|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 设备名称 | 单位 | 数量 | 控制总价 |
| 1 | 数据库服务器 | 台 | 5 | 205000 |
| 2 | 主存储设备 | 台 | 1 | 255000 |
| 3 | 光纤交换机 | 套 | 2 | 60000 |
| 4 | 外网核心交换机 | 台 | 1 | 12000 |
| 5 | 网闸 | 台 | 1 | 50000 |
| 6 | 内网安全管理及审计系统 | 套 | 1 | 42000 |
| 7 | 机柜及KVM等 | 批 | 1 | 6000 |
| 8 | 系统集成及机房搬迁 | 项 | 1 | 20000 |
| 合计 | | | | 650000 |

特别说明：参数前面打“★”为必须满足项，不满足的业主有权废标。

1. 数据库服务器

|  |  |
| --- | --- |
| 技术规格 | 机架式,2U配置2个Intel Xeon E5-2620V4处理器  本次配置128GB DDR4内存 32G \*4  2块600GB 10K SAS 2.5”热插拔硬盘  最大可扩展到≥8个PCIe插槽,以满足多配置4 个1 GbE；可选的 10/40 GbE ML2 或 PCIe 适配器；配置2块8GB单口HBA卡；内置可信平台模块,配置DVD光驱  MS Windows Sever 2008 、Red HatEnterprise Linux 和 SUSE Enterprise Linux 、Vmware ESXI Server  2冗余电源  ★合同签订前提供所涉及产品原厂商针对本项目专项授权和原厂盖章的服务承诺函 |

