**青浦区安全生产一体化综合**

**监管平台**

**招**

**标**

**需**

**求**

2024年9月

**目录**

[第一部分 项目简介 3](#_Toc709965859)

[一、项目名称 3](#_Toc977049481)

[二、项目单位 3](#_Toc1610662205)

[三、建设周期 3](#_Toc1368309000)

[四、项目预算 3](#_Toc1914470924)

[第二部分 技术规格及要求 3](#_Toc765336667)

[一、项目背景 3](#_Toc1733800386)

[二、建设目标 4](#_Toc777481359)

[三、建设内容 5](#_Toc1838692365)

[四、系统安全要求 7](#_Toc612898225)

[五、国产化云资源及产品软件要求 10](#_Toc1648896563)

[六、投标单位资质要求 10](#_Toc1875553453)

[1.投标单位资质 10](#_Toc1661913905)

[2.项目设施人员配备要求 11](#_Toc1614688453)

[七、服务和培训要求 11](#_Toc317982432)

[1.系统服务要求  11](#_Toc1391420888)

[2.运维服务人员 12](#_Toc1661432433)

[3.运维服务报告 13](#_Toc2112523137)

[4.服务时间 13](#_Toc829227708)

[5.管理要求 13](#_Toc1808702973)

[6.培训要求 14](#_Toc1239843926)

[7.其他说明 14](#_Toc1023037441)

[8.服务评估 15](#_Toc1436193005)

[9.运维服务期 15](#_Toc379642755)

[八、验收要求 15](#_Toc481868048)

# 第一部分 项目简介

## 一、项目名称

青浦区安全生产一体化综合监管平台

## 二、项目单位

上海市青浦区应急管理局

## 三、建设周期

自合同签订之日起至2025年6月30日

# 第二部分 技术规格及要求

## 项目背景

党的二十大报告明确提出“坚持安全第一、预防为主，建立大安全大应急框架，完善公共安全体系，推动公共安全治理模式向事前预防转型。推进安全生产风险专项整治，加强重点行业、重点领域安全监管”的指导精神，为各级政府部门的安全生产综合监管指明了工作方向、工作要求和目标任务。安全生产管理要着力破解瓶颈性、根源性、本质性问题，全力防范化解系统性重大安全风险，坚决遏制重特大事故，有效降低事故总量，推进安全生产治理体系和治理能力现代化，以高水平安全保障高质量发展，不断增强人民群众的获得感、幸福感、安全感。

《中华人民共和国国民经济和社会发展第十四个五年规划和2035年远景目标纲要》指出：坚持人民至上、生命至上，健全公共安全体制机制，严格落实公共安全责任和管理制度，保障人民生命安全。提高安全生产水平。完善和落实安全生产责任制，建立公共安全隐患排查和安全预防控制体系。建立企业全员安全生产责任制度，压实企业安全生产主体责任。加强安全生产监测预警和监管监察执法，深入推进危险化学品、工、交通、消防、民爆、特种设备等重点领域安全整治，实行重大隐患治理逐级挂牌督办和整改效果评价。推进企业安全生产标准化建设，加强工业园区等重点区域安全管理。加强重大灾害防治等领域先进技术装备创新应用，推进危险岗位机器人替代，在重点领域推进安全生产责任保险全覆盖。

《上海市安全生产“十四五”规划》指出：强化底线思维和红线意识，深化源头治理、系统治理和综合治理，夯实安全生产基层基础，有效防范化解重大安全风险，扎实推进安全生产治理体系和能力现代化，为上海加快建设具有世界影响力的社会主义现代化国际大都市提供安全保障，构筑与上海“五个中心”和社会主义现代化国际大都市定位相适应的安全生产发展新局面，推进安全生产治理体系和治理能力现代化迈上新的台阶，显著增强城市安全韧性，强化依法治理，强化科技赋能，强化社会共治，全面提升超大城市风险综合防控能力，不断提升城市本质安全水平，保障上海始终位于全球最安全城市之列。

