

采购需求

一、项目概况

项目名称

陕西省市场监督管理局数据分级分类服务项目

项目金额

88.434 万元

服务目标

围绕陕西省市场监督管理局数据分级分类管理及政务数据共享安全性保障需求，开展新增数据资产梳理、数据分级分类标识、数据安全策略规划，以及数据安全风险评估、数据分级分类软件运维和数据安全风险监控运维服务，为陕西省市场监管数据分级分类管理和数据共享安全做好服务。

服务范围及周期

服务范围

结合省局系统数据结构的最新变化情况，更新迭代数据分级分类咨询、标识等服务相关文档资料，开展数据安全风险评估服务及运行维护服务，运行维护服务具体包括数据分级分类软件运维服务和安全运维服务。

服务周期

一年。

二、数据安全风险评估内容及要求

数据安全风险评估服务

评估服务要求

2.1.1.1 总体要求

供应商应依据现行有效的数据安全法律法规、国家标准及本项目技术需求，按照 GB/T 45577-2025《数据安全技术 数据安全风险评估方法》的方法要求，结合陕西省市场监督管理局实际业务场景开展数据安全风险评估。评估应以现有数据分类分级成果为基础，不重复开展已经完成的数据资产分类分级工作，重点核查数据进入实际业务后的处理路径、使用边界、流动范围和安全控制有效性。

供应商应采用“总体范围全局纳入、评估对象分层、重点深评、后续逐步深化”的实施思路开展本次服务。其中，最新数据分类分级成果覆盖的全部业务场景、应用系统

及相关数据资产纳入总体风险管理视图；深度评估的范围以确认的重点评估范围为准。

2.1.1.2 评估范围与对象

本项目评估对象以业务场景为总体边界，以应用系统、数据资产和数据处理活动为具体评估对象。供应商应围绕业务、系统、数据、处理活动和安全控制建立关联分析，不得仅以单一信息系统检查替代业务场景风险评估。

正式实施时，如经确认调整具体系统或场景范围，供应商应在不降低总体评估方法、评估深度和成果要求的前提下同步调整实施清单。

2.1.1.3 实施方法要求

供应商应采用多种方法组合的方式开展评估。不同方法应相互验证，形成从事实发现到证据支撑、再到风险结论的完整证据链。

- 资料预审：审查数据分类分级成果、制度文件、系统资料、数据共享资料、接口资料、已有安全评估及整改材料等。

- 问卷调研：按照管理、业务、数据处理、系统、安全控制等角色设计问卷，形成结构化基础信息。

- 重点访谈：针对重点业务负责人、系统负责人、数据管理人员、安全管理人员及相关第三方处理主体开展访谈。

- 场景穿透：沿“业务触发—数据来源—系统处理—业务使用—共享/公开/提供—结果使用”链路追踪数据处理过程。

- 系统核查：核查账号权限、接口、日志、导出、加密脱敏、备份恢复、安全监测等控制措施。

- 必要技术验证：对确有必要验证的风险，可采用配置核查、日志分析、系统演示等非侵入方式开展验证；如需使用技术工具或进入生产环境，须经同意，且不得影响正常业务运行。

2.1.1.4 服务周期与实施要求

数据安全风险评估服务原则上应自合同签订后 6 个月内完成评估并出具报告。供应商应根据合同约定和确认的项目计划，在规定周期内完成信息调研、重点场景评估、风险分析、报告编制、成果汇报及整改建议等工作。具体时间安排应在项目启动后形成实施计划并报确认。

供应商应建立项目计划、阶段成果确认和问题台账管理机制，重大风险应及时报告，不得因等待阶段性报告编制而延迟重大风险告知。

2.1.1.5 成果与资料管理要求

供应商应建立完整的评估底稿和证据管理机制，对资料、访谈、核查、分析、风险结论及整改建议进行编号和关联。评估成果应能够从风险结论追溯至业务场景、系统、数据处理活动和证据材料。

- 供应商不得将本项目取得的数据、资料、截图、日志、配置等用于与本项目无关的目的。
- 未经书面授权，不得复制、转移、对外提供或留存项目敏感资料。
- 所有评估底稿、证据材料、报告和电子成果应按要求统一交付，并保证完整性、可读性和可追溯性。

2.1.1.6 质量要求

供应商提交的评估成果应符合以下质量要求：

- 评估范围与本技术需求、确认的实施范围保持一致，不得遗漏已确认的重点系统和重点业务域。
- 风险问题应有明确的评估对象、业务场景、数据处理活动、风险描述、风险依据和证据支撑，避免仅以概念性表述作为风险结论。
- 风险判断应区分事实、分析和结论；同类问题在不同场景下的风险等级应具有可解释性和一致性。
- 整改建议应针对问题根因提出，明确管理、流程或技术整改方向，并具有可实施、可验证特点。
- 报告应结构完整、数据准确、图表清晰，能够支撑风险决策、整改和后续复评。

