

## 项目采购需求

### 一、说明：

- 1.投标人提供的服务必须符合国家和行业标准。
- 2.标“★”为实质性参数要求和条件，投标人必须满足并在投标文件中如实作出响应，否则投标无效；标“▲”为重点指标；无标识的为一般指标。
- 3.投标人投标时必须在投标文件中对所投分标所有项目要求及技术需求内容、商务要求表中内容及附件内容（如有）逐条响应并一一对应。
- 4.“·”符号为序号的表述。

### 二、采购内容：

采购标的对应的中小企业划分标准所属行业为软件和信息技术服务业。

一、技术参数、服务内容及要求：		
服务名称	数量	服务内容及服务要求
大数据分析及应用集成平台、自然人	1项	<p><b>一、项目背景</b></p> <p>广西壮族自治区税务局大数据集成分析应用平台于2017年上线，实现了税收数据的“大归集、大共享、大治理”目标，主要功能涵盖：风险分析、税收分析、征管监控、行政执法分析、各类专项业务分析、一户式分析、一局式分析和数据资产管理等。突出了以“千人千面”展现数据；强化了数据治理，打造全面和准确的数据集市；深化了以风险分析为基础的数据分析能力。</p> <p>根据税务总局统一部署，自然人电子税务局于2018年10月起分阶段陆续上线。同时，个人税收管理系统继续保留，提供历史数据查询统计、历史完税证明开具等功能。自然人电子税务局包括税务端、扣缴端、APP端及WEB端，分别适用于税务人员、个人所得税扣缴义务人、自然人纳税人进行个人所得税相关业务办理，涉及登记、申报、征收、优惠、证明、法制、征纳互动等业务域。自2019年起，陆续上线个税申报记录查询、个税专门系统、电子文书制作等配套关联系统及功能。</p> <p>金税三期决策支持二包是由国家税务总局统推、金税三期工程的重要系统。现已建成统一的数据综合利用及管理平台，为风险管理、信用管理、稽查管理等各类分析业务提供统一的数据存储管理、加载、分析展现功能，形成了全国统一管理，税务总局、省税务局两级部署的数据分析应用格局。金税三期决策二包系统已在广西实现了比较深入的应用，成为各单位开展风险</p>

电子税务局、金税三期决策支持二包系统运维服务	<p>管理、信用管理、稽查管理等数据分析应用工作的支撑平台，为税务系统信息管税目标的实现奠定了坚实基础。</p> <p>运维服务目标是对大数据分析应用集成平台、自然人电子税务局、金税三期决策支持二包系统实施专业化、规范化、标准化的运维服务，不断优化系统运行环境，及时排查、解决系统运行中的问题，快速处理用户服务请求，保障系统安全、稳定、高效、持续运行。</p> <p><b>二、业务需求</b></p> <p><b>(一) 业务支持系统清单</b></p>																											
	<table border="1"> <thead> <tr> <th data-bbox="384 577 596 636">业务系统</th> <th data-bbox="596 577 1342 636">业务子系统</th> </tr> </thead> <tbody> <tr> <td data-bbox="384 636 596 1491" rowspan="14">大数据分析应用</td> <td data-bbox="596 636 1342 692">大数据平台门户服务</td> </tr> <tr> <td data-bbox="596 692 1342 748">数据分析应用集成平台服务</td> </tr> <tr> <td data-bbox="596 748 1342 804">外部数据交换系统</td> </tr> <tr> <td data-bbox="596 804 1342 860">涉嫌风险纳税人动态监控系统</td> </tr> <tr> <td data-bbox="596 860 1342 916">税务监控大屏服务</td> </tr> <tr> <td data-bbox="596 916 1342 972">一户式分析服务</td> </tr> <tr> <td data-bbox="596 972 1342 1028">千户重点税源企业系统</td> </tr> <tr> <td data-bbox="596 1028 1342 1084">增值税发票风险防控系统</td> </tr> <tr> <td data-bbox="596 1084 1342 1140">利益关联网络服务</td> </tr> <tr> <td data-bbox="596 1140 1342 1196">一局式查询服务</td> </tr> <tr> <td data-bbox="596 1196 1342 1252">复工复产专项系统</td> </tr> <tr> <td data-bbox="596 1252 1342 1308">DPaaS 数据资产管理平台</td> </tr> <tr> <td data-bbox="596 1308 1342 1364">机器学习平台</td> </tr> <tr> <td data-bbox="596 1364 1342 1420">广西大企业管理应用平台</td> </tr> <tr> <td data-bbox="596 1420 1342 1491">专项分析系统</td> </tr> <tr> <td data-bbox="384 1491 596 2004" rowspan="9">自然人电子税务局</td> <td data-bbox="596 1491 1342 1547">自然人电子税务局（税务端）</td> </tr> <tr> <td data-bbox="596 1547 1342 1603">自然人电子税务局（扣缴客户端）</td> </tr> <tr> <td data-bbox="596 1603 1342 1659">自然人电子税务局（web 端）</td> </tr> <tr> <td data-bbox="596 1659 1342 1715">自然人电子税务局（手机 APP 端）</td> </tr> <tr> <td data-bbox="596 1715 1342 1771">金三个人税收管理系统</td> </tr> <tr> <td data-bbox="596 1771 1342 1827">金三个人税收管理系统统一接入平台</td> </tr> <tr> <td data-bbox="596 1827 1342 1883">个税专门系统</td> </tr> <tr> <td data-bbox="596 1883 1342 1939">个税申报记录查询</td> </tr> <tr> <td data-bbox="596 1939 1342 2004">电子文书制作</td> </tr> </tbody> </table>	业务系统	业务子系统	大数据分析应用	大数据平台门户服务	数据分析应用集成平台服务	外部数据交换系统	涉嫌风险纳税人动态监控系统	税务监控大屏服务	一户式分析服务	千户重点税源企业系统	增值税发票风险防控系统	利益关联网络服务	一局式查询服务	复工复产专项系统	DPaaS 数据资产管理平台	机器学习平台	广西大企业管理应用平台	专项分析系统	自然人电子税务局	自然人电子税务局（税务端）	自然人电子税务局（扣缴客户端）	自然人电子税务局（web 端）	自然人电子税务局（手机 APP 端）	金三个人税收管理系统	金三个人税收管理系统统一接入平台	个税专门系统	个税申报记录查询
业务系统	业务子系统																											
大数据分析应用	大数据平台门户服务																											
	数据分析应用集成平台服务																											
	外部数据交换系统																											
	涉嫌风险纳税人动态监控系统																											
	税务监控大屏服务																											
	一户式分析服务																											
	千户重点税源企业系统																											
	增值税发票风险防控系统																											
	利益关联网络服务																											
	一局式查询服务																											
	复工复产专项系统																											
	DPaaS 数据资产管理平台																											
	机器学习平台																											
	广西大企业管理应用平台																											
专项分析系统																												
自然人电子税务局	自然人电子税务局（税务端）																											
	自然人电子税务局（扣缴客户端）																											
	自然人电子税务局（web 端）																											
	自然人电子税务局（手机 APP 端）																											
	金三个人税收管理系统																											
	金三个人税收管理系统统一接入平台																											
	个税专门系统																											
	个税申报记录查询																											
	电子文书制作																											

金税三期决策支持二包	风险管理系统
	跨区域风险协作系统
	信用管理系统
	涉税信用管理系统
	税务稽查双随机工作平台
	税务稽查指挥管理应用系统
	企业所得税汇算清缴政策风险提示服务系统
	企业所得税季度预缴政策风险提示服务系统
	发票风险快速反应
	增值税电子专票网格化服务
	征管 5C 系统
	(税务总局新上线子系统)

## (二) 运维服务内容

大数据分析应用集成平台、自然人电子税务局、金税三期决策支持二包系统运维服务包括但不限于以下方面：

### 1. 系统环境保障与监控

保障各系统生产环境、预生产环境应用和数据库服务正常运行。

(1) 负责软件应用数据性能基础相关的日常巡检和监控工作，及时发现和处理系统潜在运行风险。对发现和接收的问题进行调查、诊断、定性后，进行相应的管理、维护、优化处理。类型涵盖：应用软件数据管理、表空间管理、用户及权限管理、数据链接维护、索引维护、主机参数调整、应用软件数据参数调整、异常进程处理、应用服务维护等。

(2) 协助采购人解决在系统运行过程中发生的应用和数据库等基础环境相关问题，分析、定位问题原因，配合采购人拟定解决方案，做好问题处理工作。

(3) 协助采购人归纳、总结、分类软件应用数据基础相关的问题和解决方案，建立并完善相关软件应用数据环境保障知识库，提高问题响应效率和解决效率。

(4) 根据国家税务总局及自治区税务局相关要求定期开展系统检查，包含但不限于每月对各系统软件应用数据环境进行基础检查。确保除计划停机外，各系统均能正常运行。

(5) 根据国家税务总局及自治区税务局相关要求做好安全加固，包括

但不限于对各系统服务器操作系统补丁进行升级、安全漏洞进行整改等，保障各系统均能安全、平稳运行。

## 2. 问题协调沟通

### (1) 描述

中标人应建立问题协调沟通机制，由于应用系统间的相关性较强、接口较多、数据交互复杂，一个问题的产生可能涉及多个应用系统，需要各相关系统支持人员互相协作定位问题原因，并处理解决。

### (2) 处理流程

①初步分析问题：首先由运维人员对所上报的相关应用问题进行初步分析定位。

②调工申请：如果问题涉及其它应用系统或系统软件，则向采购人相关应用系统负责人申请资源，调派相关运维工程师协助定位问题原因。

③各系统工程师协同定位原因：各系统运维工程师根据应用系统负责人的调派，协同发生问题的应用系统运维人员分析问题现象，定位问题根本原因。

④出具方案及评审：运维人员根据分析定位的问题原因，结合实际情况编写问题解决方案，在方案制定完成后，由采购人对方案进行审核，审核通过后，并评估相应风险，进行。

⑤方案测试：在测试环境对技术方案进行测试，对测试过程中暴露的技术方案缺陷进行修正；

⑥方案实施：测试通过后再在生产环境进行维护。

## 3. 系统升级

根据国家税务总局及自治区税务局相关要求，及时对应用软件进行版本升级、应用部署和测试工作。

(1) 准备版本升级环境；

(2) 实施系统预生产环境发布；

(3) 完成新版本功能验证，反馈验证结果；

(4) 协助完成其他关联系统的升级影响评估，配合关联系统厂商完成相关接口和数据复制关系的回归测试，做好测试问题原因分析，配合提出解决方案；

(5) 解决与本地环境相关的问题；

(6) 按照工作规范，实施生产环境发布，并负责版本发布后生产环境可用性验证；

(7) 联调服务。系统升级时需要和外围厂商的联调测试、其他厂商的联调测试及上线配置；

(8) 及时反馈版本问题和缺陷。

#### 4. 故障分析及处理

故障处理是指在应用系统运行出现异常情况下的管理操作流程。包括在最短的时间内恢复正常的服务运营，将故障对业务运营的负面影响降至最低，保证运营系统最高级别的服务质量和可用性，力求找到引发故障的根源，并及时着手改善或纠正。

(1) 在系统运行期间出现阻断性故障、服务卡慢等问题时，要求在最短的时间内定位、排除故障，恢复业务运行。

(2) 对于涉及第三方系统无法立即排除故障的，应提出相关建议或解决方案，如涉及第三方系统暂时无法定位故障的原因，应积极参与并配合进行问题诊断。

(3) 故障处理完毕后，邀请用户进行验证，并协助采购人完成故障分析报告，在报告中应该包含故障描述，故障产生的可能原因，故障的解决办法，今后在日常维护工作中应该采取的措施，向采购人提交《故障处理报告》。

#### 5. 日常业务运维服务

(1) 日常问题受理和一般问题处理：通过运维问题管理平台、微信运维群、内网通讯工具、电话咨询等方式接收并处理省局及基层税务人员提出的系统使用过程中的各类问题。

(2) 紧急问题处理：因系统异常造成业务中断，需要技术人员能够按照紧急问题处理流程处理。

(3) 程序问题确认和处置：由于系统设计缺陷、程序 BUG 等原因造成的系统使用阻断性故障或性能低下属于程序问题，运维人员在对问题进行场景还原、复现测试和确认后，排查问题原因，提供解决方案并组织实施，实施后将确认结果反馈相关负责人。

(4) 软件功能咨询：针对涉税流转事项及征管电子档案、税收监控分析系统应用的业务处理方法、业务处理原理、业务数据流向等在软件功能上反映的问题提供及时全面的解答，完成查询、统计、报表等功能口径的解释、功能答疑等。

#### 6. 基础数据维护

由于系统或升级操作失误造成一些数据需在后台来进行维护，而数据维护涉及数据安全，为保证数据在税务系统的逻辑性、正确性、完整性，应不断加强基础数据管理。

(1) 沟通确认：对于数据维护类的运维单，需要运维工程师与用户充分沟通，了解数据维护的原因、背景和涉及的业务细节；

(2) 分析数据：通过沟通确认，取得业务环境的配置信息，分析业务环境的数据特点；

(3) 出具方案：在尊重事实的情况下，对采购人提出的数据维护类运维单提出合理的数据处理解决方案，特别是由于业务变化而不得不进行数据维护的运维单，要全面考虑各实际用户的需求，从实际角度出发，给出合理的处理方案；

(4) 方案审核：在方案制作完成后，首先要对方案进行审核；

(5) 方案测试：在测试环境对技术方案进行测试，对测试过程中暴露的技术方案缺陷进行修正；

(6) 方案实施：测试通过后在生产环境进行维护。

## 7. 系统优化

### (1) 任务来源和分类

通过系统监控、用户反馈、网上调查、调研等多方面收集需优化的功能点。优化分为可用性优化和易用性优化。其中可用性优化包括缺陷修复、功能完善；易用性优化包括性能优化和界面优化。

### (2) 系统调优

缺陷修复及功能完善：系统日志异常监控、采购人反馈问题、各地市反馈问题。根据所发现的问题和需求，由运维人员及开发人员进行缺陷修复及功能完善工作。

性能优化：定期进行调查，检查系统的性即用情况，通过分析和定位出瓶颈后，进行针对性的优化。

## 8. 数据查询服务

为保障采购人日常业务的正常实施，满足各级税务机关部门准确获取相关业务数据的需求，提供数据查询服务。具体包括以下数据查询的技术服务工作：

(1) 数据查询口径：各单位各部门提出数据查询统计需求后，需与业务人员确定数据查询统计需求口径，确保技术人员与业务人员对查询口径理解一致；

(2) 数据查询程序脚本编写：查询口径确定后，结合系统数据库中的数据表结构和数据逻辑规则，编写数据查询统计程序脚本（包括 SQL 脚本、临时表、存储过程、视图等），并进行测试和审核；

(3) 程序脚本执行：数据查询程序脚本编写完成后，对程序脚本进行执行，查询出需要的数据；

(4) 数据查询结果提交：查询出数据结果后，经分析审核确定统计数据无误后，按采购人要求以安全有效的数据传输方式提交相关人员，完成数据查询

统计服务。

### 9. 联调服务

系统升级时需要和外围厂商的联调测试、其他厂商新接入系统的联调测试及上线配置，制定联调测试方案、明确联调时间和负责人。

上线前，对事项进行全流程测试，测试通过后填写《事项对接联调确认单》，并提供测试样例。基于测试结果进行验证，验证通过后，业务单位盖章确认《联调确认单》，输出联调测试报告。

### 10. 其他工作事项

序号	事项	工作事项
1	服务器检查	服务器用户口令过期检查、修改
2		服务器 ssh、ssl 升级
3		服务器时钟检查校对
4		服务器内置防火墙维护、检查
5		服务器间网络连通性问题排查
6	数据库检查	电子底账 2.0、征管库新建 OGG 链路、OGG 链路拆分
7		电子底账 2.0、征管库 OGG 链路异常分析、处置
8		AWR 报告应用层面处置
9		按要求导出 dump 文件
10		数据库内存占用评估、扩容建议
11		数据库磁盘 asm 磁盘组评估、扩容建议
12		数据库表空间使用率评估、扩容
13		数据库表锁时常分析、处置
14		数据库会话异常分析、处置
15		数据库查时间链接分析、处置
16		数据库等待事件分析、处置
17		数据库长事务分析、处置
18		数据库表索引失效、执行计划分析、处置。
19		高 CPU 使用率语句、高内存使用率语句分析和处置
20		数据库连接数分析和处置
21		应用占用 cpu 检查和报告
22	应用占用 cpu 分析和处置	

		23		应用内存占用检查和报告
		24		应用内存占用分析和处置
		25		应用 zombie 进程检查
		26		weblogic 控制台运行情况检查和报告
		27		weblogic 控制台运行情况分析和处置
		28		应用线程独占情况检查和报告、STUCK 进程检查和报告
		29		应用线程独占情况分析和处置、STUCK 进程分析和处置
		30		应用数据源运行、链接情况检查和报告
		31	应用 检查	应用数据源运行、链接情况分析和处置
		32		应用虚拟内存使用情况检查和报告
		33		应用虚拟内存使用情况分析和处置
		34		应用端口状态检查和报告
		35		应用端口状态分析和处置
		36		应用定时任务检查
		37		应用的 osb, ejb 调用检查
		38		OSB 组件中的 tolg_server 检查
		39		总省通道服务情况检查
		40		应用消息堆积情况检查和报告
		41		应用消息堆积情况分析和处置
		42	系统 升级	申请权限获取升级应用 war 包的复制、传输、更新
		43		申请对数据库的操作（修改表结构、表参数、增加、删除
		44		申请对 OGG 进行关闭、开启等操作权限，对 ogg 操作
		45	故障 排查	对故障进行应用级排查，包括数据库、应用服务、服务总
		46		对故障进行基础环境排查，包括数据库、应用系统、中间
		47		根据问题排查结果，对现场环境进行配置解决问题。
		48		根据问题排查结果，对检查出来的应用系统 BUG，上报二
		49		对现场性能问题进行检查，如果是代码问题，提交二线进
		50	应急	出现应急问题时，根据实际情况出具应急方案并实施。
		51	联调	系统升级时需要和外围厂商的联调测试、其他厂商新接入
		52		总局运维脚本



