第六章　　用户需求书

采购人（海南省人民检察院）对投标单位在本次招标采购的要求如下：

1.项目名称：海南省人民检察院2018年统一业务应用系统等软件运维项目

项目编号：

总体说明

本项目的服务内容包含一是统一业务应用系统、检委会子系统、网上信访系统、电子卷宗、统计系统、案件信息公开等高检院下发的软件的运维，含四名技术工程师的驻点省院运维，二是全省27个检察院使用的信息发布系统、龙信使邮件、政务、日志的升级和维护。三是服务对象为海南省检察机关全体干警。

2 项目周期

本项目的运维时间为自合同签订日起一年。

3.服务内容

3.1 运维范围清单

本项目软件运维范围包括已上线运行的业务系统。具体运维范围如下清单:

序号	类别	应用软件系统名称	备注
一、已上线运行的业务系统			
1	最高人民检察院研发软件	统一业务应用软件	
2		案件信息公开系统	

3		网上信访系统	
4		AJ1203 统计系统	
5		电子卷宗应用系统	
6		案件信息公开系统	微信版
7		统一业务应用软件统计子功能	
8		统一业务应用软件执检模块	
9		全国检察机关队伍管理系统	
10		数据交换平台	
11	本省检察机关软件	案件管理系统	
12		行贿犯罪档案查询系统	
13		政务系统	
14		信息发布系统	
15		安全邮件系统	
16		全文检索系统	
17		工作日志管理系统	

3.2 总体服务内容

3.2.1 驻场技术支持服务

★针对本项目，安排驻场工程师 4 人提供基本的 5*8 小时的驻场技术支持服务，提供日常运维问题处理，如驻场工程师无法解决的问题将升级后台专家处理。

★1、提供 5*8 小时的基本响应服务；

5*8 小时响应用户服务请求、服务监督，每一个服务都有相关的记录，客服专员对处理结果反馈给用户相关负责人。

2、日常问题处理服务

驻场工程师对全省业务系统在使用过程中的问题反馈、问题跟踪和问题处理。

3、问题升级处理

现场运维人员不能解决的问题由运维单位总部技术支持团队负责协助指导处理，若系统 bug 或用户新需求，现场运维工程师需详细描述问题或需求文档，并提供省院信息中心项目负责人确认，同时协助省院项目负责人将该问题及需求反馈给系统提供方，仍需积极配合信息中心项目负责人跟踪反馈的问题最后处理结果，对客户反馈的问题最终形成闭合环。

4、驻场运维人员要求：

具有中华人民共和国国籍；政治立场坚定，在思想上政治上行动上以习近平同志为核心的党中央保持高度一致；遵纪守法，爱岗敬业；驻场省检察院的运维人员至少要有一名拥有最高人民检察院印发的统一业务相关内容培训证书,有培训资格证书的运维人员不能更换，必须驻点运维到合同结束；

★5.能力要求：运维人员应当通过掌握统一业务系统及其子系统、数据交换平台的部署原理以及维护配置工具使用方法，掌握 Oracle、达梦等数据库的操作，应当了解检察机关组织机构以及基础的业务知识，经测试合格后方能上岗。如未能通过能力测试视为违约。

3.2.2 二线技术支持服务

故障发生后，经过驻场运维工程师的初步处理及判定，如确实不能满足用户方服务响应要求，驻场工程师将向总部技术团队提出支持的服务请求。

二线技术支持团队主要职责如下：

1、 接受一线的服务支持请求、及时与用户联系，对事件进行查明、记录、归类与支持。

2、 对用户事件进行电话支持，电话中不能解决的，需在约定时间内到达用户现场，为用户提供专业服务，并将工作相关情况与服务台进行沟通交流。

3、 事件终止后提供事件的有效记录以便一线能够能够提高事件处理技能。

3.2.3 重要时刻专人值守服务

当用户举行重大活动或发生重大系统事件时，将根据事件的紧迫性，派有经验的技术工程师赶赴现场协助用户处理，重大事件可包括不限于以下内容：

重大灾难：当发生不可抵御的自然灾难，如火灾、地震、洪灾等事件时，将组织项目组第一时间赶赴现场协助用户尽力恢复系统和数据,将损失降低到最低；

重大安全事故：当 IT 系统出现重大安全事故如泄密、越权访问等，第一时

间派经验丰富的技术工程师第一时间赶赴现场，对系统进行分析、排查，利用专业工具在最短的时间内追溯到发生重大安全事故的源头。

在重要关键时刻，包括重大会议期间、业务重大割接、网络中断、机房断电或其它任何可能对业务运营产生重大影响的时刻，我公司可为客户提供重要时刻的专人有限次现场值守支持。

当发生重大事件时，根据应急管理办法，驻场运维人员第一时间反馈，由省院运维负责人视影响程度决定是否启动应急预案，一旦应急预案启动，将安排技术人员现场协助处理，具体服务流程根据应急响应流程执行。

3.2.4 节假日值守服务

逢国家节假日（周六、日及其它法定节假日）期间提供技术支持服务。

如节假日用户加班需要提供技术支持的，节假日期间安排至少 1 个工程师值班，响应级别如下：

确保节假日期间电话属于可随时接通状态。

首选通过电话、邮件等方式远程解决问题故障。

如确有必要需要现场提供技术支持，工程师将在 2 小时内赶到现场解决。

3.2.5 定期巡检服务

由驻场工程师提供定期巡检服务。

1、对运维范围清单内的应用业务系统硬件服务器状态、数据库服务器状态、数据库存储情况进行巡检，并做好巡查记录及报告，同时需将巡检结果报省院信息中心备案。

2、对所有系统的的应用服务、中间件进行检查，确保系统正常运行。若发现有报错及时反馈、及时跟踪，及时解决并查明报错原因。

本项目的巡检方式为每日常规巡检和季度深度巡检，每季度对维护系统进行现场预防性检查，并于每季度的前 15 天内向用户提交上一季度《XX 系统季度巡检报告》。

3.2.6 技术培训

技术培训服务主要由驻场工程师提供，主要为系统使用操作培训，同时公司根据用户需求提供专项技术培训。根据海南省院统一安排计划，定期或不定期开展专项远程培训、现场培训（重点针对新增功能、常见问题总结及解决方法等）。

