版本号：V1

信息安全运维

（第 2 标段：云安全服务）

采购需求

北京市智慧水务发展研究院

2025 年 12 月

信息安全运维

（第 2 标段：云安全服务）

采购需求

说明：采购需求中标注★号指标为实质性要求，实质性要求任一项不满足的将被作为无效投标否决。★号标注在序号前，指本序号所有内容均为实质性要求；★号标注在段落前，指仅本段落内容为实质性要求。一、采购标的

★（一）标的名称

信息安全运维（第 2 标段：云安全服务）。

★（二）标的内容

本项目根据运行需求，针对北京市水务局在北京市市级政务云上运行的信息系统，提供满足系统运行所需要的云安全服务，保障北京市水务局信息系统的云上安全稳定运行。

在北京市市级云计算服务的基础上提供云安全服务，具体采购内容如下：

序号	服务名称	内容明细	单位	数量
1	云端 APT 防护服务	对未知攻击威胁进行检测和防护，发现隐蔽威胁、木马后门等异常威胁。	套	2
2	主机杀毒服务	对云主机进行定期的病毒查杀，杀毒软件集中控制，对网络性能无影响。	主机	277
3	主机安全加固	针对漏扫或等级测评结果对操作系统进行安全加固，用以解决等级测评结果中所显示的漏洞。	台次	554
4	主机漏洞扫描	为用户提供针对主机层面的安全扫描服务，并反馈相关结果。	台次	1108
5	主机日志审计服务	针对操作系统进行日志收集，并且进行分析，并将结果反馈给用户，用于了解主机安全情况及资源使用情况。	台次	554
6	数据库审计服务	支持 Oracle、SQL-Server、DB2、MySQL 等数据库审计。（1 套为 1 个数据库实例）。	套	27

（三）项目概况

为贯彻落实北京市经济和信息化局关于印发《北京市市级政务云管理办法的通知》（京经信委函（2019）150 号）文件的要求，我局现有信息系统北京市水旱灾害防御综

合指挥平台、水务综合信息平台及OA系统、智慧水务1.0基础底座（一期）、水务工程安全质量生态一巡三查管理系统、北京市河长制管理信息系统、北京市水务局外网网站、“取供用排”协同监管应用（一期）已部署至北京市市级政务云。系统网络涉及互联网业务、政务外网业务、水务专网业务等多种网络类型业务；服务对象有面向水利部业务、市水务局局属单位业务、区水务局业务、公众业务等，具有“业务系统数量多、面向服务对象多、网络类型复杂”等特点。

为有效保障上述系统的安全稳定运行，北京市水务局采购相关云安全服务，为入云业务系统提供动态灵活、安全可靠的政务云服务保障。

二、商务要求

（一）项目实施期限

项目实施期限：12个月。

（二）项目实施地点

项目实施地点：北京市。

（三）付款条件

1.付款进度

第一次付款：合同签订生效且财政资金拨付到位后，采购人收到供应商提供合格发票后10个工作日内，采购人向供应商支付合同总价款的50%作为首付款；

第二次付款：汛期运行维护服务结束后，供应商按要求提交标准格式汛期服务总结报告，且采购人在收到供应商合格发票后10个工作日内，采购人向供应商支付合同总价款的35%；

第三次付款：2026年12月31日前，采购人在收到供应商合格发票后10个工作日内，支付合同总价款的15%。

2.付款方式：转账支票或汇款方式。

3.付款要求：供应商必须在采购人支付每笔款项前提供符合税法规定并符合采购人财务要求的正规合法有效的税务发票，采购人收到上述发票后10个工作日内将款项支付给供应商，否则采购人有权暂不付款，并且不承担违约责任。

4.如采购人未收到财政资金而导致逾期向供应商付款的，则采购人不承担逾期付款的责任。在实际支付时，如遇财政部门国库结账等特殊情况，具体支付将根据财政部门有关要求调整执行，由此造成的支付迟延，采购人不承担任何责任。

