# 技术文件

# 第一部分公司介绍

北京北信智科科技有限公司是由多年从事IT行业开发人员创立的年轻公司,我们致力于提供专业化的应用软件和服务，度身为客户提供完善的信息化解决方案。已经拥有了自主研发的IP呼叫中心、政务管理平台、OA、BI商业智能分析系统、CRM、CMS等产品。我们拥有强大的研发能力及丰富的项目实施经验，典型客户包括电子政务、电子商务、旅游、商旅、物流、金融保险、IT服务业、电信增值服务业、电力业、金融保险业、消费产品与服务业、家电、制造业、政府、医疗卫生、医药保健品业、邮政、交通运输、能源、人力资源、广电媒体等.THINKPBX(北信智科)所有产品都拥有自主产权的、完整的解决方案，并能提供从咨询、设计到软件开发及维护全方位的360度服务;产品系统稳定,功能全面。

本公司是一家提供领先IT解决方案和专业服务的高科技企业，致力于为政府、企业的业务信息化提供应用软件和行业解决方案、系统管理和数据安全等各类通用服务，以及基于解决方案的IT咨询规划、系统集成、定制软件开发、维护保修、资源外包等专业化服务。公司拥有一支经验丰富而又朝气蓬勃的团队，平均年龄30岁，平均行业从业年限超过5年，项目经验丰富。志存高远，锐意进取。北信科技将继续以良好的信誉和现有能力为基础，并一如既往地秉承“诚信、务实、进取、专业、共赢”的公司理念，与每一位客户共同成长与发展，为其提供更全面、更优质的信息化服务，成为其不可或缺的忠诚伙伴。同时成为员工学习、生活、发展的家园，做一个值得信赖的专业化的IT服务公司。

1.我们的优势

提供从咨询、方案设计、项目实施到运营管理培训的“一站式”服务深厚的行业知识和技术积累，严格的项目管理制度、完善的实施方法，严格按照国际化认证的标准来保证项目实施质量（ISO9001）和软件研发的质量（CMM）

2.卓越的解决方案与产品

* 您 需 要： 符合您需求的个性化的解决方案与性能稳定的产品
* 我们秉承： “全过程客户体验”的经营理念从而为客户提供量身定制解决方案及产品

3.度身定制的全方位服务

* 您 需 要： 服务 － 帮助您成功的服务。
* 我们提供： 从售前咨询、售中方案制作、售后技术支持、系统运营管理咨询全程支持。

4.良好的质量保证体系

* 您 需 要： 稳定的系统、可值信赖的合作伙伴。
* 我们奉行： “零BUG上线, 100%投诉得到响应, 100%问题得到解决”的质量目标。
* 我们导入： QAS & QCS体系以消除一切可能的质量隐患。

5.丰富的成功案例积累,深厚的项目实施经验

* 您 需 要： 业界翘楚的成功应用
* 我们执行：严格的项目管理体系
* 我们拥有：近十年服务经验、上百家客户的实施体会

人员是北信智科实际存在的生命力组成，人才是公司赖以生存和发展的基础。

北信智科的发展源自团队中每一位成员的贡献，向每一位成员提供应有的物质回报和精神需求的满足，将是北信智科不懈工作的努力目标和方向。

第二部分方案概述

* 1. **项目的需求**

1. 数据融合及治理

基于现有数据中心的数据进行质量探查、数据清洗、数据集成；执行数据标准规范和数据融合策略；解决数据不规范、标准不统一的数据质量问题、数据质量底下、数据使用者的决策依据不准确的问题；通过对数据的探查、清洗、去重、比对、监控和信息挖掘，提升数据质量。梳理数据来源、变更及审核机制。梳理学院部门之间数据资源产生、使用及管理的UC矩阵表。数据资源子集及说明表。

1. 决策分析

利用搭建数据中心的数据，将财务、科研、教师、学生、校友等方面数据进行分析。着重形成教师肖像，包含教师科研情况分析、项目成员关联分析、科研成果分析等方面，同时利用相关学生数据建立学生画像。根据为学院和各职能部门应用需要，利用数据分析与挖掘知识，实现学院财务等多方面统计信息的全面汇总分析，为院领导及相关部门提供丰富有效、高效可视的决策信息。

1. 教师工作绩效自动评估

教师工作绩效自动评估系统通过整合人事、科研、财务、教学等多门类数据信息，采用教师教学情况、经费效益、经费使用情况、项目完成情况、论文专著情况、案例情况、社会服务等多维度的评价因素，全方面呈现教师在科研和教学工作的成绩，从而为教师的入职、晋升、聘任、培训和奖惩提供定量化决策依据。为学院管理分析特色人才，精准扶持，争取各类资源，人才拔高等提供数据依据。

1. 教师人员关系图谱

团队合作是学院科研工作模式的重要组成部分，了解团队组成的关系对后续学院发展新项目、组件新项目团队以及评价项目团队合理性等方面提供极大帮助。基于学院数据中心提供的信息资源，利用数据挖掘与分析建立教师关系科研相关数据图谱，对学院科研发展提供决策分析。

1. 财务管理决策分析

支持与协同办公系统的数据集成，为学院决策分析提供预算执行情况分析报表、按项目核算报表等各类财务报表。

1. 教师肖像及学校教师一张表数据支持

为学校提供教师一张表学院级数据支持。建立学院级教师mis页面，每个教师登陆界面有个人基本信息，个人科研教学数据与学院平均值数据对比图谱及学院各类系统。并将该界面与学校mis系统集成。

1. 学生肖像及学校学生一张表数据支持

为学校提供学生一张表学院级学生数据支持。建立学生肖像及学生能力发展雷达图，支持学院学生及学生活动管理，丰富学生信息维度。支持学生行为异常监测、风险评估及预警。

1. 完善校友数据库，为校友服务提供数据支持。搭建校企合作模块，建立企业基本信息，企业来访及企业拜访记录，记录阶段性进展成果,教职工研究方向和科研项目与企业的发展相关性分析,校友企业拜访记录记录在校友数据库中。
2. 与学校、学院数据中心的集成，与学校大数据平台的集成，实现与统一

身份认证平台的对接，对接学校数据中心，集成教师、学生等数据。

1. 支持结构化及非结构化数据的存储，可对结构化数据进行决策分析。
2. 建立日常备份机制、运维体系，完成用户培训。
3. 三年内免费新版本升级及质量保证。
4. 需考虑对各个学院实施部署的通用性。

需提供驻场建设实施服务。

* 1. **对功能需求的理解**
     1. **对数据融合与治理的理解**

通过对北京交通大学智慧校园一期（以下简称“交大智慧一期”）学院数据中心功能分析，加强数据“融合性”、“统一性”、“稳定性”。可以利用BI工具定制报表，并实现下钻、导航、排序、求和、计算列等分析操作，得到有用的数据结果报表。

**1、定制报表**

各级用户可以在业务主题分析页面，定制报表包含的数据项、查询条件、图表类别、分析类别、异常阀值，将固定或通用的报表条件定义在参数化报表中，并作为报表模板存储；在生成报表时，可在报表模板基础上进行特殊的再定制，以减少重复定制的工作量，保证定制的灵活性。

**2、下钻**

“下钻”是在当前数据的基础上，查看更详细的数据。既可下钻某个成员，显示该成员所有子成员的信息；又可下钻某层次，显示该层次的所有成员信息。下钻可清楚了解当前维度参与查询的所有成员，选中成员的所有子成员或选中级别的所有成员。下钻后只显示下钻的成员，父成员及其兄弟成员的信息不再显示。

**3、导航**

相关报表之间可以按照当前报表表格交叉点的维度取值设置带参数的超级链接，传递到连接报表中显示相应的维度切块数据。

**4、排序**

提供按照某列数值升序、降序展示。

**5、求和**

按照维度父子关系显示子维度成员对应度量小计。

**6、计算列**

按照各种逻辑关系应用系统函数、条件语句，组织数据展示。

**7、筛选**

对维度成员进行筛选，得到需要的结果集。

**8、分析视图**

各级用户可以使用功能丰富的视图来进行数据分析。包括：图表、计量表、数据透视表、叙述、静态文本等。可以在部分视图中进行下钻、导航等操作。

* + 1. **对决策分析的理解**

本期项目的辅助决策分析是建立“数据融合与治理”的基础建设之上的。需要结合清洗、筛选、沉淀、融合后的数据进行分析，作出呈现趋势、关联的决策结果数据。本次需要对“数据融合与治理”后的学院多部门的信息数据汇总，部分功能为：教师工作绩效考核计算、教师人员关系的信息对称、财务统计管理与实施进度统计功能。

* + 1. **对教师肖像及学校教师一张表数据支持的理解**

需要与原有学校MIS系统进行数据接口对接，添加教师个人科研教学数据信息及学院各系平局值对比功能，以图表的形式展现。做到教师个人数据与系统数据同步类比功能。

* + 1. **对学生肖像及学校学生一张表数据支持的理解**

需要与原有学生管理系统对接，增添学院学生活动表单，建设录入、修改、删除等管理功能。通过学生成绩等信息数据的同步，扩展学生个人信息标的维度。对于超出指标的数据进行跟踪预警，增加消息提示和并通过手机向学生发送短信。

* + 1. **对完善校友数据库的理解**

增添校友信息数据库表单，开发校企合作信息功能模块包含：企业基本信息、企业来访及拜访记录、阶段性记录成果、教职工研究方向和科研项目与企业的发展相关性分析、校友企业拜访记录等。

* 1. **对数据集成需求的理解**

数据集成的过程是数据进入仓库的入口。数据集成过程所涉及到的数据源一般包括：联机事务处理系统的数据、外部数据源、脱机的数据存储介质等。从数据接口的方式来分，又可以分为数据库专用接口数据、ODBC数据源、格式化平台文件等。

针对提供的业务数据文件，数据导入层需要对这些数据进行必要的分析处理工作，包括对数据质量的检查，之后将数据加载到数据库中。

实际的数据集成过程包括如下图所示的四个部分：

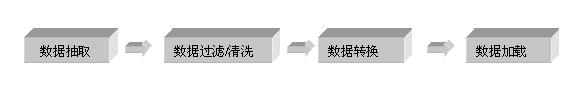


图 1 数据集成过程图

在技术上，数据集成过程主要涉及到：互连、复制、增量、转换、加载、调度和监控等几个方面。通常，数据仓库并不具有数据的实时性，即不要求与联机事务处理系统保持实时的同步，因此数据抽取可以定时批量进行，但多个抽取操作执行的时间、相互的顺序、成败对数据仓库中信息的有效性则至关重要。

具体到本期项目为与学校、学院数据中心的集成，与学校大数据平台的集成，实现与统一身份认证平台的对接，对接学校数据中心，集成教师、学生等数据。

* 1. **对非功能性需求的理解**

1、平台整合性

本项目是升级改造项目，要求升级后平台与原有系统是一体化整合、全信息集成的。

2、平台稳定性

要求平台整体及其各子系统具有稳定性，在各种情况下不会出现死机现象，更不能出现系统崩溃现象。

3、平台可靠性

要求平台数据维护、查询、分析、计算的正确性和准确性。

4、容错和自适应性能

对使用人员操作过程中出现的局部错序或可能导致信息丢失的操作，能推理纠正或给予正确的操作提示。对于关联信息采用自动套接方式按使用频度为用户预置缺省值。

5、易于维护性

要求平台的数据、业务维护方便、快捷。

6、安全性

要求保障平台数据安全、不易被侵入、干扰、窃取信息或破坏。

7、可扩展性

要求平台从规模上、功能上易于扩展和升级，制定可行的解决方案，预留相应的接口。除此之外，平台建设还需要实现与其他系统的集成，能够从其他系统中提取相应专业数据，为本系统服务。

8、适应性

平台在操作方式、运行环境、与其他软件的接口以及开发计划等发生变化时，应具有的适应能力。

1. 易用性

从界面布局、菜单的设计、及用户操作等方面，要遵循界面友好、直观，菜单简洁，菜单格式、快捷键等充分考虑用户习惯，满足用户使用方便的原则、易于修改。

* 1. **对平台性能要求的理解**

（1）页面展示及基本服务功能访问方面：响应速度不大于0.5秒；

（2）综合查询、统计类功能：响应速度不大于4秒；

（3）后台共享交换类和接入类功能：响应速度不大于8秒；

（4）稳定性方面：在利用本系统正常的工作中，不应出现妨碍工作顺利进行的系统错误或意外中止的情况；

（5）资源利用方面：在进行海量数据的查询、统计、分析的过程中，允许CPU和内存的占用率提升及网络带宽占有量的加大，但在操作结束后，应及时释放所占用的资源，以保证工作人员利用计算机顺利进行其它工作。

* 1. **对安全需求的理解**

从多方面建立全面的信息安全管理体系，有效防范内部和外部风险，保证平台信息安全。

* 1. **对实施要求的理解**

由于系统是基于已有交大智慧校园一期平台开发，对原有系统有很强的依赖性，因此在项目经验和服务品质上做如下要求：

（1）项目经验：

中标后尽快了解原系统架构，做好与原系统的一体化衔接，为升级改造提供良好的条件。

同类系统升级改造项目经验优先考虑。

同类系统开发、实施、集成经验优先考虑。

同类系统运维经验优先考虑。

（3）服务品质：

为了保障系统顺利开发、实施、上线我们要求中标单位按照以下标准施工（没有取得该资格的按照以下标准进行开发、实施）：

能够提供优质的本地化服务，派专门技术人员现场开发、维护。

建议项目承担方在项目开发、实施与技术支持的过程中，以ISO9001:2000质量体系作为提供优质服务的标准和保障，取得ISO9001:2000质量体系认证的作为更优保障条件。

建议项目承担方在软件研发管理能力、产品与服务质量等方面全面接轨国际标准和水平，承担方通过CMMI3及以上级别认证的作为更优保障条件。

由于该平台关联对接的外部系统较多，并且对软硬件集成的能力要求较高，因此具备计算机系统集成企业资质的优先考虑，资质越高优先级越高。

* 1. **设计标准和质量保证**

1.北信智科提供的所有产品，其制造商应有完善的质量检测手段和质量保证体系，产品须符合国家标准和行业标准。

2.北信智科提供的所有技术文件中的技术指标除非在技术规格中另作规定外，均应符合相应的国家标准，行业标准和国际标准。

3.北信智科所提供产品的设计在结构上实现开放性，基于国际开放式标准，包括各种广域网、局域网、计算机及数据库协议，符合国家和信息产业部的规范，符合工信部关于网站设计无障碍技术要求（YDT/1761-2012）

4.自验收合格并签署验收文件后开始计算质量保证期。北信智科提供的质量保证期不得少于12个月，且需指派至少一名工程师支持应需进行现场维护。具体保修时间和保修期内的服务北信智科须在投标文件中有详细说明。

* 1. **培训要求的理解**

1．提供现场使用培训；培训内容包含使用人员系统操作和系统管理维护人员安装、维护等。

2．投标人在投标文件中应详细说明具体培训的组织、方案等。

* 1. **技术服务要求**

1.应保证系统的使用正常。质保期内，接到买方通知后须在3小时内做出响应，有必要的需到达现场维护。

2.投标人应在投标文件中声明能够提供的其他技术支持与运维服务标准。

3.应用软件在验收合格后，投标方必须提供合同需求功能范围内的至少一年的免费功能增强性维护（增加、修改、数据维护）（大版本升级除外）及免费技术维护服务（其中包括系统维护、跟踪检测），保证用户购买的应用软件正常运行。

* 1. **工期及验收标准**

1.本项目工期要求：自签订合同起到项目交付运行6个月。

2.验收标准：双方按照合同规定的标准和程序，在工期结束后由甲方指定验收地点和时间进行验收。承诺保证在合同规定时间内本期新建系统平稳运行。系统满足合同范围内的所有功能要求以签署验收文档视为验收合格。

* 1. **方案设计概述**
     1. **方案特点**

本方案主要特点总结如下：

**1、基础设施充分利旧**

机房中的网络、安全以及存储软硬件设备均可利旧。本方案充分利旧，充分考虑利用现有共享交换平台资源和渠道，利用共享交换平台与相关机构连通的前置服务器搭载数据匹配应用，在保护原有投资的基础上，节约成本，实现效益最大化。

**2、总体架构层次清晰**

方案总体架构采用三层应用体系，具有层次结构清晰、采用统一框架结构易于扩展和部署以及统一数据易于利用的设计特色。三层应用体系结构包含表示层、业务逻辑层、数据层。在三层结构中，三个层可以分别部署，表示层用户界面只能与业务逻辑层相联系，无需直接访问后台数据库，使后台数据库与用户界面隔离，提高应用系统的可靠性和扩展性，提高系统数据的安全性。

**3、系统性能最大优化**

本方案在网络带宽、主机配置、应用服务、应用服务器部署、应用代码、数据服务和数据库性能等方面提出了系统性能优化方案，保障系统运行满足各级用户的需求。

**4、保障体系建立完善**

本方案建立了完备的安全保障体系，标准、规范及制度建设方案，项目实施组织计划及进度安排，质量保障体系，项目培训方案及项目保密措施等一系列项目保障体系，保证本次项目按时保质保量完成。

* + 1. **方案优势**

本次项目方案在国家和北京市政策法规的指导下进行建设，符合国际开放技术标准与规范，总体设计遵循总体规划、分布实施原则、安全可靠原则、先进性原则、标准性原则、可扩展性原则和实用性与易管理性原则。

考虑原有交大智慧校园一期系统现状，系统技术线路选择采用基于SOA框架，基于B/S/D三层结构开发应用系统，全面应用XML技术及Web Service技术，基于UML 2.0进行系统建模，实现信息融合共享。

方案总体架构具有层次结构清晰、采用统一框架结构易于扩展和部署以及统一数据易于利用的设计特色。

主体方案融合需求分析、总体设计、性能设计、系统安全设计、应用系统设计、业务支撑平台设计、数据资源库设计、网络及硬件系统设计、系统集成方案、质量保证方案、项目测试、验收、培训方案、技术支持与售后服务方案各方面于一体之中。

* + 1. **公司领导高度重视**

北信智科一直将电子政务作为公司的核心发展方向，公司越来越重视解决方案的成功实施。不仅要帮助客户把握信息化的发展方向，也要做到在满足客户需求的同时，结合公司业务，不断完善技术架构，保证公司在电子政务系统建设方面的可持续发展。本项目由北信智科副总亲自带队，成立项目领导小组，对项目过程进行全程监督，保证资源的充足以及资源调用的及时性和可靠性。

* + 1. **专业化项目建设团队**

公司承诺为项目提供充足的专职、全程建设人员，保证本期项目的按时保质完成，公司会为项目安排合理的项目团队人员、配备科学的项目建设设备，同时保证足够的人力、物力及财力调配权。

* + 1. **需求的理解与变更、控制能力**

为了保证对项目需求的正确理解，公司会根据客户的需求对系统持续改进，直到确定客户满意为止；根据往年的项目经验总结，北信智科已经总结了一套比较成熟的需求管理流程和方法，来进行需求的变更与控制。

* + 1. **规范化项目管理**

北信智科承诺：在项目实施过程中，将严格遵守项目和软件系统的实施规范。并将公司在其他信息化系统建设中积累和总结的目标责任体系融合在本期项目实施管理工作中。同时希望客户方可以全力配合以及遵守制定的相关标准规范，以保证项目的顺利实施。

* + 1. **高标准质量保证**

项目中的产品采购、软件开发与集成等工作，均依据合同，在规定的时间内，满足功能、性能、技术指标要求，并保证产品的质量。

公司的质量方针是：科学、高效、求实、创新。

在质量目标控制中采用PDCA循环，即：Plan（计划）-Do（执行）-Check（检查）-Action（行动）。

控制者（包括项目经理和各工作小组经理）进行控制的过程是从反馈过程得到控制系统的信息后，便着手制定计划，采取措施，输入受控系统，在输入资源转化为产品的过程中，对受控系统进行检查、监督，并与计划或标准进行比较，发现偏差进行直接修正，或通过信息反馈修正计划或标准，开始新一轮控制循环。

计划：确保所有的实施活动都在一个计划指导下进行。

执行：确保所有计划内的活动都能得到有效地执行。

检查：确保所有执行的活动都准确无误。

措施：确保所有执行中的问题都有相应的措施，并无一遗漏地落实，然后进入下一个PDCA循环。

在工作中严格执行ISO9000质量标准和业主单位关于本次应用系统开发与集成制定的相关质量标准。具体来说，质量承诺包括：

1、管理职责

公司承诺并确保管理职责已经确立并被有关人员正确理解，承诺并确保质量体系中的要素都有相应工作小组和人员负责并执行，保证管理职责能够按规定得到贯彻。

2、质量体系

为完成各项质量活动，按照国家标准和国际惯例并结合业主的实际情况，我们承诺并确保建立适宜的文件化质量体系，质量体系覆盖软件产品的生存周期全过程，以确保软件产品的质量。

3、合同评审与执行

合同对于软件项目的确立、明确供需双方的权利和义务、组织开发和售后服务等活动有指导性的意义。公司承诺并确保严格按照合同的规定和要求，在预期的资源内实现对业主方的承诺。

4、设计控制

公司承诺并确保对软件的设计开发进行控制和验证，以确保满足规定的要求。

5、文件和资料控制

公司承诺并确保软件开发的各级组织能够发布和使用适当的文件，并实行有效的管理，使员工能方便、有效地共享信息。

6、采购

公司承诺并确保采购的与软件产品质量有关的软件工具受到控制，保证分承包商提供的服务符合规定的要求。

7、提供对业主提供产品的验证

公司承诺并确保对业主提供产品的评价、验收、存储、使用和维护加以控制，以保证最终集成的应用软件系统的质量。

8、产品标识和可追溯性

公司承诺并确保提供一个标识、控制和追踪每个软件项的正式版本的机制，使产品的变化过程具有可视性，并确保各工作小组的每个工作人员在软件产品生存周期中的任何时刻都能采用正确的信息。

9、过程控制

公司承诺并确保所开发的软件产品在开发、复制、安装和维护等过程中全面受控，并保证最终产品的质量。

10、检验与试验

公司承诺并确保对所开发的软件产品进行检验和试验，确保其满足合同和需求规格说明所规定的要求。

11、检验、测量和试验设备的控制

公司承诺并确保对软件开发所采用的工具、技术、惯例和约定进行控制，确保软件产品的质量能满足规定的要求。

12、检验与试验状态

公司承诺并确保对软件项进行适当的标识，确保通过检验和测试的软件项在经过批准后才能进入下一阶段的工作。

13、不合格品的控制

公司承诺并确保对不合格的产品进行标识和隔离，防止不合格产品的非预期使用和安装。

14、纠正与预防措施

公司承诺并确保贯彻以预防为主的原则，及时采用有效措施，纠正和预防质量问题，分析和确定问题的产生原因，预防问题的再发生，不断提高服务质量。

15、搬运、储存、包装、防护和交付

公司承诺并确保对所开发的软件产品在搬运、储存、包装、防护和交付工程进行控制，承诺并确保软件产品的质量在这些过程中不会受到影响。

16、质量记录的控制

公司承诺并确保对质量记录进行控制和管理，为有追溯性要求的场合和采取纠正措施与预防措施提供证实，为产品质量符合规定要求和体系的有效运行提供证据。

17、内部质量审核

公司承诺并确保检查质量体系运行的符合性和有效性，以及质量体系文件的适宜性和有效性，及时采取预防和纠正措施，避免可能出现的问题和缺陷。

18、培训

公司承诺并确保对各工作小组的组员及与其有关的组员进行相关技术与技能的培训及质量管理培训，以保证所受培训的人员在软件开发和管理过程中具备相应的资格和能力。

公司承诺并确保对本期项目使用用户进行以下培训：

1)产品培训

2)系统软件管理员培训

3)系统的应用管理维护培训

4)系统操作人员培训。

5)项目标准培训

通过各项培训工作和交流活动，除达到所有相关人员的操作使用要求外，最主要的是使业主方的相关技术人员能够全面的了解和掌握系统的所有设计思路、实现方式、技术细节等内容，以最终达到中心技术人员对系统自主维护、自主定制、自主修改、自主升级等要求。

19、服务

公司承诺并确保软件产品在初次交付和安装后，为用户有效的服务，按照合同的规定对软件产品进行有效的维护。

* + 1. **完备的售后服务**

针对本项目，北信智科如果中标将承诺履行以下售后服务的承诺条款：

* 质量保证期限：系统验收合格、双方签署验收书之日起，提供1年免费维护服务。1年免费服务到期后，北信智科应承诺对系统的升级仅收取成本费。
* 北信智科需要提供详细的售后服务方案，包括服务人员、服务内容和措施、应急预案等内容。
* 服务响应时间：提供每周7×24小时电话咨询服务，重大故障2小时内乙方维修人员到现场处理。
* 项目验收完毕后，北信智科承诺通过定期电话、现场巡检等方式跟踪系统使用情况，听取用户意见和建议，及时分析系统存在的问题，并随时给予解决。必要时，承诺派遣技术人员去现场解决存在的问题。
* 质量保证期内，北信智科承诺会及时向用户通报系统软件升级情况，若用户需要对系统软件升级，北信智科将尽量在不影响用户使用现有系统的情况下，科学安排升级步骤，确保提供最新升级版本和相应的系统升级技术服务。
  + 1. **保密承诺**

北信智科公司同意并严格按照《招标文件》中中标合同中对安全保密协议的要求和内容执行。承诺并保证对开发中涉及的相关信息保密，未经甲方许可，绝不将将系统相关信息泄露给第三方。

第三部分性能设计方案

* 1. **系统稳定性设计**

在利用本系统正常的工作中，不应出现妨碍工作顺利进行的系统错误或意外中止的情况；系统采用高可用集群架构部署，对于单个节点的设备故障，应能够瞬时自动将负载切换到其他节点，保证系统正常运行。

同时，除了大量充分的测试以外，在设计上必须有针对可靠性的设计，基本原则是在尽量保证各服务可靠的基础之上，通过一个健壮的体系结构来确保系统能够在硬件和软件出错的情况下依然平稳的运行。本项目在考虑系统稳定性时采用以下设计。保证平台整体及其各系统具有稳定性，在各种情况下不出现死机现象，更不能出现系统崩溃现象。

* 1. **系统可靠性设计**

本期项目在数据维护、查询、分析、计算的正确性和准确性方面，应满足向各类用户提供7×24小时的不间断服务的要求。为实现系统可靠性。

* + 1. **避错设计**

避错设计原则是控制和减少程序的复杂性，体现了以预防为主的思想，在各个阶段都进行避错。

避错准则：

* 模块化与模块独立；
* 抽象和逐步求精；
* 信息隐蔽和局部化；
* 慎重使用容易引入缺陷的结构和技术。
  + 1. **查错设计**

查错设计是指在设计中赋予程序某些特殊的功能，是程序在运行中自动查找存在错误的一种设计方法。

* 被动式错误检测：在程序的若干部位设置检测点，等待错误征兆的出现。

检测原则：相互怀疑原则、立即检测原则。

* 主动式错误检测：对程序状态主动进行检查
  + 1. **容错设计**

容错设计是指在设计中赋予程序某种特殊的功能，使程序在错误已被处罚的情况下，系统仍然具有正常运行能力的一种设计方法。

容错内容包括：时间容错、结构容错、信息容错。

* + 1. **改错设计**

改错设计是指在设计中，赋予程序自我改正错误、减少错误危害程度的能力的一种设计方法。

采用权限最小化原则实现故障隔离。为了限制故障的蔓延，要求对过程和数据加以严格的定义和限制。例如，针对操作系统的故障隔离方法：不允许一个用户的应用程序引用或修改其他用户的应用程序或数据。绝对不允许一个应用程序引用或修改操作系统的编码或操作系统内部的数据等。

* 1. **系统容错和自适应性设计**

对使用人员操作过程中出现的误操作或可能导致信息丢失的操作，能给予正确的操作提示。因此本次开发中针对易出错点进行对应的信息提示，提示内容分为：引导性信息提示、错误操作类型提示、提供帮助性提示等。

* 1. **系统易维护性设计**

为保证平台的数据、业务维护方便、快捷，主要有以下设计：

1、系统日志输出应完整清晰，能够根据系统主要标识，通过日志定位系统问题。

2、用户界面提示信息简单易懂，信息能够为用户提供指导，便于用户下一步操作。

3、如出现致命问题，提示信息应显示详细，便于维护人员排查、解决问题。

4、系统代码应符合使用语言规范。

* + 1. **系统安全性设计**

系统安全性设计力求保障平台数据安全、不易被侵入、干扰、窃取或破坏。具备防病毒、黑客入侵监测和预警、漏洞扫描、网络监测与自动修复、身份认证、敏感信息密文存储和传输等功能；系统还应提供合理有效的数据备份、恢复策略和保护机制。

* + 1. **数据安全**

数据安全应具有如下能力：

* 屏蔽掉数据库系统中默认账户和默认口令。
* 自主访问控制（DAC）：DAC用来决定用户是否有权访问数据库对象。
* 验证：保证只有授权的合法用户才能注册和访问。
* 授权：对不同的用户访问数据库授予不同的权限。
* 审计：监视各用户对数据库施加的动作。
* 数据库管理软件应能够提供与安全相关事件的审计能力：试图改变访问控制许可权；试图创建、拷贝、清除或执行数据库。
* 系统应提供在数据库级和纪录级标识数据库信息的能力。
* 数据备份与灾难恢复的能力。
  + 1. **数据安全解决方案**

数据安全指数据的完整性、机密性、可用性，可分为数据存储安全和数据传输安全。

* + 1. **数据存储安全**

数据存储安全包括防止数据丢失、损坏和非授权访问、篡改，涉及物理、网络、系统、应用和管理五个层面，数据物理层安全通过设备备份解决，网络系统层面通过容灾备份和访问控制解决，应用层面通过加密和访问控制解决，管理层面通过制度约束，防止非授权拷贝来解决。解决数据存储安全最有效的方法是加密存储并结合访问控制和数据备份，为避免过度防护，保证访问的快捷性，系统的数据将不进行加密存储保护，只通过访问控制和数据备份来满足其存储安全需要。

* + 1. **数据传输安全**

数据传输安全是指数据在传输过程中的完整性和机密性保护。目前在系统中需要进行数据传输保护有：交换服务器与相关应用之间的数据传输、数据库服务器与各服务应用之间的数据传输。

* + 1. **安全日志**

通过开启操作系统、数据库自身的审计模块来实现日志审计，同时利用日志审计系统，集中将操作系统、数据库的日志信息传递到日志审计平台，具体审计措施包括：

* 操作系统审计

1. 审计功能开启和关闭；
2. 系统登录行为；
3. 对服务器的维护行为；
4. 对服务器访问的时间、类型、主体标识（访问者账号、IP地址）；
5. 重要的系统管理行为。

* 数据库审计

1. 审计功能的开启和关闭；
2. 对数据库的管理、维护行为；
3. 对数据库访问的时间、类型、主体标识（访问者账号、IP地址）。

* 行为审计

针对访问行为，审计记录至少包含审计事件的时间、类型、主体标识、客体信息、事件结果等事件相关信息。

* 审计记录的查看和分析

针对所审查的审计记录，提供必要的工具（系统自带的功能模块或辅助工具）以查看审计信息，能够提供多种查看方式（排序、分类）；对审计记录进行导出和关联性分析。

* 网络安全

核心数据中心区域增加备份磁盘阵列，采取双机热备策略，主磁盘阵列容量小，备份磁盘阵列容量大。

* 1. **系统可扩展性设计**
     1. **可扩展性接口设计**

本期项目建设项目需要实现内外部应用系统的对接，为保障系统具备良好的对接扩展性，系统采取多元化的接口设计，以满足不同类型的内外部对接需求。使得平台从架构上、功能上易于扩展和升级，应制定可行的解决方案，预留相应的接口。除此之外，平台建设还实现与其他系统的集成，能够从其他系统中提取相应专业数据，为本系统服务。相关的功能模块，如数据分析、比对等功能应具有松耦合性，能够为其它系统或平台所用。

* 平台内部组件接口

本期项目建设项目采用java组件化开发，遵循面向对象的设计开发理念。在自下而上的设计过程中，规划全局资源，确定边界条件，设计出交互过程和用户接口，保证接口的规范性、个移植性、鲁棒性、安全性、兼容性。在设计JAVA接口时严格遵循“缺省适配模式”，提供缺省抽象类的实现，严格规范外部组件使用接口，组件内部使用抽象类。

* 面向外部的接口

在与外部系统之间开发数据接口可根据时间的容忍程度规划为下面两种方式：

定时交换的数据集成接口：双方先约定数据交换格式（数据抽取方式、数据转换方式、数据加载方式），使用ETL工具进行数据的抽取转换加载，完成数据交换工作；或使用中间转换格式文件，由数据源系统导出固定格式的数据文件，数据目的系统导入该数据文件。

实时交互的Web Services接口：目的应用系统和数据源应用系统先约定数据接口API（通常为web services模式），然后由目的应用系统或数据源应用系统实现数据接口API，最后由一方（目的应用系统或数据源应用系统）填写程序调用另一方提供的数据接口API将数据加载或推送到自己的数据库中。在这种方式下，数据加载或推送流程与数据接口API调用方原有的业务或程序流程完全融合在一起。

* 接口可扩展

我们在解决问题的总方向是将复杂问题简单化，在这个总方向的指引下，广泛采用设计模式来达到最大限度的重用，在设计时尽可能的简单明了。在具体实施设计过程中，我们会将简单问题复杂化，落实到每个类的具体实现上要真正能体现系统事物的本质特征，因为事物的本质特征只有一个，代码越接近它，表示设计就是简单明了，越简单明了，系统就越可靠。更多情况是，一个类并不能反应事物本质，需要多个类的组合协调，那么能够正确使用合适的设计模式就成为重中之重。