为深入贯彻落实党的二十大精神和习近平总书记关于安全生产的重要指示批示精神、按照国务院、市委、市政府应急管理工作的总体部署，落实《青浦区应急管理“十四五”规划》指导精神，结合青浦区应急管理局2023 年工作要点，青浦区应急局为全面推进安全生产治理体系和治理能力现代化，提升安全生产单位本质安全水平，以新安全格局保障新发展格局，为青浦打造“战略赋能区、数创新高地、幸福温暖家”和建设现代化枢纽门户创造良好安全环境。按照“技术整合、资源整合”的要求，构建一体化监管、信息共享、功能协同的青浦区安全生产一体化综合监管平台。

## 建设目标

本项目以安全生产监管、监察、应急和服务为业务主线，**紧紧围绕服务于防范事故和安全生产监管监察业务，加强依法治安，深化信息化与安全生产业务融合，**充分利用大数据、人工智能等新一代信息技术，以数据资源为基础，以大数据创新应用，落实“数据赋能”“科技赋能”，建成青浦区安全生产一体化综合监管平台，实现信息整合共享、智慧协同的全生命周期安全生产管理，满足青浦区安全生产监督业务需求，同时推进数据赋能区城运、区大数据中心、街道及其他部门。打造全链条“安全生产”一站式管理平台，推进安全生产管理创新。主要实现以下目标：

**1.提升监管效率，**通过信息化手段，实现对青浦区各类安全生产活动的实时监控、数据分析与预警，从而提高监管效率，确保安全生产工作的及时性和有效性。

**2.强化风险防控，**平台应能够全面收集、整理和分析安全生产数据，帮助监管部门准确识别潜在的安全风险，制定针对性的防控措施，降低事故发生的概率。

**3.促进跨部门协作，**通过建设一体化综合监管平台，实现各部门之间的信息共享与互通，促进跨部门协作，形成合力，共同推动青浦区安全生产工作的发展。

**4.提高决策支持能力，**平台应提供强大的数据分析和可视化功能，为监管部门提供科学依据和决策支持，帮助领导层做出更加明智、精准的决策。

**5.推动企业主体责任落实，**通过平台的建设，加强对企业的安全生产监管，推动企业落实主体责任，提高安全生产管理水平，形成政府监管、企业自律、社会监督的良好氛围。

## 建设内容

本项目建设遵循安全生产顶层设计及信创要求，统筹规划解决方案，通过整合现有“青浦区企业安全员智慧管理系统”建设平台统一、信息完整、功能齐全、标准一致、资源共享、运行稳定的“青浦区安全生产一体化综合监管平台”，将系统覆盖面从原来的全区企业安全员，拓展至政府监管、安全员保障、志愿者监督的全面安全生产防护；并将原有只针对安全生产企业，覆盖至重点监管企业、厂库房、大型商超、建筑工地等单位。

投标人需根据建设内容进行的需求分析及方案设计（包含但不限于系统架构设计、功能设计、性能设计、原型设计等）。

具体建设内容包括安全生产一体化驾驶舱子系统、安全生产一站式服务子系统、安全生产一终端移动应用子系统，以及配套安全生产数据中心建设：

1. **安全生产一体化驾驶舱子系统**

该子系统是平台的核心展示与决策支持部分，通过大数据可视化技术，将各类安全生产数据进行实时展示与分析。1.数据集成与展示：整合各类安全生产数据，通过图表、地图等形式直观展示安全生产状况、风险分布、事故趋势等信息。2.预警与决策支持：基于数据分析，实现安全生产风险的预警与预测，为监管部门提供决策支持，指导安全生产工作。3.交互与操作：提供灵活的交互功能，支持用户进行数据查询、筛选、对比分析等操作，方便用户深入了解安全生产情况。

1. **安全生产一站式服务子系统**

该子系统旨在提供一站式的安全生产服务，简化流程，提高服务效率。1.安全生产工作门户：为用户提供统一的访问界面和导航服务；2.事故应急处理：用于对安全生产事故进行全过程管理，包括事故报告、调查处理、统计分析等功；3.安全隐患管理：对潜在的安全生产隐患进行识别、评估、整改和跟踪管理；4.安全检查管理：对安全生产工作进行定期检查和评估，确保各项安全生产措施得到有效执行；5.安全生产监管绩效：对监管部门和企业的安全生产工作绩效进行评估和考核，推动安全生产责任的落实；6.安全知识学习：提供在线安全培训课程，覆盖安全生产知识、技能等方面，提升企业和员工的安全意识与能力。