5.前期费用

（1）本合同价款中包含2026年1月1日至本合同签订之日期间的维护费用，供应商在收到首付款后10日内，应将该费用支付给前期维护单位。逾期支付的，采购人有权在后续合同款项支付中予以扣减。

（2）前期维护费用按照以下标准计取：以本合同确定的各维护项目单价为准。

（3）前期维护费用的确定：前期维护费用由采购人按上述标准和实际发生工作量审定。

（4）供应商因支付前期费用产生的费用包含在本合同价款中，采购人不再另行支付。

三、技术要求

★（一）基本要求

1.采购标的需实现的目标

本项目根据运行需求，针对北京市水务局在北京市市级政务云上运行的信息系统，提供满足系统运行所需要的云安全服务，保障北京市水务局信息系统的云上安全稳定运行，包括应用、主机、数据等层面的相关安全，充分保障市水务局面向全市的水务服务可用性及连续性，提升水务服务质量。

2.需执行的国家相关标准、行业标准、地方标准或者其他标准、规范

（1）国家及北京市有关政策

《关键信息基础设施安全保护条例》（中华人民共和国国务院令第745号）；

《国家政务信息化项目建设管理办法》（国办发〔2019〕57号）；

《政府采购需求管理办法》(财库〔2021〕22号)；

《关于促进政府采购公平竞争优化营商环境的通知》（财库〔2019〕38号）；

《关于进一步提高政府采购透明度和采购效率相关事项的通知》（财办库〔2023〕243号）；

《工业和信息化部信息通信管理局关于督促互联网网络接入服务企业依法持证经营的通知》（工信管函〔2018〕84号）；

《云计算服务安全评估办法》（国家互联网信息办公室、国家发展和改革委员会、工业和信息化部、财政部公告2019年2号）；

《关于加强党政部门云计算服务网络安全管理的意见》（中网办发文〔2014〕14号）；

《基于云计算的电子政务公共平台顶层设计指南》；

《河北省财政厅 北京市财政局 天津市财政局关于印发<京津冀政府采购负面行为清单>的通知》（冀财采〔2024〕18号）；

《北京市财政局关于落实好政府采购支持中小企业发展的通知（京财采购〔2022〕1143号）；

《关于印发<关于推进我市政务信息系统整合共享的实施方案>的通知》（京经信委发〔2017〕89号）；

《北京市人民政府关于印发<北京市政务信息资源管理办法（试行）>的通知》（京政发〔2017〕37号）；

《关于印发<北京市市级政务云管理办法>的通知》（京经信函〔2019〕150号）；

《北京市政务网络和数据安全管理办法》（京经信发〔2023〕57号）；

《北京市“十四五”时期智慧城市建设控制性规划要求（试行）》（京大数据发〔2021〕2号）。

（2）国家相关标准

《国家电子政务外网安全接入平台技术规范》；

《信息技术—云计算—云服务质量评价指标》（GB/T 37738-2019）；

《信息技术—云计算—云服务计量指标》（GB/T 37735-2019）；

《信息技术—云计算—云服务采购指南》（GB/T 37734-2019）；

《信息技术—云计算—云存储系统服务接口功能》（GB/T 37732-2019）；

《信息技术—云计算—云资源监控通用要求》（GB/T 37736-2019）；

《信息技术—云计算—云平台间应用和数据迁移指南》（GB/T 37740-2019）；

《信息技术—云计算—云服务交付要求》（GB/T 37741-2019）；

《信息系统灾难恢复规范》（GB/T 20988-2007）；

《信息安全技术 云计算服务安全能力要求》（GB/T 31168-2014）；

《信息安全技术 网络安全等级保护定级指南》（GB/T 22240-2020）；

《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）；

《信息安全技术 网络安全等级保护测评要求》（GB/T 28448-2019）；

《信息安全技术 信息系统密码应用基本要求》（GB/T39786-2021）；

《信息安全技术 信息安全风险评估方法》（GB/T 20984-2022）；

《信息安全技术 云计算服务安全指南》（GB/T 31167-2014）；