1. 主存储设备

|  |  |
| --- | --- |
| **项目** | **技术指标** |
| 品牌 | 具有自有知识产权和开发能力产品，非OEM； |
| 体系结构 | 一体化统一存储架构，同时支持并提供NAS、IP SAN和FC SAN模式；全冗余模块化体系结构；统一存储池架构支持LUN、VVOLs及NAS 服务器，分别提供数据块和文件访问服务；以上均需提供官网链接证明； |
| 控制器 | 控制器部件全冗余，支持NAS、FC、iSCSI数据访问服务；  控制器对称双活，双控制器能同时访问同一个份数据单元（LUN）；  1、控制器数量≥2；存储配置缓存96GB；  2、每控制器CPU≥8核，主频≥2.4GHz；  3、基于控制器的静态数据加密； |
| 磁盘存储容量 | 本次磁盘配置：15块1.2TB 10K SAS硬盘； |
| 二级缓存 | 所投存储系统可同时支持eMLC SSD、3D NAND TLC SSD；SSD单盘最大可支持3.2TB，以上需提供官网链接证明； |
| 前端主机端口 | 支持接口类型：  最大支持的FC端口≥20；  最大支持的10Gb iSCSI端口≥24；  本次配置4个16Gb/s的前端FC光纤通道端口+4个万兆电口IP接口； |
| 后端端口带宽 | 配置磁盘阵列连接磁盘的后端端口带宽≥192Gb/s，投标时提供详细技术说明 |
| 高可靠性 | 完全的硬件冗余：处理器、缓存、电源、风扇、适配卡、总线等都提供冗余，并保证在某硬件出问题时，能够进行自动切换，不出现单点故障，磁盘阵列系统具有高可靠性，达到99.999%可用性； |
| RAID保护方式 | 支持多种RAID保护方式，包括0/1,5,6；提供官网链接截图说明 |
| 扩展能力 | 具有完全在线、无需停机的扩充能力，包括系统微码升级、系统处理能力的扩充、存储容量的扩充等； |
| 支持的协议和功能 | 配置并支持以下协议及功能：   1. 数据块协议：iSCSI、光纤通道； 2. Internet控制消息协议（ICMP）； 3. Kerberos身份认证； 4. LDAP轻型目录访问协议； 5. REST API实现存储网络之间的数据自动、透明移动 6. 锁定管理器（NLM）v1、v2、v3、v4   以上6点协议及功能需要提供官方链接及截图说明 |
| 存储控制器软件 | 配置主存储控制器软件的独立运行版本，支持Windows、Linux、Unix操作系统，配置SAN、NFS、CIFS、iSCSI与VVOLs协议，配置自动存储分层功能，配置存储复制功能，能够与此次所投存储实现复制，配置服务质量管理QoS功能；配置不小于4TB的容量许可；以上均需提供官网链接证明； |
| 性能分析软件 | 配置阵列的性能分析软件，能够获取实时的性能数据和历史性能数据；产生性能报表； |
| 虚拟资源调配 | 支持并配置虚拟资源调配功能，按照实际使用的存储容量分配存储空间，提高存储利用率； |
| 磁盘降速 | 在磁盘没有IO访问的情况下，能够智能的将磁盘处于停止状态，从而降低系统对能源的消耗； |
| 服务质量管理(QoS) | 通过优化磁盘阵列中的应用程序IO队列，实现对应用程序的IOPS、带宽和响应时间的控制优化； |
| Vvol配置 | 配置vvol支持，支持数量≥9000 |
| ★连续性数据保护 | 配置vmware虚机连续数据保护软件，当虚机需要恢复时，用户可从时间点中选择，使指定虚机能够快速地以IO粒度从任一时间点恢复。此功能需与vCenter无缝集成，可以在vSphere客户端中完成虚机连续数据保护的所有操作，实现VM任意时间点恢复，并通过VMware Vcenter统一管理VM连续数据保护；  1、与VMware深度整合，可通过vSphere client发起对任意虚机的保护（提供截图说明）通过vCenter管理所有保护虚机，策略及恢复，无需额外界面及软件  2、快速创建VM保护策略截图说明；  3、本次要求配置不少于15个for vm的许可，要求提供原厂工程师现场安装服务。 |
| 数据迁移 | 要求存储系统配置具有内部数据迁移功能的软件；基于存储系统本身的控制器实现数据在不同逻辑卷之间、不同RAID类型的卷之间数据迁移，且无需中断应用访问； |
| 配置迁移工具，将存储系统中的数据在不同厂商的磁盘阵列中进行数据迁移，并且保障业务零中断。 |
| ★数据同步复制功能 | 要求配置存储系统RPS容灾软件一套包含服务与软件使用许可。要求配置本次新购存储系统的数据同步复制软件和许可与原存储实现数据底层复制，不接受网关模式，并要求提供原厂工程师现场服务，负责两套存储之间的容灾实施工作。 |
| 数据通道安全(负载均衡/链路切换) | 配置通道管理软件，实现对主机的多通道路径访问以及对应用透明的自动故障通道切换及负载均衡，具备在SAN环境中的负载均衡功能； |
| ★容灾技术支持 | A、需支持基于数据块级远程复制功能，以实现基于存储设备的灾备数据复制及恢复；配置同步/异步复制软件许可；  B、配置支持虚拟机数据复制技术，要求能够实现跨机房的虚拟机复制技术，提供详细说明以及截图说明  到货后需通过厂商官方800验证以上软件的正版性 |
| 支持操作系统 | 磁盘阵列能提供对主流操作系统的支持：能够同时支持SUN Solaris、HP-UX， IBM AIX， Linux， windows操作系统，支持服务器集群功能； |
| 服务与授权 | 提供原厂商软件与硬件3年原厂7\*24服务，合同签订前提供所涉及产品原厂商针对本项目专项授权和原厂盖章的服务承诺函，并可通过原厂800/400服务热线查询服务期限； |

1. 光纤交换机

|  |  |
| --- | --- |
| **指标项** | **技术参数要求** |
| SAN交换机 | 支持8Gb/s 4Gb/s自适应传输速率  24端口光纤交换机，当前激活端口数≥16口，每台配置16个8Gb/s SFP模块，每台SAN交换机配置1个端口为25km长距模块及 License许可，配置相应的光纤线支持ZONE分区提供图形化管理和操作界面，支持命令行及Web界面，提供端口配置功能，提供自我诊断功能，配置冗余电源 |

1. 外网核心交换机

|  |  |
| --- | --- |
| **指标项** | **技术参数要求** |
| 3层交换机 | 4端口千兆电+4端口千兆光，以太网路由交换机（1个Console口，24个千兆电口，4个千兆SFP光口；标配电源AC220V；1U高度，标准19英寸机架式安装） |

