ICS 35.240.99
CCS L67

T/CCIASC

团 体 标 准

T/CCIASC 051—2025

数据安全运维服务能力评定规范

Specification for Capability Evaluation of Data Security Operation and Maintenance Services

（征求意见稿）

2025－10－XX 发布　　2025－10－XX 实施

中国计算机行业协会　　发 布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件由由中国计算机行业协会提出。

本文件由由中国计算机行业协会归口。

本文件起草单位：中国软件评测中心（工业和信息化部软件与集成电路促进中心）、中国电力科学研究院有限公司、北京天融信网络安全技术有限公司、远光软件股份有限公司、长沙长钢计算机有限公司、江苏安国信检测技术有限公司。

本文件主要起草人：林海静、王露颖、曹顺超、张嘉欢、王翔宇、肖红阳、艾龙、郭华、殷雷、胡文奇、过佳敏。

引　言

数据安全运维服务在保障组织数据安全、预防安全事件、确保合规性以及提升员工安全意识等方面发挥着至关重要的作用。当前，很多单位正在开展数据安全运维业务，但数据安全运维服务能力参差不齐，不利于数据安全运维服务市场的健康发展和数据安全标准的有效落地。本文件通过强化对数据安全运维服务提供商的基本要求和分类要求，从核心技术能力、持续经营能力、项目管理能力3个维度进行统一分级、判定，意在构建统一规范的数据安全运维服务能力评定体系，制定有效的数据安全运维服务能力评定规范及配套评定方法。

数据安全运维服务能力评定规范

1 范围

本文件规定了数据安全运维服务能力的评定规范，给出了数据安全运维服务能力评定的基本要求、指标框架、评定流程及评定方法。

本文件既适用于第三方能力评定机构，对其开展的数据安全运维服务能力评定工作提供指引，也适用于数据安全运维服务提供商开展服务能力自评定，为提升其数据安全运维服务能力提供参考。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 22080-2025 网络安全技术 信息安全管理体系要求

GB/T 25069-2022 信息安全技术 术语

GB/T 41479-2022 信息安全技术 网络数据处理安全要求

T/ZHTEA 001-2023 高新技术企业创新能力评价

3 评定原则

a）公正性：评定工作以数据安全运维服务提供商实际情况为基础，通过系统、深入的分析得出客观、公正的评定结论；

b）透明性：评定过程公开透明，评定结论向社会公开。

4 术语和定义

GB/T 25069、GB/T 41479、T/ZHTEA 001中界定的以及下列术语和定义适用于本文件。为了便于使用，以下重复列出了GB/T 25069、GB/T 41479、T/ZHTEA 001中的某些术语和定义。

4.1 数据安全 data security

通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。

注：GB/T 41479—2022，定义3.4

4.2 风险管理 risk management

指导和控制组织相关风险的协调活动。

注：GB/T 25069—2022，定义3.168

4.3 服务工具 service tools

为达成服务目标或提高服务质量和效率所需要的设备、软件、模板、知识库等。

注：GB/T 25069—2022，定义3.184

5 评定基本要求

数据安全运维服务提供商应具备的基本要求包括：

a) 在中华人民共和国境内注册成立，由中国公民、法人投资或者国家投资的企事业单位或非独立法人的集团公司的省分公司/子公司；
b) 产权关系明晰，独立经营核算，无违法记录；
c) 法定代表人、主要负责人、主要技术人员应为中华人民共和国境内的中国公民，且无犯罪记录；
d) 未被列入失信被执行人、重大税收违法案件当事人名单和政府采购严重违法失信行为记录名单等，以及其他可能影响数据安全运维服务提供商能力和信誉的负面清单；
e) 应建立工作保密制度及相应组织监管体系；
f) 从事涉密的数据安全服务应满足国家保密机关相关要求；
g) 应具备固定办公地点。

6 评定指标框架

从核心技术能力、持续经营能力、项目管理能力3个维度分别对数据安全运维服务提出了两级能力要求，由高到低依次是二级、一级能力。其中，核心技术能力的评定指标包括人才基础、运维工具水平技术创新机制、技术转化能力等；持续经营能力包括管理者能力、规模及资质、市场占有能力、盈利能力等；项目管理能力包括人员管理、方案管理、质量管理、风险管理、成果物管理、供应商管理等。