《信息安全技术 政府网站云计算服务安全指南》（GB/T 38249—2019）；

《信息安全技术 云计算安全参考架构》（GB/T 35279—2017）；

《信息安全技术 云计算服务安全能力评估方法》（GB/T 34942—2017）；

《信息安全技术 云计算服务运行监管框架》（GB/T 37972—2019）；

《信息技术 云资源监控指标体系》（GB/T 37938-2019）；

《云计算关键领域安全指南 V4.0》。

（3）北京市相关标准

《政务云平台建设技术要求》（DB11/T 2169-2023）；

《北京市政务云安全技术规范 IaaS 云计算平台分册》；

《北京市政务云安全技术规范 IaaS 云计算平台安全监管接口分册》；

《北京市政务云安全技术规范 信息安全服务接口分册》；

注：服务标准涉及的国家标准及北京市标准有更新的，执行最新标准。

（二）具体要求

1.服务内容及要求

1.1 服务内容

（1）云端 APT 防护服务

提供对未知攻击威胁进行检测和防护，发现隐蔽威胁、木马后门等异常威胁。

（2）主机杀毒服务

提供主机杀毒服务，对云主机进行定期的病毒查杀，杀毒软件集中控制，对网络性能无影响。

（3）主机安全加固

提供主机安全加固服务，针对漏扫或等级测评结果对操作系统进行安全加固，用以解决等级测评结果中所显示的漏洞。

（4）主机漏洞扫描

提供主机漏洞扫描服务，包含但不限于主机层面、数据库层面、应用层面的安全扫描，并反馈相关结果。

（5）主机日志审计服务

提供主机日志审计服务服务，利用云主机日志审计服务技术对云主机日志进行分析、管理及合规性存储，增强云主机日志方面的监管能力。

（6）数据库审计服务

对入云业务系统的数据库进行日常操作审计，需支持 Tdsql、Oracle、SQL-Server、

DB2、MySQL 等数据库审计。

1.2 技术指标要求

（1）云端 APT 防护服务

指标项	技术指标要求
云端 APT 防护服务	提供基于云端的 APT 防护能力,对未知攻击威胁进行检测和防护，发现隐蔽威胁、木马后门等异常威胁，有效发现 APT 攻击中探测期、入侵期、潜伏期、退出期等不同阶段的安全攻击，具备 URL 异常检测、沙箱检测、异常流量分析等能力。 提供 APT 防护服务，实现恶意代码检测、恶意软件检测及攻击溯源。 无论已知还是未知恶意样本，后台都能提取出恶意行为的特征，形成特征库或策略库，并通过中心管理分发到前端。前端接收安全策略，对相应规则进行拦截，并形成整体防御体系。

（2）主机杀毒服务

指标项	技术指标要求
防病毒要求	提供基于云平台集成的杀毒软件，对云主机进行定期的病毒查杀，杀毒软件采用集中控制，云主机端无需安装代理软件，病毒库升级采取控制端统一下发的方式，对网络性能无影响。 采用轻量级 Agent 部署，无需依赖虚拟化平台 API 即可实现安全防护；客户端支持手动从控制中心获取安装，也可通过管理控制中心批量远程安装；客户端对 windows 类、linux 类的物理服务器、虚拟服务器、桌面云具备相同的防护和部署。产品应至少支持 VMware 、Ctrix、Microsoft 、Huawei、H3C、浪潮等国内外主流虚拟化厂商平台，并能够采用一个管理控制中心进行统一管理。

（3）主机安全加固

指标项	技术指标要求
安全整改与加固	支持对漏扫或等级测评结果对操作系统进行安全加固，用以解决等级测评结果中所显示的漏洞

（4）主机漏洞扫描

指标项	技术指标要求
扫描能力	支持 Windows、Linux 域扫描技术，利用域管理员权限使扫描更深入、更准确。
	支持大华、海康等视频监控类设备扫描。
	支持多种协议口令猜测，包括 SMB、Snmp、Telnet、Pop3、SSH、Ftp、RDP、DB2、MySQL、Oracle、PostgreSQL、HighGo、MongoDB、UXDB、STDB、kingbase、RTSP、ActiveMQ、WebLogic、WebCAM 等。
	支持设置口令猜测间隔 0-300 秒。
	支持对主流数据库的识别与扫描，包括：Oracle、Sybase、SQL Server、DB2、MySQL 等，支持对数据库漏洞进行扫描和修复。

