

# 江苏靖江农村商业银行股份有限公司

## 数据库审计系统采购

### 询 价 函

日 期：2023 年 10 月 26 日

# 数据库审计系统采购询价函

江苏靖江农村商业银行股份有限公司（以下简称：本行）拟采购数据库审计系统。系统需求详见“附件 1：系统需求一览表”。请贵公司本着自愿的原则，于 2023 年 10 月 30 日（周一）下午 17:00 之前将报价文件（见附件 2：报价文件）盖章密封邮寄或送至我行办公室。

报价文件投送地址：江苏省靖江市南环路 66 号靖江农商行办公大楼中五楼办公室二。联系人：仇先生，13852620880；黄先生，1537070509。邮编：214500。

报价商须知：

1、报价文件主要包括：投标报价表、售后服务措施、营业执照、法人身份证、代理人身份证复印件、原厂代理商授权书、法定代表人授权书等。

2、报价商必须准备一式二份的报价文件（正本一份 副本一份），用信封密封，封口加盖单位公章，封面上写明报价商的名称和项目名称。

3、报价包括系统软件费、税费、人力费、运费、系统安装调试费、质保服务费等直到用户正常使用为止的一切费用，用户不再支付任何其它费用。

4、主要合同条款有：

✓ 安装调试：货到现场后由供应商安排原厂工程师现场安装和调试，按买方要求配置系统，直至系统功能需求全部完成。

✓ 培训服务：负责为用户提供售前培训、现场使用培训和其他相关技术培训。

✓ 质保服务：提供三年软件原厂商质保服务，提供软件版本升级服务。

✓ 原厂服务：帮助热线服务时间 7×24 小时，接买方通知后 1 小时给予解决方案；紧急支持服务时间 7×24 小时，接买方通知后 2 小时给予解决方案，如在 24 小时内不能

解决问题，应在 48 小时内免费提供同样品牌、规格或更高配置的系统更换到位。

✓ 付款方式：安装调试验收合格后，甲方支付合同金额的 95%；剩余 5%的余款在使用一年系统正常运行后全部付清。

5、本项目成交方法采用最低价法。完全满足招标文件的实质性要求，按照报价由低到高的顺序，由采购人按照最低价法，确定最低报价的 1 家为成交供应商。当最低报价出现有两家或以上供应商时，现场抽签确定成交供应商。成交供应商确定后，采购人不对未成交供应商就评审过程以及未能成交原因做出任何解释。