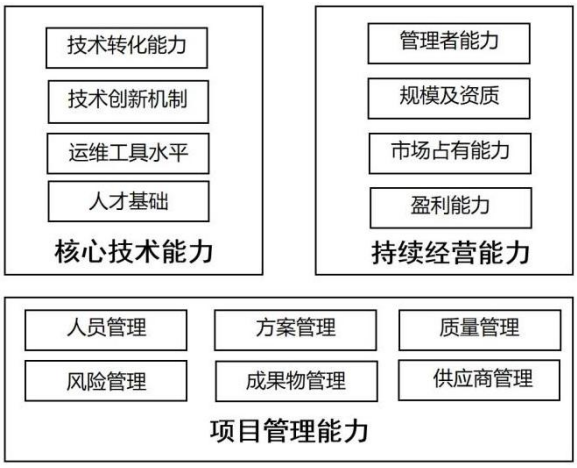

图 1 数据安全运维服务能力评定指标框架图

核心技术能力、持续经营能力、项目管理能力分别从技术、经营、服务过程维度分析企业数据安全运维服务能力。持续经营能力保障了数据安全运维高技术、人才的引进和吸收，促进了核心能力的提升；核心技术能力的提升助力企业提升硬实力，保障企业在高技术产品、服务竞争中占得优势，促进财务资源获得，增强持续经营能力；持续经营能力和核心技术能力提升了服务过程的效能，带动项目管理能力提升；项目管理能力保障市场资源获得、指引研发和生产的方向，促进持续经营能力和核心技术能力提升。

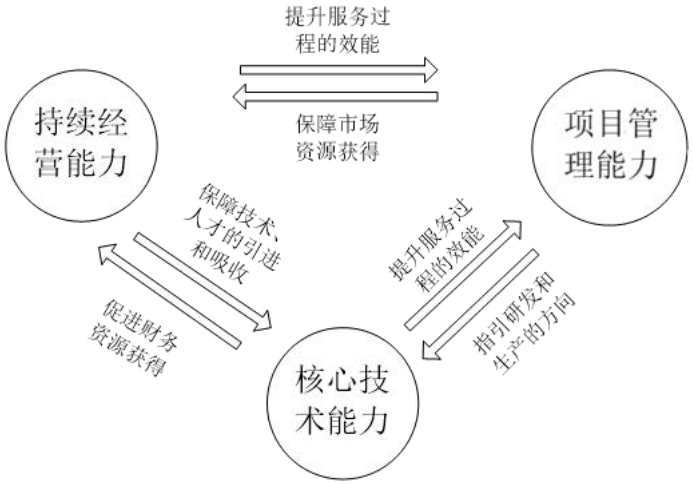

图 2　数据安全运维服务分项能力间的关系图

7　评定分类要求

7.1　核心技术能力

7.1.1　人才基础

7.1.1.1　一级要求

a)正式受聘人员不少于15人，直接从事数据安全运维服务的技术人员不低于8人；

b)直接从事数据安全运维服务的技术人员大学本科以上学历不少于50%；

c)至少5名技术人员接受过数据安全防护技术和准则的系统培训，或参与起草数据安全防护系列标准；

d)至少5名技术人员具有相关机构认可的数据安全运维专业资质；

e)制定技术人员岗前培训计划，相关人员经考核评定合格后方可上岗；

f)技术人员应具备数据安全理论基础知识，熟悉数据安全相关法律法规、政策和标准，具有一年数据安全运维服务项目经验或者参加数据安全相关比赛并获得奖励；

g)技术人员应具备良好的沟通与协调能力，能够准确理解服务需求方的业务流程和数据安全目标；

h)技术人员应具备强有力的执行能力，能够落实数据安全相关制度、策略。

7.1.1.2　二级要求

应满足本文件7.1.1.1节一级要求的所有条款，并在以下方面增强或者增加要求：

a)正式受聘人员不少于75人，直接从事数据安全运维服务的技术人员不低于20人；

b)直接从事数据安全运维服务的技术人员大学本科以上学历不少于60%；

c)至少10名技术人员具备3年以上的数据安全运维服务项目经验，且具有成功的项目案例；

d)至少10名技术人员接受过数据安全防护技术和准则的系统培训,或参与起草数据安全防护系列标准；

e)至少10名技术人员具有相关机构认可的数据安全运维专业资质；

f)技术人员应具备数据安全专业知识，如密码算法应用、数据泄露防护策略、掌握安全审计与风险评估方法等。

7.1.2 运维工具水平

7.1.2.1 一级要求

a) 应具备数据安全运维服务工具（包括设备、平台、软件、模板、知识库等）；
b) 熟练使用要求7.1.2.1 a)提及的数据安全运维服务工具，具备对工具进行深度配置、优化以及故障排查的能力。