本期项目建设项目项目将采用面向构件的系统分析与设计方法。使用构件技术的系统搭建模式建设一个综合性松耦合的、复合体系结构型系统。

* 接口可配置

接口部分采用适配开发模式，适配器的主要功能是调用其它子系统提供的接口函数，访问数据库，实现通信基础通用平台接口的功能。系统根据其它子系统提供的接口函数，实现平台接口的功能，并封装处理成数据适配器输出数据，由于不同的子系统都用于自己独立的接口函数，系统必须为每个子系统设计数据适配器。通信基础通用平台在整合数据适配器的过程中，采用SOA（面向服务的体系结构）架构设计，将应用程序的不同功能单元（称为服务）通过这些服务之间定义良好的接口和契约联系起来；同时，平台提供其他子系统的预留接口，为企业的业务发展提供强有力的技术支撑。

* + 1. **可扩展性数据交换**

系统全面采用XML、Web Service技术进行数据、服务描述及数据交换。

XML（eXtensible Markup Language,可扩展标记语言）是Internet上数据表示和数据交换的新标准。它是ISO（International Organization for Standardization，国际标准化组织）的SGML（Standard for General Markup Language，通用标记语言标准）的一个简化子集。XML关注信息本身，是Web上表示结构化信息的一种标准文本格式。与传统的注重页面信息显示的HTML（Hypertext Markup Language, 超文本链接标示语言）相比，关注于内容的XML具有诸多优点：良好的可扩展性，语言简单有效，可自行定义标记；内容与形式的分离，主要刻画数据内容，不考虑显示效果；有严格的语法要求，便于分析统一和与数据库信息转换；便于传输，为纯文本形式，可通过Http协议直接传输，可跨越防火墙；等等。

* + 1. **可扩展性应用架构**

应用J2EE架构，保证系统可移植性和可扩展性，使应用基于XML和SOAP的 Web Service技术，能够实现XML到数据库、数据库到XML和数据库到数据库之间的数据交换和共享，完全实现了跨平台操作、支持各种异构数据库的动态数据交换功能。

* + 1. **可扩展性技术架构**

系统采用SOA总体架构和可配置的构件技术，基于三层结构的系统实现，能够快速的响应业务需求和外部环境变化导致的系统变更。

* + 1. **可扩展性支撑平台**

根据服务平台的应用中间件的要求，从产品的稳定性、可扩展性、标准性、高可用性、安全性为原则来进行选型，充分利用J2EE应用中间件服务器，以HA方式部署支持今后业务增长添置新的应用服务器的需求。

* 基于SOA架构的系统技术框架

SOA（service-oriented architecture，面向服务的体系结构或面向服务架构）是指为了解决在Internet环境下业务集成的需要，通过连接能完成特定任务的独立功能实体实现的一种软件系统架构。SOA是一个构件模型，它将应用程序的不同功能单元（称为服务）通过这些服务之间定义良好的接口和契约联系起来。接口是采用中立的方式进行定义的，它应该独立于实现服务的硬件平台、操作系统和编程语言。这使得构建在各种这样的系统中的服务可以以一种统一和通用的方式进行交互。

传统的Web（HTML/HTTP）技术有效的解决了人与信息系统的交互和沟通问题，极大的促进了B2C模式的发展。WEB服务(XML/SOAP/WSDL）技术则是要有效的解决信息系统之间的交互和沟通问题，促进B2B/EAI/CB2C的发展。SOA则是采用面向服务的商业建模技术和WEB服务技术，实现系统之间的松耦合，实现系统之间的整合与协同。WEB服务和SOA的本质思路在于使得信息系统个体在能够沟通的基础上形成协同工作。

对于面向同步和异步应用的，基于请求/响应模式的分布式计算来说，SOA是一场革命。一个应用程序的业务逻辑或某些单独的功能被模块化并作为服务呈现给消费者或客户端。这些服务的关键是他们的松耦合特性。例如，服务的接口和实现相独立。应用开发人员或者系统集成者可以通过组合一个或多个服务来构建应用，而无须理解服务的底层实现。

在传统的系统体系架构中，系统功能的调整与完善极大依赖开发商，当业务需求发生变化、或不同开发商设计的系统需要集成时，往往需要极大的代价才能完成新系统的集成，甚至有时只能完全推翻原有的设计，这非常不利于保护和利用既有投资。

基于SOA的系统架构将屏蔽由于开发商选择的开发环境和手段不同带来的风险，而是将业务需求拆分到基本服务单元，做到了最大程度地柔性面对需求变化，不仅满足现在的需求，同时也增强了系统在未来的抗风险性。

* 基于Web Service的应用系统整合

系统平台的架构应该满足三个方面的应用整合需要，它们分别是：整合基本用户业务之间的业务流程和数据资源；整合基本业务与GIS等其他之间的数据资源；整合新建的信息系统与原有信息系统之间的软、硬件及数据资源。新一代的互联网技术Web Service是构建这种架构的最佳方案。

Web Service是下一代的WWW，它允许在Web站点上放置可编程的元素，能进行基于Web的分布式计算和处理。Web Service是封装成单个实体并发布到网络上供其他程序使用的功能集合。Web Service是用于创建开放分布式系统的构件。

1、Web Service可以方便地集成应用系统

异构系统间的连接，是今后系统构筑的最重要的课题之一。各个系统间不是孤立的、而是使其相互连接起来，这是最大限度享受由信息技术应用所带来的高效率、低成本实惠的前提。Web Service是解决这个问题的一种有效技术。

用户应用程序开发者都知道，在用户业务里经常要把用不同语言写成的、在不同平台上运行的各种应用程序集成起来，而这种集成将花费很大的精力。应用程序经常需要从运行在IBM主机上的程序中获取数据；或者把数据发送到HP主机或UNIX应用程序中去。即使在同一个平台上，不同软件厂商生产的各种软件也常常需要集成起来。通过Web Service，应用程序可以用标准的方法把功能和数据“暴露”出来，供其它应用程序使用。

2、Web Service是下一代分布式系统的核心

它具有如下特点：

（1）互操作性：任何的 Web Service都可以与其他Web Service进行交互。由于有了SOAP（Simple Object Access Protocol）这个所有主要供应商都支持的新标准协议，因而避免了在CORBA、DCOM 和其他协议之间转换的麻烦。还因为可以使用任何语言来编写Web Service，因此开发者无需更改其开发环境，就可生产和使用Web Service。

（2）普遍性：Web Service使用HTTP和XML进行通信。因此，任何支持这些技术的设备都可以拥有和访问Web Service。

（3）易于使用：Web Service背后的概念易于理解，并且有来自IBM和微软这样的供应商的免费工具箱能够让开发者快速创建和部署Web Service。此外，其中的某些工具箱还可以让已有的COM组件和JavaBean方便地成为Web Service。

（4）行业支持：所有主要的供应商都支持SOAP和周边Web Service技术。例如，微软的.Net平台就基于Web Service，因此用Visual Basic编写的组件很容易作为Web Service部署，并可以被IBM VisualAge 编写的Web Service使用。

3、简单对象访问协议----SOAP

Web service建好以后，你或者其他人就会去调用它。简单对象访问协议(SOAP)提供了标准的RPC方法来调用Web service。实际上，SOAP在这里有点用词不当：它意味着下面的Web service是以对象的方式表示的，但事实并不一定如此：你完全可以把你的Web service写成一系列的C函数，并仍然使用SOAP进行调用。SOAP规范定义了SOAP消息的格式，以及怎样通过HTTP协议来使用SOAP。SOAP也是基于XML和XSD的，XML是SOAP的数据编码方式。

4、Web service描述语言WSDL

Web Services Description Language的缩写，是一个用来描述Web服务和说明如何与Web服务通信的XML语言，为用户提供详细的接口说明书。WSDL元素基于XML语法描述了与服务进行交互的基本元素：

Type（消息类型）：数据类型定义的容器，它使用某种类型系统（如XSD）。

Message（消息）：通信数据的抽象类型化定义，它由一个或者多个part组成。

Operation(操作)：对服务所支持的操作进行抽象描述。

Port Type（端口类型）：特定端口类型的具体协议和数据格式规范。

Binding：特定端口类型的具体协议和数据格式规范

Port ：定义为绑定和网络地址组合的单个端点。

5、服务描述和商业注册机制--UDDI

UDDI（统一描述、发现和集成协议）计划是一个广泛的，开放的行业计划，它使得服务机构能够 (1) 彼此发现，(2) 定义他们怎样在internet上互相作用，并在一个全球的注册体系架构中共享信息。UDDI是这样一种基础的系统构筑模块，它使单位和个人能够快速，方便地使用他们自身的应用软件来发现合适的服务机构，并与其实施电子化的信息查询和业务办理。

UDDI同时也是Web Service集成的一个体系框架。它包含了服务描述与发现的标准规范。UDDI规范利用了W3C和Internet工程任务组织(IETF)的很多标准作为其实现基础，比如扩展标注语言（XML），HTTP和域名服务(DNS)这些协议。另外，在跨平台的设计特性中，UDDI主要采用了已经被提议给W3C的SOAP(Simple Object Access Protocol，简单对象访问协议)规范的早期版本。

UDDI将会给每一个服务描述和服务机构注册分配一个递增的，唯一的标识符，并且把它们存储在注册中心的数据市场和搜索引擎中。单位和个人可以查询此注册中心，以发现其用户部门的Web服务，从而建立一种业务关系。

通过使用 UDDI 注册服务机构、自定义 tModel 和 Web 服务，您可以帮助世界各地的开发人员找到您的 Web 服务。UDDI 注册表允许您发布的不只是 Web 服务端点和业务数据。使用 UDDI 的用户也可以使用该界面查找 Web 服务文档和示例。Microsoft UDDI 注册表是免费使用的。鼓励用户使用此注册表注册您的 Web 服务和机构。

6、Web Service可以提高应用软件的开发效率

在三层结构的系统中，如果中间层组件换成Web Service的话，可以直接使用Microsoft SOAP Toolkit或.NET这样的SOAP客户端，也可以使用自己开发的SOAP客户端，然后把它和应用程序连接起来。不仅缩短了开发周期，还减少了代码复杂度，并能够增强应用程序的可维护性。同时，应用程序也不再需要在每次调用中间层组件时，都跳转到相应的“结果页”。

从经验来看，在一个用户界面和中间层有较多交互的应用程序中，使用Web Service这种结构，可以节省花在用户界面编程上20%的开发时间。另外，这样一个由Web Service组成的中间层，完全可以在应用程序集成或其它场合下重用。最后，通过Web Service把应用程序的逻辑和数据“暴露”出来，还可以让其它平台上的客户重用这些应用程序。

7、Web Service可以实现软件和数据重用

软件重用是一个很大的主题，重用的形式很多，重用的程度有大有小。最基本的形式是源代码模块或者类一级的重用，另一种形式是二进制形式的组件重用。

当前，像表格控件或用户界面控件这样的可重用软件组件，在市场上都占有很大的份额。但这类软件的重用有一个很大的限制，就是重用仅限于代码，数据不能重用。原因在于，发布组件甚至源代码都比较容易，但要发布数据就没那么容易，除非是不会经常变化的静态数据。

Web Service在允许重用代码的同时，可以重用代码背后的数据。使用Web Service，再也不必像以前那样，要先从第三方购买、安装软件组件，再从应用程序中调用这些组件；只需要直接调用远端的Web Service就可以了。举个例子，要在应用程序中确认用户输入的地址，只需把这个地址直接发送给相应的Web Service，这个Web Service 就会帮你查阅街道地址、城市、省区和邮政编码等信息，确认这个地址是否在相应的邮政编码区域。Web Service 的提供商可以按时间或使用次数来对这项服务进行收费。这样的服务要通过组件重用来实现是不可能的，那样的话你必须下载并安装好包含街道地址、城市、省区和邮政编码等信息的数据库，而且这个数据库还是不能实时更新的。

另一种软件重用的情况是，把好几个应用程序的功能集成起来。现在Web上有很多应用程序供应商，都在其应用中实现了这些功能。一旦他们把这些功能都通过Web Service “暴露”出来，就可以非常容易地把所有这些功能都集成到你的门户站点中，为用户提供一个统一的、友好的界面。

将来，许多应用程序都会利用Web Service，把当前基于组件的应用程序结构扩展为组件/Web Service的混合结构，可以在应用程序中使用第三方的Web Service 提供的功能，也可以把自己的应用程序功能通过Web Service 提供给别人。两种情况下，都可以重用代码和代码背后的数据。

8、SOAP的安全扩展满足安全要求

自从SOAP规范发布以来， SOAP规范的加密性，认证和授权等安全机制一直受到人们的广泛关注。这几个方面对于任何的网上业务系统来说都是很重要的 ，但SOAP标准在制定规范时并没有过多考虑SOAP 的安全性要求。因为SOAP一个很重要的设计目标就在于它的简单性，尽可能的利用已有的标准和协议来实现相应的功能，而不是另起炉灶，重新定义一个崭新的协议，如果这样的话，会大大的降低它的实用性和兼容性。

安全性是个复杂的问题，在最低层SOAP 消息可通过 HTTPS 传递， 通用 SSL 传输信息，这就确保被编码消息内容可以避免被窃听，也确保客户端和服务器可互相验证身份。尽管 HTTPS 解决了对窃听者屏蔽消息的问题，但不能满足安全性更高的特殊用户认证的特定 Web 服务的要求。比如下面需要SOAP安全的几个场景，仅仅依靠SSL的安全机制是不满足信息的安全要求的：

（1）端对端的信息传送（End-to-end messaging）

SOAP消息可以与不同的运输层协议（如HTTP，SMTP等）捆绑在一起进行传输，传输的过程中可能经过一系列中间设备或应用程序，假如应用程序对SOAP消息进行恶意破坏，可以在SOAP消息插入一系列相似的头元素，再传给下一个中间设备或程序，从而破坏了信息的完整性。在这种情况之下，中间设备或应用程序是不值得完全信任的，它们随时可以修改传输的信息。因此，SSL/TLS并不能保证端到端传输的安全性。

（2）中间件的独立性（Middleware independence）

在应用层中保证端对端的安全要求，如果在传输中的传输的消息是平文，而不是是经过加密 的密文，极易受到黑客的攻击。但假如在应用程序中进行安全加密的处理，需要用户对加密算法有详细的了解，有许多不同的加密算法适合不同的安全要求，这对于用户来说是额外的负担。因此，标准的，安全的，独立的，透明的运输层是必要的，在SOAP中进行适当的安全扩展，保证了中间件应用程序的独立性，不用考虑过多的加密算法细节。

（3）传输的独立性（Transport independence）

SOAP消息在传输的时候可以与不同的运输层协议进行捆绑，如HTTP，SMTP协议，有可能存在这么一个场景，所有的通信连接是安全的，中间层应用程序也是值得信赖的，但是，安全信息需要经过两个运输层协议，比如前一段是经过HTTP协议传输，在下一个阶段，则需要通过SMTP协议进行传输，两者之间的转换是烦琐的，易出错的。因此，在SOAP中加入扩展信息，保证了运输层的独立性，从而使与运输层无关。

（4）驻留信息的安全性

运输层可以进行安全传输，但不能保证信息驻留时也是安全的。假如消息保存后继续向前传输，驻留信息的安全十分重要。在电子商务中，常常要求用户填写帐号和密码，这些信息通常保留在本地的COOKIE中，对于这些持久保存的信息进行加密，可通过SOAP的安全扩展来实现。

本期项目建设项目项目将基于Web Service技术整合各系统。

* 1. **系统适应性设计**

平台在操作方式、运行环境、与其他软件的接口以及开发计划等发生变化时，应具有的适应能力。

本次设计开发中为保证系统适应性采用常用SOA的体系结构，使用J2EE多层分布式架构开发，并在接口设计时正确处理后续建设工作的合理对接，增强平台的可扩展性和适应性，用信息标准数据接口规范规定了平台基础数据库与外部系统进行信息交换时应遵循的有关信息格式和数据管理规定。

* 1. **系统易用性设计**

从界面布局、菜单设计及用户操作等方面，遵循界面友好、直观；菜单布局、快捷键等设置充分考虑用户习惯，力求简洁友好、易用。因此系统易用性设计包含以下部分。

* 基于MVC的设计模式

系统借助MVC模式实现Web系统的职能分工。

Model层实现系统中的业务逻辑，通常可以用JavaBean或EJB来实现。 View层用于与用户的交互，通常用JSP来实现。 Controller层是Model与View之间沟通的桥梁，它可以分派用户的请求并选择恰当的视图以用于显示，同时它也可以解释用户的输入并将它们映射为模型层可执行的操作。

使用MVC最重要的一点是多个视图能共享一个模型，现在需要用越来越多的方式来访问你的应用程序。对此，其中一个解决之道是使用MVC，无论你的用户想要Flash界面或是 WAP 界面；用一个模型就能处理它们。由于你已经将数据和业务规则从表示层分开，所以你可以最大化的重用你的代码了。

其优点在于：

1. **低耦合性**

视图层和业务层分离，这样就允许更改视图层代码而不用重新编译模型和控制器代码，同样，一个应用的业务流程或者业务规则的改变只需要改动MVC的模型层即可。因为模型与控制器和视图相分离，所以很容易改变应用程序的数据层和业务规则。

1. **高重用性和可适用性**

随着技术的不断进步，现在需要用越来越多的方式来访问应用程序。[MVC模式](http://baike.baidu.com/view/739359.htm" \t "_blank)允许你使用各种不同样式的视图来访问同一个服务器端的代码。它包括任何WEB（HTTP）[浏览器](http://baike.baidu.com/view/7718.htm" \t "_blank)或者无线浏览器（wap），比如，用户可以通过电脑也可通过手机来订购某样产品，虽然订购的方式不一样，但处理订购产品的方式是一样的。由于模型返回的数据没有进行格式化，所以同样的构件能被不同的界面使用。例如，很多数据可能用HTML来表示，但是也有可能用WAP来表示，而这些表示所需要的命令是改变视图层的实现方式，而控制层和模型层无需做任何改变。

1. **较低的生命周期成本**

MVC使开发和维护用户接口的技术含量降低。

1. **快速的部署**

使用MVC模式使开发时间得到相当大的缩减，它使程序员（Java开发人员）集中精力于业务逻辑，界面程序员（HTML和JSP开发人员）集中精力于表现形式上。

1. **可维护性**

分离视图层和业务逻辑层也使得WEB应用更易于维护和修改。

1. **有利于软件工程化管理**

由于不同的层各司其职，每一层不同的应用具有某些相同的特征，有利于通过工程化、工具化管理程序代码。

* 采用标准的WEB2.0页面控件

系统页面展现层采用web2.0交互技术构建，充分利用ajax，json，xml等方式提高用户的使用体验。系统基于Jquery类库的标准UI界面，清新简洁大方。

* 1. **系统可移植性设计**

系统开发要遵循主流的标准和协议，可运行在不同的软硬件平台上，易于以后系统升级和移植。本次项目为保证系统可移植项采用SOA的体系结构，基于SOA的系统架构将业务需求拆分到基本服务单元，做到了最大程度地柔性面对需求变化，也增强了系统的可移植性。使用J2EE多层分布式架构开发，并在接口设计时采用通用标准，增强平台的可移植性。

* 1. **系统可追溯性设计**

系统应具备完善的使用授权、监控和日志管理机制，能够对各类访问和操作进行审计。

* 1. **兼容性设计**

系统应具备较高兼容性，满足IE6、IE7、IE8、IE9、IE10、IE11、Chrome、Firefox、Safari等主流浏览器提供兼容性视图，保证系统功能的正常展示。

终端应用设计采用基于HTML5技术的web开发。HTML 5从根本上改变了开发商开发Web应用的方式，从桌面浏览器到移动应用，这种语言和标准都正在影响并将继续影响着各种操作平台。

其具有跨平台技术优势，能够快速迭代开发，并且可以实时更新原生应用，有问题立即响应。

HTML5前端是开放的正反馈循环生态系统，大量的开源库可以使用，开发应用变得更轻松、更敏捷。 HTML是以page为单元开放代码的，它无需专门开发SDK，只要不混淆，就能与其他应用交互数据。

* 1. **系统整合性设计**

系统整合性设计目标是：

* 消除信息孤岛；
* 打破系统壁垒；
* 统一服务接口；
* 增强协同协作。

在顶层设计的指导下，基于SOA设计理念，以ESB为技术实现，结合社区公共服务综合信息平台业务需求，架构设计充分考虑平台与共享组件、数据交换支撑组件以及其他校园系统之间的协同关系。

根据不同的场景、不同的业务，分别采用同步或异步的交换方式，实现不同系统之间相互松散耦合,为各业务应用系统提供一个透明的、无差异的集成实现。分解业务系统之间的互联关系，为参与服务的各应用系统间的服务及数据交互提供安全、高性能、可扩展的集成平台。

提供丰富的、标准的适配器，并将标准规范体系的数据标准、技术标准、安全标准融入到建设中，从而保障对任意业务系统的快速接入及接入后的标准化转换。架构图如下：

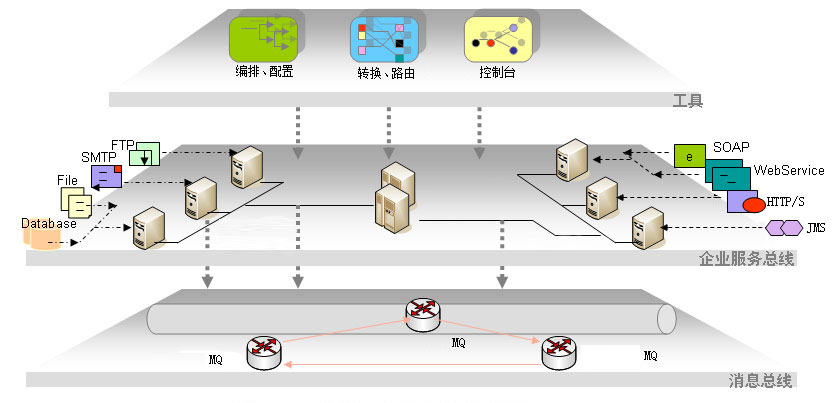


图 0‑1ESB中心服务总线架构

首先，ESB用标准的服务语言跟所有应用系统通讯，这样整个组织的应用系统有了相互交流的共同语言，不必再为各个系统采用不同的通讯协议、不同的数据格式而烦恼，因此它被称为整个企业的服务总线。

其次，ESB协调服务提供者和消费者之间的关系，起到服务中介作用，从而实现服务调用关系松耦合：

1. 各应用系统通过ESB，完成与其他应用系统的集成。
2. 应用系统可以通过ESB提供的适配器，将自己系统的专用接口协议转换成总线使用的标准协议，实现系统与总线的对接；
3. 各系统通过ESB，把系统对外的服务注册到“服务仓库”，这样所有需要这些服务的应用系统，就可以通过ESB，在总线上寻找到并使用服务；
4. 用户可以在ESB上，对所需的服务进行调用、编排、数据转换等配置工作；
5. ESB将根据用户的应用集成配置结果，完成服务调用、转换、路由等工作。

ESB使得不同系统间解除了“直连关系”，是一种轻量级的、可分布式部署的应用集成产品，它很好地解决了紧耦合问题。

* + 1. **功能描述**
* 服务集成

ESB具备服务集成功能，提供用于开发服务、组件集成开发工具，支持完整的从设计、开发、配置到打包部署整个阶段的GUI工具。通过服务生成、服务组装、流程建模、服务生成向导,服务调用示例、应用服务组件等一系列功能,实现对资源及原始功能的封装、集成、调用,从而达到从“数据”到“服务”到“应用”的服务支撑作用。

服务生成：通过可视化界面和服务生成向导，引导用户根据向导的指示，完成数据的填写和收集工作，把相应的资源生成相应的服务,并最终登记、部署、发布。

服务组合：依照服务生成向导，通过可视化的操作界面，将已有的服务或组件进行组合，生成可部署的应用或服务。可以是多个服务的整体组合，也可以是多个服务的部分内容组合。

* 协议转换

服务总线ESB提供良好的跨平台、跨网络、跨协议处理支持，当服务调用端与客户端采用不同数据传输协议（SOAP/HTTP、RMI、JMS）时，ESB通过适配器服务组件的方式，可进行自动协议转换来实现不同传输协议的服务端与客户端的适配。

适配器服务是外系统接入业务集成平台的桥梁，是多种异构系统之间互连互通及互操作的重要组件。ESB提供了大量的基于JCA规范的适配器，如文件系统、各种数据库、消息中间件、WebService等适配器。

通过适配器之间的连接与Java服务引擎以及合成服务模块，可实现各种类型、数据服务标准及通讯协议的服务之间的接入和转换，真正实现了适配器的重用。ESB支持SOAP/HTTP、RMI、JMS、JDBC等多种服务调用协议，支持多种数据库和文件系统，可以很好的满足本项目协议转换的需要。

* 消息路由

ESB提供消息路由功能，通过消息路由方式使得客户端或其他服务对于服务的调用直接面向服务总线，而不必关注服务提供者的位置。

ESB提供事件通知、动态路由选择、事务性处理和可靠传输保障机制，所有对服务的调用都通过服务总线转化为规格化消息的形式，从而在服务组件之间建立了标准的、基于消息的信息可靠传输保障机制，这种方式有效降低了服务端接口的变化或服务提供者的变化对其调用者的影响，使得系统能够更好地适应变化。

通过ESB，可以将请求的消息通过Java服务引擎进行解析判断，根据消息内容，以及配置好的路由规则，自动路由到相应的后台服务，而无需专门指定端点地址，此外，还可集成服务注册库，通过服务注册库，实现服务和消息动态路由的功能。

* 服务扩展

ESB提供丰富的适配器服务组件，通过产品提供的服务合成和服务编排功能，能够结合业务需求，在遵循服务总线相关标准和规范的前提下设计开发新的服务。这些服务可快速集成到服务总线上，并基于服务总线进行服务的配置、管理和快速发布，提供新的功能服务。良好的服务扩展是适应不断变化应用业务的基础。

ESB发布和管理的服务，支持基于SOAP/WSDL的访问方式，以及RMI直接对象访问方式，即使外部ESB及WebServic依旧可以保证良好的兼容性，保证外系统和外部服务的接入和整合。

此外，ESB支持HTTP/HTTPS、FTP、POP3/SMTP、JMS、MQ等多种跨网络通讯技术或协议，并支持基于JMS、Web Service、消息中间件、数据库、文件等方式的接入或数据资源共享交换。并且提供服务调度、服务运行管理支持，提供丰富的适配器服务和API接口，支持二次开发，以保证同特殊类型和格式的系统的兼容性。

* 服务编排

ESB提供集成开发和流程编排支持，支持通过图形化管理界面创建项目和项目元素。

服务的请求可能会涉及到多个服务提供者，可以将多个服务提供者进行组合，使用内建合成服务功能，根据定义的规则和组合逻辑，对所接入的服务进行重组和编排，或结合BPM（业务流程管理平台），实现一个包含多个服务组合的业务流程，从而满足更复杂的业务需求。在本项目的解决方案中，有合成服务功能模块，提供对应的服务组合功能。

通过ESB提供的集成开发配置工具能够根据业务需求，对服务总线上现存的服务进行有条件的顺序组合以创造出新的服务。如：可将A服务、B服务、C服务、D服务进行编排组合建立E服务。

在进行服务的编排、组合和运行时，ESB通过消息队列、JMS服务、事务处理、多线程、缓冲池、集群等机制，有效解决了服务之间大批量数据传输和规格化处理的效率的问题。可以提供良好的并发和并行处理支持，提供集群等高可靠、高可用服务支持。

* 服务集群

服务总线ESB的支持服务级集群策略，以保证高可用行和高处理能力。可以将服务注册到特定的集群中，通过服务总线中的集群服务器可实现服务的冗余设计和负载均衡，在提高服务并发访问能力的同时避免集群服务器本身的故障造成系统单点失效。

服务总线ESB通过HTTP服务器集群的代理转发功能，实现多个服务总线服务器节点上多个同等Web服务实例的并发协同处理服务消费请求。服务总线ESB服务运行容器基于Java EE技术实现，支持Web服务的封装和发布，并提供标准的Web服务运行环境，能够与标准的HTTP服务器集群进行有效集成使用，实现服务级的集群和负载均衡效果。

在实现负载均衡的同时，通过开发可以建立具有机构层次的集群管理机制，提供服务的匹配策略设置，即根据服务调用者的调用权限、工作范围、服务优先级等特征与服务端的调用权限、服务范围限定、服务优先级策略等特征进行最佳匹配，在根据各服务器的繁忙程序找到最佳的服务节点。

* 服务浏览

查看可以访问的服务列表，获取服务WSDL信息，也可以调用查询可用服务列表接口获取可以访问的服务列表。

* + 1. **统一监控管理**

对用户进行增加、修改、删除以及查询。只有成为平台用户，才有可能访问平台提供的各应用系统。

每个用户都应该具有一种以上的角色，角色不同意味着具有的操作权限不同，管理职责不同。

角色管理支持增加角色、修改删除角色、查询角色，建立角色与用户之间的对应关系。

每个角色都需要赋予一定的操作权限，权限管理通过增加权限、修改权限、删除权限实现对角色权限的调整。

* + 1. **逻辑节点管理**

逻辑节点是组件、服务及业务流程的运行环境，它包含了实现J2EE1、4规范的应用服务器。平台基于标准的J2EE1、4规范，因此在其上开发的组件、服务及相应的业务流程，最终要打包成标准的J2EE相关组件和应用，部署到相应的J2EE应用服务器上运行，逻辑节点管理包括：

* 查看逻辑节点详细信息，包括该逻辑节点的IP，端口等信息。
* 修改逻辑节点的别名。
* 配置整个逻辑节点的日志相关属性，逻辑节点日志的相关属性可以包括设置日志的类型、级别，日志文件的大小、备份等。
* 获取逻辑节点日志，在显示日志内容页面，可以通过查找关键字，快速浏览日志信息。

1. 项目监控管理

主要是针对整个项目的一个管理监控功能，包括该项目下合成应用，及合成应用相应的部署名称和运行状态等信息的查看及相应的启、停等功能。

* **项目**：查看此项目下所有的部署文件自身信息及运行状态等信息，同时可以对权限管理范围内的部署文件进行启、停控制。
* **项目警告信息处理：**可以通过过滤条件查看项目的警告信息，同时也可以手工清理相关警告信息。
* **部署管理：**查看该部署下的服务运行情况，可以对权限管理范围内的部署进行启动、停止操作。
* **合成应用：**显示该合成应用的服务连接关系图。

1. 服务监控管理

（一）服务基本信息

在服务信息中，可以查看到服务如下信息：

* 服务名：监控项目下服务的名称，与在集成开发工具中该项目下创建的适配器和服务名称一致。
* 合成应用名称：监控项目下，该服务所属的合成应用名称，与在集成开发工具中该项目下创建的合成应用名称一致。
* 容器名：监控项目下，该服务在合成应用中容器的名称，与在集成开发工具中该项目下创建的该服务容器名称一致。
* 逻辑节点IP：该服务所在的逻辑节点的IP地址。
* 逻辑节点端口：该服务所在的逻辑节点的端口号。
* 服务名：监控项目下服务的名称，与在集成开发工具中该项目下创建的适配器和服务名称一致。
* 类型：该服务的类型。
* 状态：该服务的当前活动状态，状态分为：

suspend：暂停状态；

active：正常运行状态；

unkown：非正常运行状态。

* 接口信息：该服务所用接口的名称。
* 警告数：该服务产生的警告信息数量。

（二）服务参数设置

参数设置，是根据该服务所涉及的适配器属性，显示适配器的属性设置。与集成开发工具中该项目下，在合成应用中，为每个适配器设置属性一致。当前版本，用户只能通过“参数设置”，了解适配器的属性设置内容，不可以进行修改。

（三）服务日志管理

服务日志设置

可以针对服务的日志类型、日志级别，组件名深度、保存模式等日志相关信息进行设置。

服务的日志获取

在日志查看是，可以设置需要获取日志的起始时间和终止时间，需要获取日志的条数，每页日志显示行数。

在显示日志内容页面，可以通过查找关键字，快速浏览日志信息。

（四）服务交易状况管理

服务交易状况统计可以实时监控一个业务流程在一定时间内处理业务流程的情况分析，成功处理业务多少笔，失败多少笔等信息。

（五）服务负载信息管理

在“服务信息”列表中，选中一个服务，通过设置查看该服务的负载信息统计，也可以删除一些负载信息。

* **服务负载信息统计**

1. 统计总计调用次数：服务的调用次数统计。
2. 根据时间段统计调用次数：设置某段时间内的调用次数，可以设定起始和终止时间。
3. 根据年份统计每月调用次数：统计某一年内，每个月对该服务的调用次数，可以设定年份。
4. 根据月份统计每天调用次数：统计某一年的某个月份内，每一天对该服务的调用次数，可以设定年份和月份。
5. 根据天统计每小时调用次数：统计某一年的某个月份的某一天内，对该服务的调用次数，可以设定年份，月份和日期。
6. 统一监控管理

监控管理是对平台自身的交换管理、用户认证授权和基础信息资源共享系统的工作状态、交换节点、交换流程运行状态进行集中监控管理。

1. 交换信息查看

对平台、外系统接入适配器、交换流程的历史运行状态以及Web服务的历史使用日志等进行按关键或日期查询。

1. 系统运行信息查看

系统运行信息是指平台各服务的运行信息（如数据服务器、交换服务器等）、平台运行日志信息（如，数据插入数据库失败、文件传输中断等）以及用户操作日志信息等，支持按照关键字或者日期查看系统运行信息。

1. 交换情况统计分析

对日志信息按照业务系统进行分类统计分析，得到各系统使用平台的综合情况，如数据交换的次数和数据量、用户认证次数和点击量等，实现对系统交换业务访问情况的展现和统计。

1. 信息告警通知

对节点、流程运行过程中的异常情况如，节点停止、传输中断等，以邮件的方式及时通知给相关负责人，帮助相关人员迅速了解平台的运行情况，诊断、发现并及时解决平台的各类故障问题。

