟通协调的有效性。

制度流程：考察申请方是否建立了适宜的数据安全管理制度和流程，数据采集、传输、 存储、处理、交换、销毁等各关键节点审批的明确性，以及制度流程管理的规范性、实施的有效性和一致性。

技术工具：了解申请方是否采用了必要的数据安全技术工具，以及技术工具的使用对制度流程固化执行的实现能力，技术工具对数据安全工作的支持能力。

人员能力：评估申请方人员所具备的数据安全技能是否能够满足实现安全目标的能力要求，数据安全意识以及对关键岗位的数据安全能力培养，人员对数据处理活动安全的保障情况。

8.2 能力成熟度等级维度

依据 GB/T 37988-2019《信息安全技术 数据安全能力成熟度模型》附录 A，数据安全能力成熟度认证分为一到五级，其中五级最高，一级最低。

1 级-非正式执行级：执行过程随机、无序、被动，主要依赖个人经验，无法复制；

2 级-计划跟踪级：在业务系统级别主动实现了安全过程的计划与执行，体系化形成，仅能够跟踪和控制执行进展；

3 级-充分定义级：在组织级别实现了安全过程的规范执行，过程可重复执行，执行结果可核查；

4 级-量化控制级：建立了量化的安全目标，安全过程可度量；

5 级-持续优化级：根据整体目标，不断改进和优化安全过程。

8.3 数据安全过程维度

数据采集安全：评估数据采集的合法性、合规性和准确性，是否明确了数据采集的范围和目的，是否获得了必要的授权；包含数据分类分级、数据采集安全管理、数据源鉴别及记录、数据质量管理 4 个 PA。

数据传输安全：考察数据在传输过程中的保密性、完整性和可用性，是否采用了加密等技术手段防止数据泄露和篡改；包含数据传输加密、网络可用性管理 2 个 PA。

数据存储安全：关注数据存储的安全性和可靠性，包括存储介质的管理、数据备份与恢复策略、数据加密存储等；包含存储媒体安全、逻辑存储安全、数据备份和恢复 3 个 PA。

数据处理安全：评估数据处理过程中的安全风险，如数据脱敏、访问控制、数据审计等，确保数据处理的合法性和合规性；包含数据脱敏、数据分析安全、数据正当使用、数据处理环境安全、数据导入导出安全 5 个 PA。

数据交换安全：考查数据在不同组织或系统之间交换时的安全措施，如数据共享的审批流程、数据格式的转换、数据加密等；包含数据共享安全、数据发布安全、数据接口安全 3 个 PA。

数据销毁安全：关注数据销毁的彻底性和合规性，是否有明确的数据销毁流程和记录确保数据在不再需要时能够被安全删除；包含数据销毁处置、存储媒体销毁处置 2 个 PA。

通用安全：包括数据安全策略规划、组织和人员管理、合规管理、数据资产管理、数据供应链安全、元数据管理、终端数据安全、监控与审计、鉴别与访问控制、需求分析、安全事件应急 11 个 PA 的通用数据安全管理内容。

9 认证实施流程

9.1 认证申请

9.1.1 申请范围界定

场所：认证申请方实际对业务过程或系统进行数据处理活动所在的物理场所。

活动：认证申请方申请的业务过程或系统的数据处理活动。

等级：认证申请方申请的 GB/T37988-2019 中的数据安全能力成熟度等级。

9.1.2 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，未发生数据安全事故或被执法监管部门责令停业整顿或在国家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。

9.1.3 申请材料

申请方应提供认证申请书及以下资料：

（1）有效法律地位证明复印件及适用时从事相关服务的资质和任何行政许可证明复印件；

（2）符合《GB/T 37988-2019 信息安全技术 数据安全能力成熟度模型》的现行有效的数据安全相关成文文件；

（3）组织架构图；

（4）拟申请的服务认证等级；

（5）其他认证所需相关材料。

9.2 申请评审

（1）本机构对申请材料进行审查，确定其完整性，以及与申请方的进一步确认和沟通。对申请方提交的申请书及资料进行内容审查并保存审查记录，以确保：

a）认证要求明确、形成文件并得到理解；

b）本机构和申请方之间在理解上的差异得到解决；

c）对于申请的认证内容及后续现场审查场所，本机构有能力开展服务。

（2）若存在被执法监管部门责令停业整顿或在国家企业信用信息公示系统中被列入“严重违法企业名单”的申请方，本机构不予受理其认证申请。

（3）若文档审查存在较多问题，需要及时反馈给申请方待其修改后重新提交，或向申请方发出不予受理的通知。

本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。

9.3 认证审查

本机构应对受审查方数据处理活动的数据安全能力实施服务特性的检验和服务管理审核，依据 GB/T 37988-2019《信息安全技术 数据安全能力成熟度模型》开展，并出具报告。