1. 网闸

|  |  |
| --- | --- |
| **项目** | **技术参数要求** |
| ★系统架构 | 采用“2+1”系统架构，即由两个主机系统和一个隔离交换专用硬件组成，隔离交换矩阵基于专用芯片实现，保证数据在搬移的时间内，内、外网隔离卡与内、外网系统为物理断开状态 |
| 通过国家下一代互联网信息安全专项（高性能安全隔离与信息交换系统）测试，提供相关测试报告, 加盖原厂商公章 |
| 系统要求 | ★内外网主机系统分别支持多系统引导（大于或等于三操作系统，即A,B,备份系统），并可在WEB界面上直接配置启动顺序，在A系统发生故障时，可以随时切换到B系统；且支持系统备份，提供功能截图加盖原厂商公章 |
| 主机系统采用具有自主知识产权的多核多线程ASIC并行操作系统平台 |
| ★规格接口与性能 | 标准1U机架式设备，内、外网各标配5个10/100/1000M Base-TX网络接口，共10个千兆接口；共4个USB口；内、外网主机系统分别具有独立的管理口、HA口（热备口）；内、外网主机系统分别具有1个RJ45 CONSOLE口； |
| 系统吞吐量不小于90Mbps, 并发连接数不小于2万,延时小于1ms |
| 系统监控 | 支持设备健康状态实时自我检测，如散热系统状态，并能够进行正常/异常状态指示(非液晶屏显示)，且能在异常状态下进行声音报警 |
| ★设备具有液晶面板实时显示设备工作状态及配置信息,提供设备面板照片加盖原厂商公章 |
| 强制访问控制 | 支持基于动态令牌的双因子认证方式，提供功能截图加盖原厂商公章 |
| 支持WEB认证方式和专用客户端两种认证方式 |
| ★可对用户的操作系统和进程进行检查，进行准入控制，提供功能截图加盖原厂商公章 |
| 功能模块 | 支持文件交换、FTP访问、数据库传输、数据库同步、邮件传输、安全浏览、安全通道、消息传输等基本功能； |
| ★支持文件交换IPv4、IPv6双协议栈接入，提供产品功能界面截图证明及国家权威部门针对IPV6环境适用性相关功能的检测报告 |
| 支持文件传输长度及MD5校验，并支持校验失败自动重传，提供功能截图加盖原厂商公章 |
| 支持文件格式特征过滤，并且不依赖于文件扩展名；支持文件类型检查可扩展模式，方便用户自主增加特定文件类型，并提供工具帮助用户识别不常见文件类型 |
| 支持字段级数据库间的单向或双向同步（不改变用户的库结构）。支持同步库中初始数据功能； |
| ★支持安全浏览模式下网页下载文件类型过滤；支持非法网站识别及过滤技术，详细描述技术实现原理，提供权威机构证明材料加盖原厂商公章 |
| 支持灵活的数据库冲突处理策略，当关键字数据发生冲突时可选择：覆盖/丢弃，提供功能截图加盖原厂商公章 |
| 支持数据容错处理，当数据同步失败时，用户可以查询、复位、删除未能正常传输的数据。 |
| 支持数据库同步客户端的双机热备技术，为用户提供更高的冗余技术支持 |
| 支持数据库SQL语句过滤功能。 |
| 支持FTP协议命令的黑白名单控制； |
| 支持对邮件附件大小进行控制；支持附件格式过滤； |
| 邮件收发支持时段访问控制；时间段可以是一次性执行、周循环两种方式 |
| 支持客户端与网闸间的第三方数字证书方式的身份认证，确保只有被授权的合法用户才能运行，提供功能截图加盖原厂商公章 |
| 病毒检测 | 可扩展支持病毒检测专用模块，支持自动/手动两种升级模式 |
| ★采用高级的网关级病毒防护引擎，包括病毒检测引擎和病毒分析引擎，要求详细说明技术实现原理，提供权威机构证明材料加盖原厂商公章。 |
| 采用专用国产知名病毒库。 |
| ★入侵检测功能 | 支持实时入侵检测功能，实现网络入侵特征配制方法及系统技术可设置自动阻断响应的技术，请详细描述技术实现原理，出示权威机构证明材料加盖原厂商公章 |
| 抗DDoS攻击 | 支持抗DoS、DDoS攻击功能 |
| 安全管理 | 支持HTTPS的Web方式管理，实现了远程管理信息加密传输； |
| 支持配置文件以加密的方式导出 |
| 防暴力破坏限制 | 支持系统防爆处理，对管理员登陆有密码次数限制，密码输入错误，超过限定次数，自动锁定设备，阻止非法管理员再次登录。根据限定期限，可自动解除锁定。 |
| 高可用性 | 通过独立的热备端口实现双机热备； |
| 支持抢占模式 |
| 支持配置同步，提供功能截图加盖原厂商公章 |
| ★支持与多台网闸实现负载均衡，无需第三方软硬件支持，具备一种集群模式下实现网络安全设备高可用性的相关技术，请详细描述技术实现原理，出示权威机构证明材料加盖原厂商公章 |
| 支持主、备状态实时展示 |
| 日志审计 | 支持全中文日志显示，并能实现内外网主机日志同步 |
| 日志实现按功能模块分组管理 |
| 实现对日志的浏览、查询、导出、删除等操作 |
| 支持FTP方式上传日志，提供功能截图加盖原厂商公章 |
| 日志支持远程存储，能为第三方提供日志格式，实现日志数据分析；支持SysLog标准 |
| 支持图表实时显示网口流量、CPU状态、内存状态信息； |
| 资质与服务要求 | 具备公安部《计算机信息系统安全专用产品销售许可证》（三级）； |
| 具备《军用信息安全产品认证证书》军B级 |
| 具备公安部信息安全产品检测中心检测报告（三级）； |
| ★考虑到产品的成熟度和稳定性，要求该产品生产厂商从事网闸产品研发生产时间超过12年，提供产品上市第一年的公安部销售许可证书影印件证明，并加盖原厂商公章； |
| ★考虑到产品先进性，要求提供国际权威调研机构出具的最近连续三年国内市场占有率前三名的市场报告，并加盖原厂商公章 |
| ★要求设备生产商具有信息安全应急处理服务一级资质； |
| ★合同签订前提供所涉及产品原厂商针对本项目专项授权和原厂盖章的服务承诺函 |