1. 日志管理

日志管理模块主要实现对系统自动记录的用户操作日志进行查看、查询、删除等操作，该模块主要提供给审计用户使用。

* + 1. **集成接口管理**

定义编码对外部系统开放的WebService服务的地址、方法等。提供两类服务：编码生成服务于编码查询服务。

1、编码生成服务：

* 1. 按数据规范接收外部系统传入的某一数据对象的数据。
  2. 按元数据模型提取该元数据的编码规则。
  3. 解析编码规则使用到的元数据元素数值。
  4. 按码段逐一生成编码规则，拼装产生完整的数据编码，返回调用服务的接口。
  5. 编码发生异常，返回异常信息。

2、编码查询服务：

* 1. 第三方系统调用服务，按数据规范传入数据对象。
  2. 按元数据模型解析传入数据。
  3. 将传入的数据项作为查询条件执行数据查询，如果查询结果只有唯一的一条生效数据，则返回该数据编码，如果没有对应生效数据或有多条生效数据，返回异常，提示传入的数据不足以查询唯一的编码。

3、连接测试：可对配置的接口进行连通性测试。

* + 1. **安全管理**

1. 网络接入层

* 客户端非法接入控制

保证接入ESB系统的合法性，提供应用系统和ESB系统之间的双向身份认证，采用基于证书的认证模式，系统使用的数字证书由第三方CA或者采用自运行维护的CA提供。CA证书采用离线下发的方式，以PKCS#12文件的格式安装到ESB系统和应用接入系统。身份认证完成后，双方得到一个64个字节的随机数，通讯双方使用的对称密钥都是基于这一组随机数产生，对称密钥的选取规则双方使用相同的策略。对称密钥和对方的公钥信息存放在系统主机的共享内存，方便应用系统加密使用

1. 网络传输层

* 支持SSL（包含国密算法）

数据通信采用128位的SSL技术（包括SSLv3和TLSv1）提供尖端的高安全保证，确保连接的合法性、私有数据的保密性。

数据传输通过使用身份证书，来建立具有强安全性的SSL连接。只有通过双方身份验证的连接才允许建立，并进行数据传输，在此连接上传输的数据都将被加密，保证传输机密性的安全需求。

支持的加密算法和摘要算法列表如下（包含国密算法）：

表 0‑1支持的加密算法和摘要算法

| **加密算法** | **摘要算法** | **备注** |
| --- | --- | --- |
| NULL | MD5 | SSLv3 / TLSv1 |
| NULL | SHA | SSLv3 / TLSv1 |
| RC4 | MD5 | SSLv3 / TLSv1 |
| RC4 | SHA | SSLv3 / TLSv1 |
| IDEA-CBC | SHA | SSLv3 / TLSv1 |
| DES-CBC | SHA | SSLv3 / TLSv1 |
| DES-CBC3 | SHA | SSLv3 / TLSv1 |
| AES128 | SHA | TLSv1 |
| AES256 | SHA | TLSv1 |
| SM4-ECB | SM3 | 国密算法；非对称算法使用SM2 |
| SM4-CBC | SM3 | 国密算法；非对称算法使用SM2 |

1. 应用层

* 加密接口

ESB提供了加密和解密接口，使用的算法是RC5，应用程序在发送消息之前调用加密接口，在接收消息之后调用解密接口，可以有效保证传输过程中私有数据的保密性。另外，应用程序在发送消息之前、接收消息之后，可以调用第三方提供的加密库，包括与第三方加密设备（如加密机）配合使用的加密库。

1. 管理层

配置文件加密、管理权限、用户审计

* 1. 配置文件加密

对配置文件的加密功能，加密后的配置文件以密文形式存在。加密后的配置文件只能通过管理控制台这个唯一入口进行查看和编辑，保证了对服务器管理的安全性。

* 1. 管理权限

ESB管理控制台提供了用户权限管理功能，对系统的使用者进行了角色划分，并对不同使用者对不同管理功能拥有的访问权限进行定义，从而保证系统的不同使用者只能访问被授权的系统和进行规定的访问操作。

* 1. 用户审计

用户操作审计功能，详细记录了每个用户对节点的所有操作，包括登录信息，对配置信息的查看、修改、删除等操作，为后续问题查找提供了技术支持。

* 1. **数据备份和恢复**
  + 数据备份

依托机房的集中数据存储和备份存储实现平台的本地数据存储、备份与恢复，系统数据和业务数据可联机备份、联机恢复，恢复的数据必须保持其完整性和一致性；系统应具备自动或手动恢复措施，以便在发生错误时能够快速恢复正常运行；系统支持异地备份的拓展。

数据存储与备份将采取以下策略：

1、将数据库数据存储路径定义至专用磁盘阵列存储介质；

2、采用全备份和差分备份相结合的方式进行数据备份；

3、每周进行一次全备份，每天进行一次业务数据差分备份；

4、在具备条件时，对备份数据进行异地保存管理。

* + 双机热备

实现无单点故障的全冗余双机热备方式。这种方式的特点在于：

1、存储之间的数据复制不经过网络，而是由存储之间进行复制。

2、两个存储之间的复制是完全实时的，不存在任何时间延时。

3、主备存储之间的切换时间小于500ms，以确保系统存储时不产生延时。

4、硬盘盘符及分区不因为主备存储之间的切换而改变。

5、服务器的切换，不影响存储之间的初始化，增量同步及数据复制。

6、某一存储设备的计划性停机，不影响整个服务器双机热备系统的工作。

7、存储设备之间使用重复数据删除技术，完成增量同步工作。

8、真正的7X24小时或切换的全冗余方案。

* + 灾备优化

建议充分提供数据备份与安全、系统恢复与软件应用、灾难恢复以及异地灾备四大保障来充分保障系统的业务连续性。

在数据备份与安全方面，基于磁盘“块”级别的备份，实现了实时的文件、数据库、应用程序、操作系统、逻辑卷和裸设备等的持续数据备份，可以立即对备份的数据进行查验，并且持续数据备份又实现了三个“‘0’的突破”：零停机备份、零窗口备份和零冲击备份；

在系统恢复与软件应用方面，实现了病毒、应用程序错误、人为误操作、系统瘫痪等软故障下的任意时间点的一分钟数据恢复、5分钟系统恢复以及无需停止业务的在线系统恢复；

在灾难恢复上则实现前端主机磁盘等硬件损坏故障时的操作系统远程启动，实现快速灾难恢复；

为了应对地震、火灾等自然灾害，将来将对接北京市政府密云灾备中心实现提异地容灾。

* 1. **系统处理和响应能力**

（1） 最大支持1000用户同时在线使用，高峰时支持50个用户并发访问。

（2） 对于处理不超过20个数据项的普通维护操作，要求平均响应时间在1秒以内，峰值响应时间控制在3秒内；对于处理不超过50个数据项的普通维护操作，要求平均响应时间在2秒以内，峰值响应时间控制在5秒内；对于处理超过50个数据项的维护操作，如果数据项为X，则要求平均响应时间小于（X/50）×2 秒，峰值响应时间控制在；（X/50）×4秒内，最高不超过8秒。

（3） 对于单表信息的精确查询，要求平均响应时间在1秒内；对于跨表的精确查询，平均响应时间要小于（2×相关联的表的个数）秒，峰值响应时间控制在（4×相关联的表的个数）秒内，并且最高不能超过20秒。

（4） 系统平均无故障率不低于99.5%，若发生故障，恢复时间的要求是：

* 一般故障，恢复系统正常运行所需时间不超过30分钟；
* 严重故障，不超过4小时；
* 特别严重的故障，一般不超过24 小时。

第四部分安全保障方案

* 1. **安全设计原则**

在对本系统规划设计过程中，充分考虑用户业务应用的需求，使用目前成熟、稳定且先进的技术来规划和设计整个平台的安全系统结构。本次安全的整体思想是要构建一个集安全技术体系、安全管理体系和安全运维服务体系三个体系为一体的信息安全保障体系；形成集防护、检测、响应、恢复于一体的安全保障体系，从而实现物理安全、网络安全、系统安全、数据安全、应用安全和管理安全，以满足信息系统全方位的安全保护需求。同时，由于安全的动态性，还需要建立安全风险评估机制，在安全风险评估的基础上，调整和完善安全策略，改进安全措施，以适应新的安全需求，满足等级保护以及自身安全运维的要求，保证长期、稳定、可靠运行。

本设计方案将遵循以下整体建设原则：

1、统一规划、分步实施

根据实际工作需要，从业务应用系统、信息服务系统、网络体系等方面的安全需求考虑，制定平台项目安全保障体系的整体目标和规划，并根据需求的轻重缓急情况，制定出分阶段的计划，突出重点、分步实施，确保在分步实施的过程中，避免盲目建设和低效建设。

2、需求、风险、代价平衡的原则

对信息系统建设进行切合实际的分析与设计，对系统可能面临的威胁或可能承担的风险提出定性、定量的分析意见，并制定相应的规范和措施，确定系统的安全策略。

3、综合性、整体性原则

采用适当的技术手段分析网络的安全，并制定具体措施。安全措施主要包括：行政法律手段、各种管理制度以及专业技术措施，如访问控制、加密技术、认证技术、攻击检测技术、容错、防病毒、综合审计等。

4、一致性原则

针对系统平台安全问题与整个网络的工作周期（或生命周期）提出分析意见，并保证制定的安全体系结构必须与网络的安全需求相一致。

5、易操作性原则

所采用的安全措施应保证易于操作，并保证不影响系统的争产运行。

6、适应性及灵活性原则

所采用的安全措施必须保证实现随着系统平台性能及安全需求的变化而变化，易适应、易修改。

7、多重保护原则

所建立的安全系统要确保是一个多重保护系统，各层保护相互补充，当一层保护被攻破时，其它层保护仍可保护信息的安全。

安全系统的建设目标是根据系统结构和应用模式，针对可能存在的安全漏洞和安全需求，在不同层次上提出安全级别要求，并提出相应的解决方案，制定相应的安全策略，编制安全规划，采用合理、先进的技术实施安全工程，加强安全管理，保证系统的安全性。

1、统筹规划，分步实施：明确整体安全策略，规划本系统平台信息安全保障体系并制定实施计划，结合本系统平台应用实际情况和发展需要，分阶段、分步骤，不断推进和完善信息安全保障体系；

2、统一协调，各负其责：抓好安全工作，构筑本系统平台信息安全保障体系；

3、综合防范，整体安全：在本系统平台安全体系建设中，坚持管理与技术并重，从人员、管理、安全技术手段等多方面着手，建立综合防范机制，实现整体安全；

4、分级保护、务求实效：从实际出发，综合评估信息的价值和系统所面临的风险大小等因素，科学划分网络与信息系统安全等级。依据安全等级进行安全建设和管理，综合平衡安全成本和风险，优化信息安全资源的配置，提高信息安全保障的有效性。

* 1. **安全保障体系框架**

本项目将参照国家信息化建设三级等级保护标准建设本项目工程及应用服务系统，主要从物理安全、网络安全、主机安全、应用安全以及数据库安全五个方面着手，采用当今先进而成熟的安防技术与产品，设计部署信息安全防护体系，并树立规范信息安全管理体系，完善管理机构与管理制度，全方面实现信息安全的整体要求，最终达到安全防护的目标。



图 0‑2安全保障体系框架示意图

* 1. **物理安全**

对于本系统而言，物理安全保障业务系统正常运转的基础。因此，对于承载业务系统的物理运行环境应从以下几方面予以考虑，防止意外的物理风险的发生：

* 意外事故（如自然灾害、火灾）造成的系统破坏；
* 电源故障造成的设备损坏或数据丢失；
* 设备失窃造成数据丢失或信息泄漏；

电磁辐射可能造成数据信息被窃取或偷阅。

* 1. **应用安全**

1. 4. 1. **用户身份认证**

根据《信息安全技术信息系统等级保护安全设计技术要求》，对于信息系统需建立网络接入认证机制，可采用由密码技术支持的可信网络连接机制，通过对连接到网络的设备进行可信检验，确保接入网络的设备真实可信，防止设备的非法接入。

互联网云已通过各种防护措施实现安全域的划分与边界控制，但是在网络的接入认证与控制措施上前存在一定的不足，无法对接入到网络中设备进行识别及控制和记录。为规避上述风险，建立基于网络的接入认证控制措施，即部署网络接入认证网关系统来实现对通过政务外网及内网接入网络核心的实体的身份识别、安全策略检查和权限进行控制及行为记录，增强对网络资源的使用保护。

为防止对平台信息资源的非授权访问，需建立有效的身份认证措施。将结合采用北京市CA认证管理系统登录身份鉴别机制和基于数字证书的用户身份鉴别机制，实现系统强身份认证登录。强身份认证登录将采取以下安全策略：

1、在系统层面，制定系统登录错误锁定、会话超时退出等安全策略；

2、在应用层面，采用 “数字证书＋USBKEY”认证方式来实现用户对本期项目登录访问的身份鉴别。

* + 1. **访问权限控制**

本期项目将面向北京市各校园学院、事业单位提供服务，为进一步加强对本期项目内数据信息资源访问的可控性，防止信息资源被非授权访问，建议在身份有效性识别的基础上，对不同角色人员采取授权访问措施。

系统将从系统级访问控制和资源级访问控制两方面进行设计：

1、系统级访问控制

通过账户权限最小化配置、边界并发会话阈值限制、单一资源最大化（或最小化）使用限度等方式实现，将本期项目纳入市共享交换平台进行统一认证授权管理。

2、资源级访问控制

在本期项目过程中实现细粒度的资源授权和字段级授权，以实现资源级访问控制。

* + 1. **应用软件安全**

应用软件安全保证是指在应用软件的设计、开发、测试、分发和升级等整个生命周期中通过安全的运作方式保证软件的安全性。具体包括：

1、软件的安全设计评估

任何一套软件都可能存在安全隐患，这也是被大家广为接受的概念。而针对本期项目而言，应拥有一套良好的策略和手段针对业务软件本身的安全设计进行有效的评估。

2、版本控制

在软件开发过程中，制订版本控制制度，并采用有效的版本控制或配置管理软件。对版本进行必要的访问控制。

3、测试

应用系统开发应具有完善的测试文档，对应用软件进行多样的测试，例如白箱测试、黑箱测试和压力测试等。

4、软件分发和操作

新的软件发布的时候，应按照安全策略中的有关流程进行分发，不应对现有安全策略产生影响或者违背。

* + 1. **Web应用程序安全设计**

针对Web应用程序的攻击不容易在网络边界处进行防范，并且攻击形式多样，难于完全杜绝。防止针对Web应用程序的攻击最有效的方法是在软件设计时进行安全编程考虑，从代码本身杜绝被攻击的可能性，从而做到未雨绸缪、主动防御。

针对Web程序的攻击主要分为跨站脚本攻击和SQL注入攻击两大类，以下分别从这两种攻击的攻击手段考虑，提出解决方案。Web应用程序软件开发时应根据以下建议进行安全开发。

* XSS跨站脚本攻击

1、漏洞成因

原因很简单，就是因为WEB程序没有对用户提交的变量中的HTML代码进行过滤或转换。

2、漏洞形式

这里所说的形式，实际上是指WEB输入的形式，主要分为两种：

显示输入；

隐式输入；

其中显示输入明确要求用户输入数据，而隐式输入则本来并不要求用户输入数据，但是用户却可以通过输入数据来进行干涉。

显示输入又可以分为两种：

输入完成立刻输出结果；

输入完成先存储在文本文件或数据库中，然后再输出结果；

而隐式输入除了一些正常的情况外，还可以利用服务器或WEB程序处理错误信息的方式来实施。

3、漏洞危害

比较典型的危害包括但不限于：

获取其它用户Cookie中的敏感数据；

屏蔽页面特定信息；

伪造页面信息；

拒绝服务攻击；

突破本期项目网络不同安全设置；

与其它漏洞结合，修改系统设置，查看系统文件，执行系统命令等；

其它。

一般来说，上面的危害还经常伴随着页面变形的情况。而所谓跨站脚本执行漏洞，也就是通过别人的网站达到攻击的效果，这种攻击能在一定程度上隐藏身份。

4、解决方法

要避免受到跨站脚本执行漏洞的攻击，需要程序员和用户两方面共同努力，程序员应过滤或转换用户提交数据中的所有HTML代码，并限制用户提交数据的长度；而用户方则不要轻易访问别人提供的链接，并禁止浏览器运行JavaScript和ActiveX代码。

* SQL INJECTION数据库注射攻击

1、SQL Injection定义

所谓SQL Injection ，就是通过向有SQL查询的WEB程序提交一个精心构造的请求，从而突破了最初的SQL查询限制，实现了未授权的访问或存取。

2、S2QL Injection原理

随着WEB应用的复杂化，多数WEB应用都使用数据库作为后台，WEB程序接受用户参数作为查询条件，即用户可以在某种程度上控制查询的结果，如果WEB程序对用户输入过滤的比较少，那么入侵者就可能提交一些特殊的参数，而这些参数可以使该查询语句按照自己的意图来运行，这往往是一些未授权的操作，这样只要组合后的查询语句在语法上没有错误，那么就会被执行。

3、SQL Injection危害

SQL Injection的危害主要包括：

暴露敏感信息

提升WEB应用程序权限

操作任意文件

执行任意命令

4、SQL Injection 技巧

利用SQL Injection的攻击技巧主要有如下几种：

逻辑组合法：通过组合多种逻辑查询语句，获得所需要的查询结果。

错误信息法：通过精心构造某些查询语句，使数据库运行出错，错误信息中包含了敏感信息。

有限穷举法：通过精心构造查询语句，可以快速穷举出数据库中的任意信息。

移花接木法：利用数据库已有资源，结合其特性立刻获得所需信息。

5、预防手段

要做到预防SQL Injection, 数据库管理员（MS SQL Server）应做到：

应用系统使用独立的数据库帐号，并且分配最小的库，表以及字段权限；

禁止或删除不必要的存储过程；

必须使用的存储过程要分配合理的权限；

屏蔽数据库错误信息。

WEB程序员则应做到：

对用户输入内容进行过滤；

对用户输入长度进行限制；

注意查询语句书写技巧。

* 网页防篡改

网页防篡改系统是黑客入侵防范体系的一个重要组成部分和最后一道防线。目前国内网页防篡改产品生产厂商相对较少，产品研发采用的技术主要可以分为二类：扫描技术、核心内嵌技术。下面从二种技术的实现原理上分析一下两种技术的优缺点：

扫描技术采用的方式是周期性的访问监控的网页，来判断网页的真实性。这种技术的优点是实现的技术门槛比较低，厂商能够快速的开发出网页防篡改产品。缺点是：一、不能保证被篡改网页的实时恢复，被篡改的文件存在一定的存活期；二、周期性的访问监控网页势必会加重服务器的负载，影响应用系统的正常运行。扫描技术是网页防篡改产品在初期采用的一种技术。

核心内嵌技术采用将其篡改检测模块嵌入Web服务器软件内部运行，与Web服务器无缝结合。这种技术的优点是每次Web服务器对外发送网页时，网页防篡改系统都进行检测，从而能够实时地确保每个网页的真实性。缺点是：一、被篡改文件的恢复依赖于用户的访问请求，被篡改文件存在一定的存活期，并且增加了服务器的负载；二、需要针对于不同的Web服务器提供不同版本的产品。核心内嵌技术是比扫描技术更科学、更先进的一种技术。

* 1. **数据安全**

从数据传输过程和数据存储过程两方面保障本期项目的数据的完整性和保密性。具体防护策略如下：

1、数据传输过程：通过部署和配置SSL安全通讯协议服务，确保关键数据的传输保密性和完整性；

2、数据存储过程：采用密码机制所支持的完整性校验机制，检验在系统安全计算环境中存储数据的完整性；采用密码机制所支持的保密性保护机制，对安全计算环境中的存储数据进行保密性保护。

* + 1. **传输安全与抗抵赖**

开启系统、设备的日志审核策略功能，建立网络安全审计系统，同时将系统记录的日志信息统一提交给安全管理中心的集中日志审计系统，实现关联性统计分析。

部署SSL安全传输协议信道，数显数据传输交换过程中的完整新和保密性；统一认证服务提供安全认证凭证的安全传输和校验。

* + 1. **数据存储与备份恢复**

依托新建机房的集中数据存储和备份存储实现本期项目的本地数据存储、备份与恢复，同时在中环等有条件的机房选择部署异地灾备存储环境，利用政务外网网络，实现异地数据备份。

数据存储与备份将采取以下策略：

1、将数据库数据存储路径定义至专用磁盘阵列存储介质；

2、采用全备份和差分备份相结合的方式进行数据备份；

3、每周进行一次全备份，每天进行一次业务数据差分备份；

4、在具备条件时，对备份数据进行异地保存管理。

* 数据备份

依托机房的集中数据存储和备份存储实现平台的本地数据存储、备份与恢复，系统数据和业务数据可联机备份、联机恢复，恢复的数据必须保持其完整性和一致性；系统应具备自动或手动恢复措施，以便在发生错误时能够快速恢复正常运行；系统支持异地备份的拓展。

数据存储与备份将采取以下策略：

1、将数据库数据存储路径定义至专用磁盘阵列存储介质；

2、采用全备份和差分备份相结合的方式进行数据备份；

3、每周进行一次全备份，每天进行一次业务数据差分备份；

4、在具备条件时，对备份数据进行异地保存管理。

数据层安全措施主要有数据库安全审计、数据盗窃安全防护系统等。

1、数据库安全审计

数据库对于本项目是一个复杂而又关键的系统，数据库在管理和技术上存在风险，若这些风险变为事实，则数据中心数据将遭受经济损失和法律风险。当数据库产生安全问题时很难追查和定位，因为无法查找问题发生的痕迹和证据。因此，数据库的安全审计成为数据库安全的重要组成部分，它可以通过对数据库操作的痕迹进行详细记录和审计，使数据的所有者对数据库访问活动一目了然，有据可查，及时掌握数据库的使用情况，并可对安全隐患进行调整和优化。

数据库安全审计要求支持分布式部署结构，能够同时管理多个审计引擎，并对审计引擎的审计结果信息进行集中查询、分析；集用户身份认证、基于角色的授权访问及网络内容审计三位一体；提供会话监控功能对正在进行的连接会话内容进行实时监视并可以进行手工阻断；支持对敏感行为的阻断功能，包括基于策略和手工两种方式。能够根据制定的策略对违规行为进行实时自动阻断，支持将正在发生的违规行为通过操作系统显示界面以手工方式阻断当前会话连接。发现安全隐患，并对网络活动的相关信息进行存储、分析和协议还原，并对网络中的可疑网络行为实施记录、告警和阻断。

2、数据存储安全

在信息系统中存储的信息主要包括纯粹的数据信息和各种功能文件信息两大类。以数据库信息的保护最为典型，对应用终端数据安全保护也很重要。

数据库安全：提供多级数据库的安全机制，并能支持数据加密存储和传输及冗余控制。对数据库系统所管理的数据和资源提供安全保护，一般包括：物理完整性，即数据能够免于物理方面破坏的问题，如掉电等；逻辑完整性，保持数据库的结构，如对一个字段的修改不影响其它字段；元素完整性，包括在每个元素中的数据是准确的；用户鉴别，确保每个用户被正确识别，避免非法用户入侵；可获得性，可访问数据库和所有授权访问的数据。

应用终端的数据存储安全：主要解决计算机信息的安全保护问题，一般的安全功能有：基于口令或（和）密码算法的身份验证，防止非法使用机器；强制存取控制，防止非法访问文件；多级权限管理，防止越权操作；存储设备安全管理，防止非法拷贝和硬盘启动；数据和程序代码加密存储，防止信息被窃；预防病毒，防止病毒侵袭；严格审计跟踪，便于追查责任事故。

* 双机热备

实现无单点故障的全冗余双机热备方式。这种方式的特点在于：

1、存储之间的数据复制不经过网络，而是由存储之间进行复制。

2、两个存储之间的复制是完全实时的，不存在任何时间延时。

3、主备存储之间的切换时间小于500ms，以确保系统存储时不产生延时。

4、硬盘盘符及分区不因为主备存储之间的切换而改变。

5、服务器的切换，不影响存储之间的初始化，增量同步及数据复制。

6、某一存储设备的计划性停机，不影响整个服务器双机热备系统的工作。

7、存储设备之间使用重复数据删除技术，完成增量同步工作。

8、真正的7X24小时或切换的全冗余方案。

* 灾备优化

建议充分提供数据备份与安全、系统恢复与软件应用、灾难恢复以及异地灾备四大保障来充分保障系统的业务连续性。

在数据备份与安全方面，基于磁盘“块”级别的备份，实现了实时的文件、数据库、应用程序、操作系统、逻辑卷和裸设备等的持续数据备份，可以立即对备份的数据进行查验，并且持续数据备份又实现了三个“‘0’的突破”：零停机备份、零窗口备份和零冲击备份；

在系统恢复与软件应用方面，实现了病毒、应用程序错误、人为误操作、系统瘫痪等软故障下的任意时间点的一分钟数据恢复、5分钟系统恢复以及无需停止业务的在线系统恢复；

在灾难恢复上则实现前端主机磁盘等硬件损坏故障时的操作系统远程启动，实现快速灾难恢复；

为了应对地震、火灾等自然灾害，将来将对接北京市政府密云灾备中心实现提异地容灾。

* + 1. **数据保护**

为了对那些必须保护的记录提供足够的保护，而对那些不重要的记录不提供多余的保护，应该对所有记录给予评价，并作出分类。

1类（关键性的）记录：对设备的功能来说是最重要的，不可替代的，火灾或灾害后立即需要但又不能再制的那些记录。如关键程序、主记录、设备分配图表、加密、并法、密钥等秘级很高的记录。

2类（重要的）记录：这类记录是很重要的，可以在不影响系统最主要功能的情况下进行复制，但比较困难和昂贵。如某些程序、存贮及输入输出数据等属于该类。

3类（很有用的）记录：其丢失可能引起极大的不便，但可以很快复制。已留有拷贝的程序、扫描的影像数据等属此类。

4类（不重要的）记录：在调动时很少需要的记录

* + 1. **数据脱敏脱密**
* 数据脱敏

数据脱敏是指对某些敏感信息（如：账号、身份证号、电话、地址、密码）通过脱敏规则进行数据的变形，实现敏感隐私数据的可靠保护。这样，就可以在开发、测试和其它非生产环境以及外包环境中安全地使用脱敏后的真实数据集

数据脱敏是为了确保在非生产环境下使用生产数据更加安全，但是其又与纯粹的数据加密不同，数据加密可能是将数据库中有意义的字符通过加密后转变成了无意义字符，而脱敏是将数据通过一定的算法变成另一种样式，而这种样式是可读的，并且与元数据是同一类的。

一个好的数据脱敏过程必须具备以下特点：可用性、数据关联关系、业务规则关系、数据分布、易用性和可定制。从而在针对不同系统进行数据脱敏时，制定良好的脱敏方法，是整个数据脱敏关键所在，本项目中数据脱敏目标如下：

1.防止生产库中敏感数据泄露

通过对生产库中的身份信息、地址信息、银行卡号信息、电话号码信息等敏感数据进行混淆、扰乱后再提供给第三方使用，防止生产库中的敏感数据泄露；

通过对生产中或扰乱后的数据进行局部数据抽取，实现非生产环境下数据集合使用的最小化。

2.提升测试、开发和培训数据质量

在数据漂白和数据子集的过程中，通过内置的策略和算法，保证脱敏后数据的有效性（保持原有数据类型和业务格式要求）、完整性（保证长度不变化、数据内涵不丢失）、关系性（保持表间数据关联关系、表内数据关联关系），以提升在测试、开发和培训环节的真实有效性。

3.提高数据维护和数据共享安全性

通过对生产数据库访问者的用户名、IP、工具类型、时间等多个访问者身份维度，控制对生产数据访问结果的差异化，返回结果可以为真实数据返回、数据掩码，同时可以进行数据阻断、行数限定。

脱敏功能设计如下：

1.静态数据脱敏

支持全流程的静态数据脱敏：

1）数据漂白

通过高效的数据脱敏算法，能够针对不同数据类型进行数据脱敏及掩码扰乱，支持的脱敏算法包括屏蔽、变形、替换、随机、格式保留加密（FPE）和强加密算法（如AES）。

2）数据装载

可将脱敏后的数据按用户需求，装载至不同环境中。按照场景不同，可提供文件至文件，文件至数据库，数据库至数据库，数据库至文件的不同装载方式。

2.动态数据脱敏

对需要共享的生产数据或时效性很高的数据测试、培训场景，提供基于网络代理模式的动态脱敏技术；动态脱敏可实现对业务系统数据库中敏感数据进行透明、实时脱敏。

1）动态脱敏可以依据数据库用户名、IP、客户端工具类型、访问时间，甚至业务用户身份等多重身份特征进行访问控制；

2）动态脱敏对生产数据库中返回的数据可以进行放行、屏蔽、加密、隐藏、返回行控制等多种脱敏策略。

3.数据子集

提供多种的数据子集抽取方式：

1）基于事实表发起的百分比抽取方式；

2）基于基础信息表中的身份信息或商品类别发起的向下延展的数据抽取方式；

3）针对多表的灵活条件设定的抽取方式。

4.敏感数据管理

实现全面的敏感数据管理功能，帮助组织实现有序、一致的可视化脱敏数据管理。

1）敏感数据发现

能够按照用户指定的一部分敏感数据或预定义的敏感数据特征，在执行任务过程中对数据进行自动识别，发现敏感数据。与此同时，既可发现数据之间的主外键关系，也可以智能分析出用户赋予数据间的依赖关系、同类数据间的联动关系，为数据子集管理、脱敏数据关联性保留等功能提供了保障。

2）敏感数据字典管理

以敏感数据为中心，对数据库字段进行分类管理；对同库多表、多库多表的同一类敏感数据实施统一的脱敏算法和策略，保证同一单位或行业内跨系统、跨库之间的数据脱敏后一致性；并支持敏感数据字典导入、导出等功能。

3）脱敏方案管理

针对每一脱敏项目，在基础性脱敏算法的基础上，可以配置专门的脱敏策略，或者实现脱敏算法的扩展；

可实现脱敏策略的导入导出，以帮助脱敏策略的复用，保障在同一组织架构内脱敏策略的一致性。

4）脱敏任务管理

可对任务数据进行停止、启动、重启、暂停、继续，并且支持任务并发，充分利用系统资源，提高脱敏效率。脱敏过程中可跳过异常数据，持续执行任务。

* 数据脱密

本项目所存储的信息涉及到涉密数据，需要对开发环境和测试环境中的数据建立统一的管理规范，对于必须使用生产数据的系统开发、测试、维护项目，生产数据必须经过脱密，才能被加载到开发、测试或维护环境。此脱密过程称做“数据漂白”。

数据漂白后的要求：

1.去掉隐私信息。

2.保持数据脱密后的数据构成、合法性标准（如果目标系统需要对该数据字段进行校验的话。

3.保持数据库的数据一致性和参考完整性。

4.应用系统间关联使用的有效性。

5.保持聚合字段、行/列计算字段有效性。

6.脱密算法不可破解。

针对于本项目，数据加/脱密处理的主要流程设计如下：

1）对数据库命令进行语法分析，如果语法正确，转下一步；如不正确，则转6），直接将SQL命令交数据库服务器处理。

2）是否为数据库加/脱密引擎的内部控制命令？如果是，则处理内部控制命令，然后转7）；如果不是则转下一步。

3）检查数据库加/脱密引擎是否处于关闭状态或数据库命令是否只需要编译？如果是则转6），否则转下一步。

4）检索加密字典，根据加密定义对数据库命令进行加脱密语义分析。

5）数据库命令是否需要加密处理？如果是，则将数据库命令进行加密变换，替换原数据库命令，然后转下一步；否则直接转下一步。

6）将数据库命令转送数据库服务器处理。

7）数据库命令执行完毕，清除数据库命令缓冲区。

* 1. **系统安全和监控体系**
  2. 1. **安全监控总体框架**

为了有效防范和化解风险，保证信用数据的安全，实现信息系统的平稳运行以及业务应用的持续稳定进行，必须按照统一规划、统一建设、统一管理和统一服务的原则，建立可靠的安全保障体系，增强信息安全风险防范能力。

系统的安全监控体系设计将建立纵深防御体系：包括“人”、技术”和“操作”三个方面入手，对系统的信息安全进行全方位的安全管理，并且作为实际的安全措施来实行，构建系统的安全监控体系。其中“人”即指管理安全措施；技术”指保护网络和基础设施、保护网络边界、保护计算环境及支撑性基础设施；“操作”指运行安全措施。

* + 1. **事前防护安全设计**

1、安全管理

对于信息安全，除了配置较为完善的技术设备外，还必须制定好相应的规章制度：

（1）成立信息安全小组。主要任务是贯彻执行和完善信息安全的规章制度，对日常工作进行认真检查、监督、指导和教育。

（2）制定安全规范。根据各应用系统的建设情况和对信息资源的需求，将在安全领域制定一系列的标准规范，以进一步加强信息安全。该规范主要包括安全管理措施、安全技术标准、运行安全措施。

2、安全域划分

通过安全域划分，形成清晰、简洁、稳定的 IT 组网架构，实现系统之间严格访问控制的安全互连，更好的解决复杂系统的安全问题；安全域划分后，安全域间的信息流控制遵循如下原则：

* 跨安全域的数据流须经过定义好的边界控制组件控制。
* 在边界控制组件中，缺市情况下，除了明确被允许的流量，所有的流量都将被阻止。
* 边界控制组件的故障将不会导致跨越安全域的非授权访问。
* 所有来自互联网的流量需要被严格控制和监控，每个连接必须被授权和审计。

