合同编号：2025339

北京跨境电商综试区线上综合服务平台系统运行维护项目

合同书

2025 年 12 月

目录

甲方：北京市商务局

法定代表人：朴学东

地址：北京市通州区运河东大街57号院5号楼

联系人：王喜艳

联系方式：010-55579415

乙方：北京中海友成科技发展有限责任公司

法定代表人：杨全华

地址：北京市朝阳区望京利泽中园二区208号1号楼1317室

联系人：曹磊

联系方式：010-81318611

北京跨境电商综试区线上综合服务平台系统运行维护项目中所需的运维服务经中钢招标有限责任公司以 2541STC44812 号招标文件在国内公开招标。经评标委员会评定， 北京中海友成科技发展有限责任公司 为中标人。甲、乙双方同意按照下面的条款和条件，签署本合同。

下列文件构成本合同的组成部分，应该认为是一个整体，彼此相互解释，相互补充。为便于解释，组成合同的多个文件的优先支配地位的次序如下：

a. 本合同书及相关附件

b. 中标通知书

c. 投标文件(含澄清文件)

d. 招标文件(含补充通知)

一、定义

项目：指北京中海友成科技发展有限责任公司为北京市商务局建设的北京跨境电商综试区线上综合服务平台系统运行维护项目。

合同总额：指在合同项下由甲方付给乙方的履行合同的费用总额。

合同正本名称：《北京跨境电商综试区线上综合服务平台系统运行维护项目合同书》

二、合同标的

本合同的标的为**北京跨境电商综试区线上综合服务平台系统运行维护**。

服务及办公地点：北京，采购人指定地点。

本项目运维的服务期限：自合同签订之日起一年。

三、权利与义务

甲方权利与义务

(1)甲方人员应对“项目”的服务实施给乙方以协助。

(2) 甲方有权对项目实施监控，随时对乙方的服务质量提出意见和要求。

(3) 负责“项目”实施中必要的协调工作。

(4) 负责组织“项目”的验收。

(5) 按合同要求支付乙方合同款。

乙方权利与义务

(1)乙方受甲方委托，全面保障北京跨境电商综试区线上综合服务平台的正常运转，负责合同及招标文件第五章采购需求(详见附件)要求的项目维护和技术支持服务。

(2)运维队伍的人员结构配备要合理，并能始终保持驻场工作的人员投入。

(3)制定一套沟通计划，便于甲、乙双方开展工作。

(4)向甲方提供项目运维方案。

(5)按照甲方要求配备人员，按期保质保量完成“项目”的各方面需求。

(6)配合甲方进行“项目”的验收。

(7)乙方对“项目”的质量和知识产权等承担瑕疵担保责任。

(8)有关乙方的驻场人员的人身、财产安全等一切责任由乙方负责，与甲方无关。

（9）未经甲方书面同意，乙方不得私自将本合同项下全部或部分委托事务转让给任何第三方履行。

四、运维实施及验收

“项目”运维服务内容：

（1）业务目标

保障北京跨境综试区线上综合服务平台IT基础设施正常持续运

行，保障系统运行环境、中间件版本最新，安全漏洞及时修复，通过人工和系统为系统提供监控服务，对于存在的问题进行告警和提示，保证技术人员可以第一时间处理解决。

对于系统平台保证功能持续可用，对于存在的功能问题进行修复，系统性能进行优化，始终保持系统高效平稳运行。

提供基础运行环境和系统平台安全保障，对于存在的安全隐患及时进行修复。

为企业提供跨境业务数据传输通道，并保障通道联通性，解决企业申报中遇到的问题，保证企业顺利完成跨境申报业务。

（2）技术目标

安排技术人员对IT基础设施资源进行维修和维护，包括服务器资源、存储资源、防火墙、网络设备、基础软件、安全软件等，保障设备和软件的稳定运行，对出现问题的硬件设备进行及时更换，基础软件进行升级，保证平台系统正常运行。

对出现故障的服务器设备、防火墙设备、网络设备、存储设备进行维护维修，做到2小时内进行响应，对于一般故障做到12小时内恢复设备运行，特殊情况需要购买备件的情况做到3-5个工作日内完成故障零件更换，更换期间保证系统运行正常，不能出现业务中断情况，可根据实际情况提供备机。

提供5×8小时人工电话支持，网络远程支持，对一般性问题提供咨询解答；对于节假日和重大节日安排专人提供保障工作。

安排人员对机房设备进行7×24小时值守，值守期间做好巡检工

作，对于故障报警进行提示通报。

安排人员在节假日提供远程或现场的运维保障工作。

安排人员在特殊时期（国内国际重大会议期间、重保期间等）安排人员提供现场运维保障和安全支持工作。

安排人员对系统平台提供技术支持，包括功能可用性，易用性，安全性等。

安排人员对基础环境，系统运行进行定期巡检，包括操作系统日志，中间件日志，系统运行日志等。

安排人员对基础环境，应用系统，中间件，系统运行日志等进行备份。

安排人员定期对数据库、系统进行备份操作。

安排技术人员对数据库进行优化，保证运行效率。

安排技术人员对涉及电子口岸专网的服务器操作系统进行国产化替换。

安排人员对网站访问所需的SSL证书进行采购，完成续签申请、更新替换操作。

安排网络人员对域名解析进行维护，对新增二级域名进行配置。

为企业提供申报通道服务，保障企业可以正常申报跨境报文并收到对应审核回执。

对于出现的安全漏洞和隐患进行及时修复。

（3）运维服务周期

运维服务周期为一年。

（4）保障人员需求名单

职务	数量
技术经理	1名
项目经理	1名
产品经理	1名
开发人员	2名
测试经理	1名
运维经理	1名
运行负责人	1名
安全负责人	1名
现场值守人员	若干

“项目”的运维服务须覆盖整个合同期限。

运维服务期满，由乙方提交验收相关技术文档，并对运维情况向甲方进行汇报，甲方组织开展验收工作。

五、技术文档

运维服务期满，乙方需向甲方提交运维技术文档。文档应包括：

- 巡检报告；
- 维护记录；
- 维修记录；
- 工作总结。

涉及系统更新的，还应包括：

- 技术方案；
- 需求规格书明书；

- 详细设计说明书；
- 测试报告。

技术文档、本合同及附件一起作为项目验收的依据。

六、合同金额与付款方式

合同总额：

本合同总额为人民币壹佰壹拾万陆仟元整，小写：¥1,106,000.00元。此费用为本协议项下乙方完成全部承办委托事项甲方应支付乙方的全部费用，除此费用以外，甲方无需另行支付其他费用。