9.3.1 组建审查组

（1）充分考虑审核所涉及的人员能力、专业能力和公正性要求，组建审查组；

（2）审查员应熟悉 GB/T 37988-2019《信息安全技术 数据安全能力成熟度模型》国家标准及相关法律法规要求，具备相应的知识和技能，必要时可选择技术专家参加审查组；

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

（4）审查组可以有实习审查员，其要在审查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查组中的审查员承担责任。

9.3.2 审查准备

（1）审查组长应负责组织前期准备工作，包括制定审核计划、任务分配、资源的申请等；

（2）审查组长应确保成员了解审查的方法、计划、申请方的情况、审查中适用的工具等；

（3）审查组成员根据分配的任务制定项目执行过程文档；

（4）审查组全体成员签订《认证审查组公正性、保密性承诺》（https://www.dscc.org.cn/service/service-2.html）。

9.3.3 首次会议

审查组到达现场后，会同受审查方按照认证程序召开首次会议，受审查方的管理层（或其委托的管理者代表）和数据安全相关的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：

（1）介绍审查组成员及其职责；

（2）阐明审查的目的和准则；

（3）确定审查日程安排；

（4）介绍审查方法和程序；

（5）确认审查组陪同人员、所需资源和设施；

（6）说明审查结果的提交方法和可能存在的审查结论。

9.3.4 服务特性测评

审查组按照 GB/T37988-2019 标准，开展服务特性的测评，具体如下：

（1）服务管理的符合性审核。根据 GB/T37988-2019 标准各 PA 中关于服务管理要求（包含组织和制度的要求），实施适当的抽样，通过人员访谈、文件评审和旁站验证等方式开展服务管理的审核，收集服务管理审核信息，对收集的信息进行归类和分析，作为审核证据，对照审核准则实施评价，判断符合性。

a）人员访谈：审查组按照抽样的要求对认证范围内涉及的核心角色和支持角色进行访谈，确认受审查方数据安全组织架构对组织业务的适用性，组织承担工作职责的明确性；

b）文档审查：审查组审查数据安全相关的文档材料，确定是否涵盖数据采集、传输、存储、处理、交换、销毁的数据生命周期的 PA 和控制项，制度流程的执行情况是否可跟踪，并建立更新机制；

c）旁站式验证：审查人员在现场通过实地观察了解受审查方的组织运作沟通协调的有效性，查阅管理制度的执行记录验证服务管理的符合性。

（2）服务特性的评价。通过人员访谈、配置检查、工具测试、旁站式验证等方式开展服务特性的评价，对受审查方申请的业务过程或系统的数据采集、传输、存储、使用、交换、销毁全生命周期和通用安全等数据处理活动进行检验，评价其满足 GB/T37988-2019 标准各 PA 中技术和人员能力要求的情况，判断符合性。

a）人员访谈：审查组按照抽样的要求对认证范围内涉及的核心角色和支持角色进行访谈，了解人员的数据安全意识，以及是否具备数据安全相关专业知识和技能，能否有效地执行数据安全制度并利用安全技术工具保护数据生命周期和通用过程的数据处理活动安全；

b）配置检查：根据受审查方提供的技术材料，审查人员登录相关的终端设备、系统平台或网站等，检查核实其功能和配置是否与安全策略、合规要求等保持一致；了解受审查方是否采用了必要的数据安全技术工具，以及技术工具的运行是否满足数据生命周期和通用过程的数据处理活动各 BP 的服务特性要求；

c）工具测试：审查人员利用技术工具对系统平台进行必要的测试，验证其是否符合受审查方申请的数据安全成熟度模型等级的技术能力要求，适当时，可采信第三方机构的测试结论；

d）旁站式验证：审查人员在现场通过实地观察，了解受审查方的人员操作、工具运行、技术设施和环境状况，评价人员的安全意识和业务能力以及技术设施的运营情况。了解受审查方申请认证范围内的业务过程或系统的数据处理活动现状，验证技术和人员能力服务特性的符合性。