3、链路负载均衡

在互联网出口部署两台链路负载均衡设备对互联网接入线路进行链路负载均衡。对于外部用户访问“基础支撑平台”应用的入站访问，链路负载均衡设备可以通过智能 DNS 解析功能，动态选择最佳链路，将外部用户导向到内部站点中的资源。同时链路负载均衡设备会随时监测每条链路的状况，当发现任何一条 ISP 链路故障时，都不会再把该 ISP 的 IP 地址解析给用户，从而保证用户可以 7\*24 小时的访问到内部应用并且提高用户的访问速度。

4、Web 防火墙

在“支撑平台”DMZ 区域部署两台 Web 防火墙，主要是对 Web特有入侵方式的加强防护，如 DDOS 防护、SQL 注入、XML 注入、XSS 等。WEB 应用防火墙部署于门户网站服务器群的前端，通过抗扫描、防注入、防跨站脚本、防后门攻击等安全策略加强门户网站的安全防护能力，最大限度的杜绝网站被黑客入侵的可能。

5、网页防篡改系统

为保证Web 前端服务器的安全性，系统需部署网页防篡改系统，防止对外提供服务的信用北京网被非法、恶意篡改。网页防篡改系统分为三个相对独立的子系统，分别是监控代理Monitor Agent（简称 MA）、同步代理 Synchronization Agent（简称SA）和管理中心 Management Center（简称 MC）。监控代理 MA 部署于网站服务器，负责实时监控保护网站文件，发现篡改企图或篡改操作实时发送恢复请求，并及时提交告警信息。同步代理 SA 部署于同步服务器，负责实时监控备份文件变更，以及监控代理提交的恢复请求，并根据请求执行向网站服务器的文件同步。管理中心 MC 逻辑上部署于管理服务器，作为用户与系统之间的接口，负责将操作指令传达给监控代理和同步代理；同时，负责实时接收来自代理端的各种告警信息并及时通知用户。

6、防火墙方案设计

本项目需要采用双层异构防火墙防护技术，在互联网外部部署安全网关，在内部网络部署异构防火墙，从网络安全方面提供整体防护能力。安全网关集成防火墙、IPS、防病毒等功能，加强整个内外网网络边界的区域安全性及服务器区域安全性；通过防火墙有效隔离和阻断来自互联网的非授权访问，阻断和处理来自互联网的攻击，防范从互联网流入流到内部网络的病毒、间谍软件、木马等攻击行为。

7、防病毒方案设计

根据国家信息系统安全等级保护中“主机系统安全--恶意代码防范、入侵防范”的要求，方案设计中采用集成基于主机 IPS 防范的网络防病毒技术，对服务器、工作站进行全面的安全保护。在“基础支撑平台”包括的所有主机上安装防病毒客户端，接受防病毒服务器的统一管理。

8、服务器虚拟化安全设计

采用服务器虚拟化提供的虚拟化安全整体解决方案，可针对数据中心内的网络威胁提供基本的防护,提供采用基于基本流量信息的策略的应用程序防火墙, 按主机进行部署。对虚拟机之间的流量进行基本的防火墙保护，这样便能够根据 5 元组（源 IP 地址、目标 IP地址、源端口、目标端口、协议）对连接进行筛选和分组，根据网络、应用程序端口、协议类型（TCP、UDP）、应用程序类型强制实施安全保护。

9、CA 证书体系安全设计

充分利用市级法人一证通平台，提供在线证书状态认证服务（基于在线证书状态协议，即 OCSP 协议），签名、验签服务和加密、解密服务。设计以 CA 证书体系为核心的信用数据的管理系统，这个系统的核心是信用数据管理中心，提供信用数据管理系统的认证、授权、审计等功能。由于证书的发放、使用有严格的登记、管理流程，此系统有较强的审计、追溯能力，以及防抵赖能力。

* + 1. **事中监控安全**

1、系统运行监控

通过部署业界先进的 IT 监控软件，采用集中统一的监控平台，通过全局、直观的监控展现，保障业务系统平台稳定、高效的运行，实现业务应用、基础架构与网络架构集中监控，实时掌握核心关键业务应用、主机服务器、中间件、数据库、网络设备等关键指标运行状况，及告警信息及时预警机制。通过 IT 监控软件的部署，可将被动式服务转换为主动式服务，提升运维服务质量、服务能力与服务水平，提高系统的可用性，减少系统问题的发生，实现系统安全稳定健康的运行。

2、日志集中管理

本项目通过日志集中管理系统，对该平台中包括的所有服务器、网络设备进行集中日志审计管理，日志集中管理系统包括管理（审计）中心和可选的日志采集器两个部分。日志集中管理系统支持同时采集多个不同网段的日志信息，适用于逻辑隔离的多个网络。

3、运维审计管理

本项目需要一台运维审计系统（堡垒机），对所有运维人员的 IT 操作行为进行监控、审计，实现 IT 运维操作的集中认证、授权、审计。通过在运维审计系统上配置所有服务器的开放资源以及所有需要访问服务器的运维管理人员的帐号，并利用运维审计系统的访问控制和授权功能，实现对所有访问服务器进行运维操作的行为进行控制与监控，从而达到运维审计的要求。

* + 1. **事后恢复安全**

1、备份软件及磁带库安全设计

在本方案中选用业界领先的备份管理软件作为本系统备份的核心软件，使用物理磁带库，作为备份介质。数据备份方式有：LAN 备份、LAN-Free 备份和Server-Free 备份三种。LAN 备份针对所有存储类型都可以使用， LAN-Free 备份和 Server-Free 备份只能针对 SAN 架构的存储。本系统采取 LAN 备份，LAN-FREE 备份和 SERVER-FREE 相结合的手段，对重点主机中数据读写要求速度快的做 LAN-FREE 备份，特大数据做SERVER-FREE 备份，其他普通主机做 LAN 备份。

以下详细描述针对不同应用系统所做的不同备份策略：

（1）基于 LAN 的数据备份方式--针对 IP 网络的普通服务器：传统数据备份方式需要在每台主机上安装磁带机备份本机系统，采用 LAN 备份策略，在数据量不是很大时候，可采用集中备份。一台中央备份服务器将会安装在 LAN 中，然后将应用服务器和工作站配置为备份服务器的客户端。中央备份服务器接受运行在客户机上的备份代理程序的请求，将数据通过 LAN 传递到它所管理的、与其连接的本地磁带机资源上。这一方式提供了一种集中的、易于管理的备份方案，并通过在网络中共享磁带机资源提高了效率。本系统中的归集服务器、清洗服务器、比对服务器和应用服务器等机器，运行在 IP 网络，服务器中保存的内容主要包括网页、源代码、文档、配置文件等，备份数据量不是太大，可采用 LAN 备份方式，以较低的投入达到较为理想的效果。

（2）LAN-Free 数据备份方式：由于数据通过 LAN 传播，当需要备份的数据量较大，备份时间窗口紧张时，网络容易发生堵塞。在 SAN 环境下，可采用存储网络的 LAN-Free 备份，需要备份的服务器通过 SAN 连接到磁带机上，在 LAN-Free 备份客户端软件的触发下，读取需要备份的数据，通过 SAN 备份到共享的磁带机。这种独立网络不仅可以使 LAN 流量得以转移，而且它的运转所需的CPU 资源低于 LAN 方式，这是因为光纤通道连接不需要经过服务器的 TCP/IP 栈，而且某些层的错误检查可以由光纤通道内部的硬件完成。此时，需要一台主机来管理共享的存储设备以及用于查找和恢复数据的备份数据库。本系统中运行在互联网的信用北京网数据库，由于备份数据量较大，备份时间较长。因此，可以考虑采用 LAN -Free 的备份方式。

（3）Server-Free 数据备份方式：Server-Free 对需要占用备份主机的 CPU 资源，如果备份过程能够在 SAN 内部完成，而大量数据流无需流过服务器，则可以极大降低备份操作对生产系统的影响。SAN Server-Free 备份就是这样的技术。本系统中政务外网的本期项目核心数据库，由于备份数据量非常大，备份时间长，备份时不能对主机有较大影响。因此，可以考虑采用 Server-Free 的备份方式。

以上三种数据备份方式中，LAN 备份数据量最小，对服务器资源占用最多，成本最低；LAN-free 备份数据量大一些，对服务器资源占用小一些，成本高一些；Server-free 备份方案能够在短时间备份大量数据，对服务器资源占用最少，但成本最高。

2、容灾方案设计

系统运行支撑环境为用户提供应用访问服务时，当主数据中心遭遇自然灾害而不可用时，将带来不可预计的严重后果。通过建立容灾数据中心，可以大大提高整体平台的业务连续性。容灾数据中心的主要建设内容如下：

——磁带数据容灾：通过备份系统将业务系统数据备份至磁带，实现数据离线异地保存。

——数据级容灾：利用存储的同步复制技术，将主数据中心的数据实时同步至容灾中心，实现数据级容灾。

——通过容灾软件组件，将主数据中心的所有虚拟机复制到容灾中心，实现应用级容灾。系统容灾数据中心将交由市政务信息资源中心统筹建设。

* 1. **项目主要风险及防范措施**
  2. **项目风险管理机制**

项目风险是客观存在的，主要包括技术风险、管理风险和系统风险。技术风险包括项目的技术结构、项目的规模以及项目实施方的技术能力和经验。管理风险主要来自于项目人员组织的有效性，项目时间、资源计划的确定性和可控性，以及项目质量监控的力度和立场。系统在这里指的是由信息化相关要素组成的动态联系的有机体系。主要指的是用户自身的组织规范化、组织的观念转变、组织责任与控制体系的适应性等。所以，建立风险管理机制是降低和化解风险的有效手段。

* + 1. **风险监督机构**

借助于专业人员，建立内部监督机构，对该应用系统的实施进行风险分析和跟踪，并提出防范措施。

* + 1. **长期合作关系**

要实行对项目的有效监督，不仅要对项目的实施进行监控，而且对甲方的长期发展战略有全面、深刻的了解。这样，监督人员才能站在战略的高度，分析应用系统的发展方向，把握系统建设的目标。

* + 1. **全过程风险管理**

对本项目风险的管理，不能只停留在实施完成后对项目的评估上，更重要的是防范和化解风险。监督分为定期阶段评估和终审评估，它们贯穿于项目的全过程，从规划、准备、实施到系统运行。定期评估是监督人员根据项目的实施进度，制定计划，在现场做实际分析，通过分析来发现潜在的问题和风险，及时提出修改建议。各实施小组采取相应的措施加以改进。终审评估是在实施完成后，对运行系统所做的全面评价。定期评估是预防性监督，全过程监督的内容不仅是对各项风险进行专项跟踪，更包括对工作质量的跟踪；审核项目实施计划，确认计划的完整；跟踪实施进展，判断项目实施是否得到有效的控制；审核实施的阶段性成果，如系统的分析报告、设计报告、测试报告等，确认实施是否达到阶段目标。

* 1. **项目主要风险及防范措施**

针对本项目来说，项目风险主要包括进度、技术、管理、质量和人员等五个主要部分。

* + 1. **进度风险**

1、风险识别

项目实施周期为半年，从2017年1月初至2017年6月初。项目整个实施工作大体划分为如下的6个主要阶段。

* 1. 前期准备和需求调研
  2. 系统需求分析
  3. 系统概要设计和详细设计
  4. 系统开发和测试
  5. 系统试运行
  6. 系统正式运行和验收

商务合同签订后的1个月内，完成项目需求调研、系统初步设计、系统整体设计和系统详细设计工作，并进行专家论证和确认。2个月内，完成项目的开发、测试、安装、部署工作。软件集成测试通过后，1个月内进入系统试运行。系统试运行合格后，1个月内完成项目的系统初步验收以及用户上线。培训工作完成后，进行系统终验。终验合格后，工程建设完工，进入质量保证期。即在此期间完成从需求分析到软件集成测试，并包括整个项目培训、试运行前的所有工作。项目对时间进度的要求较高。

2、风险分析

可能造成进度风险的因素包括：

1）项目承担单位工作任务分解时，考虑到的主要工作进度主线，各分解工作最早开始时间完成时间、最迟开始时间完成时间以及契合、交叉工作任务划分不尽合理，或考虑不够周全。

2）项目承担单位对分解的工作任务配备的人员和人员组成结构不能保证该工作任务的按时完成。

3）项目承担单位主要里程碑中，尤其是完成项目的需求分析、设计并通过审至完成开发、集成和测试，有两点需要注意，一是开发工作须以需求分析、系统设计通过评审为前置条件；二是开发、集成和测试工作需要在2个月内完成。时间较紧，如果项目承担单位不在需求分析和系统设计阶段，不在可能范围内预先开展开发的准备工作，则很有可能造成进度延误。

4）业主单位为共同开展项目建设配备的相关业务协调人员和业务协同部门，如果不全力指导、配合项目建设，则需求分析和系统设计进度难以保障。

5）业务较大变更和项目涉及各方有效沟通存在问题等，也会对项目进度带来重大影响。

3、风险规避

针对以上主要风险因素，可以采取的风险规避措施主要包括：

1）合理进行工作任务分解。目承担单位在明确项目范围后，应在各实施组充分参与条件下，共同制定WBS。

2）根据工作任务统筹考虑参与任务的人员和人员结构组成。

3）在需求分析和系统设计阶段，采用原型迭代法，开发原型系统，以更好了解业务单位需求，缩短评审通过后的编码开发时间。

4）对于确认后需求分析和系统设计，在不影响业务主要使用前提下，在编码开发阶段尽量不作变更。必要的变更可在项目应用软件系统编码、集成、联调、测试并通过第三方测评后进行。

5）在项目涉及各方间建立有效的沟通机制。

* + 1. **技术风险**

1、风险识别

项目涉及个人隐私信息，能够对工作主管部门、其他政府部门、服务评级机构和社会公众等各类用户提供查询、统计分析等项内容。另外，在系统建设中需要统一考虑的还有系统整体框架、数据库建设、应用支撑平台以及标准规范等。项目涉及的技术内容较多，存在一定风险。

2、风险分析

本建设项目的技术风险主要包括：

1）数据存取、调用等数据层操作方法和接口等在多个系统中不一致导致的风险。

2）应用支撑平台中各基础组件的结构化和一致性较差可能导致的风险。

3）应用系统专业组件封装方法和提供接口不一致或灵活性较差导致的复用度不够造成的风险。

4）系统间互调用、互操作设计不合理导致的联通性较差的风险。

5）系统对于大量多并发访问以及性能等方面要求不能满足，而造成的使用风险。

6）业务系统中的多维分析、计算、统计的实现可能存在技术风险。

7）在系统的开发、使用和运维中，没有明确统一的标准规范和要求，而造成的风险等。

3、风险规避

针对以上主要技术风险，可以采取的风险规避措施主要包括：

1）采用原型迭代法进行前期系统开发，识别关键技术和主要解决方法。

2）利用项目承担单位已有的应用软件构件库和类似项目开发技术，最大程度解决可能出现的技术风险。

3）在项目编码开发前，完成标准规范特别是技术标准规范的制定，指导规范应用软件开发、集成工作。

* + 1. **管理风险**

管理风险主要来自于项目人员组织的有效性，项目时间、资源计划的确定性和可控性，以及项目质量监控的力度和立场。项目共分五类角色：用户方的业务人员、用户方的决策人员、集成商的技术人员、集成商的项目管理人员以及项目的监管者如何有效组织，并协同发挥积极因素是一个项目组织的课题，存在很多的不确定性。而项目进度的计划和项目预算是否具有确定性直接影响项目的可控程度。最后，项目监控的力度和立场在实际过程中会面临来自各方面的干扰和阻力。

本项目的顺利实施离不开相关部门和单位的密切配合，本项目建设将涉若干政府部门，重点在于参与案件转办的单位与其他职能单位的沟通协调，存在的风险较小。

* + 1. **质量风险**

1、风险识别

本建设项目要求在规定的进度范围内，采用合理先进的技术实现项目要求，更重要的是，必须满足质量的要求，达到立项和系统使用要求。

2、风险分析

项目质量风险主要包括：

1）项目相关提交物的质量风险。其中需求分析规格说明书、系统概要设计、系统详细设计、系统集成设计等交付物需要得到评审通过，以指导项目后续工作。这方面的质量风险是由业务单位和项目承担单位共同承担。其他阶段和过程，重点是编码开发质量需要由项目承担单位严格控制、监督检查的。

2）项目管理过程的风险。本项目涉及范围广、内容多，规范性强。必须采用严格的项目管理规定和制度。在项目整体开发进度要求下，项目管理的实施需要对实施过程各阶段各要素进行严格规划、定义、检查监督，也就是说，项目管理会带来时间、费用、人力等的成本，可能会对项目的进度造成影响。

3）项目质量实际上包括项目管理的各主要要素，有时间、费用、人力、沟通、采购等，这些因素同样会影响到项目质量。

3、风险规避

针对以上主要质量风险，可以采取的风险规避措施主要包括：

进行项目全过程的监督。对本项的质量管理，不能只停留在实施完成后对项目的评估上，更重要的是防范和化解质量风险。监督分为定期阶段评估和终审评估，它们贯穿于项目的全过程，从规划、准备、实施到系统运行。定期评估是质量管理人员根据项目的实施进度，制定计划，在现场做实际分析，通过分析来发现潜在的问题和风险，及时提出修改建议。各实施小组采取相应的措施加以改进。终审评估是在实施完成后，对运行系统所做的全面评价。定期评估是预防性监督，全过程监督的内容不仅是对各项风险进行专项跟踪，更包括对工作质量的跟踪；审核项目实施计划，确认计划的完整；跟踪实施进展，判断项目实施是否得到有效的控制；审核实施的阶段性成果，如系统的分析报告、设计报告、测试报告等，确认实施是否达到阶段目标。

* + 1. **人员风险**

1、风险识别

本建设项目涉及内容较多、时间进度要求较紧。如果没有充足的人员保障，没有合理的人员结构分析，要在进度规定下完成项目是不可能的。

2、风险分析

项目人力资源风险包括：

1）投入项目的总的实施人数、实施人员的素质能力和实施团队结构的安排如果不合理，不能满足人力资源计划和项目计划，则项目存在巨大风险。

2）足备合格的实施人员不能同分解的工作任务有机结合，即制定的工作任务对应的人员、人员结构组成和目标不能合理匹配，则项目存在风险。

3）人员分配和人员费用计划不能有效结合，不能在进度规定范围内，在一定费用匡算下，完成项目工作任务要求的目标，则项目存在风险。

4）项目承担单位制定人员计划时，可能现有人力资源不能全部满足项目实施需要，而在人力组织时没有考虑到解决方法，则项目存在风险。

3、风险规避

针对以上主要人力资源风险，可以采取的风险规避措施主要包括：

1）本项目投入使用人员全部定岗、定职，精力全部投入本项目建设。

2）在项目启动阶段，结合项目范围要求，制定项目工作计划，完成工作任务分解，必须完成人员计划制定，并根据实际工作开展情况适当变更。

3）根据人员计划，明确组织结构和岗位分配，进行人员配置管理。

4）根据配置管理要求，选派单位内部合格人员参与项目建设，进行必要的现有工作交接和针对项目的前期沟通、培训。

5）制定合理的外聘人员计划和合作计划，选择适当外聘人员。

6）项目人员适当的复用和合理沟通是确保项目成功的要素之一，如需求分析人员适当参与系统设计工作、培训人员应由项目主要开发集成人员组成等。

7）结合项目范围管理、时间管理、质量管理等要求，进行团队绩效考核和个人绩效考核。

第五部分应用系统方案设计

* 1. **设计依据**
     1. **在国家和北京市政策法规的指导下进行建设**

国家政策法规是本工程的基础保障环境，具有约束、威慑以及不得已情况时的非常手段，保证项目顺利施行与最终目标的达成。本次建设应遵循国家、北京市、信息化建设领域的各种标准、规范和制度。

* + 1. **符合国际开放技术标准与规范**

系统设计和建设要符合国际开发技术标准，系统设计的各种接口在遵循规范性原则的基础上，保证其可以继承不同设备的厂商、系统或平台供应商、软件供应商的产品，保证系统的设备管理、系统扩容和业务维护不依赖于单一设备厂商、系统或软件供应商的产品。

同时，为了使系统具有较强的生命力和开放性，系统建设应遵循当前业界认可的、先进的技术思想和国际标准。系统开发应严格遵照国家软件工程规范进行，根据开发进度及时提供有关开发文档，包括软件需求说明书、系统设计说明书、数据库设计说明书、测试计划、用户手册、测试分析报告、系统维护手册、操作手册等。

* + 1. **政策与法规**

1. 《国家电子政务工程建设项目管理暂行办法》（发改委令55号〔2007〕）；
2. 《北京市信息化工作领导小组关于加强信息安全保障工作的实施意见》（京办发〔2004〕3号）；
3. 《北京市电子政务建设管理办法（试行）》(京信息办发〔2004〕39号）；
4. 《北京市电子政务总体技术框架》；
5. 《北京市政务与公共服务信息化工程建设管理办法》（市政府第67号令）。
6. 《国务院办公厅关于政府向社会力量购买服务的指导意见》(国办发〔2013〕96号)
   * 1. **安全性原则**

系统应该保证不同权限级别的人访问不同级别的信息，任何非法的访问都被杜绝。保证信息的有效性、机密性、完整性、可靠性和标识，系统在网络、数据库、应用操作权限和身份认证方面，加载全面的信息安全保护措施。

本平台对安全要求较高。平台设计将安全可靠性作为首要的先决条件，确保系统能够长期、高效和安全可靠运行。系统采用流行、成熟、稳定、先进的操作系统、数据库等，保证系统的稳定性。

* + 1. **标准与规范**

1. 《计算机软件需求说明编制指南》（GB9385-1988）；
2. 《功能建模方法IDEF0》（IEEE 1320.1-1998）；
3. 《信息建模方法》（IEEE 1320.2-1998）；
4. 《信息安全技术信息系统灾难恢复规范》（GB20988-2007-T）
5. 《信息技术安全技术信息安全管理体系要求》（GBT22080-2008）
6. 《计算机软件产品开发文件编制指南》（GB/T 8567-1988）；
7. 《计算机信息系统安全保护等级划分准则》（GB/T 17859-1999）；
8. 《信息技术开放系统互联高层安全模型》（GB/T 17965-2000）；
9. 《信息技术开放系统互联基本参考模型》（GB/T 9387）；
10. 《信息技术开放系统互联应用层结构》（GB/T 17176-1997）；
11. 《信息技术开放系统互联开放系统安全框架》（GB/T 18794）；
12. 《信息技术开放系统互联通用高层安全》（GB/T 18237）；
13. 《电子信息系统机房设计规范》（GB 50174-2008）；
14. 《计算机信息系统设备电磁泄漏发射限值》（GGBB1-1999）；
15. 《计算机信息系统设备电磁泄漏发射测试方法》（GGBB2-1999）；
16. 《电子信息系统机房建设规范》（GB50174-2008）；
17. 《电子信息系统机房施工及验收规范》（GB50462-2008）。
    1. **总体设计原则** 
       1. **先进性原则**

系统应当采用当今国内、国际上先进和成熟的技术，使新建立的系统能够最大限度地适应今后技术发展变化和业务数字化发展的需要。

本项目选择先进的计算机网络、信息存储、信息处理等高新技术手段，合理设计、规划与配置系统的整体结构，实现系统结构合理、技术先进、性能稳定的整体设计目标。

* + 1. **实用性原则**

系统总体设计要充分考虑各用户层当前的不同层次应用要求，对各级用户来说，业务应用操作简便、易用；能够最大限度地满足实际工作要求，使系统始终与用户的实际需求紧密结合，增加系统的实用性。

* + 1. **可靠性原则**

系统应采用成熟的信息化技术和软硬件设备，关键部分要求有备份措施；系统业务软件应能长期稳定运行，并具有较强的容错和自动恢复能力。

* + 1. **兼容性原则**

系统要求能够平滑接入平台目前已建的业务体系中，以保证中心呼叫业务系统运行的完整性。平台设计时，所采用的技术手段遵循相关标准，保证各应用系统间的无缝连接，并具有较高的灵活性，适应后续的升级或引进新技术的需要。

* + 1. **可扩展性原则**

系统设计要求具备良好的开放性和高弹性化结构。系统应采用结构化、模块化的设计理念，可根据业务需要修改某个模块、增加新功能或重组系统结构，以达到程序可重用的目的；数据结构设计合理、规范，同时具有可维护性，对数据库表的修改维护可在很短时间内完成。

系统设计将充分保证系统容量、处理能力和业务范围具有良好的扩展能力；满足项目未来发展的需要，保护投资，避免重复建设；因此系统设计时必须采用当前先进设计思想和主流技术，既要考虑软硬件支撑环境的先进性，更要考虑系统结构、应用设计、网络、硬件的扩展、数据结构和系统二次开发的需要，并支持未来可能出现的新业务的需要。系统网络结构易于扩充，以适应今后的较大任务负载；硬件平台可升级，当需要时可以通过新的设备同原有设备一起工作以提高系统的处理能力，从而保护原有投资。

* + 1. **可维护性原则**

系统应具有较好地可维护性，能够对网络、设备故障、系统配置、系统性能和安全等系统基础环境设备进行管理。设备出现故障时能及时告警并定位，实现运行和维护工作的有效的运维展示。便于系统管理员管理，要能有效辅助系统管理员诊断排除故障，采取有效的措施，使得系统时刻处在良好运行的状态。

* + 1. **实用性与易管理性原则**

系统功能充分满足用户的实际需求，人机界面友好，易于使用、管理、维护、扩展；系统的建设将采用成熟、稳定、完善的产品和技术，满足当前应用需求，使整个系统具有灵活的权限管理机制，系统管理员可以根据使用系统的不同角色对用户进行权限分配，日常维护工作简单、易操作，无需高级计算机用户即可进行系统的日常维护工作。

* + 1. **总体规划、分步实施原则**

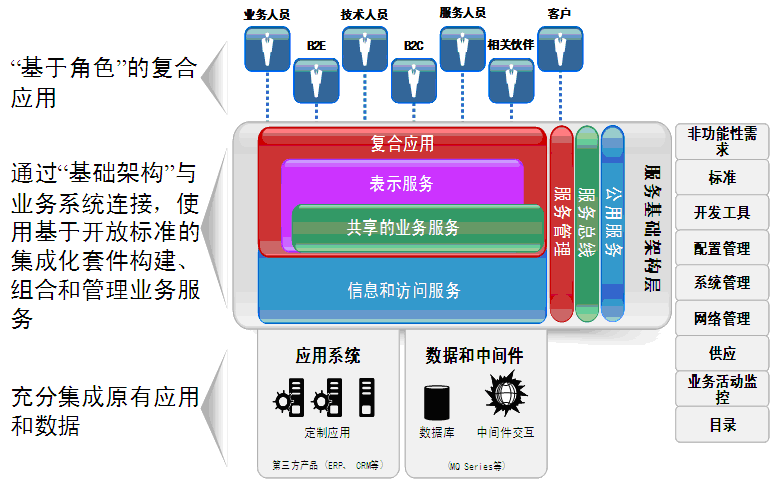
项目建设遵循“总体规划、分步实施”的原则推进，通过设定阶段目标，保证平台建设能够稳步扩展，使平台服务内容和范围能够更为广泛。

* 1. **系统技术线路**
     1. **采用基于SOA框架**

面向服务的架构（SOA）是一种创新思维，它是一种不局限于任何特定技术或厂商的架构方法，屏蔽了不同平台、编程语言、操作系统和硬件架构之间的差异，将企业应用系统中的分散功能组合成可互操作的、基于标准的服务，使其能被重新组合和重用，从而快速满足业务的需求，帮助弥合业务需求与企业IT支持能力之间的鸿沟。采用SOA架构实现应用服务运行管理框架的设计。通过SOA技术实现了服务的注册、查找、管理、监控。通过研究，我们认为服务分为2种，一种由内部组件提供，成为内部服务，包括组织身份服务、访问控制服务等。另一种由外部注册到服务仓库的服务构成，例如会议系统提供的会议室查询服务，此类称之为外部服务。

参考SOA架构的系统将不同的服务通过服务之间定义良好的接口和契约联系起来。服务独立于实现服务的操作系统和编程语言之外，接口采用中立的方式进行定义。构架在各种系统中的服务通过统一且通用的方式进行交互，保证了业务系统的互联互通。采用SOA技术构建的应用系统可以非常方便地实现业务整合、接口整合、信息整合、UI整合。SOA具有松耦合、标准化服务调用、跨平台等灵活特性，很好的规避了系统信息孤岛的产生。

SOA架构模型如下图所示：



图表0‑1SOA架构模型图

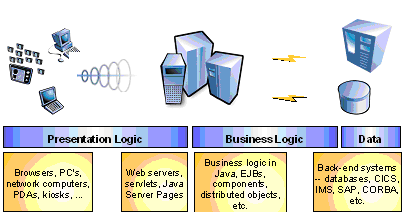
1. 应用系统采用SOA架构的优点

| **特点** | **描述** | **优点，应用性能以及注解** |
| --- | --- | --- |
| 松散耦合 | 服务提供者和消费者可以用定义良好的接口来独立开发。服务实现者可以更改服务中的接口、数据或者消息版本，而不对消费者造成影响。 | 松散耦合消除了对系统两端进行紧密控制的需要。就系统的性能、可伸缩性以及高可用性而言，每个系统都可以实现独立管理。它并没有消除任何的运行时依赖性。它可以划分众多服务提供者的依赖性，但如果该运行时系统需要 24x7 的可用性以及每秒 50000 的吞吐量的话，那么对服务提供者的这些需求必须得到满足。  实现的改变被隐藏了起来。松散耦合给服务提供者和消费者提供了独立性，但要求基于标准的接口和中间物来积极地管理和代理终端系统之间的请求。 |
| 基于行业标准 | 真正的行业标准是由技术旗舰如BEA、IBM、Microsoft、Sun、Oracle、W3C 以及 Oasis 所认可的。SOA 由于其可以用基于标准的技术来实现，所以它被广泛接受。消除了拥有私有客户的需要。 | 使用基于标准的技术可打破行业垄断并促进供应商产品的最优组合。松散耦合层的概念依赖于在内部和外部对标准的广泛支持。 |
| 可重用的服务 | 由于服务是在目录中发布并且在整个网络中都可用，所以它们变得更加容易被发现和重用。如果某个服务不能被重用，那么它可能根本不需要服务接口。为了不同的目的再次将服务组合，这种方式也可以实现服务的重用。 | 服务重用避免了重复开发之苦，同时提高了实现中的一致性。服务的重用比起组件或者类的重用更容易实现，在过去曾尝试过组件和类的重用，但很少成功。 |
| 同步服务调用 (RPC 方式) | 在同步服务调用中，调用方进行调用、传递所需的参数、中断并等待响应。 | 如果服务提供者可用，那么同步服务调用可为请求提供立即响应。同步服务对于要求实时响应的应用程序来说是至关重要的。 |
| 异步服务调用(文档方式) | 在异步服务调用中，调用方向消息收发服务发送一个包含完全上下文的消息，收发服务将该消息传递给接收者。接收者处理该消息并通过消息总线向调用方返回响应。在消息正在处理的过程中，调用方不会中断。 | 由于粗粒度消息和消息收发服务的使用，可以对服务请求进行排队并以最合适的系统速度来处理它们。这种方法具有高度可伸缩性，原因是队列允许的长度是多少，消息收发系统就能够对多少请求进行排队。调用方并不在处理过程当中保持网络连接，并且由于调用方并不会中断，所以它们不会受处理延迟的负面影响，也不会受异步服务执行中所存在问题的负面影响。  本实现采用回调的支持，这本身并不是 Web 服务标准的一部分。 |
| 无干扰开发（通过使用现有的软件组件来开发服务） | 现有的软件组件并不需要修改就可以将其功能作为服务提供出来。服务是用组件的接口定义开发或生成的。 | 消除了修改、测试以及维护现有软件的需要。有了组合服务，来自现有投资的功能可以被重用并重新组合来为企业创造新的价值。 |
| 策略管理 | 当把共享的服务应用于应用程序中时，针对每个应用程序所特有的规则被外化为策略。在设计和运行时，必须就每个服务进行策略的管理和应用。 | 基于策略的计算可以促进普通的可重用服务的创建。随着特定应用程序服务定制的外化，应用程序实现的变化被减少到了最低限度。  通常实施策略的是一个组织的操作和支持小组，并非开发小组。如果不使用策略的话，应用程序的开发人员以及操作和支持小组不得不在应用程序开发过程中并肩工作来实现并测试策略。策略的使用使得开发人员能够集中精力于应用逻辑，而使操作和支持小组专注于规则。 |
| 数据访问服务 | 数据访问、集成、转换以及重用服务。 | 隐藏数据源的复杂性，同时加强跨数据源的一致性、完整性以及安全性。 |
| 组合服务 | 组合服务将新的现有的应用程序逻辑和事务处理进行了合并。 | 充分利用现有的 IT 投资。适用于绿地和遗留实现。装配或者编排产品简化了异构系统的集成。 |
| 共享的或企业的基础架构服务 | 基于 SOA 构建的所有应用程序所使用的公共服务称为共享的基础架构服务。使用共享的基础架构来提供公共服务可以避免每一个应用程序构建类似的服务。 | 使用共享的基础架构服务可提供一致性，并允许单点管理。  其他的共享服务（例如与安全相关的服务）可以通过将现有的产品作为服务直接提供出来的方式创建。 |
| 细粒度服务 | 细粒度服务实现最小的功能，同时消耗并返回最小量的数据。  细粒度服务可以用 Web 服务来实现，也可以利用基于RMI、 .Net 或者 CORBA 的分布式对象来实现。 | 细粒度服务的优点是可在粒度级实施严格的安全和访问策略。  实现和单元测试很简单，而且相互独立。 |
| 粗粒度服务 | 粗粒度服务比细粒度服务实现更多的功能，并消耗不同数量的结构化数据或者消息。它们返回类似的数据或者消息，可能还含有内嵌的上下文。 | 粗粒度服务不需要通过网络多次调用来提供有意义的业务功能。 |