2.1.1.7 交付成果要求

提交完整的评估报告、风险问题清单、证据清单/底稿、重点场景分析成果、数据流转分析成果及整改建议等交付成果。

最终版交付成果需通过成果评审，并对评审意见完成修改。

序号	成果名称	主要内容	交付形式
1	项目实施计划	项目组织、工作计划、调研安排、成果节点和质量控制措施	Word/PDF
2	信息调研成果	管理、业务、系统、数据处理和安全控制调研记录及证据目录	Word/Excel

3	重点业务场景 分析成果	重点业务域的业务流程、数据处理活动、风险节点和控制分析	Word/PDF/图
4	风险问题清单	风险编号、类别、对象、场景、处理活动、事实、证据、可能性、影响、风险等级、整改建议	Excel
5	数据安全风险评估报告	总体情况、评估方法、现状分析、风险分析、综合结论、整改与治理建议	Word/PDF
6	整改建议及验证材料	重点问题整改建议、验证标准、整改复评记录及风险状态更新	Word/Excel
7	项目成果汇报材料	面向管理层的成果汇报材料及汇报支撑	PPT/其他可编辑格式

评估服务内容

2.1.1.8 项目启动与评估准备

供应商应完成项目启动、工作范围确认、项目计划制定、资料需求清单编制、评估工具及模板准备、人员组织和保密要求确认。应基于提供的最新数据分类分级成果及相关项目资料建立评估基础台账。

2.1.1.9 信息调研与现状分析

供应商应分别面向数据安全、业务、系统、数据管理、安全技术及相关第三方处理主体开展调研。形成管理现状、业务现状、系统现状、数据处理现状和安全控制现状等基础分析，并对已取得资料进行一致性核验。

2.1.1.10 业务场景与数据处理活动分析

供应商应围绕重点业务域梳理业务流程、业务数据来源和去向，识别数据采集、存储、使用、加工、共享、公开、提供、委托、导出、备份、归档和删除/销毁等处理活动，形成重点业务场景画像。

2.1.1.11 数据流转与共享开放分析

供应商应识别重点数据在系统内部、系统之间、部门之间及外部主体之间的实际流转情况。对共享、开放、公示和对外提供，应以实际发生的对象、数据范围、方式、频率、依据、审批和公开机制为核查重点。

2.1.1.12 数据安全评估

供应商应评估数据安全组织责任、制度体系、分类分级成果应用、风险管理、人员管理、供应链治理以及重大业务/系统/数据变化触发机制，识别制度与实际流程、系统控制之间的脱节问题。

2.1.1.13 数据安全技术与控制措施评估

供应商应重点核查身份认证、账号生命周期、访问权限、最小权限、接口认证与传输保护、日志审计、加密脱敏、备份恢复、导出控制、安全监测和运维访问等安全控制措施，并判断控制是否存在、是否有效、是否可提供证据证明。

2.1.1.14 个人信息保护与第三方处理评估

供应商应利用现有个人信息标识成果识别重点场景，评估处理目的、必要性、最小权限、敏感个人信息、查询导出、委托/共同处理和事件处置等情况；同时核查第三方访问范围、授权、合同、安全责任、再委托和退出清理机制。

2.1.1.15 数据安全事件、历史问题与整改评估

供应商应调查数据安全事件、历史漏洞、既有风险问题及整改情况，核查监测、报告、处置、复盘和整改验证机制，对重复出现或长期未闭环问题分析根因并提出整改要求。

2.1.1.16 风险识别、分析与评价

供应商应从风险源、脆弱性、风险事件、影响及现有控制有效性等方面识别和分析风险；综合考虑风险发生可能性、影响程度、数据重要性、业务重要性和控制有效性形成风险等级及处置优先级，并形成全局、业务场景、系统、数据处理活动和风险类别多维风险画像。

2.1.1.17 评估报告及风险清单编制

供应商应形成数据安全风险评估报告，至少包括评估范围、方法、现状分析、主要风险、风险等级、证据依据、风险画像、综合结论和治理建议；形成可编辑的风险问题清单、整改台账和证据索引。

2.1.1.18 提出整改建议

供应商应针对重点风险问题提出具体整改建议，明确问题、风险、原因、整改方向、优先级和验证方式。

分级分类咨询及培训

文档资料持续更新迭代

严格对齐最新的国家/总局标准（GB/T 43697—2024《数据安全技术 数据分类分级

规则》、GA/T 2380—2026《信息安全技术 网络安全等级保护数据安全基本要求》），基于国家市场监督管理总局在2022年下发的《市场监管数据分类分级管理规则（试行）》、《市场监管大数据资源体系及编码规范》、《市场监管数据资源目录编制指南》等，以及《陕西省市场监管数据分类分级管理规则（试行）》，并结合省局系统数据结构最新的变化，针对新增、变更等数据结构变化情况提供数据分级分类标识服务。