9.3.5 末次会议

审查组会同申请方按照认证程序召开末次会议，申请方的管理层（或其委托的管理者代表）和数据安全相关的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：

（1）告知审查结论；

（2）告知审核后续事项和发证流程；

（3）告知如获得证书后，到期换证、变更及年度监督审查的要求；

（4）告知投诉、申诉程序。

如审查组长在本阶段审查中列出不符合项和观察项（适用时），则需在该阶段末次会议中由受审查方现场签字确认，并要求受审查方在要求期限之内按照要求完成不符合项的纠正，并由审查组进行验证。

9.3.6 审查报告

（1）不符合项验证：本机构针对末次会议提出的不符合项，验证申请方所采取的纠正措施及其结果的有效性。

（2）审查报告编制：审查组长根据审查组的审核结果与内部讨论意见，编制审核报告，经本机构批准后，提交受审查方。

9.4 认证复核与认证决定

（1）本机构在收到审查组提交的全套审核资料后，组织开展认证复核与认证决定工作。审查组成员不得参与对审查项目的认证复核与认证决定。获准认证/注册的受审查方，应符合下列条件：

a）满足申请方要求；

b）认证程序符合规定要求，上报资料完整、手续齐全；

c）文件化资料符合认证标准或其他引用文件的要求；

d）不符合项已按要求完成了纠正措施并经审查组验证符合要求。

（2）对于不符合认证要求的受审查方，本机构以书面的形式明示其不能获得认证的原因。审查结果符合要求的，本机构将向受审查方提供经批准的书面报告并启动证书制作和发放流程。

（3）受审查方如对认证决定结果有异议，可在 15 个工作日内向本机构提出书面申诉，本机构将对申诉事件进行受理，并将处理结果书面通知申诉方。

9.5 证书的制作和发放

（1）受审查方确认认证证书内容后，本机构完成证书制作和发放；

（2）本机构在颁发认证证书后，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；

（3）获证组织可通过数据安全认证（贵州）有限公司官网（https://ds.dscc.org.cn/dscc/open/organization/certification）与国家认监委网站（www.cnca.gov.cn）专栏查询本机构颁发的认证证书信息。

10 认证保持

10.1 监督审核

10.1.1 监督审核周期

（1）认证证书有效期为 3 年，在证书有效期内，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）当本机构收到关于获证组织发生重大数据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。

10.1.2 监督审核内容

监督时应包括但不限于以下内容：

（1）上次评价以来组织活动及运行的资源是否有变更；

（2）组织数据安全特性有关的活动是否有效运行；

（3）涉及法律法规规定的，相关法律法规或技术标准是否发生变化，是否持续符合相关规定；

（4）数据安全能力是否持续保持；

（5）获证组织对认证标志的使用或对认证资格的引用是否符合相关的规定；

（6）是否及时接受和处理投诉；

（7）针对投诉的问题，及时制定并实施了有效的持续改进。

监督至少应包括服务管理审核，且在一个认证周期内至少开展一次服务特性检验，监督采用条款抽样的方式开展，抽样 PA 的数量应不低于认证依据条款的 1/2。

10.1.3 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，需向获证组织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，报送年度监督审核结果至国家认证认可监督管理委员会。