图表0‑2SOA架构的优点表

* + 1. **基于B/S/D三层结构开发应用系统**

采用Browser/WebServer/DataBaseServer三层结构进行应用系统的开发。

* ****

图表0‑3三层结构应用开发图

Browser/WebServer/DataBaseServer三层结构如上图所示，下面对B/S/D三层结构作详细的阐述。

1、数据与应用逻辑分离的特征

Browser/WebServer/DataBaseServer结构指硬件的体系结构，也有相应的逻辑的体系结构相对应。在Browser / Web Server / Data Base Server计算模型中，要完成的功能在浏览器、Web应用服务器和数据库服务器之间进行划分。

硬件的Browser/WebServer/DataBaseServer结构，通常是指某项请求任务在浏览器或Web应用服务器和数据库服务器之间进行分配，其中浏览器用来发送请求和前端表示处理，Web应用服务器处理来自浏览器的请求，数据库服务器处理数据查询逻辑处理。

对逻辑系统体系来说，分为表示层、商业逻辑处理层、和数据处理层三层客户\服务器结构。

鉴于两层结构(C/S)在设计和应用的局限性，将复杂的业务数据处理提出，将复杂的业务数据处理提出，将系统的逻辑结构和物理结构分离，形成三层结构的客户\服务器结构，运用基于组件的分布式技术，从结构上就避免两层结构的局限性.三层结构具体内涵如下：

2、用户服务(客户层)

用户服务层是应用的用户接口部分，是用户与系统间交互信息的窗口。它的主要功能是检查用户输入的数据，显示系统输出的数据。

如果用户服务层需要修改时，只需改写显示控制和数据校验程序，而不影响其他两层。检查的内容也只限于数据格式和取值范围，不包括有关业务本身的处理逻辑。该层是浏览器。

3、商业服务(中间层)

崭新的一层是商业服务层，它是应用的主体，它包括了应用中全部的业务处理程序。除了输入/输出在用户服务层、数据库在数据服务层外，全部的统计、汇总、分析、打印功能全部封装在商业服务层。

他的一方面起传递数据作用，一方面进行强大的数据处理。该层还承担安全性检查的任务。

4、数据服务（数据库）

数据服务层就是数据库管理系统（DBMS），负责管理对数据库数据的读写。DBMS能迅速执行大量的数据的更新和检索。一般商业服务层通过发送SQL命令来操作数据库的数据。

5、采用B/S/D架构的优势

浏览器Browser/WEB服务器Server/数据库服务器Database是解决公共信息服务以及交互相应动态服务最适用的一种应用模型。实现了真正意义上的瘦客户，大大简化了应用系统的分发、配置管理和版本管理工作。

6、分布式

C/S技术的出现，给系统集成方案带来了集中的信息和本地的PC环境，但其数据的共享程度是很不够的。当今的信息技术需要新的解决方案，它提供以客户为中心的用户界面和Web的分布结构，它带有IT环境的个人特征，如数据存取、安全性能等，这就是我们通常所说的三层结构。

7、Web结构的优势

在Web结构中，事务层和数据逻辑层放在中间组件层，这是关键，是与C/S结构的最大区别，它能解决以下几个问题：

客户端很瘦小，并且很容易在运行时自动升级；

事务层可在跨平台的客户端上共享；

不同逻辑组件的分离意味着图形设计人员、事务逻辑开发人员和数据库分析人员可以独立地设计他们各自的部分；

统一的、抽象的用户界面可使用户更有效地从同一数据源中存取数据；

8、开放性

Web是一个开放的环境，应用由复用组件集成，通过标准语言汇编、跨平台的统一协议发布，用标准用户界面显示，它与硬件平台和操作系统无关。

1）充分利用现有IT资源

由于系统必须适应不断变化的业务需求，利用已有的资源系统方面的投资，而不是重新制定全盘方案就变得很重要。这样，一个以渐进的方式建立在已有系统之上的服务器端平台机制是系统所必需的。

2) 高效的开发

这样开发人员可以把精力集中在如何创建逻辑上，相应地缩短开发时间。由中间件提供复杂的中间件服务。

状态管理服务—让开发人员写更少的代码，不用关心如何管理状态，这样能够更快地完成程序开发。

持续性服务—让开发人员不用对数据访问逻辑进行编码就能编写应用程序，并且生成更轻巧，与数据库无关的应用程序，这种应用程序更易于开发与维护。

分布式共享数据对象CACHE服务—让开发人员编制高性能的系统，极大提高整体部署的伸缩性。

* + 1. **全面应用XML技术及Web Service技术**

系统全面采用XML、Web Service技术进行数据、服务描述及数据交换。

XML（eXtensible Markup Language,可扩展标记语言）是Internet上数据表示和数据交换的新标准。它是ISO（International Organization for Standardization，国际标准化组织）的SGML（Standard for General Markup Language，通用标记语言标准）的一个简化子集。XML关注信息本身，是Web上表示结构化信息的一种标准文本格式。与传统的注重页面信息显示的HTML（Hypertext Markup Language, 超文本链接标示语言）相比，关注于内容的XML具有诸多优点：良好的可扩展性，语言简单有效，可自行定义标记；内容与形式的分离，主要刻画数据内容，不考虑显示效果；有严格的语法要求，便于分析统一和与数据库信息转换；便于传输，为纯文本形式，可通过Http协议直接传输，可跨越防火墙；等等。

在XML基础上发展起来的Web服务（Web Service）使用基于XML的消息处理作为基本的数据通讯方式，消除使用不同组件模型、操作系统和编程语言的系统之间存在的差异，使异类系统能够作为计算网络的一部分协同运行。开发人员可以使用像过去创建分布式应用程序时使用组件的方式，创建由各种来源的Web服务组合在一起的应用程序。由于Web服务是建立在一些通用协议的基础上，如HTTP（Hypertext Transfer Protocol, WWW服务程序所用的协议），SOAP（Simple Object Access Protocol，简单对象访问协议），XML，WSDL（Web Services Description Language，Web服务描述语言），UDDI（Universal Description，Discovery，and Integration，通用描述发现和集成协议）等，这些协议在涉及到操作系统、对象模型和编程语言的选择时，没有任何倾向，因此Web服务有很强的生命力。

* + 1. **基于UML 2.0进行系统建模**

整个系统将采用UML2.0 “41”视图进行系统建模。广义地看UML，它已经不仅仅是一种建模语言，而是一个可以用于定义语言家族的元元核心和一个通用建模元语言的结合体；作为狭义的UML，UML 2.0较之以前的版本，在基于构件的软件工程、实时和嵌入式系统、业务过程的描述能力等方面都有很大的增强。 OMG的UML修订任务组和分析设计组的联合主席Cris Kobryn表示，UML 2.0已经变成一个基础更坚实的规范，可以为未来的软件工程、测试和业务规则建模提供更强大的支持。

* + 1. **面向构件技术及方法论**

面向构件技术整合了传统的构件技术、模型驱动技术和面向服务技术。构件的意义超越了技术层面的代码集合，而是真正做到与业务层面的内容相映射。构件将成为表达业务需求的最小单元，在特定行业中，通过积累可以形成相对完备的客户业务需求构件库，以构件组装的形式快速搭建客户的应用；以构件修改和构件增减的方式快速满足客户业务需求的变化。其次，从构件的技术实现角度来说，可以用四个要素来陈述软件构件模型：构件本身、该构件的插口、构件与其他构件协作的能力、以及构件的使用者。

面向构件的开发是一种软件开发手段，在开发周期的不同阶段和不同方面，包括需求分析、结构、设计、建立、测试、上线、支撑性技术架构、项目管理等，都以构件为基础，同时为了使构件可随时用于组装，这些构件必须作为项目的零件来建造。

本系统将采用面向构件的系统分析与设计方法。

* + 1. **基于组件模型的系统内核结构**

组件模型是系统架构的一种形式，软件开发过程从过程功能模型、面向对象模型、到组件模型。广义上讲，组件就是实现一类业务功能的、可重用的、可独立部署和设计的程序集合，这些程序有明确和完善的接口定义，通过接口完成功能请求，具体实现则通过封装机制屏蔽，而内部通过多种设计模式，保证组件的合理性。

采用组件模型可以通过业务功能封装在不同的组件中，实现功能分解，降低系统的耦合度，保证系统中的各个组件能够独立地修改和扩展。同时，组件模型还支持通过组件扩展系统功能，保证系统能够可持续的进行扩展。

在本系统的设计过程中，通过提炼业务功能需求和系统需求，分解业务处理流程，把系统划分为若干通用组件和若干业务功能组件。通过系统平台提供的组件管理工具实现组件的配置和管理，通过流程和功能把组件整合成相应的系统功能，这样，可以从两个方面保证系统的可持续扩展能力：

1、充分利用已有的成熟通用组件，加快系统的开发速度，通过更换这些通用组件，可以实现基本功能层面的功能扩展；

2、抽象并实现业务功能组件，实现业务功能的快速搭建，通过扩展业务组件，可以实现业务功能扩展。

通用组件和业务组件是应用系统稳定、持续、高效运行的核心组成部分。总的来说是将逻辑及应用的同类或相似的概念和方法抽象出来，以类的形式加以约束和实现，并定义相应的接口，也即定义数据的输入输出的规范；再将逻辑或功能相关的类集合在一起构成一个组件（类包），来完成一个或一组功能的实现；最后是将各个组件统一进行封装，给表示层提供清晰明确的接口，并通过自身相对数据层的访问接口与其进行通信。

* 1. **系统功能设计**
     1. **数据中心升级改造**

1.数据仓库

统计分析系统的真正关键是数据仓库的存储和管理。数据仓库的应用目标和数据的组织管理方式决定了它有别于传统数据库。要决定采用什么产品和技术来建立数据仓库核心，则需要从数据仓库的技术特点着手分析。

数据仓库中的数据是来源于联机事务处理系统长期积累的历史数据，

数据仓库所涉及的数据量比传统事务处理大得多,而且随时间的推移，其数据量还在不断的增加。从现有技术和产品来看,只有大型关系数据库系统能够担当此任，关系数据库经过近30年的发展,在数据存储和管理方面已经非常成熟, 非其他数据管理系统可比。目前不少关系数据库系统已支持数据分割技术,能够将一个大的数据库表分散在多个物理存储设备中,进一步增强了系统管理大数据量的扩展能力。采用关系数据库管理数百个GB甚至到TB的数据已是一件平常的事情。目前交大学院数据中心使用了ORACLE数据库，可满足此重任。

数据仓库中的数据存储首先涉及到数据缓存区。数据缓存区区域是临时数据存放区，其数据模型完全按照原始系统的数据格式。

ODS为操作性数据存储区，它基本保持业务源系统的数据结构不变，由数据缓存区提供每天增量数据加载到ODS。ODS根据具体需要，一般保存3-6个月的历史数据，为历史交易查询和操作性报表和操作性应用等提供数据支持。

DWD是整个系统的核心，依据逻辑数据模型划分10大数据模型主题存储和管理来自各种源数据系统的数据（包括当前及长期的历史数据），并为访问用户提供数据服务。

数据转换和存储层还包含从属数据集市，应用数据区就是一系列从属数据集市（DM），这些数据集市的数据来自DWD或DWA，可以确保其数据质量和数据一致性。对于某些特定的应用，例如某些业务报表其实时性要求非常高，那么也可以通过数据缓存区区域为其提供数据。

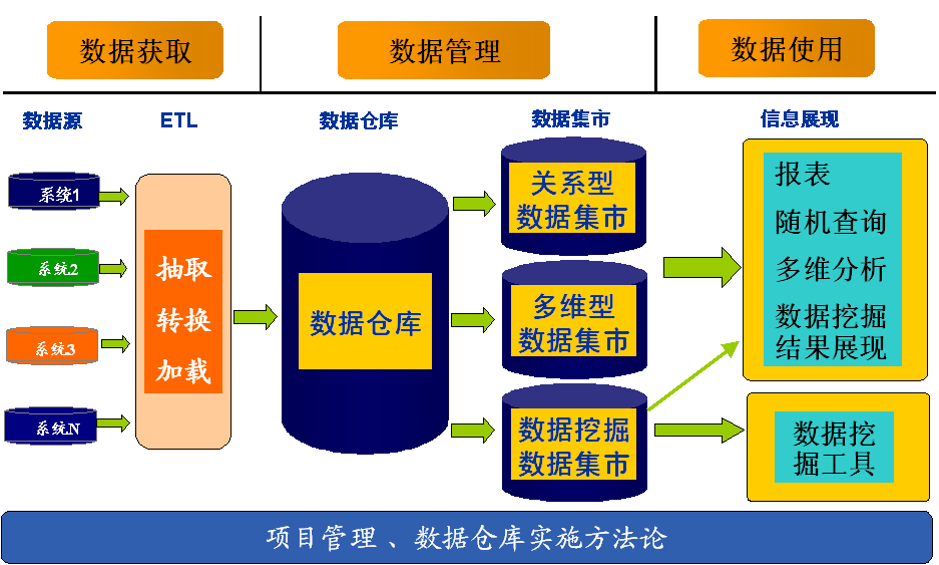


图 2 数据仓库逻辑结构图

基于交大学院数据中心信息构建的微型数据库存储，主要是将案件、服务商等的基础数据按照数据标准化进行清洗、转化，为OLAP分析模型提供数据支撑。

数据仓库为所有用户服务，具备极高的扩展性和性能，提供完整的、即时的数据，强化BI和分析能力。

2.数据ETL

针对分析模块中的数据进行数据的清洗以及抽取等。ETL过程，完成将业务源系统的数据，进行抽取、转换、（清洗）、加载到数据仓库的过程（同理，数据仓库的数据向数据集市的流转也需经过ETL过程）。通常，ETL过程的具体内容包括，将分布的、异构的数据源中的数据如关系数据、平面数据文件等抽取到临时中间层后进行清洗、转换、集成，最后加载到数据仓库或数据集市中，成为联机分析处理、数据挖掘的基础。

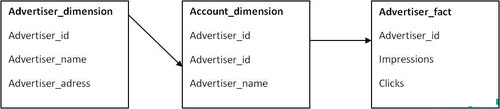
ETL是数据中心建设过程中的非常重要的一环。它是承前启后的必要的一步。在技术上，ETL主要涉及到关联、转换、增量、调度和监控等几个方面。数据仓库系统中，数据不要求与联机事务处理系统（业务系统）中数据实时同步，所以ETL可以定时进行。但多个ETL的操作时间、顺序和成败对数据仓库中信息的有效性至关重要。ETL过程、实现方式（设计）与质量，最终影响数据仓库与数据集市加载数据的准确性、完整性、一致性、完备性、有效性、时效性和可获取性等几个特性。

ETL过程中，通常处理的内容包括：空值处理、规范化数据格式、拆分数据、验证数据正确性、数据替换、Lookup等。

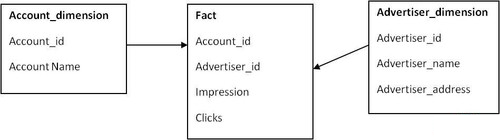
3.OLAP模型

根据多维模型建设原则，将DM层的数据按照前端展现的要求进行业务模型、物件模型等的星型或雪花型构建，满足即席查询、报表分析的需求。

雪花模型使用的是规范化数据，也就是说数据在数据库内部是组织好的，以便消除冗余，因此它能够有效地减少数据量。通过引用完整性，其业务层级和维度都将存储在数据模型之中。



相比较而言，星形模型实用的是反规范化数据。在星形模型中，维度直接指的是事实表，业务层级不会通过维度之间的参照完整性来部署。



雪花模型使得维度分析更加容易，比如：交大学院数据中心某特定加盟服务商，有哪些区域潜在客户或者客户在某日寻求此类服务商的服务。

星形模型用来做指标分析更适合，比如：交大学院数据中心某类型型的案件，接单率、派单率、满意率是多少。

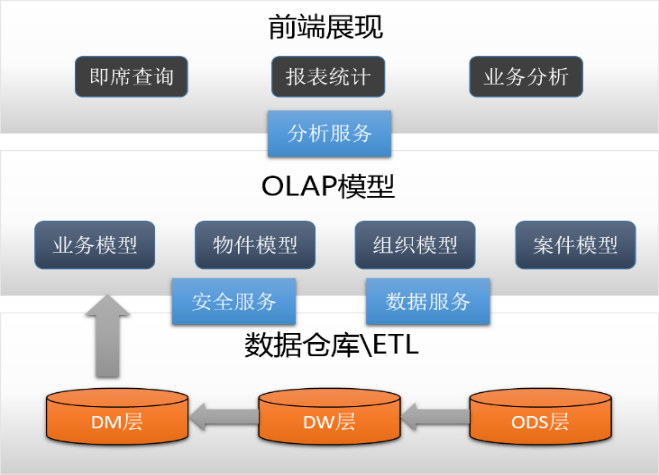


图 3 数据模型示意图

OLAP提供多维数据管理环境，典型的应用是对案件办理的建模与数据分析。

OLAP展现在用户面前的是一幅幅多维视图。

维（Dimension）：是人们观察数据的特定角度，是考虑问题时的一类属性。

维的层次（Level）：观察数据的某个特定角度（即某个维）还可以存在细节程度不同的各个描述方面（时间维：日期、月份、季度、年）。

维的成员（Member）：维的一个取值，是数据项在某维中位置的描述。（“某年某月某日”是在时间维上位置的描述）。

度量（Measure）：多维数组的取值。（例如：2014年12月1日，大峪街道，案件，10）。

OLAP的基本多维分析操作有钻取（Drill-up和Drill-down）、切片（Slice）和切块（Dice）、以及旋转（Pivot）等。

4.数据展现

数据分析和表现是数据仓库的门面，必须借助专业厂商的专业工具。它们主要集中在多维分析、数理统计分析、图表等。

数据仓库通过OLAP技术，能完成即席查询和动态报表的生成。数据仓库赋予数据多维的概念，使得用户可以从多种角度来观察数据，可以对数据进行任意的旋转、切分和钻取。这使得用户可以随机的查询数据仓库中的数据，获得数据仓库中的任意的数据。这就使得用户在完成特殊的查询时不需要编写程序，而仅仅通过简单的人机交互即可完成。

从人机界面来说，目前的工具都支持多种类型的常用图表，如报表、直方图、饼图、折线图等；另外，基于展现应用服务器的系统还可以为用户提供基于WEB的访问方式，大大提高的系统的易用性和易维护性。

5.统一用户

用户管理系统的建设目标是，统一管理交大学院智能统计分析系统的用户及其权限分配等管理功能；实现与交大学院系统无缝对接，实现统一用户登录。应用系统实现统一认证和单点登录提供基础的数据服务。

用户管理系统负责对平台的多类用户进行管理，主要包括以下部分：

1、用户管理：在系统中对用户采用分级分类管理的方式，即系统管理员可以管理所有用户，为所有用户分配操作使用权限，而拥有“组管理”权限的用户也可以管理与自己同组织的用户。具体功能模块包括用户注册、用户审核及授权、用户信息及状态修改、察看用户资料。

2、用户组管理：用户组是用户的集合体，类似于现实工作中的组织结构。注册用户可以隶属于用户组。用户组采用树型结构进行管理和显示，同时可以通过查看用户信息，了解用户所属组织和角色。

3、组织机构配置：用户组就是反映的用户隶属的组织机构，采用树型结构显示和管理，通过改变其父节点的位置，整体的移动组织机构节点和子节点的隶属关系。

4、角色管理：角色是具有相同职能的用户集合。管理员可以自由定义角色以及角色所拥有的权限。

5、权限分配：针对角色的权限进行分配组合，形成该角色的具体权限列表。

6、资源访问控制：针对细粒度的访问控制，提供资源项的定义，进而配置ACL访问控制列表，达到细粒度的数据访问控制管理

7、日志管理：记录用户的操作轨迹和系统的状态，如用户登录、非授权访问、敏感操作等。系统管理员可以利用日志管理提供的信息作为系统的监视、诊断和维护的依据。日志信息包括三种类型：信息、告警和错误。

* + 1. **决策辅助分析系统**

1.数据仓库设计

* 面向主题

操作型数据库的数据组织面向事务处理任务，各个业务系统之间各自分离。而数据仓库中的数据是按照一定的主题进行组织的。

* 集成

数据仓库中的数据是在对原有分散的数据库数据抽取、清理的基础上经过系统加工、汇总和整理得到的，必须消除源数据中的不一致性，以保证数据仓库内的信息是关于整个系统的一致的全局信息。

* 相对稳定

数据仓库的数据主要供决策分析之用（本项目用于Oracle BI系统以及呈现各种报表之用），所涉及的数据操作主要是数据查询，一旦某个数据进入数据仓库以后，一般情况下将被长期保留，也就是数据仓库中一般有大量的查询操作，但修改和删除操作很少，通常只需要定期的加载、刷新。

* 反映历史变化

数据仓库中的数据通常包含历史信息，系统记录了从过去某一时点（如，开始应用数据仓库的时点或业务系统起用的时点）到目前的各个阶段的信息，通过这些信息，可以对交大学院的发展历程和未来趋势做出定量分析和预测。

数据仓库从业务处理系统获得数据，主要以星型模型和雪花模型进行数据组织，并为用户提供各种手段从数据中获取信息和知识。

2.数据集市设计

数据集市是一个从集合数据中，为满足面向某个主题更专业分析而提供数据的平台。其数据组成是从数据仓库中抽取、再加工出来的。那么，数据集市就是企业级数据仓库的一个子集。数据集市可以分为两种类型：独立型数据集市、从属型数据集市。独立型数据集市直接从操作型环境获取数据，从属型数据集市从企业级数据仓库获取数据，带有从属型数据集市的体系结构。

3.元数据库设计

元数据是描述数据仓库内数据的结构和建立方法的数据。可将其按用途的不同分为两种，信息资源目录元数据和指标元数据。

指标元数据是数据仓库的设计和管理人员用于开发和日常管理指标数据仓库使用的数据。包括：数据源信息；数据转换的描述；数据仓库内对象和数据结构的定义；数据清理和数据更新时用的规则；源数据到目的数据的映射；用户访问权限；数据备份历史记录；数据导入历史记录；信息发布历史记录等。

信息资源目录元数据从决策服务业务的角度，描述了数据仓库中的信息资源目录的原数据。包括：决策分析主题的描述包含的数据、查询和报表。

4.基础数据库设计

1、数据层次划分

在基础数据库的存储层次划分上，逻辑上可划分以下几个层次：

 静态字典数据

 动态字典数据

 基础字典数据

各层次的存储内容如下：

表 1存储内容

| **层次** | **对象** | **内容** |
| --- | --- | --- |
| 静态字典 | 系统运行参数 | 组织机构、角色、资源等 |
| 动态字典 | 行业标准、规范 | 标准、电子政务规范等 |
| 基础字典 | 安全信息 | 系统ACL访问控制设计等 |

2、数据规范

基础数据库的建设必须遵循严格的标准规范进行，以避免数据的歧义以及使用混乱。建设规范重点考虑以下两个方面：

（1）编码规则

对于各类字典的代码编码需要统一定义，明确编码组成含义；对于需要关联的基础数据建立外键进行关联；编码的本身的组成以定长的数字或者字符组成。通过编码规则的统一，实现将唯一信息存储在一个地方，唯一性调用。

（2）数据项定义

各类数据对象的数据项根据交大学院相关单位用户确定，并在此基础上进行适当的项目扩展，以适应未来业务发展需要。

3、数据管理

为确保基础数据库数据的唯一性和可靠性，数据管理方面，需要注意三个方面：

（1）角色授权

对于各类角色与基础数据的操作需要严格的授权，授权形式可按照组织结构分级授权，实现集中与分布的多级管理模式。

（2）操作授权

在角色授权的基础上，对数据的增加、删除、修改、查询进行细化授权，原则上不允许对基础数据库的数据删除；对于增加、修改操作根据数据保密性质进行操作授权，修改时不允许对主键进行修改。

（3）数据安全

基础数据中类似口令、核心参数等数据采用加密算法进行数据加密存储，防止数据被篡改，此外也可通过校验算法增加校验位来确保数据的安全。

（4）数据监控

对所有的基础数据的改动系统提供日志记录（包括修改人、修改时间、修改项目等信息），关键数据提供历史修改记录。

5.智能分析

专题分析是高级的BI分析页面，根据交大学院的具体情况设定，可设置为老服务专题、志愿服务专题、便民服务专题等，供领导使用。通过仪表板对同类业务中的重点业务、关键维度、关键度量进行分析展现，以共享维度为基础，展现当前最新的业务数据，为领导提供最关心的业务分析结果；让用户一眼就大概明了自己要重点了解那一部分信息。仪表盘包含各种图表，初始粒度大，同时支持很深的下钻，可以钻取到相关的明细报表当中查看问题的疑点所在。仪表盘主要通过饼图、柱状图、趋势图、散点图、预警信息、记分卡等较为直观的展现形式表达业务信息。

提供用户自主在线动态分析功能，提高了决策系统的自主应用性。

6.阀值管理

通过设置阀值制定KPI的合理范围，对于超过范围的异常显示。

通过KPI（Key Performance Index ，关键性能指标）可以监控关键数据的发展趋势和状态。

7.报表视图

提供了两种以企业常见的报表格式为基础的分析控件：分析树、表格控件和图表控件、选取元数据查询的维度树，构建报表初始查询。通过设置报表参数生成参数化报表从而能够生成新报表。

8.动态分析

通过访问系统功能模型利用BI工具实现上钻、下钻、展开、转轴等分析操作，得到有用的数据结果报表。

报表的条件定制非常灵活。将固定或通用的报表条件定义在参数化报表中，并作为报表模板存储，再生成报表时，只需在报表模板基础上进行特殊的再定制，减少了重复定制条件的工作量，保证了定制的灵活性。

包括：

* 连接数据源
* 使用维度树选取维度和成员，构建查询
* 使用图表和表格视图显示数据
* 图表中的其它查看操作
* 基础分析操作
* 排序数据、过滤、标明异常值、时间智能等高级分析操作
* 设置报表参数，制定参数化报表

9.综合仪表板

用户还可以把自己相关的报表、图片、以及其他系统页面连接等信息资源联合组织进入综合仪表板，以得到关于某个主题相关指标的综合显示。

**1、添加窗口**

用户可以添加窗口显示已存报表到综合仪表板。

**2、添加标签**

用户可以添加标签主题显示特定主题的报表到综合仪表板

**3、综合仪表板管理**

用户可以对综合仪表板进行添加、删除操作，对名城以及其中标签 、窗口修改，设定用户访问权限等。

10.监控预警

定义和选取预警指标，监测绝对差异和相对差异的变化，不同领域的发展高低值之间的差异，设定预警指标临界值。

11.周期报告

周期报告是交大学院对一段时间内中心业务数据的统计汇总以及发展分析的总结与共享。通过对数据进行整理，按照默认模板，系统化输出文字性描述、数据报表，并按照菜单选项定义输出简单的饼图、柱状图或趋势图。同时，可在平台界面选择添加文本框，定义文本标题，用户可在界面进行文本编辑。

支持以Word、PDF等格式导出。

12.信息日报

用户编写《信息日报》上报，分类统计当日求助件数量。通过选择时间段，出具平台日受理案件总体情况。包括总体情况介绍、重点工作介绍，按照案件类型对案件进行分类统计。提供文字性叙述模板，确定报表格式，以饼图或柱状图的形式输出。用户可根据权限进行编辑修改。

包括时间定义、数据查询、图形选择、内容添加、模板修改、报告导出、历史查询等，根据权限不同，设置报告提交与报告审核功能。

13.信息周报

信息周报是对上一周（以日为单位进行划分）的案件、服务商等数据进行汇总统计，并进一步分析。用户对周报时间进行设置之后，系统根据模板对数据进行输出，并以柱状图或饼状图的形式进行直观展示。同时提供空白文本框，供执行部进行文本描述或模板设置。

包括时间定义、数据查询、图形选择、内容添加、模板修改、报告导出、历史查询等，根据权限不同，设置报告提交与报告审核功能。

14.信息月报

信息月报是对上一月（以周为单位进行划分）的案件、服务商等数据，进行汇总统计，并进一步分析，同时对上一月的诉求办理情况、加盟企业服务情况进行统计，为考核分析提供数据基础。用户对月报时间进行设置后，系统根据模板对数据进行输出，并以饼图或柱状图的形式进行直观展示。同时提供空白文档，供用户进行文本描述或模板设置。

包括时间定义、数据查询、图形选择、内容添加、模板修改、报告导出、历史查询等，根据权限不同，设置报告提交与报告审核功能。

15.即席查询

除了中心报表和仪表盘这一类固定报表，智能统计分析系统还将设计后台对相关人员进行开放，设计后台以报表设计区域为主，模型区域中的各种维表和事实表字段均按照业务人员能够理解的方式进行命名，将模型字段拖拽到设计区域很容易就能做出用户希望的报表，同时还可以将报表保存到个人文件夹下，方便重复利用和查看。

用户根据自己的需求，灵活的选择查询条件，轻松快速地创建、修改和编制报告、图表、数据透视表和信息仪表盘，系统能够根据用户的选择生成相应的统计报表。

即席查询的用户可分为三类：

1、决策用户：可使用的信息为面向全区所有信息；

2、执行部：决策用户信息应用的实现者，同时负责信息的主动挖掘、总结和发布；

3、其他部门业务用户：可使用的信息为部门业务相关信息。

16.综合统计

对行政管理中各类数据和相关业务数据的处理、统计、分析，提供数据的整合能力。

* + 1. **教师肖像数据表支持**

需要与原有学校MIS系统进行数据接口对接，添加教师个人科研教学数据信息及学院各系平局值对比功能，以图表的形式展现。做到教师个人数据与系统数据同步类比功能。

* + 1. **学校肖像数据表支持**

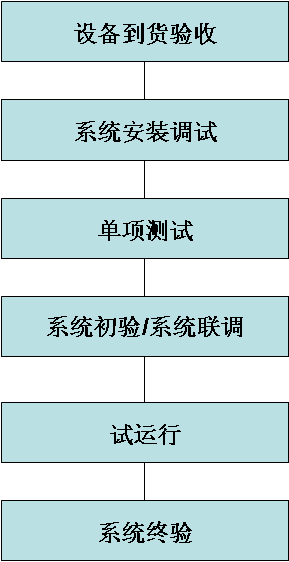
需要与原有学生管理系统对接，增添学院学生活动表单，建设录入、修改、删除等管理功能。通过学生成绩等信息数据的同步，扩展学生个人信息标的维度。对于超出指标的数据进行跟踪预警，增加消息提示和并通过手机向学生发送短信。

* + 1. **完善校友数据库**

增添校友信息数据库表单，开发校企合作信息功能模块包含：企业基本信息、企业来访及拜访记录、阶段性记录成果、教职工研究方向和科研项目与企业的发展相关性分析、校友企业拜访记录等。

* 1. **设备到货验收方案**
     1. **设备验收流程**

设备的验收流程如下所示：



图表4设备的验收流程图

* + 1. **设备到货验收**

设备由我公司运输至最终客户机房，开箱验货需由最终用户、代理商，以及设备原厂商的系统维护工程师三方共同进行。

我公司首先和最终客户确认机房条件安装条件。机房安装条件应符合设备安装要求。设备到达最终客户现场后，首先由我公司清点外包装箱的个数。同时系统维护工程师将协助进行外包装箱运输受损情况的检查，（主要检查在运输的过程中是否有碰撞及倾斜以及是否为原设备包装箱）。

设备开箱应该在最终用户、我公司、设备原厂商系统维护工程师三方到场的情况下进行，在产品维护工程师的协助和监督下进行开箱工作，开箱后需按照随箱所带的设备装箱单进行设备及配件的清点。如有与装箱单不符的情况需要在开箱/安装检查表上进行详细的纪录。并返回产品提供商的客户服务部门进行核查。

清点设备及配件完成并无误后，产品维护工程师将对负责安装的设备进行相应的安装工作，该工作需要最终用户及代理商进行相应的配合。安装完成后，产品维护工程师将按照设备安装手册的规定进行加电测试，如果系统加电正常，无任何报错代码和信息则设备验收和安装工作完成。如有相关设备报错信息，则致电产品技术支持中心进行相应的报修。

设备验收和安装工作完成后，产品维护工程师将在装机报告单上进行详细的纪录并请最终客户进行签字确认。

* + 1. **系统安装调试**

根据工程实施方案以及具体要求对到货设备进行调试安装，并按照合同要求，对系统进行集成。

我公司在对项目涉及的设备进行安装、配置与调试时，应对整个安装、配置与调试的每一步骤以及在安装调试过程中出现的各种问题及解决方法详细地记录到现场安装调试记录中，同时对系统中可能出现的问题及其解决方法形成注意事项向业主的技术工程师进行详细讲解。

安装、调试完成之后，按照建设方对工作环境恢复的要求，恢复工作环境，梳理机柜内和设备之间的连接线缆，使之美观、整齐，利于维护。

我公司在系统安装调试完毕后，向业主提交《工程实施手册/操作手册》（一式两份），验收完毕双方代表签字后各执一份。

* + 1. **系统联调测试/工程初验**

完成安装调试、单项测试检验后，进行整个系统的联合调试检验。我公司根据技术规范中的要求负责系统的联调，之后即进行系统初验工作，以检验系统是否可以投入试运行，改进并完善在联合调试检验中发现的问题。

在项目实施前，根据系统安装调试记录的有关要求，我公司工程师将与业主协商集成工作的测试时间、测试组组成人员、测试内容以及测试步骤和接收条件等，制定《工程初验测试方案》，《工程初验测试方案》需经用户方项目负责人签字认可并作为项目测试的测试依据，同时形成测试记录。

