启东市数据局政务服务软件系统改造项目建设方案

第 一 章 现状分析

本局现有自建应用系统 1 个，未进行国产化替代，具体情况如下表：

现有系统汇总表														
序号	系统名称	使用单位	部署网络	部署位置	开发单位	建设年份	建设资金（万元）	部署架构	主要开发语言	用户数	应用范围	安全测评情况	前期是否替代	系统使用状态	项目名称
1	启东市新产业服务中心信息系统	启东市数据局	政务网互联网	政务云	国泰新点软件股份有限公司	2022-2023	2133.2	B/S	JAVA	7476	启东市区部门及企业群众	等保贰级	否	在用	启东市新产业服务中心信息系统（软件）项目

1.1 系统当前功能建设情况

序号	应用系统名称	一级模块	二级模块	改造计划
1	智慧政务服务一体化平台	多元化线上服务门户	江苏旗舰店（启东市）	**整合改造适配**
			全流程网办移动端应用服务	
			智能客服启小 i 智算升级	
			老年人服务	
			移动端服务	

			政务地图服务	
		智慧化线下服务大厅	政务大厅现场服务系统建设	
			政务大厅自助服务系统	
			政务大厅综合业务管理系统	
		政务服务业务应用系统	统一制证中心（AI 审批、电子证照）	
			跨区域通办	
			高效化日常事务管理	
2	数字驾驶舱	驾驶舱应用场景		**整合改造适配**
		驾驶舱控制台		
3	数据交换、系统对接与整合	与排队叫号系统对接		**整合改造适配**
		与短信网关的对接		
		与江苏省政务服务网对接		
		与市一体化平台对接		
		与市数据共享交换平台对接		
		基础中间库		
		与审批系统对接		
		统一数据共享接口		
		与智能化硬件设备对接		
		与现有一件事系统对接		
		系统接口扩展		

1.2 资源使用情况

现有系统资源使用情况汇总															
序号	系统名称	部署位置	服务器			存储设备		操作系统		数据库		中间件		其他支撑软件	
			部署方式	品牌型号	数量	品牌型号	数量	品牌型号	数量	品牌型号	数量	品牌型号	数量	品牌型号	数量
1	启东市新产业服务中心信息系统	政务云	docker	虚拟机 合计：CPU214 核，内存 416G，存储 21T	35	NFS	1	Centos7	34	mysql	4	tomcat	25	nginx	1
								windows	1	MongDB	2	RabbitMQ	2		
												redis	1		

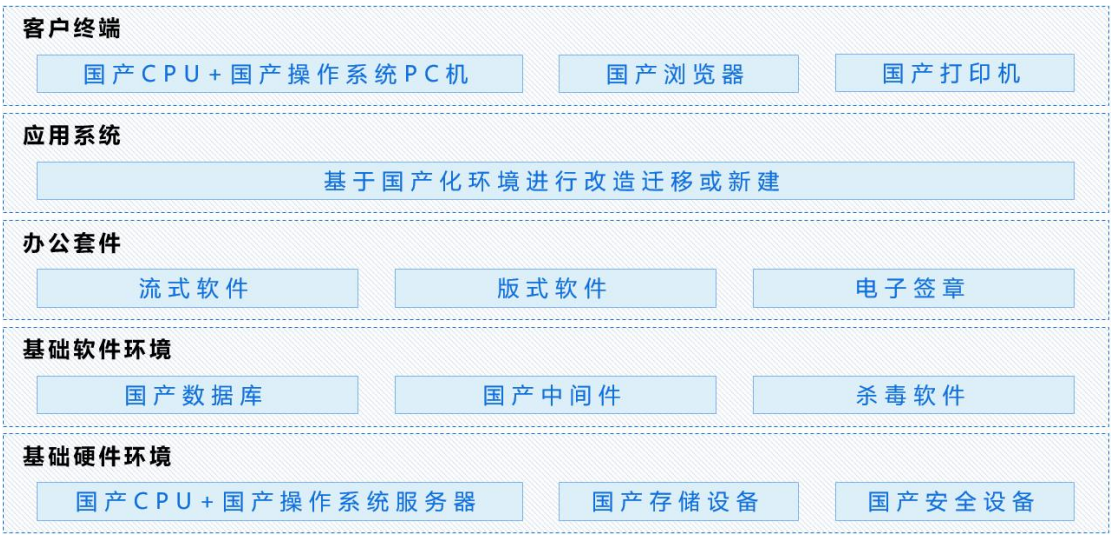
第 二 章 总体建设方案

2.1 总体建设内容

总体建设内容包含：智慧政务服务一体化平台、数字驾驶舱的国产化适配改造及数据对接整合工作。

2.2 系统总体结构和逻辑结构

平台国产化适配总体架构主要包括以下几个方面：基础硬件环境改造、基础软件环境改造、办公套件替换、应用系统改造、客户终端替换 5 个方面，如下图所示：



（一）基础硬件环境改造

基础硬件环境改造是国产化适配的基础工作，基础硬件环境改造包括国产 CPU、国产操作系统服务器升级改造；国产存储设备改造以及国产安全设备改造。基础硬件环境改造完成后，才能实现关键核心技术设备、信息产品和服务等的自主可控，是实现保障网络信息安全的前提条件。

（二）基础软件环境改造

基础硬件环境改造是保障网络信息安全的前提条件，基础软件环境改造是在硬件环境改造基础上，对保障网络信息安全的有效补充。基础软件环境改造包括替代国产数据库、国产中间件以及国产杀毒软件等。

（三）办公套件替换

基础软硬件环境改造完成后，对使用最频繁的办公套件也需要替换成国产软件。办公套件替换主要包括流式软件、版式软件和电子签章等。

（四）应用系统改造

基础软硬件和办公套件国产化适配升级改造完成后，为政务服务平台运行提供了国产化基础环境。在国产化软硬件基础环境下，需要对政务服务平台国产化适配进行升级改造。应用系统升级改造主要体现在3个方面：

政务服务平台能够在国产化基础软、硬件环境、国产化办公套件下正常运行；

网络和通信层改造，基于SSL安全接入网关服务建立一条安全的信息传输通道；

系统应用安全改造，系统对政务服务平台关键环节采用国密算法SM2、SM3、SM4算法进行改造。

（五）客户终端替换

平台国产化适配对服务器端改造完成后，还需对访问客户终端进行替换。客户终端替换主要包括客户端国产化CPU、国产操作系统PC机、国产浏览器及国产打印机等。

2.3 启东市新产业服务中心信息系统

2.3.1 智慧政务服务一体化平台

2.3.1.1 多元化线上服务门户

2.3.1.1.1 江苏旗舰店（启东市）

1、功能栏目

功能栏目需包括查、看、评栏目、热门服务轮播推荐以及侧边栏功能。

（1）查、看、评栏目

在旗舰店首页中增加查、看、评功能模块。

（2）热门服务轮播推荐

应提供热门服务轮播推荐功能，需包括公告轮播、热门功能轮播。

（3）侧边栏功能

在侧边栏展示智能客服、政务服务APP二维码、办件查询和老年人服务。

2、办事服务专区

应在旗舰店首页开设办事服务专区，将办事服务划分为法人服务、个人服务分别展示。

（1）法人服务

将法人服务划分成单事项以及一件事，并展示法人办事热门事项。需包括单

事项办理、一件事办理。

（2）个人服务

将个人服务划分成单事项、一件事以及全生命周期，并展示个人办事热门事项。需包括单事项办理、一件事办理。

3、特色服务专区

在旗舰店首页开设特色服务专区。在专栏中对高效办成一件事、远程踏勘等一系列特色服务进行展示。

4、优化营商环境专区

在旗舰店首页开设优化营商环境专区。在专区中展示与营商环境指标相关内容。

2.3.1.1.2 全流程网办移动端应用服务

需基于江苏政务服务网 APP（启东站点）建设，本次建设提供事项全流程网办服务。基于“一网通办”平台，对全程网办事项进行网厅申报，完成全程网办。同时完成受理审批端，包括申报接受、受理端基础应用服务支撑对接。

2.3.1.1.3 智能客服启小 i 智算升级

在 PC 端，移动端（基于苏服办 app）提供智能客服咨询服务，企业或个人在申报时遇到问题，可通过智能客服对问题进行咨询，满足专业化、7*24 小时的互动需求，功能包括问答交互、智能提示、基本语义理解、快捷短语等。

（1）交互界面升级

多端界面焕新：重构 PC/移动端首页交互模块，优化会话记录管理及热门推荐模块，提升用户操作流畅性。

咨询场景增强:统一咨询流程设计,优化回复卡片动态效果与用户反馈机制。

（2）智能体能力整合

电信智能体对接：接入第三方专业智能体接口，实现业务咨询场景深度赋能（如事项办理流程、材料清单等专业问答），同步强化 RAG 技术应用，提升知识检索精准性。

（3）后台效能提升

话术与规则配置：管理后台支持指令命中逻辑和话术配置，实现精细化服务

管控。

通过界面优化与智能体深度协同，打造"精准响应、主动服务"的政务智能客服体系，推动咨询效率提升30%以上。

（4）算力资源

需提供一套MAXKB智能体平台，支持持 RAG 检索增强、工作流编排、MCP 工具调用能力。支持对接各种主流大语言模型，广泛应用于智能客服、企业内部知识库问答、员工助手、学术研究与教育等场景。

需提供部署智能体平台所需的云主机一台，配置为16核32G，系统盘500G的云主机。

需提供一台昇腾8卡910B算力一体机，整机可提供2.5PFLOPS（FP16）的算力。

需提供了一条100M互联网专线，用于提供外网接入与云资源监控。

需提供机房托管服务以及本地基础运维保障服务。

需保障互联网专线稳定，需提供外网访问端口，

需保障智能体平台的稳定运营并需提供相应的平台技术支持。

算力服务仅在合同期内生效。

2.3.1.1.4 老年人服务

政务服务门户设立老年人服务专区，打造线上“关爱模式”，结合老年人生理特点，提供辅助功能；根据老年人特点进行放大字体、简化操作、点读改造。

（1）专区引导服务

老年人首次登入老年人服务专区，应提供模块介绍、操作指引功能，方便老年人快速掌握了解专区内各功能，引导老年人进行界面操作。

（2）关爱模式

进入老年人服务专区，在页面右侧展示关爱模式，在老年人服务专区页面顶端展示悬浮条，悬浮条需包含文本模式切换按钮功能、页面背景切换按钮功能、语音点读按钮功能、辅助线按钮功能、辅助屏按钮功能。

2.3.1.1.5 移动端服务

1、移动服务平台

依托江苏省统一政务服务 APP，完善移动旗舰店功能。提供预约号、楼层引

导、大厅 VR、自助申报等功能。

2、移动工作平台

（1）待办事宜

平台应提供待办事宜功能模块，根据办理与否，分为待办事宜和已办事宜。

（2）公务邮件

应提供中心工作人员及领导邮件相关的收件箱、发件箱、写稿件以及草稿箱功能。

（3）通知公告

通知公告模块需包括公告等相关栏目信息。

（4）通讯录

通过同步组织框架，自动显示从服务器端同步过来的组织架构列表，可查看各个部门人员相关通讯录信息。

（5）考勤签到

应提供考勤签到功能。系统自动进行定位并签到，显示考勤人员姓名、部门、时间、地点、签到记录信息。

（6）请销假管理

应支持通过手机端进行请销假操作。填写请假的申请人姓名、申请人所在的部门、申请时间、开始时间、结束时间、请假的小时数、请假原因。

应支持查看本人的所有请假信息，可对相关请假执行销假操作。

（7）移动审批业务

应支持通过手机处理请假审核审批。

（8）我的日程

应支持对个人日程进行管理，主页面以日历的进行展示，系统自动显示当前时间段内所有已设定的日程，并标记显示。

（9）数据同步

应支持同步组织架构按钮，进行组织架构的更新。

（10）软件更新

检查软件是否有更新，若存在更新，系统提示是否下载更新。

（11）附件管理

应支持对通知公告和邮件下载模块的附件进行管理。

（12）系统设置

系统设置需包括消息设置、缓存清理等相关功能。

3、PC 端功能移植

针对建设的部分功能可移植至移动端，完成 PC 和移动端双向互联互通。

4、一码通服务

结合江苏省“苏服码”系统，应建设启东市一码通应用服务。需包括“码”上预约、扫“码”识别、“码”上亮证、“码”上评价。

2.3.1.1.6 政务地图服务

1、政务地图应用平台

需维护业务办理点信息，对接办理点相关情况，实现数字政务地图展示，便于办事人在线快速定位就近办理点，可查看附近办理点的开放情况、可办事项情况，辅助实现业务就近可办。

（1）办理点搜索

系统应提供办理点搜索功能，支持按区域搜索以及按事项搜索两种方式，并在政务地图上提供对应办理点的信息展示功能，供用户查看。需包括按区域搜索、按事项搜索、办理点展示。

（2）最佳路径推荐

应支持在政务服务网站的政务地图模块对启东的服务办理点进行浏览。同时，根据需要对申报事项及办理点地址范围进行检索，提供路线导航。

（3）详情查看

应支持查看对应办理点的基础情况信息、现场各个窗口的情况信息以及办理事项的详情信息，同时提供问题反馈的功能。需包括中心基础情况事项详情信息、问题信息反馈。

2、服务延伸（移动端）

移动端以 html5 技术进行设计开发，使页面可在各种系统环境下能够自适应显示，并符合相关规范要求。

（1）导航服务

应支持主动发起导航，自动调用第三方地图的出行路线接口，享受无缝服务

切换，提升用户体验。

（2）接入政务服务 APP

在移动端，需要将数字政务地图与启东政务服务 APP 进行对接，通过用户体系的对接、页面框架、消息中心的融合，嵌入启东政务服务 APP 的整体框架，实现政务服务的统一入口。

3、政务地图管理平台

应建立政务地图管理模块，由管理人员使用，支持按层级进行分层管理，包括办理点维护、问题反馈管理功能，为启东数字政务地图系统提供数据支撑。

（1）办理点维护

应提供政务服务中心录入功能，支持对各地区办理点进行维护，对办理点运行事项、办理点详细地址、办理点工作时间维护，形成数字政务地图。

（2）问题反馈管理

平台后台管理员可以收到用户反馈的问题信息。

（3）地图运行管理

系统应支持对启东数字政务地图资源进行统一运行管控，包括办件量、定位量可视化展现。

（4）第三方地图服务接入

应支持第三方地图服务接入，需包括点聚合 API、信息窗体 API、行政区浏览。

2.3.1.2 智慧化线下服务大厅

2.3.1.2.1 政务大厅现场服务系统

现场服务系统运用当前主流的云计算、移动互联及物联网技术，通过智能化设备的集成应用，为群众提供全方位、高智能、更加方便快捷的服务体验。需基于南通市市县一体化在线政务服务平台进行建设。需搭配大厅智能化设备进行新建。