支付方式：

(1) 合同生效后15个工作日内，甲方向乙方支付首款，即合同总额的60%（663,600元，即人民币陆拾陆万叁仟陆佰元整）。

(2) 服务满半年，甲方向乙方支付合同总额的30%（331,800元，即人民币叁拾叁万壹仟捌佰元整）。

(3) 验收通过后15个工作日内，甲方向乙方支付剩余合同金额¥110,600元，即人民币壹拾壹万零陆佰元整。

(4) 上述款项由甲方按时支付，以支票或汇入乙方制定账户。乙方在收到每笔款项前5个工作日内向甲方出具等额发票。

(5) 费用的支付需以相应财政资金实际拨付至甲方账户为前提，若因相应财政资金未能及时到账或财政国库结算而导致的延期支付，不属于违约行为，甲方不承担违约责任。

七、履约保障的内容与责任

1.任何一方违反本合同项下的任何约定，均构成违约。除本合同另有约定或法律另有规定外，违约方应承担继续履行、采取补救措施、赔偿损失等违约责任。

2.若乙方未能按合同约定的时间、标准或要求履行技术服务义务，甲方有权采取以下措施：

（1）限期整改：甲方可向乙方发出书面通知，要求其在指定期限内（例如：5个工作日）完成整改。

（2）扣减服务费用：若乙方未在指定期限内完成整改，每发生一次，甲方有权合同总金额【5%】的违约金。

（3）解除合同：若乙方累计【3次】未能按时完成整改，或单次违约情节严重给甲方造成重大损失的，甲方有权单方解除本合同。

3.乙方或其工作人员，存在未经甲方授权，擅自篡改甲方业务数据，利用甲方现有业务应用系统、网络平台或者冒用甲方身份获取非法利益以及其他损害甲方或任何第三方合法权益的行为的视为重大违约，对此甲方有权要求解除本合同，要求乙方退回已支付的款项，并且赔偿甲方及第三方因此遭受的全部损失。

4.乙方或其工作人员违反本合同约定保密义务的，甲方扣减本合同金额10%款项，扣减金额不足以弥补甲方损失的，乙方还应继续赔偿。

5.本合同中的“损失” 是指甲方因乙方违约而遭受的全部损失，包括甲方的直接财产减损、为修复问题而额外支出的费用、对第三方

承担的赔偿或罚款、以及为处理违约事件而支出的合理费用以及因乙方违约导致甲方需要向第三方支付的赔偿、和解金、罚款及其他费用等。

八、合同变更和终止

任何一方均可以对合同内容以书面形式提出变更、修改、取消或补充的建议，经双方协商签定补充条款后发生法律效力。

九、不可抗力

如任何一方因不可抗力，如战争、火灾、台风、洪水、地震或其它双方共同认为属于不可抗力的事件而被迫停止或推迟合同的执行，则合同执行顺延。但不能因为不可抗力的延迟而调整价格。

受到不可抗力影响的一方应在不可抗力事件发生后三日内将所发生的不可抗力事件的情况书面通知另一方确认，受影响的一方同时应尽量设法缩小这种影响和由此而引起的延误，一旦不可抗力的影响消除后，应将此情况立即书面通知对方，并恢复合同的执行。

如不可抗力事件的影响持续到六十天以上时，双方应通过友好协商解决本合同执行问题。如不可抗力因素致合同已无法履行，双方应终止本合同。如甲方已经付款，乙方应在扣除实际发生的有确切合法有效单据证明的费用后在3 日内向甲方返还余款。如甲方未付款，甲方应在乙方开具正规发票后60 日内向乙方支付不可抗力发生前产生的实际费用。

十、保密

双方一致同意在任何时候对其所持有的有关另一方的工程事务、事务操作方法、技术资料、商业材料及其他机密信息实行严格保密。除非确有必要并得到另一方书面授权，任何一方不得在任何时间向任何人透露另一方的任何保密信息。双方同意不对保密信息进行拷贝或抄写。

未经对方书面同意任何一方不得向与本合同项目无关的第三方透露有关合同内容。

甲、乙双方对在合作过程中所获知的对方的企业、技术情报和资料均负有保密义务，任何一方不得将获知的对方技术、商业秘密泄漏给第三方。

本章所述的保密条款对以下内容不适用：

（1）已属于常识且不受版权保护的内容；

（2）已通过出版物或其他原因（未经授权行为或疏忽除外）而成为不受版权保护的内容；

（3）由第三方未加限制提供的内容，且该第三方对这些内容无任何明确、暗含或暗示的保密义务；

（4）按法律、行政法规规定需要向有关机关、机构或媒介公开的内容。

任何一方对违反本章规定所造成对方的损失承担赔偿责任。

十一、合同争议的解决

本合同适用法律为中华人民共和国法律。

凡与本合同有关而引起的一切争议，双方应通过友好协商解决，如果协商不能解决，可向甲方所在地人民法院提起诉讼。

十二、其它

本合同有效期从服务期始起到服务期结束为止。（即自合同签订之日起一年），如有索赔则完成理赔后止。

本合同下所有附件是本合同不可分割的组成部分，具有同等法律效力。

本合同未尽事宜，由甲、乙双方协商签订补充条款，补充条款与本合同具有同等法律效力。

本合同一式五份，甲方、乙方各执两份，采购代理机构一份。

本合同经双方法定代表人或授权代表签字并加盖公章后生效。

十三、合同附件：

附件：采购需求

（以下无正文）

（本页无正文，为签署页）

甲方

北京市商务局

（盖章）

地址：北京市通州区运河东大街57号院5号楼

法定代表人/授权代表：

（签字/签章）

签字日期：2015 年 12 月 16 日

乙方

北京中海友成科技发展有限责任公司

（盖章）

地址：北京市朝阳区望京利泽中园二区208号1号楼1317室

法定代表人/授权代表：

（签字/签章）

开户银行：中国工商银行金台路支行

帐号：0200020219200143163

税号：911101057693606624

电话：81318635

签字日期：2015年12月16日

附件：采购需求

1.建设目标

1.1 业务目标

保障北京跨境综试区线上综合服务平台 IT 基础设施正常持续运行，保障系统运行环境、中间件版本最新，安全漏洞及时修复，通过人工和系统为系统提供监控服务，对于存在的问题进行告警和提示，保证技术人员可以第一时间处理解决。