6、凡参加本次报价的供应商应当明确，一旦我行收到报价文件，供应商则构成要约。我行一旦承诺，供应商须按上述须知的 1-5 条及其要约内容，与我行签订合同。

江苏靖江农村商业银行股份有限公司

2023 年 10 月 26 日

附件 1：系统需求一览表

功能指标	指标要求
设备配置要求	采用软硬一体的标准机架式设备，配置不少于 4 个千兆电口，冗余电源。
数据库类型	支持 ORACLE、MYSQL、MSSQL、SYBASE、DB2、达梦 6/7、人大金仓、神州通用、INFORMIX、PostgreSQL、Gbase、Hive、MongoDB、Redis、TeraData、cache、Kafka、ElasticSearch、HANA、MariaDB、Hbase 等多种数据库类型。
	支持 OCI/JDBC/OLEDB/ODBC 等常见协议。
防护手段	支持日志的风险等级自定义。
规则条件	客户端 IP、源应用程序、主机名、系统用户名、客户端端口、客户端 MAC、数据库用户名、数据库 IP、列、数据库、操作对象、操作对象类别、操作类型、SQL 关键字、SQL 模式、SQL 结果内容、执行时长、删除行数、响应状态等。
数据分析	支持语句大小为 30MB 内的超长语句的审计与展示，页面不仅展示超长语句全文，还可统计出语句大小。（提供功能截图并加盖公章）
	支持基于 SQL 模板设置模板状态，过滤匹配该模板的语句，并能根据以下条件查询模板信息：关键字、触发规则、状态，且可根据所需选择排序字段。同时支持 SQL 模版和关联的具体语句的相互跳转查看；（提供功能截图并加盖公章）
全局参数	支持全局参数配置，方便不同策略引用，可以配置的参数有：客户端 IP 集、源应用程序集、系统用户名、主机名、数据库用户集、表组集、存储过程集、数据库列集、SQL 关键字组集、数据库用户组集。（提供功能截图并加盖公章）
策略管理	支持策略的添加、删除、导入、导出。
内置规则	支持内置高风险规则，防范维护人员执行 no where 删除、truncate table 等合法的授权的高危操作检测。（提供功能截图并盖章）
默认全记录	支持默认情况下全部记录的规则。
超级白名单	支持数据库连接工具白名单功能，自动忽略数据库连接工具访问数据库的默认操作。
默认高风险规则	支持内置高风险操作特征规则，包含：清表（delete no where 、truncate table）、删表（drop table）、提权（alter、grant）。（提供功能截图并盖章）
数据库自动发现	支持通过监控网络流量自动发现未审计数据库。（提供功能截图并盖章）
SQL 注入	支持基于 CVE 的 SQL 注入漏洞检测，其中 Oracle 特征不少于 470 个。（提供功能截图并盖章）
缓冲区溢出检测防护	支持特征方式的缓冲区溢出检测规则。
日志内容	日志内容能够详尽的显示访问行为发生的具体特征，具体信息包括：访问的时间、访问客户端 IP、客户端 MAC、客户端端口号、客户端连接工具名、数据库用户名、数据库 IP、数据库 MAC、数据库实例、表、列、操作类型、SQL 内容、SQL 结果内容、执行时间（毫秒）、响应状态、影响行数、查询返回行、匹配的策略、风险等级。（提供功能截图并盖章）

	章)
解析能力	支持双向审计、Oracle 变量绑定审计。(提供功能截图并盖章)
日志模糊化	支持日志模糊化处理，保护访问数据安全。(提供功能截图并盖章)
日志查询	按访问的时间查询。
	按访问源查询：访问客户端 IP、客户端 MAC、客户端操作系统主机名、客户端操作系统用户名、客户端连接工具名、数据库用户名。
	按访问的目标查询：数据库 IP、数据库 MAC、数据库实例、表、列等。
	按操作类型查询。
	按 SQL 内容查询。
	按匹配的策略查询。
	按风险等级查询。
日志检索	支持检索条件保存功能。
	支持检索结果导出，导出文件格式 PDF、EXCEL、WORD。
会话回放	支持会话回放功能，还原用户的访问行为。
用户行为轨迹分析	以曲线连接多点的形式展示用户的访问来源、目标、操作的轨迹。
	支持轨迹定位到具体日志信息。
流量监控	支持实时的网络流量监控。
告警查询	支持以相同的规则进行告警日志汇总显示。
	支持以引擎的方式对进行告警日志汇总显示。
	支持以风险等级、匹配的策略、时间、其他操作条件对告警日志进行查询。
告警方式	支持告警日志外发至第三方日志平台，外发格式有 SYSLOG、SNMP、FTP、EMAIL、短信。
告警策略	支持自定义告警的等险等级，包括低风险、中风险、高风险三个等级。
告警处理	支持对误报的告警日志进行处理：禁用 SQL 注入规则。
攻击趋势	支持以图的形式显示风险趋势。
访问来源趋势	支持以柱状图的形式显示访问来源趋势。
访问量分析	支持以折线图的形式分析访问量的情况。
实时报表	支持系统内置报表模板形式的实时统计分析。
	支持可以根据需要再使用内置模板的情况下，设置检索条件进行实时统计分析。
	支持的内置报表模板不少于 10 个，可以从来源分析、执行时长分析、操作类型分析、登录情况等维度展示数据库的访问情况。
定时报表	支持系统内置模板的周期型报表。
	支持定时报表可以通过邮件形式外发。
	支持定时报表可以按照周期时间生成后发送。