10.2 扩大认证范围

扩大认证范围可以包括活动范围的扩大，组织范围的扩大，地域或场所的扩大等。

10.2.1 扩大认证范围的条件

（1）获证组织申请扩大认证范围在法律地位文件和资质规定的范围内；

（2）获证组织的获证服务覆盖申请扩大的认证范围，并符合认证标准/规范性文件要求；

（3）至少近一年来，获证组织在申请扩大认证范围内未发生重大事故和国家检查不合格。

10.2.2 扩大认证范围的程序

（1）获证组织向本机构提出扩大认证范围申请和相关附件；

（2）本机构向获证组织提供与扩大认证范围有关信息的公开文件，获证组织已知悉并理解；

（3）获证组织与机构签署认证合同补充协议，并按规定支付相关认证费用；

（4）获证组织申请扩大认证范围所涉及的获证服务经本机构审查组的审查已符合认证标准/规范性文件和其他必要的附加要求，对认证合格者按程序更换证书。

10.3 缩小认证范围

10.3.1 缩小认证范围的条件

（1）获证组织的认证范围内部分业务活动、服务范围、区域等持续地或严重地不满足认证要求；

（2）获证组织的认证范围内部分业务范围、现场、区域、主要过程等不愿再继续保持认证资格；

（3）获证组织不再从事某种业务活动、服务，相关的获证服务不再存在；

（4）未能在规定的时限内解决造成暂停的不符合项，在不影响获证组织责任和标准完整性前提下，与获证组织协商，可以将不满足要求的部分，从认证范围中删除。

10.3.2 缩小认证范围的程序

（1）获证组织向本机构正式提交缩小认证范围的认证申请书，或本机构提出缩小获证组织认证范围的建议，并提供书面理由和事实证据。

（2）本机构识别缩小认证范围后对认证范围内持续符合认证要求的影响，并确认不可能产生的负面影响或增加的认证风险，机构领导签批认证决定，换发认证证书。

11 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）复审过程与初次认证保持一致，再认证条款与初次认证相同；

（3）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。

12 认证证书和认证标志

12.1 认证证书

12.1.1 认证证书内容

本机构的数据安全能力成熟度认证证书具备中英文版本，当对英文内容发生争议时，以中文为准，其内容如下：

（1）获证组织名称、地址和统一社会信用代码；

（2）证书编号；

（3）认证依据标准的编号与版次；

（4）数据安全能力成熟度获证等级；

（5）认证范围描述；

（6）认证证书的首次签发日期、颁发日期和有效期（变更情况发生时，首次签发日期和颁发日期不一致）；

（7）监督审核的提示；

（8）证书查询方式；

（9）本认证机构的名称、地址、网址和标志；

（10）本认证机构的签字和盖章。

12.1.2 认证证书样式

本机构的数据安全能力成熟度管理体系认证证书样式如下：


数据安全能力成熟度认证证书

证书编号：DSCC-2025-DSMM-D-XXX-R0

兹证明

XXXXXX有限公司

统一社会信用代码：91310115688xxxxxxx

注册地址：XXXXXXXXX

经营地址：XXXXXXXXX

经评估达到

数据安全能力成熟度X级

评估依据GB/T 37988-2019

认证范围包括：XXXXXXXXXXX

首次签发日期：XXXX年X月XX日
颁 发 日 期：XXXX年X月XX日
有 效 日 期至：XXXX年X月XX日

在一个监督周期后，本证书须与DSCC签发的监督审核合格通知书合并使用，方可有效
查询证书请登录全国认证认可信息公共服务平台（www.cnca.gov.cn）或https://www.dscc.org.cn

数据安全认证(贵州)有限公司

中国·贵阳·林城西路·摩根中心B座9楼 550000

https://www.dscc.org.cn


CERTIFICATE OF DATA SECURITY CAPABILITY MATURITY

No.:DSCC-2025-DSMM-D-XXX-R0

this is to certify that

XXXXX Co.,Ltd.

Unified Social Credit Code :9131011568XXXXXXXX

Registered Address:XXXXXXXX

Office Address:XXXXXXXX

Has been succefully appraised at

Data Security Capability Maturity Level X

According to:GB/T 37988-2019

Certification scope including:XXXXXX

Date of first issue: XX XX,XXXX
Date of issue:XX XX,XXXX
Date of expiry: XX XX,XXXX

After one supervision cycle, this certificate must be used together with the supervision and audit qualification notice issued by DSCC before it can be valid, please log in the national certification and accreditation public sevice platform (www.cnca.gov.cn) or https://www.dscc.org.cn

Data Security Certification (Guizhou) Co.,Ltd

9th Floor, Block B, Morgan Center, Lincheng West Road, Guiyang, China 550000

https://www.dscc.org.cn

12.1.3 认证证书的使用

（1）在认证证书的有效期内获证组织有权正确使用认证证书；

（2）认证证书可以展示在文件、网站、通过认证的工作场所、销售场所、广告和宣传材料中或广告宣传等商业活动，但不得利用认证证书和相关文字、

符号，误导公众认为认证证书覆盖范围外的数据安全能力获得认证， 宣传认证结果时不应损害本机构的声誉；

（3）获证组织可以在有效认证证书覆盖的领域和业务范围内按以下文字描述的方式将认证证书的有关信息展示在文件、网站、通过认证的工作场所、销售场所、广告和宣传资料中、广告宣传等商业活动。如：“本组织（或企业）通过数据安全认证（贵州）有限公司的数据安全能力成熟度 x 级认证，证书号为 xxxxx”；