对于系统平台保证功能持续可用，对于存在的功能问题进行修复，系统性能进行优化，始终保持系统高效平稳运行。

提供基础运行环境和系统平台安全保障，对于存在的安全隐患及时进行修复。

为企业提供跨境业务数据传输通道，并保障通道联通性，解决企业申报中遇到的问题，保证企业顺利完成跨境申报业务。

1.2 技术目标

安排技术人员对 IT 基础设施资源进行维修和维护，包括服务器资源、存储资源、防火墙、网络设备、基础软件、安全软件等，保障设备和软件的稳定运行，对出现问题的硬件设备进行及时更换，基础软件进行升级，保证平台系统正常运行。

对出现故障的服务器设备、防火墙设备、网络设备、存储设备进行维护维修，做到 2 小时内进行响应，对于一般故障做到 12 小时内恢复设备运行，特殊情况需要购买备件的情况做到 3-5 个工作日内完成故障零件更换，更换期间保证系统运行正常，不能出现业务中断情况，可根据实际情况提供备机。

提供 5×8 小时人工电话支持，网络远程支持，对一般性问题提供咨询解答；对于节假日和重大节日安排专人提供保障工作。

安排人员对机房设备进行 7×24 小时值守，值守期间做好巡检工作，对于故

障报警进行提示通报。

安排人员在节假日提供远程或现场的运维保障工作。

安排人员在特殊时期（国内国际重大会议期间、重保期间等）安排人员提供现场运维保障和安全支持工作。

安排人员对系统平台提供技术支持，包括功能可用性，易用性，安全性等。

安排人员对基础环境，系统运行进行定期巡检，包括操作系统日志，中间件日志，系统运行日志等。

安排人员对基础环境，应用系统，中间件，系统运行日志等进行备份。

安排人员定期对数据库、系统进行备份操作。

安排技术人员对数据库进行优化，保证运行效率。

安排技术人员对涉及电子口岸专网的服务器操作系统进行国产化替换。

安排人员对网站访问所需的 SSL 证书进行采购，完成续签申请、更新替换操作。

安排网络人员对域名解析进行维护，对新增二级域名进行配置。

为企业提供申报通道服务，保障企业可以正常申报跨境报文并收到对应审核回执。

对于出现的安全漏洞和隐患进行及时修复。

1.3 运维服务周期

运维服务周期为一年。

1.4 保障人员需求名单

职务	数量
技术经理	1 名
项目经理	1 名
产品经理	1 名
开发人员	2 名

测试经理	1 名
运维经理	1 名
运行负责人	1 名
安全负责人	1 名
现场值守人员	若干

2.运行环境介绍

2.1 应用服务器部署

2.1.1 交换平台服务器部署

序号	逻辑域	名称	部署应用	部署路径	内网 IP	外网 IP	备注	配置
1	对外接入	对外接入服务器	1、MQ 申报服务 2、接口申报服务 3、进口业务报文处理服务 4、出口业务报文处理服务 5、向总署发送报文服务 6、接收总署回执服务 7、IBM MQ 8、ROCKET MQ 9、报文处理结果查询服务 10、IBM MQ 队列管理平台	\root\owinfo\docker-owinfo	172.22.16.48	211.147.144.115		32GB 内存|16vCPU|500GB 磁盘
2	对外接入	对外接入服务器	1、进口业务报文处理服务 2、出口业务报文处理服务 3、向海关总署发送	\root\owinfo\docker-owinfo	172.22.16.64			32GB 内存|16vCPU|

			报文服务 4、IBM MQ 5、ROCKET MQ 6、IBM MQ 队列管理平台					500GB 磁盘
3	政务云		1、企业申报查询系统前端	nginx:/usr/local/nginx 2、前端应用:/home/page	192.159.73.7			32GB 内存、16vCPU、500G 磁盘

2.1.2 电子口岸专网服务器部署

序号	逻辑域	名称	部署应用	部署路径	内网 IP	备注
1	对外接入区	数据对接服务器	RABBITMQ 队列商品溯源海关端；现场机检线验放接口	D:\bjcebcptsserver_tomcat	172.22.16.103	
2	对外接入区	数据对接服务器	企业税务联网核查服务接口	1、前端页面 D:\mz_zongshiqu\web 后台服务 D:\mz_zongshiqu\	172.22.16.105	
3	对外接入区	数据对外查询服务	数据服务	C:\intpub\wwwroot\	172.22.16.27	
4	核心数据区	专网审批服务器	bjcebcpmdcusserver	/home/cebcuser/apache-tomcat-8.5.54	172.22.26.50	
5	数据区	数据采集服务器	商品溯源采集 B2B 数据采集	C:\bjcebcptsserver_tomcat C:\bjcebcpdcserver	172.22.18.112	

2.1.3 政务云服务器部署

序号	逻辑域	名称	部署应用	部署路径	内网 IP	外网 IP	备注	配置
1	对外接入	对外接入服务	1、统计分析系统后端服务 2、线下门店审批	\root\owinfo\docker-owinfo	172.22.16.48	211.147.144.115（edi.bj		16GB 内存 |

		器	后端服务 3、大屏幕后端服务 4、金融服务系统后端服务			kjb2c.com）		8vCPU | 100GB 磁盘
2	服务层		统计分析系统前端 统计分析大屏幕前端 金融服务系统前端	nginx:/usr/local/nginx /usr/local/sams/bjkj-sams， /usr/local/monitor/bjkj-monitor	192.159.73.7			32GB内存、16vCPU、500G磁盘
4	服务层	应用服务器	企业台账管理系统 商品溯源查询系统 跨境医药企业备案系统 金关二期系统	/home/bjcebc/nginx/html/bjcebcpdafront /home/bjcebc/nginx/html/bjcebcptsentfront /home/bjcebc/nginx/html/bjcebcpmdentfront /home/bjcebc/cross_border_bonded/custom_addons	192.159.73.7			
5	数据传输层	队列服务器	1、rabbitmq	/usr/local/rabbitmq_server-3.8.0	192.159.73.10			
6	数据存储层	数据库服务器	PostgreSQL、MySQL	/home/postgres/pgsql10.132/usr/local/mysql	192.159.73.19			
7	数据存储层	数据库服务器	Mysql	/usr/local/mysql	192.159.73.19			
8	数据存	数据库服务器	Mysql	/usr/local/mysql	192.159.73.11			