53	其他 处理	审计数据 DMP/月
54		总局监控对接和处置
55		协助信息中心运维工作：网络调整、设备更换、设变迁
56		压力测试
57		原国地税环境问题处置

产出物/提交物：

应用系统基础环境巡检结果表

应用系统基础环境故障处理报告

应用系统基础环境运行情况月报

### 11. 技术咨询服务

提供技术咨询服务，推动提升采购人人员问题处理能力，及时将上述工作中形成的相关知识向采购人人员转移。包括：归集系统问题知识，编写并及时更新常见问题处理技术文档；每年组织两次技术交流。

### 12. 其他问题处理

包括总局相关运维脚本、总局监控对接和处理，协助信息中心开展网络调整、设备更换、设变迁移、停机、攻防演练等工作；开展压力测试、环境问题处理等。

### 13. 运维问题分析报告

#### (1) 运维问题收集

运维过程中对各个渠道收集的纳税人和税务人员的问题进收集记录，对较复杂的关键问题和纳税人反映较多的进行重点收集。

#### (2) 运维问题分析

每个月征期完成之后，运维人员把各人收集的问题进行整理、汇总。问题分析人员把汇总的问题分类，分析其中有共性问题，进行说明找出最优解决办法，并编写手册进行下发培训。减少同类问题的发生，减轻运维问题的工作量。并分析问题根源，及时提出系统优化意见。

#### (3) 运维问题报告

根据每个收集的问题，进行分类统计，并根据分析的问题解决方案归集为每月的问题分析报告。

### 14. 应急预案

协助采购人处理应用系统的突发事件，使系统能够恢复正常运转。根据采购人要求拟定相关应急预案，突发事件造成的服务对象系统无法使用，根据应

急预案进行响应支持。预案的制定、落实和演练，遵循“发现或预判问题→启动预案→上报问题→信息发布→处置问题→形成总结”流程；对系统应用高峰期可能出现的网络拥堵、系统性能下降等问题，提前预判并启动应急预案；根据采购人要求，应用系统每年开展应急演练工作，演练内容包含数据丢失、服务器瘫痪等各种极端情况，根据演练结果分析总结形成演练工作报告并逐步完善应急体系，以保障在重大故障发生后能有效应对。

### 15. 培训服务

依据采购人需要，结合系统优化升级的情况，对大数据分析应用集成平台、自然人电子税务局、金税三期决策支持二包等系统进行相关业务培训。

### 16. 应急保障

在系统运行过程中，可能会出现各类故障，系统故障是指系统无法为工作人员及用户提供服务、或者是其他影响到用户体验等的事件，如应用软件无法访问、数据混乱、页面打开速度极度缓慢、某些业务功能不可用等情况都属于系统故障范畴。为了保障系统正常运行，需做好应急保障，包括系统的应急预案，运维二线快速支持服务等，确保故障能在规定时限的处理完成。

#### (1) 故障类型和响应时限

故障分类	描述	响应时限	处理时限
P1	灾难性故障，系统登录、接口异常、计算异常、领票业务办理、开具发票业务办理、实施链路异常等核心功能无法使用，影响绝大部分用户（30%以上）。	5分钟	2小时
P2	重大故障，系统登录、接口异常、计算异常、领票业务办理、开具发票业务办理、实施链路异常、等核心功能无法使用，影响绝大部分用户（10%~30%）；或系统非核心功能无法使用，影响绝大部分用户。	5分钟	4小时
P3	一般故障，系统的非核心功能无法使用，影响部分用户（1%~10%）。	1小时	48小时
P4	轻微故障，除P1、P2、P3的故障，系统的周边功能无法使用，影响小部分用户（1%以下）。	2小时	1周内

#### (2) 系统故障响应流程

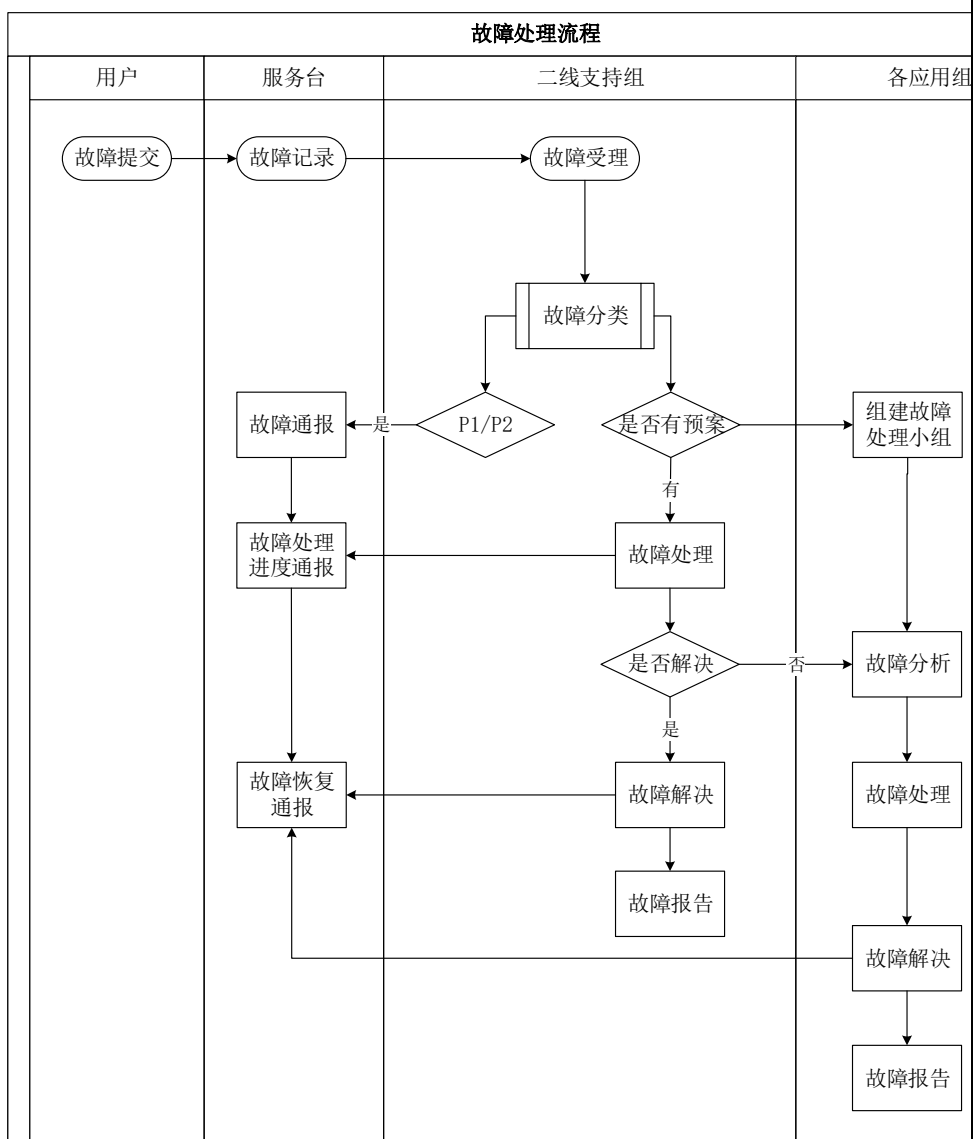
1. 运维小组从用户侧获得故障报告后，应及时记录并提交运维组服务台

(以下简称服务台) 进行记录, 服务台通知二线支持组进行故障受理, 如果是 P1/P2 级别故障, 及时进行通报, 通报给采购人、各相关厂商。

2. 二线支持组应及时分析故障、做好故障处理, 及时通报故障处理进度, 故障解决后出具故障报告。

3. 如果二线支持组无法解决故障, 则转给对应的应用组或是相应厂商, 由该组组建故障处理小组, 分析解决故障, 及时通报故障处理进度, 故障解决后出具故障报告。

下图为系统故障响应流程图:



### (三) 各系统个性化运维服务内容

#### 1. 大数据平台主要功能运维

##### (1) 指标标签管理

指标标签管理是依托于大数据平台, 以指标管理平台为支撑, 集标签创建和标签应用分析于一体的功能模块。具体功能包括: 新建标签、标签维

护、信息加工、探索分析、我的分析、业务标签库。

**新建标签：**通过录入标签基本信息、语义模型、加工方式等内容建立标签规则，新建成功的标签进入标签维护页面。

**标签维护：**对建立的标签进行维护，支持对标签进行修改、删除、发布、预览、收藏等操作。

**信息加工：**对标签扫描状态进行监控，对加工失败的标签可以重新启动扫描，对尚未加工的标签可以立即执行扫描，扫描成功后的标签内容将包含对应的纳税人清册。同时，扫描成功后的标签进入标签库中。

**探索分析：**支持用户在不断试错不断调整的思维模式驱动下，探索性的选择相应的标签，逐步过滤得到满足业务需要的纳税人清册。

**我的分析：**容纳用户保存的层虑分析结果，支持用户对分析结果进行查看、修改、删除等操作。

**业务标签库：**标签库容纳所有加工完成的标签，支持用户对标签进行查看、预览、收藏等操作。

## **(2) 指标模型拓展服务**

### **大数据分析应用集成平台的风险模型分析服务**

负责对风险模型进行系统可加载实现的分析，分析内容包括：指标元、指标预警值、打分公式、指标分类、风险应对指南等信息，形成系统可定义加载的指标模型信息。根据分析后的指标模型需求，将业务口径转化为数据口径，结合梳理的指标元涉及的业务表单完成对模型的指标元、指标、模型的数据支持分析，针对数据进行数据质量分析，发现数据质量问题以及得出是否符合模型要求的结论，形成可加载的风险模型指标清单。

### **大数据分析应用集成平台业务标签分析服务**

负责对业务标签进行系统可加载实现的分析，形成系统可定义加载的业务标签信息。根据分析后的业务标签需求，将业务口径转化为数据口径，结合梳理的业务标签涉及的业务表单完成对指标元、指标、模型的数据支持分析，针对数据进行数据质量分析，发现数据质量问题以及得出是否符合模型要求的结论，形成可加载的业务标签清单。

### **风险模型及业务标签加载验证服务**

提供指标模型和业务标签的加载工程师在大数据分析应用集成平台中进行指标、模型、业务标签加载实现，内容包括：指标元加载、指标加载、模型加载、指标预警值测算、应对指南加载、业务标签加载。加载完成后，形成已加载待验证优化的指标模型清单和业务标签清单。

对已加载的模型和业务标签开展数据验证工作，一是用数据来验证业务加载的指标模型和业务标签是否与业务供应存在差异。二是按业务表单验证数据项与指标元是否一致。三是验证指标模型的计算是否存在错误，验证通过后正式发布。

#### **大数据分析应用集成平台的风险模型研究服务**

根据采购人各业务处室提出的风险模型业务需求，结合实际的税源情况、数据情况，安排风险模型研究业务专家分析研究，输出符合实际状况的风险模型清册，包括分析思路、具体模型、预警值、风险指向、应对指引，提供给采购人，并向采购人解释模型的设计原理和指向性。

#### **风险扫描选户服务**

通过在系统中正式的风险扫描，结合扫描产生的疑点纳税人的结果数据，采购人的专家与服务提供商的业务专家双方共同探讨，根据风险等级、命中模型的重要性等情况，最终确认选取下发的风险纳税人清册。

#### **风险模型优化服务**

根据业务标签和风险模型在风险应对过程中暴露的问题，尤其是针对异常情况导致部分风险纳税人风险不存在，由服务提供商负责对业务模型进行优化，提升风险模型指向性和命中率。

同时，协助完成大企业税收风险指标模型研发加载工作。

①在指标模型设计阶段，根据业务需求对指标模型进行字段级的拆解和映射，做好数据相关准备工作，包括数据抽取、加工、清洗等。

②在指标模型研发阶段，做好模型定义工具的操作培训，取数口径的讲解、具体模型搭建等协助工作。

③指标模型研发完毕后，协助开展指标模型有效性验证，主要是通过实际运用检验指标模型的研发准确性、取数准确性，并根据运用反馈进行优化调整等。

#### **“黑匣子”模块运维服务**

广西大企业管理应用平台需要通过总省联动“黑匣子”模块调用总局大企业管理系统风险指标模型库进行税收风险扫描，因此需要负责“黑匣子”模块的本地应用保障。

①负责总省联动“黑匣子”模块升级版本的本地部署及验证工作。根据税务总局版本变更情况，及时在预生产环境中进行版本发布和验证测试。验证通过后按要求将新版本发布到生产环境中。

②负责解决总省联动“黑匣子”日常使用中出现的的问题，确保模块正常运

转、与大企业数据集市有效对接，指标模型取数准确、风险扫描报告及时生成。

### **(3) 数据资产管理**

对大数据平台数据进行统一管理：

可视化资产展示：通过数据可视化的手段，将平台中的数据资产情况、数据对象间关系、数据流向等信息简便直观地按逻辑分类准确展示。

数据对象管理：通过数据资产平台，对抽取加工的数据资产信息进行标识和维护，以便于后续使用管理。

数据资产信息权限管理：数据资产平台内部可以对数据资产信息的访问权限进行自定义分配和设置，以达到灵活管控的目的。

### **(4) 日常数据支持服务**

#### **数据准备和加工服务**

根据风险模型和业务标签分析后的数据需求，完成数据来源和口径分析，建立数据模型，编写数据抽取脚本，并完成数据抽取脚本部署、执行、加工、验证，确保数据完整性和数据质量，形成能支撑风险模型运行的数据条件。

#### **数据服务**

数据准备和加工服务：根据省市两级提出的数据加工需求，完成数据来源和口径分析，建立数据模型，编写数据抽取脚本，并完成数据抽取脚本部署、执行、加工、验证，确保数据完整性和数据质量，并将完成情况及时反馈给用户。

数据提取服务：对用户提出的数据服务需求，按采购人的流程审批通过后，进行业务需求分析，口径编写，结果验证等工作。包括但不限于以下内容：

①针对需上报给总局、省局的业务数据提供查询、统计服务，满足省市两级的其他数据提取服务需求。

②保障系统运行过程中业务数据正确性、有效性；

③针对业务的数据问题处理，如分析基础数据口径问题、数据对接问题、数据抽取问题、数据验证问题和数据质量问题等提供方案设计、验证以及实施服务。

数据抽取保障：数据抽取分为日常增量抽取和全量抽取，日常增量抽取由系统设定的定时任务自动执行，全量抽取由技术人员手动执行。主要是保障数据抽取的任务调度正常，抽取的执行结果正常。主要工作内容包括：

①数据抽取任务调度状态维护。数据服务人员，每日检查数据抽取任务的调度配置状态，发现问题及时解决。并根据数据量及业务办理日期变化等情况，对任务调度进行必要的调整。

②日常增量抽取保障。数据服务人员每日对抽取的结果进行检查，检查各

抽取任务是否执行完毕、是否执行正常，发现问题及时解决。对抽取的结果日志进行分析，采用技术工具对抽取结果进行技术性校验。

③全量抽取。在业务系统数据源发生较大变化时，应采用全量抽取的方式重新进行全量抽取。数据服务人员在采购人系统管理员的要求下，停止增量抽取任务，手工启动全量抽取的任务，监控全量抽取过程，检查全量抽取结果。

数据加工保障：数据加工是对已经抽取到数据仓库的业务数据进行汇总、统计、分析的过程，数据加工的结果数据以数据集市的形式存储在数据库中。数据加工过程根据数据仓库的数据产生情况，采用全量加工或增量加工两种方式，主要是保障数据加工的任务调度正常，加工的执行结果正常。主要工作内容包包括：

①数据加工任务调度状态维护。数据服务人员，每日检查数据加工任务的调度配置状态，发现问题及时解决。并根据数据量及业务办理日期变化等情况，对任务调度进行必要的调整。

②日常增量加工保障。数据服务人员每日对加工的结果进行检查，检查各加工任务是否执行完毕、是否执行正常，发现问题及时解决。对加工的结果日志进行分析，采用技术工具对加工结果进行技术性校验。

③全量加工。在业务源数据全量抽取后，需采用全量加工的方式对数据进行加工。数据服务人员在采购人系统管理员的要求下，停止增量加工任务，手工启动全量加工的任务，监控加工过程，检查加工结果。

#### 数据问题分析、处理与咨询

负责大数据分析应用数据问题分析与处理、数据结构咨询等工作。及时响应和解决采购人使用系统中遇到的数据问题。负责分析、定位数据问题原因，拟定处理方案，按采购人流程审批后完成数据处理和结果验证。

#### ①理解模型设计

- 理解该模型（表）属于哪个业务域（登记域、申报域）
- 理解该模型的源数据来自那些源系统、那些业务域
- 理解该模型的类型：维度表、明细表、汇总表、快照表？
- 了解该模型目前适用的应用系统、应用场景
- 理解该模型的加工频率（天、周、月、季、半年、年）