3.2.7 软件更新升级

★根据检察院各个应用系统的升级发布情况，结合海南检察机关实际需求及要求，对运维范围内的本省检察机关软件(第 11-第 17)应用业务系统提供软件更新升级服务，更新升级先在测试环境验证，驻场工程师须将每次升级包的测试情况汇报省院具体负责人，由双方协商是否升级，由运维工程师编写升级计划、升级步骤、升级预案等文档报省院信息中心领导及负责人批准后，运维工程师协助发布升级通知，最后安装计划进行系统升级并验证测试。

3.2.8 系统后台协助管理

目前各个系统均采用了分级管理模式，系统中新增人员、人员调岗、重置账号密码、人员授权等操作由各院系统后台管理员操作，运维工程师需提供技术支持，协助各院系统后台管理员完成上述工作。

3.2.9 主动响应服务

运维工程师可以开展现场回访或远程回访模式，进一步了解各个系统在应用中的问题及现状，交流分享运维过程中经验及不足，加以改进、以秉承“做用户最贴心的信息系统服务伙伴”，实现和谐共赢的服务。

3.2.10 遗留问题处理

本运维项目中，因软件系统本身开发设计缺陷，而驻场人员无法解决的遗留问题，需要申请二线开发人员处理。

3.2.11 运维统计和报告

将每日的系统运维记录在运维管理系统中，内容包括：服务时间、服务对象、运维内容、处理情况、运维类别分类以及运维各数据统计。每个月的 30 号或 31 号对《xx 月份运维统计.xls》进行数据统计，然后将该报告发送省院信息装备处领导。每个月 5 号前根据高检院要求报送统一系统运维月报。每季度要形成《xx 季度运维报告.doc》并上报给省院信息装备处。

3.2.12 应急响应服务

紧急故障应急措施应以快速恢复客户使用为目标，第一时间将使用状态恢复到正常，避免或尽量减少因故障而导致的损失。整个应急服务包含了应急预案管理、应急处理措施、启动应急流程及成立应急处理小组以及处理过程等几大部分，由于系统提供商家不同，应急服务需要大家共同协助，积极响应，才能第一时间完成应急需求。

3.2.12.1 应急预案管理

1. 培训

（1）根据受训人员和工作岗位的不同，选择培训内容，制定培训计划。

（2）培训内容：鉴别异常情况并及时上报的能力与意识；如何正确处理各种事故；与上下级联系的方法；紧急状态下如何行动，保密内容培训。

2. 演练

按照假设的事故情景，组织进行现场实际演练，将演练方案及经过记录在案。

3. 大力协助

由其他公司的提供的软件，需要省院协助要求第三方软件方提供驻场工程师的应用培训，需要对软件的常见问题及系统维护提供应用培训及指导。

3.2.12.2 应急处理措施

3.2.12.2.1 应急处理原则

1. 一旦发生灾难，由应急负责人主导：首先确保人员安全；其次保关键设备、数据安全；三是保一般设备安全。
2. 人员疏散的程序是：运行人员立即按响火警警报，并通过 119 电话向公安消防请求支援，所有人员戴上防毒面具，所有不参与灭火的人员按照预先确定的线路，迅速从机房中撤出。
3. 人员灭火的程序是：首先切断所有电源，启动自动喷淋系统，运行人员戴好防毒面具，从指定位置取出泡沫灭火器进行灭火。
4. 人员若在疏散时如有受伤情况，立刻拨打 120 电话向近邻的医院请求支援。

3.2.12.2.2 应急解决办法

1. 软件问题

驻场人员立即诊断软件故障，查明原因。属于操作类的立即解决；属于软件本身 BUG 问题，立即向信息中心汇报，并协助信息中心向最高人民检察院相关部门或研发单位汇报。

2. 高端技术问题

驻场人员无法排除的故障，需要及时汇报省院信息，同时求助软件提供厂家。

3. 设备故障解决办法

配合硬件供货商和硬件运维单位解决问题，备份数据、恢复数据。

4. 重大灾难

对于重大灾难，包括火灾、水灾、地震等重大灾难，运维单位尽力协助用户解决。

3.2.12.3 启动应急流程

当驻场运维服务人员收到通知，判断该问题属于重大事故时，则启动应急处理流程。重大事故包括以下几种情况：

- 大范围系统中断；
- 区域性系统崩溃；
- 关键业务中断；
- 大范围病毒爆发；

- 系统严重破坏；
- 数据严重破坏。

根据重大事故的紧急程度和状态不同，驻场运维人员可采取以下方式启动应急流程：

- 当紧急事件发生时，运维人员首先要进行故障分析，确定故障的范围和程度，确认为紧急故障的，在查找原因和解决问题的同时，要同步将故障解决情况通报给部门领导、及向客服中说明事件发生的状况。如需其他部门协助的，需要请求相关部门共同尽快解决故障。
- 对于病毒突发事件，当病毒大面积地感染终端，投标人的现场服务人员将已感染的终端从局域网中断开，投标人的运行人员将第一时间收集病毒信息，并向现场人员提供有针对性的应急方案；如果应急方案没有效果，要立即和杀毒软件厂方联络，由双方共同协同提供有效的应对措施。
- 对于网络中断事件，运维人员首先要判断中断原因，如果是局域网本地设备或线路造成的，依网络运行处理流程优先快速处理；如果是电信服务提供商造成的，要立即联络电信技术部门解决问题。
- 对于系统故障事件，运维人员首先要启用备用系统，再判断故障类型：硬件损坏、操作系统故障、软件故障。硬件损坏的情况，首先向服务器供应商报障；操作系统故障多数情况都和硬件故障同时出现，处理方式相同；软件故障如果是由购买的软件造成的，立即向软件厂商寻求技术支持；如果是运维单位自行开发的软件，立即向相关人员联系并排除故障。
- 对于自然灾害性事件，运行管理人员要尽可能将设备转移到安全地带，将损失降低到最少。
- 对于电力中断事件，由于机房多采用 UPS 防止断电带来的系统停机现象，在 UPS 还能供应电力期间恢复供电，对系统使用不会有影响；但遇到特殊情况导致供电部门在短期内不能恢复供电时，如有备用发电设备要启用备用发电设备供电，否则要关闭所有设备，确保突然断电造成设备损坏。
- 在故障排除之后，运行管理人员要填写故障记录，如果故障是由于项目实施中存在的隐患造成的问题，具体操作请参见上层文件《网络系统维