	储层							
9	数据代理	代理服务器	nginx	/usr/local/nginx	192.159.73.27			
10	数据代理	代理服务器	nginx	/usr/local/nginx	192.159.73.15			
11	服务层	应用服务器	1、综试区门户网站前端页面 2、cas 单点登录系统 3、cms 后台管理系统前端页面 4、统一身份认证管理前端页面 5、统一身份认证管理后台 6、门户、cms 服务后台 7、门户、cms 服务后台配置项	1、/opt/bjzsq/bjzsq-tomcat/webapps/ROOT 2、/opt/bjzsq/bjzsq-tomcat/webapps/cas 3、/opt/bjzsq/bjzsq-tomcat/webapps/cms 4、/opt/bjzsq/bjzsq-tomcat/webapps/bjzsq 5、/opt/bjzsq/server/auth 6、/opt/bjzsq/server/gateway 7、/nfs/bjzsq	192.159.73.6			
12	服务层	应用服务器	1、综试区门户网站前端页面 2、cas 单点登录系统 3、cms 后台管理系统前端页面 4、统一身份认证管理前端页	1、/opt/bjzsq/bjzsq-tomcat/webapps/ROOT 2、/opt/bjzsq/bjzsq-tomcat/webapps/cas 3、	192.159.73.5			

			面 5、统一身份认证管理后台 6、门户、cms服务后台 7、门户、cms服务后台配置项	/opt/bjzsq/bjzsq-tomcat/webapps/cms 4、/opt/bjzsq/bjzsq-tomcat/webapps/bjzsq 5、/opt/bjzsq/server/auth 6、/opt/bjzsq/server/gateway 7、/nfs/bjzsq				

2.2 数据库服务器

序号	逻辑域	名称	部署应用	部署路径	内网 IP	外网 IP	备注	配置
1	政务云	数据库服务器	1、PostgreSQL 2、MySQL	1、/home/postgres/pgsql10.13 2/usr/local/mysql	192.159.73.19			
2	政务云	数据库服务器	Mysql	/usr/local/mysql	192.159.73.19			
3	政务云	数据库服务器	Mysql	/usr/local/mysql	192.159.73.11			
4	口岸专网数据区	数据库服务器	SQL Server2012	C:\Program Files\	172.22.18.101			
5	口岸专网数据区	数据库服务器	SQL Server2012	C:\Program Files\	172.22.18.102			

2.3 服务器、网络设备和安全设备

产品类型	产品名称	品牌	供货型号	详细配置	数量

服务器	pc服务器	联想	ThinkServer RQ940	联想 ThinkServer RQ940 四路服务器 Intel Xeon E7-4800V2 系列 CPU*4（8 核，2.0GHz），256GB 内存，512MB 硬件 RAID 卡（含电池，RAID0/1/10/5），300GB 15K SAS 硬盘*4，千兆网口*8，8Gb/s FC HBA 卡*2，2+2 冗余电源，冗余风扇，IKVM 模块，PDU 电源；	5
	pc服务器	联想	联想 ThinkServer RD640	联想 ThinkServer RD640 两路服务器 Intel Xeon E5-2600V2 系列 CPU*2（6 核，2.1GHz），32GB 内存，512MB 硬件 RAID 卡（含电池，RAID0/1/10/5），300GB 15K SAS 硬盘*4，千兆网口*3，1+1 冗余电源，冗余风扇，IKVM 模块，PDU 电源；	4
存储设备	SAN 存储	EMC	EMC VNX5300	EMC VNX5300 双控制器，16GB 高速缓存， 8 个 8Gbps 连接主机端口， 4 个 6Gbps 磁盘端口， 25 块 600GB 10K 硬盘， 单机柜部署	2
	SAN 光纤交换机	EMC	EMC DS6510	24 个 16 Gbps 光纤端口，全激活	2
	存储整合设备	EMC	EMC VPLEX	EMC VPLEX 双控制器， 72GB 高速缓存， 8 个 8Gbps 连接主机端口， 8 个 8Gbps 连接存储端口 单机柜部署	2
网络与安全设备	防火墙	天融信	天融信 TG-61040 防火墙	2U 机箱 最大配置为 34 个接口，默认包括 4 个可插拔的扩展槽和 2 个 10/100/1000BASE-T 接口，标配双冗余电源。 加配：	2

				1 个 2 个 SFP+插槽的万兆接口扩展卡； 2 个万兆 SFP 多模模块； 1 个 4 光 4 电千兆接口扩展卡； 4 个千兆 SFP 多模模块 整机吞吐率：>40Gbps 最大并发连接数：>450W	
	接入交换机	H3C	H3C 5820V2-52Q	H3C S5820V2-52Q L3 以太网交换机主机,支持 48 个 XGT 端口,4 个 QSFP+端口 650W 交流电源模块 端口侧进风,电源侧出风风扇 40G QSFP+ 3m 电缆 SFP+ 万兆模块(850nm,300m,LC)	2
	核心路由器	H3C	H3C SR6608-X	H3C SR6608-X-RTWZ16608X-路由器机框-国内版 功能模块-H3C SR6600-X-RTWM1MPUD-路由交换引擎 X2-国内海外合一版 功能模块-H3C SR6600-RTWM1AC1200-交流电源模块-1200W-国内版 H3C SR6600 主机软件费用(标准版) 48 端口千兆电口以太网接口模块	3

3.运维服务内容

3.1 基础环境运维

基础性的保障和维护工作，从网络安全、主机及存储、数据库、中间件等维度展开，以确保应用系统安全稳定运行。

1） 系统网络、安全系统运维服务，从网络的连通性、网络的性能、网

络的监控管理三个方面实现对网络系统的运维管理。其基本服务包括现场备件安装、现场软件升级，电话远程技术支持，并根据实际情况参照服务级别提供现场故障诊断。

序号	服务模块	内容描述
1	现场备件安装	配合用户进行，将设备备件进行安装更换，调试备件运行效果
2	现场软件升级	配合用户进行软件升级
3	现场故障诊断	按服务级别提供：7×24 小时 5×8 小时
4	电话远程技术支持	7×24 小时
5	问题管理系统	对遇到的问题进行记录

用户现场技术人员值守

可根据用户的需求提供长期的用户现场技术人员值守服务，保证网络的实时连通和可用，保障接入交换机、汇聚交换机和核心交换机的正常运转。现场值守的技术人员每天检查网络交换机的端口是否可以正常使用，网络的转发和路由是否正常进行，交换机的性能检测，进行整体网络性能评估，针对网络的利用率进行优化并提出网络扩容和优化的建议。