7.1.2.2 二级要求

应满足本文件7.1.2.1节一级要求的所有条款，并在以下方面增强或者增加要求：
a) 具备数据资产管理、数据资产防护、数据行为防控、数据开放利用、数据备份与恢复、数据安全管理与策略类工具平台或综合管理类工具平台等一种或多种；
b) 数据安全运维服务工具应具有至少3个成功使用的案例。

7.1.3 技术创新机制

7.1.3.1 一级要求

a) 具备人才引进、知识产权申请、科技成果转化等相关能力提升激励机制；
b) 持续追踪并掌握数据安全运维领域的前沿技术动态，密切关注数据安全事件的发生与发展态势。

7.1.3.2 二级要求

应满足本文件7.1.3.1节一级要求的所有条款，并在以下方面增强或者增加要求：
a)具备数据安全研究、开发相关的组织管理制度；
b)设立内部数据安全技术研究开发机构并具备相应的科研条件，与国内外数据安全研究开发机构开展多种形式产学研合作；
c)具备数据安全技术人员的技能培训、培养进修以及研发考核等制度。

7.1.4 技术转化能力

7.1.4.1 一级要求

a) 了解数据安全相关科技成果转化的主要方式；
b) 具备数据安全运维的成果转化能力，包括但不限于安全监控、威胁检测、应急响应、漏洞管理、日志审计等运维实践，能够将安全策略有效落地并持续优化，确保系统稳定运行与数据资产保护。
c) 提供运维记录，该记录须严格遵循统一规范格式，全面涵盖安全监控、威胁检测、应急响应、漏洞管理、日志审计等各项运维工作详情，详细记录操作时间、操作人员、具体操作内容以及最终处理结果等关键要素，确保记录完整无遗漏、准确无误且具备可追溯性。

7.1.4.2 二级要求

应满足本文件7.1.4.1节一级要求的所有条款，并在以下方面增强或者增加要求：
a) 近3年内数据安全相关科技成果转化的年平均数不少于2项；

b) 具备数据安全运维的开发、测试能力，包括但不限于安全监控、威胁检测、应急响应、漏洞管理、日志审计等运维工具与系统的开发与测试；
c) 应提供定制化运维服务，保证运维方案的灵活性，适应多变的业务场景与安全需求；
d) 能够深入钻研并应用前沿技术，将技术研究成果转化为数据安全运维相关的可交付成果物（如运维工具、解决方案、技术报告等），以此推动数据安全运维能力持续迭代升级，显著提升运维效率与安全防护水准。

7.2 持续经营能力

7.2.1 管理者能力

7.2.1.1 一级要求

a) 单位法人或负责人具备一定的战略能力、组织能力；
b) 明确质量负责人，且具备2年以上的质量管理经验；
c) 明确数据安全技术负责人，且具备2年以上的数据安全项目运维经验。

7.2.1.2 二级要求

应满足本文件7.2.1.1节一级要求的所有条款，并在以下方面增强或者增加要求：
a) 数据安全技术负责人具备中级及以上职称；
b) 数据安全技术负责人具备本科及以上学历；
c) 数据安全技术负责人具备5年以上的数据安全项目运维经验。

7.2.2 规模及资质

7.2.2.1 一级要求

a) 应具备1年以上的数据安全行业从业时间；
b) 产权关系明晰，注册资金（或开办资金）不少于500万元人民币；
c) 具有信息安全管理相关的制度规范；
d) 具备至少1项信息安全服务资质，或至少1个信息安全服务项目获奖。

7.2.2.2 二级要求

应满足本文件7.2.2.1节一级要求的所有条款，并在以下方面增强或者增加要求：
a) 应具备3年以上的数据安全行业从业时间；
b) 产权关系明晰，注册资金（或开办资金）不少于1000万元人民币；
c) 具备至少3项信息安全服务资质，或至少3个省部级及以上信息安全服务项目获奖。

7.2.3 市场占有能力

7.2.3.1 一级要求

a) 至少承担2个数据安全运维服务项目，单个项目合同金额不低于20万元人民币，项目合同总金额不低于100万元人民币；
b) 至少终验通过2个数据安全运维服务项目；
c) 近1年没有出现因各阶段验收未通过或企业自身原因而废止的数据安全运维服务项目。