护管理指引》。故障记录汇总到“系统运行故障记录表”，重大事故由故障处理人填写故障报告。

3.2.12.3 成立应急小组

《启动应急流程申请单》获批准后（包括口头批准），由信息主管部门负责组建应急小组。应急小组由多方人员组成，例如信息中心代表、运维代表、供应商代表以及其他第三方人员等。

应急小组对发生的重大事故进行讨论分析并制定应急处理方案。

3.2.12.4 应急处理过程

运维人员根据应急小组制定的应急处理方案具体实施应急处理活动，并将实施过程和结果记录在《应急处理过程记录》中。涉及到客户现场服务的应取得客户的签字确认。

应急处理实施过程中涉及需要协调配合的工作由服务主管填写《资源申请单》，说明需要获得的资源、需要协调配合的工作等，经应急小组审批通过后由相关人员代表配合实施。

应急处理实施过程中涉及需要采购的，由服务主管填写《资源申请单》，说明需要采购的产品名称、型号/规格/功能、厂商/供应商、费用等。《资源申请单》经应急小组审批通过后由运维工程师实施采购，并将采购过程和结果记录在《资源申请单》中，应急小组对采购结果进行确认。

应急处理实施过程中涉及需要变更的，由服务主管填写《变更请求表》，说明变更内容、变更原因、变更方案等，经应急小组批准后直接由运维工程师根据《变更请求表》中的变更方案实施变更，并将变更过程和结果记录在《变更日志》中。

所有应急处理活动均应记录在《应急处理过程记录》中。

3.2.12.5 应急处理结果评估

应急处理过程完成后，服务主管向应急小组提交应急处理过程相关表单，包

括《启动应急流程申请单》、《应急处理过程记录》、《资源申请单》、《变更请求表》、《变更日志》等。应急小组对应急处理结果进行评估和确认，并在《应急流程评估单》中填写评估意见。

如果应急小组评估意见为达到要求，则应急流程结束。

如果应急小组评估意见为未达到要求，则由应急小组讨论分析原因，根据分析结果可采取以下措施：

- 如果需要继续进行应急处理，则由应急小组提出应急处理方案，进行应急处理过程；
- 如果不需要继续进行应急处理：
  - ✓ 如果有新的问题产生，则由服务主管填写《运维工作单》，转【问题管理】流程处理；
  - ✓ 如果有新的变更需求，则由服务主管填写《变更请求单》，转【变更管理】流程处理；
  - ✓ 否则应急流程结束。

应急流程结束时，由服务主管在《运维工作单》中记录应急处理结果及关联表单编号。配置管理员对应急处理结果进行检查，登记新的配置项或更改后的配置项。

3.2.12.6 统计和报告

由助理每月或每季度对应急流程情况进行统计，形成《应急流程管理报告》，并提交给服务主管。《应急流程管理报告》内容包括：启动应急流程次数（不同类别的次数）、原因分析、影响分析、完成情况、所需时间、各项资源利用情况、费用情况、意见和建议等。

《应急流程管理报告》经服务主管确认后提交数据部。

3.2.13 用户方安排的其它相关工作

派驻运维工程师驻点于用户现场，接受用户方安排的其它相关工作，相关工作包括但不局限于：

－协助检查和更新用户单位服务器存储资产表、整理维护用户单位台账记录；

－针对当前安全形势，向客户发送安全公告；

－协助开展专项保密检查服务；

－协助业务系统迁移改造；

－运维服务体系的持续改善。

运维工程师接受用户安排的其它相关工作，在现场值守过程中，用户方在权限、技术材料、相关人员方面提供必要的配合。

3.3 已上线系统针对性服务

已上线系统包括高检院研发软件运维和本省检察机关软件运维。

3.3.1 高检院研发软件运维

3.3.1.1 统一业务应用软件运维

3.3.1.1.1 日常运维

依据《关于加强统一业务应用系统日常运行维护工作的通知》，日常运维主要包括服务器主机系统、应用系统的监控、存储备份系统、数据维护、交换平台的监控、全省检察机关的统一应用软件的应用咨询、软件终端维护等等。

3.3.1.1.1.1 服务器监控

1) 服务器硬件状态监控

在服务过程中，运维工程师通过服务器的外部状态灯对服务器的硬件状态进行检查，以便及时发现服务器的硬件故障（很多故障无法从服务器的应用方面反映出来，例如 RAID5 中磁盘损坏），通过硬件状态检查，现场值守运维工程师都需要对服务器的硬件状态进行监控，以避免由于硬件故障导致的服务中断、数据损坏与丢失。

2) 服务器设备事件管理服务

根据服务器的情况制订相应的事件管理文档，由现场值守运维工程师对服务

器发生的事件进行记录、跟踪与分析，通过对事件的分析，及时发现服务器中存在的潜在问题，并进行解决或提出相应的解决方案。

3）服务器性能监控

每天由现场值守服务人员根据制定的性能监测模板对服务器的性能监控，监控的参数为服务器的 CPU、内存、硬盘和网络，并根据各服务器的应用情况，分析出服务器性能的基本基准线。