1. **安全生产一终端移动应用子系统**

通过整合“青浦区企业安全员智慧管理系统”现有移动端，并进行优化拓展，方便用户随时随地了解安全生产情况。1.移动监管：支持监管人员通过移动设备进行现场监管，实时上传检查记录、发现问题，并与后台数据进行同步；2.企业自查自报：提供企业用户自查自报功能，企业可以定期上报安全生产情况，实现自我管理与自我监督；3.信息推送与提醒：根据用户需求，推送安全生产相关的通知、提醒等信息，确保用户及时了解安全生产动态。

1. **安全生产数据中心**

数据中心是平台的数据存储与管理中心，为其他子系统提供数据支持。根据实际需求建立安全生产单位、事件、人员、知识专题数据库，建立高效的数据存储与管理机制，确保数据的安全性、完整性和可用性。同时利用青浦区大数据资源平台能力，将现有青浦区重点监管行业安全生产风险监测预警系统、青浦区防灾减灾综合一体化平台、青浦区应急指挥调度系统等系统的数据资源以接口形式赋能本项目的应用；并与现有实有人口库、实有企业库实现数据比对对接，以保障系统基础数据的准确性和完整性。

## 系统现状

### 1.现有系统概况

现有《青浦区企业安全员智慧管理系统》根据对企业安全员管理的工作要求，提供应用工具包括企业安全员移动应用及配套管理后台。通过安全员上岗签到、隐患排查、隐患处置等功能提升事故的预测预警预防能力，通过系统分解责任，细化措施，抓好落实，动态隐患清零，现场有效管理，有力稳控安全形势，遏制事故发生。本次项目建设将原有青浦区企业安全员智慧管理系统移动应用整合至本项目内，并在原有基础上进行功能拓展优化。

### 2.现有网络架构

原有系统部署了3台服务器在政务云机房，1台作为数据库服务器，1台作为WEB应用服务器上，1台作为小程序服务器，接入政务网环境。



### 3.现有服务器及产品化软硬件资源情况

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **云主机名称** | **服务器配置** | **操作系统** | **其他软件** | **部署域** |
| 1 | web应用服务器 | CPU8核、内存32G、硬盘600G | 银河麒麟v10 sp1 | 东方通V6.1.4.0 | 政务外网区 |
| 2 | 数据库应用服务器 | CPU4核、内存16G、硬盘600G | 银河麒麟v10 sp1 | 达梦数据库v7.1.5 | 政务外网区 |
| 3 | 移动应用服务器 | CPU2核、内存8G、硬盘200G | 银河麒麟v10 sp1 | 东方通V6.1.4.0 | 互联网区 |

## 系统性能要求

**1、系统稳定性指标**

1）系统保证7\*24 小时不间断运行；

2）平均故障间隔时间（MTBF）≥8500 小时；

3）平均修复时间MTTR≤1小时；

4）可用率≥99.99%。

**2、系统应用性能指标**

采用基于可扩展、可插拔、支持分布式部署基于SOA架构的技术路线。

并发<100新增、修改、删除、查询统计、列表显示页面<=1.5秒。

100<并发<=1000新增、修改、删除、查询统计、列表显示页面<=3秒。

**3、系统响应时间指标**

单个用户，操作最长不超过2秒；系统响应时间≤0.5 秒。

当用户做一些处理时间较长的操作时，能给出提示信息提醒用户。在返回数据量过大导致响应时间过长时，能提供部分响应，例如分页取数据等，减少操作人员等待的时间。

**4、系统并发处理能力指标**

系统能够支持同时从多个部门或地方并发使用，要求系统不能由于用户连接的增加明显降低系统的响应时间。支持同时在线用户数1000人；并发用户数100人。

## 系统安全要求

本次项目要求部署在青浦区电子政务云平台，系统需要符合信息系统等级保护三级要求。

### 1.安全系统建设主要目标

计算机信息系统的安全就是保护信息内容的安全性，防止和检测计算机用户进行未经授权的活动。对计算机信息网络安全系统的建设，目前主要包括以下六个要素：

机密性：确保信息不暴露给未授权的实体。

* 完整性：只有得到允许的人才能修改数据，并且能够判别出数据是否已被篡改。
* 可用性：得到授权的实体在需要时可访问数据，即攻击者不能占用所有的资源而阻碍授权者的工作。
* 可控性：可以控制授权范围内的信息流向及行为方式。
* 可审查性：对出现的网络安全问题提供调查的依据和手段。
* 抗抵赖性：提供技术手段，防止对关键操作的抵赖。