1、智能机器人

引进智能机器人，为办事群众提供更为人性化、智能化的办事引导、问询、自助巡检服务。

（1）咨询问答

应提供语音交互功能，能够回答办事群众的各种问题。回答的内容以语音形式进行播报，且支持多媒体回复，包括图片和视频。

（2）智能查询

应提供语音询问、触屏选择的业务查询功能。通过机器人显示屏展示对应的办事流程以及相关介绍，方便办事人员进行相关业务查询。需包括信息查询、办件查询、公告查询。

（3）问路引领

应支持通过多轮对话的方式与办事群众进行沟通，了解需要办理的事项、对应的办事窗口信息，从而主动为办事群众提供路线指引和带路服务。

（4）导览讲解

根据预先设定好的路线，由机器人进行语音导览讲解。机器人带领领导参观各个宣传点位，讲解一些动态的信息，触摸屏可显示静态的信息，如中心的宣传视频、图片。智能机器人可控制显示大屏进行 PPT 讲解，支持暂停、开始、上一页、下一页、结束语音指令。

2、室内导航系统

办事群众可通过移动端大厅 VR 应用选择需要前往的地点系统支持实景导航的方式进行 VR 引导。

3、楼层引导系统

以平面图的形式展现出政务服务中心各个楼层区域分布，为办事群众提供智能化自动引导服务。

（1）楼层指南

应提供对应的各个楼层的平面展示图，包括各个部门、分区、窗口、办公室、会议室位置，方便办事群众了解大厅的整体布局。

（2）路线指引

办事群众在平面地图上选择想去的目的地位置，在确认导引服务后，系统应自动生成路线引导，指导办事群众如何前往。

4、触摸查询系统

应支持群众完成办件、办事指南、中心信息、法律法规、公示公告等相关的信息查询。

5、排队叫号系统

通过完善的系统管理功能，统计客户流量、服务状况、业务办理类型、窗口人员的工作情况信息，为办事群众灵活分配办事区域，将办事群众均衡地疏导至各个业务办理区域，有效分流，平衡各个办事窗口的工作负担。

（1）信息采集

办事群众首次在实体大厅办理业务时，系统应提示办事群众在取号终端的身份证识别区刷身份证，系统自动获取办事群众姓名、身份证号相关信息，同时系统还将要求办事群众提供相应的联系方式（手机号码），以便后期为办事群众提供全流程业务信息智能推送服务。

（2）预约取号

办事群众在线上提前取号预约，到达现场后在排队取号终端上进行预约取号操作。办事群众可以通过刷身份证、人脸识别方式完成取号操作。

（3）现场取号

办事群众在排队取号终端上通过刷身份证、人脸识别方式完成排队取号操作后，排队取号终端将打印排队叫号单，并提醒办事群众取出排队叫号单。排队叫号单上会显示窗口号、办理业务、排队号、前方等待人数和二维码信息，办事群众通过扫描二维码，即可实时获取当前排队进度信息。

（4）窗口叫号

窗口工作人员可在系统中进行叫号，需包括呼叫、重呼、下一位、过号功能。系统还显示当前叫号的号码、等待人数信息，方便窗口人员了解排队叫号的相关信息。

（5）叫号提醒

政务服务大厅排队呼叫方式以短信推送或大厅广播呼叫为主，当窗口进行呼叫时，被呼叫的办事群众会收到提醒消息、广播叫号提醒，提醒办事群众到相应窗口办理业务。

（6）窗口信息显示

以窗口上方的液晶显示屏或LED显示屏为载体，通过该设备进行窗口信息和排队叫号信息发布，能够显示窗口名称、窗口状态（如正在办理、空闲、暂停）、当前办理事项、当前呼叫号码信息，便于办事群众及时找到自己所要办理业务的

窗口。

（7）等待信息显示

以等待区的液晶显示屏或LED显示屏为载体，与排队叫号系统相结合，实现叫号信息实时动态展示。

（8）绿色通道

系统需提供绿色通道功能。针对老人、孕妇、耳背等特殊人群提供特殊优先级。

6、电子样表系统

（1）事项展示

提供事项信息检索功能，需包括模糊检索、关键字检索，方便办事群众快速定位办理事项，找到相应的表单样例。

（2）样表示例

应支持对政务事项上传的样表材料进行分类展示，申请人通过电子样表系统可快速查找到所需填写表格的电子样例，方便申请人对照电子样例进行表格填写。

（3）表单检索

系统应支持按照表单名称进行电子表单检索。

（4）缩略图展示

应支持以缩略图的形式展示样表，点击后可查看详细样表信息。

7、智能窗口管理系统

应建立智能窗口管理系统，实现单点登录集成、排队叫号集成、身份信息采集、窗口服务状态和运行数据采集功能，实现窗口的智能化管理。

（1）排队叫号集成

将排队叫号系统集成至统一桌面工作台，需包括呼叫、重呼、下一位、过号功能，显示当前叫号的号码、等待人数内容，方便窗口人员了解排队叫号的相关信息。

（2）身份信息采集

应支持办事人员的身份信息采集，方便后续事项的办理以及办事进度的跟踪。

（3）窗口服务状态

通过窗口屏或互动终端展示窗口工作人员服务状态，如果窗口人员需要暂时

离岗，可以通过系统切换为暂停服务状态。

（4）窗口运行数据

将窗口当天的业务办理情况、呼叫情况、评价信息情况上传到后台管理系统方便后续进行统计分析，为优化窗口工作提供数据支撑。

2.3.1.2.2 政务大厅自助服务系统

提供包括申报、填表功能的政务服务，提供公积金查询、不动产查询等的公共服务，支持“长三角”一体通办。与省级、市级相关系统对接。

1、自助办事服务子系统

提供包括申报、填表功能的政务服务，提供公积金查询、不动产查询等的公共服务，支持“长三角”一体通办。与省级、市级相关系统对接。

2、自助扩展打印子系统

支持部分证照从机器进行打印。

3、自助材料存取子系统

通过自助材料存取系统，实现自助发证、取证，方便办事群众。

2.3.1.2.3 政务大厅综合业务管理系统

面向大厅业务进行管理，工作人员可根据业务实际需求对相关功能进行配置，需包括智能引导管理、排队叫号管理、样表配置管理、窗口配置管理、自助终端管理、自助打印管理、材料存取管理功能。

1、智能引导管理

应支持政务大厅服务事项配置管理，对事项的情形、办理类型进行梳理和配置，从而让群众办事更方便；应提供政务服务智能机器人后台配置管理，让智能机器人更加实用，能够为办事群众提供有效的服务。需包括事项配置管理、机器人后台配置管理。

2、排队叫号管理

应提供排队叫号相关功能的配置，需包括取号分类配置、区域配置管理、取号时段配置、取号限额配置、预约取号配置、取号权限配置、取号黑名单管理以及取号类型配置。

3、样表配置管理

应提供样表配置管理，需包括事项信息配置、表单模板配置、填写提示配置。

4、智能推送管理

应提供智能推送管理，需包括定时推送服务、接收人员配置、推送内容配置。

5、窗口配置管理

根据窗口实际布局以及事项办理情况进行窗口配置管理，满足实际业务办理需要。功能需包括区域窗口配置、窗口人员配置、窗口设备配置以及窗口事项配置。

6、自助终端管理

应支持对大厅中每台自助服务终端进行基本信息登记，登记内容需包括自助服务设备序列号、所在区域、设备类型、网络 IP 地址、方位坐标，方便后台进行统一管理。

7、自助打印管理

应支持对自助打印机相关模块进行配置，以适应不同的业务对打印的需求。需包括打印设备配置、打印模块配置。

8、材料存取管理

应支持对自助材料存取设备信息进行管理；对使用自助材料存取设备的人员进行权限分配；还可以根据业务要求，记录存取的状态。需包括存取设备配置、人员权限配置、存取柜配置、取件通知管理。

2.3.1.3 政务服务业务应用系统

需基于南通市市县一体化在线政务服务平台进行建设。

2.3.1.3.1 统一制证中心

构建集“AI 审批、电子证照、实体制证”于一体的智能化制证中枢，包括自助申报材料审查、证照或批文自助打印、自助出柜。

2.3.1.3.2 跨区域通办

采用页面跳转模式实现事项的异地办理。各个区域平台把本地区的接入地址发布的长三角一体化平台上，启东市只需要把其他区域的平台链接接入到本区域的平台上，根据长三角一体化平台提供的地区切换地址，将业务功能信息接入到启东市自助服务终端系统中。办事群众通过自助服务终端设备上进行跨区域通办，点击地区切换按钮，页面操作会自动跳转到某地区平台上，办事群众可以在异地平台上进行事项办理。同时，各个区域通过长三角一体化平台共享用户登录信息，避免用户二次登录。

2.3.1.3.3 高效化日常事务管理

1、中心人员管理

（1）人员信息管理

中心人员可对个人信息进行维护，包括个人资料，如办公电话、手机号码、消息配置、密码修改模块。

（2）部门信息管理

部门管理员可以配置部门信息，包括部门名称、中心部门名信息。

（3）配置部门人员

部门信息完善后，可对部门管理中配置人员，可从中心人员清单中拉取，并根据实际情况配置人员权限、考勤时间信息。

2、中心人员考勤管理

主要对工作人员进行日常考勤管理。

（1）考勤统计

系统提供考勤统计功能，对工作人员所有考勤情况进行统计，并生成相应的系统报表，包括：每日考勤表、考勤统计月总表和考勤统计年总表，表单中包含部门、姓名、日期、应到天数、迟到天数、旷工天数、早退天数字段来统计大厅的整体考勤情况。需包括每日考勤表、考勤统计月总表、考勤统计年总表。

（2）考勤规则配置

实现考勤规则设置，对中心人员考勤内容要求进行配置管理，需包括考勤时间、考勤周期、上下班考勤时间点内容及规则。

（3）工作日设置

管理人员可以根据常规的工作日程安排或临时任务对工作日进行配置。可以配置基础日历、轮班以及上班时间，也可以根据季节变化调整更改工作时间，以便对日常工作考勤进行适当的安排。

3、中心人员请假管理

主要实现对中心工作人员的各类请销假管理，包括请假的申请、审批、查看、核销。

4、窗口人员智能监控管理

通过与审批系统的对接、与考勤系统的对接、与排队叫号系统的对接，实时

动态监管大厅所有窗口状态信息，状态包括未登录、空闲、正在办理、暂停办理、考勤异常。

5、中心人员绩效管理

（1）指标配置

绩效考核指标是指通过明确绩效考核目标，对承担中心服务过程及结果，各窗口人员完成指定任务的服务价值创造的判断过程。实现考评指标配置，对窗口绩效考评维护，需包括考评方式、扣分项及分值、考评内容及考评规则指标。

（2）绩效考核

对窗口人员进行绩效考评。实现在线考评流程管理，。实现窗口人员考评情况的查询，查看评分原因及评分分数情况，查询窗口人员月度考评分值、年度考评分值及评分汇总情况。监察室人员在巡检时，发现工作人员的违规行为，可进行手动扣分。

（3）申诉处理

系统应提供考核结果申诉功能，主要针对窗口工作人员对考核扣分有异议的，可以在规定的时限内进行在线申诉，陈述申诉理由，申诉申请提交后由政务服务管理机构人员进行查证。不是由于窗口工作人员的误操作而造成扣分的，可将相应扣分加回。

（4）绩效统计

系统统计内容主要需包括考核数据统计，包括：年/季度不同维度满意度测评数据展示。

（5）个人绩效情况

系统通过个人绩效情况对中心人员展示绩效分数，方便中心人员对绩效做出针对性的整改，提升个人服务质量。

6、中心资产管理系统

资产管理系统为用户提供一个易用的资产管理功能，实现了对资产采购及使用情况的查看及电子化管理功能，其包括了资产的分类、入库、申请、审批、出货及相关的查询统计功能。资产管理系统的建成，提高了用户对资产情况的了解，避免资产使用时产生的各种问题及矛盾，提高工作效率和资产使用率。

（1）资产管理

需包括入库登记、发放登记、维修管理、报废管理。

（2）资产列表

需包括个人资产列表、部门资产列表。

（3）资产申领

● 资产申领

用户填写《申领表单》，直接选取需要领取的物品。

● 我的资产申领

中心人员可在系统中关注到以申购资产的状态。

（4）资产统计

需包括库存汇总、入库统计、出库统计。

在实际使用过程中完成对应的升级优化。

2.3.2 数字驾驶舱

需基于南通市市县一体化在线政务服务平台进行建设。

2.3.2.1 数字驾驶舱应用场景

2.3.2.1.1 一网通办主题

一网通办主题依托政务服务中心和各部门资源，通过对海量数据的整合、关联、挖掘、分析，以总体态势、企业服务、便民服务为切入点，从政务事项、业务办理、服务渠道、服务对象、成效分析维度分析政务服务总体运行态势，同时针对企业和个人以全生命周期为切入点，分析当前群众办事的痛点堵点，及群众目前所关注的热门事项，便于及时掌握群众办事情况并发布对应的政策优化群众办事体验。

通过对政务数据的挖掘、关联、分析，形成对应的可视化分析页面，为政务服务运行管理提供更科学的监测分析和预警决策能力，更高水平的智能化执行能力，不断推动政务服务建设的持续优化和改进，提升群众幸福感。

1、政务服务一张图

以“1+2”模式设计一网通办主题。首先，从总体态势上，围绕政务服务运行态势、今日政务、成效分析进行分析展示，展示启东市政务服务整体情况。其次，从用户角度出发，分企业服务与便民服务两个角度，以全生命周期视角，关注各阶段事项办理的便捷度，围绕政务服务工作重点和政务服务创新特色，抓重

点、找亮点，不断帮助政府及时发现政务服务业务中存在的问题，推动实现政务服务全流程闭环管理模式。

2、总体态势

从运行态势、地图服务、成效分析三块内容整体展示启东市政务服务运行情况。

（1）运行态势

从服务事项、业务办理、服务渠道、服务对象四方面宏观展示启东市政务服务整体情况。

（2）地图服务

结合GIS地图进行数据展示，需包括今日政务和渠道建设两大情况。

● 今日政务

在GIS地图上，以浮动窗口展示今日受理情况，需包括申报数、受理量、办结量、满意度情况，展示当日实时服务情况。

● 渠道建设

在GIS地图上展示线下各服务渠道的实时运行情况，综合大厅、专厅和便民服务中心主要展示基本信息、进驻情况、窗口设置、服务人员、今日业务量趋势、近一年业务量趋势情况，自助终端主要展示自助终端数量、社区/单位、地址、可办事项以及常用功能使用情况。