现场值守人员还进行安全设备的日常运行状态的监控，对各种安全设备的日志检查，对重点事件进行记录，对安全事件的产生原因进行判断和解决，及时发现问题，防患于未然。

此外还需要对服务器进行巡检，检查运行状态，检测硬件故障报警。

现场巡检服务

现场巡检服务是对客户的设备及网络进行全面检查的服务项目，通过该服务可使客户获得设备运行的第一手资料，最大可能地发现存在的隐患，保障设备稳定运行。同时将有针对性地提出预警及解决建议，使客户能够提早预防，最大限度降低运营风险。

2） 主机、存储系统的运维服务

主机、存储系统的运维服务，主要包括主机、存储设备的日常监控，设备的运行状态监控，故障处理，设备零件更换，操作系统维护，补丁升级等内容。

序号	服务模块	内容描述

1	补丁服务	消除软件漏洞给系统带来的安全隐患，并对安装补丁所引起的系统连锁反应进行排查处理。
2	升级服务	对系统进行软件升级，检查系统补丁情况，对系统补丁安装测试和应用程序兼容性测试。保证在补丁实施后，对系统和应用程序无影响。
3	安全服务	定期对安全软件的病毒库进行升级，提升系统抵抗病毒感染的能力和防范黑客攻击。
4	设备零件更换	对出现故障的零件，如电源、风扇、硬盘、内存等。更换设备为原型号或兼容的型号
5	现场故障诊断	按故障类型分为： 7×24 小时 5×8 小时
6	电话远程技术支持	7×24 小时
7	问题管理系统	对遇到的问题进行汇总，记录
8	系统优化	对系统的主机、存储设备、操作系统、提供优化服务。

现场值守人员可进行监控管理的内容包括：

- CPU 性能管理；
- 内存使用情况管理；
- 硬盘利用情况管理；
- 系统进程管理；
- 主机性能管理；
- 实时监控主机电源、风扇的使用情况及主机机箱内部温度，对于损坏的电源、风扇进行更换；
- 监控主机硬盘运行状态，对于损坏的硬盘进行更换；
- 监控主机网卡、阵列卡等硬件状态；
- 监控主机HA运行状况；
- 主机系统文件系统管理；

- 监控存储交换机设备状态、端口状态、传输速度；
- 监控备份服务进程、备份情况（起止时间、是否成功、出错告警）；
- 监控记录磁盘阵列、磁带库等存储硬件故障提示和告警，并通过更换损坏设备解决故障问题；
- 对存储的性能（如高速缓存、光纤通道等）进行监控；
- 对其它设备进行监控管理，对于损坏的设备部件进行更换。

3） 数据库运维服务

提供的数据库运行维护服务包括主动数据库性能管理。通过主动式性能管理可了解数据库的日常运行状态，识别数据库的性能问题发生在什么地方，有针对性地进行性能优化。同时，密切注意数据库系统的变化，主动地预防可能发生的问题。

提供的数据库运行维护服务还包括快速发现、诊断和解决性能问题，在出现问题时，及时找出性能瓶颈，解决数据库性能问题，维护高效的应用系统。

日常的数据库运行维护服务，主要工作是使用技术手段来达到管理的目标，以系统最终的运行维护为目标，提高用户的工作效率。

具体数据库运行维护监控的基本服务内容包括：

序号	服务模块	内容描述
1	数据库现场服务响应	数据库宕机； 数据存储坏块； 影响业务运行的数据库问题； 软件产品更新维护
2	数据库产品健康检查	对系统的配置及运作框架提出建议，以帮助用户得到一个更坚强可靠的运作环境； 降低系统潜在的风险，包括数据丢失、安全漏洞、系统崩溃、性能降低及资源紧张； 检查并分析系统日志及跟踪文件，发现并排除数据库系统错误隐患； 检查数据库系统是否需要应用最新的补丁集； 检查数据库空间的使用情况； 协助进行数据库空间的规划管理； 检查数据库备份的完整性； 监控数据库性能； 确认系统的资源需求； 明确系统的能力及不足。
3	数据库产品性能调优	优化数据库参数设置； 评估硬件和资源的使用情况，提出合理升级建

		议。

4） 中间件运维及巡检服务

对中间件进行的运维服务，主要包括对中间件的日常维护管理和监控工作，包括 IBMMQ、Rabbit MQ、RocketMQ、IIS 等中间件的日常维护管理和监控工作，提高对中间件平台事件的分析解决能力，确保中间件平台持续稳定运行。中间件监控指标包括配置信息管理、故障监控、性能监控。

系统巡检人员要定期规范检查各硬件设备的运转情况和应用软件运行情况，同时做好日常的数据增量备份和定期全备份。每周到现场对系统进行健康检查，及时诊断并避免系统发生问题。

（1）对部署在电子口岸专网的数据库至少每 3 个月进行备份归档，重要数据库至少每月进行备份归档。

（2）对于系统运行过程中发现的一些错误日志信息要进行监控，做到及时的分析处理，消除系统隐患。

5） 应用系统日常运维

系统日常运维服务主要包括对应用系统进行日常巡检、监控及维护操作，同时针对企业提供对接上线及日常问题咨询服务，提供系统需求反馈及统计服务。

定期对应用系统定期进行备份，备份后由专人进行验证，保证备份可用。

运维人员任务主要包括：

每周会安排驻场技术人员到现场机房对应用服务器进行巡检、监控及维护操作；

对于部署在政务云上的服务器，会安排技术人员通过远程方式进行服务器进行巡检、监控及维护操作：

（1）对涉及到系统安全、稳定运行的日志数据进行定期的备份、清理，同时避免因日志数据文件过大导致系统无法高效运行。

（2）对于系统运行过程中发现的一些错误日志信息要进行监控，做到及时的分析处理，消除系统隐患。

序号	服务模块	服务描述
1	现场日常巡检	配合用户定期进行现场或远程巡检
2	现场软件升级	分析软件升级的必要性和风险，配合用户

		进行软件升级
3	现场故障诊断	根据服务级别：5×8 小时 7×24 小时
4	电话技术支持	7×24 小时支持
5	问题管理系统	对遇到的问题进行汇总、记录归档

对系统运行中出现的各类故障进行应急处理，包括系统报错、系统崩溃等。

为将系统遇到意外的事件及可能造成的损失降到最低，配合北京市商务局和北京海关制定系统备份和恢复策略，做好数据的存储、备份、恢复以及容灾等数据保护工作。

运维人员积极配合地方工作，出现问题，积极解决问题，远程协助地方实施修复，保证企业的正常运作。对企业日常使用过程中的问题提供咨询并及解决防范，及时修改系统中存在的缺陷，确保系统全天候 24 小时不间断正常运行，平均无故障运行时间达到 96%以上。