资产管理	支持以 txt、csv、dat、xls 等格式进行资产列表的导入。
产品升级、维护	支持实时提醒当前的系统消息，包括报表下载消息、升级内容消息、日志下载消息等。 支持控制台功能，可以通过控制台对系统进行操作和设置，例如重启和关闭系统、修改系统和网络配置、查看漏扫引擎状态并提供网络诊断工具。

（5）主机日志审计服务

指标项	技术指标要求
日志采集	满足支持新增 Lotus Domino 的日志采集任务；新增 CheckPoint 的日志采集任务。
	日志审计中心可以集中对独立安装的日志采集器进行统一管理，能够对日志的解析策略进行统一下发。
部署要求	支持单级部署和级联部署，支持分布式部署。
资产管理	满足系统提供基于资产的拓扑视图，可以按列表和拓扑两种模式显示资产拓扑节点；可查看每个资产设备本身产生的事件信息、关联告警信息，并且支持向下钻取，直接进入事件列表、关联告警列表； 满足能够根据收到的事件的设备地址自动识别新的资产并自动添加到资产库中。
工作台	满足系统内置基本的仪表板。用户可以在工作台中自定义仪表板，按需设计仪表板显示的内容和布局，可以为用户建立不同维度的仪表板。 满足仪表板中的每个显示区域都能够放大、缩小、拖动。
日志管理	满足日志可加密压缩传输 支持加密压缩方式转发，定时转发。 满足支持日志源管理功能，对断点日志源可以产生告警。
日志范式化	满足范式化字段至少应包括事件接收时间、事件产生时间、事件持续时间、用户名称、源地址、源 MAC 地址、源端口、操作、目的地址、目的 MAC 地址、目的端口、事件名称、事件摘要、等级、原始等级、原始类型、网络协议、网络应用协议、设备地址、设备名称、设备类型等；针对不支持的事件类型做范式化不需改动编码，通过修改配置文件即可完成。 满足产品界面支持范式化文件的导入导出功能。
日志分析	满足系统需内置不同分析场景，包括各种实时分析场景、历史统计场景、实时统计等。并支持支持自定义场景。 满足可以手工对选中日志进行告警或者加入观察列表中。 满足自定义事件查询策略，基于事件类型的查询条件不少于 10 大项 50 小项。 满足可以对选中的日志提供在线/离线地图定位、视网膜图、事件拓扑图等多种分析工具。 可以显示一段时间的动态日志移动图，能够在图上显示每个时间切片的日志数量、等级，并能够在图上显示每秒事件数。用户点击每个时间切片，可以查看该切片内的日志。
关联分析	满足提供基于图形化方式的规则编辑器；规则可导入导出。

	满足在编辑规则条件的时候，可以针对事件属性引用规则、应用资产属性、引用资源。
综合显示	满足能够显示告警状态雷达图，日志趋势曲线图；最近事件览图；最近一段时间不同日志分类的日志数量，不同等级的日志的数量，事件 EPS 曲线。