（3）成效分析

从政务服务能力评估、满意度分析、创新服务改革分析三个维度来综合展示政务服务所获取的成效。

3、企业服务

（1）企业全生命周期服务

从企业全生命周期的角度入手，分析企业各生命阶段中，企业的办件情况。同时，基于办件量分析热门办理事项的TOP5的行业信息、创新服务办件情况，基于各阶段业务量变化趋势，了解企业在不同阶段的诉求；分析企业不同阶段办事重点，为企业主题服务改革提供有力抓手。

（2）地图服务

根据各阶段办件情况展示办件企业地图分布情况。

（3）成效分析

从满意度分析、创新服务事项展示企业服务各生命周期的服务能力及服务情况，同时从企业开办、项目审批、不动产登记三个重点服务改革展现整体服务能力。

4、便民服务

从个人全生命周期、地图服务、成效分析三个维度展示自然人整体服务情况。

（1）个人全生命周期服务

结合个人全生命周期服务，分析出生、入学、就业不同阶段，查看各阶段的服务事项、服务能力信息，方便领导进行横向比对，发现自然人在哪个阶段需求较多、办事最“堵”。

（2）地图服务

- 办件热点

根据各阶段自然人办件量情况在地图上通过颜色进行热力展示，分析哪个区域的办件量比较多。

- 咨询热点

基于GIS地图展示各区域的咨询情况，分析各区域的自然人办事需求情况。

- 投诉热点

基于GIS地图展示各区域的投诉情况，分析各区域自然人的办事堵点情况。

- 区划统计

基于GIS地图展示各区划，用列表展示人口总数、月度自然人申办量、月度咨询量、月度投诉量信息，查看该区划的基本服务情况。

- 月度热点事项

通过列表展示各阶段自然人的办事热点，及时了解民生热点需求。

（3）成效分析

从满意度分析、创新服务事项展示便民服务各生命周期的服务能力及服务情况。

5、算法模型

（1）政务热点挖掘模型

通过从政策文件中分析政策热点以及根据办件数据统计分析市民关注的焦

点问题，挖掘当下的政务热点，也辅助领导感知当下的热点动向。

（2）好差评评价内容挖掘分析模型

结合评价内容的特点，充分应用大数据、自然语言处理技术，通过语义分析挖掘出好差评的典型标签，从而进行标签管理。根据好差评的标签特性，分析总结出不同部门、事项、大厅的办事成效，定位市民关注的热点问题，挖掘出好差评的潜在价值，为业务优化提供指导依据，辅助决策，进一步提升管理能力。

（3）办件趋势预测分析模型

根据政务大厅的历史办件量数据，建立预测模型，预测未来一段时间内的办件量，为领导及相关部门提供参考，做出相应决策，合理配置资源。同时根据预测误差分析原因，生成政策影响、社会事件重要事件的预警线索，推送给领导及时决策分析。

2.3.2.1.2 营商环境主题

营商环境专题从整体营商环境评估为切入点，围绕商事主体画像、法人办事情况及中小微企业扶持三个方面，挖掘地区整体营商环境的突出问题、明确地区商事主体的类型及行业分布、找到法人办件的待优化方向。

依托营商环境分析评估结果的实时监测情况，并通过展现地区核心产业、企业办件难点，明确当前地区在发展过程中的瓶颈，能够辅助领导及有关部门，掌握优化轨迹，精准发力，建设营商环境最优区，为企业发展提供便利。

1、营商环境一张图

（1）营商环境评估

营商环境评估主要围绕总体得分情况、地图服务、得分地区对比三个维度来进行展现。

（2）商事主体画像

商事主体服务主要围绕类型分布、行业分布、注册资本三个角度进行展现。

（3）法人办事分析

法人办事分析围绕与企业相关的政务服务情况及优化提升两个维度来对法人办事情况进行展现。

2、企业开办场景

从政务服务角度，分析企业开办整个生命周期的事项办理便捷度、办理时效。

发现企业开办服务改革的成效与不足，为部门监督管控及优化企业开办服务提供辅助依据。

3、工程建设项目审批场景

针对工程项目建设全过程审批“部门多、环节多、要求多、时间长”的问题，从工程建设项目审批角度，跟踪工程建设项目全链审批流程，发现流程中的异常项目、超时项目，分析流程节点、提高项目审批流程的效率。

4、不动产登记场景

深入贯彻落实国务院“放管服”改革要求，以推进不动产登记工作提质增效为目标。通过对不动产登记的办理环节、时间、材料、成本四个方面的分析评估，为分类压缩不动产登记办理时限、环节，有序减少不动产登记申请材料，有效降低办事成本提供辅助依据，从而优化不动产登记办理服务，提升服务效率和水准。

2.3.2.2 驾驶舱控制台

2.3.2.2.1 我的主题应用

1、查询主题应用

默认查询自己新增的所有主题应用以图片列表形式展示。应支持按应用名称、创建时间、应用类型、当前状态条件查询。

2、新增主题应用

应支持新增主题应用，输入内容需包括应用名称、应用类型、应用标签、应用图片、使用场景、使用对象、应用需求描述、附件上传、需求登记人、联系电话、所属部门、需求提出让、联系电话、所属部门、要求完成时间。

3、修改主题应用

应支持对草稿、退回状态下的主题应用进行修改。

4、删除主题应用

应支持对草稿、退回状态下的主题应用进行删除。

2.3.2.2.2 主题应用管理

1、查询主题应用

默认查询除草稿之外所有状态下的主题应用以图片列表形式展示。应支持按应用名称、创建时间、应用类型、应用标签、当前状态、需求登记人、需求提出人条件查询。

2、主题应用需求分析

对新增主题应用进行需求分析，具体操作可以退回，也可以反馈需求分析结果送下一步。退回输入内容包括：退回意见。反馈需求分析结果输入内容包括：应用分析结果、附件上传、需求分析人、联系电话、所属部门。

3、主题应用需求确认

需求审核人员根据提交的需求分析结果进行确认，具体操作可以退回，也可以审核通过送下一步。需包括主题应用需求开发、主题应用工单派发、主题应用工单接收、主题应用工单反馈、主题应用工单验收、主题应用成果反馈、主题应用成果验收、主题应用成果发布、可视化布局设计。

4、应用资产管理

需包括查询应用资产、发布应用资产。

2.3.2.2.3 配置管理

1、专班配置

可以进行设置数字驾驶舱转班配置，专班与部门进行绑定，选择一个或者多个业务部门人员组成转班人员并且从组织架构通同步联系方式,如果没有联系必须要手动录入联系方式。

2、PC 大屏驾驶舱管理

（1）栏目管理

配置 PC 大屏驾驶舱展示的栏目并且绑定给专班，可以对栏目的排序进行控制，栏目必须绑定给专班进行管理，所属专班可以有栏目的管理权限。可对栏目下的版块进行排序并且进行添加删除修改。一个栏目下必须配置一个版块否则此栏目无效。栏目下默认展示排序最小的版块作为首页。

（2）版块管理

配置 PC 大屏驾驶舱展示的版块，在分析应用开发完成后将地址注册到新建的驾驶舱版块中，并且大屏端页面地址与中屏端页面地址，前端根据识别的分辨率来跳转不同的页面地址。

3、移动驾驶舱管理

（1）栏目管理

栏目管理用于对移动驾驶舱首页元素的动态管理,如部门直通车、预警雷达，

应支持对栏目的新增、修改、删除、排序功能，新增栏目时包含栏目名称（必填）、栏目图标、栏目跳转地址、栏目排序、栏目描述字段。

（2）版块管理

基于栏目显示栏目下的版块，版块信息包括版块名称、版块类型、版块图标、排序号、版块 url、板块描述字段，版块可进行角色授权。

（3）卡片管理

点击卡片配置按钮可以选择相应领域内的指标进行关联，并且支持对选择后的指标排序。支持业务权属的配置，包含责任部门（必填）、责任人（必填）、分管领导（必填）、专班（必填）字段，其中专班可以从专班配置管理进行选择。

2.3.2.2.4 智库信息发布

需实现富文本信息的编辑发布，可以针对标题、发布时间、发布人、发布内容、附件进行编辑，发布内容中可以添加图片，但是不能添加表格。

2.3.2.2.5 指标管理

1、指标集管理

可以对已配置完成的指标根据业务域进行划分，将同一业务域的指标配置到同一指标集中，以便后续与业务专题场景进行绑定使用，业务专题场景只可以调用指标集范畴以内的指标或者是配置的额外指标。

2、指标属性管理

指标属性管理用于对各专题领域的指标进行梳理定义以及数据属性的配置，指标定义后可以进行数据预览，如是预警指标提供预警规则配置的快捷入口。

3、预警管理

需包括预警配置、预警处置。

4、指标库查询

以部门与业务（指标集）维度展现系统中存在的指标内容，各部门可以通过指标库查询实现指标检索，可以线上申请查看利用指标，指标归属部门审核通过后可以进行查看并且通过指标接口进行调用。

5、指标任务管理

应支持对指标任务定时类型进行配置，配置完成之后按照设定时间定时执行任务。

2.3.2.2.6 问题反馈管理

可以对指标异常、驾驶舱问题进行快捷反馈，指标异常在反馈是可以附带指标标题、描述、代码信息方便后台进行快速查找定位。后台运维人员在收到问题后可以进行快速反馈或者转主题应用需求进行深度分析处理。

2.3.2.2.7 日志统计

1、日志管理

用户日志管理，应支持日记的搜索查询。 支持按用户、时间段、专题属性进行搜索查询。

2、统计看板

应提供运营相关的数据看板，如用户访问量、日活、月活数据，每个专题的访问数据、卡片的访问数据，为运营分析提供数据支撑。

2.3.2.2.8 数据服务

需提供数据服务，包括 API 市场、API 管理、权限与安全和运行监控。

2.3.3 数据交换、系统对接与整合

应采用统一的接口标准规范，与之对接的各平台在交换数据时须符合接口规范的要求。

2.3.3.1 与排队叫号系统对接

需与现有政务服务网排队叫号系统对接，实现排队取号预约功能。

2.3.3.2 与启东市短信网关的对接

需与启东市运营商短信网关对接，系统调用短信网关，实现收发短信。

2.3.3.3 与江苏省政务服务网对接

需与江苏省政务服务网对接，优化启东市政务服务网，构建智能客服、企业服务、老年人服务。

2.3.3.4 与南通市市县一体化在线政务服务平台对接

需与南通市市县一体化在线政务服务平台对接，构建启东市特色业务应用系统，实现数据汇聚共享。

2.3.3.5 与启东市数据共享交换平台对接

需与启东市数据共享交换平台对接，实现企业/个人、办件数据共享交互。

2.3.3.6 基础中间库

系统需建立一个基础中间库，业务系统将相关需要发布的信息推送至中间库，本系统从中间库统一获取中心现场需要发布的信息内容，经审核通过后，自动发布到对应的显示屏上。

2.3.3.7 与审批系统对接

需提供与审批系统对接接口，与审批系统进行对接，实现对审批事项相关信息的采集、分类、整合、交换、发布及推送操作。

2.3.3.8 统一数据共享接口

需建设“一业一证”服务系统统一数据接口，对于平台受理的“一业一证”办件数据，通过统一接口方式提供各部门自建系统获取办件材料数据，实现“一业一证”服务系统与部门自建系统的数据交换。

2.3.3.9 与智能化硬件设备对接

需通过 API 接口，实现对智能化硬件设备基础资源数据的分类推送。以 API 的方式同步获取相关硬件信息，提供相关硬件设备的远程控制功能。

2.3.3.10 与现有一件事系统对接

需与启东市现有一件事系统对接，在平台增设一件事模块，点击后跳转至现有一件事系统中进行后续操作。

2.3.3.11 系统接口扩展

本次系统的计算机网络需基于中心现有网络实现和 INTERNET 及其他内部网络相连接，采用有线或无线网络传输，实现项目信息智能化管理等多项功能。

第 三 章 系统建设方案

3.1 适配改造方案

4.2.1 代码改造

启东市新产业服务中心信息系统国产化改造中，代码改造部分包括将多个关键系统和功能迁移部署到国产化服务器并进行适配。依赖库替换：替换国外开源组件（如 Log4j、Jackson）为国产或可控版本（如 Logback、Fastjson），审查许可证合规性。

数据库适配：调整 SQL 语法（如分页查询从 ROWNUM 改为 LIMIT）、修改 JDBC 驱动，兼容达梦、人大金仓等国产数据库。

国密算法集成：替换加密算法（如 SHA-256→SM3）。

硬编码优化：修正路径分隔符（\→/）、移除对国外 API（如 Google 服务）的硬编码依赖。

中间件兼容：调整连接池、缓存等配置

4.2.2 数据库改造

重新规划数据库表结构，包括分片设计、分布设计以及对象优化调整，以确保数据存储和分布的合理性。处理语法和函数差异、以及数据类型、精度、长度、字符集，需要进行相应的转换和适配。对数据库和 SQL 进行性能优化，包括驱动层、网络层、代理层、节点层。将原有系统中的数据迁移到新的国产化环境中，确保数据的完整性和一致性。数据库进行主从备份。

1、数据库结构规划

分片设计 ：将大型数据库中的表按照一定的分片规则（如按业务区域、时间范围等)分割成多个较小的数据分片,每个分片存储在不同的服务器或节点上。

对象优化调整 ：对数据库中的表、索引、视图、存储过程等对象进行优化调整。包括合理设计表结构，减少数据冗余；创建合适的索引以提高查询速度；优化视图和存储过程，避免不必要的复杂计算和数据传输等，以确保数据存储和分布的合理性，提升数据库的整体性能。

2、数据库适配与转换

语法和函数差异处理：不同数据库系统之间存在语法和函数的差异，如 MySQL 和国产数据库达梦（DM）在 SQL 语法和内置函数方面有所不同。需要对原有的 SQL 语句和应用程序代码进行检查和修改,将不符合国产数据库语法的部分进行转换和适配。例如，将 MySQL 中的“LIMIT”子句转换为 DM 中的“TOP”子句来实现查询结果的限制。

数据类型转换：不同数据库对数据类型的定义和存储方式可能不同。在数据迁移过程中，需要对数据类型进行转换，以确保数据在国产数据库中能够正确存储和处理。例如，将 Oracle 数据库中的“NUMBER”类型转换为 DM 数据库中的“INT”或“DECIMAL”类型，同时要考虑到数据的精度和范围要求，避免数据丢失或溢出。