#### ②理解加工逻辑

- 理解该模型的来源表有些，包括来源主表、关联表
- 理解关键字段加工逻辑
- 理解关联条件、关键过滤条件，切记避免关联后笛卡尔积
- 分析来源主表、来源关联表的主键关系

•理解模型主键跟业务唯一键的关系

③分析数据特性

•分析所有来源表的数量级、索引情况、分区情况

•分析模型与来源主表数据量的比例关系

•分析来源表数据质量情况（关键字段、代码字段、关联字段）

•确定该模型的抽取模式（全量、增量），增量模式（业务时间、时间戳），增量范围（最新时间、天、周、月、季、半年、年）

•分析该模型的数量级，规划主键、索引、分区、审计字段

④开发抽取作业

•根据逻辑的复杂度确定脚本的类型（存储过程、标准 ETL）

•根据所有来源表的主键、索引、关联字段、分区情况，以及模型的抽取模式（全量、增量），增量模式（业务时间、时间戳），增量范围，确定最优加工逻辑，确保性能最优

•全量抽取，考虑大表的性能，根据源表的索引情况、分区情况循环抽取

•增量抽取，对于逻辑较复杂时或者目标表数据量较大时，可以拆分加工到多张临时表，在插入到最终临时表（结果跟目标表保持一致），再更新到目标表。

•增量抽取，使用固定业务周期作为增量条件（增量周期为月、季度、半年、年度），先 truncate partition 分区，再插入增量数据

•ETL 精简表适合大部分表关联的情况，极大降低数据库 IO，注意：按照来源主表数据量来确定抽取作业的抽取模式（全量、增量），两种场景如下：

第 1 是存量数据 100 万以上，使用增量抽取

第 2 是每年新增记录 50 万以上的，使用增量抽取

⑤开发验证作业

•抽取作业需要配套的验证作业

•复杂加工逻辑的抽取作业，其验证作业采用自定义查询模式

•SJZBQ、S0 的验证作业，验证作业的模式使用配置查询、配置查询（跨作业），数据量大的作业，可以使用纳税人采样或者增量模式。

•SJZBQ、S0 的验证作业，原则上其验证日志支持修复作业直接修复，此类作业是按稳定时间字段进行比较源、目标之间的差异。

注意：验证作业的抽取模式参照其对应的抽取作业

作业抽取模式为全量的，无需为其开发验证作业

⑥开发修复作业

•修复作业主要修复 SJZBQ、S0 的作业

•SJZBQ 的修复作业需要同时支持全量、增量



•S0 的作业无全量、增量只分，需要验证作业的日志支持实现数据修复  
注意：抽取作业常态模式为全量的，无需为其开发验证作业

⑦作业评审

- 模型设计、加工逻辑是否理解到位
- 数据特性是否分析全面
- 三类作业开发是否齐全、规范
- 作业流配套设置是否齐全
- 作业性能是否达标
- 加工数据能否得到需求方验收

**数据库优化**

协助采购人提供合理高效的数据库备份和恢复策略，进行数据库备份和数据库恢复。

**数据库安全管理方案**

①Oracle 安全要求

1) 身份鉴别

- 用户身份标识

安全规范要求	应对进入数据库系统的用户进行身份鉴别。应确保所标识用户在信息系统生存周期内的唯一性，并将用户标识与审计相关联。
全配置说明	使用数据库角色（ROLE）来管理对象的权限
安全配置操作步骤	<p>以 DBA 用户 sqlplus 登陆到数据库中； 检查是否对不同用户采用不同角色进行权限管理： select * from dba_role_privs where grantee = '&amp;grantee' order by GRANTED_ROLE; select * from user_role_privs where username = '&amp;username' order by GRANTED_ROLE; select * FROM DBA_SYS_PRIVS WHERE GRANTEE = '&amp;GRANTEE' ;</p> <p>如未使用不同数据库角色来进行权限管理，则通过命令进行配置</p>

	<p>创建角色，指定密码： create role &lt;rolename&gt; identified by &lt;passwd&gt;;</p> <p>修改角色： alter role &lt;rolename&gt; identified by &lt;passwd&gt;;</p> <p>给角色授予权限： grant select on &lt;Table_name&gt; to &lt;rolename&gt;;</p> <p>把角色赋予用户： grant &lt;rolename&gt; to &lt;username&gt;;</p> <p>角色不能立即起作用，需断开此次连接，下次连接才能起作用。</p>
<b>配置风险</b>	操作风险、关联风险
<b>备注</b>	
<p>➤ 用户口令策略</p>	
<b>安全规范 要求</b>	<p>数据库管理系统用户的管理用户身份标识符和口令应符合复杂度要求，口令长度至少 8 位，并包括数字、小写字母、大写字母和特殊符号 4 类中至少 3 类混排。定期修改口令（账户口令的生存期不长于 90 天），且口令需以密文状态存储，对于采用静态口令认证技术的数据库，应配置数据库，使用户不能重复使用最近 5 次（含 5 次）内已使用的口令。</p> <p>应设置数据库管理系统登录失败处理功能，包括结束会话、限制非法登录次数和自动退出等措施。</p>
<b>安全配置 说明</b>	为数据库管理用户设置口令复杂度、密码最长使用时间等密码策略和失败登录锁定策略。
<b>安全配置 操作步骤</b>	<p>以 DBA 用户 sqlplus 登陆到数据库中；</p> <p>检查是否对所有用户采用密码复杂度等密码策略： select * from dba_profiles; select username,profile FROM dba_users;</p> <p>可通过以下命令来创建 profile，并把它赋予所有数据库用户： @?/rdbs/admin/utlpwdmg.sql #启用密码复杂度函数 (/u01/app/oracle/product/11.2.0/db_1/rdbs/admin/)</p> <p>CREATE PROFILE &lt;profilename&gt; LIMIT FAILED_LOGIN_ATTEMPTS 6 #失败登录次数上限</p>

	<p>PASSWORD_LIFE_TIME 90 #口令生命期</p> <p>PASSWORD_REUSE_TIME 90 #口令 90 天内不得重用</p> <p>PASSWORD_REUSE_MAX 5 #口令只有被修改 5 次后才能被重用</p> <p>PASSWORD_VERIFY_FUNCTION verify_function #配置密码复杂度</p> <p>PASSWORD_GRACE_TIME 30; #口令过期后的缓冲期</p> <p>ALTER USER &lt;username&gt; PROFILE &lt;profilename&gt;;</p>
<b>配置风险</b>	操作风险
2) 访问控制	
➤ 禁止非授权用户对数据库资源的访问	
<b>安全规范要求</b>	应允许命名用户的身份规定并控制对数据库资源的访问，并阻止非授权用户对数据库资源的访问
<b>安全配置说明</b>	所有用户访问数据库均需要身份鉴别，不存在匿名登录等绕过身份鉴别的情况。
<b>安全配置操作步骤</b>	<p>以 DBA 用户 sqlplus 登陆到数据库中；</p> <p>Select username from all_users order by username;</p> <p>Select username from dba_users order by username;</p> <p>删除或锁定无效账户：</p> <p>alter user &lt;username&gt; account lock; #锁定用户</p> <p>drop user &lt;username&gt; cascade; #删除用户</p> <p>对用户属性进行资源限制：</p> <p>show parameter resource_limit;</p> <p>alter system set resource_limit=true; #开启资源限定功能</p>
<b>配置风险</b>	操作风险、关联风险
<b>备注</b>	
➤ 用户权限最小化	
<b>安全规范要求</b>	需按照最小权限原则，根据数据库系统内不同用户角色仅授予用户最小的权限访问系统资源
<b>安全配置说明</b>	根据用户的业务需要，配置其所需的最小权限。

<b>安全配置操作 步骤</b>	<p>以 DBA 用户 sqlplus 登陆到数据库中；</p> <p>查看目前用户的权限：</p> <pre>select * from user_sys_privs; select * from user_role_privs; select * from user_tab_privs;</pre> <p>修改用户权限：</p> <pre>grant 权限 to username;      #给用户赋相应的最小权限 revoke 权限 from username;   #收回用户多余的权限</pre>
<b>配置风险</b>	<p>操作风险、关联风险</p>
<b>备注</b>	<p>需由应用厂商细化权限</p>
<p>3) 日志审计</p> <p>➤ 启用日志审计</p>	
<b>安全规范要求</b>	<p>启用数据库系统的日志审计功能，对数据库系统内所有用户登录、操作等行为进行审计，审计日志应包括时间、主体、客体、操作等事项</p>
<b>安全配置说明</b>	<p>配置日志功能，对数据库系统内所有用户登录、操作等行为进行审计，审计日志应包括时间、主体、客体、操作等事项。</p>
<b>安全配置操作 步骤</b>	<p>以 DBA 用户 sqlplus 登陆到数据库中；</p> <p>配置日志功能，对用户登录进行记录，记录内容包括用户登录使用的账号、登录是否成功、登录时间以及远程登录时用户使用的 IP 地址：</p> <pre>SQL&gt; create table logon_audit( user_id varchar2(200), session_id number(38), logon_time date, logoff_time date, host varchar2(200)); SQL&gt; create or replace trigger logon_audit_trigger after logon on database begin insert into logon_audit</pre>

			<pre> values (user, sys_context( 'userenv' , 'sessionid' ), sysdate, null, sys_context( 'userenv' , 'host' )); end; </pre> <p>配置日志功能，记录用户对数据库的操作，包括但不限于以下内容：账号创建、删除和权限修改、口令修改、读取和修改数据库配置。记录需要包含用户账号，操作时间，操作内容以及操作结果：</p> <p>创建日志存储表</p> <pre> SQL&gt; create table ddl_log( username varchar2(200), change_date date, object_type varchar2(200), object_owner varchar2(200), database varchar2(200)); </pre> <p>创建 DDL 触发器：</p> <pre> SQL&gt; create or replace trigger ddl_log_trigger after ddl on database begin insert into ddl_log values (ora_login_user, sysdate, ora_dict_obj_type, ora_dict_obj_owner, ora_database_name); end; / </pre>
		<b>配置风险</b>	操作风险
		<b>备注</b>	
➤ 日志本地和远程存储			

安全规范要求	数据库系统的审计日志存储方式应包括本地和远程存储，审计日志至少存储三个月以上，当审计日志存储空间满时，应能及时提供告警
安全配置说明	配置归档日志，包括归档到本机和远程主机，日志至少保存三个月
安全配置操作步骤	<p>以 DBA 用户 sqlplus 登陆到数据库中； 查看数据库是否处于归档模式： SELECT log_mode FROM v\$database; 查看归档进程是否已启动： ho ps -ef  grep ora_arc 配置归档日志： 设置 LOG_ARCHIVE_DEST_n 参数， alter system set log_archive_dest_1 = ‘LOCATION=XXXXXXXX’ alter system set log_archive_dest_2 = ‘SERVICE=XXXXXX’ 对于远程归档日志，SERVICE 选项需要指定远程数据库的网络服务名（在 tnsnames.org 文件中配置）</p>
配置风险	操作风险、数据丢失
备注	需应用厂商提供远程日志服务器地址
➤ 日志文件保护	
安全规范要求	应对数据库系统的审计日志进行安全保护，防止非法获取或破坏审计日志
安全配置说明	设置日志文件权限，仅数据库超级管理员可以访问日志文件，其他用户不能访问日志文件。
安全配置操作步骤	<p>以 root 用户登录到数据库所在的操作系统中，执行命令： chown -R oracle: oinstall \$ORACLE_HOME/rdbms/log chown -R oracle: oinstall \$ORACLE_HOME/log chown -R oracle:oinstall \$ORA_CRS_HOME/log #RAC 数据库日志</p>

	<pre> chmod -R 750 \$ORACLE_HOME/rdbms/log chmod -R 750 \$ORACLE_HOME/log chmod -R 750 \$ORA_CRS_HOME/log </pre>
<b>配置风险</b>	操作风险、关联风险
<b>备注</b>	
<p>4) 资源控制</p> <ul style="list-style-type: none"> <li>➤ 设置最大并发连接数</li>   <li>➤ 设置会话超时时间</li> </ul>	
<b>安全规范要求</b>	应对数据库系统访问的最大并发数使用进行限制，提高数据库系统的稳定性
<b>安全配置说明</b>	对数据库系统访问的最大并发数使用进行限制
<b>安全配置操作步骤</b>	<p>以 DBA 用户 sqlplus 登陆到数据库中；</p> <p>查看数据库当前进程数：</p> <pre>select count(*) from v\$process;    获取数据库目前的进程数</pre> <pre>select value from v\$parameter where name = 'processes' ;    获取连接数的上限</pre> <p>设置最大连接数：</p> <pre>alter system set processes = 2000 scope = spfile;</pre>
<b>配置风险</b>	操作风险、关联风险
<b>备注</b>	
<b>安全规范要求</b>	应设置数据库自动断开长时间未活动的连接，保证数据库系统的资源负载合理
<b>安全配置说明</b>	设置数据库自动断开长时间未活动的连接，保证数据库系统的资源负载合理。
<b>安全配置操作步骤</b>	<p>以 DBA 用户 sqlplus 登陆到数据库中；</p> <pre>alter system set resource_limit=true;    #开启资源限定功能</pre> <pre>create profile &lt;profilename&gt; limit idle_time 10; #设置连续不活动的会话超过 10 分钟后强制释放</pre> <pre>alter user &lt;username&gt; profile &lt;profilename&gt;;</pre>

	<p>以安装 oracle 用户登录到数据库所在的操作系统中，执行命令：</p> <pre>vi \$ORACLE_HOME/network/admin/sqlnet.ora</pre> <p>如不存在以下一行，增加</p> <pre>sqlnet.expire_time=10</pre>
<b>配置风险</b>	操作风险
<b>备注</b>	如应用需求有长连接形式存在，该项有一定风险。
<p>5) 安全管理</p> <p>➢ 数据库系统版本和补丁</p>	
<b>安全规范要求</b>	应定期对数据库系统版本进行更新，并安装安全补丁，保证数据库系统安全
<b>安全配置说明</b>	定期对数据库系统版本进行更新，安装安全补丁
<b>安全配置操作步骤</b>	<p>以 DBA 用户 sqlplus 登陆到数据库中；</p> <p>查看版本与官方版本对比：</p> <pre>select * from v\$instance;</pre> <pre>select banner from sys.v_\$version;</pre> <pre>\$ORACLE_HOME/OPatch/opatch lsinventory</pre> <p>个别补丁用 Opatch 软件\$ORACLE_HOME/OPatch/opatch apply</p> <p>将补丁文件拷贝至 Oracle 服务器相关目录下，进入该目录并在控制台中输入</p> <pre>opatch apply</pre> <p>在提示是否进行更新时输入 y，即可自动进行相应补丁的升级</p>
<b>配置风险</b>	操作风险
<b>备注</b>	
<p>➢ 数据库系统备份</p>	
<b>安全规范要求</b>	应对数据库系统制定相应的备份策略，定期对数据库系统内数据进行备份
<b>安全配置说明</b>	对数据库系统制定相应的备份策略，定期对数据库系统内数据进行备份



安全配置操作步骤	询问管理员是否对数据库系统制定相应的备份策略，定期对数据库系统内数据进行备份。 查看系统中是否存在相应备份文件。
配置风险	
备注	

#### 5) 安全加固

随着互联网技术的普及，互联网用户数量的增长，互联网信息安全越来越受到大家的重视。信息安全性要求更高。不仅要重视互联网的信息安全，更要在内部服务器、甚至服务层面进行信息安全的防护。应对接下来全国性的安全扫描工作，确保产品不出现中问题。

根据自治区税务局要求，包括但不限于对大数据分析应用集成平台各系统各服务器操作系统补丁进行升级、安全漏洞进行整改等，保障大数据分析应用集成平台各系统均能安全、平稳运行。具体工作包含但不限于：

- 通过对操作系统管理权限进行三权分立、强制访问控制、强认证等对主机服务器操作系

统内核层面的安全加固；

- 对文件/目录进行强制访问控制；
- 对进程进行强制访问控制；
- 对注册表进行强制访问控制；
- 对文件/服务/驱动/注册表进行完整性检测；
- 对服务进行的强制访问控制；
- 全面的审计日志记录；
- 对已知和未知攻击手段的免疫。
- 基于硬件的安全策略分发器
- 基于硬件 USB-KEY 的强身份认证；
- 剩余信息保护、入侵防范、恶意代码防范、资源控制、完整性检测和集中

管理功能；

- 符合国家信息系统安全等级保护三级要求。

除上述要求外，投标技术/软件产品应同时满足以下具体要求：

- 基于硬件 USB-KEY 的强身份鉴别机制

针对操作系统本身提供的身份认证所存在的不足，该技术/软件对其进行加强了：

该 USB-KEY 为用户身份的唯一标识，当用户登录服务器系统时，需要插入

USB-KEY, 然后系统对用户进行双因子身份认证, 用户只有拥有合法的 USB-KEY, 并且输入正确的操作系统口令, 才能登录操作系统。

- 安全标记

通过对主客体设置安全标记来限制主客体间的操作, 以及信息的流动, 实现对系统资源的保护和建立多级安全系统。

- 强制访问控制

1) 主体可包括: 进程、用户, 客体可包括: 文件、注册表名、进程、服务、用户

2) 用户只要按照需要, 通过产品控制台设置一组访问规则, 就可确保相关客体不被未授权的主体访问与破坏

3) 强制访问控制有效的约束了原有系统管理员的权限, 对系统管理员权限进行了有效的分离: 该技术/软件安全管理员负责设定访问规则、系统管理员负责对系统本身的管理操作、该技术/软件审计记录管理员负责对系统内的所有安全事件、管理员操作进行审查, 实现了三权分立, 有效防止了管理员权限的一权独大的模式。