测试组成员按《工程初验测试方案》中要求的测试时间进入测试现场，根据计划中规定的测试内容及测试步骤对系统性能指标进行逐项测试，得出测试结果，形成《工程初验测试记录》并由测试组成员签字确认。

根据《工程初验测试记录》得出的测试结果和合同书中规定的功能及性能指标要求及系统接收准则，由测试组出具《工程初验报告》，并由测试组成员会签认可。

* + 1. **试运行**

在工程初验合格后，整个项目将进入系统试运行期。试运行期将进行以下工作：

1．试运行调查记录

在系统试运行期间，我公司的项目执行人员要对系统的功能、性能、稳定性以及系统的运行效果等各项关键因素进行全面的监测与记录，对出现的问题及时处理并形成系统试运行记录。

同时进行项目培训、文档整理等收尾工作。

2．得出试运行结论

试运行期满后，项目经理根据系统试运行记录得出的系统试运行结果，写出系统试运行报告，做出系统试运行结论，并经甲乙双方签字确认。

3．提交终验申请

各系统均通过测试与试运行后，项目经理根据《工程初验报告》及《系统试运行报告》向建设方提出项目验收申请。

* + 1. **工程终验**

“系统试运行”期满后，检验业主审计信息系统是否可以投入正式运行而进行的验收。

1．项目终验

建设方同意项目验收申请后，根据合同的要求组织项目验收。验收的时间及安排需经用户方、和我公司协商确定。

在项目实施前，根据系统安装调试记录的有关要求，我公司工程师将与业主协商集成工作的测试时间、测试组组成人员、测试内容以及测试步骤和接收条件等，制定《工程终验测试方案》，《工程终验测试方案》需经用户方项目负责人签字认可并作为项目测试的测试依据，同时形成测试记录。

测试组成员按《工程终验测试方案》中要求的测试时间进入测试现场，根据计划中规定的测试内容及测试步骤对系统性能指标进行逐项测试，得出测试结果，形成《工程终验测试记录》并由测试组成员签字确认。

根据《工程终验测试记录》，按照合同的要求对项目中设备的到货情况、系统功能的实现、项目文档的完整性以及项目的系统培训等重要项目进行验收并得出终验结论，业主与我公司签署《系统终验报告》，自三方签字之日起系统进入售后服务期。

2．顾客满意度调查

验收后要请用户协助填写《顾客满意度调查表》，了解顾客对项目的满意程度和存在的问题及顾客进一步的希望，以便不断改进我们的工作。

* + 1. **文档的验收**

我公司在整个工程的实施前、实施中、实施后向用户提交项目的整个文档，文档共分六类，分别为：技术文件类文档、安装计划类文档、网络配置计划类文档、安装结构类文档、系统测试类文档、系统验收类文档。

第六部分实施及进度方案

* 1. **项目实施方法论** 
     1. **项目策划阶段**

提出概念性设想，就项目各个方面的任务进行策划，进行项目风险分析，并就项目可能存在的关键性技术问题进行专题研究。

项目前期准备

1、主要任务

* 项目启动会议
* 确认项目范围和主要目标
* 确认项目阶段性验收及总体验收标准
* 确认项目实施计划
* 成立项目组
* 确定各项目小组的成员及各自的工作职责
* 确定各项目小组的阶段性工作目标
* 确定服务流程及方式

2、输出内容

* 《项目组织机构》
* 《项目实施计划》
  + 1. **需求分析与设计阶段**

进行需求访谈，收集相关资源和样例数据，获得客户需求，对需求调研收集的资料进行分析，得到各项应用或整体系统需求。根据获得的应用或系统需求对平台功能模块和数据项进行分析，实现系统全部功能。

1、业务需求调研

1)主要任务

* 确定系统用户，即确定哪些人将是建成后平台的最终用户群
* 确定需求调研的单位、部门与人员
* 确定系统数据源的采集范围
* 结合合同约定、以及用户的具体需求确定最终的数据采集范围，此时的数据范围指系统级
* 进行用户需求调研、访谈与确认
* 用户需求和数据源的筛选和分析
* 对用户的需求进行分析与挖掘，并分析用户需求的数据源支撑情况，了解哪些需求是没有数据源支撑的或难以支撑的，以便最终确定可施的需求的范围。
* 对收集的大量用户需求进行整理、归并，形成用户的总体功能需求和具体功能需求列表
* 对用户需求的优先级进行排序

根据用户对业务需求的急迫状况、需求本身产生效益的、数据源的支撑状况、处理流程的复杂程度等，制定业务需求的实现顺序。

2)输出内容

* 《业务需求说明书》
* 《软件功能清单》

2、需求分析与功能定义

1)主要任务

* 用户需求概要分析

通过对用户需求的分析，确定用户需求所涉及的、详细的数据源情况，包括数据的来源、粒度的要求。

* 业务需求定义

对实现用户需求所要建设的应用功能进行定义，包括分析的指标、权限要求等进行详细的分析与定义。

* 应用功能分析

对应用功能需求进行分析，区分技术性需求和非技术性需求。

2)输出内容

* 《软件功能需求规格说明书》

3、概要设计

1）主要任务

* 应用体系结构设计
* 业务流程分析
* 对原始数据、单据、报表进行分析，了解并分析数据间固有的业务关系；对系统涉及的业务流程进行分析，了解数据之间的业务规则、数据流向
* 建立实体模型
* 建立实体间依赖关系
* 分析并定义实体的所有属性项和关系属性
* 建立过程模型，以及过程中每个步骤涉及的表单和角色
* 建立数据库结构视图
* 按照关系范式理论，结合业务流程分析结果、功能实现的便利性，设计数据库结构并进行优化，包括实体、属性、关系的优化、历史类实体的处理。
* 功能模块分析
* 根据IPO（输入/处理/输出）理论对所有功能点详细分析，确认所有的功能的输入/输出和处理逻辑

2）输出内容

* 《概要设计说明书》
* 《数据库设计说明书》
  + 1. **系统实现阶段**

按照概要设计进行编码和单元测试，实现系统功能，并进行模块的装配测试和模块之间接口测试。

1、应用开发与单元测试

1）主要任务

* 开发环境安装配置
* 为团队开发环境准备必要的开发工作站、文件服务器、数据库服务器和应用服务器，并安装必要的开发工具和开发辅助工具
* 创建数据库
* 根据《数据库设计说明书》生成数据库创建脚本，并在数据库服务器上执行脚本
* 编写测试用例和测试数据
* 测试人员根据《需求规格说明书》编写测试用例和测试数据
* 应用功能开发与单元测试
* 开发人员根据《概要设计说明书》和项目进度阶段计划中所分配的任务编写功能模块代码，并进行功能模块调试和单元测试。
* 项目经理定期组织项目组成员对开发的功能模块进行互测
* 撰写帮助文档和用户使用手册

2）输出内容

* 数据库创建脚本
* 应用程序代码
* 测试用例和测试数据
* 《用户使用手册》
* 集成测试

3）主要任务

* 建立系统测试计划
* 执行系统测试计划
* BUG记录、整理、汇总
* 修正应用功能中的错误（BUG）
* BUG跟踪
* 生成系统测试报告

4）输出内容

* 《系统测试计划》
* 《系统测试报告》
* 《BUG记录与跟踪表》
  + 1. **系统运行与收尾阶段**

对安装部署的系统确认在实际运行环境中运行的适用性，后续通过不断的系统调优，确认系统达到开发预定的各项目标和标准。

1、系统上线试运行

1）主要任务

* 应用程序编译打包、安装
* 编写系统上线试运行操作流程说明和操作手册，修订相关的管理规定，并与相关业务人员确认其内容
* 下发数据接口规范、操作流程说明和操作手册等文档
* 收集历史数据样本，了解历史数据特征、定义情况
* 编写历史数据导入接口
* 历史数据导入/录入
* 现场联网测试
* 执行系统割接计划
* 试运行跟踪与现场服务支持

2）输出内容

* 《系统操作流程说明》
* 《系统操作手册》
* 修订后的管理规范和管理制度
* 《试运行跟踪日志》

2、项目验收

1）主要任务

* 建立并执行系统验收测试计划
* 移植开发系统到生产系统
* 执行用户培训计划
* 项目实施完成
* 签署项目验收报告

2）输出内容

* 《项目验收报告》
* 《项目总结报告》
  1. **项目实施进度**

本项目工期要求：自签订合同起到项目交付运行6个月。在时间紧、任务重的情况下，我们会加大人员投入、加班加点，利用系统开发期间进行安装和实施工作。总体实施计划如下：

* 1. 调研、需求分析，1个月内；
  2. 系统概要设计、详细设计，1个月内
  3. 系统研发，2个月左右；
  4. 系统试运行，1个月；
  5. 系统正式运行及验收，1个月。

实际实施过程中，以合同签订日为项目启动日，其他时间点依次顺推

项目进度时间表如下：

|  |  |  |
| --- | --- | --- |
| **项目编号** | **项目内容** | **实施时间** |
| 1 | 前期准备、调研 | 2017年1月 |
| 2 | 需求分析 | 2017年1月 |
| 3 | 系统设计 | 2017年2月 |
| 4 | 系统研发 | 2017年3月-4月 |
| 5 | 系统试运行 | 2017年5月 |
| 6 | 正式运行和验收 | 2017年6月 |

图表5项目进度时间表

* 1. **工作阶段划分**

项目整个实施工作大体划分为如下的4个大阶段。

* + 1. **需求梳理、分析和确认**

公司专家团队将对调研后的需求进行梳理分析，并经过内部需求评审后最终形成可提交客户的《需求分析说明书》。

* + 1. **系统设计**
* 概要设计阶段

概要设计阶段主要是建立目标系统的逻辑模型，完成数据库设计、划分功能模块、建立各功能模块间的层次结构及调用关系、确定模块间的接口及人机界面等。

* 详细设计阶段

详细设计阶段是对概要设计的一个细化，主要任务是设计每个模块的实现算法、所需的局部数据结构。

* + 1. **系统的开发、测试工作**

1. **系统编码阶段**
2. 阶段目标（里程碑）

完成整个项目系统的研发及功能修改工作，提交可测试的版本。

1. 客户工作事项

积极配合公司进行开发功能的确认；为公司提供及时的反馈信息。

1. 公司（实施方）工作事项

根据系统需求报告、设计文档进行编码。

1. **系统测试阶段**
2. 阶段目标（里程碑）

完成整个项目研发的测试工作，提供合格的产品；形成《系统测试报告》。

1. 客户工作事项

为公司提供及时的反馈；对测试结果进行评审，并协助公司项目组完成系统测试的确认工作。

1. 公司（实施方）工作事项

进行系统的全面测试；测试结束，提供规定的测试阶段文档。

* + 1. **系统的验收和试运行工作**

1. **系统验收阶段**

系统验收阶段包括初验和终验。系统初验是按照双方约定的初验条件我方发起初验申请并提供初验阶段需要的各个文档，用户方相关人员进行初验工作。

验收通过，要完成各单位的培训工作。

1. **系统试运行阶段**
2. 阶段目标（里程碑）

* 完成软件安装部署工作。
* 开发完成后将使用系统的各用户进行软件的试运行使用。

1. 客户工作事项

* 各级参与试运行的业务部门设置系统的各类参数。
* 督促检查基层单位工作的进展情况，保证基层单位的工作进度。
* 收集下属单位的意见，定期汇总后转交给公司进行解决。

1. 基层单位工作事项

* 执行上级部门制定的任务，进行组织结构、基础数据等数据的初始化。
* 使用交大学院本期项目系统的各项功能进行日常管理。

1. 公司（实施方）工作事项

* 协助客户进行系统的初始化和数据的初始化。
* 系统环境搭建部署。
* 解决软件使用过程中的问题，提供及时的技术支持。
* 协助客户进行系统权限、参数的设置。
* 对其它运行过程中出现的问题进行解决、完善和优化系统。

系统的维护工作从系统试运行便开始，我们将以钻石般的品质为用户提供优质的服务，具体方案可参见技术支持服务章节。免费维护期从终验通过之日起算，提供1年免费维护期。并根据软件使用情况，在质量保证期内免费进行修改、完善，确保系统软件质量良好和运行稳定。

* + 1. **各阶段交付物**

在项目实施过程中，我们将按计划提交下列文档：

| **序号** | **文档类型** | **文档名称** |
| --- | --- | --- |
|  | 招投标文档 | 项目招标书 |
|  | 项目投标书 |
|  | 项目合同 |
|  | 项目管理文档 | 项目计划书 |
|  | 质量控制计划 |
|  | 配置管理计划 |
|  | 用户培训计划 |
|  | 质量总结报告 |
|  | 会议记录 |
|  | 项目需求变更单 |
|  | 实施计划 | 项目实施计划 |
|  | 需求文档 | 需求调研报告 |
|  | 需求分析说明书 |
|  | 设计文档 | 概要设计说明书 |
|  | 详细设计说明书 |
|  | 数据库设计说明书 |
|  | 测试文档 | 测试计划 |
|  | 测试用例 |
|  | 测试报告 |
|  | 用户手册 | 管理员手册 |
|  | 安装部署手册 |
|  | 用户操作手册 |
|  | 培训手册 | 培训手册 |
|  | 试运行文档 | 试运行计划 |
|  | 试运行总结报告 |
|  | 验收文档 | 项目验收申请 |
|  | 项目验收方案 |
|  | 项目实施总结报告 |
|  | 项目总结报告 |

图表6各阶段交付物表

第七部分技术支持与售后服务

北京北信智科科技有限公司通过了有关系统集成、软件开发业务ISO9001质量认证和CMMI4认证。在公司的ISO9001程序文件中，对于工作人员在工作中的每一个方面都有着严格的规定。我公司关于售后的ISO9001程序文件规定了售后服务（发货、安装、调试、培训、维护、维修）的质量控制方法和要求。在售后服务与技术支持的过程中，公司以ISO9001质量体系作为提供优质服务的标准和保障，一个项目从立项到实施，到最终提交给用户及提交后系统的维护和产品维修，都有非常严格的制度和规定。这样做，不但能确保我们的工作可以按步骤有计划地进行，最重要的是确实保证了用户的利益，保证了我们提供的产品与服务满足用户的需要。

* 1. **售后服务与技术支持体系**
     1. **服务承诺**

针对本项目，北信公司如果中标将承诺履行以下售后服务的承诺条款：

1. 承诺免费送货、安装，提供良好的技术支持
2. 对用户提供7\*24小时不间断电话收接，1小时内电话响应，2小时内免费上门服务的优秀服务机制。
3. 硬件承诺原厂保修，实行三包
4. 提供原厂承诺保修函，采购服务器等大型硬件设备提供三年保修承诺
5. 除满足厂家标准服务外，为用户提供本公司其他优质服务内容
6. 在北京市内设有常驻机构，并针对本期项目配有专业的技术工程师 定期进行常规维修维护服务
7. 北信公司承诺自验收合格并签署验收文件后提供12个月质量保证期。即在1年的质量保质期内承诺对所开发系统免费维护和免费升级。
8. 北信承诺提供对本项目全方位的、有效的、及时的技术支持和服务。

对于项目中提供的硬件设备承诺免费维护三年，软件产品免费升级及维护一年，并且提供技术设备安装、调试、使用、维护、升级和新技术推荐等方面的免费咨询服务。

1. 远程技术支持。当系统出现故障，经用户许可后，北信公司将利用远程登录用户系统，进行故障分析、问题定位并提供解决方案。但对系统进行的任何配置、数据改动及其它可能对系统和业务造成不良影响的操作，将会经用户确认后进行。
2. 定期跟踪。项目验收完毕后，北信公司承诺通过定期电话、现场巡检等方式跟踪系统使用情况，听取用户意见和建议，及时分析系统存在的问题，并随时给予解决。必要时，承诺派遣技术人员去现场解决存在的问题。
3. 系统软件升级。质量保证期内，北信公司承诺会及时向用户通报系统软件升级情况，若用户需要对系统软件升级，北信公司将尽量在不影响用户使用现有系统的情况下，科学安排升级步骤，确保提供最新升级版本和相应的系统升级技术服务。
4. 现场服务。自系统验收之日起一年内，提供至少一名具备三年以上相关平台技术支持与运维经验的技术人员常驻用户现场服务。在驻现场人员以及通过远程支持均不能及时解决问题的情况下，将派技术支持人员在4小时内赶赴现场，协助用户完成故障排除、升级或迁移操作，对系统进行完整性检查并跟踪运行。
5. 免费维护期后的服务。在质量保证期结束后，北信公司继续提供对产品故障处理、软件升级等的服务，不以任何借口拖延或中断对产品的售后服务。
6. 保修期结束检查。在保修期结束前，由北信公司工程师和用户代表进行一次全面检查，任何缺陷由北信负责，再修理之后，北信将缺陷原因、修理内容、完成修理及恢复正常的时间和日期等报告给用户负责人。
   * 1. **服务理念**

北信公司依据ISO9001规范，以其在信息技术支持与服务领域丰富的实践经验和良好的信誉，以及雄厚的技术资源，与客户共同解决所面临的问题，为客户在IT运营管理方面提供一种高素质、高效率，全方位的服务。

“一切价值由专业化服务创造”，我们的服务理念是通过对IT系统(软/硬件)提供专业、标准和高效的运维支持和管理服务，通过提高IT系统的运营效率和可靠性、安全性，最终创造可靠的在线业务环境，提供优质的网络应用服务。

* 1. **售后服务组织机构设置** 
     1. **服务组织架构**

北信公司建立人员稳定、有业务素养的技术支持与服务队伍，不断跟踪业务需求的变化，进行系统的完善，提供全面的技术支持服务。北信公司系统开发项目客户服务体系组织结构包括：管理支持部、技术开发部、运维服务部。

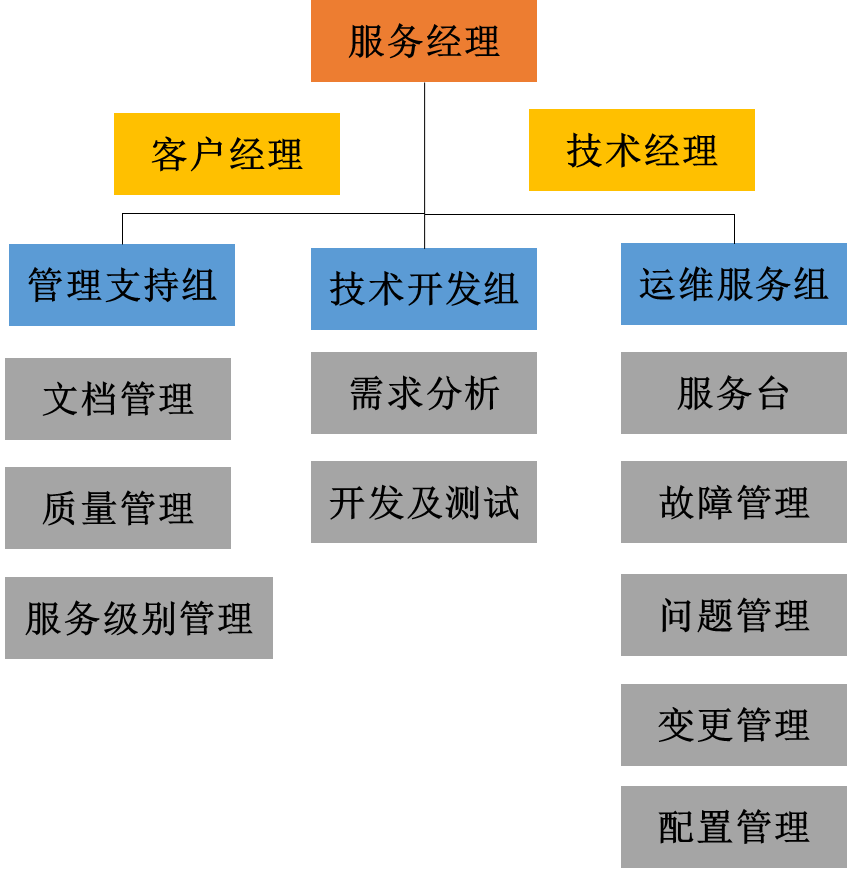


图 26售后报务组织架构图

1）服务经理，总体负责售后服务和技术支持工作，确保售后服务和支持功能能够达到向业主方承诺要求。

2）客户经理，与业主方进行必要的商务沟通。

3）技术经理，负责售后服务和技术支持的总体技术工作，负责服务团队的技术管理，协调解决各类技术问题。

4）管理支持部，按照公司管理要求，对售后服务和技术支持过程进行管理，确保各项工作规范有序，并对各类技术文档进行管理。

5）技术支持部，根据用户需求，进行相应的设计、开发、测试和集成调试工作，以及技术升级服务。

6）运维服务部，提供日常的技术支持和系统维护服务、系统巡检、性能调优、对潜在的故障点进行预防、技术升级、应急保障等工作。

* + 1. **人员保障措施**

对于项目负责人变更对本项目带来的风险的规避，一方面尽量保持项目组成员的稳定性，另一方面采用完善的文档管理制度，尽可能做到某个工作任务情况以文档为准绳，做到不完全依赖于该项目实施人员。项目组成员在工作的每个阶段都提交一定的工作文档，设专人监督和管理项目文档。

* 1. **售后服务与技术支持计划**

北信公司将针对北京市交大学院信息系统安全防护建设向业主方承诺技术后援支持。承诺自双方签署最终验收文件之日起1年内为开发软件系统的质量保证期，其中承诺提供为期1年的软件产品升级服务，所开发系统1年免费维护服务，并提供质量保证期满后的调试、维护、升级和新技术推荐等方面的免费咨询服务。

* + 1. **服务方式**

北信公司为本项目提供现场服务、热线服务和在线服务三种服务方式。

* + 1. **现场服务**

本项目承诺在售后服务与技术支持过程中，除出现以下情况：1）需要到现场进行故障调查、诊断、解决时，提供现场支持服务；2）用户的扩展服务，包括用户培训等；3）用户需要现场咨询和指导；4）应用系统的安装、调试等，提供现场支持外，保证在系统验收之日起一年内提供至少一人，具备3年以上与相类似平台运维经验的技术服务人员常驻用户现场服务。

* + 1. **热线服务**

对售后服务与技术支持过程中，出现以下情况提供7×24热线支持：1）用户故障申报、服务请求时；2）可以通过热线支持解决的故障；3）通过热线提供的咨询和指导；4）软硬件设备服务目录查询；5）故障解决进展情况；6）服务投诉。

* + 1. **在线服务**

在线服务包括Email、QQ、远程登录等形式。对本项目售后服务与技术支持过程中，出现以下情况提供热线支持：1）用户故障申报、服务请求；2）可以通过在线支持解决的故障等；3）通过在线提供的咨询和指导；4）软硬件设备服务目录查询；5）故障解决进展情况；6）服务投诉；7）电子文档传输等。

* + 1. **响应时间**

售后服务和技术支持可以分为：设备故障申报、用户技术咨询、服务请求和投诉处理。这些服务受理的统一接口是服务台，服务台受理故障后，由现场服务工程师或专业技术支持小组处理这些相关的服务。下面分别讲述服务响应时间。

* + 1. **服务受理时间**

1）服务台提供7×24小时固定客户服务热线服务；

2）提供 7×24小时移动客户服务热线服务；

3）同时提供7×24小时的EMAIL/FAX/书面/口头/QQ/WEB等多种方式服务，保持与用户的沟通渠道通畅、有效。

* + 1. **故障申报响应时间**

对于如服务中断、数据丢失、主要功能不能正常工作等系统故障，北信公司提供快速的响应时间：

1）提供7×8小时固定电话热线支持，7×24小时的手机热线支持；

2）工作日1小时内响应，8小时内解决问题；休息日2小时内响应，8小时内解决问题。

* + 1. **技术支持与服务内容**

北信公司为项目提供1年的质量保证期，为系统提供免费维护服务，并根据软件使用情况，在质量保证期内免费进行修改、完善，确保系统软件质量良好和运行稳定。质量保证期自系统验收合格并签署验收文件后开始计算。

* + 1. **质量保证期内技术服务内容**

一、常规支持服务

在1年质量保证期内，北信协助业主方完成日常系统及应用的维护工作，保证系统的正常运行。

1）产品的安装和调试

北信公司派遣工程师现场进行系统的安装、调试和测试，并记录产品安装日志在用户和公司备案。

2）故障处理

系统用户可通过北信公司的热线服务和在线服务（EMAIL、QQ、远程登录）方式报告问题。正常工作日内，北信公司服务团队将在正式接到用户通知后4小时内进行有效响应，例如电话支持，远程解决问题等，如问题不能解决，我们将派有经验的技术人员到达现场进行系统调试，履行其维护义务，帮助处理紧急事故。

3）定期检测服务

北信公司为系统提供定期检测服务，用户也可根据系统运行情况提出检测要求，系统检测将对系统存在的潜在安全或故障隐患进行分析并提出相应的解决方案加以排除。

4）系统升级服务

在系统终验报告签订后2年内，如果本项目涉及的北信公司自有软件产品推出新的版本，将为用户提供产品升级方案及升级服务，如升级中涉及对第三方软件产品的升级要求，将为用户提供一年免费升级服务。系统升级后，公司将提供系统变更的全部技术资料并完成相应培训。

随着业务需求的变化，对于用户所提出的修改、优化原有系统和增加新功能的要求，售后服务小组将需求提交系统开发组，系统开发组进行工作量评估，对于工作量较小的部分，系统开发组将进行及时的修改，并为用户提供最新的补丁程序。对于一些工作量较大的功能或结构变化，北信将在下一个版本中进行修正。以上修改，如发生在项目终验之前，北信将提供免费的产品支持，如发生在保修期内和保修期后，会以优惠价格对系统进行相应的修改。

在保修期内，如果北信公司对合同系统行了技术改进（包括但不限于相关的软件和硬件），如果业主方认为有必要，北信公司免费向业主方提供与这些改进有关的详细技术资料，并对本合同系统进行免费改进。

5）技术咨询服务

北信公司为提供系统调试、维护、升级和新技术推荐等方面的技术咨询服务。

二、应急保障服务

紧急情况的反应和处理是服务质量的重要方面。当前，信息系统往往承担着用户的重要甚至关键的业务或管理系统。当严重的信息系统故障（如宕机）发生，或影响生产的较大故障较长时间不能得到有效处理时，对客户而言，该故障实际上就形成了紧急情况。

北信公司将对于对客户业务造成较大影响、较为复杂的紧急情况，启动危急情况处理体系。由专职服务经理负责，成立危急情况处理小组，调集相关的资源。该小组需每天向公司汇报处理进展，每小时更新紧急情况处理系统的相关记录。该小组具有高度权威，能快速调动相关资源，找到北信公司及原厂商、合作伙伴中最具经验的专家，防止问题处理的任何环节出现延迟，以尽快解决问题。

北信公司将结合多年的运维和重大活动应急保障经验，将为系统应急保障提供完整的解决方案。对于系统在8小时内（节、假日也不例外）未解决故障和问题，北信公司将采取紧急预案，使系统得以正常运行。

* + 1. **质量保证期外技术服务内容**

保修期过后，北信公司将继续为本项目提供多样的支持服务手段。

1）技术咨询服务。保修期后北信公司提供调试、维护、升级和新技术推荐等方面的免费咨询服务。

2）软件技术支持服务。在法定工作时间内，以优惠价格继续为用户提供与服务期内相同质量的技术支持。

* + 1. **技术支持与服务流程**

以下为典型的技术支持与服务流程：

1）故障受理

服务台负责接受用户的技术支持与服务请求，提供7×24小时的受理服务。服务台接受到用户服务请求后，认真填写《故障记录表》，并把问题转交指定的问题管理组。问题管理组直接和客户交流，协调公司内各种技术资源帮助用户解决问题，并分析系统运行过程的隐患和问题，并形成纪录报告，提交技术支持部备案。

2）远程处理

指定处理问题的工程师查询客户文档并与用户现场维护人员联系，根据掌握的故障现象，向用户维护人员提出问题处理指导或远程故障诊断。

（1）电话指导：判断故障由外部原因造成或者故障板件、软件设置等引起，则问题处理人可以电话指导用户做相应的处理措施。

（2）远程故障判断和处理：在掌握故障信息不足以对故障做定位，或者需要远程登陆设备后才能实施解决措施，同用户进行沟通了解必要信息后再进行相关的作业。

（3）现场技术支持准备：在对用户进行电话指导或实施远程登录手段的同时，将依据故障的性质作好必要的现场技术支持的准备工作。

准备备品、备件、维修或升级软件和相关设备。

查阅用户档案，了解设备组网、版本情况，关注其特殊设置或遗留问题。

人员联系信息的汇集：包括用户维护人员联系电话、公司相关技术支持工程师的联系电话。

工程人员解决问题后应将问题处理的结果记录在《问题记录表》中，记录详细的故障信息及处理过程，有无遗留问题等，回复问题的报告人，并将电子文档拷贝给客户代表并归档保存到FAQ库中以备后用。否则落实工程师到现场处理问题。

3）现场处理

如果需要现场进行解决的问题，故障处理组技术人员必须拟定现场解决方案。解决方案经客户同意后才能进行现场实施，双方的确认必须是书面形式，并传真给技术中心。成功实施后再通知客户进行维护。对未经过客户同意的解决方案绝对不允许实施于客户的系统。技术人员解决问题后应将处理的结果记录在《问题记录表》中，并将电子文档拷贝给客户代表归档保存到FAQ库中以备后用。如果现场实施失败，必须上报技术中心，由技术中心出面与客户协商问题解决时间并指定专门小组负责该问题。

如果问题无法按照普通解决方法予以解决，由故障处理研究是否需要并制定升级方案、替代方案，成立专门小组，和用户协商，对系统进行升级和替换。

4）回访

问题解决后，三天内责任工程师将对系统运行情况做进一步的跟踪了解，确保系统能正常稳定运行。

* + 1. **服务质量保证措施**

北信公司基于对客户及其业务驱动的理解，通过建立客户服务规范和用户满意度指标，进行项目客户满意度测评和现场服务满意度测评来了解并掌握客户对服务的感知，据此采取改进措施，提升服务水平与服务质量，不断提高客户的满意度。

* + 1. **客户服务规范**

北信公司根据自身业务特点，建立客户服务规范，规定提供客户现场服务的人员应遵守公司《现场服务守则》：

1）虚心接受客户批评与建议。处理好客户关系，在任何情况下不得以任何借口与客户发生冲突。

2）工作积极主动，谁接待谁负责，不相互推诿，实行“首问负责制”。

3）进房间前先敲门，经允许后方可进入；如客户不在，应在门外静候。

4）服务结束后，征得客户同意后方可离开，并保持环境整洁、干净。

5）主动归纳、汇总服务中出现的问题、经验和教训。

6）使用标准文明礼貌用语与客户交谈，见面要说“您好”。

7）举止大方得体、彬彬有礼，维护公司利益。

8）衣着整洁，仪表端庄，有良好的精神风貌。

* + 1. **服务报告制度**

为确保售后服务质量，并让客户更清晰地了解售后服务实施情况，北信再每一次安全服务完成后，将提供售后服务实施报告。内容包括实施服务的类型、时间、问题分析、解决方案或处理策略建议、实施步骤、实施内容等，使客户可以全面地了解系统运行状态、售后服务情况，便于客户做出正确的决策。

* 1. **其他优质服务**

为了保证本期安全系统等级保护测评的顺利有效进行，测评前参照附件1公安部颁发的系统安全等级保护测评评分标准，提前按照等保三级要求进行软件自测，涉及到的应用系统包括：门户网站，业务系统，呼叫中心相应系统，及时发现问题并整改，减少业主方时间成本与资金成本。

第八部分项目培训

* 1. **系统培训概述**

为了保证北京交通大学学院系统本期项目系统能够顺利移交用户方使用，我公司特为本项目制定了详细的培训方案，以便用户单位进一步明确系统操作细节，保证系统使用实效。

培训内容包括：系统应用培训、数据库管理培训和用户操作培训、系统整体日常运维培训、系统故障应急处理培训、系统使用人员安全意识培训。

通过培训可以使本系统的多级使用者从系统的结构、设备系统的性能、操作使用方法、维护管理技术、定制和升级等各个方面得到全面的掌握。

本方案适用于系统试运行阶段、正式推广阶段及系统长期使用过程中涉及的各个用户。

* + 1. **培训目标**

用户培训目的是让用户能够掌握相关软件操作、维护和管理工作，达到能进行独立使用、日常故障排除、日常维护等目的，保证我公司开发的系统能够正常、安全地运行，切实对用户业务带来帮助。

培训内容在专业化的基础上，将充分考虑用户对象和日常使用系统的内容不同，设定不同的课程，确保每个接受培训的人都能够顺利进行业务操作，完成本岗位工作，提高工作效率。

* + 1. **培训内容划分**

培训内容分为：日常运维培训、软件使用培训。

1．日常运维培训：

日常运维培训包括：系统整体日常运维培训、系统故障应急处理培训、系统使用人员安全意识培训、应用操作系统培训。

* 系统整体日常运维培训是指我公司针对本系统提交系统运行阶段日常维护工作方面的培训。
* 系统故障应急处理培训是指我公司针对本系统试运行阶段与其他类似信息化项目的系统故障处理办法方面的培训。
* 系统使用人员安全意识培训是指根据本项目系统安全建设要求结合客户要求对系统使用人员、系统维护人员进行安全操作方面常识的培训。

应用操作系统培训是指对本系统涉及的部分操作系统日常操作方法进行培训。

2.软件使用培训：

软件使用培训包括系统应用培训、数据库管理培训和用户操作培训。

* 系统应用培训是指我公司针对客户系统管理员进行系统访问、指标定义等定制开发方面的培训。
* 数据库管理培训指本系统日常数据备份、恢复等数据库管理方面的培训。
  1. **培训对象**