并对分类分级标识服务相关咨询文档进行更新迭代，文档资料包括：陕西省市场监督管理局数据分级分类标签库、陕西省市场监督管理局数据分级分类规则模型清单、陕西省市场监督管理局数据分级分类结果清单。

知识库扩充完善

基于市场监管业务场景和行业词汇，构建“市监业务术语库”；结合合规要求，动态更新“分级规则库”；搜集编制“行业合规案例库”与“常见问题解决方案库”，便于检索使用。

培训服务

提供数据安全专项合规培训、运维管理操作培训，设计培训计划，编制培训课件，辅以线上课程、案例教学等多形式培训资源，提升相关人员的数据安全治理能力。其中线下培训地点由陕西省市场监督管理局指定。

三、软件运维内容及要求

软件运维服务

运维服务要求

服务对象：数据分级分类软件。

运维服务内容

3.1.1.1 季度巡检服务

服务期内定期派专业人员到现场走访，开展季度巡检及性能调优。

3.1.1.2 技术支持服务

针对数据分级分类软件工具，提供每周7×24小时不间断的电话支持服务，解答服务过程中遇到的问题，及时提出解决问题的建议和对策。供应商需对数据分级分类软件各个模块所提供的功能有透彻的了解，并且需要非常熟悉每个模块所采用的技术和运行机制。

3.1.1.3 紧急故障响应服务

提供7×24小时紧急故障响应服务。

故障等级定义：

一级（紧急）：系统瘫痪、数据异常、核心功能失效、数据丢失/错乱，影响全局业务开展；

二级（重要）：非核心功能失效、性能显著下降，影响部分业务正常运行；

三级（一般）：局部功能异常、操作体验问题，不影响核心业务开展。

故障处理时限：紧急故障≤4 小时，重要故障≤8 小时，一般故障≤24 小时。

系统优化改善

优化改造

在现有系统核心框架的基础上，进行优化完善，增加以下功能模块。

1、数据分级结果溯源，构建全链路数据分级血缘图，通过下钻功能，可一键查询任一分级结果的原始依据与演变历程。

2、敏感数据分级分类结果一致性校验，通过建立数据主体唯一标识关联机制，自动识别同一数据主体在不同系统中的分级差异，形成校验报告并给出标准化修正建议。

3、数据分级结果共享接口，建立分级分类结果跨部门互认机制，通过标准化 API 接口向外输出统一数据标签，明确不同级别数据的共享范围、使用权限和防护要求，解决跨部门数据共享的安全与合规痛点。

4、分级安全防护策略管理，根据数据分级结果自动联动安全管控策略，内置多种防护策略，支持动态下发同步安全防护管理要求。

5、数据安全运营监控，通过可视化图表技术制作数据安全运营监控界面，展示数据安全风险统计指标情况；数据分级分类监控，按月度生成分级分类运营指标看板、运营分析报告，按月动态统计新纳管资产数、分类分级覆盖率等指标。

6、高敏感数据异常访问管理，针对核心企业信息和个人敏感信息，支持自定义时间、IP、下载量等维度阈值，实现细粒度安全防控。

四、安全运维内容及要求

安全运维服务

运维服务要求

服务对象：需持续开展数据安全风险监测的业务信息系统及相关数据环境，监控通过应用软件访问数据库的行为。

运维服务内容

4.1.1.1 动态风险监测

供应商可提供数据安全动态风险监测服务，并根据业务系统变化持续优化风险检测规则，提高风险识别准确性。

通过数据访问行为分析，对敏感数据异动、非工作时间异常访问、异常数据流转行为等风险进行持续监控，并针对监测发现的异常访问行为开展分析研判，过滤误报风险，协助省局运维团队开展风险处置。

4.1.1.2 重点系统专项复测

供应商应针对前期风险评估中识别出的高风险点位、重点系统开展专项复测，跟踪分级管控策略落地及风险整改情况，复测周期原则上按季度开展。

具体内容包括：配合开展整改咨询、材料复核、配置核验、日志验证或场景复测，并更新风险状态。

五、实施要求

人员配置要求

供应商应根据本项目服务内容及实施要求，组建专业服务团队，保障数据安全风险评估、软件运行维护、安全运维及系统优化工作顺利开展。

项目团队应包括项目负责人、数据安全风险评估人员、系统开发人员、系统运维人员、安全运维人员等角色。

设施设备与工具配置要求

供应商应根据项目实施需要，配置必要的软件工具、分析工具及技术资源，保障项目顺利实施。供应商应确保使用工具符合国家相关安全管理要求，不得影响采购人业务系统正常运行。

其他要求

无。