针对以上信息系统安全建设的六要素，在网上办案平台系统建设中，安全系统建设的主要建设目标可归纳为以下几点：

（1）网络传输安全保障功能

对于通过公共网络传输的重要信息经过加密设备的加密，以防止网络上的窃听。任意一个用户在进入系统时都必须经过严格、有效和快速的验证，并且只有经过一定授权的用户才能访问其权限之内的信息，防止非法用户的侵入。实现用户端到服务器端的端-端的传输安全。

（2）抗服务攻击、入侵检测和审计

对来自外部的恶意入侵和违规操作进行识别、跟踪、记录、分类和报警，并为遭到破坏的网络及信息系统的恢复提供技术性支持。

（3）数据分析和内容检测

能够对系统中传输的各种协议进行分析，检测数据流，让合法的网络数据流顺利通过，阻止非法使用网络，监控上网的内容，防止出现有害信息。

（4）网络病毒防杀技术

对网络上的计算机病毒能自动进行检测、报警；能够监控查杀网络病毒，具备网络病毒检测、预防病毒、病毒诊断和删除与恢复被病毒感染的系统与文件；能够发现新型网络化病毒，并且通过网络进行版本的更新，增加查杀新型病毒的能力；在一定范围和程度上，能够有效追溯病毒源头。

（5）严格的访问控制和信息安全保护技术

对用户进入系统，实施身份认证和授权管理，防止非法获得信息资源。

（6）系统安全检测技术

能够对多种网络安全漏洞进行检测与扫描；具有多线程快速并行扫描能力；具有灵活的策略配置。

（7）应急反应和安全管理技术体系

建立一套网络安全管理系统，能够组织和协调各种资源对系统进行保护，自动告警系统遭受攻击，并且采用相应的保护措施；自动告警系统被破坏，并且进行恢复。

### 2.安全系统总体架构要求

按照网络OSI的7层模型划分，网络信息系统的安全建设贯穿于网络系统整个7层架构，针对网络系统实际运行的TCP/IP协议，网络安全系统建设主要对应于网络信息系统的4个层次。

针对本项目，其安全系统的建设需求是全方位的、整体的，需要在不同层次解决不同的安全问题。

### 3.系统整体安全集成

安全系统的构建决不是安全设备的简单堆砌，需要在安全设备配置的基础上进行系统的整体安全集成及配置，具体说来，主要包括以下工作：

（1）防火墙安全策略制定和规则设置

根据网络资源管理系统的网络结构、运作方式，对外提供的服务等各方面信息，制订网络防御的总体按全策略，并对防火墙进行细致的设置实现既定的安全策略，做到保证系统正常运转前提下对外部提供最小访问权限。

（2）安全审计系统规则设置

根据网络资源管理系统的运作方式适当设置审计系统的规则（例如针对特殊端口的审计，针对特定服务器的登录操作审计等），提高审计系统的运行效率，并对所有重要的网络操作进行报警，并配置相应的反应措施（如阻断等）。

（3）网络设备安全性设置，访问控制规则设置

根据整个系统的运作方式，正确设置所有网络设备，做到网络设备自身的安全性，并适当设置网络访问控制权限，在确保系统正常运行的前提下控制内部和外部网络的网络访问，开放最小访问权限。此外，还将通过各个安全部件保障网关系统的安全运转。

（4）操作系统裁减、文件系统、用户开设等安全性设置

根据网络资源管理系统的特定情况，对各个主要服务器、工作站、客户机的操作系统进行裁减，在保证系统正常运行的前提下，关闭不需要的功能，加载必要的补丁，改变缺省配置，包括文件系统和用户系统等，加强主机自身的安全性。

（5）Web自检恢复系统自身安全防护措施与其它安全部件整合

为确保WEB自检恢复系统安全、稳定、有效地运行，将采用身份验证系统，授权管理系统，审计系统来保护WEB自检恢复系统，对该系统的管理操作进行限制，记录，对该系统运行进行监控等，防止该系统失效。