（6）数据库审计服务

指标项	技术指标要求
审计协议	支持 Tdsql、Oracle、SQL-Server、DB2、MySQL 等数据库审计。
	支持高斯(Gauss)、人大金仓 KingBase、神通(OSCAR)、达梦(DM)、南大通用(GBase) 等数据库进行审计。
	支持 MongoDB、Redis、Hbase、hive、ES 等数据库进行审计。
	支持 FTP、Rlogin、Radius、NFS、X11 等协议审计。
审计能力与效果	系统应内置规则集，对数据库 DML、DCL、DDL 等语句及 FTP、Telnet 等协议中的命令进行归类，便于用户定制审计策略。
	审计策略支持时间、源 IP、目的 IP、协议、端口、登陆账号、命令作为响应条件。
	审计策略支持数据库客户端软件名称、数据库名、数据库表名、数据库字段名、数据库返回码作为响应条件（非正则表达式方式）。
	提供对数据库返回码的实时说明，帮助管理员快速对返回码进行识别。
	支持对数据库 DML、DCL、DDL 语句的审计。
	审计策略支持数据库客户端软件名称、数据库名、数据库表名、数据库字段名、数据库返回码作为响应条件。
	审计策略支持时间、源 IP、目的 IP、协议、端口、登陆账号、命令作为响应条件。
	支持对数据库绑定变量方式访问的审计。
	支持访问数据库的源主机名、源主机用户的审计。
	支持 SQL 操作响应时间的审计。
	支持 Select 操作返回行数和返回内容的审计。
	支持对超长 SQL 语句的审计。
	支持访问数据库的源主机名、源主机用户、SQL 操作响应时间、数据库操作成功、失败的审计。
	支持频次告警，某一操作在周期时间内达到设定的次数阀值即可告警，周期事件和次数可按需配置。
	支持数据库并发会话数、并发进程数、并发用户数、并发游标数、并发事务数、数据库锁等超过限制的审计。
	支持数据库操作类、表、视图、索引、触发器、存储过程、域、Schema、游标、事物等各种对象的 SQL 操作审计。
	支持 Telnet 协议的审计，能够审计用户名、操作命令、命令响应时间、返回码等。
	支持对 FTP 协议的审计，能够审计用户名、命令、文件、命令响

指标项	技术指标要求
	应时间、返回码等。
	支持审计网络邻居的用户名、读写操作、文件名等。
	支持审计 NFS 协议的用户名、文件名等。
	支持审计 Radius 协议的认证用户 MAC、认证用户名、认证 IP、NAS 服务器 IP。
	支持对针对数据库的 XSS、SQL 注入攻击行为进行审计。
	支持对 Oracle 数据库状态的自动监控，可监控会话数、连接进程、CPU 和内存占用率等信息。
业务关联审计	支持中间件环境下的 SQL 语句关联到 HTTP 操作，HTTP 操作关联到 HTTP-ID，实现中间件环境下的审计追溯。
	支持实时关联，实时显示关联结果，无需时候手动查询。
数据库异常行为审计	支持根据网络数据流自动建立数据库操作行为基线。
智能发现	满足数据库审计支持用户数据库中敏感信息的自动发现，方便针对敏感信息配置针对性的审计策略。
	满足敏感信息发现支持探测器和正则表达式两种方式，探测器至少包含：姓名、地名、银行卡、身份证、IP 地址、密码等多种探测器。
事件查询统计与报表	满足支持基于场景的操作异常分析；可直观展现数据库异常、异常账号的访问、同账号多 IP 登录、上下班操作量对比异常、操作响应时间分析。
	满足支持疑似暴力破解、疑似撞库攻击场景的操作异常分析；行为周期与阀值可按需定义。
	查询需支持返回全部符合条件的结果，无上限限制。
	可支持 sql 语句关键字查询,查询结果包含该关键字的 sql 语句。
第三方扩展接口与联动功能	支持与 Web 应用防火墙（WAF）的联动，可对 WAF 上报的应用系统攻击实现场景还原展示。
	支持与 APT 检测产品的联动,对于网络传输的文件不仅可以审计，还支持恶意代码检测，报告可疑的攻击文件。

2.服务标准

（1）供应商为采购人提供的服务质量应符合国家或相关行业的标准。

（2）供应商在服务期间，应根据采购人购买的安全服务清单，向采购人部署在北京市市级政务云上的应用系统提供持续性的安全防护服务及技术支持，保障云上业务及数据安全。

（3）服务响应率 100%。

3.为落实政府采购政策需满足的要求

（1）本项目不专门面向中小企业预留采购份额。

（2）根据《政府采购促进中小企业发展管理办法》（财库[2020]46 号），供应商

为小型或微型企业，价格给予 10%的扣除。

（3）根据《财政部民政部中国残疾人联合会关于促进残疾人就业政府采购政策的通知》（财库〔2017〕141 号），残疾人福利性单位视同小微企业。

（4）根据《关于政府采购支持监狱企业发展有关问题的通知》（财库〔2014〕68 号），监狱企业视同小微企业。

★（5）本项目采购产品必须为国产，不接受进口产品。

4.技术支持

（1）日常运维服务

供应商需利用监控系统或人工对采购人部署在北京市市级政务云上的应用系统的运行情况进行 7*24 小时的不间断巡检监控，及时发现安全风险，通知相关人员及时处理，并形成监控报告。