4）服务器应用维护

服务器应用服务包括统一业务应用软件平台的连接，解决应用服务连接的健康状态，当使用或连接出现任何问题时，维护人员负责对故障的排查，并与管理中心维护人员联系，共同查找业务系统使用过程中的故障情况，并即时排除，在维护过程中现场维护人员将做好维护记录和解决方法记录。

5）服务器进程与服务检查

服务人员定期对关键服务器的进程与启动的服务进行检查，以达到对服务器进程与启动服务的管理，对发现的异常的进程或增加的进程进行检查，以及时发现服务器中存在的安全问题。

6）服务器磁盘空间监控

对服务器的磁盘空间进行监控，通过估算出相应服务器磁盘空间的增长率，对服务器的磁盘能力与本地存储（服务器自身存储）或外部存储（如果有磁盘阵列等外部存储设备）的划分提供有效的数据，并对引起磁盘空间增长的程序进行相应的设置，以避免磁盘空间过渡增长等问题的发生。

7）系统配置与变更管理

- 服务器设备、操作系统、数据库、应用系统资料整理，配置参数整理；
- 根据系统的特点分别设计相应的系统配置管理文档，并建立系统配置管理文档；
- 当系统配置发生变更时，及时更新发生变更的系统配置，保持系统配置文档与实际设备配置的一致性。

3.3.1.1.1.2 统一业务应用软件运维服务应用维护

1） 应用服务 ICE 状态服务检查：每天检查应用服务 ICE 状态是否正常，确保统一业务应用软件正常运行。没有启动的服务，要立即启动，并查明

关闭的原因。

2） 统一业务应用软件后台维护

后台维护主要包括单位后台管理、案件后台管理、权限管理等。

- 单位后台管理包括部门管理、用户管理、密码管理；
- 案件后台管理涉及处理案件流程节点回退，案件超期预警处理、文书内容模板等等；
- 权限管理是根据用户生成的系统应用申请对相应的人员进行授权；

3） 统一业务应用软件业务咨询解答

- 解答承办人在统一业务应用软件流转案件的过程中所遇到的操作问题咨询；
- 处理承办人在统一业务应用软件流转案件的过程中所遇到的问题；
- 收集承办人在统一业务应用软件流转案件的过程中所遇到的问题并上报给省院相关领导及高检院运维中心；

4） 终端运维服务

终端用户运维服务主要包括系统使用操作问题、日常问题答疑、故障处理等。

- 用户终端的基础环境安装，如 office、pdf、.net 等等；
- 用户终端客户端安装及登录，客户端是否自动升级成功等等；
- 用户终端客户端使用异常，如打开系统报错，打开文书报错等等；

3.3.1.1.1.3 存储备份系统

3.3.1.1.1.3.1 存储备份系统监测

- 健康检查：每次磁盘阵列完成开机后要进行健康状态检查，在日常的维护工作中也需要定期对磁盘阵列的运行状况进行健康状态检查；
- 检查存储池容量的使用情况；
- 检查调度的作业是否按照正常执行。
- 检查 ftp 文书存储空间使用情况。