1. 内网安全管理及审计系统

|  |  |
| --- | --- |
| **指标项** | **技术规格参数** |
| 性能指标 | 客户端数量：200 |
| 适应能力 | 客户端操作平台：支持Win2000、WinXp、Win2003、Vista、Win7、Win8、Win2008 |
| 客户端平台架构：支持x86和x64 |
| 网络结构：支持工作组、NT域 |
| 客户端接入方式：支持有线、无盘工作站、无线（3G等）终端 |
| 安全防护功能 | 1. 设备监控   支持对主机常用外设（光驱、软驱、移动硬盘、磁带机、红外线设备、蓝牙设备、1394控制器、串行口、并行口、MODEM、无线网卡、PCMCIA卡、声卡、人体学设备等）进行监控 |
| ★2.刻录监控  支持对光盘刻录操作进行实时监控与审计，要求能审计刻录机型号、光盘名称、光盘属性、文件路径、文件名、文件类型、文件大小等（提供界面截图） |
| 1. 文件监控   支持对固定磁盘（硬盘或光驱）和移动盘（如移动硬盘、移动光驱、U盘等）的所设定的文件类型的文件操作进行实时监控与审计 |
| ★4.文件防护 （提供界面截图）   1. 支持根据策略对文件和文件夹进行新建、读、写、删除、重命名的防护 2. 支持自定义文件类型进行防护 3. 文件路径和文件夹路径能支持环境变量 |
| 1. 进程监控   支持通过设计审计的白名单进程策略和违规的黑名单进程策略进行应用进程审计和违规软件管理 |
| 6.打印监控  通过对打印机（同时支持网络打印机、共享打印机、本地打印机）打印资料行为进行授权或监视；  支持禁止主机的打印功能，也可对打印行为进行审计；  支持详细记录远程主机的IP地址、打印资料名称、打印时间、打印页数、打印份数、打印结果等； |
| 7.准入控制  准入控制包括非法主机接入控制及代理主机准入控制   1. 非法主机接入控制，同时提供ARP监控、SNMP监控、802.1X认证等三种方式，防止终端未经授权接入安全内网造成信息涉密 2. 代理主机准入控制对安全内网的代理主机进行安全性检查，包括操作系统环境检查、杀毒软件检查、上网代理软件检查以及基于进程、文件和注册表自定义组合条件策略的P2P软件、游戏软件、即时聊天软件检查等，对不符合安全条件的代理主机进行发现并隔离 |
| 1. 外联监控   采用主动防御方式对使用MODEM拨号、无线网卡等手段违规进入互联网的行为进行监控，严防“一机两用” |
| ★9.网络防火墙监控（提供界面截图）   1. 需要支持基于传输层（TCP/UDP）和网络层(IP)的主机防火墙功能，可对ARP包、IP包（包括ICMP、TCP、UDP协议等）以及应用层域名进行防护和监控，实现基于进程的网络行为的细粒度监控 2. 防火墙具有支持时间策略功能（可配置上下班不同时间段防火墙策略） 3. 防火墙能手动指定协议号进行监控配置 |
| 安全运维功能 | 1. 资产管理   资产管理包括对安全内网中可网管设备的管理及终端主机的硬件、软件资产管理   1. 系统能自动收集安全内网中包括终端主机在内的可网管设备及其相关信息，同时提供手工的配置功能供管理人员对设备进行标识（如设备位置、密级、使用人等），对终端主机可供管理的信息包括主机位置、所属部门、使用人、密级、主机IP地址、主机MAC地址、主机名、机型、硬盘系列号等 2. 系统能自动收集代理主机的硬件、软件资产，并能报告资产的变更（增加和减少）情况。其中硬件资产包括设备型号、设备名称、制造商、驱动商、硬件ID、出厂系列号等；软件资产包括程序组、程序名、菜单位置、软件版本、出版商、安装路径、安装时间等 3. 系统提供相关资产的查询、统计及报表输出功能 |
| 2.性能监控  实时监控内网终端主机的CPU利用率、内存利用率、网络流量（入口流量、出口流量和总流量），可对监控字段进行排序，方便管理员发现异常行为主机，快速定位并排故障 |
| 1. 远程协助   首先由代理主机端发起远程协助请求，管理员根据请求发起远程桌面协助请求，由代理主机端确认允许后管理员方可进行远程桌面协助，同时也提供网络聊天方式方便管理员与代理主机用户进行对话 |