运维审计	支持类型：TELNET、POP3、SMTP、IMAP、FTP、SSH、VNC 等主流协议的运维审计。
报表与查询	支持普通查询、模糊查询、明细查询、词组查询、流水号查询五种匹配命中方式，同时可叠加多达 27 种查询条件，其中包含会话语句种类、重复程度、耗时、数量、排除关键字及时段选择，查询结果支持多种格式导出。（提供功能截图并盖章）
	系统支持在线回档，并查看历史归档数据。可通过历史数据回档客户端，在不删除现有审计数据的情况下查询设备挂载已归档数据。同时，无缝衔接系统查询模块，支持在线对归档数据多条件组合查询。（提供功能截图并盖章）
漏洞扫描	支持类型：ORACLE、MSSQL、SYBASE、DB2、达梦 7、INFORMIX。
状态监控	支持类型：ORACLE、MYSQL、MSSQL、SYBASE、DB2、达梦 7。
敏感发现	支持类型：ORACLE、MYSQL、MSSQL、SYBASE、DB2、达梦、神州通用、INFORMIX、PostgreSQL、Gbase、Hive、MongoDB、Redis、cache、Kafka、MariaDB。（提供功能截图并盖章）
旁路模式	支持以交换机镜像方式对数据库进行审计分析。
集群审计	支持集群采集，采集数据丢包率小于万分之一，支持采集设备的横向扩展。
探针集管	支持多探针（Agent），自动部署、统一配置、集中管理及监控。（提供功能截图并盖章）
	支持以旁路情况下，在数据库服务器上、应用服务器上部署探针的方式对数据库进行审计。
双因子认证	支持对登录审计系统的用户进行双因子认证。（提供功能截图并盖章）
角色管理	支持三权分立的内置用户设置，不同用户负责产品不同模块的配置与使用。
	默认管理员可以根据自身的权限对新增用户进行授权。
	授权范围包括自身角色下的所有功能页面。
	可以针对某些功能页面进行授权。
备份还原	支持审计日志的全量备份。
	支持的备份方式有：手工备份、定时自动备份、自动远程备份。
	支持手工方式还原。
	支持备份文件手工清理。
配置管理	支持系统时间手工、自动与 NTP 服务器同步，保证审计日志时间准确性。
	支持接口配置、用户登录安全管理等。
升级	支持页面方式进行升级。
	支持不丢失配置情况下升级。
系统诊断	支持系统能够自动对审计进程、解析进程、存储进程、检索进程进行监控，方便用户排除故障。
磁盘使用率监控	支持磁盘使用率监控，当磁盘使用率达到预定的阈值时，页面弹框提示管理员。
系统状态监控	支持系统 CPU、内存、网络吞吐率、磁盘的使用率监控，支持磁盘的读写速率监控。
系统告警	支持系统 CPU、磁盘使用率超限告警。
系统磁盘清理	当磁盘使用率达到预定的阈值时，系统停止记录日志或者覆盖以前的记录。

## 附件 2：报价文件

### （一） 投标报价表（单位：元、含税）

日期：2023 年 月 日

货币单位（人民币：元）

产品名称	生产厂商	设备参数	数量	总价
数据库审计系统	知道创宇	标准机架式设备，配置不少于 4 个千兆电口，冗余电源。设备支持 ORACLE、MYSQL、MSSQL、SYBASE、DB2、达梦 6/7、人大金仓、神州通用、INFORMIX、PostgreSQL、Gbase、Hive、MongoDB、Redis、TeraData、cache、Kafka、ElasticSearch、HANA、MariaDB、Hbase、HDFS 等多种数据库类型；客户端 IP、源应用程序、主机名、系统用户名、客户端端口、客户端 MAC、数据库用户名、数据库 IP、列、数据库、操作对象、操作对象类别、操作类型、SQL 关键字、SQL 模式、SQL 结果内容、执行时长、删除行数、响应状态等。	1 套	
总价（大写）：				

注：

- 1、 报价应包含完成该项目全部评估服务涉及到的人力、交通、餐饮、食宿、各种税费以及支付给员工的工资和国家强制缴纳的各种社会保障资金等一切费用。
- 2、 报价应包含原厂商三年质保。

报价单位公章：

代理人(被授权人)签字：

（二）具体售后服务承诺和实现承诺的保障及相应措施：

（三）营业执照的复印件(加盖单位公章)

（四）原厂代理商授权书

（五）法定代表人授权书

本授权书声明        公司的        为本公司的合法代理人，代表本公司全权处理江苏靖江农村商业银行采购数据库审计系统的询价报价、合同的签订、执行、保修以及一切与之有关的事务。

本授权书于        年    月        日签章生效， 特此声明。

单位公章

法定代表人签字或盖章：

代理人(被授权人)签字或盖章：