- 文件加解密

通过该技术/软件提供的文件加解密功能, 实现对系统文件的加解密。

- 安全审计

1) 违规日志:

记录系统内的所有违反强制访问控制规则的事件, 并提供日志查询、删除、日志分析等功能。

2) 操作日志

记录管理员对该技术/软件的所有操作事件, 并提供日志查询、删除、功能。

- 剩余信息保护

1) 剩余信息粉碎:

提供彻底删除数据的功能, 管理员可以能过该技术/软件彻底删除指定的文件或目录, 使数据恢复软件也无法找回所删除数据, 对重要数据做到完全清除。

2) 用户使用痕迹清理:

提供对用户使用的各种临时数据的一键清理功能, 如: 上网记录, 文件使用记录等等。

- 恶意代码防范

能通过该技术/软件强制访问控制, 可有效限制恶意代码的执行。

- 提供操作系统管理

通过该技术/软件提供对操作系统的管理功能,包括系统日志、进程、用户、文件、注册表、服务等的管理功能。

- 完整性检测

- 1)文件:

可检测对指定文件或目录的内容、大小、时间等信息的变化,支持多种检测选项:按文件后缀进行检测、支持递归与非递归检测等。

- 2)注册表:

可检测制定注册表项键和键值的增加、删除等变化。

- 3)驱动:

可检测出系统驱动的增加和删除的变化。

- 4)服务:

可检测出系统中服务条目、状态、属性等信息的变化。

- 基于硬件的安全策略分发器

通过该技术/软件提供了一个硬件设备可以对产品进行统一的策略管理以及日志审计。可以集中管理多台受该技术/软件保护的服务器,并检查其运行状态。

#### (5) 社保费管控平台

社保费管控平台建设,着力于生产系统实际“痛点”,根据社保费征收业务特点和流程、部门职责以及信息共享平台业务需求,税务部门 and 人社部门需要在社会保险参保登记(税务登记)、申报缴费、异常业务处理(如缴费异常业务、特殊缴费业务、退费业务等)、业务财务对账等业务环节实现信息共享和业务协同。为使各环节、全流程衔接紧密,业务经办顺畅,方便监控各环节业务异常情况。

#### (6) 一户式分析

以单户纳税人为中心,全方位聚合纳税人各类标签信息,包括登记、认定、申报、征收、优惠、评估、稽查、风险、信用等个体信息,任职、投资、交易等关系信息,以仪表盘的方式直观动态的进行展示,使得税务干部能够全方位、深入解剖每一个纳税人。

**基础信息:**展示纳税人登记信息、税费种认定、税收社保、财务报表、税款征收。

**关键指标:**系统根据常见的税收分析和财务分析而设置的指标方式,在满足用户需求的情况下,由系统自动进行指标分析,并得出结果。

**发票透视:**该功能可以查看纳税人的发票往来信息。

**关联关系:**发现纳税人自身关系,如总分机构、对外投资、发票购销、股

东关系；还可以挖掘和其他纳税人的关联关系，如同购票员的企业、同财务负责人的企业、同办税员的企业和同法定代表人的企业。可以通过列表切换了解关联关系的详细信息，从各个角度更为全面掌握纳税人的关联信息。

#### **(7) 一局式分析**

展现数据根据用户权限机关统计相应层级数据。省局权限用户统计全省数据，市局用户统计全市数据，区县用户统计全区县数据。

税务登记：登记户数、企业户数、个体户数、非正常户数

1) 登记户数指截止当前数据更新时点的纳税人登记总户数。点击图标跳转到纳税人登记情况分析表。

2) 企业户数指截止当前数据更新时点的纳税人企业户数。点击图标跳转到纳税人登记情况分析表。

3) 个体户数指截止当前数据更新时点的纳税人个体户数。点击图标跳转到纳税人登记情况分析表。

4) 非正常户数指截止当前数据更新时点的纳税人状态为非正常的户数。点击图标跳转到纳税人登记情况分析表。

税收分析：税收收入、税收增长率、计划完成率、分税种收入及增长率

1) 税收收入指本年累计入库数。点击图标跳转到入库情况的分地区税收收入库情况。

2) 税收增长率指本年累计入库数同上年同期入库数的增长数。 $(本年 - 上年) / 上年 * 100\%$ 。点击图标跳转到入库情况的分地区税收收入库情况。

3) 计划完成率指本年累计入库数/本年计划完成数\*100%。点击图标跳转到入库情况的分地区税收收入库情况。

4) 增值税、消费税、企业所得税，入库数各多少，同比增长或下降。点击图标跳转到入库情况的分税种税收收入库情况表。

税源税负：增值税税负、增值税税负同比，企业所得税贡献率，企业所得税贡献率同比。需要在首页标明数据所属季度。

1) 增值税税负指本区域的税负值，取上一季度。点击图标跳转到一般纳税人增值税税负分析情况表。

2) 增值税税负同比指本区域的税负值上年同比。点击图标跳转到一般纳税人增值税税负分析情况表。

3) 企业所得税贡献率指本区域的贡献率，取上一季度。点击图标跳转到企业所得税贡献率分析（分单位）。

4) 企业所得税贡献率同比指本区域的贡献率上年同比。点击图标跳转到企业所得税贡献率分析（分单位）。

### **(8) 增值税发票风险防控系统**

支持查询发票发明细信息，明细信息包括开具单位、受票单位、发票号码、发票代码、货物名称、型号、单价、数量、金额、税额等信息。具体分为发票明细查询、发票台账查询、企业上下游和货物上下游。从宏观层面掌握全国发票的交易流向情况，具体功能包括行政区域发票流、经济区域发票流。行政区域发票流，主要监控全国各个省之间的发票流向情况。查询与纳税人有交易关系的企业的发票链条数据，可以查询当前企业的上下游企业交易信息，以及以上下游企业为扩展的交易层级追溯。可以按照交易金额、税额、发票份数筛选重点关注的纳税人，再追溯这类企业的交易链条关系。

### **(9) 复工复产及非接触式办公**

利用大数据平台整合来自核心征管、发票系统、防伪税控的数据。统计疫情期间申报业务‘非接触式’申报率、发票领用业务‘非接触式’申报率、疫情期间延期申报申请平均审批时间、疫情期间延期缴纳纳税申请平均审批时间。

### **(10) 风险一户式**

构建智能、便捷的“一户式”全税费种风险全景分析模块，加强“一户式”风险归集应用，充分运用总局云平台、金税三期系统和大数据分析应用集成平台中风险成果，解决系统中风险信息分散、风险信息联动不足、风险孤岛等问题，为基层提供单户纳税人风险分析、区域风险分析、风险运行趋势分析的个性化数据应用服务，实现全税费种风险横向联动，为基层税务机关开展风险管理提供坚实数据支撑。

### **(11) 广西大企业管理应用平台**

汇集大数据平台各类税收数据并按集团维度形成大企业主题数据集市，设有数据管理、事务管理、风险分析、税源监控、集成分析、服务管理等模块，包括名册展示、财报监控、风险扫描和报告生成、风险人工复评和风险应对任务流转、风险任务查询统计和跟踪、电子帐套数据查阅和分析、集团税源结构分析、集团入库情况统计、集团涉税事项监控、大企业服务工作台账、大企业纳税信用查询和预警等功能菜单，为开展集团化税收管理提供数据支持和应用保障。在数据方面，定期维护大企业主题数据集市，进行数据归集和清洗、数据提取和加工等；在应用方面，保障相关应用功能平稳运行，及时解决日常使用过程中发现各类功能问题。

#### **①广西大企业管理应用平台运维服务内容**

##### **1) 数据问题分析、处理与咨询**

负责广西大企业管理应用平台数据问题分析与处理、数据结构咨询等工作。

(一) 工作内容

1. 及时响应和解决采购人使用系统中遇到的数据问题。负责分析、定位数据问题原因，拟定处理方案，按采购人流程审批后完成数据处理和结果验证。

主要包含：

(A) 大企业名册数据运维：

每年根据采购人提供的大企业名单（含千户集团、列名集团及其成员单位）匹配相关信息后并更新广西大企业管理应用平台中的名册信息，并将名册数据同步至“黑匣子”数据库中，确保广西大企业管理应用平台各功能正常使用，也确保“黑匣子”名册信息完整。

(B) 财报监控数据运维：

①根据采购人财报监控业务需要，对采购人的需求进行分析、脚本编写、数据抽取，调整财报数据校验规则；

②针对大企业每个季度财务报表报送以及年度财务报表报送情况进行监控，根据采购人提供的白名单，在后台做白名单更新处理；

③根据采购人在财报监控工作中，针对数据校验不通过的问题进行分析、定位问题原因，并将原因及处理方案告知采购人；

④根据采购人工作需要，调整财报后台数据自动刷新频率，必要时需人为刷新，协助采购人财报监控工作进行顺利；

⑤按照采购人要求，每次财报工作完成后，在规定时间内做好数据快照；

⑥针对快照数据创建失败的问题进行排查、分析及处理，如处理不了的，需及时向采购人说明及提供处理方案。

(C) 通讯录顺序调整：

采购人根据人员工作调动情况提供通讯录名单，运维人员需要按照名单上的顺序在后台数据库进行数据更新、调整。保障广西大企业管理应用平台通讯录功能模块能按需显示。

(D) 风险任务运维：

①按照采购人提供的风险名单及工作安排，建立风险任务对名单数据进行风险扫描，分析、排查并处理扫描过程中出现的问题，扫描完成后，把相关风险报告通过内网提供给采购人；

②根据采购人在风险分析或风险应对工作的安排，针对采购人提出的问题对相关风险任务（如任务完成时间等）进行后台数据调整，协助采购人风险工作进行顺利。

(E) 税务人员税务机关调整：

采购人根据人员工作调动情况提供人员名单，运维人员需要按照名单上的

信息在后台数据库进行数据更新、调整。保障开通权限的用户能正常登录广西大企业管理应用平台并能根据当前所属税务机关相关权限使用平台中的相关功能。

(F) 大企业过期用户数据运维

按照数据安全规范要求，运维人员需要按照采购人指示，不定期对离职人员、长时间未登录平台的用户账号进行停用或者删除用户处理。

(G) 通知公告数据调整

按照采购人要求，屏蔽、删除、恢复采购人指定的通知公告。

(H) 信用数据问题排查（信用日常和历年信用）

①运维人员每月月初需要手动执行信用月度预评数据基础数据抽取作业，对作业执行后不出数据的问题进行分析、排查、处理，保障广西大企业管理应用平台信用日常功能数据正常；

②根据采购人在使用信用日常功能提出的问题进行分析、排查、处理；

③根据采购人在使用历年信用功能提出的问题进行分析、排查、处理。

针对上述应用业务数据的正确性、有效性保障。

归纳、总结、分类数据问题处理方案，建立并完善广西大企业管理应用平台数据问题处理知识库，提高数据问题的处理效率。

负责为采购人提供广西大企业管理应用平台数据结构的技术支持，梳理提供数据结构技术文档，协助采购人开展广西大企业管理应用平台数据查询分析工作。

4. 协助采购人开展广西大企业管理应用平台错误数据清理，根据异常错误数据，提出错误数据清理方案，并组织实施清理。

**2) 数据服务**

针对大企业平台的个性化需求，需从指定的业务系统数据源将数据经过抽取、清洗、加载后，存储到大企业主题数据集市。主要工作内容如下：

**a. 数据抽取保障**

数据抽取分为日常增量抽取和全量抽取，日常增量抽取由系统设定的定时任务自动执行，全量抽取由技术人员设置定时任务或手动执行。主要目标是保障数据抽取的任务调度正常，抽取的执行结果正常。主要工作内容包括：

数据抽取任务调度状态维护。技术人员每日检查数据抽取任务的调度配置状态，发现问题及时解决；根据数据量及业务办理日期变化等情况，对任务调度进行必要的调整。

日常增量抽取保障。技术人员每日对抽取的结果进行检查，检查各抽取任务是否执行完毕、是否执行正常，发现问题及时解决；对抽取的结果日志进行

分析，采用技术工具对抽取结果进行技术性校验。

全量抽取。在业务系统数据源发生较大变化时，应采用全量抽取的方式重新进行全量抽取。技术人员在采购人责任人的要求下，停止增量抽取任务，手工启动全量抽取的任务，监控全量抽取过程，检查全量抽取结果。

#### **b. 数据加工保障**

数据加工是对已经抽取到大企业主题数据集市的业务数据进行汇总、统计、分析的过程，数据加工过程根据数据集市的数据产生同步需求，采用全量加工或增量加工两种方式，主要是保障数据加工的任务调度正常，加工的执行结果正常。

#### **c. 数据运算性能调优**

技术人员对接收到和检查发现的数据运算性能问题进行分析，同时定期对数据运算整体性能情况进行检查，根据分析结果采取脚本调优、性能参数调整等方法分别实施优化。主要工作内容包括：

运行监控。定期监控和分析数据及应用的性能状况。

接收问题。接收采购人责任人、系统使用人员、运维人员等提出的与系统性能相关的问题。

出具解决方案。针对接收到和发现的性能问题进行分析定位，针对具体问题确定需执行的操作，并制定相应解决方案。

处理问题。针对具体性能问题执行解决方案。

### **②大企业电子账套数据采集和加载服务**

为采购人每年定期开展的大企业电子帐套数据采集工作提供技术支持服务（包括千户集团及广西列名大企业），并协助完成数据加载工作（广西列名大企业）。

#### **1) 服务对象**

采购人每年对广西千户集团和部分广西列名大企业开展电子账套数据采集工作。根据往年情况预估，涉及千户集团为 26 个集团、约 2400 户成员企业，涉及广西列名大企业约 25 个集团、约 500 户成员企业。具体企业数量根据当年工作安排确定。

#### **2) 前期准备工作**

根据采购人要求，基于总局标准版工具制作广西列名大企业电子帐套数据采集工具及加载工具，采集测试环境搭建、协助完成软件操作培训、操作视频录制、企业财务软件信息维护、自主导出模板制作等工作。

#### **3) 企业技术支持服务**

按照采购人工作安排，向开展数据采集工作的千户集团和广西列名大企业



提供以下技术支持服务。

一是提供 5×8 的热线电话应答支持。安排专人对大企业在数据采集过程中涉及电子帐套采集软件使用方面的问题进行解答。

二是提供线上远程指导。建立专属 QQ 群，集中解答大企业提出的采集软件使用相关问题；根据企业需要，通过电脑远程协助的方式解决企业财务人员在采集过程中遇到的相关问题。

三是提供采集模板定制服务。对于采集软件未内置千户集团电子帐套采集模板的，根据企业需要配合定制采集模板，提供给对应企业使用。

四是提供上门现场支持服务。在必要情况下，根据采购人安排到企业（广西范围内）实地解决企业财务人员在采集过程中遇到的疑难问题。每年上门现场支持的次数、涉及企业和实施时间等由采购人根据需要进行安排；每次上门现场支持的天数根据具体任务确定，一般为 1-2 户企业 1 天（不含外地往返时间）。

#### **4) 数据加载管理**

维护广西列名大企业电子帐套加载功能及其数据库，确保电子帐套数据可以正常加载到数据库中；电子帐套浏览功能可精准解析、还原所采集的数据，分析功能可正常使用；加强电子帐套浏览权限的管理，确保内控内生化机制有效运转，只有被分配相关风险管理任务或被授权的账号才可通过应用功能调阅对应企业帐套。

#### **5) 列名企业账套数据迁移**

为确保电子帐套数据安全，广西列名大企业帐套加载数据库应独立管理，不得与其他系统及其数据库共用服务器。目前因为账套数据加载端设置及安全策略防护设置问题，数据无法直接加载到大企业账套数据库服务器中进行存储。需要加载至一体机数据库后，再把相关账套数据迁移至账套数据库服务器中进行存储。

#### **6) 数据保密要求**

电子帐套数据是企业高度敏感的数据，涉及帐套数据采集、加工、存储、应用等方面的技术人员均要与采购人签订保密协议，在工作中严格遵守数据保密各项要求，不得以任何方式泄露电子帐套数据。运维服务商应加强员工管理，不随意更换涉及电子帐套数据相关工作的技术人员，并配合采购人做好数据安全教育和数据安全管理工作。

#### **③平台数据迁移**

广西大企业管理应用平台原生产环境数据库部署在一一体机上，此前针对数据库表空间做过评估，表空间使用率已经超过 90%，而一体机又无法扩容，有

可能导致部分功能数据抽取失败、应用功能模块会因此受到影响。为保障平台各应用功能模块不受影响，需要出具平台数据迁移方案提供给采购人，需经与采购人沟通、确认后实施数据迁移工作。确保广西大企业管理应用平台生产环境数据安全、无遗漏进行迁移。

#### **④其他运维事项**

##### **1) 月度报告**

运维周期内，每月月初，运维人员需要撰写上个月月度运维报告。报告中包含但不限于上个月运维过程中对监控配置项、版本升级、版本积压情况、业务受理情况、本月重点工作事项的说明等。

##### **2) 年度报告**

运维期结束后，运维人员需要撰写一份年度运维报告。报告中包含但不限于上一年度运维过程中对监控配置项、版本升级、版本积压情况、业务受理情况、本月重点工作事项的说明等。