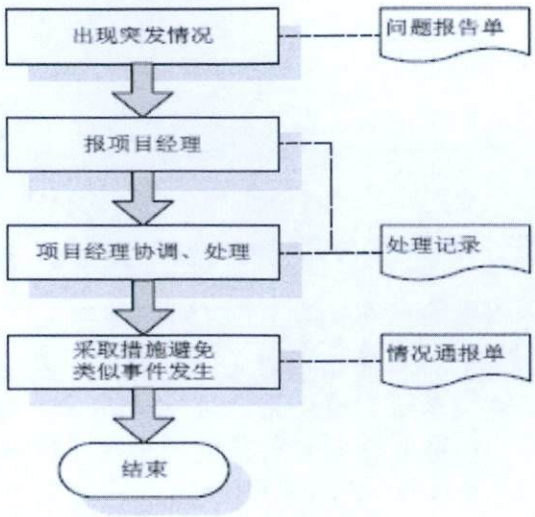
安排专人为企业和业务现场提供支持服务，帮助企业解决传输和申报问题，帮助业务现场解决通关问题。

针对系统使用人员对系统提出的需求与问题，将内容分类归纳，反馈并提供解决方案。收集常见问题，分析发生的原因和解决方案。遇到疑难问题，与多方积极沟通，共同解决棘手问题。及时上报可能的问题状况，开发人员与维护人员形成良好的交流体系，不断升级系统，提高使用率，提升稳定性。

随着业务的开展，越来越多的企业会进驻到系统中，运维工作人员需对每个对接的企业进行记录，并实时跟进其对接进度，为企业提供接入联调及测试工作，及时为企业用户解答对接中的疑问，并为企业安装部署对接跨境系统。

6） 系统应急处理服务

针对本项目制定详尽应急处理预案，整个流程需严谨而有序。在服务维护过



维护服务应急处理流程

程中，意外情况将难以完全避免。对项目实施的突发风险进行详细分析，并且针对各类突发事件，设计相应的预防与解决措施，同时提供了完整的应急处理流程。

针对跨境项目运维服务过程中可能遇到的各种各样的风险，总结多年维护服务经验，针对一些可能出现的情况，制定了一系列预防处理措施，举例如下：

类型	时间	预防措施	处理
应用软件	无法启动软件可执行文件	上门人员提前准备好软件安装程序	将应用软件数据配置文件备份后，进行重新安装
	软件打开过程中或运行中异常错误关闭	上门人员准备好安装程序，操作系统优化和修补软件，查杀病毒软件	判断出错原因，备份数据,采取相关修复措施
操作系统	用户本机操作系统异常或系统资源占用严重	准备好系统检查程序及修补程序，以及查杀病毒软件	告知使用者错误原因可能类型，提出解决方案，经使用者认可后采取相应措施
	B/S 结构系统,IE 浏览器异常或无法下载控件	准备修复浏览器软件、查杀病毒软件	检查 IE 浏览器选项设置，分析原因进行修复
网络或服务器	系统网络流量异常或服务器登录异常	判断服务器是否异常，否则准备杀毒软件	检查网络流量,流量异常则报修网络服务商或进行

			网络安全时间排查

7） 突发事件响应时间

提供 7×24 小时的响应服务。当发生系统故障时，将查找故障原因，并给出处理建议，在不影响通关情况下，尽快实施处理操作。在故障处理完成后提供故障分析和处理情况报告，帮助预防同类的问题再次发生。对于由其他公司负责实施的内容的质量原因出现的意外故障，予以协助解决。

序号	系统故障级别	系统故障定义	系统故障响应时间
1	一级故障	指系统崩溃，无法提供任何服务，对业务的正常运行造成重大影响。	运维人员发现或接到通报后，第一时间做出响应，安排高级工程师在 1 个小时内找到故障并排除。
2	二级故障	系统主要功能不能正常工作或系统不稳定，并有周期性的中断，对业务的正常运转造成较大影响	运维人员在 3 小时内找到问题并提出修改方案。安排高级工程师排除故障。
3	三级故障	系统有故障，但能够提供主要功能服务，对业务的正常运转有一定的或轻微影响。	我司会安排技术人员在 6 小时内给出问题原因并排除故障

8） 突发事件应急策略

系统运维应急方案是对中断或严重影响业务的故障，如宕机、数据丢失、业务中断等，进行快速响应和处理，在最短时间内恢复业务系统，将损失降到最低。在系统维护过程中，突发事件的出现将是很难完全避免的，针对这种情况，设计完善的突发事件应急策略。

系统巡检人员要定期规范检查各硬件设备的运转情况和应用软件运行情况，同时做好日常的数据增量备份和定期全备份。对发现的问题在报各级负责人的同时，要协调相关资源分析问题根源，确定解决方案和临时解决措施，避免造成更大的影响。问题得到稳定或彻底解决后，要形成问题汇报，避免以后类似重大紧急情况的发生。

通过现场运维总结的问题记录，并根据长期以来的客户服务工作经验，建立

常用知识库，其中包括多种常见技术故障和突发事件的应急策略。当获悉出现突发事件时，运维和技术支持人员可以立即从知识库中获取相应的应急策略，并综合用户方的具体情况，给出相关解决方案，然后在第一时间以电话、邮件支持或现场服务的方式帮助用户解决问题，尽最大努力减小突发事件对用户日常应用的影响。

紧急情况	预防措施	应急策略
硬件损坏	项目单位操作用电脑硬件损坏	在磁盘数据未丢失情况下，保证数据安全性，建议项目单位替换相关硬件。
操作失误	加强培训力度，掌握培训效果，检验操作人员操作水准，提示注意事项。	操作失误未造成即成结果或数据未丢失情况下，保障数据安全，反之，协调相关部门，进行补救。对操作人员强调注意事项。
配置丢失	培训时强调使用前配置方法和步骤，并特别提示需在使用前按要求操作。	派员上面进行维护、培训人员重新配置。
数据丢失	培训时强调使用过程中注意定期备份重要数据,日常维护过程中,上门服务人员实时备份数据并告知用户	协调有关部门，进行补救，无法补救，提交报告说明原因。