供应商负责设立技术支持热线，并安排专人值守，为北京市水务局提供 7*24 小时热线支持服务。

（2）故障响应服务

供应商应当提供高效的技术支持服务，有效防范系统风险，供应商需保持 7*24 小时电话畅通，工作时间内发生安全或故障事件时，能够协调技术人员在 10 分钟内响应，在 30 分钟之内处置完成；非工作时间 10 分钟内响应，技术人员 1 小时内到达运维现场提供服务，2 小时之内处置完成。故障处理完毕后提供相关系统事件分析处置报告。

（3）驻场服务（签订合同后提供具体人员，投标阶段不需提供）

供应商需根据采购人的云上业务运行管理要求，指定至少 2 名专业的技术能力较强的驻场工程师，配合采购人开展相关维护、策略开通服务，协助采购人开展政务云的日常运行管理工作。

（4）安全应急响应服务

提供安全专家应急响应服务，针对水务局日常运行或重保期间发生或可能发生的网络安全事件，提供安全专家应急响应分析，协助水务局进行安全事件排查及故障处置，提供安全事件分析报告。

（5）特殊时期保障服务

供应商应在春节、五一、国庆、汛期（6 月 1 日-9 月 15 日）以及全国（含北京）重大活动期间等重要时期安排至少 1 名驻场服务人员，到采购人处进行现场 7*24 小时值守，以确保政务云上信息系统在敏感时期安全稳定运行，通过日志分析、状态检测等

手段，及时发现潜在安全隐患或者突发安全事件，协助采购人完成隐患排查、应急事件的处置，提升采购人在特殊时期的安全保障能力。

（6）部署迁移服务

针对本项目，供应商应为采购人提供持续稳定的各项服务。如采购人中途更换其应用系统部署的北京市市级政务云平台，本项目供应商应根据采购人要求，在 5 个工作日内迁移其提供的各项服务到新的政务云平台，迁移过程中产生的所有费用由供应商承担。如供应商未在规定时间内完成服务迁移，采购人有权与其解除合同并要求其赔偿采购人相应损失。

如供应商提供本合同下相关服务需向北京市市级政务云部署相关采集、分析等设备或软件，供应商需自行与北京市市级政务云资产方和管理方协调软硬件设备进驻、部署、运行、维护等事宜，过程中产生的费用由供应商自行承担。

（7）安全培训服务

为有效提升市水务局在业务系统日常运行、管理中的安全防护意识，供应商需向采购人提供包括不限于政务云云安全、等保安全等相关的安全培训，培训次数不少于 1 次。

（8）管理咨询服务

供应商应为采购人提供其云上业务管理咨询服务，并有义务对现有政务云管理制度提出合理优化的建议，同时配合、协助采购人修订原有管理办法，并严格执行。

5.解决方案或者组织方案

（1）工作组织方案

1）云端 APT 防护服务

第一等次：制定了工作组织方案，包括工作方法及流程、时间安排、人员安排等主要内容；工作方法及流程清晰，关键点、重点明确，有利于项目实施保障；时间安排计划明确到具体时间；人员安排明确到具体人员，并明确了人员分工职责。

第二等次：制定了工作组织方案，包括工作方法及流程、时间安排、人员安排等主要内容；但工作方法及流程阐述简单，关键点、重点不明确，不利于项目实施保障；或时间安排计划未明确到具体时间；或人员安排未明确到具体人员，或未明确人员分工职责。