7.2.3.2 二级要求

应满足本文件7.2.3.1节一级要求的所有条款，并在以下方面增强或者增加要求：

a) 至少承担3个数据安全运维服务项目，单个项目合同金额不低于30万元人民币，项目合同总金额不低于180万元人民币；
b) 至少终验通过4个数据安全运维服务项目。

7.2.4 盈利能力

7.2.4.1 一级要求

a) 近1年净利润、净资产收益均为正；
b) 近1年收入增长率或净利润增长率为正。

7.2.4.2 二级要求

a) 近3年净利润、净资产收益均为正；
b) 近3年收入增长率或净利润增长率为正。

7.3 项目管理能力

7.3.1 人员管理

7.3.1.1 一级要求

a) 设置与数据安全运维服务项目规模相适应人员团队，并建立项目人员清单，明确项目人员职责；
b) 与项目服务人员签订保密协议，并定期进行保密教育、风险排查、自查检查；
c) 具备完善的外包人员管理制度，涵盖外包人员的准入审核、日常行为规范、绩效评估、退出机制等各个环节，从制度层面保障外包人员管理的规范性和有效性，防范因外包人员管理不当引发的各类风险。

7.3.1.2 二级要求

应满足本文件7.3.1.1节一级要求的所有条款，并在以下方面增强或者增加要求：

a) 建立项目服务人员档案，包括服务人员的录用、离岗或离职、资质证明、培训/考核记录、从业经历、实际参与项目及分工等信息，档案至少保存至项目服务人员离职后5年，有关法律法规、行业管理另有规定的除外；
b) 根据项目特点制定项目服务人员行为规范，包括但不限于遵守需求方管理制度，遵守数据安全服务保密管理制度，规范使用专用设备和工具，规范管理成果物等。

7.3.2 方案管理

7.3.2.1 一级要求

a) 建立完善的制定方案制度，确保能够严格按照合同要求制定出内容清晰、逻辑严谨的方案；
b) 编制的方案应获得需求方确认；
c) 编制的方案应具备可操作性，目标应具体、可行，操作计划应详细清晰。

7.3.2.2 二级要求

应满足本文件7.3.2.1节一级要求的所有条款，并在以下方面增强或者增加要求：

a) 编制的方案应明确数据安全运维服务范围、服务目标、服务依据、服务内容、服务成果等；
b) 编制的方案应明确项目人员（包括项目负责人、项目实施技术人员的职责等）、服务流程（包括计划或进度等）、服务环境、服务方法、服务工具、服务保障（包括资源保障、质量管理、保密管理、风险控制等）等服务要素，对资金、人员、工具等资源的调配方案具备可操作性。

7.3.3 质量管理

7.3.3.1 一级要求

a) 建立数据安全运维服务项目质量管理制度，明确项目管理责任部门、责任范围、责任人、工作流程、及与其他部门的统筹协调等，明确数据安全运维服务项目计划、质量要求及监督检查工作；
b) 实施过程符合需求方安全管理相关要求，对服务过程中的关键活动和原始数据进行记录，实施的过程文档记录应准确、完整；
c) 具备客户服务电话热线号码，并提供7×24小时电话热线支持或同等响应级别的客户服务。

7.3.3.2 二级要求

应满足本文件7.3.3.1节一级要求的所有条款，并在以下方面增强或者增加要求：

a) 设置项目质量管理岗位，建立项目服务质量控制机制；
b) 根据方案组织项目实施，定期通过通知、例会、报告（如周、月报）等多种形式与需求方沟通反馈项目质量。

7.3.4 风险管理

7.3.4.1 一级要求

a) 在开展项目实施前分析评估活动潜在风险，识别可能出现的各类风险，针对不同等级的风险制定差异化、可操作的应对策略，明确风险预警阈值与应急处理流程。
b) 在进行数据安全运维服务时，应获得需求方授权，执行过程中发现数据安全事件，及时向需求方报告，并记录事件相关内容；
c) 在进行数据安全运维服务过程中发现产品（含硬件、软件）的安全问题时，及时向需求方报告；
d) 使用服务工具，有可能对服务需求方系统或平台的功能、性能，数据的保密性、完整性、可用性等造成影响的，需向需求方进行风险提示，在采取风险规避措施并得到服务需求方同意后方可使用；
e) 采取必要的监督、审计措施，确保项目服务人员对系统或数据的操作严格按照服务协议及需求方授权范围进行；
f) 编制和签订满足需求方项目保密事项的协议文件，确保需求方运维服务的数据安全。