3.3.1.1.1.3.2 存储系统数据备份

为保证海南省检察机关业务数据的安全，建议省院购买专业的备份软件，采用专业的备份体系，并将手动备份与自动备份相结合的方式，利用全备份和增量

备份相结合技术策略实现业务数据备份，并根据业务数据的重要性，采取不同的备份频率

3.3.1.1.1.4 数据库维护

数据库管理服务范围包括最高检统一业务软件支撑系统中运用到的数据库系统。

（1）数据库系统定期巡检维护，包括：

- 每日系统状态监控和预警、系统日志检查；
- 每季度垃圾数据处理、清理日志等。

（2）数据库系统环境的故障响应、诊断与解决，核心系统故障隔离。

（3）数据库系统配置的调整优化，系统迁移等。

（4）数据库系统的配置文件和配置信息备份管理。

（5）技术文档管理。根据运维需要，及时总结技术维护文档，并对技术文档进行动态更新、管理。

3.3.1.1.1.5 交换平台监测

1. 对 ORACLE GOLDENGATE 的日志、进程、数据同步进行监测，以及数据交换平台是否正常运行

3.3.1.1.2 专题培训服务

根据海南省院统一安排及部署，针对全省检察机关使用统一业务应用系统实际应用情况，组织专题培训和疑难解答，解决干警使用中普遍存在的问题。

- 新进干警操作技能专题培训；
- 该软件升级内容进行专题培训；
- 对干警共性问题进行专题培训；

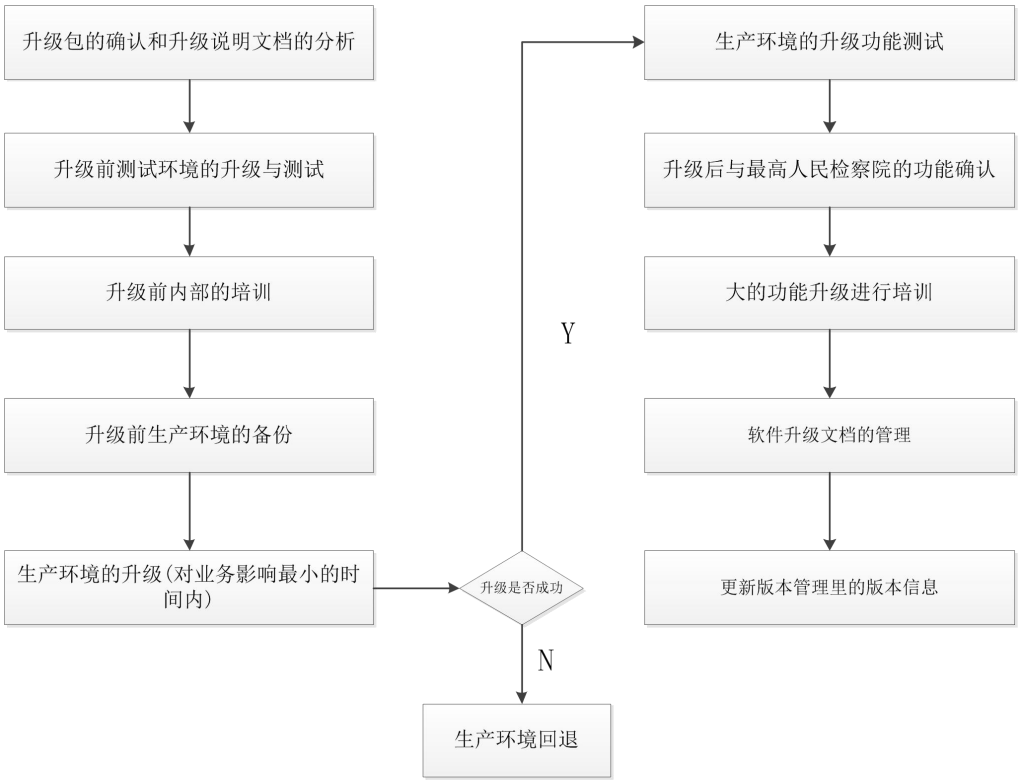
3.3.1.1.3 软件升级服务

3.3.1.1.3.1 软件升级范围

软件升级服务范围包括最高检统一业务应用软件的升级服务，同时也包含海南省检察院特色业务应用的升级发布。

3.3.1.1.3.2 软件升级服务流程

软件升级服务按如下流程进行升级。



1) 先查看和确认高检发布的补丁包和升级说明。
2) 将升级说明提交省院项目负责人审批。
3) 省院项目负责人审批通过后，根据升级说明编写具体详细的升级步骤。
4) 测试版系统停止服务，对测试系统应用程序和数据进行备份；
5) 按照升级步骤和升级方法进行升级测试系统，同时对照升级步骤进行整理调整为正式升级准备详细文档。
6) 测试系统升级完成后，进行系统验证。是否升级成功，验证系统升级之后与高检发布的系统升级解决问题是否一致。向省院汇报测试升级情况。
7) 编写《xx 升级计划》和《升级内容及解决问题说明》发布正式升级通知，并协助省院将《升级内容及解决问题说明》发布到内网，让全省干警了解本次升级内容及解决问题说明。
8) 发布正式升级前的最后通知，然后停止统一业务系统应用服务。
9) 备份数据库数据、备份应用服务数据等系统数据。
10) 按照升级文档对正式系统进行升级。正式升级完成后，启动系统应用服

务。

11) 登录系统检查是否升级成功。如检查插入 uKey 是否能登录系统、是否能查询到数据及数据是否准确，是否能打开案件，查看案件信息等等。

12) 发布统一业务系统升级完成通知，向领导汇报正式升级情况。

13) 升级完成后，需要紧跟升级后的运行情况，实时将升级后的运行情况汇报省院项目负责人。

3.3.1.1.4 需求管理服务

对全省各级人民检察院提出的需求进行汇总、整理，形成需求报告报海南省人民检察院相关部门，并协助进行后续处理。

- 整理、汇总全省检察机关对统一软件使用中提出的业务需求，汇总形成需求报告；
- 协助海南省检察院将需求报告提交最高人民检院相关部门；
- 海南省检察机关特色业务应用需求调研，制作需求报告；
- 需求任务管理，跟进后续处理过程，形成闭环的需求管理服务。

3.3.1.1.5 定期巡检服务

对本项目建设内容在有维护责任期内，每月软件运维和硬件运维一起进行一次月检查并形成运维月报报省院项目负责人，定期巡检的主要内容有，需要对运维中的各个系统服务器、应用系统和省院对应的部门进行现场回访、跟踪近期系统应用情况，驻场运维服务情况等多项现场运维跟踪及总结，以确保系统运行的稳定性、可靠性和安全性，形成巡检报告报省院项目负责人。

3.3.1.1.6 故障处理服务

3.3.1.1.6.1 故障事件级别

针对故障事件引起的后果，针对系统非网络、硬件及软件原因出现故障，定义了四级故障事件，具体的故障事件等级定义如下：

故障事件等级	事件描述
一级故障事件	应用服务器、数据库服务器同时或其中之一，出现宕机、性能严重下降或无法访问等故障，使应用系统不能对外提

	供服务，用户在线业务工作无法进行。
二级故障事件	应用系统使用时出现主要业务流程或模块无法正常运行，严重影响用户在线业务工作。
三级故障事件	应用系统使用时出现操作性能受损，个别非主要业务流程或模块出现功能错误，但大部分在线业务工作仍可正常工作。
四级故障事件	应用系统能够正常运行，但仍需要优化完善。本级故障事件对用户在线业务工作几乎无影响，或根本没有影响。