精度、长度和字符集调整 ：对数据的精度、长度进行检查和调整，以满足国产数据库的要求。例如，对于小数类型的数据，要确保其精度（即小数位数）

符合业务需求且不超过数据库支持的最大精度；对于字符串类型的数据，要合理设置长度，避免过长或过短。同时，统一字符集设置，如将原有数据库的字符集从“GBK”转换为国产数据库支持的“UTF－8”字符集，确保字符数据的正确存储和显示，避免乱码问题。

3、数据库性能优化

驱动层优化：选择与国产数据库兼容且性能优良的数据库驱动程序，并对其进行参数配置和优化。例如，调整连接池的大小、超时时间等参数，以提高数据库连接的效率和稳定性，减少因数据库连接问题导致的性能瓶颈。

网络层优化：优化数据库服务器与应用服务器之间的网络连接，包括增加网络带宽、减少网络延迟、配置合适的网络协议等。同时，可以采用数据压缩技术，减少数据在网络传输过程中的流量，提高数据传输速度。例如，在分布式数据库环境中，通过优化网络配置，确保各个节点之间的数据同步和通信高效稳定。

代理层优化：如果使用了数据库代理（如读写分离代理、分片代理等），对代理层进行优化配置。如合理设置读写分离策略，将读操作分散到多个从节点，减轻主节点的负载；优化分片代理的路由算法，提高数据分片查询的效率和准确性。

节点层优化：在数据库服务器节点层面，进行硬件资源的合理分配和优化，如增加内存、优化磁盘 I/O 性能等。同时，对数据库的配置参数进行调整，如缓存大小、日志文件配置等，以提高数据库的读写性能和并发处理能力。例如，根据数据库的实际负载情况，调整数据库的缓冲池大小，增加内存缓存，减少磁盘 I/O 操作，从而提升查询性能。

4、数据迁移与备份

数据迁移：制定详细的数据迁移方案，包括数据备份、数据抽取、数据转换、数据加载等步骤。在迁移过程中，采用专业的数据迁移工具（如国产数据库提供的数据迁移工具）或自研的迁移脚本，确保数据从原有系统准确无误地迁移到新的国产化数据库环境中。同时，对迁移后的数据进行完整性校验，通过比对源数据和目标数据的关键字段、记录条数、数据和等，确保数据的完整性。例如，在迁移一个大型企业的财务数据库时，要严格按照迁移方案执行，确保财务数据的准确性和完整性，避免因数据迁移错误导致财务核算问题。

主从备份：搭建数据库的主从备份架构，在主数据库上配置从数据库，实现

数据的实时同步或定期同步。当主数据库出现故障时，从数据库可以迅速接管，保证业务的连续性。同时，定期对备份数据进行测试和恢复演练，确保备份数据的有效性和可用性。例如，采用国产数据库的主从复制功能，将主数据库的数据实时同步到从数据库，在发生故障切换时，从数据库能够在短时间内完成角色转换，继续为应用系统提供数据服务。

4.2.3 国产化部署

国产化容器部署将应用及其依赖打包成独立的容器镜像，实现应用的快速部署和迁移。针对重点应用，部署集群，部署消息中间件，如 RabbitMQ、Kafka 的国产化版本，用于实现系统间的异步通信和消息传递。部署预览等组件的国产化版本，实现文件预览等功能。

1、应用容器化与快速部署迁移

应用及依赖打包：将应用程序及其所有依赖（包括运行时环境、库文件、配置文件等）整合到一个独立的容器镜像中。这种打包方式确保应用在一个完整的、自包含的环境中运行，避免因环境差异导致的兼容性问题。

快速部署：通过容器编排工具（如国产化的 Kubernetes 发行版），能够快速在服务器上创建、启动容器实例。当需要部署应用时，只需将镜像拉取到目标服务器并运行，容器引擎会根据镜像内容迅速搭建起完整运行环境，相比传统部署方式大大缩短部署时间。比如在一个拥有多个节点的集群中，几分钟内就可以部署数十个应用实例。

便捷迁移：由于容器镜像的标准化和环境隔离性，使得应用迁移变得轻松。无论是迁移到不同的物理机、虚拟机还是云服务器上，只要目标系统安装了容器运行时（如国产的容器运行时软件），就可以直接运行镜像而无需额外的环境配置工作，保障应用在不同基础设施之间的平滑迁移。

2、重点应用集群部署

高可用集群构建：对于关键应用，采用集群部署方式。通过在多台服务器上启动多个相同的容器实例，形成一个应用集群。容器编排系统负责管理这些实例的生命周期，当某个实例出现故障时，能自动重启或在其他正常节点上重新创建实例，确保应用的持续可用性。例如，一个电商网站的订单服务部署为集群，某一容器实例因硬件故障不可用时，其他实例可继续处理订单请求。

负载均衡：在集群中，配套的负载均衡器（可使用国产的负载均衡软件或插

件）会将进入的请求合理分配到各个容器实例上。根据预设的策略（如轮询、最少连接数等），使各实例的负载保持均衡，提高整体性能和资源利用率。以一个高并发的新闻资讯应用为例，负载均衡器能有效分发大量用户访问请求到不同实例，避免单点过载。

3、消息中间件国产化部署及应用

RabbitMQ 国产化版部署与功能：在国产服务器操作系统上安装经过适配优化的 RabbitMQ 国产化版本。通过容器化部署，可方便地进行版本管理、横向扩展等操作。例如，在金融行业的交易系统中，利用容器快速部署多个 RabbitMQ 国产化实例组成集群。

功能：实现系统间的异步通信，如在订单处理系统中，当用户下单后，前端应用将订单信息发送到 RabbitMQ 消息队列，后端的库存扣减、支付处理等服务异步消费消息进行相应操作，提高系统响应速度和可靠性；支持多种消息协议，方便与不同的应用系统集成。

4、Kafka 国产化版部署与功能 ：

部署 ：基于国产化的容器平台，在大规模数据处理场景下部署 Kafka 国产化集群。通过调整容器资源参数（如 CPU、内存限制）来适应高吞吐量的数据处理需求。例如，在电信运营商的日志收集分析系统中，部署多节点 Kafka 国产化集群。

功能 ：用于处理大量实时数据流的异步传递，如在物联网数据采集平台中，大量设备产生的数据通过 Kafka 消息队列进行缓冲和传输，下游的数据处理应用（如数据分析、存储系统）按需消费消息；具备高可扩展性和容错性，能应对节点故障等异常情况，保障消息的可靠传输和持久化存储。

5、国产化预览组件部署及应用

文件预览功能实现 ：部署国产化的文件预览组件容器镜像，该组件支持多种常见文件格式（如 PDF、Office 文档、图片等）的在线预览。当用户在应用系统（如政务服务网、企业办公系统）中请求预览文档时，前端应用调用预览组件提供的接口，组件在服务器端快速生成预览所需的轻量级文件（如缩略图、HTML5 渲染页面等）并返回给客户端展示。例如，在线政务办事系统中，用户提交的各类申请材料（如身份证扫描件 PDF、申请表 Word 文档）可通过预览组件直接在浏览器中查看，无需下载安装额外的软件。

高效集成与性能优化：国产化预览组件与国产操作系统、浏览器等进行深度适配和优化，确保在国产化技术栈中稳定运行且预览速度快、资源占用低。其容器化部署方式便于与各类应用系统集成，通过简单的 API 调用或配置即可实现文件预览功能的嵌入，降低开发成本和集成难度。

4.2.4 对接联调

启东市新产业服务中心信息系统原对接内容：排队叫号系统、南通市CA电子印章、启东市短信网关、第三方支付平台和银行、江苏省政务服务网、南通市市县一体化在线政务服务平台、启东市数据共享交换平台、部门业务系统、基础中间库、审批系统、统一数据共享接口、智能化硬件设备、新大厅采购的智能化硬件设备、现有一件事系统、系统接口扩展对接联调。

公共资源交易电子档案管理平台对接内容：与公共资源电子交易系统对接、与第三方业务系统对接、与档案馆对接、电子交易系统、限额以下交易平台对接联调。

3.2 数据处理和存储方案

历史数据同步至国产化数据库，后续系统产生的数据统一存储至国产化数据局。

1、数据处理方案

数据采集与集成：通过数据交换平台，采用多种方式如数据库表、Web Service、文件等，将历史数据进行迁移和整合，实现数据共享。同时，利用ETL工具对采集到的数据进行清洗、转换、加载，统一数据格式和编码规则，确保数据的一致性和准确性。

数据开放与共享：在保障数据安全的前提下，通过数据开放平台，以接口调用等方式，将经过脱敏和授权的政务数据向社会开放，促进数据的流通和创新应用。

2、数据存储方案

集中存储与分布式存储相结合：对于结构化数据，如政务事项办理过程中的业务数据、电子证照库等，采用国产的集中式关系型数据库进行存储，确保数据的完整性和事务处理能力。对于非结构化数据，如文档、图片、音视频等，则采用国产的分布式文件存储或对象存储系统，利用其高扩展性和存储成本低的特点，满足海量非结构化数据的存储需求。

块存储与文件存储的融合：在一些对存储性能和可靠性要求较高的场景下，如政务云平台的虚拟化资源存储、关键业务系统的数据存储等，采用国产的块存储技术，提供高性能、低延迟的存储服务。同时，结合文件存储系统，方便用户进行文件的共享和访问，满足不同应用场景下的存储需求。

数据备份与容灾：建立完善的数据备份机制，采用国产的备份软件和硬件设备，对重要数据进行定期备份，备份策略包括全备份、增量备份、差异备份等。

3.3 系统部署方案

整合后资源需求统计																
序号	系统名称	子系统名称	部署位置	服务器			存储设备		操作系统		数据库		中间件		其他支撑软件	
				服务器用途	配置	数量	品牌型号	数量	品牌型号	数量	品牌型号	数量	品牌型号	数量	品牌型号	数量
1	启东市新产业服务中心信息系统	启东市新产业服务中心信息系统	政务云	应用服务器/中间件服务器	CPU8 核/内存 16G/存储 200GB	16	NFS	1	银河麒麟 Kylinv10arm	25	达梦	4	tomcat	10	nginx	1
				应用服务器	CPU16 核/内存 32G/存储 300GB	4							RabbitMQ	1		
				附件库服务器	CPU4 核/内存 8G/存储 1000GB	1							redis	1		
				数据库服务器	CPU8 核/内存 32G/存储 500GB	1										
				数据库服务器	CPU16 核/内存 32G/存储 500GB	3										

第 四 章 系统安全设计

4.1 网络安全总体结构和逻辑结构

本次启东市新产业服务中心信息系统信创改造项目依托现有南通市信创云提供的安全环境、安全资源达到等保要求。

本项目网络信息安全主要是指保护系统，使其没有危险、不受威胁、不出事故。从技术角度来说，系统网络信息安全的目标主要表现在系统的可靠性、可用性、机密性、完整性等方面。

可靠性是本系统安全的最基本要求之一，是本系统的建设和运行目标。本项目在设计、开发中采用现代微服务架构、RESTful API 技术和容器化技术，综合运用新一代云计算、大数据分析技术，以保障系统稳定。

可用性是本系统面向用户的安全性能，用户的需求是随机的、多方面的、有时还有时间要求,本系统规划设计的功能贴近实际应用需要,符合用户操作习惯,提高用户数据收集、处理、分析、应用效率，保证大多数的用户可以较好地使用系统。用户在对系统进行操作时，由于各种原因会进行误操作，或者输入错误的数据等，系统对这些情况进行处理，保证个别模块出现问题不会对其他模块造成影响。

机密性是本系统信息不被泄露给非授权的用户，信息只为授权用户使用。本系统采用完整的用户认证体系及登录认证保护措施,确保了系统信息只被授权用户进行访问，并设置了完整的权限控制体系，确保用户只能够接触权限范围内的系统信息。本系统采用网络数据传输方法、通信终端和计算机可读存储介质技术，通过数据加密、解密技术和重要性标识保证网络数据传输过程中的安全性。

完整性是本系统信息在存储或传输过程中保持不被偶然或蓄意地删除、修改、伪造、乱序、重放、插入等破坏和丢失的特性。完整性是一种面向信息的安全性，它要求保持信息的原样，即信息的正确生成和正确存储和传输。

4.2 密码应用方案

项目建设的系统部署在信创云,具备完备的安全防护方案,如网络安全设计、主机安全设计、应用安全设计等。

4.2.1 计算平台密码应用方案

4.2.1.1 物理和环境安全

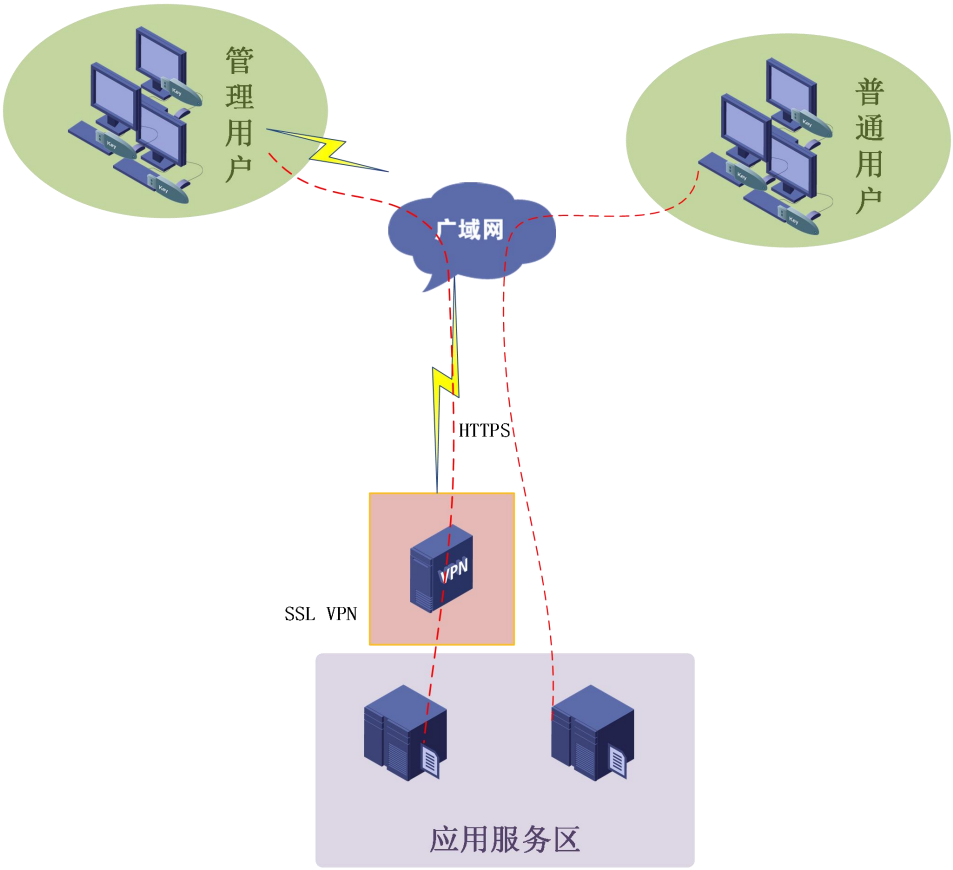
本系统部署在南通市信创云机房，该机房物理和环境安全由机房运营单位统一负责。目前，该机房使用电子门禁控制系统对人员进出进行管理，门禁权限只开放对应的运维人员，进出机房须进行登记发起流程审批，审批通过后由机房管理人员陪同才能进入机房区域。部署在机房出入口的门禁系统能控制(人脸识别)、鉴别和记录进入的人员身份，门禁系统运行正常。同时机房出入口及重要部位已部署了视频监控系统记录人员进出情况，视频监控室配备 24 小时专人值守，可有效降低未使用国密算法对物理环境进行有效防控的风险，保障物理机房的访问控制安全。