7.3.4.2 二级要求

应满足本文件7.3.4.1节一级要求的所有条款，并在以下方面增强或者增加要求：

a) 制定有效的风险应急预案，并确保其可行、易操作，定期开展应急预案演练并保存记录；
b) 采取必要措施识别服务范围、服务内容、服务流程、服务环境、服务资源等实施过程中可能产生的风险，并更新风险应急预案；

c) 建立项目风险沟通与应急处置机制，确定双方接口人，及时处理服务实施过程中产生的争议、投诉、突发事件等项目风险，并形成处置结论或解决方案。

7.3.5 成果物管理

7.3.5.1 一级要求

a) 应建立数据安全运维服务成果物编制管理机制；
b) 应具备数据安全运维成果物的编制能力，掌握运维报告、日志分析、风险评估报告等相关要求，熟悉成果物的编制流程与规范；
c) 按服务协议中规定的关键节点，提交运维成果物，如运维方案、监控报告、应急响应记录、漏洞修复报告、总结报告等，并获得需求方确认；
d) 确保所有交付的运维成果物具备真实性、准确性和完整性，能够真实反映运维过程与结果；
e) 完成运维服务交付后，主动清理、交还相关数据、资料、账号、设备工具等，并向需求方提供由运维负责人签字的承诺或确认函，确保无遗留风险。

7.3.5.2 二级要求

应满足本文件7.3.5.1节一级要求的所有条款，并在以下方面增强或者增加要求：
a) 应定期更新数据安全运维成果物模板，定期对运维成果物编制、审核等相关服务人员进行培训，确保成果物符合最新规范与业务需求；
b) 建立、维护运维成果物（包括但不限于运维方案、监控记录、应急响应报告、漏洞修复报告、总结报告等）档案管理规定，严格管理运维档案的查询、借阅行为，档案至少保存5年，有关法律法规、行业管理另有规定的除外。

7.3.6 供应商管理

7.3.6.1 一级要求

a) 建立供应商管理制度，明确供应商管理责任部门、职责范围、责任人，规范供应商引入、评估、合作及退出的工作流程，以及与其他部门的协作机制；
b) 制定供应商资质审查标准，对供应商的营业执照、行业资质、技术能力等基本信息进行审核，确保供应商具备合法经营和提供相应服务或产品的能力；
c) 与供应商签订合作合同，明确服务范围、质量标准、交付周期、违约责任等关键条款，保障双方权益；
d) 建立供应商服务质量反馈渠道，收集对供应商服务或产品的评价信息，对重大问题进行记录和跟进处理；

7.3.6.2 二级要求

应满足本文件7.3.6.1节一级要求的所有条款，并在以下方面增强或者增加要求：
a) 设置专职供应商管理岗位，建立供应商分级分类管理机制，根据供应商重要程度和合作规模，实施差异化管理策略；
b) 制定科学的供应商评估指标体系，从技术能力、服务质量、交付及时性、价格合理性、安全合规等维度，定期（如季度、年度）对供应商进行全面绩效评估；

c） 建立供应商激励与约束机制，对表现优秀的供应商给予业务倾斜、奖励等激励措施，对不达标供应商进行整改督促，整改无效的按合同约定终止合作；
d） 与核心供应商建立长期战略合作伙伴关系，开展技术研发合作、联合培训等深度合作，共同提升数据安全运维服务能力；
e） 提供7×24小时的供应商紧急事务响应支持，确保在突发情况下能及时与供应商协同处理问题。

8 评价方法

8.1 资料收集法

通过企业自身提供内部文档或第三方进行资料收集后，申请评定。

8.2 专家评审法

借助专家意见进行评定。邀请相关领域专家，采用询问、访谈、查阅资料、实地查看、调查统计等方式进行，一般不少于3位。

9 评定程序

数据安全运维服务提供商申请能力评定等级为一级或二级的，应当将申报材料提交到评审机构，能力评定按下列程序进行：

数据安全运维服务提供商提交的申请材料应符合本文件第5-7章相关内容，经评审机构初审合格后，由评审机构组织专家对数据安全运维服务提供商进行现场评定。通过专家现场评定后，数据安全运维服务提供商将获颁对应等级的证书，并接受评审机构的持续监督。