培训对象分为三个角色：一般使用人员、系统维护人员和管理（领导）人员。

* 1. **培训方式**

我公司经过多年的积累已经形成了完善的培训和知识转移体系，并由公司经验丰富的实施人员及培训讲师组建了一支实力强大的培训团队，专项完成北京交通大学学院系统本期项目系统用户培训及知识转移工作。

* 1. **个性化培训**

在上述培训方式的基础上，针对用户各使用单位提出的个性化培训需求，我们将会参照集中培训和分区域培训制定的培训目标及培训计划，派出培训教师并提供培训资料。具体的培训内容或方式也可根据具体的个性化要求双方沟通制定。

对于后续的培训需求，由于不属于事先约定免费培训的范围，我公司将按照规定收取相关的培训费用，费用由双方协商确定。

* + 1. **培训流程**

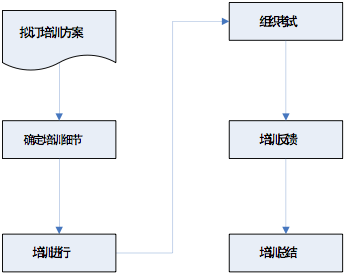


图 27培训流程

培训流程图说明：

* 根据项目需求，初步拟订培训方案，确定培训方法，培训人员组成等。
* 进一步确定培训时间，每期人数等细节
* 按照培训方案及确定的时间组织培训，合理安排培训课程。
* 培训结束后组织进行系统考核。
* 填写培训反馈表，搜集培训意见及建议，为完善后续培训提供参考资料。
  + 1. **培训教材**

我公司将为本项目编制专门的培训教材，培训教材全部为专门编写的实用性教材，我公司提供给参加培训人员人手一套，包括：

* 《培训大纲》
* 《培训计划及指南》
* 《信息系统安装、部署手册》
* 《信息系统运行维护手册》
* 《信息系统故障应急处理手册》
* 《信息系统涉及操作系统操作手册》
* 《信息系统数据库管理员手册》
  1. **培训课程**

根据北京交通大学学院系统本期项目系统的实际情况，我公司制订了详细的、富有针对性的培训课程计划。

* + 1. **培训课程介绍**

北京市交大学院信息系统安全防护建设项目使用培训：

|  |  |
| --- | --- |
| **技能要求和前提** | **课程描述** |
| 掌握计算机基本操作，熟悉浏览器、上网等基本操作，熟悉本单位的数据处理工作制度和流程 | 1.学会使用系统  2.掌握各种数据编辑录入、调整、审核、数据提交使用等实际操作  3.熟悉综合查询分析  4.掌握简单的系统应用技巧 |

表格 23平台系统使用培训表

北京市交大学院信息系统安全防护建设项目管理维护培训：

|  |  |
| --- | --- |
| **技能要求和前提** | **课程描述** |
| 掌握计算机基本操作，熟悉浏览器、上网等基本操作，熟悉本单位的业务制度和流程，有应用系统管理的经验 | 1.掌握系统的安装和配置  2.学习系统运行状态的监控方法  3.学会解决系统常见的故障或错误处理办法  4.掌握系统管理的各项功能  5.系统权限设置  6.日常的基本维护等 |

表格 24平台系统管理维护培训表

北京市交大学院信息系统安全防护建设项目领导使用培训：

|  |  |
| --- | --- |
| **技能要求和前提** | **课程描述** |
| 掌握计算机基本操作，熟悉浏览器、上网等基本操作，熟悉本单位的业务制度和流程。 | 1.软件功能基本操作。  2.掌握系统常用查询。  3.掌握系统查询分析功能使用。 |

表格 25平台系统领导使用培训表

* + 1. **培训风险控制**

针对以上可能出现的风险，在培训中需要注意以下几点，以最大限度减少在培训过程中风险发生的可能性：

* 项目双方确定培训工作负责人，以保证培训工作中双方有效沟通和责任明确。
* 严格按照计划控制项目进度，保证培训计划按时实施的充分可能性。
* 对于确定的培训需求及细节要有相关的文档确认，以保证需求不出现较大变化。
* 合理搜集集中培训结束后本系统使用单位的个性培训需求，由客户培训方面负责人要求系统使用单位上报培训需求，经汇总统计后将培训需求提交给培训负责人，由我公司负责具体培训工作的安排。我公司培训负责人在得到培训需求后，提交给具体的项目培训小组安排培训实施计划，双方确认。
* 我公司将全力保证培训计划的顺利实施。
  + 1. **培训承诺**

我公司向用户郑重承诺：将在北京交通大学学院系统本期项目系统实施完成后，由选派专业培训人员，严格按照项目要求，制定培训计划和培训内容，按照项目培训计划和培训规范，以及用户要求，圆满的完成项目的培训工作，保证系统培训能够高效、顺利、圆满的完成。

总结

根据以上分析，得出以下结论：

1. 北信公司从需求分析、技术架构、解决方案到实施安排、技术支持、售后服务各方面做好了充分准备，请各位专家放心地选用北信公司作为本次项目的合作伙伴。

2. 从项目系统安全、进度、扩展性、集成性出发，要选用稳定、成熟、能够持续服务的合作伙伴。

北京市交大学院本期项目系统招标书表达精准，路线明确。在此，深深感谢前期领导和专家提供的思路。

# 技术文件

# 第一部分公司介绍

北京北信智科科技有限公司是由多年从事IT行业开发人员创立的年轻公司,我们致力于提供专业化的应用软件和服务，度身为客户提供完善的信息化解决方案。已经拥有了自主研发的IP呼叫中心、政务管理平台、OA、BI商业智能分析系统、CRM、CMS等产品。我们拥有强大的研发能力及丰富的项目实施经验，典型客户包括电子政务、电子商务、旅游、商旅、物流、金融保险、IT服务业、电信增值服务业、电力业、金融保险业、消费产品与服务业、家电、制造业、政府、医疗卫生、医药保健品业、邮政、交通运输、能源、人力资源、广电媒体等.THINKPBX(北信智科)所有产品都拥有自主产权的、完整的解决方案，并能提供从咨询、设计到软件开发及维护全方位的360度服务;产品系统稳定,功能全面。

本公司是一家提供领先IT解决方案和专业服务的高科技企业，致力于为政府、企业的业务信息化提供应用软件和行业解决方案、系统管理和数据安全等各类通用服务，以及基于解决方案的IT咨询规划、系统集成、定制软件开发、维护保修、资源外包等专业化服务。公司拥有一支经验丰富而又朝气蓬勃的团队，平均年龄30岁，平均行业从业年限超过5年，项目经验丰富。志存高远，锐意进取。北信科技将继续以良好的信誉和现有能力为基础，并一如既往地秉承“诚信、务实、进取、专业、共赢”的公司理念，与每一位客户共同成长与发展，为其提供更全面、更优质的信息化服务，成为其不可或缺的忠诚伙伴。同时成为员工学习、生活、发展的家园，做一个值得信赖的专业化的IT服务公司。

1.我们的优势

提供从咨询、方案设计、项目实施到运营管理培训的“一站式”服务深厚的行业知识和技术积累，严格的项目管理制度、完善的实施方法，严格按照国际化认证的标准来保证项目实施质量（ISO9001）和软件研发的质量（CMM）

2.卓越的解决方案与产品

* 您 需 要： 符合您需求的个性化的解决方案与性能稳定的产品
* 我们秉承： “全过程客户体验”的经营理念从而为客户提供量身定制解决方案及产品

3.度身定制的全方位服务

* 您 需 要： 服务 － 帮助您成功的服务。
* 我们提供： 从售前咨询、售中方案制作、售后技术支持、系统运营管理咨询全程支持。

4.良好的质量保证体系

* 您 需 要： 稳定的系统、可值信赖的合作伙伴。
* 我们奉行： “零BUG上线, 100%投诉得到响应, 100%问题得到解决”的质量目标。
* 我们导入： QAS & QCS体系以消除一切可能的质量隐患。

5.丰富的成功案例积累,深厚的项目实施经验

* 您 需 要： 业界翘楚的成功应用
* 我们执行：严格的项目管理体系
* 我们拥有：近十年服务经验、上百家客户的实施体会

人员是北信智科实际存在的生命力组成，人才是公司赖以生存和发展的基础。

北信智科的发展源自团队中每一位成员的贡献，向每一位成员提供应有的物质回报和精神需求的满足，将是北信智科不懈工作的努力目标和方向。

第二部分方案概述

* 1. **项目的需求**

1. 数据融合及治理

基于现有数据中心的数据进行质量探查、数据清洗、数据集成；执行数据标准规范和数据融合策略；解决数据不规范、标准不统一的数据质量问题、数据质量底下、数据使用者的决策依据不准确的问题；通过对数据的探查、清洗、去重、比对、监控和信息挖掘，提升数据质量。梳理数据来源、变更及审核机制。梳理学院部门之间数据资源产生、使用及管理的UC矩阵表。数据资源子集及说明表。

1. 决策分析

利用搭建数据中心的数据，将财务、科研、教师、学生、校友等方面数据进行分析。着重形成教师肖像，包含教师科研情况分析、项目成员关联分析、科研成果分析等方面，同时利用相关学生数据建立学生画像。根据为学院和各职能部门应用需要，利用数据分析与挖掘知识，实现学院财务等多方面统计信息的全面汇总分析，为院领导及相关部门提供丰富有效、高效可视的决策信息。

1. 教师工作绩效自动评估

教师工作绩效自动评估系统通过整合人事、科研、财务、教学等多门类数据信息，采用教师教学情况、经费效益、经费使用情况、项目完成情况、论文专著情况、案例情况、社会服务等多维度的评价因素，全方面呈现教师在科研和教学工作的成绩，从而为教师的入职、晋升、聘任、培训和奖惩提供定量化决策依据。为学院管理分析特色人才，精准扶持，争取各类资源，人才拔高等提供数据依据。

1. 教师人员关系图谱

团队合作是学院科研工作模式的重要组成部分，了解团队组成的关系对后续学院发展新项目、组件新项目团队以及评价项目团队合理性等方面提供极大帮助。基于学院数据中心提供的信息资源，利用数据挖掘与分析建立教师关系科研相关数据图谱，对学院科研发展提供决策分析。

1. 财务管理决策分析

支持与协同办公系统的数据集成，为学院决策分析提供预算执行情况分析报表、按项目核算报表等各类财务报表。

1. 教师肖像及学校教师一张表数据支持

为学校提供教师一张表学院级数据支持。建立学院级教师mis页面，每个教师登陆界面有个人基本信息，个人科研教学数据与学院平均值数据对比图谱及学院各类系统。并将该界面与学校mis系统集成。

1. 学生肖像及学校学生一张表数据支持

为学校提供学生一张表学院级学生数据支持。建立学生肖像及学生能力发展雷达图，支持学院学生及学生活动管理，丰富学生信息维度。支持学生行为异常监测、风险评估及预警。

1. 完善校友数据库，为校友服务提供数据支持。搭建校企合作模块，建立企业基本信息，企业来访及企业拜访记录，记录阶段性进展成果,教职工研究方向和科研项目与企业的发展相关性分析,校友企业拜访记录记录在校友数据库中。
2. 与学校、学院数据中心的集成，与学校大数据平台的集成，实现与统一

身份认证平台的对接，对接学校数据中心，集成教师、学生等数据。

1. 支持结构化及非结构化数据的存储，可对结构化数据进行决策分析。
2. 建立日常备份机制、运维体系，完成用户培训。
3. 三年内免费新版本升级及质量保证。
4. 需考虑对各个学院实施部署的通用性。

需提供驻场建设实施服务。

* 1. **对功能需求的理解**
     1. **对数据融合与治理的理解**

通过对北京交通大学智慧校园一期（以下简称“交大智慧一期”）学院数据中心功能分析，加强数据“融合性”、“统一性”、“稳定性”。可以利用BI工具定制报表，并实现下钻、导航、排序、求和、计算列等分析操作，得到有用的数据结果报表。

**1、定制报表**

各级用户可以在业务主题分析页面，定制报表包含的数据项、查询条件、图表类别、分析类别、异常阀值，将固定或通用的报表条件定义在参数化报表中，并作为报表模板存储；在生成报表时，可在报表模板基础上进行特殊的再定制，以减少重复定制的工作量，保证定制的灵活性。

**2、下钻**

“下钻”是在当前数据的基础上，查看更详细的数据。既可下钻某个成员，显示该成员所有子成员的信息；又可下钻某层次，显示该层次的所有成员信息。下钻可清楚了解当前维度参与查询的所有成员，选中成员的所有子成员或选中级别的所有成员。下钻后只显示下钻的成员，父成员及其兄弟成员的信息不再显示。

**3、导航**

相关报表之间可以按照当前报表表格交叉点的维度取值设置带参数的超级链接，传递到连接报表中显示相应的维度切块数据。

**4、排序**

提供按照某列数值升序、降序展示。

**5、求和**

按照维度父子关系显示子维度成员对应度量小计。

**6、计算列**

按照各种逻辑关系应用系统函数、条件语句，组织数据展示。

**7、筛选**

对维度成员进行筛选，得到需要的结果集。

**8、分析视图**

各级用户可以使用功能丰富的视图来进行数据分析。包括：图表、计量表、数据透视表、叙述、静态文本等。可以在部分视图中进行下钻、导航等操作。

* + 1. **对决策分析的理解**

本期项目的辅助决策分析是建立“数据融合与治理”的基础建设之上的。需要结合清洗、筛选、沉淀、融合后的数据进行分析，作出呈现趋势、关联的决策结果数据。本次需要对“数据融合与治理”后的学院多部门的信息数据汇总，部分功能为：教师工作绩效考核计算、教师人员关系的信息对称、财务统计管理与实施进度统计功能。

* + 1. **对教师肖像及学校教师一张表数据支持的理解**

需要与原有学校MIS系统进行数据接口对接，添加教师个人科研教学数据信息及学院各系平局值对比功能，以图表的形式展现。做到教师个人数据与系统数据同步类比功能。

* + 1. **对学生肖像及学校学生一张表数据支持的理解**

需要与原有学生管理系统对接，增添学院学生活动表单，建设录入、修改、删除等管理功能。通过学生成绩等信息数据的同步，扩展学生个人信息标的维度。对于超出指标的数据进行跟踪预警，增加消息提示和并通过手机向学生发送短信。

* + 1. **对完善校友数据库的理解**

增添校友信息数据库表单，开发校企合作信息功能模块包含：企业基本信息、企业来访及拜访记录、阶段性记录成果、教职工研究方向和科研项目与企业的发展相关性分析、校友企业拜访记录等。

* 1. **对数据集成需求的理解**

数据集成的过程是数据进入仓库的入口。数据集成过程所涉及到的数据源一般包括：联机事务处理系统的数据、外部数据源、脱机的数据存储介质等。从数据接口的方式来分，又可以分为数据库专用接口数据、ODBC数据源、格式化平台文件等。

针对提供的业务数据文件，数据导入层需要对这些数据进行必要的分析处理工作，包括对数据质量的检查，之后将数据加载到数据库中。

实际的数据集成过程包括如下图所示的四个部分：

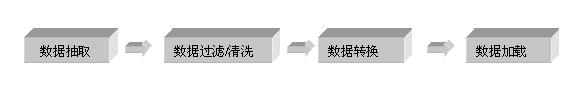


图 1 数据集成过程图

在技术上，数据集成过程主要涉及到：互连、复制、增量、转换、加载、调度和监控等几个方面。通常，数据仓库并不具有数据的实时性，即不要求与联机事务处理系统保持实时的同步，因此数据抽取可以定时批量进行，但多个抽取操作执行的时间、相互的顺序、成败对数据仓库中信息的有效性则至关重要。

具体到本期项目为与学校、学院数据中心的集成，与学校大数据平台的集成，实现与统一身份认证平台的对接，对接学校数据中心，集成教师、学生等数据。

* 1. **对非功能性需求的理解**

1、平台整合性

本项目是升级改造项目，要求升级后平台与原有系统是一体化整合、全信息集成的。

2、平台稳定性

要求平台整体及其各子系统具有稳定性，在各种情况下不会出现死机现象，更不能出现系统崩溃现象。

3、平台可靠性

要求平台数据维护、查询、分析、计算的正确性和准确性。

4、容错和自适应性能

对使用人员操作过程中出现的局部错序或可能导致信息丢失的操作，能推理纠正或给予正确的操作提示。对于关联信息采用自动套接方式按使用频度为用户预置缺省值。

5、易于维护性

要求平台的数据、业务维护方便、快捷。

6、安全性

要求保障平台数据安全、不易被侵入、干扰、窃取信息或破坏。

7、可扩展性

要求平台从规模上、功能上易于扩展和升级，制定可行的解决方案，预留相应的接口。除此之外，平台建设还需要实现与其他系统的集成，能够从其他系统中提取相应专业数据，为本系统服务。

8、适应性

平台在操作方式、运行环境、与其他软件的接口以及开发计划等发生变化时，应具有的适应能力。

1. 易用性

从界面布局、菜单的设计、及用户操作等方面，要遵循界面友好、直观，菜单简洁，菜单格式、快捷键等充分考虑用户习惯，满足用户使用方便的原则、易于修改。

* 1. **对平台性能要求的理解**

（1）页面展示及基本服务功能访问方面：响应速度不大于0.5秒；

（2）综合查询、统计类功能：响应速度不大于4秒；

（3）后台共享交换类和接入类功能：响应速度不大于8秒；

（4）稳定性方面：在利用本系统正常的工作中，不应出现妨碍工作顺利进行的系统错误或意外中止的情况；

（5）资源利用方面：在进行海量数据的查询、统计、分析的过程中，允许CPU和内存的占用率提升及网络带宽占有量的加大，但在操作结束后，应及时释放所占用的资源，以保证工作人员利用计算机顺利进行其它工作。

* 1. **对安全需求的理解**

从多方面建立全面的信息安全管理体系，有效防范内部和外部风险，保证平台信息安全。

* 1. **对实施要求的理解**

由于系统是基于已有交大智慧校园一期平台开发，对原有系统有很强的依赖性，因此在项目经验和服务品质上做如下要求：

（1）项目经验：

中标后尽快了解原系统架构，做好与原系统的一体化衔接，为升级改造提供良好的条件。

同类系统升级改造项目经验优先考虑。

同类系统开发、实施、集成经验优先考虑。

同类系统运维经验优先考虑。

（3）服务品质：

为了保障系统顺利开发、实施、上线我们要求中标单位按照以下标准施工（没有取得该资格的按照以下标准进行开发、实施）：

能够提供优质的本地化服务，派专门技术人员现场开发、维护。

建议项目承担方在项目开发、实施与技术支持的过程中，以ISO9001:2000质量体系作为提供优质服务的标准和保障，取得ISO9001:2000质量体系认证的作为更优保障条件。

建议项目承担方在软件研发管理能力、产品与服务质量等方面全面接轨国际标准和水平，承担方通过CMMI3及以上级别认证的作为更优保障条件。

由于该平台关联对接的外部系统较多，并且对软硬件集成的能力要求较高，因此具备计算机系统集成企业资质的优先考虑，资质越高优先级越高。

* 1. **设计标准和质量保证**

1.北信智科提供的所有产品，其制造商应有完善的质量检测手段和质量保证体系，产品须符合国家标准和行业标准。

2.北信智科提供的所有技术文件中的技术指标除非在技术规格中另作规定外，均应符合相应的国家标准，行业标准和国际标准。

3.北信智科所提供产品的设计在结构上实现开放性，基于国际开放式标准，包括各种广域网、局域网、计算机及数据库协议，符合国家和信息产业部的规范，符合工信部关于网站设计无障碍技术要求（YDT/1761-2012）

4.自验收合格并签署验收文件后开始计算质量保证期。北信智科提供的质量保证期不得少于12个月，且需指派至少一名工程师支持应需进行现场维护。具体保修时间和保修期内的服务北信智科须在投标文件中有详细说明。

* 1. **培训要求的理解**

1．提供现场使用培训；培训内容包含使用人员系统操作和系统管理维护人员安装、维护等。

2．投标人在投标文件中应详细说明具体培训的组织、方案等。

* 1. **技术服务要求**

1.应保证系统的使用正常。质保期内，接到买方通知后须在3小时内做出响应，有必要的需到达现场维护。

2.投标人应在投标文件中声明能够提供的其他技术支持与运维服务标准。

3.应用软件在验收合格后，投标方必须提供合同需求功能范围内的至少一年的免费功能增强性维护（增加、修改、数据维护）（大版本升级除外）及免费技术维护服务（其中包括系统维护、跟踪检测），保证用户购买的应用软件正常运行。

* 1. **工期及验收标准**

1.本项目工期要求：自签订合同起到项目交付运行6个月。

2.验收标准：双方按照合同规定的标准和程序，在工期结束后由甲方指定验收地点和时间进行验收。承诺保证在合同规定时间内本期新建系统平稳运行。系统满足合同范围内的所有功能要求以签署验收文档视为验收合格。

* 1. **方案设计概述**
     1. **方案特点**

本方案主要特点总结如下：

**1、基础设施充分利旧**

机房中的网络、安全以及存储软硬件设备均可利旧。本方案充分利旧，充分考虑利用现有共享交换平台资源和渠道，利用共享交换平台与相关机构连通的前置服务器搭载数据匹配应用，在保护原有投资的基础上，节约成本，实现效益最大化。

**2、总体架构层次清晰**

方案总体架构采用三层应用体系，具有层次结构清晰、采用统一框架结构易于扩展和部署以及统一数据易于利用的设计特色。三层应用体系结构包含表示层、业务逻辑层、数据层。在三层结构中，三个层可以分别部署，表示层用户界面只能与业务逻辑层相联系，无需直接访问后台数据库，使后台数据库与用户界面隔离，提高应用系统的可靠性和扩展性，提高系统数据的安全性。

**3、系统性能最大优化**

本方案在网络带宽、主机配置、应用服务、应用服务器部署、应用代码、数据服务和数据库性能等方面提出了系统性能优化方案，保障系统运行满足各级用户的需求。

**4、保障体系建立完善**

本方案建立了完备的安全保障体系，标准、规范及制度建设方案，项目实施组织计划及进度安排，质量保障体系，项目培训方案及项目保密措施等一系列项目保障体系，保证本次项目按时保质保量完成。

* + 1. **方案优势**

本次项目方案在国家和北京市政策法规的指导下进行建设，符合国际开放技术标准与规范，总体设计遵循总体规划、分布实施原则、安全可靠原则、先进性原则、标准性原则、可扩展性原则和实用性与易管理性原则。

考虑原有交大智慧校园一期系统现状，系统技术线路选择采用基于SOA框架，基于B/S/D三层结构开发应用系统，全面应用XML技术及Web Service技术，基于UML 2.0进行系统建模，实现信息融合共享。

方案总体架构具有层次结构清晰、采用统一框架结构易于扩展和部署以及统一数据易于利用的设计特色。

主体方案融合需求分析、总体设计、性能设计、系统安全设计、应用系统设计、业务支撑平台设计、数据资源库设计、网络及硬件系统设计、系统集成方案、质量保证方案、项目测试、验收、培训方案、技术支持与售后服务方案各方面于一体之中。

* + 1. **公司领导高度重视**

北信智科一直将电子政务作为公司的核心发展方向，公司越来越重视解决方案的成功实施。不仅要帮助客户把握信息化的发展方向，也要做到在满足客户需求的同时，结合公司业务，不断完善技术架构，保证公司在电子政务系统建设方面的可持续发展。本项目由北信智科副总亲自带队，成立项目领导小组，对项目过程进行全程监督，保证资源的充足以及资源调用的及时性和可靠性。

* + 1. **专业化项目建设团队**

公司承诺为项目提供充足的专职、全程建设人员，保证本期项目的按时保质完成，公司会为项目安排合理的项目团队人员、配备科学的项目建设设备，同时保证足够的人力、物力及财力调配权。

* + 1. **需求的理解与变更、控制能力**

为了保证对项目需求的正确理解，公司会根据客户的需求对系统持续改进，直到确定客户满意为止；根据往年的项目经验总结，北信智科已经总结了一套比较成熟的需求管理流程和方法，来进行需求的变更与控制。

* + 1. **规范化项目管理**

北信智科承诺：在项目实施过程中，将严格遵守项目和软件系统的实施规范。并将公司在其他信息化系统建设中积累和总结的目标责任体系融合在本期项目实施管理工作中。同时希望客户方可以全力配合以及遵守制定的相关标准规范，以保证项目的顺利实施。

* + 1. **高标准质量保证**

项目中的产品采购、软件开发与集成等工作，均依据合同，在规定的时间内，满足功能、性能、技术指标要求，并保证产品的质量。

公司的质量方针是：科学、高效、求实、创新。

在质量目标控制中采用PDCA循环，即：Plan（计划）-Do（执行）-Check（检查）-Action（行动）。

控制者（包括项目经理和各工作小组经理）进行控制的过程是从反馈过程得到控制系统的信息后，便着手制定计划，采取措施，输入受控系统，在输入资源转化为产品的过程中，对受控系统进行检查、监督，并与计划或标准进行比较，发现偏差进行直接修正，或通过信息反馈修正计划或标准，开始新一轮控制循环。

计划：确保所有的实施活动都在一个计划指导下进行。

执行：确保所有计划内的活动都能得到有效地执行。

检查：确保所有执行的活动都准确无误。

措施：确保所有执行中的问题都有相应的措施，并无一遗漏地落实，然后进入下一个PDCA循环。

在工作中严格执行ISO9000质量标准和业主单位关于本次应用系统开发与集成制定的相关质量标准。具体来说，质量承诺包括：

1、管理职责

公司承诺并确保管理职责已经确立并被有关人员正确理解，承诺并确保质量体系中的要素都有相应工作小组和人员负责并执行，保证管理职责能够按规定得到贯彻。

2、质量体系

为完成各项质量活动，按照国家标准和国际惯例并结合业主的实际情况，我们承诺并确保建立适宜的文件化质量体系，质量体系覆盖软件产品的生存周期全过程，以确保软件产品的质量。

3、合同评审与执行

合同对于软件项目的确立、明确供需双方的权利和义务、组织开发和售后服务等活动有指导性的意义。公司承诺并确保严格按照合同的规定和要求，在预期的资源内实现对业主方的承诺。

4、设计控制

公司承诺并确保对软件的设计开发进行控制和验证，以确保满足规定的要求。

5、文件和资料控制

公司承诺并确保软件开发的各级组织能够发布和使用适当的文件，并实行有效的管理，使员工能方便、有效地共享信息。

6、采购

公司承诺并确保采购的与软件产品质量有关的软件工具受到控制，保证分承包商提供的服务符合规定的要求。

7、提供对业主提供产品的验证

公司承诺并确保对业主提供产品的评价、验收、存储、使用和维护加以控制，以保证最终集成的应用软件系统的质量。

8、产品标识和可追溯性

公司承诺并确保提供一个标识、控制和追踪每个软件项的正式版本的机制，使产品的变化过程具有可视性，并确保各工作小组的每个工作人员在软件产品生存周期中的任何时刻都能采用正确的信息。

9、过程控制

公司承诺并确保所开发的软件产品在开发、复制、安装和维护等过程中全面受控，并保证最终产品的质量。

10、检验与试验

公司承诺并确保对所开发的软件产品进行检验和试验，确保其满足合同和需求规格说明所规定的要求。

11、检验、测量和试验设备的控制

公司承诺并确保对软件开发所采用的工具、技术、惯例和约定进行控制，确保软件产品的质量能满足规定的要求。

12、检验与试验状态

公司承诺并确保对软件项进行适当的标识，确保通过检验和测试的软件项在经过批准后才能进入下一阶段的工作。

13、不合格品的控制

公司承诺并确保对不合格的产品进行标识和隔离，防止不合格产品的非预期使用和安装。

14、纠正与预防措施

公司承诺并确保贯彻以预防为主的原则，及时采用有效措施，纠正和预防质量问题，分析和确定问题的产生原因，预防问题的再发生，不断提高服务质量。

15、搬运、储存、包装、防护和交付

公司承诺并确保对所开发的软件产品在搬运、储存、包装、防护和交付工程进行控制，承诺并确保软件产品的质量在这些过程中不会受到影响。

16、质量记录的控制

公司承诺并确保对质量记录进行控制和管理，为有追溯性要求的场合和采取纠正措施与预防措施提供证实，为产品质量符合规定要求和体系的有效运行提供证据。

17、内部质量审核

公司承诺并确保检查质量体系运行的符合性和有效性，以及质量体系文件的适宜性和有效性，及时采取预防和纠正措施，避免可能出现的问题和缺陷。

18、培训

公司承诺并确保对各工作小组的组员及与其有关的组员进行相关技术与技能的培训及质量管理培训，以保证所受培训的人员在软件开发和管理过程中具备相应的资格和能力。

公司承诺并确保对本期项目使用用户进行以下培训：

1)产品培训

2)系统软件管理员培训

3)系统的应用管理维护培训

4)系统操作人员培训。

5)项目标准培训

通过各项培训工作和交流活动，除达到所有相关人员的操作使用要求外，最主要的是使业主方的相关技术人员能够全面的了解和掌握系统的所有设计思路、实现方式、技术细节等内容，以最终达到中心技术人员对系统自主维护、自主定制、自主修改、自主升级等要求。

19、服务

公司承诺并确保软件产品在初次交付和安装后，为用户有效的服务，按照合同的规定对软件产品进行有效的维护。

* + 1. **完备的售后服务**

针对本项目，北信智科如果中标将承诺履行以下售后服务的承诺条款：

* 质量保证期限：系统验收合格、双方签署验收书之日起，提供1年免费维护服务。1年免费服务到期后，北信智科应承诺对系统的升级仅收取成本费。
* 北信智科需要提供详细的售后服务方案，包括服务人员、服务内容和措施、应急预案等内容。
* 服务响应时间：提供每周7×24小时电话咨询服务，重大故障2小时内乙方维修人员到现场处理。
* 项目验收完毕后，北信智科承诺通过定期电话、现场巡检等方式跟踪系统使用情况，听取用户意见和建议，及时分析系统存在的问题，并随时给予解决。必要时，承诺派遣技术人员去现场解决存在的问题。
* 质量保证期内，北信智科承诺会及时向用户通报系统软件升级情况，若用户需要对系统软件升级，北信智科将尽量在不影响用户使用现有系统的情况下，科学安排升级步骤，确保提供最新升级版本和相应的系统升级技术服务。
  + 1. **保密承诺**

北信智科公司同意并严格按照《招标文件》中中标合同中对安全保密协议的要求和内容执行。承诺并保证对开发中涉及的相关信息保密，未经甲方许可，绝不将将系统相关信息泄露给第三方。

第三部分性能设计方案

* 1. **系统稳定性设计**

在利用本系统正常的工作中，不应出现妨碍工作顺利进行的系统错误或意外中止的情况；系统采用高可用集群架构部署，对于单个节点的设备故障，应能够瞬时自动将负载切换到其他节点，保证系统正常运行。

同时，除了大量充分的测试以外，在设计上必须有针对可靠性的设计，基本原则是在尽量保证各服务可靠的基础之上，通过一个健壮的体系结构来确保系统能够在硬件和软件出错的情况下依然平稳的运行。本项目在考虑系统稳定性时采用以下设计。保证平台整体及其各系统具有稳定性，在各种情况下不出现死机现象，更不能出现系统崩溃现象。

* 1. **系统可靠性设计**

本期项目在数据维护、查询、分析、计算的正确性和准确性方面，应满足向各类用户提供7×24小时的不间断服务的要求。为实现系统可靠性。

* + 1. **避错设计**

避错设计原则是控制和减少程序的复杂性，体现了以预防为主的思想，在各个阶段都进行避错。

避错准则：

* 模块化与模块独立；
* 抽象和逐步求精；
* 信息隐蔽和局部化；
* 慎重使用容易引入缺陷的结构和技术。
  + 1. **查错设计**

查错设计是指在设计中赋予程序某些特殊的功能，是程序在运行中自动查找存在错误的一种设计方法。

* 被动式错误检测：在程序的若干部位设置检测点，等待错误征兆的出现。

检测原则：相互怀疑原则、立即检测原则。

* 主动式错误检测：对程序状态主动进行检查
  + 1. **容错设计**

容错设计是指在设计中赋予程序某种特殊的功能，使程序在错误已被处罚的情况下，系统仍然具有正常运行能力的一种设计方法。

容错内容包括：时间容错、结构容错、信息容错。

* + 1. **改错设计**

改错设计是指在设计中，赋予程序自我改正错误、减少错误危害程度的能力的一种设计方法。

采用权限最小化原则实现故障隔离。为了限制故障的蔓延，要求对过程和数据加以严格的定义和限制。例如，针对操作系统的故障隔离方法：不允许一个用户的应用程序引用或修改其他用户的应用程序或数据。绝对不允许一个应用程序引用或修改操作系统的编码或操作系统内部的数据等。

* 1. **系统容错和自适应性设计**

对使用人员操作过程中出现的误操作或可能导致信息丢失的操作，能给予正确的操作提示。因此本次开发中针对易出错点进行对应的信息提示，提示内容分为：引导性信息提示、错误操作类型提示、提供帮助性提示等。

* 1. **系统易维护性设计**

为保证平台的数据、业务维护方便、快捷，主要有以下设计：

1、系统日志输出应完整清晰，能够根据系统主要标识，通过日志定位系统问题。

2、用户界面提示信息简单易懂，信息能够为用户提供指导，便于用户下一步操作。

3、如出现致命问题，提示信息应显示详细，便于维护人员排查、解决问题。

4、系统代码应符合使用语言规范。

* + 1. **系统安全性设计**

系统安全性设计力求保障平台数据安全、不易被侵入、干扰、窃取或破坏。具备防病毒、黑客入侵监测和预警、漏洞扫描、网络监测与自动修复、身份认证、敏感信息密文存储和传输等功能；系统还应提供合理有效的数据备份、恢复策略和保护机制。