（6）病毒防杀系统自身安全防护措施与其它安全部件整合

对病毒防杀系统自身安全防护措施进行规划，达到病毒防护系统与其它安全系统的整和，一方面保障其它安全系统不受木马操控，并在发现病毒情况时向审计系统报警，另一方面，其他的安全防护措施将保障病毒中心服务器的安全。

本次项目安全系统统一使用区电子政务云平台现有设备。

## 密码安全建设要求

投标人应根据《密码应用基本要求》，从物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全、安全管理等层面，围绕重要数据、系统角色、关键软硬件设备、关键业务环节、关键操作行为等重点对象,对本项目进行分析，在项目建设中配套密码应用建设并在投标文件中提供配套密码应用建设方案。

同时，投标人在中标后需按照密码应用建设方案对本项目进行密码应用建设。本项目在通过相应密码应用测评，具备《商用密码应用安全性评估报告》后，方可进行项目验收。

## 国产化云资源及产品软件要求

本项目的服务器资源，拟采用青浦区政务云资源形式进行申请，投标人无需自行采购。投标人需对本项目软件系统的运算量、存储、网络并发等性能需求进行分析，并对云资源提出明确产品选型，以便作为项目实施过程的云资源申请依据。

**同时，拟建的软件系统需要按照国产化要求的技术框架开发，需要兼容以下**备计算机或信息化行业**：**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **类型** | **品牌** | **版本** |
| 1 | 操作系统 | 中标麒麟 | 7U6 |
| 2 | 数据库 | 达梦 | V8 |
| 3 | 中间件 | 东方通 | 7.0.E.2 |

## 投标单位资质要求

### 1.单位资质要求

1、投标人需具备质量管理体系认证证书；

2、投标人需具备环境管理体系认证证书；

3、投标人需具备职业健康安全体系认证证书；

4、投标人需具备国家认证机构颁发的ISO27001信息安全管理体系认证证书。

### 2.项目设（实）施人员配备要求

软件开发团队具备工业和信息化部门颁发的如下证书：

项目负责人具有计算机行业高级职称；项目团队人员具备系统集成项目管理工程师、网络工程师、安全防范工程师、软件开发工程师、软件设计师等相关证书，一人具有多张证书的算一个。

提供以上所有人员在投标单位自2024年1月1日以来任意连续3个月的社保证明，否则不予认可。

## 服务和培训要求

服务要求响应:服务内容由采购人组织相关部门和人员对项目进行验收。然后进入运行服务期。

### 1.系统服务要求

**服务范围**

本项目的服务范围包括对构成项目的所有服务器、网络、应用软件等的维护、维修、产品升级和培训等。

**服务内容**

服务内容包括日常运维、升级优化、服务咨询、特殊保障。

#### （1）日常运维

中标人安排固定工作人员进行售后日常运维服务，且**安排不少于2名人员进行7\*8小时驻点服务**，掌握系统运行情况，主动巡检，接受临时维修、保修要求，记录并向管理负责人汇报，管理负责人及时安排相关人员进行维修。每次维修行为要有维修单，详细记录保修时间、修复时间、保障情况、处理办法和结果、维修单要有甲方书面确认。驻点工作人员须经培训合格后并获得相关职业上岗证书方可上岗。

#### （2）升级优化

1）系统更新。中标人应根据应用系统运行情况定期向采购方提供系统的数据更新、应用界面更新，并确保应用系统相关业务功能正常运行，确保系统以最优状态运行。

2）文档更新。中标人应建立完备的资料库，包括用户的电路资料、点位地址、备份情况、应用特性以及用户配置等，这些资料应作为成果提交给用户。一旦资料进行了版本更新，应在3天内向采购人提供最新版本的资料。

3）升级服务。中标人应提供设备内嵌软件、产品操作系统、第三方采购软件和应用软件的升级服务，产品升级后，需要进行再次测试.