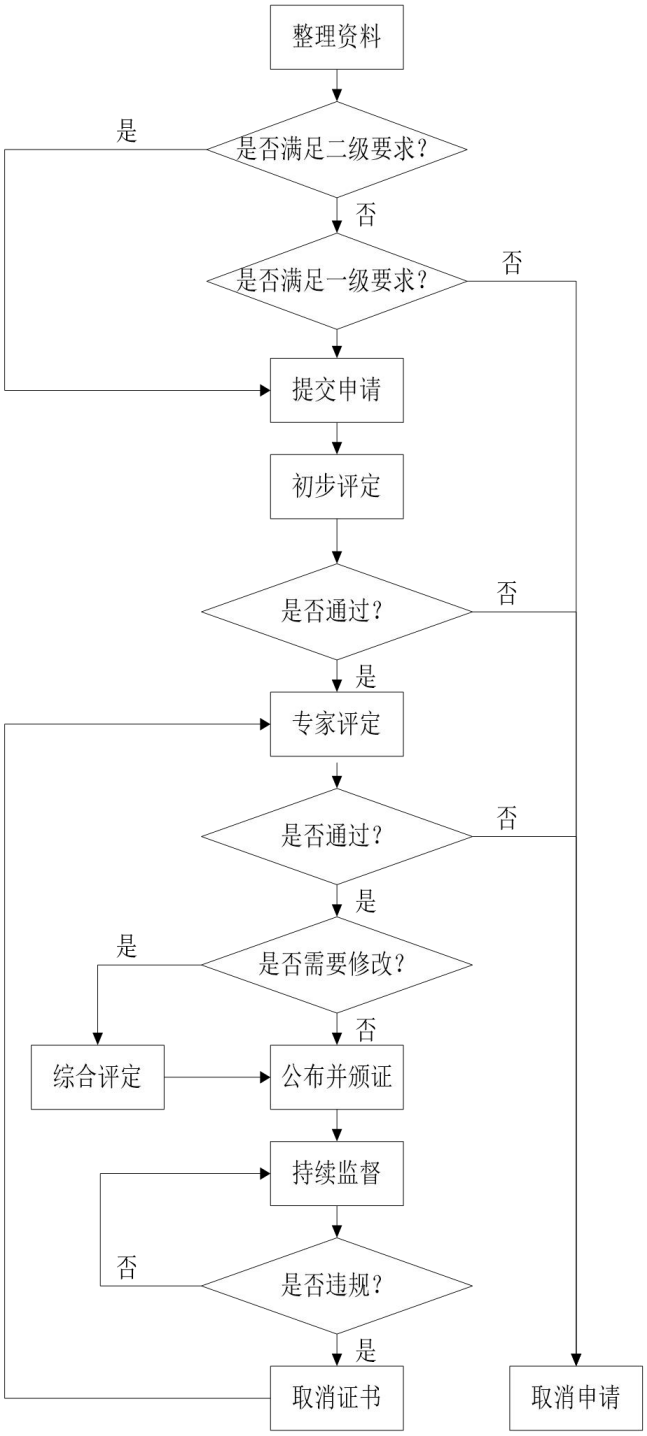

图 3　数据安全运维服务能力评定流程图

10　评定结果

a)　评定通过后，数据安全运维服务能力评定结果和监督检查结果应在数据安全产业公共服务平台官方网站进行公布，并获颁评定证书；

b） 评定证书有效期为三年，获证的数据安全运维服务提供商应邀请评定机构每年进行一次年检；
c） 获证的数据安全运维服务提供商在证书到期前六个月申请重新评定和换证，复申程序参照本文件第9章评定程序执行。

参 考 文 献

[1] GB/T 22080-2025 网络安全技术 信息安全管理体系要求
[2] GB/T 25069-2022 信息安全技术 术语
[3] GB/T 30271—2013 信息安全技术 信息安全服务能力评估准则
[4] GB/T 30276—2020 信息安全技术 网络安全漏洞管理规范
[5] GB/T 31168—2023 信息安全技术 云计算服务安全能力要求
[6] GB/T 35273-2020 信息安全技术 个人信息安全规范
[7] GB/T 35274-2017 信息安全技术 大数据服务安全能力要求
[8] GB/T 37973-2019 信息安全技术 大数据安全管理指南
[9] GB/T 37988-2019 信息安全技术 数据安全能力成熟度模型
[10] GB/T 41479-2022 信息安全技术 网络数据处理安全要求
[11] JGJ/T 67-2019 办公建筑设计标准
[12] YD/T 3644-2020 面向互联网的数据安全能力技术框架
[13] YD/T 3802-2020 电信网和互联网数据安全通用要求
[14] T/ZHTEA 001—2023 高新技术企业创新能力评价
[15] DB34/T 3901-2021 金融服务外包基本要求