##### **3) 操作手册编写及更新**

运维周期内，运维人员需要根据平台功能模块的调整，编写平台操作手册，功能模块有调整或者有新增功能时，需要及时更新操作手册。

##### **4) 更新相关业务流程图**

运维周期内，如平台具有业务流转的功能模块有流程变更时，运维人员需及时更新业务流程图。

##### **5) 操作视频录制**

运维周期内，运维人员需要录制广西大企业管理应用平台操作视频，供采购人人员学习使用，如功能模块有调整、或新增功能时，运维人员需及时录制并更新相关操作视频。

##### **6) 资料下载常用工具维护**

运维周期内，运维人员需要根据采购人要求更新资料下载-常用工具功能模块中的资料。

##### **7) 供应链材料准备**

运维周期内，运维人员需要根据采购人信息中心的工作要求撰写、打印广西大企业管理应用平台供应链材料，装订好后提交给采购人指定人员。

##### **(12) 集成平台岗责权限体系维护**

大数据集成平台门户集成多个厂商应用系统，集成平台岗责权限体系复杂，需要定期梳理、保障大数据应用集成平台各系统正常运行。维护集成平台与各子系统权限权限体系

#### **2. 自然人电子税务局运维服务内容**

自然人电子税务局为自然人和扣缴义务人提供远程办税功能的相应渠道，包括手机 APP、WEB 网站、扣缴客户端，为自然人、法人提供个税涉税服

务，同时根据自然人电子税务局建设规范，为广大纳税人提供如消息互动、公众服务、办税查询等纳税服务。主要包括：自然人统一办税门户（WEB）及应用，自然人统一办税门户（APP）及应用，客户端统一办税门户及应用，同时还包括账户中心、第三方支付平台、消息中心、云 workflow 平台、客户端统一升级服务、产品集成平台、短信平台、云应用集成平台等通用服务功能。

自然人电子税务局税务端作为个税核心征管生产交易系统，将承担个税核心业务如登记、优惠、申报、征收、核算、证明、异议申诉、催报催缴后续管理、统计分析等核心业务处理和数据存储，同时提供税务人员端所有个税依申请和依职权业务受理渠道，并对自然人电子税务局相关业务功能提供数据查询和接入并进行统一业务校验和数据存储。

个人税收管理系统作为个税核心征管生产交易系统，将承担个税核心业务如登记、优惠、申报、征收、核算、证明、异议申诉、催报催缴后续管理、统计分析等核心业务处理和数据存储，同时提供税务人员端所有个税依申请和依职权业务受理渠道，并对自然人电子税务局相关业务功能提供数据查询和接入并进行统一业务校验和数据存储。

### **（1）自然人电子税务局**

#### **1) 云上运维服务内容**

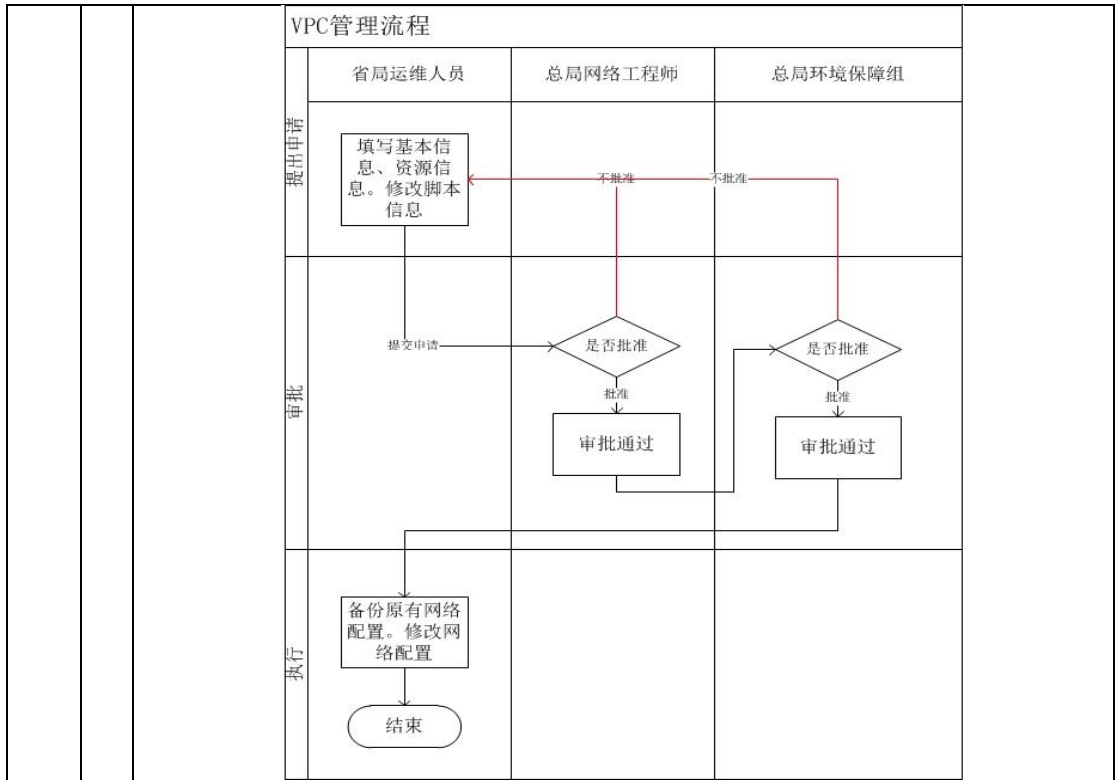
##### **①VPC 管理服务**

根据业务发展需求，采购人可能需要申请云上的 VPC 资源进行使用，或者是管理已经基于 VPC 网络的计算资源，或者是将 VPC 接到省局端的专有网络中，形成一个按需定制的网络环境，实现应用的平滑迁移上云和对数据中心的扩展。

在实际使用的过程中，需要运维人员对各种网络资源进行配置，运维人员可以在 VPC 上完全掌控该网络资源，例如选择 IP 地址范围、配置路由表和网关等，也可以在自己定义的专有网络中使用阿里云资源如 ECS、RDS、SLB 等。

为了更好的利用好 VPC 资源，需要对 VPC 进行管理。其中最重要的是保障运维人员操作的可靠性。因此需要引入管理流程制度。

VPC 管理流程如下图所示



VPC 管理流程

采购人运维人员在拟定好 VPC 网络拓扑方案、资源说明、配置脚本后，向总局网络工程师发出申请。网络工程师经技术角度分析后，如果发现网络配置等不合理，则立即驳回，要求重新填写；如果发现诉求合理，则提交总局环境保障组人员审批。总局环境保障组从环境配置角度查看该请求，如不符合实际情况则驳回，如符合要求，则审批通过。

审批通过后，采购人运维人员则需对现有的 VPC 网络配置进行备份操作。然后进行 VPC 网络分配操作。

②虚拟云权限管理服务

在采购人端，运维人员负责权限的申请及验证工作。

1) 权限管理服务原则

权限申请遵循最小化原则，只申请必要的权限，不申请过度的授权。

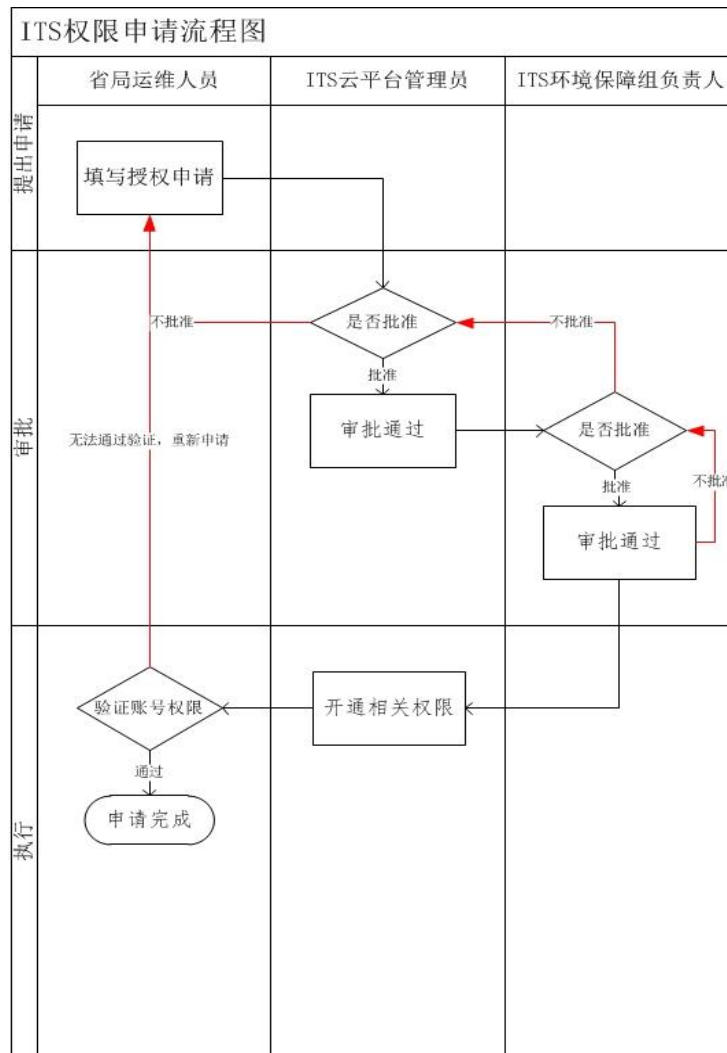
权限严格验证原则，对总局下发的权限进行仔细验证，对于不符合申请的权限做驳回操作，并请求总局再次下发。

2) 权限管理服务范围

1. 云平台管控平台权限
2. 云平台服务器权限
3. 租户内资源权限
4. 堡垒机管理权限

### 3) 权限申请及验证流程

权限申请及验证流程如下图所示：



权限申请流程图

采购人运维人员负责向云平台申请授权，待权限开通后，采购人运维人员对账号权限进行验证，如果验证无法通过，则重新申请权限。如果验证通过，则完成申请。

### 2) 云端资源管理服务

根据业务发展需要，采购人端系统有时需要申请总局云端资源，待使用完成后，需要将该资源释放。为了能高效利用云端资源，提高工作效率，需要对资源进行管理。资源管理服务分为：资源分配服务和资源释放服务。

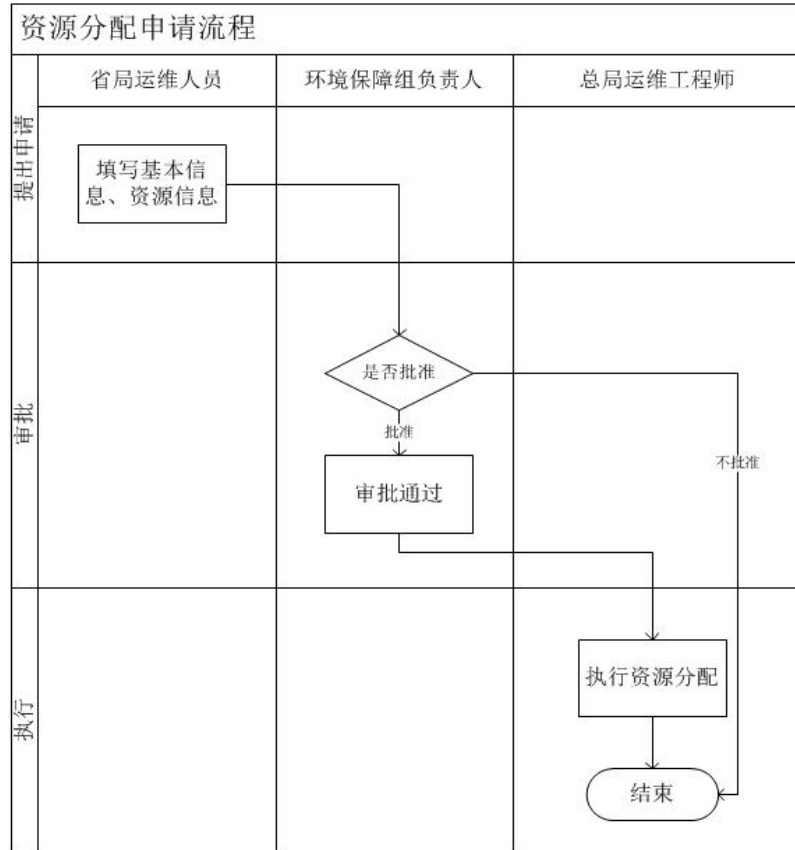
#### ①资源分配服务

申请流程为：申请人填写基本信息、资源信息，环境保障组负责人审批，审批通过，交由运维工程师执行资源分配；审批不通过，结束流程。

其中，申请人基本信息包括：项目名称、资源申请环境（开发测试、联调

或正式)、所在部门,提供申请单位、申请人、联系方式及邮箱。

资源申请及资源分配流程如下:



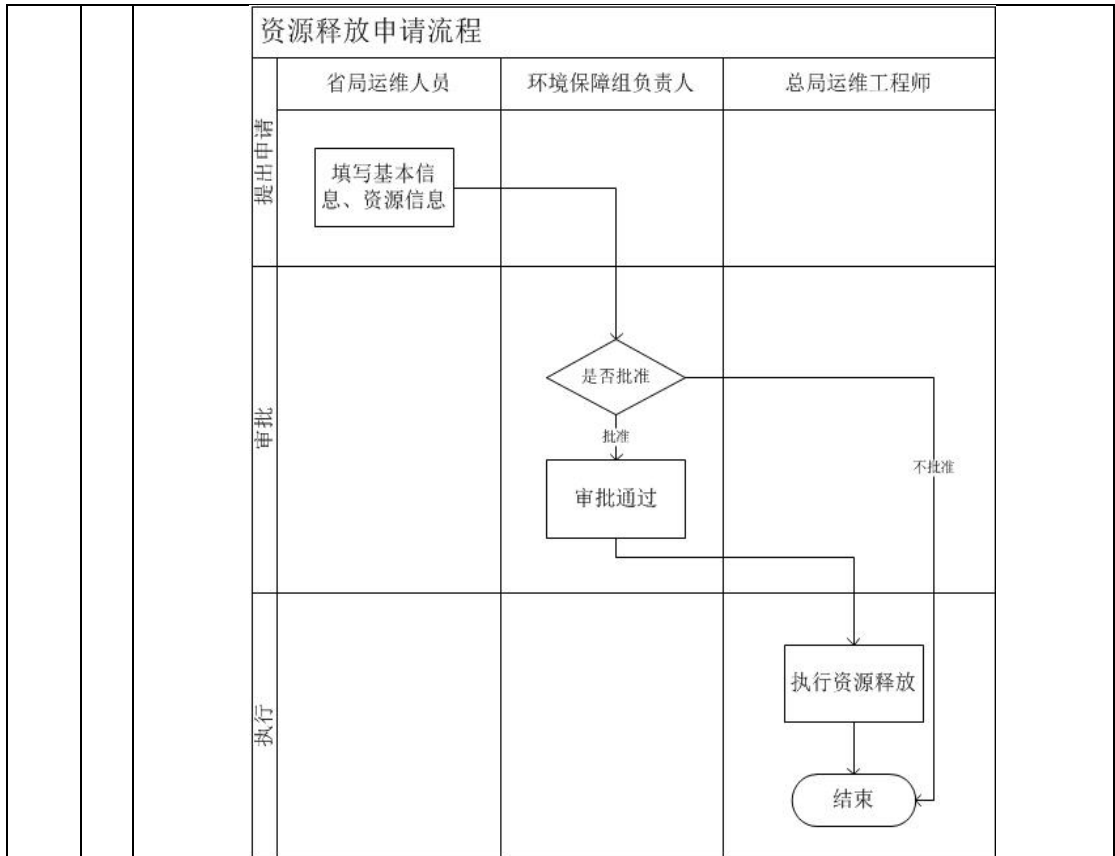
资源分配流程图

### ②资源释放服务

申请流程为: 申请人填写基本信息、申请释放资源信息, 环境保障组负责人审批, 审批通过, 交由运维工程师执行资源释放; 审批不通过, 结束流程。

其中, 申请人基本信息包括: 项目名称、申请资源释放环境(开发测试、联调或正式)、所在部门, 提供申请单位、申请人、联系方式及邮箱。

资源释放流程如下:



资源释放流程图

### 3) 云下运维服务内容

#### 1) 日常巡检服务

##### ① 巡检服务范围

巡检包括但不限于以下内容：

- A. 机房基础设施及硬件
- B. 网络情况
- C. 云平台
- D. 自然人电子税务局系统
- E. 其他软硬件系统

##### ② 巡检工作内容及流程

巡检人员对机房基础设施及硬件、网络情况、云平台、自然人电子税务局系统进行巡检，并对巡检结果进行记录、截图。生成巡检报告。巡检人员结合巡检报告初步判读巡检结果。

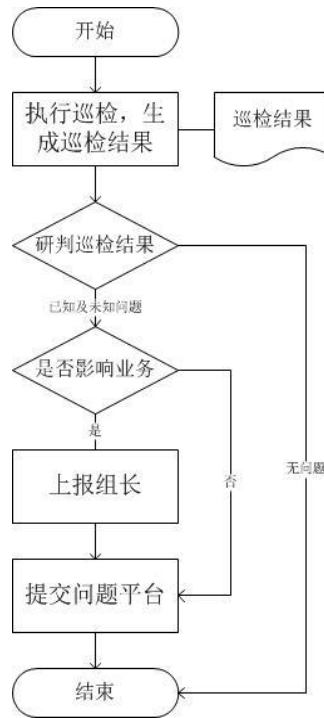
如果巡检结果一切正常，则结束巡检工作。

如果巡检结果有问题，则需分类已知问题和未知问题。

对未知问题，需要判定业务影响。如果影响业务或疑似影响业务，第一时间电话通知组长。

对已知问题，如果超过一周仍未解决，则通知组长，推动收敛。

工作流程图如下：



### ③巡检服务标准

对于非疑难异常问题，要求 12 小时内对该问题进行解决，并关闭问题单。

对于疑难问题，要求迅速拉通运维、研发对该问题进行评估，及时通知业主，输出问题解决方案、时间计划等。

日常巡检服务于每日开展至少 1 次，开始时间不晚于早 9 时整。

巡检工作需有截图记录。

问题需及时反馈，重大问题不超过 5 分钟报送运维组长层面。

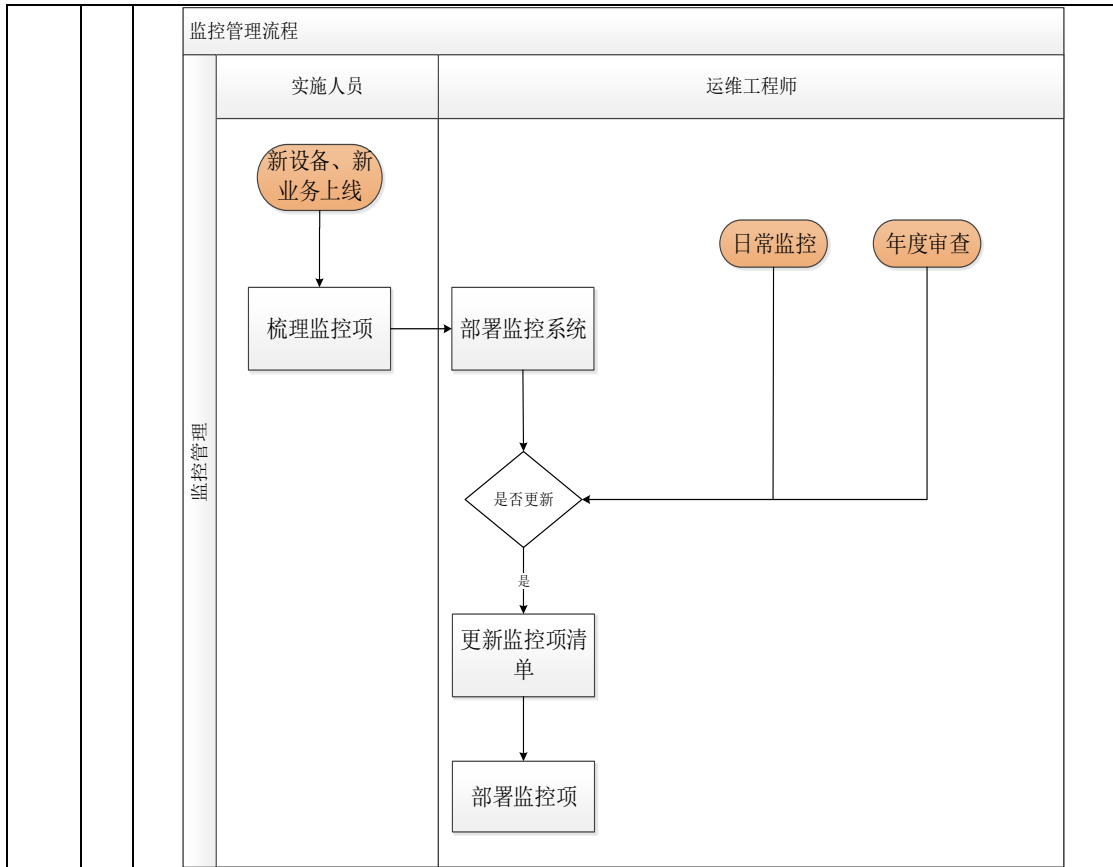
#### 2) 自然人电子税务局省局端系统监控服务

自然人电子税务局省局端系统监控服务是运维服务当中的重要工作。监控服务是指对自然人电子税务局系统的运行情况进行实时、不间断的查看，以保障系统的顺利运行。

该监控服务可以分为：日常监控服务、监控项变更服务、新增监控项服务、新业务上线监控服务、监控审查服务等。

监控工作流程如下图所示：





①日常监控服务

在日常监控工作中，运维工程师保持监控屏幕实时刷新，注意接收告警信息，及时发现异常并及时处理。并可以对业主关心的业务进行重点监控。

②监控项变更服务

当监控项的阈值或监控条件发生变更时，运维工程师需要及时在监控系统对监控项进行变更，变更完成后，及时更新监控项清单。

③新增监控项服务

当发生新增监控项，如业务变化、新增资源、新增节点等情况时，运维工程师需及时将监控项部署到监控系统，部署完毕后，及时更新监控项清单。

④新业务上线监控服务

新业务上线前，运维人员梳理新系统的监控项，运维人员将监控脚本部署到监控系统，并实时对上线过程进行监控。上线完成后，最终出具监控项清单，以及监控系统的运维手册。

⑤监控审查服务

运维人员可以对监控工作开展年度审查。运维团队可以通过分析发现问题，提出监控优化建议，并根据建议进行监控项开发，将调整的监控项或者新增的监控项部署到监控系统，并更新监控项清单。

⑥版本管理服务

当总局端自然人电子税务局发布新版本时，省局运维人员需配合总采购入面，做好自然人电子税务局系统省局端新版本的验证和升级工作。

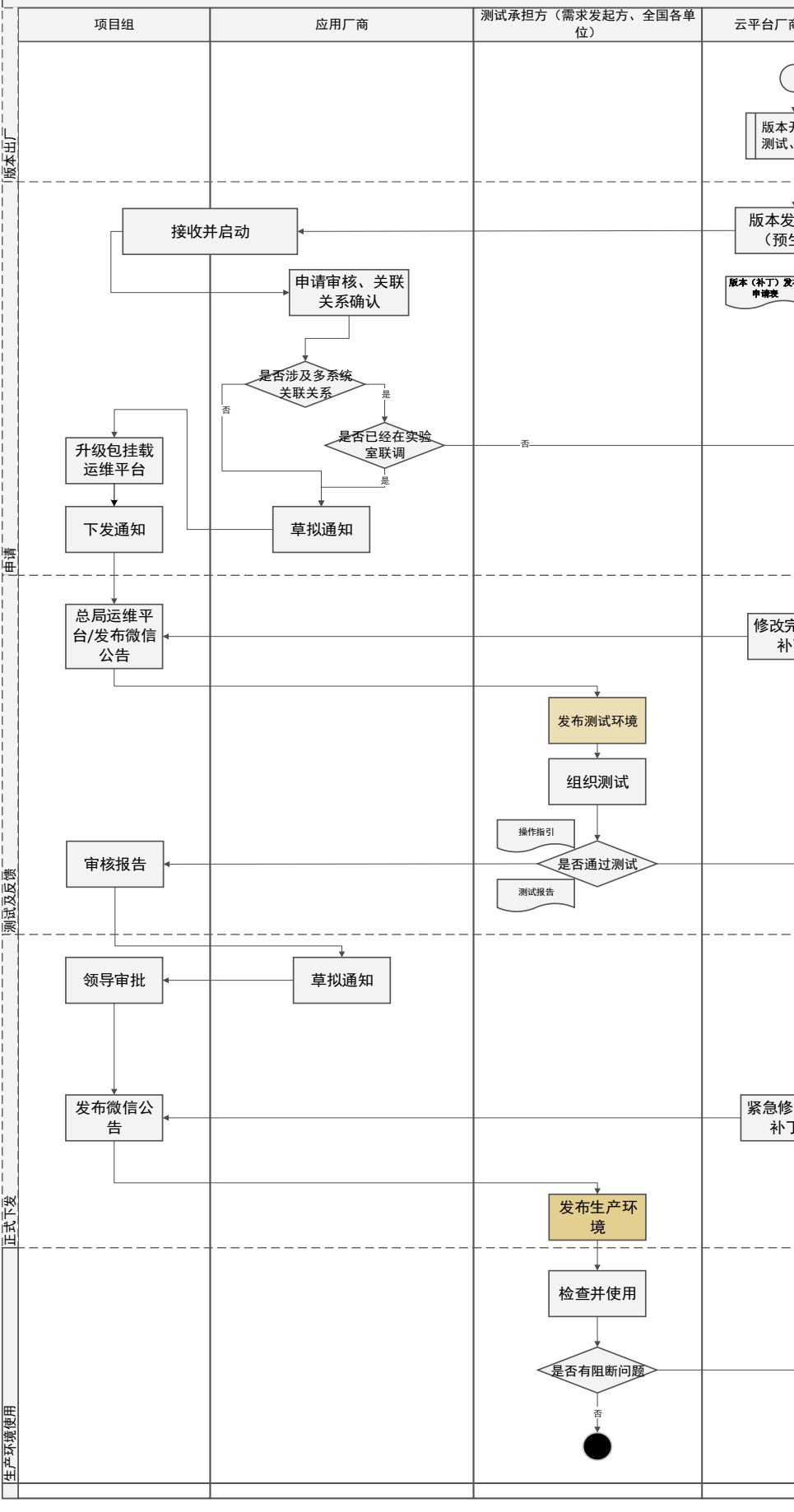
在新版本发布后，采购人运维人员需要先在测试环境下对新版本进行部署、测试验证。如测试不通过，则需向总局反馈相关问题。如测试通过，则经项目组审批后进入生产环境进行验证。

在生产环境中，采购人运维人员通过使用真实数据对新版本内容进行验证，若遇阻断问题且涉及代码修改的，应反馈开发单位修复并下发紧急补丁；若遇阻断问题且不涉及代码修改的，应反馈给开发单位修复问题。

在版本顺利发布后三天之内，采购人运维人员需对系统进行密切监控，如发现异常启动相关应急预案，必要时回退版本。

**版本管理的整体流程如下图所示：**

版本发布流程



根据上图，运维人员版本管理服务流程归纳总结如下：

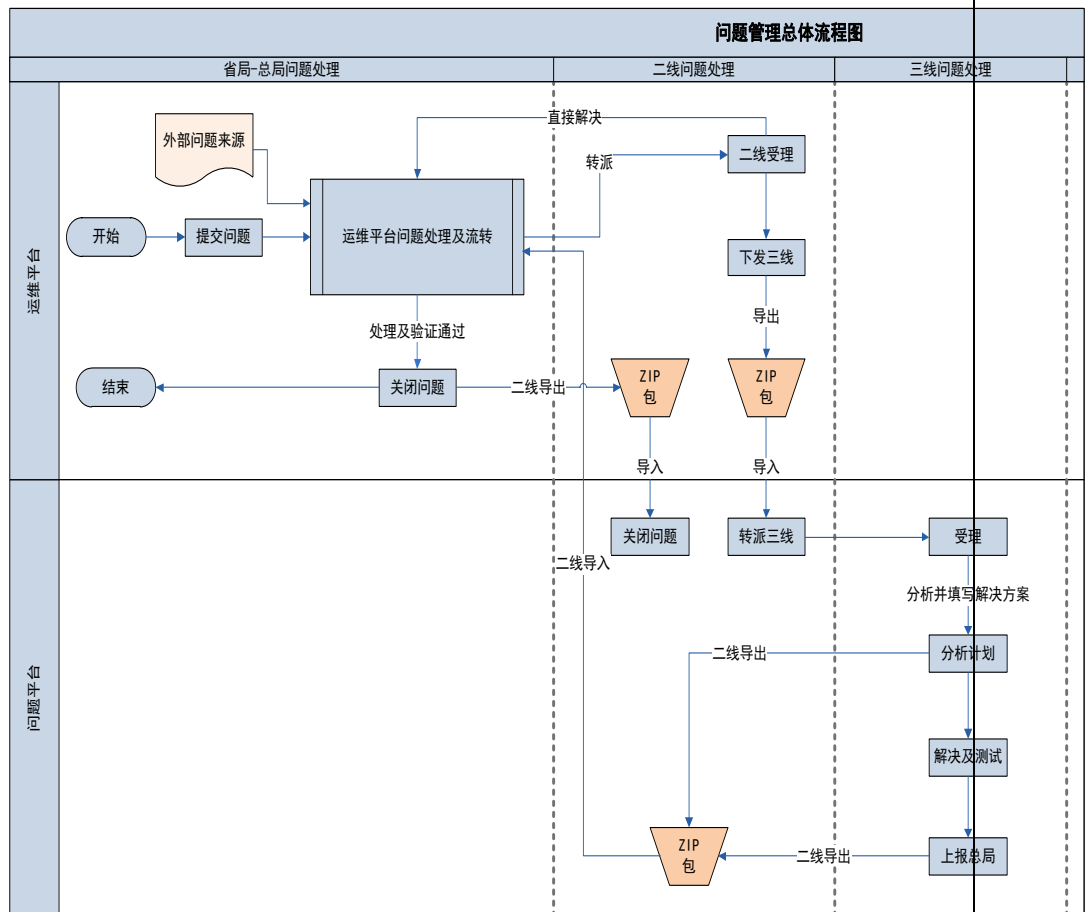
序号	流程	责任方	说明
1	版本发布执行（测试环境）	运维人员	完成测试环境部署及验证。
2	版本发布执行（生产环境）	运维人员	完成生产环境部署及验证。
3	版本发布监控	运维人员	版本发布结束（程序包完成部署验证）3天内，需对新版本上线运行情况进行密切监控，发现异常启动相关应急预案，必要时回退版本。

### 3) 问题管理服务

目前，自然人电子税务局系统采用税务总局—省—市—县四级运维模式。

系统进入正常运维阶段后，对运行保障提出了更高的要求。为进一步强化应用系统运行维护管理工作、提高效率，确保应用系统稳定、安全、高效运行，各省局应使用总局运维管理平台对系统问题进行统一管理。

问题管理流程如下图所示：



运维人员在运维平台服务管理系统中录入问题单，当录入的问题单在区内

或一线人员解决不了需要二线人员或三线人员解决时，将这类问题单通过运维平台填写好相关信息后上报到总局运维平台服务管理系统的问题流程中形成问题单，上报到总局运维平台的运维问题单会转派到二线运维岗进行评估分析，此时问题单的状态标志位为“待解决”。

#### 4) 数据运维服务

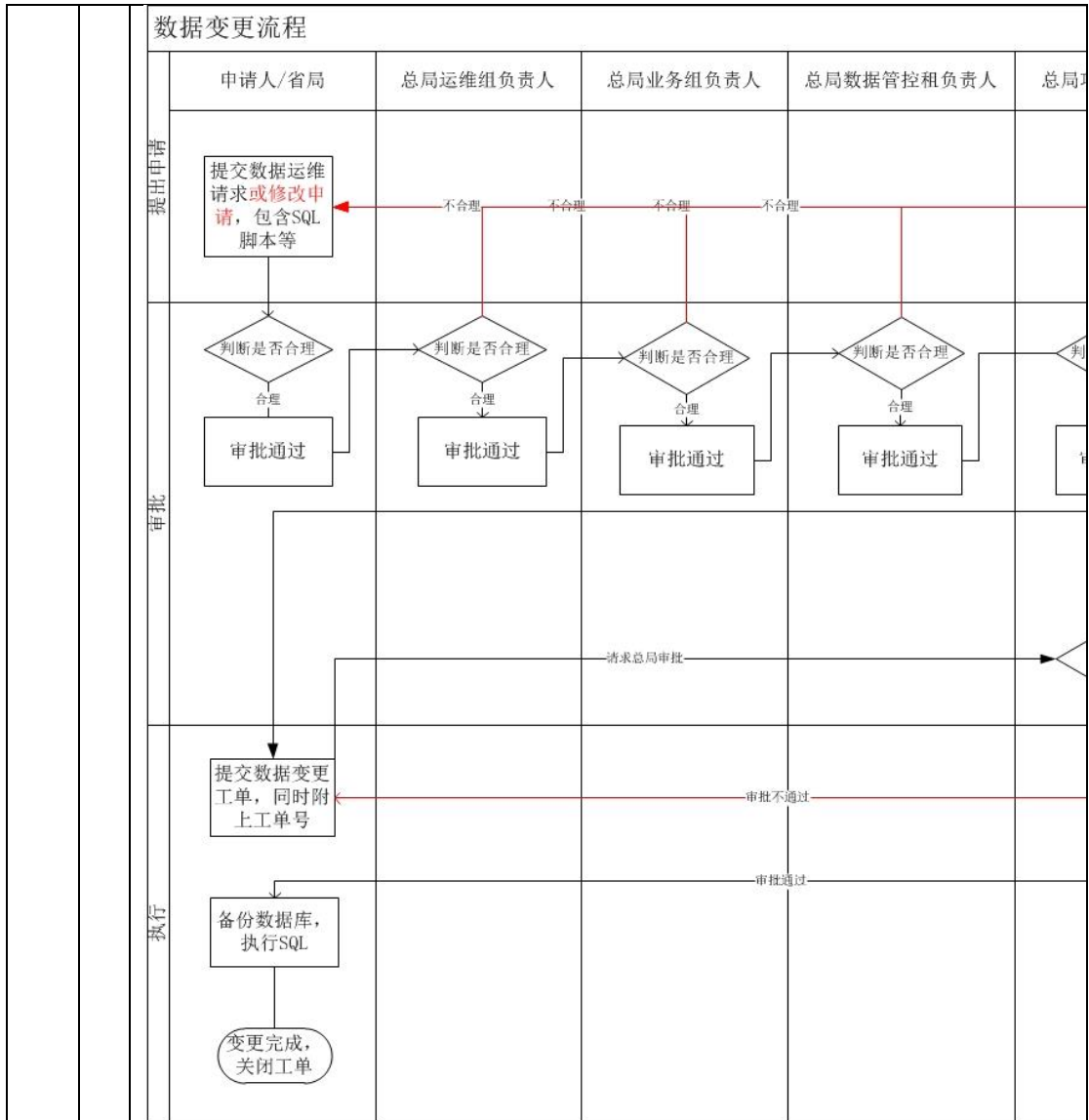
数据运维服务包括：数据查询服务，报表支持服务，数据变更服务。

数据查询服务是指现场运维人员根据业主需求，对业主所关心的数据进行检索、查询、筛选，并将结果输出给业主。

报表支持服务是指现场运维人员根据业主需求，对业主所关心的复杂数据诉求进行报表化处理并输出数据报表。

数据变更服务是指对业务数据和代码参数进行增删改操作，此类操作风险性较高，应提交数据变更运维申请单，通过数据变更运维流程确保运维的规范性和正确性。

下图为数据变更流程：



**数据运维服务流程图**

从图中可以看出，数据运维的提出者、变更脚本编写者均为省局侧的现场运维人员。总局人员和其他运维团队负责对现场运维人员提出的数据变更方案进行审核。如果审批通过，则现场运维人员需要先对数据库进行备份。随后执行更新脚本。更新完毕后，如果经测试没有问题，则可以认为完成了此次数据运维变更服务。