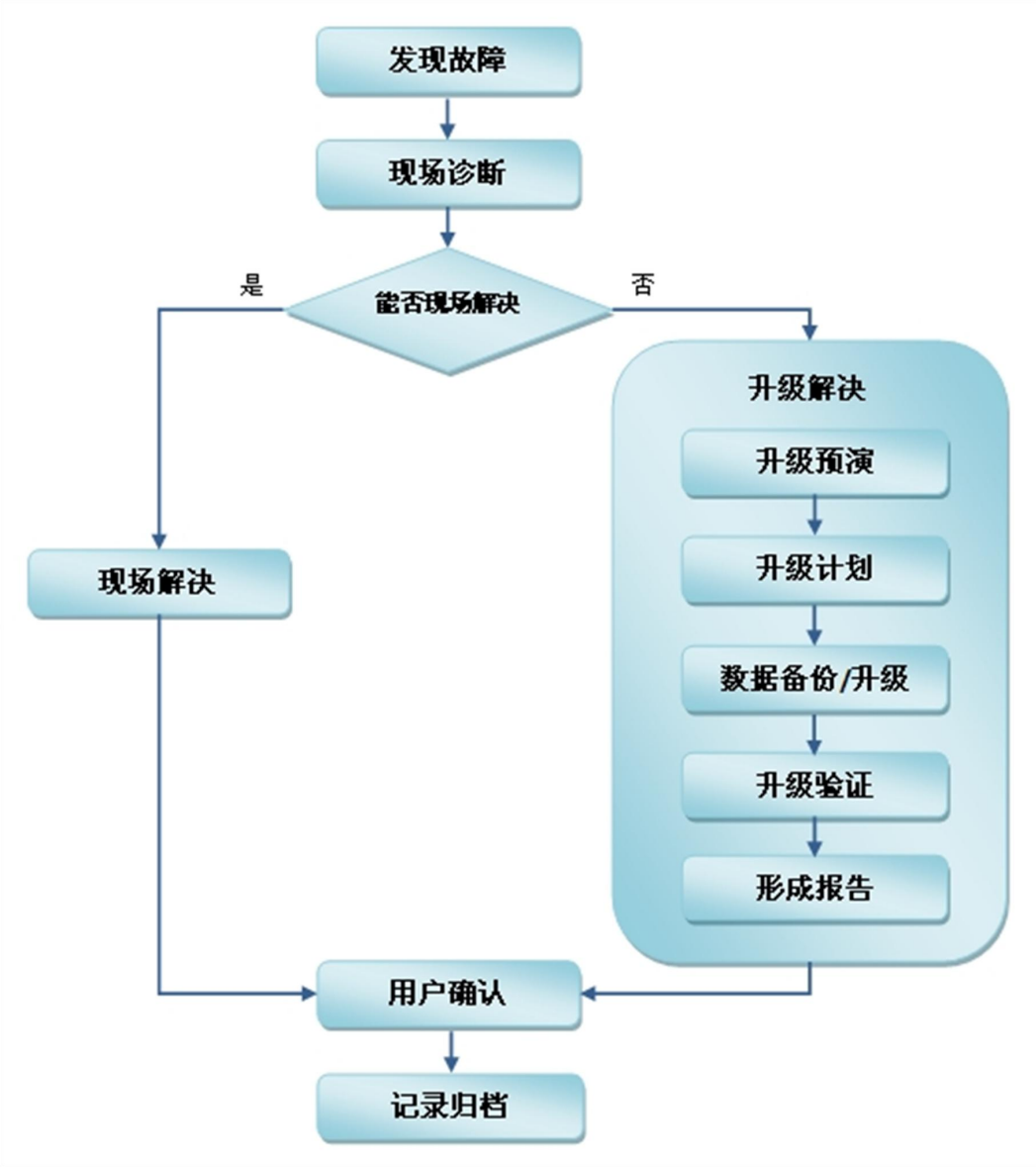
3.3.1.1.6.2 故障响应时间

针对本项目维护要求及结合故障事件级别，各级故障事件的最晚响应时间、解决时间如下表：

故障事件等级	最晚响应时间	最晚解决时间
一级故障事件	30 分钟	24 小时
二级故障事件	30 分钟	24 小时
三级故障事件	30 分钟	8 小时
四级故障事件	30 分钟	8 小时

3.3.1.1.6.3 故障处理流程

针对本项目运维服务，制定如下故障处理流程：



3.3.1.1.6.4 故障处理服务承诺

系统在运行过程中出现故障或异常时，或是在巡检过程中发现系统存在故障隐患时，将提供如下服务：

- 在维护期内将提供免费上门维护服务，并在第一时间赶赴现场进行查看分析，并对系统进行现场维护服务，如果现场无法维护，维护人员将告知用户最快的系统脱机维护时间；
- 针对应用系统宕机、数据丢失、业务使用中断等，驻点维护人员争取在最短时间内恢复业务系统，将损失降到最低；
- 在第一时间直接为客户提供必要的技术支持，确定问题所在并解决问题，如下级单位出现故障，根据省院的安排，驻点人员前往故障点处理；