#### （3）服务咨询

中标人应设立专用的服务调度中心提供免费的服务热线电话，接受系统故障保修、使用帮助要求、业务和技术咨询、服务投诉等。该服务调度中心应该7\*24小时全天候运行，应配备足够的咨询人员或技术工程师，热线电话的拨通率应达到95%以上。在热线电话发生故障情况下，应提供其它备份的方便和迅速的联系方式。

#### （4）特殊保障

临时保障。采购人如有重大事件、临时现场监控等较特殊的保障措施，中标人能按时提供服务。

安全保障。采购人如有安全保卫、系统接管等较特殊的要求，中标人能按照要求提供服务。

### 2.运维服务人员

本项目运维服务人员分为驻场人员、技术支持人员2类。

**1）驻场人员要求：**

具有应用系统运维服务经验**（需提供相关能力证明）**；

必须为中标单位在职人员**（需提供相关社保缴纳证明文件）；**

在项目运维服务期间，若驻场人员更换也必须为中标单位在职人员**（需要在投标文件中做出相应承诺）。**

**2）技术支持人员要求：**

具有系统运维、服务器管理、数据库管理经验**（需提供相关能力证明）**；

### 3.运维服务报告

在整个运维服务周期内，中标人应与用户建立完善的沟通协调机制，应及时提供运维服务的各种报告。包括每日运维服务日志、重大故障维修报告、每月故障总结报告、每季度的系统管理报告等。此外用户还可根据实际情况需要，要求中标人就特定事件提交说明报告。中标人应提供各种设备管理的原始数据（包括设备故障数据），接受用户的独立检查。

### 4.服务时间

1、提供7\*24小时服务承诺。中标人需承诺提供全天候7\*24小时的故障维护服务和技术业务咨询服务，并有专业的技术人员负责及时解决系统出现的任何故障。

2、在接到故障报修后，中标人须在30分钟内响应，技术工程师1小时到达现场。到达现场后4小时内排除设备故障（遇到自然灾害等不可抗拒事故除外）。对于一时无法按时排除故障，要求在24小时内解决（对于特殊情况经双方协商决定排除故障时间，如基础设备损坏等），由此产生的费用由中标人承担。

### 5.管理要求

中标人应根据运维服务要求建立完善的服务管理体系，保障承诺的服务内容的实施。有关要求如下：

1、服务组织机构

中标人应建立专门的服务管理机构，设立专门的技术服务队伍，配备专业维护工程师。中标人应在提交给采购人的相关文件中详细描述组织机构的构成、人员配备及其各层级的职责分工。

2、服务流程

中标人应建立各项服务流程，按照流程要求提供高质量、响应快的服务。服务商应提交给采购人的相关文件中详细描述相应的服务流程。

3、维护场地要求

为保障响应速度，要求中标人设立办公场地，由工程师常住，

可以确保维护服务保障能够及时响应。

### 6.培训要求

1）对采购人的技术人员和日常监控操作人员进行系统的使用、维护和保养培训，该培训将教会学员在日常和紧急情况下如何操作系统。

2）在培训工作开始前向采购人免费提供培训资料，能进行实际操作和日常维护、排除一般故障。

3）采购人的技术人员和日常监控操作人员经过培训应能进行日常设备运行维护工作，掌握软件、硬件的操作，熟悉硬件基本功能。能有效的组织、开展业务应用能力。

4）当系统升级或者改造时，应进行免费系统升级及改造专门培训，具体时间由双方协调培训时间。

5）要求组织每年年度培训，包括对运行维护、技术、管理操作人员的培训，时间不低于两天时间。

### 7.其他说明

（1）无论何时，系统中的声音、图像和数据信息的所有权和使用权都属甲方。未经甲方允许中标人无权使用、转让或处理系统中的声音、图像和数据信息。中标人应妥善保存系统的声音、图像和数据信息。

（2）在维护期内涉及的所有的系统方案文档、设计文档、测试文档、设备使用说明书、施工设计方案、施工图纸、软件说明书、系统维护手册、运维文档、项目管理文档等与本工程有关文档的知识产权中标人所有。

（3）中标人应在签订合同后承担建设、售后质保维护等工作中的保密义务，与甲方签订保密责任书。涉及到的相关工作内容终身保密。

### 8.运维服务期

1）服务期1年，服务开始计时时间为系统验收合格正式投入使用之日。

2）服务期届满后，无论是否续签运维服务协议，中标公司都必须保证平台的正常运行和功能完善。

## 验收要求

系统验收合格的条件必须至少满足以下四个要求：

(1) 已提供了合同的全部服务和资料；

(2) 试运行时性能满足合同要求；

(3) 性能测试、功能测试和试运行验收时出现的问题已被解决；

(4) 按照上海市青浦区信息化建设项目的程序和要求，通过由业主方或相关主管部门组织的项目竣工验收。