5) 安全管理服务

安全管理服务包括：资产安全管理、安全巡检、安全评估与加固、安全漏洞修复、安全策略运营等。

**资产安全管理**是指，运维人员定期调研整理资产清单，包括设备、云平台、应用系统。

**安全巡检**是指，运维人员定期利用安全产品进行安全巡检工作，主要对

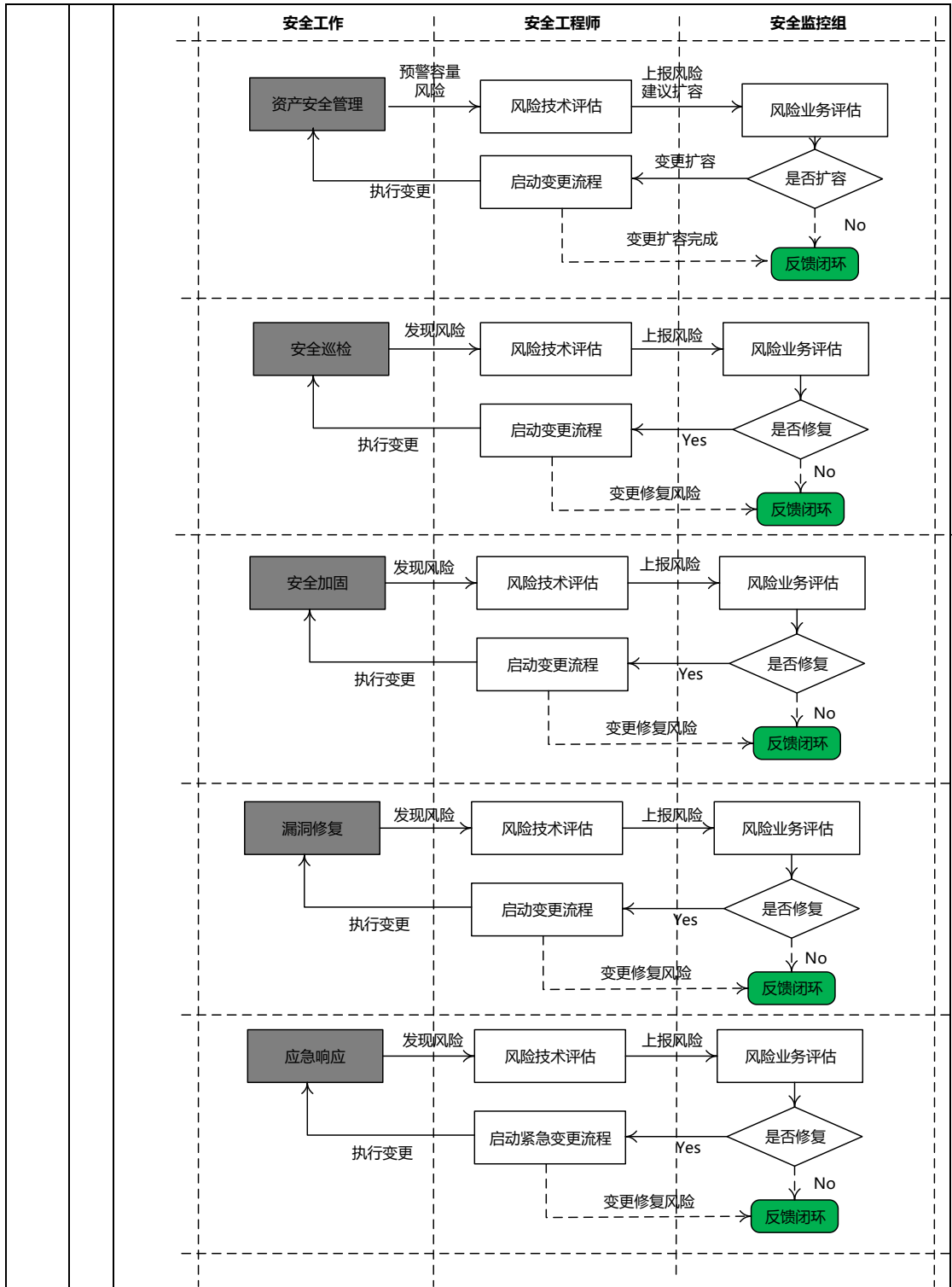
流量安全监控、安全审计和主机入侵检测产生的安全风险进行处理。

**安全评估与加固**是指，运维人员定期针对设备、云平台、应用系统进行安全评估，发现存在的网络安全、主机安全、应用安全隐患，并针对发现的安全隐患进行加固。

**安全漏洞修复**是指，运维人员对系统运行过程中发现的安全配置问题和弱口令进行修复；对云产品的安全漏洞提供修复方案，由运维工程师负责修复。

**安全策略运营**是指，对云平台、操作系统、网络的默认安全策略以及变更进行检查加固。

上述所有的安全管理工作都需要制定规范化的流程，下图即为安全管理服务流程图：



**安全管理服务流程图**

所有安全管理服务都需要参照上图中的流程进行。其中，安全工程师由运维团队指派专人负责。安全监控小组可以由现场运维人员、省局业主、总局业主、总局运维人员等共同组成。

安全管理工作需保持一定的频率才可以起到理想效果。故需制定频率规划表，对各类服务工作的频率进行规划化管理。



下表为安全管理工作执行频率规划表：

安全工作	执行频率
资产安全管理	年度
安全巡检	月度
安全评估与加固	季度
平台漏洞修复	发现漏洞当天响应
应急响应	紧急安全事件 30 分钟内响应

#### 安全管理工作执行频率表

所有安全管理服务工作的频率都需要参照上表中的要求进行。

#### 6) 故障管理服务

在省局端，部署有大量的软硬件系统，同时省级系统还需要和云端系统交互。在系统运行过程中，可能会出现各类故障。为了保障系统正常运行，需进行故障管理服务。

##### ①系统故障定义

系统故障是指系统无法为工作人员及用户提供服务、或者是其他影响到用户体验等的事件。如应用软件无法访问、数据混乱、页面打开速度极度缓慢、某些业务功能不可用等情况都属于系统故障范畴。

##### ②系统故障分类

故障分类	描述
P1	灾难性故障，系统的核心功能无法使用，影响绝大部分用户。
P2	重大故障，系统的核心功能无法使用，影响部分用户。
P3	一般故障，系统的非核心功能无法使用，影响部分用户。
P4	除 P1, P2, P3 的故障，系统的周边功能无法使用，影响小部分用户。

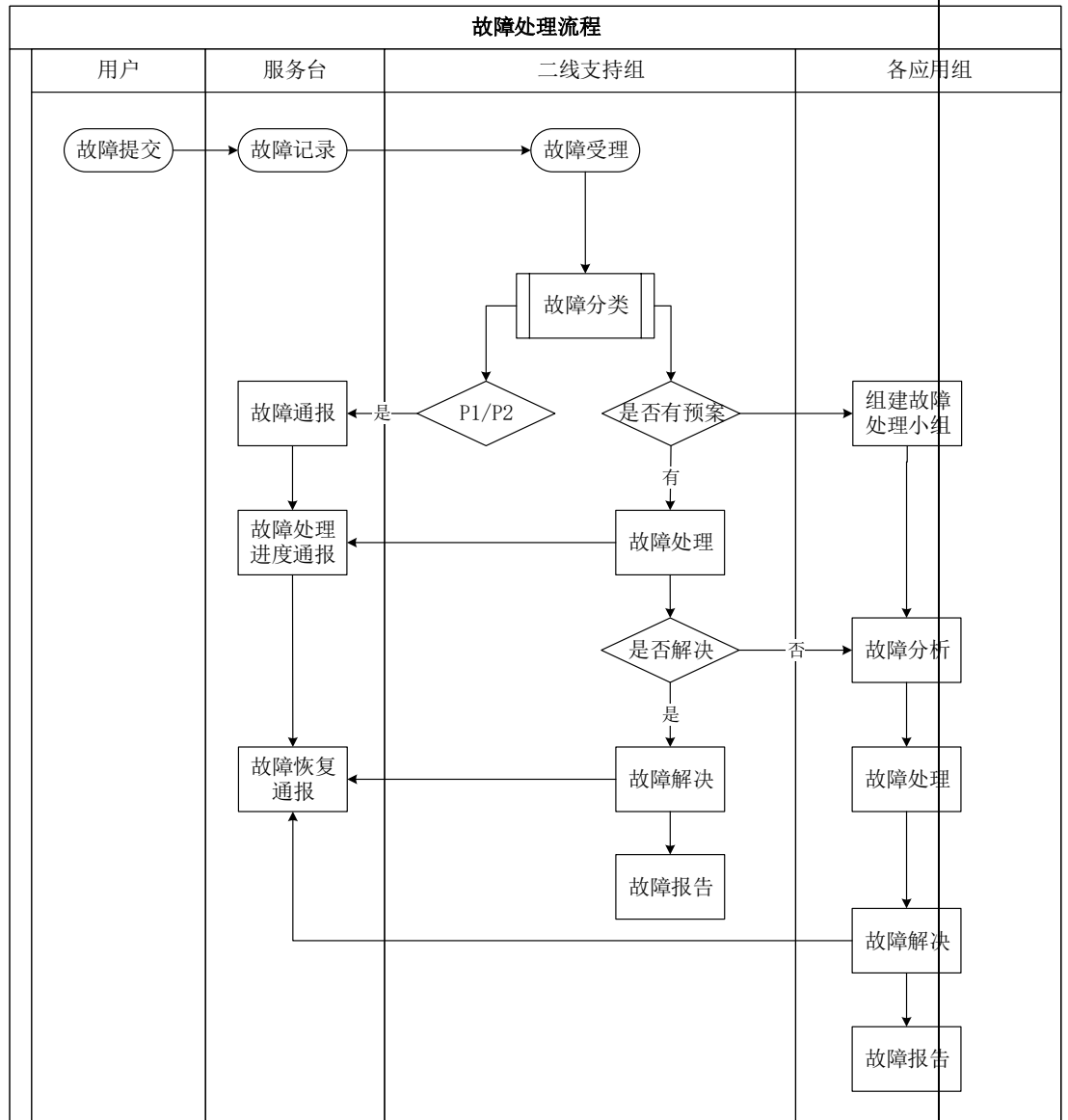
##### ③系统故障响应流程

运维小组从用户侧获得故障报告后，应及时记录并提交运维组服务台（以下简称服务台）进行记录，服务台通知二线支持组进行故障受理，如果是 P1/P2 级别故障，及时进行通报，通报给采购人、各相关厂商。

二线支持组应及时分析故障、做好故障处理，及时通报故障处理进度，故障解决后出具故障报告。

如果二线支持组无法解决故障，则转给对应的应用组或是相应厂商，由该组组建故障处理小组，分析解决故障，及时通报故障处理进度，故障解决后出具故障报告。

下图为系统故障响应流程图：



**系统响应流程图**

④系统故障响应时限

对于每一类的故障，应制定响应时间规划。根据现场情况，各类故障的响应时间应如下表所示：

故障分类	响应时限	处理时限
P1	5 分钟	2 小时
P2	5 分钟	4 小时
P3	5 小时	48 小时
P4	5 小时	1 周内

**响应时限表**

#### 4) 云上-云下链路管理服务

由于目前整体架构上分为“税务总局系统（云上）”和“各省级税务局系统（云下）”两个部分。这两部分系统需频繁进行交互，才能保障系统正常运行。

所以，保障“云上-云下”链路畅通是运维工作的重要工作内容。

各省局的网络链路运维管理需遵循总局网络链路运维管理规范。网络日常运维管理应主要完成以下工作：

①负责建立和维护网络配置信息，负责制定日常运维管理流程。

②落实网络日常监控工作，含性能监控、状态监控、告警监控等。

③开展网络健康检查工作，含网络链路检查和网络设备检查等。

④执行网络例行维护工作，含配置备份、修改密码、清理配置信息、检查标签等。

⑤做好网络故障处理工作，含故障发现、故障排查、故障处置等。

⑥开展网络运行情况析工作，编制运行报告，提出优化建议。

⑦做好操作手册、拓扑图、配置项表等文档的管理工作。

⑧做好与当地电信运营商的沟通工作，定期审查省局 IDC 机房出口链路。

#### (2) 个税专门系统、个税申报记录查询、电子文书

●个税专门系统：是根据中央部门提出的安全整改要求，为保障个税信息安全，需要加强个税相关信息的保密措施，针对涉密单位及人员、敏感单位及人员的相关信息采取用特殊的方式单独建设的一套信息系统，实现涉密单位及人员、敏感单位及人员的相关信息“不纳入个税征管、不上互联网、不用 APP”的目标。涉密和敏感单位人员的个人所得税在系统外计算，涉密和敏感单位将个人数据汇总后，可按照汇总方式或明细方式进行申报纳税。个税专门系统包括税务端和离线客户端两部分，税务端业务模式是明细或汇总申报，客户端业务模式可以明细申报并实现汇总。

●个税申报记录查询：是面向自然人收入信息查询功能，前台页面主要功能包括收入纳税明细查询、申报记录异议处理、申报记录查询等，后台应用处理包括云上/云下数据加工、本地金三数据加工、数据加工监控、系统日志留存、关键链路监控等。

#### ①数据支持服务

1) 数据分析：根据采购人工作安排，协助服务对象应用系统数据库的数据查询、数据修改和主题统计工作。

3) 数据加工：根据采购人工作安排，协助采购人将第三方数据抽取到服务对象应用系统数据库，并进行数据清洗、数据归集、数据建模、主题数据加工等操作，满足采购人在日常工作中的数据分析及展示需求。

4) 数据查询：根据采购人工作安排，协助进行相关数据的提取、整理等工作。

5) 技术支持：根据采购人工作安排，协助采购人为相关应用系统提供数据加工和数据运用接口服务

### ②高级技术支持

对于现场运维人员不能解决的疑难问题，提供解决办法；对遇到的重大事件和疑难问题，提供资深专家级技术人员进行会诊，快速确定问题原因，提出相应的解决办法，并采取相应措施以确保系统的正常运行；根据采购人工作安排，遇到现场运维及远程驻场服务人员都无法解决的疑难问题，需要到现场分析解决的，及时安排二线人员（系统研发或其他相关人员）根据应急处置相关要求到达现场。

## 3. 金税三期决策支持二包系统运维服务内容

### (1) 数据问题分析、处理与咨询

负责金税三期决策支持二包系统数据问题分析与处理、数据结构咨询等工作。

#### (1) 工作内容

1. 及时响应和解决采购人使用系统中遇到的数据问题。负责分析、定位数据问题原因，拟定处理方案，按采购人流程审批后完成数据处理和结果验证。

主要包含：

#### (1) 受理风险管理系统如下数据运维需求：

①针对需上报给总局的系统运行过程及成效数据提供查询、统计服务；

②针对系统运行过程中指标模型、风险信息、风控报告、任务信息等业务

(不完全列示，以系统实际功能模块为准)数据正确性、有效性保障；

③针对系统预置指标模型业务的数据问题处理，如分析基础数据口径问题、数据对接问题、数据抽取问题、数据验证问题和数据质量问题等提供方案设计、验证以及实施服务。

#### (2) 受理信用管理系统如下数据运维需求：

①配合采购人进行纳税信用管理评价结果发布；

②信用等级评价基础数据抽取、验证、导入、导出；

③信用等级评价数据处理；

④信用等级评价数据按采购人要求进行适当手工调整；

⑤复评、补评、动态调整三类每月常规工作所需要的数据支持工作。

(3) 受理稽查双随机系统、所得税税收政策风险提示系统和金税三期决策支持二包系统在本服务期内增加的子系统如下数据运维需求：

1. 针对上述系统运行过程中应用业务数据的正确性、有效性保障。
2. 归纳、总结、分类数据问题处理方案，建立并完善金税三期决策支持二包系统数据问题处理知识库，提高数据问题的处理效率。
3. 负责为采购人提供金税三期决策支持二包系统数据结构的技术支持，梳理提供数据结构技术文档，协助采购人开展金税三期决策支持二包系统数据查询分析工作。
4. 协助采购人开展金税三期决策支持二包系统错误数据清理，根据异常错误数据，提出错误数据清理方案，并组织实施清理。