9）　其他服务

除了提供以上服务外，针对采购方特殊需求，还应提供以下服务，并制定相应的服务管理规范，保障系统运行质量。

保障用户在服务期内享受产品补丁程序升级，小版本升级，调整现有功能模块。

安排熟悉跨境业务的客服团队为企业提供 5×8 小时服务，帮助企业了解跨境进出口相关业务。

安排专业技术人员指导企业进行传输对接。

安排熟悉业务系统的技术人员解答用户在使用本系统时遇到的问题。

配合完成与其他应用系统的集成或接口的调试工作，并及时解决与其他应用系统之间存在的问题。

3.2 数据对接通道运维

在保障企业数据通道畅通的同时，针对新加入的企业进行数据交换通道的开通工作。

- 为企业提供交换报文标准；
- 建立企业专有上下行数据通道队列；
- 针对需要的企业进行交换客户端的部署；
- 与企业进行通道对接测试，报文测试；
- 解决企业数据交换中遇到的问题。

3.3 平台系统运维

运维人员定期对跨境综试区各子系统进行备份，对运行的中间件、Web 容器、队列等进行备份；

运维人员利用工具对跨境综试区各子系统运行情况进行监控，对异常进行告警，利用工具自动处理异常；

运维人员实时监控系统运行情况，确保所有门户网站及各子系统实际可用。

运维管理人员负责应用系统的数据备份；

定期检查并确认数据备份存放路径，检查备份文件是否可用；

定期检查培训视频内容可用，保证播放效果；

运维人员定期检查企业存证数据，确保数据真实、完整、有效；

运维人员定期检查数据大屏可用，确保数据展示准确。

3.3.1 备份范围

根据系统可将信息分为以下几类：应用程序、数据、日志文件这 3 类。详细说明如下：

大类别	小类别	说明	备份等级
应用软件	部署软件包	发布可运行的程序包（jar 包、docker 镜像）	阶段备份
数据	数据库文件	数据库脚本：表、视图、索引等	定期备份

	应用数据	数据库中的应用数据信息	定期备份
日志	系统日志	软件系统的运行日志、与业务无关	阶段备份
	应用日志	与业务相关的应用系统日志	定期备份
运行环境	中间件	提供给应用软件运行环境的容器	阶段备份
	操作系统配置	操作系统的相关运行环境配置	阶段备份

3.3.2 应用系统备份

应用系统只需要进行阶段备份即可，要求在生产环境的应用软件进行更新后，必须进行手动的备份，政务云系统应用备份放在不同服务器中，口岸专网应用备份放置在专用备份空间。备份后由专人进行测试验证。

3.3.3 数据备份

对部署在电子口岸专网的应用系统数据库进行备份操作。涉及的数据库种类有 MS SQL Server。

电子口岸专网数据库为 MS SQL Server，主要存储海关管理端数据、报文交换数据、查询统计相关数据。至少每周进行增量备份，每月进行全量备份。报文交换数据由于量较大，存储空间有限，且统计数据另行存储，所以只需保留 3 个月数据即可，定期进行数据清理，以保证磁盘空间可用。

3.4 平台系统功能性问题修复

针对各子系统使用中、运行中出现的错误进行修复。

3.5 平台系统优化更新

系统运维人员需按规定要求，定期对系统维护升级。系统维护升级内容包括，北京跨境电子商务公共信息平台的维护升级、系统新需求、新系统的部署安装和维护升级。

配合北京市商务局调整和优化系统运行环境的部署，根据北京海关要求进行

安全策略调整。

对系统功能及接口进行版本化、规范化管理，加强接口安全访问机制。

提供与系统相关的内容变更和升级的详细资料；提供开发和运行环境安装调试及变更的详细资料。

优化跨境数据交换服务，提高数据处理能力。

3.6 平台系统功能完善

加强交换数据安全性，防止企业交换数据泄露。

增加数据交换方式，除现有队列方式外，应提供接口方式，允许企业自行选择交换方式。

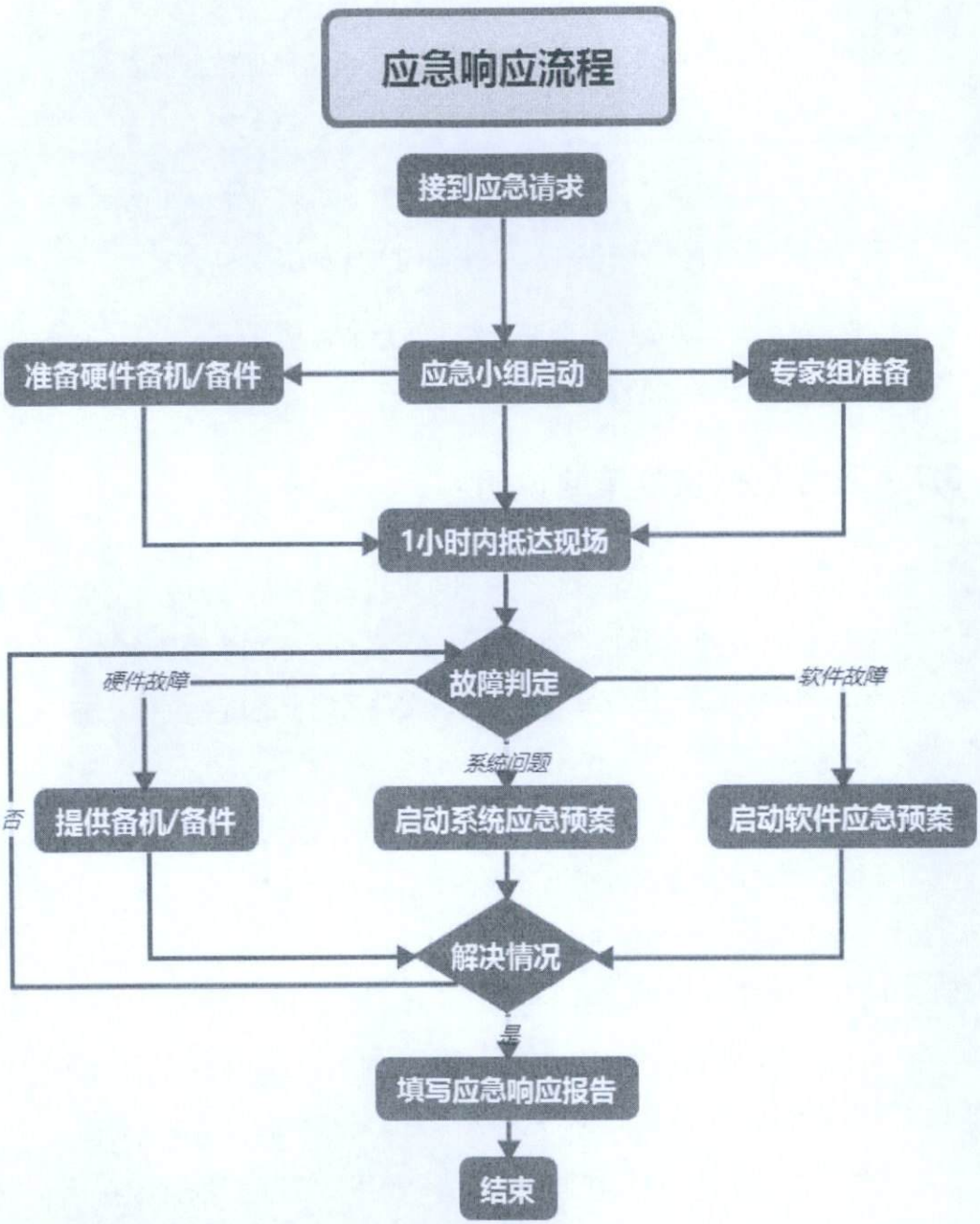
优化重点企业数据交换服务，拆分进出口交换通道，保障重要企业不会因数据积压导致申报受影响。