（4）在证书有效期内组织有权按照《认证证书和标志管理程序》（DSCC-QP06）合理使用认证证书；

（5）获证组织应妥善保管好证书，以免丢失、损坏。如发生证书丢失、损坏的，获证组织可申请补发；

（6）保证证书覆盖范围内的数据安全获证服务运行稳定；

（7）认证证书有效期内，获证组织名称、地址等发生变化时，获证组织应当向本机构提出变更申请；

（8）当获证组织的获证服务发生重大变化并影响认证资格的保持时，应向本机构申请变更并接受本机构的调查或监督审核，调查前及监督审核不合格者，不得继续使用已获得的认证证书；

（9）证书不准伪造、涂改、出借、出租、转让、倒卖、部分出示、部分复印；

（10）获证组织应按时交纳认证费用，以获得或保持证书；

（11）证书被暂停、撤销或注销，获证组织应按要求将证书交还本机构，并同时停止在文件、网站、通过认证的工作场所、广告和宣传资料中展示认证证书和停止将有关认证信息用于广告宣传等商业活动；

（12）在认证范围被缩小时，修改所有设计原认证范围的广告材料。

12.2 认证标识

12.2.1 认证标识样式

本机构的数据安全能力成熟度管理体系认证标志如下：

12.2.2 认证标识的使用

（1）数据安全能力成熟度认证标志不能应用于产品或消费者所见的产品包装之上，或以任何其他可解释为表示产品符合性的方式使用的信息，并向获证组织提供；

（2）获证组织在使用获证组织标志时不可使公众误认为本机构对获证组织的特定的产品或服务进行了认证；

（3）获证组织不得将获证组织标志使用在与被认证领域和业务范围无关的各类业务及各类宣传媒体上进行误导宣传；

（4）获证组织不得将标志被用于实验室检测、校准或检查的报告，此类报告被视为产品；

（5）获证组织在使用标志时只能使用与本机构所提供色调一致、排列方式一致的标志；

（6）获证组织在使用获证组织标志时可按比例放大或缩小，但字迹必须清晰，标志必须完整，也不得将其变形使用；

（7）获证组织保证只在涉及证书所限定的范围的场合使用获证组织标志；

（8）获证组织应接受本机构对标志使用情况的监督检查；

（9）获证组织在认证有效期内的数据安全管理不符合认证要求，本机构将责令获证组织限期改正，在纠正期间不得使用获证组织标志。

13 暂停

（1）具备相关证明材料表明获证组织存在影响认证的持续有效性和公信力的以下情况之一时，本机构将实施暂停：

a）获证组织的法律地位、资质不再符合国家的最新要求，或认证范围已不在现行有效的法律地位文件和资质规定的范围内，但仍有可能在短期内符合规定要求；

b）获证组织未能在规定的期限或频次内接受监督审核；

c）获证组织的获证服务发生重大变更已不满足原认证要求，未及时通知本机构以得到妥善处理；

d）获证组织于获证期间在认证范围内发生影响信息安全绩效的重大事故，或国家行业监察发现重大问题；

e）获证组织在获证期间未按规定使用认证证书和认证标志；

f）获证组织未履行与本机构签署认证合同中规定的责任和义务，如未按照认证合同规定按时支付认证费用等；

g）监督审核中发现的不符合项在商定期内未采取有效纠正和纠正措施；

h）获证组织主动请求暂停；

i）对其投诉或任何其他信息证实表明获证组织不再符合机构的相关规定要求。

（2）当做出证书暂停处理后，本机构将向获证组织发出书面通知，通知获证组织其证书已被暂停。被暂停认证资格期间，获证组织不得使用认证证书和认证标志；

（3）一般情况下，认证资格暂停时间不超过 6 个月；

（4）在暂停期限到期前，获证组织提供的证明材料表明，已针对暂停认证资格的原因采取了有效的纠正措施，产生原因已经消除，重新符合了相关的认证要求，本机构将取消暂停，恢复其认证资格。暂停期间，经获证组织确认并同意后，可能在暂停期到期前撤销其认证资格。