4.2.1.2 网络和通信安全

1、通信身份鉴别

外部用户访问系统时，须使用 SSL VPN 客户端通过身份鉴别后与应用平台边界设备 SSL VPN 建立加密隧道，与业务系统区所在网络服务区建立访问通道。SSL VPN 即指采用 SSL 协议来实现远程接入的一种 VPN 技术，用以提供端对端加密和验证服务。

SSL 提供了两种安全机制：认证和加密。认证机制使 IP 通信的数据接收方能够确认数据发送方的真实身份以及数据在传输过程中是否遭篡改。加密机制通过对数据进行加密运算来保证数据的机密性，以防数据在传输过程中被窃听。示意图如下：



安全通道示意图

本方案设计在本系统服务端部署使用国密算法的 SSL 站点证书，建立 Https 连接，通过此措施降低重要数据在传输过程中被窃取和篡改的风险。

2、信息完整性保护服务

信息完整性是指确保系统中用户信息的完整和真实可信。保证信息完整的主要措施是采用强有力的访问控制技术，防止对系统的数据越权删除、更改、复制和破坏。此外，还防止意外损坏与丢失。任何对系统信息有特性或状态的中断、窃取、篡改和伪造都是破坏系统信息完整性的行为。其中中断是指在某一时间段内因系统的软件、硬件故障或恶意破坏删除造成系统信息的受损、丢失或不可利用；窃取是指系统的信息被未经授权的访问者获取，造成信息不应有的泄露，使信息的价值受到损失或者失去存在的意义；篡改是指故意更改正确的数据，破坏了数据的真实性状态；伪造是指恶意的未经授权者故意在系统信息中添加假信息，造成真假信息难辨，破坏了信息的可信性。为保障信息数据在传输过程中的完整性，设计以下方式对网络信息数据做完整性保护：

（1）使用 SSL VPN 和 Https 协议建立安全传输通道；

（2）传输数据的双方都总希望确认消息未在传输的过程中被修改。加密使得第三方想要读取数据十分困难，然而第三方仍然能采取可行的方法在传输的过程中修改数据。此时，对所传输的数据信息数据签名就尤为重要了。数字签名有两种功效：一是能确定消息确实是由发送方签名并发出来的，因为别人假冒不了发送方的签名。二是数字签名能确定消息的完整性。因为数字签名的特点是它代表了文件的特征，文件如果发生改变，数字摘要的值也将发生变化。不同的文件将得到不同的数字摘要。一次数字签名涉及到一个哈希函数、接收者的证书或公钥、发送方的私钥。

3、信息机密性保护

对信息进行机密性保护有两种方法：

（1）基于访问控制，只有授权实体才能访问信息；

（2）任何实体可以访问表示信息的数据，但是，只有授权拥有某些机密信息的实体才能读懂这种数据。

本方案中设计通过在本系统服务端前部署 SSL VPN，当系统管理人员对业务系统进行管理时，登录 SSL VPN，建立安全管理通道，通过对数据进行加密运算来保证数据的机密性，以防数据在传输过程中被窃听。

此外，针对普通用户，使用 Https 协议访问 Web 服务，通过数字证书、加密算法、非对称密钥等技术完成互联网数据传输加密，实现网络传输安全保护。保证数据内容在传输的过程中不会被第三方查看。

4.2.1.3 设备和计算安全

本系统部署在信创云机房，由信创云运营单位提供运行业务系统所需相关设备，其运营管理由信创云运营单位统一管理，不在本次建设范围内。

4.2.2 密码应用设计目标及原则

4.2.2.1 密码服务机构

由南通市信创云密码资源池提供统一密码服务。

4.2.2.2 接入方式

对接南通市信创云密码资源池，开放统一密码服务接口进行系统对接。

4.2.2.3 接口和功能遵循标准

接口和功能遵循标准一览表

接口及功能类型	密码应用场景	可遵循的标准
接口调用	密码支撑平台通过接口提供密码功能,业务应用通过接口调用密码功能	GB/T38629　信息安全技术签名验签服务器技术规范
		GM/T 0019　通用密码服务接口规范
		GM/T 0020　证书应用综合服务接口规范
		GM/T 0067　基于数字证书的身份鉴别接口规范
实体鉴别	应用系统调用密码功能，按照标准实现身份鉴别协议	GB/T 15843(所有部分)　信息技术 安全技术 实体鉴别
		GB/T 38556　信息安全技术 动态口令密码应用技术规范
		GM/T 0067　基于数字证书的身份鉴别接口规范
		GM/T 0069　开放的身份鉴别框架
		GM/T 0113　在线快捷身份鉴别协议
加解密、签名、验签和完整性计算	应用系统调用密码功能，按照标准对数据加密、解密、签名、验签、计算消息鉴别码	GB/T15852(所有部分) 信息技术 安全技术 消息鉴别码
		GB/T 17964　信息安全技术 分组密码算法的工作模式
		GB/T 35276　信息安全技术　SM2 密码算法使用规范
基础标准	应用系统调用密码功能时，指名算法和用法	GB/T 33560　信息安全技术　密码应用标识规范
	应用系统管理用户实体时，关联用户的数字证书	GB/T 20518　信息安全技术　公钥基础设施　数字证书格式
	应用系统对数据加密或签名时，对数据进行封装	GB/T 35275　信息安全技术　SM2 密码算法加密签名消息语法规范

4.2.2.4 密码支撑方式

对接南通市信创云密码资源池，以接口调用的方式提供密码服务。

4.2.2.5 密码功能

1、身份认证服务

提供面向本系统网络内实体的统一可信、安全规范的身份认证，采用全网统一规范的身份认证协议和身份票据传递机制，为本系统内网络用户身份互信互认、业务应用安全协同、跨部门业务应用单点登录提供安全支撑。

统一身份认证既是为网络实体提供可信身份鉴别的服务系统，也是基于可信身份对访问业务应用等网络行为实施控制的系统。安全规范的身份认证应用服务是实现身份互信互认、业务应用安全协同的重要基础。

统一认证服务为持有数字证书并在统一信任支撑体系中的用户提供统一的身份认证、票据签发，票据验证服务，为适应国密 SM2 证书认证体系，应用系统需进行同步改造开发，其他功能特点如下：

（1）基于 PKI 技术实现用户身份认证，同时支持双向身份认证；

（2）能够支持 B/S 及 C/S 不同的应用模式；

（3）消息加密和数据完整性保护；

（4）采用数字签名技术，防止信息在传输过程中被篡改和发送者抵赖其发送信息；

身份认证服务包括身份认证、票据颁发与验证、网络接入控制、业务应用访问控制等。统一身份认证基于电子认证基础设施颁发的数字证书，实现用户、应用和设备等实体身份认证、身份认证结果传递、证书验证和单点登录，实现访问控制等功能。

2、完整性保护服务

完整性保护服务通过调用南通市信创云密码资源池中签名验签服务器的签名接口实现。并通过密码服务接口对外提供统一的数据完整性保护服务。符合 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》中对于三级信息系统完整性保护要求。

完整性保护服务中，采用 SM3 算法+HMAC 对数据做消息鉴别码运算，采用 SM2 算法对数据做签名和验签。

3、数据加解密服务

数据加解密服务通过调用南通市信创云密码资源池中服务器密码机的加密、解密和签名、验签接口，实现数据的机密性保护。并通过密码服务接口对外提供统一的数据加解密和签名验签服务。符合 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》中对于三级信息系统机密性保护要求。

机密性保护服务中，采用 SM1 算法与 SM4 算法对数据做加解密运算，采用 SM2 算法对数据做签名和验签。

4、链路通信加密服务

SSL VPN 提供远程管理基于数字证书的身份鉴别、高强度数据加密传输、完整性验证服务，保护用户远程访问的安全性。

（1）产品遵循国密 VPN 标准规范：《SSL VPN 技术规范》、《SSL VPN 网关产品规范》；

（2）产品支持国密 SSL 单向及双向认证功能；

（3）SSL VPN 产品支持主流国际协议，包括但不限于 SSL3.0、TLS1.0、TLS1.1、

TLS1.2、TLS1.3；

（4）支持 PKI 证书认证，支持本地或第三方 CA 签发的证书；支持国密 SM2 证书；支持双证书体系；

（5）提供内网资源授权及访问控制管理，包括但不限于：支持用户、用户组、角色、内网应用资源的管理；支持基于角色的资源授权和访问控制；支持对 IP 地址/端口、URL 资源的访问控制；支持根据访问时间进行访问控制；

（6）SSL 客户端支持主流 Window 平台/龙芯/飞腾等国产信创平台；支持不同厂商智能密码钥匙认证；支持终端和用户绑定；

（7）SSL 客户端支持用户可访问资源自动下载；支持原生 Https 协议免改造穿透；

（8）提供密钥全生命周期安全管理；提供密钥加密存储；支持顶层密钥分割安全备份。

4.2.2.6 密钥管理方式

本系统无独立的对称密钥管理系统，使用的数字证书由第三方可信 CA 机构颁发。为部署在本系统中的密码设备颁发数字证书，并制定严格的 CA 管理操作规程，保证密钥等信息和系统的部署、使用安全。本系统选用通过检测认证的商用密码产品且产品均支持国密算法，根据这些商用密码产品提供的安全策略，制定密钥管理方案，并严格遵照该方案进行使用和实施。

1、密钥存储安全

依据 GB/T39786-2021《信息安全技术 信息系统密码应用基本要求》中，关于密钥存储，达到等级保护第三级信息系统的要求密钥加密存储,并采取严格的安全防护措施，防止密钥被非法获取；密钥加密密钥存储在符合 GM/T 0028 的二级及以上密码模块中。

2、密钥分发安全

依据 GB/T39786-2021《信息安全技术 信息系统密码应用基本要求》中，关于密钥分发，达到等级保护第三级信息系统的要求密钥分发采取身份鉴别、数据完整性、数据机密性等安全措施,能够抗截取、假冒、篡改、重放等攻击，保证密钥的安全性。

3、密钥导入与导出安全

依据 GB/T39786-2021《信息安全技术 信息系统密码应用基本要求》中，关

于密钥导入与导出，达到等级保护第三级信息系统的要求采取安全措施，防止密钥导入导出时被非法获取或篡改，并保证密钥的正确性。

4、密钥使用安全

依据GB/T39786-2021《信息安全技术 信息系统密码应用基本要求》中，关于密钥使用，达到等级保护第三级信息系统的要求密钥明确用途,并按用途正确使用；对于公钥密码体制，在使用公钥之前对其进行验证;有安全措施防止密钥的泄露和替换；密钥泄露时，停止使用，并启动相应的应急处理和响应措施。按照密钥更换周期要求更换密钥;采取有效的安全措施,保证密钥更换时的安全性。

5、密钥备份与恢复安全

依据GB/T39786-2021《信息安全技术 信息系统密码应用基本要求》中，关于密钥备份与恢复,达到等级保护第三级信息系统的要求制定明确的密钥备份策略，采用安全可靠的密钥备份恢复机制，对密钥进行备份或恢复；密钥备份或恢复进行记录，并生成审计信息；审计信息包括备份或恢复的主体、备份或恢复的时间等。

6、密钥归档安全

依据GB/T39786-2021《信息安全技术 信息系统密码应用基本要求》中，关于密钥归档安全，达到等级保护第三级信息系统的要求采取有效的安全措施,保证归档密钥的安全性和正确性;归档密钥只能用于解密该密钥加密的历史信息或验证该密钥签名的历史信息；密钥归档进行记录，并生成审计信息；审计信息包括归档的密钥、归档的时间等;归档密钥进行数据备份,并采用有效的安全保护措施。

7、密钥销毁安全

依据GB/T39786-2021《信息安全技术 信息系统密码应用基本要求》中，关于密钥销毁,达到等级保护第三级信息系统的要求具有在紧急情况下销毁密钥的措施。

4.2.2.7 安全性设计

应用系统需要满足密码测评等相关标准，因此本项目从物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全等方面进行构建。

1、物理和环境安全

机房重要区域和主要出入口须部署安全门禁系统和视频监控系统,以满足对

进出机房和重要区域人员的身份鉴别和视频记录。

2、网络和通信安全

（1）终端接入安全

对终端接入网络进行控制，保证非授权终端或安全策略不合格的终端不能接入网络。

（2）网络访问控制

在网络边界实施访问控制和受控交换，阻止非授权及越权访问，对不同安全区域进行隔离和访问控制，严格控制对重要安全域的访问权限。

（3）网络设备防护

对网络设备、安全设备、服务器等进行集中运维，便于设备维护且能有效保证运维安全性。

3、设备和计算安全

计算环境安全包含服务器、计算机终端和应用系统的安全，其中服务器端在漏洞检测、基线检查、入侵监测、事件日志溯源功能方面进行增强，其它安全防护可和固定终端采用同样安全防护措施。

（1）主机监控

部署能够对主机入网计算机终端、服务器提供外设端口控制、违规外联监控、软件白名单管控、安全审计等主机安全监控功能，且主机监控审计系统需与PKI公钥基础设施完成集成，且实现对和非的终端、服务器的集中监控。