根据海关总署和北京海关要求，修改海关管理端系统页面，统一页面样式，操作流程，集成到北京海关统一入口中。

优化跨境电商数据统计服务，完善进出口相关统计内容，根据用户要求增加查询条件，满足用户不同使用场景。

3.7 应急策略

3.7.1 应急响应流程



1）应急小组成员要保证手机 24 小时开机。

2）当接到应急响应请求时要在 1 小时内抵达现场。

3）硬件应急维护人员要携带硬件备件及相应的维护工具。

4）在应急响应人员抵达现场前，维护小组要尽最大努力做好系统备份工作和故障初步诊断。

5）应急小组抵达现场后一方面要听取维护小组的故障描述和诊断，同时根据情况要制定相应的解决方案。

6）在实施解决方案前要对数据进行备份，保证数据的安全完整，故障解决后要进行 48 小时持续监控。

7）在故障解决后，应急响应小组要仔细分析故障产生的原因并检测其它类似系统是否存在潜在故障，并提出预防和解决方法。

8）对于安全类故障，除要对发生故障的系统进行全面安全检测，还同时对其它类似和关联的系统也要进行检测以防患未然。

3.7.2 应急数据恢复策略说明

为了加强数据的安全性，各种不同的备份软件也就应运而生了，现在在备份可分为以下几种：完全备份，增量备份，差异备份，累加备份策略等

1：完全备份：就是 拷贝给定计算机或文件系统上的所有文件，而不管它是否被改变。

2：增量备份：是指备份在上一次备份后增加，改动的部分数据。增量备份可分为多级，每一次增量都源于上一次备份后的改动部分。

3：差异备份：是指备份在上一次完全备份后有变化的部分数据。如果只存在俩次备份，则增量备份和差异备份内容一样。

4：累加备份：采用数据库的管理方式，记录积累每个时间点的变化，并把变化后的植备份到相应的数组中，这种备份方式可恢复到指定点的时间点

一般在使用过程中，这几种策略经常结合使用，常用方法有：完全备份，完全备份加增量备份，完全备份加差异备份，完全备份家累加备份。

3.7.3 系统应急切换步骤

1、发生计算机软件系统故障后，系统使用人员应立即保存数据，停止该计算机的业务操作，并将情况报告应急小组，不得擅自进行处理。

2、应急小组立刻派出技术人员进行处理，必要的情况下，通知各业务处室

停止业务操作和对系统数据进行备份。

3、应急小组组织有关人员在保持原始数据安全的情况下，对计算机系统进行修复，修复成功后，利用备份数据恢复丢失的数据。

4.保障工作方案

4.1 网络保障

1. 网络线路有中断或硬件设备发生故障，网络管理员应立即向项目经理报告。
2. 网络管理员要迅速判断故障节点，尽全力查明故障原因，并及时予以恢复。
3. 如果网络线路同时中断，或者发生故障的硬件设备一时无法修复的，网络工程师应在判断故障节点，查明故障原因后，尽快处理解决，同时向上级汇报。自己一时无法处理解决的，经领导同意后，并立即向网络供应商请求援助解决。

4.2 数据库保障

1. 数据库安全由负责人员每日监测其数据完整性。
2. 发现数据异常时，及时通报情况，并作好记录。
3. 系统管理员妥善保存网络数据交换记录、日志或审核记录，将有关情况汇报，并及时追查非法操作信息来源。
4. 一旦数据库崩溃，计息部人员应立即进行数据及系统修复，修复困难的，可向主管领导汇报情况，以取得相应的支持。在此情况下无法修复的，应向公司领导报告，在征得许可的情况下，可立即向软硬件提供商请求支援。在取得相应技术支援也无法修复的，应及时向公司领导报告，在征得许可，并可在业务操作弥补的情况下，利用最近备份的数据进行恢复。

4.3 安全保障

1. 软件系统、数据库定期备份，并保存在指定备份服务器。
2. 发现安全事件时，管理员首先要将被攻击（或病毒感染）的服务器等设备从网络中隔离出来，保护现场，并同时通报情况。

3. 管理员负责恢复与重建被攻击或被破坏的系统，恢复系统数据，并及时追查非法信息来源。必要时，可向领导汇报情况，取得相应的支持。

4. 利用常规工具和漏洞库对系统进行扫描探测，分析检查，消除弱口令和因为操作人员对安全机制了解不够，配置不当等造成的安全隐患。

5. 定期对网络中的设备，如防火墙、IDS、IPS、路由器等的配置策略进行人工审核，防止因为配置不当导致安全事件发生。

6. 定期对 WEB 服务的配置、日志进行检测，安全工程师定期进行渗透测试，了解 WEB 服务的安全现状和入侵攻击的途径。最大限度的保证 WEB 服务的安全。

7. 定期对服务器登录密码、数据库访问密码、中间件访问密码进行更新，密码强度符合标准，长度不小于 8 位，包含大小写字母、数据和字符。

8. 对数据库账户进行最小权限设定，不允许系统访问出现超级账户的现象。

9. 对部署在电子口岸专网的防病毒终端策略进行调整，增加安全防护及业务稳定性。

10. 对部署在电子口岸专网应用的网络访问流量进行核查，分析 IDS、IPS、流量分析等安全监控设备的异常访问，并及时对异常 IP、异常事件进行处置，保障业务安全稳定。

11. 定期对部署在电子口岸专网的服务器进行漏扫，根据漏扫报告进行修复、加固。