## **(2) 数据服务**

金税三期决策支持二包系统数据分析应用基础环境管理人员承担数据抽取、数据加工和数据运算性能调优等工作。金税三期决策支持二包系统数据抽取服务指的是从系统指定的业务系统数据源将数据抽取、清洗、加载到金税三期决策支持二包系统应用数据集市的过程。

工作内容：

1. 数据运算性能调优：接收技术人员对数据脚本、语句性能问题，同时周期性对数据整体性能情况进行检查，对接收到和检查发现的数据性能问题进行分析，根据分析结果采取脚本调优、性能参数调整等方法分别实施优化。主要工作内容包括：

(1) 运行监控：周期性监控和分析数据及应用的性能状况。

(2) 接收问题：接收运维人员、系统管理员、使用用户等提出的与系统性能相关的问题。

(3) 出具解决方案：针对接收到和发现的性能问题登陆到系统进行分析定位。针对该性能问题确定对应的需要执行的操作，并制定相应解决方案。

(4) 分析处理问题：针对该性能问题执行解决方案。

(5) 记录问题：针对该性能问题产出相关文档，并反馈结果给相关负责人。

2. 数据抽取保障：数据抽取分为日常增量抽取和全量抽取，日常增量抽取由系统设定的定时任务自动执行，全量抽取由技术人员手动执行。主要是保障数据抽取的任务调度正常，抽取的执行结果正常。主要工作内容包括：

(1) 数据抽取任务调度状态维护。数据服务人员，每日检查数据抽取任务的调度配置状态，发现问题及时解决。并根据数据量及业务办理日期变化等情况，对任务调度进行必要的调整。

(2) 日常增量抽取保障。数据服务人员每日对抽取的结果进行检查，检查各抽取任务是否执行完毕、是否执行正常，发现问题及时解决。对抽取的结果日志进行分析，采用技术工具对抽取结果进行技术性校验。

(3) 全量抽取。在业务系统数据源发生较大变化时，应采用全量抽取的方式重新进行全量抽取。数据服务人员在采购人系统管理员的要求下，停止增量抽取任务，手工启动全量抽取的任务，监控全量抽取过程，检查全量抽取结果。

3. 数据加工保障：数据加工是对已经抽取到数据仓库的业务数据进行汇总、统计、分析的过程，数据加工的结果数据以数据集市的形式存储在数据库中。数据加工过程根据数据仓库的数据产生情况，采用全量加工或增量加工两种方式，主要是保障数据加工的任务调度正常，加工的执行结果正常。主要工作内容包括：

(1) 数据加工任务调度状态维护。数据服务人员，每日检查数据加工任务的调度配置状态，发现问题及时解决。并根据数据量及业务办理日期变化等情况，对任务调度进行必要的调整。

(2) 日常增量加工保障。数据服务人员每日对加工的结果进行检查，检查各加工任务是否执行完毕、是否执行正常，发现问题及时解决。对加工的结果日志进行分析，采用技术工具对加工结果进行技术性校验。

(3) 全量加工。在业务源数据全量抽取后，需采用全量加工的方式对数据进行加工。数据服务人员在采购人系统管理员的要求下，停止增量加工任务，手工启动全量加工的任务，监控加工过程，检查加工结果。

### **(3) 业务数据支撑服务**

#### 1. 运维内容：

数据运维包含业务数据错误，数据迁移脏数据，政策延迟执行导致业务数据不准确，通过业务数据运维，确保数据正确。

#### 2. 服务指标：

##### (1) 业务数据运维工作范围

业务数据迁移引起的错误数据修复、应用系统错误引起的数据修复、缺少补偿业务，无法采用应用系统处理的操作错误数据修复、系统操作引起的错误数据修改。

对误操作录入的历史业务数据通过脚本及辅助工具进行数据质量监控，从被动到主动发现数据问题，报请采购人共同分析后，按照数据运维的工作要求及时处理。

##### (2) 业务数据修改范围

对于系统已经正式投入使用的正常情况下，数据均应该通过前台系统操作写入，但是以下数据只能通过编写脚本，在后台数据库修改数据。

数据迁移的错误数据：该类数据属于数据迁移遗留问题，系统前台不支持该类数据的修改，只能通过后台修改数据。

系统 bug 产生的错误数据：该类数据是由于系统 bug 产生的，通过正常的补偿业务无法进行修正，只能通过后台修改，需开发人员分析错误产生原因，编写脚本修正数据，解决系统 bug。

异常操作或系统限制需修改的数据：由于异常操作或系统限制，无法对数据进行直接操作，需通过后台编写脚本修改数据。

(3) 提供数据维护

采购人因临时工作需要，对业务数据的数据维护工作。

(4) 业务数据运维的工作要求

运维人员对“数据维护”类问题应遵循“前台调整为主，后台调整为辅”以及“经采购人运维负责部门审核确认，驻场运维厂商人员负责实施”的基本原则。对于无法通过系统前台修改、且不修改会造成后续业务无法运行或严重影响数据质量，或者前台修改工作量大、需要后台进行批量问题统一调整的情形，需通过运维平台进行提报采购人，对执行修改代码进行审核确认后，方可实施修改，由后台统一调整数据。驻场运维人员应对后台“数据维护”内容进行全面分析，及时与运维负责部门沟通，确保调整需求理解准确后，提出可行性建议和调整方案。在系统中调整前应先做好数据备份，便于可回退、可追溯、可监控。应将数据调整结果情况及时反馈问题提报人，便于提报人做好后台数据调整之后的验证、监控和使用，确保数据调整准确，后续业务运行正常。对涉及敏感数据的数据调整，或风险较高的后台数据调整，由运维负责部门审批同意后方可实施。根据管理权限需要总局修改的，或者采购人无法自行完成修改的，按照相关规定上报总局。

**(四) 人员要求：**

本项目需要提供不少于 18 人提供相关服务，具体如下：

序号	岗位	人员数量要求
1	运维岗	13 人或以上
2	数据运维岗	2 人或以上
3	数据支持岗	2 人或以上
4	指标模型拓展岗	1 人或以上
合计		18 人或以上

1. **运维岗**需要计算机相关专业，本科或以上学历，熟练掌握 Linux 操作系统、ORACLE 数据库技术、OGG 数据同步技术、weblogic 中间件技术、webserver 技术等，相关工作经验 1 年或以上，人员数量 13 人或以上。岗位职责如下：

- (1) 负责系统业务问题受理；负责跟踪已转入开发部门程序问题的处理  
况；
- (2) 负责内数据运维脚本的编写工作；负责系统紧急问题的判定与处  
理；
- (3) 负责版本发布和进行系统测试；协助采购人进行业务培训，新功能  
解；
- (4) 负责处理采购人运维相关问题的咨询解答；整理常见问题库定期给  
采购人提供。
- (5) 负责系统应用版本发布前通知协调局里及各相关系统厂商工作；
- (6) 负责系统应用版本发布工作；
- (7) 负责系统数据库版本发布前通知协调甲方及各相关系统厂商工作；
- (8) 负责系统数据库版本发布工作；
- (9) 按照国家税务总局软件版本开发升级要求准备所涉及的所有文档资  
料如需求变更说明、操作手册、用户培训手册等；
- (10) 负责评估其它应用系统升级对系统影响，并确定升级时间；
- (11) 对软件发布进行管理，提供软件版本补丁升级发布清单，做好  
文件备份、版本管理及各相关厂商协调；
- (12) 负责版本升级后核心应用检查以及协调各厂商应用系统运行状  
态的检查工作；
- (13) 对系统涉及的小型机进行日常监控工作，系统部署；
- (14) 对系统涉及中间件（Weblogic）进行日常监控工作；
- (15) 对系统涉及数据库（oracle）进行日常监控工作；对系统涉及  
的服务器进行日常监控工作；
- (16) 对系统系统运行性能和效率进行监控，每月对监控情况进行汇  
报分析，提出优化方案；
- (17) 负责提系统和数据库设计有关资料，提供系统对外集成的接  
口以及集成其他系统的工作；
- (18) 及时处理系统应用环境所发生的故障；编制并提交每月监控报  
告；
- (19) 负责千户集团及广西列名大企业账套采集技术支持；协助采购  
对企业进行操作培训；负责广西列名大企业采集工具和加载工具的更新维护

**2. 数据运维岗**需要计算机相关专业，本科或以上学历，熟练掌握 Linux 操作系统、ORACLE 数据库、Weblogic 中间件，数据加工和处理相关工作经验 2 年或以上，人员数量 2 人以上。岗位职责如下：



- (1) 数据问题分析、处理与咨询;
- (2) 数据准备和加工;
- (3) 数据提取,对相关系统进行业务需求分析,口径编写;
- (4) 对数据进行管理,包括数据比对、数据同步、数据清洗整理等工作;
- (5) 协助客户实施数据查询以及后期数据的其他分析应用工作;
- (6) 负责审核运维脚本并进行归档;
- (7) 负责数据运维脚本的执行,以及数据备份工作;
- (8) 通过后台脚本及辅助工具进行数据质量监控,从被动到主动发现问题,并对问题数据分析及处理。

**3. 数据支持岗**需要计算机相关专业,本科或以上学历,对 ORACLE/MYSQL 数据库的架构有较深入理解,具备较强的海量数据处理和数据库调优经验;具有一定的 JAVA 开发经验,熟悉服务端的接口和模型设计能力,数据加工和处理相关工作经验 3 年或以上,人员数量 2 人或以上。岗位职责如下:

(1) 提供多表联合查询、复杂报表处理、大批量数据处理的数据查询服务。包括按照要求进行业务分析,确定统计口径,明确数据统计可行性,编写数据统计脚本,确认统计脚本的执行,分析及优化统计结果等服务;

(2) 针对个性化、大工作量的数据需求,对复杂度高的数据处理业务,提供全流程高级数据处理技术支持;

(3) 针对外部系统传递的异常数据,提供问题排查定位、问题解决方案定、维护脚本开发、数据维护执行、数据检查验证等技术支持服务;

(4) 通过撰写慢 sql、无效索引等监控脚本、定期收集 awr 报告、业务系统性能指标监控等方式,发现系统性能问题,由高级技术专家提供性能问题分、处理、调优等服务,确保系统高效稳定运行;

(5) 数据库优化,提供合理高效的数据库备份和恢复策略,进行数据库备份和数据库恢复。

**4. 指标模型拓展岗**需要计算机相关专业,本科或以上学历;熟练掌握 Linux 操作系统、ORACLE 数据库、Weblogic 中间件、NGINX 和 REDIS 等开源软件,数据加工和处理相关工作经验 3 年或以上,人员数量,1 人或以上。岗位职责如下:

(1) 负责风险模型分析,对风险模型进行系统可加载实现的分析;

(2) 负责业务标签分析,对业务标签进行系统可加载实现的分析,形成统可定义加载的业务标签信息;

(3) 风险模型及业务标签加载验证,指标模型和业务标签的加载;

(4) 风险模型研究，跟进采购人提出的风险模型业务需求，结合实际的原情况、数据情况，安排风险模型研究业务专家分析研究。

#### (五) 服务方式要求

工作日，工程师提供日常 5\*8 小时驻场技术服务；非工作日，中标人需按照采购人要求提供运维服务，可以采用远程方式提供服务，但对于远程方式不能解决处理的需按照要求及时提供现场服务；法定节假日期间需按照采购人要求提供运维服务，可以采用远程方式提供服务，但对于远程方式不能解决处理的需按照要求及时提供现场服务；中标人需在放假最后一天安排人员对本项目涉及的主机、存储、网络、应用系统等软硬件环境进行全面检查，及时解决存在的问题，确保收假后正常上班期间本项目软硬件环境的正常运行。要求服务厂商每月需按照招标采购单位的统一要求及时报送运维服务工作报告及相关资料，工作报告应包括全区运维综合情况、取得成效、存在问题和改进措施等核心主体内容、且内容需详实具体，以确保全区运维服务切实发挥积极作用并得到持续优化及提升。

#### 三、验收要求

项目验收工作由广西壮族自治区税务局按照内部验收的有关制度和流程组织开展。

中标人在合同约定的结束后的一个月内向广西壮族自治区税务局提出验收申请，广西壮族自治区税务局负责审核是否满足项目验收准入条件。满足验收准入条件后，予以启动项目验收程序。

#### (一) 项目验收准入条件

本需求书中包含的服务需求内容全部完成。

服务响应、服务流程、服务质量、服务成果以及组织管理和项目文档满足本技术需求书的规定要求。

#### (二) 项目验收标准

采购人以本技术需求书中相关内容为依据，作为项目验收标准。中标人是否按照本招标需求书中定义的各项服务内容和项目管理开展各项工作，工作流程和结果是否符合甲方质量管理要求，是否在规定时间内提交相关工作文档。

#### (三) 项目验收流程

符合项目验收准入条件后，投标人可提出项目验收申请。

投标人书面提出项目验收申请；

向采购人提交《项目验收工作总结报告》和《年度运行维护支持工作报告》；

向采购人整理提交项目相关管理、技术文档电子版文件；

采购人组织进行项目验收评审会议，对项目工作内容及文档进行验收评

审；

项目验收评审通过后，采购人出具项目验收报告。

#### （四）验收交付物

根据广西壮族自治区税务局内部验收有关制度提交验收交付物，中标人要保证文档质量。所有文档符合文档管理规范。

#### 四、其他要求

##### ★1. 信息安全保密要求

（1）中标人须严格遵守国家税务总局广西壮族自治区税务局的安全保密制度。

（2）中标人投入的项目人员须保证遵守国家有关版权和知识产权保护的政策、法律、法规和制度。

（3）中标人投入的项目人员应对本项目中接触到的国家税务总局广西壮族自治区税务局所有的知识产权、商业秘密、技术成果等信息负保密义务。未经国家税务总局广西壮族自治区税务局书面同意，不得向社会公众或第三方通过任何途径出示、泄露，不得许可使用，不得对上述信息进行复制、传播、销售；保证不向外泄漏任何相关数据，不向外泄漏任何保密的技术资料。如出现支持人员泄密事件，中标人应负有连带责任。

（4）中标人须与国家税务总局广西壮族自治区税务局签署合同项目实施期间的信息保密协议。

（5）中标人投入的项目人员须与国家税务总局广西壮族自治区税务局签署合同项目实施期间的信息保密承诺书。

##### ★2. 供应链安全管理要求

（1）中标人应要求供应链厂商严格落实供应链安全管理各项规定，包括按照国家相关法律法规开展的安全审查、安全评估、渗透测试等，并将供应链厂商落实情况作为项目验收的检查内容。

（2）中标人应要求供应链厂商严格遵守采购合同、协议、承诺书等文件中的安全相关条款，对供应链厂商履行网络安全责任不到位、造成安全事件或产生不良影响的行为，采购人将视安全事件严重程度按合同金额的 20%-30%的比例进行扣减。

##### ★3. 网络安全和数据安全管理要求

中标人投入的项目人员在合同期间应严格按采购人的网络安全和数据安全相关规定开展工作，由于中标人投入的项目人员网络安全工作落实不到位引发安全事件的，采购人将视安全事件严重程度按合同金额的 20%-30%的比例进行扣减。

	<p>安全事件具体内容主要包括(但不限于)以下内容:</p> <p>(1) 因补丁升级、漏洞修复、系统杀毒、数据备份、应用监控、网络监控等工作未落实到位, 发生服务器被控制和应用系统被攻破的安全事件, 被主管部门通报的。</p> <p>(2) 因违规进行税费数据查询、导出和拷出等操作造成敏感数据泄漏, 以及发生非法窃取数据行为。</p> <p>(3) 因运维操作处置不当导致重要应用系统发生严重卡顿、停用的重大事件。</p> <p><b>★4. 罚责条款</b></p> <p>项目建设和运维过程中, 因系统在对接、运行等服务中, 导致其他系统受到影响的, 由中标人负责组织相关服务厂商共同排查, 明确问题根源、责任并报告采购人。中标人无法判定问题根源的, 由中标人承担全部责任。采购人将视问题轻重、中标人责任大小等情况, 按不高于合同金额的 5%的比例进行扣减。</p>
<p><b>二、商务条款要求:</b></p>	
<p><b>★项目服务地点</b></p>	<p>广西壮族自治区内采购人指定地点。</p>
<p><b>★项目服务期限</b></p>	<p>1 年。</p>
<p><b>★付款方式</b></p>	<p>签订合同之日起 30 日内, 采购人支付合同总金额的 30%; 服务期满 6 个月 30 日内, 采购人支付合同总金额的 30%; 服务期满, 采购人对项目进行验收, 并根据项目验收标准及本项目合同罚则条款进行考核, 按考核结果对合同服务费进行核算后, 30 日内支付合同相应的剩余款项。</p> <p>采购人付款前, 中标人应向采购人开具等额有效的增值税发票, 采购人未收到发票的, 有权不予支付相应款项直至中标人提供合格发票, 并不承担延迟付款责任。</p>
<p><b>其他要求</b></p>	<p>投标人可以根据项目要求, 在投标文件中提供包括但不限于: 对项目需求理解、运行维护方案、培训方案等。</p>