（2）数据完整性

对重要数据库进行安全审计，对流经数据库的操作进行检测、记录、分析和过滤。

（3）数据机密性

对重要数据进行加密，对重要敏感字段进行过滤，保障数据不被非法外泄，保障涉密信息不在非涉密网络中流转。

（4）访问控制

对应用系统设置访问控制策略，对访问来源、数据流量、身份鉴别等进行控制。

（5）应用安全审计

应用系统包含审计功能，对访问用户、操作内容、操作时间、操作结果等进

行安全审计，记录用户对系统的访问行为。

4、应用和数据安全

（1）身份鉴别

使用具备国密数字证书的智能密码钥匙（USB Key）实现 PC 端登录用户的身份鉴别。

（2）完整性保护

通过调用南通市信创云密码资源池中签名验签服务器，对业务平台的用户权限信息、系统日志、重要可执行程序、备份数据等进行完整性保护；

使用智能密码钥匙对业务系统中流转的业务文件、数据进行签名保护，实现对传输数据的完整性保护。

（3）机密性保护

通过调用南通市信创云密码资源池中服务器密码机对重要数据进行安全防护。

4.3 信息安全风险评估方案

系统信息安全风险评估是一个系统性的过程，用于识别、分析和评估信息系统面临的各种安全威胁和漏洞，以及这些威胁和漏洞可能对系统、组织或业务造成的潜在影响。

4.3.1 确定评估范围

本次评估范围为本系统及其会对其他相关系统造成的影响。

4.3.2 资产识别与分析

在一个全面的风险评估中，威胁、脆弱性、资产是构成风险的三要素，资产是风险评估的中心对象。在这三个要素中，威胁和脆弱性都是以资产为中心的，针对资产而客观存在的。威胁利用资产自身的脆弱性使得安全事件的发生成为可能，这些安全事件一旦发生，将对资产造成一定的影响，从而形成了风险。因此资产的评估是风险评估的出发点，全面、客观、准确地对资产进行识别、确定和估价将为后面所有因素的评估和最终风险的准确判定奠定基础。

资产评估的工作内容主要包括：对评估范围内的资产进行识别，确定所有的评估对象，然后根据评估的资产在业务和应用流程中的重要程度为资产进行估价。业务系统的调研需调查和统计被评估信息系统的资产信息，主要包括网络设备、主机、应用软件、业务系统、数据，明确目前网络状况，调查现有安全设备的部

署情况和安全策略等。

1、资产识别

一般地，信息资产包括了逻辑的和物理的资产，为了便于评估，可以把资产主要分为以下几类：

（1）硬件资产：即可见资产，它包括服务器设备、终端设备、网络设备、存储设备及其它设备；

（2）软件资产：即运行于服务器设备、终端设备或网络设备上面的软件应用程序，它包括操作系统、数据库系统、应用信息系统；

（3）数据资产：这里主要是指存在于服务器设备、终端设备或存储设备上面的数据信息，包括系统数据，业务数据，办公数据，其它业务和应用数据、备份数据等；

（4）文件资产：公司的规章制度、各类文件记录。

（5）人员资产：系统管理人员。

在进行评估时应重点关注信息资产。因为在信息安全风险评估中，资产主要指信息与信息系统，而信息系统是用来操作和处理信息的，信息是单位的核心价值所在，是信息安全保护的核心。

管理资产由管理文档和人员两部分资产组成。对管理资产赋值的主要依据是管理文档资产：根据文档的涉密性、重要性及文件丢失所产生的影响等；

人员资产：根据人员接触涉密程度、管理权限等。

2、资产抽样

由于被评估单位资产种类复杂、数量众多，本次技术评估采用抽样方法进行，其目的是确定技术检测的重点对象和目标。抽样评估的对象和目标代表信息系统的安全现状，抽样范围应覆盖整个评估对象中所涉及的各类资产，在抽样时遵循了典型性、全面性和特殊性原则。对同一单位配置完全相同的资产进行抽样，要求覆盖到每一类资产，对于有特殊用途的资产也将作为抽样对象。另外，在其它技术测试过程中如发现有高危漏洞，也将该资产纳入到抽样对象当中。抽样比例可根据现场测试结果具体调整，原则上抽样比例不低于测试数据总数的 20%。

抽样原则具体描述如下：

（1）典型性原则：对同一应用中配置、性能完全相同的资产抽样部分资产；

（2）全面性原则：对每一类资产都要抽样；

（3）特殊性原则：对于有特殊用途的资产，全部检测。

3、资产赋值

在确定了需要抽查的资产后，将形成检测资产清单列表。参照GB/T 20984《信息安全风险评估方法》，分别判断资产在保密性、完整性和可用性三个方面的要求，从而给出资产的最终赋值。

赋值依据

等级	标识	描述
5	VH（很高）	非常重要，其安全属性破坏后可能对信息系统造成非常严重的损失
4	H（高）	重要，其安全属性破坏后可能对信息系统造成比较严重的损失
3	M（中）	比较重要，其安全属性破坏后可能对信息系统造成中等程度的损失
2	L（低）	不太重要，其安全属性破坏后可能对信息系统造成较低的损失
1	VL（很低）	不重要，其安全属性破坏后可能对信息系统造成很小的损失，甚至忽略不计

4.3.2.1 业务系统调研与分析

在对被评估信息系统的风险评估中，风险的所有重要因素都紧紧围绕着业务信息资产为中心，威胁、脆弱性以及风险都是针对资产而客观存在的。威胁利用资产自身的脆弱性使得安全事件的发生成为可能，从而形成了风险。这些安全事件一旦发生，将对资产甚至是整个系统都将造成一定的影响。

与以往将每个网络设备、服务器、人员甚至业务信息资产分别独立的识别、赋值并划分重要程度等级不同，为达到分析业务影响性和整体安全风险的目的，就不能孤立对单个设备进行估价，更重要的是考虑资产对于业务的重要性，即根据资产损失所引发的潜在的业务影响来决定。因此，本项目对业务系统相关资产及其业务架构进行梳理和分析。

4.3.2.2 脆弱性识别与分析

1、脆弱性识别的工作内容

脆弱性识别也称为弱点识别，弱点是资产本身存在的，如果没有相应的威胁发生，单纯的弱点本身不会对资产造成损害。而且如果系统足够强健，再严重的威胁也不会导致安全事件，并造成损失。即，威胁总是要利用资产的弱点才可能造成危害。

脆弱性识别主要从技术和管理两个方面进行，技术脆弱性涉及物理层、网络层、系统层、应用层等各个层面的安全问题。管理脆弱性又可分为技术管理和组织管理两方面，前者与具体技术活动相关，后者与管理环境相关。

2、脆弱性种类分析

脆弱性识别时的数据应来自于资产的所有者、使用者，以及相关业务领域和软硬件方面的专业人员等。脆弱性识别所采用的方法主要有：问卷调查、工具检测、人工核查、文档查阅等。

脆弱性种类清单

类型	识别对象	识别内容
技术脆弱性	物理环境	从机房场地、机房防火、机房供配电、机房房防静电、机房接地与防雷、电磁防、通信线路的保护、机房区域防护、机房设备管理等方面进行识别。
	网络结构	从网络结构设计、边界保护、外部访问控制策略、内部访问控制策略、网络设备安全配置等方面进行识别。
	系统软件	从补丁安装、物理保护、用户账号、口令策略、资源共享、事件审计、访问控制、新系统配置、注册表加固、网络安全、系统管理等方面进行识别。
	应用中间件	从协议安全、交易完整性、数据完整性等方面进行识别。
	应用系统	从审计机制、审计存储、访问控制策略、数据完整性、通信、鉴别机制、密保保护等方面进行识别。
管理脆弱性	技术管理	从物理和环境安全、通信与操作管理、访问控制、系统开发与维护、业务连续性等方面进行识别。
	组织管理	从安全策略、组织安全、资产分类与控制、人员安全、符合性等方面进行识别。

4.3.2.3 安全威胁识别与分析

威胁是指可能对资产或组织造成损害事故的潜在原因。作为风险评估的重要因素，威胁是一个客观存在的事物，无论对于多么安全的信息系统，它都存在。

风险评估的这一过程，不仅要对组织需要保护的每一项关键资产进行威胁识别，确认威胁的主体和客体，而且对每种威胁发生的可能性进行分析赋值。

安全威胁是一种对系统、组织及其资产构成潜在破坏的可能性因素或者事件。产生安全威胁的主要因素可以分为人为因素和环境因素。人为因素包括有意因素和无意因素。环境因素包括自然界的不可抗力因素和其它物理因素。

威胁可能是对信息系统直接或间接的攻击，例如非授权的泄露、篡改、删除等，在保密性、完整性或可用性等方面造成损害。威胁也可能是偶发的、或蓄意的事件。一般来说，威胁总是要利用网络、系统、应用或数据的弱点才可能成功地对资产造成伤害。

安全事件及其后果是分析威胁的重要依据。但是有相当一部分威胁发生时，由于未能造成后果，或者没有意识到，而被安全管理人员忽略。这将导致对安全威胁的认识出现偏差。

威胁分析方法可以首先需要考虑威胁的来源，然后分析存在哪些威胁种类，最后进行威胁赋值。

1、威胁来源分析

信息系统的安全威胁来源

威胁来源		威胁来源描述
环境因素		由于断电、静电、灰尘、潮湿、温度、鼠蚁虫害、电磁干扰、洪灾、火灾、地震等环境条件和自然灾害；意外事故或由于软件、硬件、数据、通讯线路方面的故障。
人为因素	恶意人员	不满的或有预谋的内部人员对信息系统进行恶意破坏：采用自主或内外勾结的方式盗窃机密信息或进行算改，获取利益；外部人员利用信息系统的脆弱性，对网络或系统的机密性、完整性和可用性进行破坏，以获取利益或炫耀能力。
	非恶意人员	内部人员由于缺乏责任心，或者由于不关心和不专注，或者没有遵循规章制度和操作流程而导致故障或信息损坏；内部人员由于缺乏培训、专业技能不足、不具备岗位技能要求而导致信息系统故障或被攻击。

2、威胁种类分析

按照威胁的主体或来源的不同，可以分为系统合法用户、非法用户和物理环境类型。在本次风险评估中，将对安全威胁进行考虑，通过调查问卷的方式，并对相关网络系统管理员、安全管理员进行了调查，获取了与威胁有关的客观、准确、全面的资料。

威胁种类

威胁种类	威胁描述	威胁子类
软硬件故障	对业务实施或系统运行产生影响的设备硬件故障、通讯链路中断、系统本身或软件缺陷等问题	设备硬件故障、传输设备故障、存储媒体故障、系统软件鼓掌、应用软件故障、数据库软件故障、开发环境鼓掌等
物理环境影响	对信息系统正常运行造成影响的物理环境问题和自然灾害	断电、静电、灰尘、潮湿、温度、鼠蚁虫害、电磁干扰、洪灾、火灾、地震等
无作为或操作失误	应该执行而没有执行相应的操作、或无意执行了错误的操作	维护错误、操作失误等
管理不到位	安全管理无法落实或不到位，从而破坏信息系统正常有序运行	管理制度和策略不完善、管理规程缺失、职责不明确、监督管控机制不健全等
恶意代码	故意在计算机系统上执行恶意任务的程序代码	病毒，特洛伊木马、蠕虫、陷门、间谍软件、窃听软件等
越权或滥用	通过采用一些措施，超越自己的权限访问了本来无权访问的资源，或者滥用自己的权限，做出破坏信息系统的行为	非授权访问网络资源、非授权访问系统资源、滥用权限非正常修改系统配置或数据、滥用权限泄露秘密信息等
网络攻击	利用工具和技术通过网络对信息系统进行攻击和入侵	网络探测和信息采集、漏洞探测、嗅探（账号、口令、权限等）、用户身份伪造和欺骗、用户或业务数据的窃取和破坏、系统运行的控制和破坏等
物理攻击	通过物理的接触造成对软件、硬	物理接触、物理破坏、盗窃等

威胁种类	威胁描述	威胁子类
	件、数据的破坏	
泄密	信息泄露给不应了解的他人	内部信息泄露、外部信息泄露等
篡改	非法修改信息、破坏信息的完整性使系统的安全性减低或信息不可用	篡改网络配置信息、篡改系统配置信息、篡改安全配置信息、篡改用户身份信息或业务数据信息等
抵赖	不承认收到的信息和所做的操作和交易	原发抵赖、接受抵赖、第三方抵赖等

威胁发生的可能性受下列几个因素的影响：

（1）资产的吸引力和暴光程度，组织的知名度，主要在考虑人为故意威胁时使用；

（2）造成威胁的技术难度；

（3）资产转化成利益的容易程度，包括财务的利益，黑客获得运算能力很强和大带宽的主机使用等利益。主要在考虑人为故意威胁时使用。

实际评估过程中，威胁的可能性赋值，除了考虑上面两个因素，还需要参考下面三方面的资料和信息来源，综合考虑，形成在特定评估环境中各种威胁发生的可能性：

（1）通过过去的安全事件报告或记录，统计各种发生过的威胁和其发生频率；

（2）过去一段时期内所遭受的威胁攻击信息。

为了便于对不同威胁发生的可能性概率数据进行类比、度量，采用了统一的度量标准：采用相对等级的方式进行度量，等级值为 1-5，1 为最低，5 为最高。

属性评估准则参照表

等级	标识	定义
5	很高	出现的频率很高（或>=1 次/周）；或在大多数情况下不可避免；或可以证实经常发生过
4	高	出现的频率较高（或>=1 次/月）；或在大多数情况下很有可能会大声；或可以证实多次发生过
3	中	出现的频率中等（或>1 次/半年）；或在某种情况下可能会发生；或被正式曾经发生过
2	低	出现的频率较小；或一般不太可能发生；或没有被证实发生过
1	很低	威胁几乎不可能发生，仅可能在非常罕见和例外的情况下发生

4.3.3 风险及规避措施

4.3.3.1 时间选择

为减轻漏洞扫描对网络和主机的影响，漏洞扫描时间尽量安排在业务量不大的时段或晚上进行。

4.3.3.2 攻击策略集选择

为防止漏洞扫描造成网络和主机的业务中断，在漏洞扫描中不使用含有拒绝服务的测试策略，在整个测试过程中不使用社会工程类攻击。

对于不能接受任何可能风险的主机系统，或者可选择如下保守策略：

1、复制一份目标环境，包括硬件平台，操作系统，数据库管理系统，应用软件等；

2、对目标的副本进行漏洞扫描。

4.3.3.3 系统备份策略

为防止在漏洞扫描过程中出现的异常的情况，所有被评估系统均在被评估之前作一次完整的系统备份或者关闭正在进行的操作，以便在系统发生灾难后及时恢复。

4.3.3.4 系统恢复策略

在漏洞扫描过程中，如果出现被评估系统没有响应或中断的情况，当立即停止测试工作，与客户方配合人员一起分析情况，在确定原因后，及时恢复系统，并采取必要的预防措施（比如调整测试策略）之后，确保对系统无影响，并经客户方同意之后才可继续进行。