14 撤销和注销

（1）有证据表明获证组织获证后不能持续满足本认证规则的要求，存在以下情况之一时，本机构将采取撤销的措施：

a）获证组织在认证范围内的组织单元、服务及其过程和活动无法满足适用的最新法律法规的要求，并在短期内无法采取措施或采取措施无效的；

b）获证组织于获证期间在认证范围内发生重大事故和国家检查不合格，并造成严重影响（证明材料须附相关调查分析报告）；

c）获证组织在获证期间发生大量误用认证证书和认证标志，并未能在规定时间内及时有效地采取纠正和纠正措施，造成严重影响的；

d）获证组织对顾客或相关方的重大投诉不作处理的；

e）获证组织单方面宣布不履行与 DSCC 签署认证合同中规定的责任和义务的，或长期拖缴认证费用，并催缴无效的；

f）获证组织转让认证证书和认证标志；

g）获证组织被暂停认证资格后，未能在规定的期限内采取有效地纠正措施，或未申请恢复认证资格的。（证明材料须附暂停认证证书通知书及对不符合纠正情况跟踪验证的情况报告）；

h）破产、严重违反国家法规或 DSCC 有关规定的获证组织（证明材料须附违反本机构规定的具体说明）；

i）其他重大影响认证有效性的情况，证明材料须具体说明。

（2）获证组织主动申请不再保持认证资格的，本机构将采取注销措施。

15 收费

为规范认证收费行为，保护认证双方的利益，本机构制定了收费管理办法和审查人日计算方式，收费项目包括：

（1）固定费用：含申请费 、批准及注册费（含证书费）、变更费、年金、换证费；

（2）认证审核费：含文档审查费、认证实施费、认证决定费、监督审核费；

固定费用收费见本机构网站公开的《收费管理办法》（https://www.dscc.org.cn/service/service-2.html），认证审核费根据受审查方的规模大小、审核现场场地分布、数据处理活动的复杂程度以及申请的数据安全能力成熟度认证级别等，确定所需人日数来核定审核费，详见附件 《审核时间》。

16 申诉/投诉、争议及处理

获证组织对认证过程或决定有异议时，本机构接受获证组织申诉并及时进行处理，在 90 日内将处理结果形成书面通知送交获证组织。书面通知应当告知获证组织，若认为本机构未遵守认证相关法律法规或本规则并导致自身合法权益受到严重侵害的，可以直接向所在地认证监管部门或国家认监委投诉，也可以向相关认可机构投诉。本机构参照公开的《投诉、申诉和争议的处理程序进行管理》（https://www.dscc.org.cn/service/service-2.html）。

17 信息报送与公开

17.1 信息报送

认证机构在颁发认证证书后，应当在 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证认可监督管理委员会。

17.2 信息公开

认证机构为方便认证企业、广大消费者获得认证信息，发挥社会监督作用，通过认证机构的网站向社会公布获证企业证书信息。与认证相关的向社会公众公告的相关信息，主要包括获证企业证书信息、证书状态信息、《数据安全能力成熟度服务认证规则》《认证证书和认证标志管理办法》《投诉、申诉和争议的处理程序》《收费管理办法》和《公正性承诺》。

附件 审核时间

（1）审核策划阶段（5～8 人日）

a）认证申请受理，对提交的相关资料开展审核；

b）组建审查组，编制审查计划；

c）审查计划审核并与客户确认。

（2）实施阶段

为确保认证审查的完整有效，本机构以下表所规定的审查时间为基础，根据申请方所覆盖的活动范围、特性、技术复杂程度和覆盖范围内人数等情况，核算并拟定完成审查工作需要的时间。

等级 / 认证覆盖人员规模	一级（人日）	二级（人日）	三级（人日）	四级（人日）	五级（人日）
微型（≤10 人）	1	2	3	4	5
小型（11～25 人）	2	3	4	5	6
中型（26～50 人）	3	4	5	6	7
大型（≥50 人）	4	5	6	8	10

上表为审查时间一般约定，具体审核时间需结合实际企业规模、企业人员数量、数据规模、 审核范围、数据安全管理的复杂程度等因素来综合确定。在特殊情况下，可以调整审查时间，但减少的时间不得超过上表所规定的审查时间的 20%；监督审核的人日不低于初次认证 1/3，再认证审核的人日不低于初次认证 2/3；表中人日为实际工作时间，不含审核组往返申请方所在地的时间。

（3）整改验证阶段，不含申请方整改时间（1～3 人日）

（4）报告编制阶段（4～6 人日）

（5）认证决定与证书阶段（8～10 人日）