| 安全审计 | 1. 资源审计   审计主机的CPU（含CPU利用率）、内存（含内存利用率）、磁盘（含磁盘空间使用情况）等资源信息 |
| 1. 设备审计   审计主机的所有设备信息（类似于系统设备管理器） |
| 1. 进程审计   审计主机所有进程信息（类似于系统进程管理器），可以查看进程和SOCKET通信绑定端口的关联情况，作为诊断木马或后门程序的辅助工具 |
| 1. 共享审计   审计主机所有共享目录信息 |
| 1. 用户审计   审计主机操作系统的所有用户和用户组信息 |
| 移动存储管理 | 1.移动存储设备管理  具有移动存储设备管理，对通用移动存储设备（含普通的通用U盘）从注册、使用、销毁整个生命周期提供完整的授权、控制和管理   1. 注册授权：移动存储介质在使用前需要经过注册中心统一注册授权，注册时可以写入注册授权信息，包括密级（普通、秘密、机密、绝密）、注册日期、所属部门、责任人、使用人等。 2. 访问控制：能一键禁用未授权的通用U盘的使用，不需要复杂配置；对已注册授权过可信移动存储介质依据预设的策略进行访问控制 3. 数据粉碎：在移动存储使用过程中，为保证重要资料的安全删除，可对存储设备上的文件进行安全删除，安全删除过的文件不可恢复；同时也可以根据需求做全盘销毁删除 4. 审计跟踪：对移动介质的入库登记、授权使用、违规操作、文件访问等提供详细日志审计功能   e) ★ 自我保护：经授权注册的移动存储设备需要提供完善的自我保护措施，如下：  口令破解限制：打开注册的移动存储设备可以设定认证口令，当输入口令的错误次数达到设定值时，将自动锁定（提供界面截图）；  使用次数限制：使用次数达到设定值时,将自动锁定（提供界面截图）；  使用期限限制：可设定移动存储设备到期时间，超出到期时间将自动锁定（提供界面截图）；  加密要求：移动存储管理需要采用高强度加解密算法和TTDS算法实现全盘数据加解密，采用一卡一密的算法保证移动存储介质的身份唯一性和数据存储的安全性； |
| AP监控功能 | ★1.无线热点监控功能   1. AP监视功能：能够发现拥有无线网卡的客户端主机附近的无线热点信号，能监控到AP的SSID、MAC、距离、频带等信息，可手工标注AP信息（提供界面截图） 2. AP控制功能：能够对客户端主机进行AP访问授权控制，管理员可配置主机能够访问的AP白名单策略，对于没有授权的AP热点将无法访问并生成告警信息（提供界面截图） |
| 日志管理 | 1. 主机系统日志   支持获取主机本身的操作系统日志，实时获取主机上的安全日志、系统日志、应用程序日志 |
| 1. 系统审计日志   安全审计员可查询系统管理员或操作员的操作日志 |
| 1. 报表打印   具有灵活的日志查询及实用的报表输出及打印功能 |
| 1. 日志数据参数   a)支持设置日志数据保存的天数，超出保留天数则自动删除  b)支持设置日志数据空间报警阀值参数，剩余空间达到报警阀值后自动产生告警信息，并按百分比自动删除数据 |
| ★电子文档粉碎功能 | 支持对文件、目录及整个移动介质进行粉碎，客户端主机用户能右键直接使用粉碎功能，实现被删除的文件在磁盘中的数据块进行彻底清理、覆盖，使其无法还原（提供界面截图） |
| ★联动功能 | 支持与SOC产品实现联动，以达到禁止非法访问控制（提供界面截图） |
| 产品资质  （出具加盖厂商公章的复印件） | 具备国家版权局颁发的《软件著作权登记证书》 |
| 具备公安部颁发的《计算机信息系统安全专用产品销售许可证》 |
| 具备国家保密科技测评中心颁发的《涉密信息系统产品检测证书》 |
| 具备中国人民解放军信息安全测评认证中心颁发的《军用信息安全产品认证证书》 |
| 厂商资质  （出具加盖厂商公章的复印件） | 厂商具备ISO20000、ISO27001和CMMI 3级或以上证书 |
| 厂商必须具备中国信息安全认证中心（ISCCC）颁发的应急处理服务资质 |
| 具备中国信息安全认证中心（ISCCC）颁发的信息系统安全集成一级资质 |
| 具备中国信息安全评测中心颁发的信息安全服务资质证书 |
| 为省级或省级以上计算机信息网络安全协会指定服务单位 |
| 服务 | 合同签订前提供所涉及产品原厂商针对本项目专项授权和原厂盖章的服务承诺函 |