4.3.3.5 过程监控

本项目在过程监控根据评估过程中采用以下方式：

1、全程监控：采用类似 Ethereal 或 Sniffer Pro 的嗅探软件进行全程抓包嗅探。优点是全过程都能完整记录。缺点是数据量太大，不易分析；需要大容量存储设备。

2、择要监控：对扫描过程不进行录制，仅仅在安全工程师分析数据后，准备发起扫描前，才开启类似 Ethereal 或 Sniffer Pro 的软件进行嗅探。

3、主机监控：仅监控受测主机的存活状态，避免意外情况发生。

4.4 数据安全保护方案

4.4.1 数据安全级别分析

根据数据在经济社会发展中的重要程度，以及一旦遭到篡改、破坏、泄露或者非法获取、非法利用，对国家安全、公共利益或者个人、组织合法权益造成的危害程度，分为不敏感数据、低敏感数据和高敏感数据三个级别，其中如系统数据涉及个人信息等数据，应定为低敏感数据，如系统数据涉及重要政务数据或个

人敏感信息等数据，应定为高敏感数据。承载低敏感数据或高敏感数据的项目应开展数据安全风险评估工作。

根据上述数据安全级别定义，按照自主定级原则，项目建设单位对本部门管辖的政务数据进行分类分级保护，项目的政务数据安全级别定位为低敏感数据。

4.4.2 数据安全风险和需求分析

数据安全是降低敏感数据向内、外部泄露风险的最有效层面之一。在该层面，防护的焦点在于数据本身，不论其传播途径如何，其目的在于确保数据安然无恙。数据的移动性正日益加强，因此数据安全防护至关重要。

在项目总体规划设计中，对于数据安全方面我们提出以下要求或原则，以保证数据的安全、可靠。

4.4.2.1 数据安全风险分析指标

数据安全风险分析指标

数据处理活动	数据威胁分类	数据威胁描述
数据收集	恶意代码注入	数据入库时，恶意代码随着数据注入到数据库或信息系统，危害数据机密性、完整性、可用性
	数据无效写入	数据入库时，数据不符合规范或无效
	数据污染	数据入库时，攻击者接入采集系统污染待写入的原始数据，破坏数据完整性
	数据分类分级或标记错误	数据分类分级判断错误或打标记错误，导致数据受保护级别降低
数据传输	数据窃取	攻击者伪装成外部通信代理、通信对端、通信链路网关通过伪造虚假请求或重定向窃取数据
	网络监听	有权限的员工、第三方运维与服务人员接入，或攻击者越权接入内部通信链路与网关、通信代理监听数据； 攻击者接入外部通信链路与网关、通信代理、通信对端监听数据
	数据篡改	攻击者伪装成通信代理或通信对端篡改数据
数据存储	数据破坏	由于信息系统自身故障、物理环境变化或自然灾害导致的数据破坏，影响数据完整性和可用性
	数据篡改	篡改网络配置信息、篡改系统配置信息、篡改安全配置信息、篡改用户身份信息或业务数据信息等，破坏数据完整性和可用性
	数据分类分级或标记错误	数据分类分级或数据标记被篡改，导致数据受保护级别降低
	数据窃取	在数据库服务器、文件服务器、办公终端等存储系统安装恶意攻击窃取数据
	恶意代码执行	故意在数据库服务器、文件服务器、员工终端等存储上执行后门、病毒、木马、蠕虫、窃听软件、间谍软件等恶意程序或代码，窃取、篡改或破坏数据
	数据不可控	依托第三方云平台、数据中心等存储数据，没有有效的约束与控制手段；

		在使用云计算或其他技术时，数据存放位置不可控，导致数据存在境外数据中心,数据和业务的司法管辖关系发生改变
数据使用、数据加工	注入攻击	数据处理系统可能遭到恶意代码注入、SQL 注入等攻击，造成信息泄露，危害数据机密性、完整性、可用性
	数据抵赖	人员访问数据后，不承认在某时刻用某账号访问过数据
	使用权限混乱	处理系统调用数据接口权限混乱,导致能访问未开放的数据
	数据过度获取	由于相关业务对数据需求不明确，或未实现基于业务人员、系统与所需要数据的关系的访问控制,导致业务人员或处理系统获取超过业务所需数据，容易造成数据泄露
	数据不可控	依托第三方机构或外部处理系统处理数据,没有有效的约束与控制手段
	敏感元数据未脱敏使用	处理系统可直接调取敏感元数据，容易导致信息泄露
数据提供、数据公开	共享数据未脱敏	与第三方机构共享数据时,第三方机构及其人员可以直接获取敏感元数据的调查、查看权限
	数据窃取	因共享通道未加密，攻击者可到共享通道进行网络数据监听，从而实现数据的窃取
	共享权限混乱	与第三方机构共享数据时，接口权限混乱，导致第三方能访问其他未开发的数据
	数据过度获取	由于业务对数据需求不明确,或未实现基于业务人员与所需要数据的关系的访问控制,业务人员获取超过业务所需的数据，容易造成数据泄露
	数据不可控	数据可被内部员工获取，组织对内部员工对所获数据的保存、处理、再转移等活动不可控; 数据可被第三方服务商、合作商获取，组织对第三方机构及其员工对所获数据的使用、留存、再转移等活动未约束或不掌握; 数据共享给恶意的第三方机构
数据销毁	数据到期未销毁	数据失效或业务关闭后，遗留了敏感数据仍然可以被访问，破坏了数据的机密性
	数据未正确销毁	被销毁数据通过技术手段可恢复，破坏数据的机密性

4.4.2.2 数据分级分类

项目总体规划设计及平台建设全过程，要求提供详细的数据分类支持。数据分类利用多级安全性解决在实际中遇到的数据安全和隐私问题。

4.4.2.3 对数据限制性访问的要求

在不影响应用程序功能的前提下快速而高效地保护现有程序：

1、限制 DBA 和其他授权用户访问应用程序数据；

2、防止应用程序 DBA 操纵数据库和访问其他应用程；

3、更好的控制何人、何时、何地可以访问应用程序。

可用于严格地控制应用程序的安全性，限制何人、何时、何地、如何访问应用程序。可以在不更改现有应用程序下灵活机变地使用这些特性来实施授权。如日期时间、数据库客户端在网络上的位置之类的因素，或特定于企业的客户因素

可用于控制访问应用程序的能力。

4.4.2.4 数据完整性

能够检测到系统管理数据、鉴别信息和重要业务数据在传输过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施；能够检测到系统管理数据、鉴别信息和重要业务数据在存储过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施。

4.4.2.5 数据保密性

采用加密或其他有效措施实现系统管理数据，鉴别信息和重要业务数据传输保密性；采用加密或其他保护措施实现系统管理数据、鉴别信息和重要业务数据存储保密性。

4.4.2.6 备份和恢复

提供本地数据备份与恢复功能，定期进行完全数据备份，采用冗余技术设计网络拓扑结构，避免关键节点存在单点故障；提供主要网络设备、通信线路和数据处理系统的硬件冗余，保证系统的高可用性。

4.4.3 项目建设过程中的数据安全保障措施

4.4.3.1 岗位职责

设置系统的关键岗位并加强管理，配备系统管理员、应用开发管理员、安全审计员，要求三个岗位各自独立。要害岗位人员必须严格遵守保密法规和有关信息安全管理规定。

1、系统管理员

负责系统的运行管理，实施系统安全运行细则；

(1) 严格用户权限管理，维护系统安全正常运行；

(2) 认真记录系统安全事项，及时向信息安全人员报告安全事件；

(3) 对进行系统操作的其他人员予以安全监督。

2、应用开发管理员

(1) 负责在系统开发建设中，严格执行系统安全策略，保证系统安全功能的准确实现；

(2) 系统投产运行前，完整移交系统相关的安全策略等资料；

(3) 不得对系统设置“后门”；

(4) 对系统核心技术保密等。

3、安全审计员

负责对涉及系统安全的事件和各类操作人员的行为进行审计和监督。

(1) 按操作员证书号进行审计；

(2) 按操作时间审计；

(3) 按操作类型审计；

(4) 事件类型进行审计；

(5) 日志管理等。

4.4.3.2 统一权限管理

通过权限管理服务来实现用户权限的管理和控制，确保合法用户拥有合适的操作权限，并确保应用系统资源得到有效的访问权限控制。

4.5 系统应用系统安全方案

4.5.1 等级保护二级测评

系统需通过具有测评资质的第三方机构对项目的二级等保测评。

4.5.1.1 服务介绍

由等保专家顾问对目标系统的建设情况、运行情况进行了解，从技术层面和管理层面给出整改规划，包括系统安全加固、安全策略配置、安全设备采购、安全管理制度编制等，并协助客户定级备案，对测评对象进行模拟测评，进行差距分析，根据结果进行加固整改，然后选定符合要求测评机构进行测评，并根据测评机构提出的整改建议进行整改，直至等保测评顺路通过。

1、建设目标

安全建设是落实网络安全等级保护制度的核心和落脚点，等级保护建设是在等级保护对象定级工作基础上深入开展的一项工作，使网络系统可以按照保护等级的要求进行设计、规划和实施，并且达到相应等级的基本保护水平和保护能力。

依据网络安全等级保护相关标准和指导规范，本次安全建设方案提出总体安全目标如下：

保障 IT 基础网络安全、保障业务应用安全，实现等级保护对象安全稳定运行，同时符合国家相关法律法规要求。

具体目标描述如下：

（1）IT 基础网络安全

安全的IT基础网络能够提供稳定的IT基础设施环境，保障设备和线路冗余，

同时为业务应用系统提供稳定、可靠的运行环境；保障网络和系统运行处于可控状态，统一实施对各类网络设备、服务器设备、控制终端设备等的管理，确保业务系统 IT 基础设施的安全稳定运行。

（2）业务应用运行安全

通过统一的安全管理措施，统一的访问控制策略，统一的安全审计、网络监控措施，及统一的授权、认证措施，保障业务系统不受恶意攻击的影响，防止业务中断。

（3）满足国家相关法律法规要求

按照国家等级保护工作的要求确定了安全保护等级，需要按照国家等级保护相关技术标准和规范开展等级保护工作，实施相应等级强度的安全保护，满足国家等级保护要求。

2、建设原则

按照“统一规划、重点明确、合理建设、同步建设”的基本原则，在安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心和安全管理等方面进行安全规划与建设，使得安全防护能力达到安全等级保护第三级安全要求。

基于业务系统安全需求，结合网络（安全）产品、服务器（操作系统、数据库、中间件）、安全服务、管理制度等安全防护措施，建立全网的安全防控管理服务体系，从而全面提高安全防护能力。

（1）分区分域防护原则

任何安全措施都不是绝对安全可靠的，为保障攻破一层或一类保护的攻击行为而不会破坏整个信息系统，以达到纵深防御的安全目标，需要合理划分安全域，综合采用多种有效安全保护措施，实施多层、多重保护。

（2）均衡性保护原则

对任何类型网络，绝对安全难以达到，也不一定是必须的，需正确处理安全需求、安全风险与安全保护代价的关系。因此，结合适度安全防护实现分等级安全保护，做到安全性与可用性平衡，达到技术上可实现、经济上可执行。

（3）技术与管理相结合原则

信息安全涉及人、技术、操作等方面要素，单靠技术或单靠管理都不可能实现。因此在考虑网络安全建设时，必须将各种安全技术与运行管理机制、人员思

想教育、技术培训、安全规章制度建设相结合。

（4）动态调整与可扩展原则

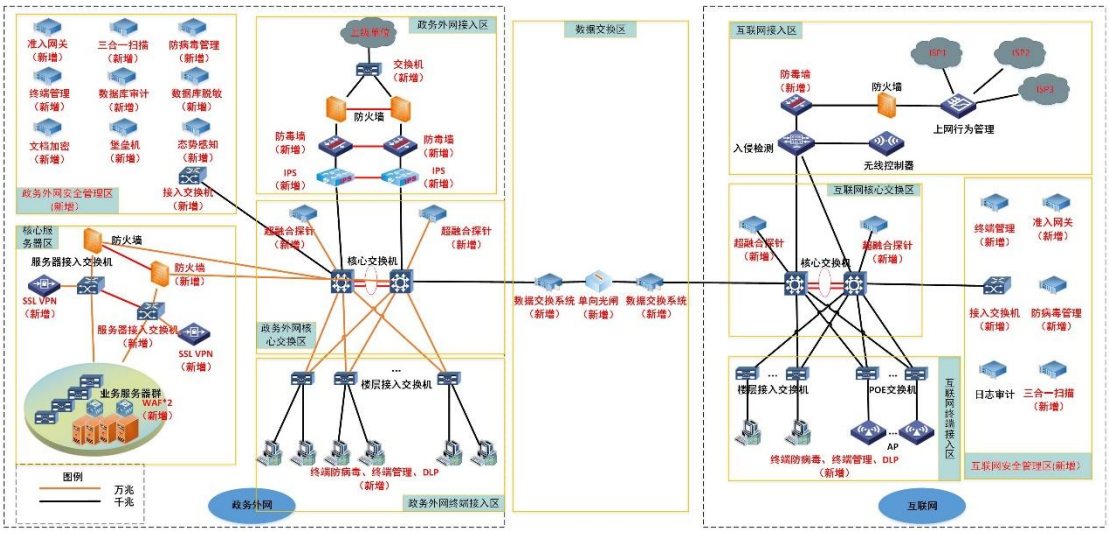
由于网络安全需求会不断变化，以及环境、条件、时间的限制，安全防护一步到位，一劳永逸地解决网络安全问题是不现实的。网络安全建设可先保证基本的、必需的安全保护，后续再根据应用和网络安全技术的发展，不断调整安全策略，加强安全防护力度，以适应新的网络安全环境，满足新的信息安全需求。

（5）网络安全三同步原则

信息系统在新建、改建、扩建时应当同步建设网络安全设施，确保其具有支持业务稳定、持续运行性能的同时，保证安全技术措施同步规划、同步建设、同步使用，以保障信息安全与信息化建设相适应。

4.5.1.2 总体安全防护体系

体系以安全合规要求为基础，以实际业务安全需求为驱动，构建信息安全等级保护深度防御体系。在建设过程中，遵循统一规划、统一标准、统一管理、适度保护、重点保护、强化管理的原则。