第三等次：制定了工作组织方案，但方案整体简单，工作方法及流程或时间安排或人员安排等主要内容有缺失。

第四等次：未制定工作组织方案，或存在不合理。

2）主机杀毒服务

第一等次：制定了工作组织方案，包括工作方法及流程、时间安排、人员安排等主要内容；工作方法及流程清晰，关键点、重点明确，有利于项目实施保障；时间安排计划明确到具体时间；人员安排明确到具体人员，并明确了人员分工职责。

第二等次：制定了工作组织方案，包括工作方法及流程、时间安排、人员安排等主要内容；但工作方法及流程阐述简单，关键点、重点不明确，不利于项目实施保障；或时间安排计划未明确到具体时间；或人员安排未明确到具体人员，或未明确人员分工职责。

第三等次：制定了工作组织方案，但方案整体简单，工作方法及流程或时间安排或人员安排等主要内容有缺失。

第四等次：未制定工作组织方案，或存在不合理。

3）主机安全加固

第一等次：制定了工作组织方案，包括工作方法及流程、时间安排、人员安排等主要内容；工作方法及流程清晰，关键点、重点明确，有利于项目实施保障；时间安排计划明确到具体时间；人员安排明确到具体人员，并明确了人员分工职责。

第二等次：制定了工作组织方案，包括工作方法及流程、时间安排、人员安排等主要内容；但工作方法及流程阐述简单，关键点、重点不明确，不利于项目实施保障；或时间安排计划未明确到具体时间；或人员安排未明确到具体人员，或未明确人员分工职责。

第三等次：制定了工作组织方案，但方案整体简单，工作方法及流程或时间安排或人员安排等主要内容有缺失。

第四等次：未制定工作组织方案，或存在不合理。

4）主机漏洞扫描

第一等次：制定了工作组织方案，包括工作方法及流程、时间安排、人员安排等主要内容；工作方法及流程清晰，关键点、重点明确，有利于项目实施保障；时间安排计划明确到具体时间；人员安排明确到具体人员，并明确了人员分工职责。

第二等次：制定了工作组织方案，包括工作方法及流程、时间安排、人员安排等主要内容；但工作方法及流程阐述简单，关键点、重点不明确，不利于项目实施保障；或时间安排计划未明确到具体时间；或人员安排未明确到具体人员，或未明确人员分工职

责。

第三等次：制定了工作组织方案，但方案整体简单，工作方法及流程或时间安排或人员安排等主要内容有缺失。

第四等次：未制定工作组织方案，或存在不合理。

5）主机日志审计服务

第一等次：制定了工作组织方案，包括工作方法及流程、时间安排、人员安排等主要内容；工作方法及流程清晰，关键点、重点明确，有利于项目实施保障；时间安排计划明确到具体时间；人员安排明确到具体人员，并明确了人员分工职责。

第二等次：制定了工作组织方案，包括工作方法及流程、时间安排、人员安排等主要内容；但工作方法及流程阐述简单，关键点、重点不明确，不利于项目实施保障；或时间安排计划未明确到具体时间；或人员安排未明确到具体人员，或未明确人员分工职责。

第三等次：制定了工作组织方案，但方案整体简单，工作方法及流程或时间安排或人员安排等主要内容有缺失。

第四等次：未制定工作组织方案，或存在不合理。

6）数据库审计服务

第一等次：制定了工作组织方案，包括工作方法及流程、时间安排、人员安排等主要内容；工作方法及流程清晰，关键点、重点明确，有利于项目实施保障；时间安排计划明确到具体时间；人员安排明确到具体人员，并明确了人员分工职责。

第二等次：制定了工作组织方案，包括工作方法及流程、时间安排、人员安排等主要内容；但工作方法及流程阐述简单，关键点、重点不明确，不利于项目实施保障；或时间安排计划未明确到具体时间；或人员安排未明确到具体人员，或未明确人员分工职责。