- 日常工作时间 5*8 小时驻点服务，工作时间之外的采取 7*24 小时值班制度。

3.3.1.2 案件信息公开系统

根据高检院的部署要求，案件信息公开系统在海南省于 2014 年 9 月正式上线，运维内容包括：

积极协助省院开展案件信息公开工作，积极协助应用、保障系统运维及升级该系统等工作。

3.3.1.3 全文检索系统

全文检索系统运维内容包括：

1）法律文书查询，确保在统一业务应用系统中能够正常查询法律文书及数据完整。

2）协助全省应用推进，跟着用户反馈问题，并及时将反馈的问题进行整理汇总，报省院相关部门确认。

3.3.1.4AJ2013 统计系统

AJ2013 统计系统运维内容包括：

1） 积极配合协助案管处使用全省检察机关应用 AJ2013 系统。

2） 问题收集处理：收集用户反馈的问题以及需求进行整理并提交省院相关负责人确认。

3.3.1.5 电子卷宗应用系统

电子卷宗系统运维内容包括：

1） 电子卷宗导入

解决或者收集无法将电子卷宗资料上传至电子卷宗系统的问题

2） 电子卷宗导出

解决或者收集无法将从统一业务应用系统中将电子卷宗导出的问题。

3） 电子卷宗系统后台管理

电子卷宗系统后台管理包括部门管理、人员管理、人员权限管理、参数配置等等。

4） 电子卷宗系统升级优化

将升级包对海南省电子卷宗系统按照升级文档进行升级优化。

5） 维护电子卷宗系统正常运行。

定期的对电子卷宗应用服务器和数据库服务器进行检查，包括 cpu 使用率、物理内存使用、磁盘使用情况等等。

6） 协助全省应用推进，跟着用户反馈问题，并及时将反馈的问题进行整理汇总，报省院相关部门确认。

3.3.1.6 全国检察机关队伍管理系统

队伍管理系统运维内容包括：

1） 维护队伍管理系统稳定运行。

定期的对队伍管理应用服务器和数据库服务器进行检查，包括 cpu 使用率、物理内存使用、磁盘使用情况等等。

2） 队伍管理系统后台管理

队伍管理系统后台管理包括部门管理、人员管理、人员权限管理、参数配置等等。

3） 协助全省应用推进，跟着用户反馈问题，并及时将反馈的问题进行整理汇总，报省院相关部门确认。

3.3.1.7 网上信访系统

网上信访系统运维内容包括：

1） 维护网上信访系统稳定运行。

定期的对网上信访应用服务器进行检查，包括 cpu 使用率、物理内存使用、磁盘使用情况等等。

2） 系统升级优化

根据高检院和省院的部署安排，按照升级文档对网上信息系统进行升级。

3.3.2 本省检察机关软件运维

3.3.2.1 案件管理系统运维

海南省检察机关案件管理系统运维内容有：

1) 检务外网监所业务维护

保障运维检务外网监所业务系统正常运行同时需要保障该业务的统计汇总数据的稳定性、准确性等。

2) 协助历史数据查阅

协助海南省检察机关领导及干警对该系统历史数据的查阅。

3.3.2.2 行贿犯罪档案查询系统运维

海南省行贿犯罪档案查询系统运维内容包括：

1) 省级行贿犯罪档案数据库维护。

2) 省级行贿犯罪档案查询系统应用管理维护。

3) 省级行贿犯罪档案系统数据交换平台维护。

4) 省院行贿犯罪档案查询系统应用培训工作。

5) 全省行贿犯罪档案查询系统日常应用维护。

3.3.2.3 政务系统运维

海南省检察机关政务管理系统

运维内容包括：

1) 解决解答用户提出的流程问题或其他问题。

2) 根据情况对用户进行业务流程培训。

3) 对各级院提出的需求进行汇总、整理，形成需求报告报省检察院负责部门批准后反馈给进行软件系统调整，并协助进行后续处理。

4) 处理收发文在流转中出现的操作问题，如回退节点，删除文等等。

3.3.2.4 信息发布系统运维

海南省检察机关信息发布系统运维的主要内容包括如下：

1）全省 27 家检察院信息发布系统日常运维工作以及帮忙解决数据库无法启动、连接问题，应用服务无法访问或有报错问题。

2）确保全省信息发布系统版本一致性，负责给全省各级院进行优化升级。

3）对于用户紧急的需求，必须安排技术人员进行处理，并且在 1-3 工作日内给予答复。

4）提供该系统迁移和数据迁移方案。

5）解答全省各级院对该系统的业务咨询。

3.3.2.5 安全邮件系统

海南省检察机关安全邮件系统

运维主要内容包括如下：

1）积极配合协助全省检察机关应用安全邮件系统。

2）对邮件系统数据库进行定时备份，定期检查数据备份情况。

3）将根据需求及要求，驻场运维工程师需对邮件系统进行升级完善，技术支持团队将积极配合运维工程师完成系统升级。

3.3.2.6 工作日志管理系统

海南省检察机关案件管理系统日常账号管理维护。

4.项目实施计划

4.1 服务机构人员组成

针对系统维护服务，派遣 4 名技术人员驻场服务，3-5 名远程技术支持人员协助。 驻场运维人员及远程技术支持人员至少有一名三年以上的相关运维工作经验，承担过数据库项目的工作或者接受过高检院组织的大统一业务应用软件培训。驻场运维人员及远程技术支持人员应具备对统一业务应用系统及其他系统的维护能力，了解各个系统所使用的操作系统、数据库、应用服务和中间件，并且能够熟练掌握相关操作系统、数据库、应用服务和中间件的基本操作。当各个系统出现问题时，具体一定的判断能力和解决能力。

- 4.2 制定详细的实施方案

4.3 运维周期管理

4.3.1 运维服务周期

本项目的运维周期为自合同签订日起一年。

4.3.2 运维服务地点及场所

（1）用户方将为方提供用户指定运维服务工作场所，方将严格按照省院办公场所管理办法。

（2）方在用户方提供的办公场所内，方自行维护办公环境的卫生和安全。

4.3.3 运维值班

4.3.3.1 值班时间

为全省提供 7*24 小时响应服务，提供 5*8 小时现场技术支持服务。

4.3.3.2 运维值班内容

值班业务处理主要包括监控网络、服务器等设备运行状态，受理业务申告、技术咨询，处理软硬件故障和安全事件等内容。

4.3.3.3 运维值班承诺

针对本项目，方承诺在值班时间内遵守以下要求：

当日值班员及时监控软硬件系统运行状态，按照流程及时处理业务申告、技术咨询、软硬件故障及各种告警信息。

交接班时发生系统运行障碍，一般由交班人员负责处理后再行交接；本班未处理完的事项，交接班后由接班人员继续处理。

遇有重大系统故障，值班人员应立即通知主管部门领导，主管部门领导应迅速组织相关技术人员到达现场查明原因、排除故障、尽快恢复。事后应认真分析原因，总结经验，制定措施，并层报最高人民检察院主管部门。

4.3.3.4 值班情况表

为了更好的服务该项目，运维方将积极配合省院提供重大节日值班服务，根据初步规划，运维驻场人员值班情况表如下表，省院可以根据实际情况，对运维人员进行动态调配值班顺序及值班要求，在值班期间，运维人员需积极主动配合省院值班人员开展相关运维保障工作，协助值班人员开展相关事务工作。