安全保护体系从安全技术、安全管理以及安全运营三个维度进行设计。基于《网络安全等级保护安全设计技术要求》（GB/T 25070-2019）的安全防护理念，构建“纵深防御+主动防御+持续监测”安全防护体系，即基于等级保护“一个中心，三重防护”的纵深防御体系，融合“网络安全，以人为本”的理念，构建自主评估、风险驱动、实时预警、动态防护、安全检测、及时响应于一体的主动防御闭环防护体系，同时对整个等级保护对象安全状况持续监测，及时感知安全态势。

4.5.1.3 总体安全策略

1、信息技术安全体系总体策略

（1）参照以《网络安全等级保 护基本要求》中三级保护要求为控制要求，建设基础安全技术体系框架。

（2）安全技术体系建设覆盖物理环境、通信网络、区域边界、计算环境和安全管理中心五个方面。

（3）通过业界成熟可靠的安全技术及安全产品，结合专业技术人员的安全技术经验和能力，系统化的搭建安全技术体系，确保技术体系的安全性与可用性的有机结合，达到适用性要求。

（4）建设集中的安全管理平台，实现对系统的统一认证、分权管理、集中管控。

2、信息安全管理体系总体策略

（1）建立信息安全领导小组和信息安全工作组，形成等级保护基本要求的信息安全组织体系职责。

（2）建立信息安全管理制度和策略体系，形成符合等级保护基本要求的安全管理制度要求。

（3）建立符合系统生命周期的安全需求、安全设计、安全建设和安全运维的运行管理要求。

（4）安全建设过程应落实等级保护定级备案、建设整改、等级测评等管理要求。

（5）系统安全运行过程应落实等级保护监督检查的管理要求。

3、信息安全运营体系总体策略

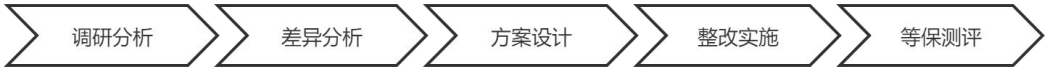
（1）通过互联网等领域所形成的新技术适当提升安全能力，强化风险识别、预警、监测、防护、处置、溯源等能力。

（2）建立规范的信息化安全运营体系，以安全视角规范信息系统安全运营的整个过程，形成安全业务标准与流程。

（3）建立信息安全运营中心，安全运营实行分级保障，加强安全运营的可持续性建设。

4.5.1.4 服务流程及说明

- **服务流程**



调研分析：调研客户信息系统安全现状，包括物理环境、网络环境、应用系统、管理制度等，梳理业务系统以及相关资产清单，明确信息系统的安全保护等级，如果是首次测评则协助客户编制定级报告。

差异分析：由等保专家对测评对象进行一次模拟测评，根据测评要求，对系统进行安全评估，分析目标当前存在的问题，从网络、主机、应用、数据、策略、组织架构、人员、建设管理、运维管理等方面进行分析，给出差异性分析报告。

方案设计：根据差异分析报告针对性的给出整改实施方案，包括物理环境、系统环境、安全管理制度等方面，如果需要采购安全设备的，给出采购方案。

整改实施：由安全运维工程师以及实施工程师根据整改实施方案对目标进行整改加固，需要采购安全设备的提交客户进行采购。

等保测评：通过全国合作渠道选定符合要求的测评机构进行测评，等保专家配合测评公司完成整个测评工作，并对测评过程中提出的问题进行整改，直至测评通过。

- **服务范围**

达到网络安全等级保护二级以及三级的信息系统。

- **服务模式**

三级一年一次/二级两年一次。

- **服务方法**

现场测评：提供专业的等保专家抵达客户现场进行等保准备以及测评协助，测评机构现场进行测评。

4.5.1.5 安全产品部署说明

序号	安全产品	部署位置	主要功能	满足要求
1	防火墙	各安全域边界、接入网边界	边界访问控制、基于应用协议的访问控制，边界访问安全审计	安全区域边界
2	网闸	数据中心数据交换区	不同网络之间的逻辑隔离，数据安全交换	安全区域边界
3	入侵检测系统	核心交换机、汇聚交换机旁	攻击检测、监测内部攻击行为	安全区域边界

序号	安全产品	部署位置	主要功能	满足要求
4	入侵防御系统	互联网或接入网出口	攻击检测和阻断、限制外部攻击行为	安全区域边界
5	抗DDOS攻击系统	互联网出口	DDOS攻击检测与阻断、流量清洗	安全区域边界
6	APT攻击系统	互联网出口	APT及新型威胁攻击检测与告警	安全区域边界
7	防病毒网关	互联网或接入网出口	病毒、木马、蠕虫检测与阻断	安全区域边界
8	IPSEC VPN	局域网对端	远程通信加密、访问控制	安全区域边界、安全通信网络
9	SSL VPN	互联网出口	移动PC或手机用户身份认证、远程通信加密、准入控制、访问控制	安全区域边界、安全通信网络
10	网络准入控制	核心交换机	终端认证准入、终端用户管理、可信终端检查	安全区域边界
11	堡垒机	安全管理区	管理设备准入、远程通信加密、身份认证、访问控制、管理用户审计	安全区域边界、安全通信网络
12	WAF	应用服务器前	WEB应用服务器的安全防护，防篡改、防入侵	安全区域边界
13	终端安全管理系统	服务器+客户端	终端补丁管理、终端准入、终端审计、介质管理、非法外联、端口管控等	安全计算环境、安全管理中心
14	服务器安全加固	服务器	服务器身份鉴别、访问控制、数据保护、入侵防范、安全审计等	安全计算环境
15	上网行为管理系统	互联网出口	应用控制、用户行为审计、URL访问审计与过滤、流量控制等	安全计算环境、安全区域边界
16	网络安全审计	核心交换机	网络设备日志集中审计、集中存储、异常告警、日志报表	安全区域边界
17	身份认证系统	安全管理区	用户管理、证书管理、传输加密	安全计算环境
18	身份认证和访问控制类产品	安全管理区	应用单点登录、身份认证、细粒度访问控制、应用审计	安全计算环境
19	数据防泄密（DLP）	安全管理区+主机	数据全生命周期管理、数据透明加解密、文件保险箱、用户操作行为审计等	安全计算环境
20	数据库审计系统	数据库服务器区	数据库操作行为审计、事件关联分析、报表报告	安全计算环境

序号	安全产品	部署位置	主要功能	满足要求
21	超融合探针	核心交换区	超融合检测探针采用特征检测技术与异常行为检测相结合的技术路线。其中，特征检测技术具体通过内置特征库、病毒库、恶意样本库、恶意 URL 库和自定义特征实现。异常行为检测技术具体通过内置 C&C、网络扫描、蠕虫等行为模型实现。	安全计算环境
22	安全态势感知系统（SOC）	安全管理区	日志收集与存储、关联分析、实时安全监测、流量分析、威胁情报、告警和通报、综合安全态势分析	安全管理中心

4.5.2 商用密码应用安全性评估

系统需通过具有测评资质的第三方机构对项目的商用密码应用性安全评估。

由密保专家顾问对测评目标收集信息，进行初步评估，选定国家密码管理局公布的密评机构目录上的测评机构，按照测评流程，对测评目标进行测评。根据测评机构提供的测评报告，协助用户提供整改方案、技术支撑。

总体密码测评服务流程如下：

信息收集：对测评目标的资产信息进行梳理，了解当前的物理环境、网络通信、应用数据等技术现状，通过对管理制度、管理现状的梳理，为评估做准备。

差异分析：对收集的信息按照密码测评要求进行初步分析，根据当前测评目标的现状，提出与密码测评要求不符的问题，初步整改能够完善改进的问题。

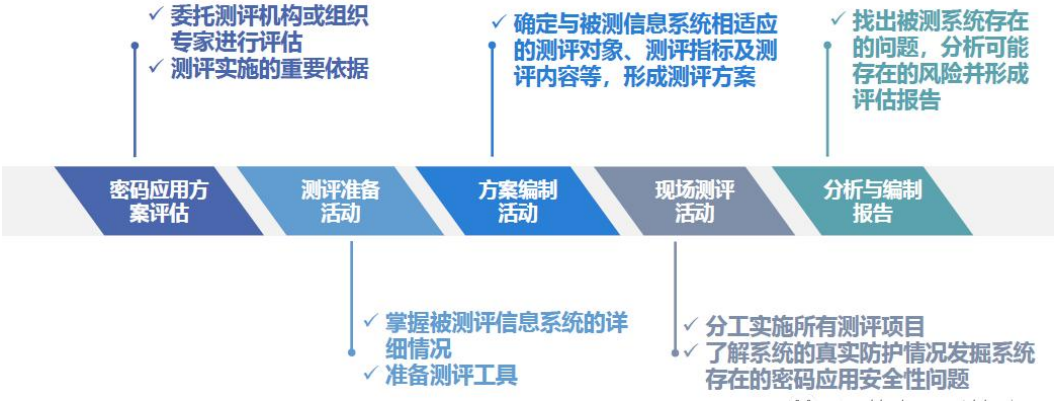
密码测评：选择有密码测评资质的测评机构，进驻现场对测评目标进行正式测评，协助测评机构评估。

整改实施：测评完成后，根据测评机构提供的测评报告，提供问题的处置意见，协助用户整改。

整改检查：整改完成后，进行整改检查，确认整改到位并联系测评机构复测。

正式测评流程分为五个部分，分别为：密码应用方案评估、测评准备活动、

方案编制活动、现场测评活动、分析与报告编制，具体流程见图：



4.5.2.1 密码应用方案评估

针对已建系统，明确信息系统的详细拓扑，梳理已有的密码产品，梳理密钥管理层次，给出生命管理过程，针对重要或敏感信息，梳理其在信息流转过程和受保护情况。

密码应用建设方案由责任单位组织商用密码产业单位编写，三个方案需经过专家或测评机构评审。

建设方案一：密码应用解决方案

确保解决方案内容的完整，密码应用的合规性、正确性、有效性。

✓ 密码应用体系架构

✓ 算法使用

✓ 密钥管理

建设方案二：密码应用实施方案

确保实施方案的科学合理性和可行性。

✓ 实施路线图

✓ 升级改造方案

✓ 责任机构和责任人

✓ 工作计划和任务分工

建设方案三：应用应急处置方案

确保应急处置方案文档的完整性，风险分析的完备性，处置措施和应急方案的合理周密性。

✓ 分析潜在意外事件

✓ 制定多套应急处置预案

- ✓ 明确处理人员角色和责任
- ✓ 应急事件通告策略
- ✓ 损失评估程序
- ✓ 预案激活条件

4.5.2.2 测评准备

填写商用密码应用安全性评估系统调查表（调查表中填写的密码算法、密码产品、密码应用情况等内容需要在现场进行以防客户信息填写错误）。

1. 掌握被测评信息系统的详细情况

系统基本信息：

(1) 系统名称保持与等保测评证书上一致（选择正式的名称）

(2) 等保备案情况（收集等保证书、等保测评报告（核查资产是否瞒报））

(3) 是否投入运营（收集上一次密测结果（如有））

(4) 是否具备密码应用方案（收集 3 个密码应用方案、评估结果报告（如有））

系统主要构成：

(1) 按备注说明要求填写

(2) 信息安全人员：填写甲方人员，非外包开发方

(3) 制度：密码应用相关制度

2. 准备测评工具

(1) 抓包工具、基线测试工具等。

4.5.2.3 方案编制

确定与被测信息系统相适应的测评对象、测评指标及测评内容，形成测评内容等，形成**测评方案**。

(1) 整理测评准备活动中获取的信息系统相关材料

(2) 确定测评对象（根据系统调查表确认）

(3) 确定测评指标（确定不适用的指标）

(4) 根据测评内容（根据作业指导书、测评对象、测评指标确定测评内容）

(5) 确定测试根据及方法（测评工具接入点、不影响业务系统）

(6) 编制及确认方案

4.5.2.4 现场测评

进行现场测评,分工实施所有测评项目了解系统的真实防护情况发掘系统存在的密码应用安全性问题，测评阶段如下：

第一阶段：首次会议

(1) 介绍测评对象

(2) 明确密码测评网络环境、网络边界、实施场所

(3) 明确密码测评工作配合人员代表（信息安全人员）

(4) 明确系统承建方密码专业技术人员（密码承建人员）

第二阶段：测评实施

(1) 密码产品及关键设备的登录与配置查看

(2) 密码算法、技术、服务等密码应用的详细说明

(3) 测评小组测评接入

(4) 制度解释说明

(5) 测评实施过程风险提示

第三阶段：末次会议

(1) 现场测评汇总结果的确认

(2) 测评实施后系统运行状态确认

(3) 制度文件、配置管理文档归还交接

(4) 结束现场测评

(5) 提供密码应用解决方案、实施方案、信息安全相关制度、应急预案

(6) 密码产品型号证书、密码服务许可（查询验证）

(7) 现场测评实施授权

(8) 测评小组介绍测试周期、工作内容

测评内容包括：

(1) 密码算法： AES、DES、MD5、RSA1024、SHA-1此类算法为已公布的高危算法,3DES、RSA-2048、SHA-256合规性问题

(2) 密码产品：

1) 带一部分密码功能但主要为业务服务的设备（不列入表格）

2) 自己实现的密码功能但未通过产品检测的设备（列入表格但不合规）。

3) 密码产品并检测通过具有产品证书（列入表格且合规）

(3)密码技术：使用了什么技术（签名验签、数字证书、加解密等）怎么实现的（密码产品、软实现）

（4）密码服务： 使用哪一家的密码服务，是否具有许可

4.5.2.5 分析与报告编制

找出被测系统存在的问题，分析可能存在的风险并形成**评估报告。**

(1) 对单元测试结果进行分析，汇总首测信息系统整体结果，并进行风险分析和评价

(2) 更具业务、部署环境及关联系统分析面临的外在安全风险

(3) 测评结论形成并编制报告

4.6 安全经费概算

本项目将在南通市政务信创云已有的网络安全防护体系基础上接入市密码服务平台，账户密码存储采用国密算法，并在验收前完成等级保护测评（二级）、密码应用安全性评估和信息安全风险评估，信息安全风险评估、密码应用安全性评估相关费用已在项目中预留。

第 五 章 项目实施进度

5.1 项目建设期

本项目的建设周期为 2026 年 5 月至 2026 年 10 月。

5.2 实施进度计划

序号	总体计划	分期计划	
1	启东市新产业服务中心信息系统	开发适配	合同签订后 4 个月内完成开发适配
		试运行阶段	试运行 1 个月
		正式运行	试运行并完善后进入正式运行