1. 附件

|  |  |
| --- | --- |
| 机柜及KVM等 | 服务器机柜1个及1个KVM等 |

1. 系统集成

|  |  |
| --- | --- |
| **指标项** | **指标要求** |
| 系统集成服务 | 1. 完成现有的数据库服务器双机双柜整合。 2. 完成现有的虚拟化服务器双机双柜整合。 3. 迁移现有的HIS系统到新的双机双柜平台。 4. 完成包括服务器虚拟化的整体虚拟化平台建设，包括虚拟平台的搭建以及相关系统的P2V迁移。 5. 完成整个存储平台的整合，消除HIS、LIS、EMR系统数据库的存储单点故障，完成本地硬件容灾平台的建设，提高整体基础架构可靠性和稳定性。确保单台存储故障不会导致业务的中断。 6. 完成三大系统(HIS、LIS、EMR)的数据库系统的应用级容灾系统的搭建，以及其它系统的同构平台的数据容灾系统的搭建工作。 7. 完成整体虚拟平台的备份，确保数据安全，并要求整个备份工作在可控的备份窗口内完成，不影响日常业务。 8. 容灾系统的调试，保障整个系统无单点故障，在HIS系统的两台服务器和两台存储的集群系统中，保障在任意时刻无论是服务器还是存储出现故障不会影响HIS系统的使用。 9. 容灾系统的调试，保障整个系统无单点故障，在PACS系统的两台服务器和两台存储的集群系统中，保障在任意时刻无论是服务器还是存储出现故障不会影响PACS系统的使用。 10. 容灾系统的调试，保障整个系统无单点故障，在EMR系统的两台服务器和两台存储的集群系统中，保障在任意时刻无论是服务器还是存储出现故障不会影响EMR系统的使用。 11. 要求系统集成商除完成以上各平台的搭建、调试、迁移外，另提供三年的技术支持服务，确保各个系统的可用性和故障的快速解决，在整个项目实施过程中需要确保业务系统的正常稳定运行，任何发生的业务非正常中断和数据丢失均由系统集成商负责。 |