第三等次：制定了工作组织方案，但方案整体简单，工作方法及流程或时间安排或人员安排等主要内容有缺失。

第四等次：未制定工作组织方案，或存在不合理。

（2）项目管理人员组织安排

1）供应商拟派项目负责人的能力

第一等次：拟派项目负责人具有信息安全相关专业高级及以上技术职称或者信息系统项目管理师职业资格。

第二等次：拟派项目负责人具有信息安全相关专业中级技术职称或者信息安全工程师职业资格。

第三等次：其他。

注：需提供有效职称证书或信息系统项目管理师职业资格证书或信息安全工程师职业资格证书复印件或扫描件作为证明材料，信息安全相关专业以职称证书上写明的专业为准，未提供有效证明不予计分。

2）供应商拟投入本项目其他专业技术人员的能力（除项目负责人外）

第一等次：拟投入本项目其他专业技术人员中有信息安全工程师、网络工程师、网络规划设计师。

第二等次：拟投入本项目其他专业技术人员中有上述任意 2 类人员。

第三等次：拟投入本项目其他专业技术人员中有上述任意 1 类人员。

第四等次：其他。

注：需提供有效信息安全工程师职业资格证书或网络工程师职业资格证书或网络规划设计师职业资格证书复印件或扫描件作为证明材料，未提供有效证明不予计分。

（3）特殊时期保障服务方案

第一等次：制定了特殊时期保障服务方案，包括对特殊时期保障人员的安排、响应程序、对可能出现的安全隐患或者突发安全事件的预判与解决方案等内容；处置措施到位。

第二等次：制定了特殊时期保障服务方案，包括对特殊时期保障人员的安排、响应程序，但未对可能出现的安全隐患或者突发安全事件做出预判或未提出针对性的解决方案，或处置措施简单，保障性较差。

第三等次：制定了特殊时期保障服务方案，但方案整体简单，特殊时期保障人员的安排或响应程序有缺失。

第四等次：未制定特殊时期保障服务方案，或存在不合理。

（4）质量控制措施

第一等次：制定了质量控制措施，方案包括针对各项工作内容制定相应的质量控制方法和流程、时间安排、人员安排等主要内容；质量控制方法和流程阐述系统详尽，关键点、重点突出，有利于项目实施保障；时间安排计划明确到具体时间；人员安排明确到具体人员，并明确了人员分工职责。

第二等次：制定了质量控制措施，方案包括针对各项工作内容制定相应的质量控制

方法和流程、时间安排、人员安排等主要内容；但质量控制方法和流程阐述简单，关键点、重点不明确，不利于项目实施保障；或时间安排计划未明确到具体时间；或人员安排未明确到具体人员，或未明确人员分工职责。

第三等次：制定了质量控制措施，但方案整体简单，各项工作内容制定相应的质量控制方法和流程或时间安排或人员安排等主要内容有缺失。

第四等次：未制定质量控制措施，或存在不合理。

（5）资源配置计划

第一等次：项目实施所需工器具及设备配置充足，且工器具及设备具有智能、先进等特点，能提高工作质量和效率。

第二等次：项目实施所需工器具及设备配置满足需求，但工器具及设备智能、先进性不足。

第三等次：项目实施所需工器具及设备配置满足需求，但比较落后。

第四等次：未提供项目实施所需工器具及设备，或不满足项目需求。

（6）保密方案及保障措施

第一等次：结合项目组织实施，制定了有效的保密制度，明确重点、难点，并提出保障措施。

第二等次：结合项目组织实施，制定了有效的保密制度，但没有明确重点、难点及保障措施。

第三等次：制定了保密制度，但未与本项目实施结合，针对性差。

第四等次：未制定保密制度，或存在不合理。

（三）验收标准

供应商应于合同履行期结束后的 15 个工作日内向采购人提交项目验收申请及项目验收材料，经采购人审核后组织召开双方参与的会议，汇报年度服务情况和合同执行情况。

项目验收材料包括但不限于以下内容：项目合同、周期报告、工作总结报告、验收申请报告等。采购人检查验收材料，对运维情况进行评价，并出具正式的验收意见。项目验收通过后，供应商应按照档案归档要求整理验收资料，并将资料移交给采购人。验收不合格的，由供应商按要求弥补缺陷后再次组织验收，直至验收合格。

具体验收方案见合同履约验收方案。