具体值班表的详细安排双方共协商确定执行。

4.3.4 运维服务阶段

1）基础软件运维

业务应用软件包括应用软件、数据库系统、应用服务器中间件以及业务应用系统的调试及优化。

- 根据软件安装部署及优化要求，分别需要对已经填写《设备（软件）安装配置记录表》、《服务端/单机软件配置记录表》、《客户端软件配置记录表》进行同步更新并审批通过。根据应用系统、工具类软件所需要的服务器数量，分配 IP 地址范围；工具类软件的域名要求，在 DNS 服务器上配置相关域名、IP 地址的映射；根据分级保护的要求，在相关设备上开通需要的服务端口；依据应用软件的安装部署手册，安装对应的操作系统以及相关应用软件；
- 安装优化完毕后对相关资料进行归档。

2）业务软件运维

针对业务软件平台的功能，在具体运维划分为两类情况进行处理：

- 操作问题、咨询类通过服务电话、邮件或论坛等方式当场解答业务应用软件在使用操作上的问题，并向咨询人提供指导意见。
- 系统类问题需要将申请人及时将问题整理形成书面资料，通过逐级提交、诊断、确认、处理和回复等环节，处理涉及到系统设置、后台数据修改以及软件优化、二次开发等方面。

3）其他应用软件

- 按照系统软件提供商提供的补丁升级程序定期对系统进行更新和升级服务；

- 针对各类系统的安装、调试、技术支持、相关文件、升级包分别进行归档处理，建立历史档案。

4）工作总结

运维单位将每个季度、年终定期向检察院定期汇报工作，重大事件及时汇报等。

- 系统维护工作报告

在日常运维工作中，依据《日常故障处理记录(基础模板)》、《事件处理报告(基础模板)》、《问题反馈表(基础模板)》详细记录日常工作情况。

- 系统季度运行报告

依据运维管理平台的详细记录情况，在《xxxx 年 xx 运维服务报告》中反映当前季度应用系统的运行情况。

- 系统年度运行报告

依据运维管理平台的详细记录情况，在《xxxx 年运维服务总结》中反映当前本年应用系统的运行情况。

6）重大事项报告

针对发生了一级故障事件，《xxxx 年度维护情况表》中反映当前本年应用系统的运行情况。

7）运维改进计划

将在每年进行运维服务工作总结，总结上年度运维工作中的得失，编制下年度的《xxxx 年度运维改进工作计划》。

4.3.5 服务总结阶段

在服务期末，运维单位将对本次运维期间的工作进行总结，并着手继续后续年度的工作计划。对不在继续服务的工作进行移交，主要包括：

- 硬件设备型号、数量、版本等信息统计资料；
- 软件产品型号、版本和补丁光盘等信息统计资料；
- 其它附属设备的统计资料、归档资料、文件。

4.4 运维保密

针对本项目运维服务，采取如下措施，实现对信息安全保密。

1）运维服务提供单位与海南省人民检察院签署《信息安全保密协议书》，采取切实可行的措施保障甲方的网络与信息安全。认真遵守海南省人民检察院对运维运维单位所制定的相关规定，认真遵海南省人民检察院其它各项安全保密的相关规定。定期对运维服务人员进行安全保密管理和思想教育，加强保密意识和安全生产意识。

2）派驻用户现场的运维服务人员须经过国家保密局的保密培训，并持有 SM 人员资格证。

3）驻场运维人员与海南省人民检察院签订的《信息安全保密协议书》。认真遵守国家保密法律、法规和规章制度，履行保密义务。

4）对在该项目过程中接触到的涉及海南省人民检察院信息的资料、文件、数据等承担保密义务；在该项目过程中不去刺探或者以其他不正当手段获取海南省人民检察院的机密信息。

5）任何情况下，不将海南省人民检察院的机密信息泄漏、告知、公布、发布、出版、传授、转让给任何第三方或以其他任何方式予以披露。

6）因该项目需要所持有或保管的一切记录着上述检察院信息的文件、资料、报告、信件、传真、磁带、磁盘以及其他任何形式的载体，须在海南省人民检察院院要求下的任何时候予以交还，本人不得留有这些文件的任何复制文件。

7）如发生失泄密事件，按照国家相关法律法规要求办理。

4.5 运维质量保证

运维服务质量保证，主要是通过服务能力、服务质量保证及运维服务评价体系来保证整个运维的质量。

运维单位应具备从事检察行业信息化工作经验，具有涉密信息系统集成资质、涉密信息系统软件单项开发等相关资质。

4.5.1 服务网点

运维单位在海南省院需派驻驻场人员，如果遇到重大或者驻场人员无法解决的问题，运维单位总部技术人员及相关技术专家提供远程协助支持。

5.验收方法及标准

本项目的服务周期为一年，采用一次验收的方式进行项目考核。

5.1 验收方法及标准

项目的验收标准参照《海南省工业和信息化厅_海南省财政厅关于印发省本级预算单位政务信息化项目建设管理若干事项的具体规定（暂行）的通知》、《海南省工业和信息化厅关于进一步做好海南省政务信息化工程建设项目初步验收工作的函》。

5.2 验收程序

5.2.1 运维验收会议

A、提出验收申请

由运维公司向建设单位提出验收申请，并准备好相关材料。

B、运维验收会议

由信息装备处向省院主要部门发邀请函参加运维验收会议；运维单位准备材料进行运维工作情况汇报；参与运维验收会议的部门进行评价和提出意见，最后进行运维满意度调查。

C、运维验收报告

由运维单位编写运维验收报告，双方确认运维材料齐全，同意验收后，签字盖章。

5.3 验收交付文档

所有正式交付件在提交给项目经理及相关的部门使用的同时，应做好如下的

归档工作：

5.3.1 项目类文档

- 运维服务单（含各审批件复印件）
- 项目总结报告
- 项目验收申请表
- 项目服务费用一览表
- 项目服务内容总结
- 其他必要的文档资料

5.3.2 技术类文档

- 故障分析报告
- 重大事件处理报告
- 问题跟踪处理表
- 各系统升级记录
- 系统故障情况统计
- 系统运维统计清单