* + 1. **数据安全**

数据安全应具有如下能力：

* 屏蔽掉数据库系统中默认账户和默认口令。
* 自主访问控制（DAC）：DAC用来决定用户是否有权访问数据库对象。
* 验证：保证只有授权的合法用户才能注册和访问。
* 授权：对不同的用户访问数据库授予不同的权限。
* 审计：监视各用户对数据库施加的动作。
* 数据库管理软件应能够提供与安全相关事件的审计能力：试图改变访问控制许可权；试图创建、拷贝、清除或执行数据库。
* 系统应提供在数据库级和纪录级标识数据库信息的能力。
* 数据备份与灾难恢复的能力。
  + 1. **数据安全解决方案**

数据安全指数据的完整性、机密性、可用性，可分为数据存储安全和数据传输安全。

* + 1. **数据存储安全**

数据存储安全包括防止数据丢失、损坏和非授权访问、篡改，涉及物理、网络、系统、应用和管理五个层面，数据物理层安全通过设备备份解决，网络系统层面通过容灾备份和访问控制解决，应用层面通过加密和访问控制解决，管理层面通过制度约束，防止非授权拷贝来解决。解决数据存储安全最有效的方法是加密存储并结合访问控制和数据备份，为避免过度防护，保证访问的快捷性，系统的数据将不进行加密存储保护，只通过访问控制和数据备份来满足其存储安全需要。

* + 1. **数据传输安全**

数据传输安全是指数据在传输过程中的完整性和机密性保护。目前在系统中需要进行数据传输保护有：交换服务器与相关应用之间的数据传输、数据库服务器与各服务应用之间的数据传输。

* + 1. **安全日志**

通过开启操作系统、数据库自身的审计模块来实现日志审计，同时利用日志审计系统，集中将操作系统、数据库的日志信息传递到日志审计平台，具体审计措施包括：

* 操作系统审计

1. 审计功能开启和关闭；
2. 系统登录行为；
3. 对服务器的维护行为；
4. 对服务器访问的时间、类型、主体标识（访问者账号、IP地址）；
5. 重要的系统管理行为。

* 数据库审计

1. 审计功能的开启和关闭；
2. 对数据库的管理、维护行为；
3. 对数据库访问的时间、类型、主体标识（访问者账号、IP地址）。

* 行为审计

针对访问行为，审计记录至少包含审计事件的时间、类型、主体标识、客体信息、事件结果等事件相关信息。

* 审计记录的查看和分析

针对所审查的审计记录，提供必要的工具（系统自带的功能模块或辅助工具）以查看审计信息，能够提供多种查看方式（排序、分类）；对审计记录进行导出和关联性分析。

* 网络安全

核心数据中心区域增加备份磁盘阵列，采取双机热备策略，主磁盘阵列容量小，备份磁盘阵列容量大。

* 1. **系统可扩展性设计**
     1. **可扩展性接口设计**

本期项目建设项目需要实现内外部应用系统的对接，为保障系统具备良好的对接扩展性，系统采取多元化的接口设计，以满足不同类型的内外部对接需求。使得平台从架构上、功能上易于扩展和升级，应制定可行的解决方案，预留相应的接口。除此之外，平台建设还实现与其他系统的集成，能够从其他系统中提取相应专业数据，为本系统服务。相关的功能模块，如数据分析、比对等功能应具有松耦合性，能够为其它系统或平台所用。

* 平台内部组件接口

本期项目建设项目采用java组件化开发，遵循面向对象的设计开发理念。在自下而上的设计过程中，规划全局资源，确定边界条件，设计出交互过程和用户接口，保证接口的规范性、个移植性、鲁棒性、安全性、兼容性。在设计JAVA接口时严格遵循“缺省适配模式”，提供缺省抽象类的实现，严格规范外部组件使用接口，组件内部使用抽象类。

* 面向外部的接口

在与外部系统之间开发数据接口可根据时间的容忍程度规划为下面两种方式：

定时交换的数据集成接口：双方先约定数据交换格式（数据抽取方式、数据转换方式、数据加载方式），使用ETL工具进行数据的抽取转换加载，完成数据交换工作；或使用中间转换格式文件，由数据源系统导出固定格式的数据文件，数据目的系统导入该数据文件。

实时交互的Web Services接口：目的应用系统和数据源应用系统先约定数据接口API（通常为web services模式），然后由目的应用系统或数据源应用系统实现数据接口API，最后由一方（目的应用系统或数据源应用系统）填写程序调用另一方提供的数据接口API将数据加载或推送到自己的数据库中。在这种方式下，数据加载或推送流程与数据接口API调用方原有的业务或程序流程完全融合在一起。

* 接口可扩展

我们在解决问题的总方向是将复杂问题简单化，在这个总方向的指引下，广泛采用设计模式来达到最大限度的重用，在设计时尽可能的简单明了。在具体实施设计过程中，我们会将简单问题复杂化，落实到每个类的具体实现上要真正能体现系统事物的本质特征，因为事物的本质特征只有一个，代码越接近它，表示设计就是简单明了，越简单明了，系统就越可靠。更多情况是，一个类并不能反应事物本质，需要多个类的组合协调，那么能够正确使用合适的设计模式就成为重中之重。

本期项目建设项目项目将采用面向构件的系统分析与设计方法。使用构件技术的系统搭建模式建设一个综合性松耦合的、复合体系结构型系统。

* 接口可配置

接口部分采用适配开发模式，适配器的主要功能是调用其它子系统提供的接口函数，访问数据库，实现通信基础通用平台接口的功能。系统根据其它子系统提供的接口函数，实现平台接口的功能，并封装处理成数据适配器输出数据，由于不同的子系统都用于自己独立的接口函数，系统必须为每个子系统设计数据适配器。通信基础通用平台在整合数据适配器的过程中，采用SOA（面向服务的体系结构）架构设计，将应用程序的不同功能单元（称为服务）通过这些服务之间定义良好的接口和契约联系起来；同时，平台提供其他子系统的预留接口，为企业的业务发展提供强有力的技术支撑。

* + 1. **可扩展性数据交换**

系统全面采用XML、Web Service技术进行数据、服务描述及数据交换。

XML（eXtensible Markup Language,可扩展标记语言）是Internet上数据表示和数据交换的新标准。它是ISO（International Organization for Standardization，国际标准化组织）的SGML（Standard for General Markup Language，通用标记语言标准）的一个简化子集。XML关注信息本身，是Web上表示结构化信息的一种标准文本格式。与传统的注重页面信息显示的HTML（Hypertext Markup Language, 超文本链接标示语言）相比，关注于内容的XML具有诸多优点：良好的可扩展性，语言简单有效，可自行定义标记；内容与形式的分离，主要刻画数据内容，不考虑显示效果；有严格的语法要求，便于分析统一和与数据库信息转换；便于传输，为纯文本形式，可通过Http协议直接传输，可跨越防火墙；等等。

* + 1. **可扩展性应用架构**

应用J2EE架构，保证系统可移植性和可扩展性，使应用基于XML和SOAP的 Web Service技术，能够实现XML到数据库、数据库到XML和数据库到数据库之间的数据交换和共享，完全实现了跨平台操作、支持各种异构数据库的动态数据交换功能。

* + 1. **可扩展性技术架构**

系统采用SOA总体架构和可配置的构件技术，基于三层结构的系统实现，能够快速的响应业务需求和外部环境变化导致的系统变更。

* + 1. **可扩展性支撑平台**

根据服务平台的应用中间件的要求，从产品的稳定性、可扩展性、标准性、高可用性、安全性为原则来进行选型，充分利用J2EE应用中间件服务器，以HA方式部署支持今后业务增长添置新的应用服务器的需求。

* 基于SOA架构的系统技术框架

SOA（service-oriented architecture，面向服务的体系结构或面向服务架构）是指为了解决在Internet环境下业务集成的需要，通过连接能完成特定任务的独立功能实体实现的一种软件系统架构。SOA是一个构件模型，它将应用程序的不同功能单元（称为服务）通过这些服务之间定义良好的接口和契约联系起来。接口是采用中立的方式进行定义的，它应该独立于实现服务的硬件平台、操作系统和编程语言。这使得构建在各种这样的系统中的服务可以以一种统一和通用的方式进行交互。

传统的Web（HTML/HTTP）技术有效的解决了人与信息系统的交互和沟通问题，极大的促进了B2C模式的发展。WEB服务(XML/SOAP/WSDL）技术则是要有效的解决信息系统之间的交互和沟通问题，促进B2B/EAI/CB2C的发展。SOA则是采用面向服务的商业建模技术和WEB服务技术，实现系统之间的松耦合，实现系统之间的整合与协同。WEB服务和SOA的本质思路在于使得信息系统个体在能够沟通的基础上形成协同工作。

对于面向同步和异步应用的，基于请求/响应模式的分布式计算来说，SOA是一场革命。一个应用程序的业务逻辑或某些单独的功能被模块化并作为服务呈现给消费者或客户端。这些服务的关键是他们的松耦合特性。例如，服务的接口和实现相独立。应用开发人员或者系统集成者可以通过组合一个或多个服务来构建应用，而无须理解服务的底层实现。

在传统的系统体系架构中，系统功能的调整与完善极大依赖开发商，当业务需求发生变化、或不同开发商设计的系统需要集成时，往往需要极大的代价才能完成新系统的集成，甚至有时只能完全推翻原有的设计，这非常不利于保护和利用既有投资。

基于SOA的系统架构将屏蔽由于开发商选择的开发环境和手段不同带来的风险，而是将业务需求拆分到基本服务单元，做到了最大程度地柔性面对需求变化，不仅满足现在的需求，同时也增强了系统在未来的抗风险性。

* 基于Web Service的应用系统整合

系统平台的架构应该满足三个方面的应用整合需要，它们分别是：整合基本用户业务之间的业务流程和数据资源；整合基本业务与GIS等其他之间的数据资源；整合新建的信息系统与原有信息系统之间的软、硬件及数据资源。新一代的互联网技术Web Service是构建这种架构的最佳方案。

Web Service是下一代的WWW，它允许在Web站点上放置可编程的元素，能进行基于Web的分布式计算和处理。Web Service是封装成单个实体并发布到网络上供其他程序使用的功能集合。Web Service是用于创建开放分布式系统的构件。

1、Web Service可以方便地集成应用系统

异构系统间的连接，是今后系统构筑的最重要的课题之一。各个系统间不是孤立的、而是使其相互连接起来，这是最大限度享受由信息技术应用所带来的高效率、低成本实惠的前提。Web Service是解决这个问题的一种有效技术。

用户应用程序开发者都知道，在用户业务里经常要把用不同语言写成的、在不同平台上运行的各种应用程序集成起来，而这种集成将花费很大的精力。应用程序经常需要从运行在IBM主机上的程序中获取数据；或者把数据发送到HP主机或UNIX应用程序中去。即使在同一个平台上，不同软件厂商生产的各种软件也常常需要集成起来。通过Web Service，应用程序可以用标准的方法把功能和数据“暴露”出来，供其它应用程序使用。

2、Web Service是下一代分布式系统的核心

它具有如下特点：

（1）互操作性：任何的 Web Service都可以与其他Web Service进行交互。由于有了SOAP（Simple Object Access Protocol）这个所有主要供应商都支持的新标准协议，因而避免了在CORBA、DCOM 和其他协议之间转换的麻烦。还因为可以使用任何语言来编写Web Service，因此开发者无需更改其开发环境，就可生产和使用Web Service。

（2）普遍性：Web Service使用HTTP和XML进行通信。因此，任何支持这些技术的设备都可以拥有和访问Web Service。

（3）易于使用：Web Service背后的概念易于理解，并且有来自IBM和微软这样的供应商的免费工具箱能够让开发者快速创建和部署Web Service。此外，其中的某些工具箱还可以让已有的COM组件和JavaBean方便地成为Web Service。

（4）行业支持：所有主要的供应商都支持SOAP和周边Web Service技术。例如，微软的.Net平台就基于Web Service，因此用Visual Basic编写的组件很容易作为Web Service部署，并可以被IBM VisualAge 编写的Web Service使用。

3、简单对象访问协议----SOAP

Web service建好以后，你或者其他人就会去调用它。简单对象访问协议(SOAP)提供了标准的RPC方法来调用Web service。实际上，SOAP在这里有点用词不当：它意味着下面的Web service是以对象的方式表示的，但事实并不一定如此：你完全可以把你的Web service写成一系列的C函数，并仍然使用SOAP进行调用。SOAP规范定义了SOAP消息的格式，以及怎样通过HTTP协议来使用SOAP。SOAP也是基于XML和XSD的，XML是SOAP的数据编码方式。

4、Web service描述语言WSDL

Web Services Description Language的缩写，是一个用来描述Web服务和说明如何与Web服务通信的XML语言，为用户提供详细的接口说明书。WSDL元素基于XML语法描述了与服务进行交互的基本元素：

Type（消息类型）：数据类型定义的容器，它使用某种类型系统（如XSD）。

Message（消息）：通信数据的抽象类型化定义，它由一个或者多个part组成。

Operation(操作)：对服务所支持的操作进行抽象描述。

Port Type（端口类型）：特定端口类型的具体协议和数据格式规范。

Binding：特定端口类型的具体协议和数据格式规范

Port ：定义为绑定和网络地址组合的单个端点。

5、服务描述和商业注册机制--UDDI

UDDI（统一描述、发现和集成协议）计划是一个广泛的，开放的行业计划，它使得服务机构能够 (1) 彼此发现，(2) 定义他们怎样在internet上互相作用，并在一个全球的注册体系架构中共享信息。UDDI是这样一种基础的系统构筑模块，它使单位和个人能够快速，方便地使用他们自身的应用软件来发现合适的服务机构，并与其实施电子化的信息查询和业务办理。

UDDI同时也是Web Service集成的一个体系框架。它包含了服务描述与发现的标准规范。UDDI规范利用了W3C和Internet工程任务组织(IETF)的很多标准作为其实现基础，比如扩展标注语言（XML），HTTP和域名服务(DNS)这些协议。另外，在跨平台的设计特性中，UDDI主要采用了已经被提议给W3C的SOAP(Simple Object Access Protocol，简单对象访问协议)规范的早期版本。

UDDI将会给每一个服务描述和服务机构注册分配一个递增的，唯一的标识符，并且把它们存储在注册中心的数据市场和搜索引擎中。单位和个人可以查询此注册中心，以发现其用户部门的Web服务，从而建立一种业务关系。

通过使用 UDDI 注册服务机构、自定义 tModel 和 Web 服务，您可以帮助世界各地的开发人员找到您的 Web 服务。UDDI 注册表允许您发布的不只是 Web 服务端点和业务数据。使用 UDDI 的用户也可以使用该界面查找 Web 服务文档和示例。Microsoft UDDI 注册表是免费使用的。鼓励用户使用此注册表注册您的 Web 服务和机构。

6、Web Service可以提高应用软件的开发效率

在三层结构的系统中，如果中间层组件换成Web Service的话，可以直接使用Microsoft SOAP Toolkit或.NET这样的SOAP客户端，也可以使用自己开发的SOAP客户端，然后把它和应用程序连接起来。不仅缩短了开发周期，还减少了代码复杂度，并能够增强应用程序的可维护性。同时，应用程序也不再需要在每次调用中间层组件时，都跳转到相应的“结果页”。

从经验来看，在一个用户界面和中间层有较多交互的应用程序中，使用Web Service这种结构，可以节省花在用户界面编程上20%的开发时间。另外，这样一个由Web Service组成的中间层，完全可以在应用程序集成或其它场合下重用。最后，通过Web Service把应用程序的逻辑和数据“暴露”出来，还可以让其它平台上的客户重用这些应用程序。

7、Web Service可以实现软件和数据重用

软件重用是一个很大的主题，重用的形式很多，重用的程度有大有小。最基本的形式是源代码模块或者类一级的重用，另一种形式是二进制形式的组件重用。

当前，像表格控件或用户界面控件这样的可重用软件组件，在市场上都占有很大的份额。但这类软件的重用有一个很大的限制，就是重用仅限于代码，数据不能重用。原因在于，发布组件甚至源代码都比较容易，但要发布数据就没那么容易，除非是不会经常变化的静态数据。

Web Service在允许重用代码的同时，可以重用代码背后的数据。使用Web Service，再也不必像以前那样，要先从第三方购买、安装软件组件，再从应用程序中调用这些组件；只需要直接调用远端的Web Service就可以了。举个例子，要在应用程序中确认用户输入的地址，只需把这个地址直接发送给相应的Web Service，这个Web Service 就会帮你查阅街道地址、城市、省区和邮政编码等信息，确认这个地址是否在相应的邮政编码区域。Web Service 的提供商可以按时间或使用次数来对这项服务进行收费。这样的服务要通过组件重用来实现是不可能的，那样的话你必须下载并安装好包含街道地址、城市、省区和邮政编码等信息的数据库，而且这个数据库还是不能实时更新的。

另一种软件重用的情况是，把好几个应用程序的功能集成起来。现在Web上有很多应用程序供应商，都在其应用中实现了这些功能。一旦他们把这些功能都通过Web Service “暴露”出来，就可以非常容易地把所有这些功能都集成到你的门户站点中，为用户提供一个统一的、友好的界面。

将来，许多应用程序都会利用Web Service，把当前基于组件的应用程序结构扩展为组件/Web Service的混合结构，可以在应用程序中使用第三方的Web Service 提供的功能，也可以把自己的应用程序功能通过Web Service 提供给别人。两种情况下，都可以重用代码和代码背后的数据。

8、SOAP的安全扩展满足安全要求

自从SOAP规范发布以来， SOAP规范的加密性，认证和授权等安全机制一直受到人们的广泛关注。这几个方面对于任何的网上业务系统来说都是很重要的 ，但SOAP标准在制定规范时并没有过多考虑SOAP 的安全性要求。因为SOAP一个很重要的设计目标就在于它的简单性，尽可能的利用已有的标准和协议来实现相应的功能，而不是另起炉灶，重新定义一个崭新的协议，如果这样的话，会大大的降低它的实用性和兼容性。

安全性是个复杂的问题，在最低层SOAP 消息可通过 HTTPS 传递， 通用 SSL 传输信息，这就确保被编码消息内容可以避免被窃听，也确保客户端和服务器可互相验证身份。尽管 HTTPS 解决了对窃听者屏蔽消息的问题，但不能满足安全性更高的特殊用户认证的特定 Web 服务的要求。比如下面需要SOAP安全的几个场景，仅仅依靠SSL的安全机制是不满足信息的安全要求的：

（1）端对端的信息传送（End-to-end messaging）

SOAP消息可以与不同的运输层协议（如HTTP，SMTP等）捆绑在一起进行传输，传输的过程中可能经过一系列中间设备或应用程序，假如应用程序对SOAP消息进行恶意破坏，可以在SOAP消息插入一系列相似的头元素，再传给下一个中间设备或程序，从而破坏了信息的完整性。在这种情况之下，中间设备或应用程序是不值得完全信任的，它们随时可以修改传输的信息。因此，SSL/TLS并不能保证端到端传输的安全性。

（2）中间件的独立性（Middleware independence）

在应用层中保证端对端的安全要求，如果在传输中的传输的消息是平文，而不是是经过加密 的密文，极易受到黑客的攻击。但假如在应用程序中进行安全加密的处理，需要用户对加密算法有详细的了解，有许多不同的加密算法适合不同的安全要求，这对于用户来说是额外的负担。因此，标准的，安全的，独立的，透明的运输层是必要的，在SOAP中进行适当的安全扩展，保证了中间件应用程序的独立性，不用考虑过多的加密算法细节。

（3）传输的独立性（Transport independence）

SOAP消息在传输的时候可以与不同的运输层协议进行捆绑，如HTTP，SMTP协议，有可能存在这么一个场景，所有的通信连接是安全的，中间层应用程序也是值得信赖的，但是，安全信息需要经过两个运输层协议，比如前一段是经过HTTP协议传输，在下一个阶段，则需要通过SMTP协议进行传输，两者之间的转换是烦琐的，易出错的。因此，在SOAP中加入扩展信息，保证了运输层的独立性，从而使与运输层无关。

（4）驻留信息的安全性

运输层可以进行安全传输，但不能保证信息驻留时也是安全的。假如消息保存后继续向前传输，驻留信息的安全十分重要。在电子商务中，常常要求用户填写帐号和密码，这些信息通常保留在本地的COOKIE中，对于这些持久保存的信息进行加密，可通过SOAP的安全扩展来实现。

本期项目建设项目项目将基于Web Service技术整合各系统。

* 1. **系统适应性设计**

平台在操作方式、运行环境、与其他软件的接口以及开发计划等发生变化时，应具有的适应能力。

本次设计开发中为保证系统适应性采用常用SOA的体系结构，使用J2EE多层分布式架构开发，并在接口设计时正确处理后续建设工作的合理对接，增强平台的可扩展性和适应性，用信息标准数据接口规范规定了平台基础数据库与外部系统进行信息交换时应遵循的有关信息格式和数据管理规定。

* 1. **系统易用性设计**

从界面布局、菜单设计及用户操作等方面，遵循界面友好、直观；菜单布局、快捷键等设置充分考虑用户习惯，力求简洁友好、易用。因此系统易用性设计包含以下部分。

* 基于MVC的设计模式

系统借助MVC模式实现Web系统的职能分工。

Model层实现系统中的业务逻辑，通常可以用JavaBean或EJB来实现。 View层用于与用户的交互，通常用JSP来实现。 Controller层是Model与View之间沟通的桥梁，它可以分派用户的请求并选择恰当的视图以用于显示，同时它也可以解释用户的输入并将它们映射为模型层可执行的操作。

使用MVC最重要的一点是多个视图能共享一个模型，现在需要用越来越多的方式来访问你的应用程序。对此，其中一个解决之道是使用MVC，无论你的用户想要Flash界面或是 WAP 界面；用一个模型就能处理它们。由于你已经将数据和业务规则从表示层分开，所以你可以最大化的重用你的代码了。

其优点在于：

1. **低耦合性**

视图层和业务层分离，这样就允许更改视图层代码而不用重新编译模型和控制器代码，同样，一个应用的业务流程或者业务规则的改变只需要改动MVC的模型层即可。因为模型与控制器和视图相分离，所以很容易改变应用程序的数据层和业务规则。

1. **高重用性和可适用性**

随着技术的不断进步，现在需要用越来越多的方式来访问应用程序。[MVC模式](http://baike.baidu.com/view/739359.htm" \t "_blank)允许你使用各种不同样式的视图来访问同一个服务器端的代码。它包括任何WEB（HTTP）[浏览器](http://baike.baidu.com/view/7718.htm" \t "_blank)或者无线浏览器（wap），比如，用户可以通过电脑也可通过手机来订购某样产品，虽然订购的方式不一样，但处理订购产品的方式是一样的。由于模型返回的数据没有进行格式化，所以同样的构件能被不同的界面使用。例如，很多数据可能用HTML来表示，但是也有可能用WAP来表示，而这些表示所需要的命令是改变视图层的实现方式，而控制层和模型层无需做任何改变。

1. **较低的生命周期成本**

MVC使开发和维护用户接口的技术含量降低。

1. **快速的部署**

使用MVC模式使开发时间得到相当大的缩减，它使程序员（Java开发人员）集中精力于业务逻辑，界面程序员（HTML和JSP开发人员）集中精力于表现形式上。

1. **可维护性**

分离视图层和业务逻辑层也使得WEB应用更易于维护和修改。

1. **有利于软件工程化管理**

由于不同的层各司其职，每一层不同的应用具有某些相同的特征，有利于通过工程化、工具化管理程序代码。

* 采用标准的WEB2.0页面控件

系统页面展现层采用web2.0交互技术构建，充分利用ajax，json，xml等方式提高用户的使用体验。系统基于Jquery类库的标准UI界面，清新简洁大方。

* 1. **系统可移植性设计**

系统开发要遵循主流的标准和协议，可运行在不同的软硬件平台上，易于以后系统升级和移植。本次项目为保证系统可移植项采用SOA的体系结构，基于SOA的系统架构将业务需求拆分到基本服务单元，做到了最大程度地柔性面对需求变化，也增强了系统的可移植性。使用J2EE多层分布式架构开发，并在接口设计时采用通用标准，增强平台的可移植性。

* 1. **系统可追溯性设计**

系统应具备完善的使用授权、监控和日志管理机制，能够对各类访问和操作进行审计。

* 1. **兼容性设计**

系统应具备较高兼容性，满足IE6、IE7、IE8、IE9、IE10、IE11、Chrome、Firefox、Safari等主流浏览器提供兼容性视图，保证系统功能的正常展示。

终端应用设计采用基于HTML5技术的web开发。HTML 5从根本上改变了开发商开发Web应用的方式，从桌面浏览器到移动应用，这种语言和标准都正在影响并将继续影响着各种操作平台。

其具有跨平台技术优势，能够快速迭代开发，并且可以实时更新原生应用，有问题立即响应。

HTML5前端是开放的正反馈循环生态系统，大量的开源库可以使用，开发应用变得更轻松、更敏捷。 HTML是以page为单元开放代码的，它无需专门开发SDK，只要不混淆，就能与其他应用交互数据。

* 1. **系统整合性设计**

系统整合性设计目标是：

* 消除信息孤岛；
* 打破系统壁垒；
* 统一服务接口；
* 增强协同协作。

在顶层设计的指导下，基于SOA设计理念，以ESB为技术实现，结合社区公共服务综合信息平台业务需求，架构设计充分考虑平台与共享组件、数据交换支撑组件以及其他校园系统之间的协同关系。

根据不同的场景、不同的业务，分别采用同步或异步的交换方式，实现不同系统之间相互松散耦合,为各业务应用系统提供一个透明的、无差异的集成实现。分解业务系统之间的互联关系，为参与服务的各应用系统间的服务及数据交互提供安全、高性能、可扩展的集成平台。

提供丰富的、标准的适配器，并将标准规范体系的数据标准、技术标准、安全标准融入到建设中，从而保障对任意业务系统的快速接入及接入后的标准化转换。架构图如下：

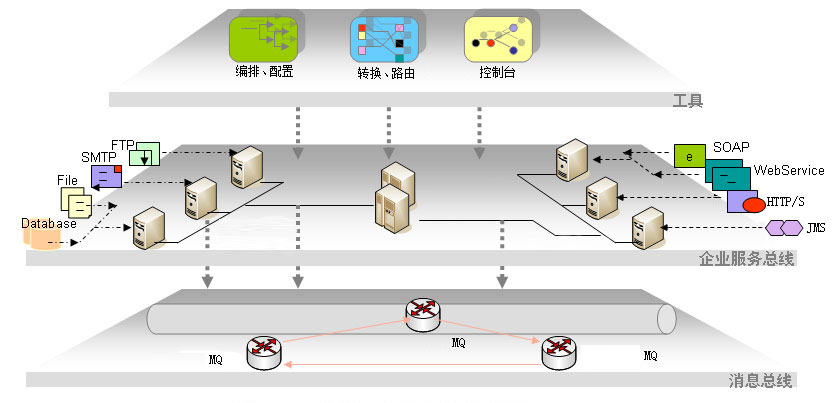


图 0‑1ESB中心服务总线架构

首先，ESB用标准的服务语言跟所有应用系统通讯，这样整个组织的应用系统有了相互交流的共同语言，不必再为各个系统采用不同的通讯协议、不同的数据格式而烦恼，因此它被称为整个企业的服务总线。

其次，ESB协调服务提供者和消费者之间的关系，起到服务中介作用，从而实现服务调用关系松耦合：

1. 各应用系统通过ESB，完成与其他应用系统的集成。
2. 应用系统可以通过ESB提供的适配器，将自己系统的专用接口协议转换成总线使用的标准协议，实现系统与总线的对接；
3. 各系统通过ESB，把系统对外的服务注册到“服务仓库”，这样所有需要这些服务的应用系统，就可以通过ESB，在总线上寻找到并使用服务；
4. 用户可以在ESB上，对所需的服务进行调用、编排、数据转换等配置工作；
5. ESB将根据用户的应用集成配置结果，完成服务调用、转换、路由等工作。

ESB使得不同系统间解除了“直连关系”，是一种轻量级的、可分布式部署的应用集成产品，它很好地解决了紧耦合问题。

* + 1. **功能描述**
* 服务集成

ESB具备服务集成功能，提供用于开发服务、组件集成开发工具，支持完整的从设计、开发、配置到打包部署整个阶段的GUI工具。通过服务生成、服务组装、流程建模、服务生成向导,服务调用示例、应用服务组件等一系列功能,实现对资源及原始功能的封装、集成、调用,从而达到从“数据”到“服务”到“应用”的服务支撑作用。

服务生成：通过可视化界面和服务生成向导，引导用户根据向导的指示，完成数据的填写和收集工作，把相应的资源生成相应的服务,并最终登记、部署、发布。

服务组合：依照服务生成向导，通过可视化的操作界面，将已有的服务或组件进行组合，生成可部署的应用或服务。可以是多个服务的整体组合，也可以是多个服务的部分内容组合。

* 协议转换

服务总线ESB提供良好的跨平台、跨网络、跨协议处理支持，当服务调用端与客户端采用不同数据传输协议（SOAP/HTTP、RMI、JMS）时，ESB通过适配器服务组件的方式，可进行自动协议转换来实现不同传输协议的服务端与客户端的适配。

适配器服务是外系统接入业务集成平台的桥梁，是多种异构系统之间互连互通及互操作的重要组件。ESB提供了大量的基于JCA规范的适配器，如文件系统、各种数据库、消息中间件、WebService等适配器。

通过适配器之间的连接与Java服务引擎以及合成服务模块，可实现各种类型、数据服务标准及通讯协议的服务之间的接入和转换，真正实现了适配器的重用。ESB支持SOAP/HTTP、RMI、JMS、JDBC等多种服务调用协议，支持多种数据库和文件系统，可以很好的满足本项目协议转换的需要。

* 消息路由

ESB提供消息路由功能，通过消息路由方式使得客户端或其他服务对于服务的调用直接面向服务总线，而不必关注服务提供者的位置。

ESB提供事件通知、动态路由选择、事务性处理和可靠传输保障机制，所有对服务的调用都通过服务总线转化为规格化消息的形式，从而在服务组件之间建立了标准的、基于消息的信息可靠传输保障机制，这种方式有效降低了服务端接口的变化或服务提供者的变化对其调用者的影响，使得系统能够更好地适应变化。

通过ESB，可以将请求的消息通过Java服务引擎进行解析判断，根据消息内容，以及配置好的路由规则，自动路由到相应的后台服务，而无需专门指定端点地址，此外，还可集成服务注册库，通过服务注册库，实现服务和消息动态路由的功能。

* 服务扩展

ESB提供丰富的适配器服务组件，通过产品提供的服务合成和服务编排功能，能够结合业务需求，在遵循服务总线相关标准和规范的前提下设计开发新的服务。这些服务可快速集成到服务总线上，并基于服务总线进行服务的配置、管理和快速发布，提供新的功能服务。良好的服务扩展是适应不断变化应用业务的基础。

ESB发布和管理的服务，支持基于SOAP/WSDL的访问方式，以及RMI直接对象访问方式，即使外部ESB及WebServic依旧可以保证良好的兼容性，保证外系统和外部服务的接入和整合。

此外，ESB支持HTTP/HTTPS、FTP、POP3/SMTP、JMS、MQ等多种跨网络通讯技术或协议，并支持基于JMS、Web Service、消息中间件、数据库、文件等方式的接入或数据资源共享交换。并且提供服务调度、服务运行管理支持，提供丰富的适配器服务和API接口，支持二次开发，以保证同特殊类型和格式的系统的兼容性。

* 服务编排

ESB提供集成开发和流程编排支持，支持通过图形化管理界面创建项目和项目元素。

服务的请求可能会涉及到多个服务提供者，可以将多个服务提供者进行组合，使用内建合成服务功能，根据定义的规则和组合逻辑，对所接入的服务进行重组和编排，或结合BPM（业务流程管理平台），实现一个包含多个服务组合的业务流程，从而满足更复杂的业务需求。在本项目的解决方案中，有合成服务功能模块，提供对应的服务组合功能。

通过ESB提供的集成开发配置工具能够根据业务需求，对服务总线上现存的服务进行有条件的顺序组合以创造出新的服务。如：可将A服务、B服务、C服务、D服务进行编排组合建立E服务。

在进行服务的编排、组合和运行时，ESB通过消息队列、JMS服务、事务处理、多线程、缓冲池、集群等机制，有效解决了服务之间大批量数据传输和规格化处理的效率的问题。可以提供良好的并发和并行处理支持，提供集群等高可靠、高可用服务支持。

* 服务集群

服务总线ESB的支持服务级集群策略，以保证高可用行和高处理能力。可以将服务注册到特定的集群中，通过服务总线中的集群服务器可实现服务的冗余设计和负载均衡，在提高服务并发访问能力的同时避免集群服务器本身的故障造成系统单点失效。

服务总线ESB通过HTTP服务器集群的代理转发功能，实现多个服务总线服务器节点上多个同等Web服务实例的并发协同处理服务消费请求。服务总线ESB服务运行容器基于Java EE技术实现，支持Web服务的封装和发布，并提供标准的Web服务运行环境，能够与标准的HTTP服务器集群进行有效集成使用，实现服务级的集群和负载均衡效果。

在实现负载均衡的同时，通过开发可以建立具有机构层次的集群管理机制，提供服务的匹配策略设置，即根据服务调用者的调用权限、工作范围、服务优先级等特征与服务端的调用权限、服务范围限定、服务优先级策略等特征进行最佳匹配，在根据各服务器的繁忙程序找到最佳的服务节点。

* 服务浏览

查看可以访问的服务列表，获取服务WSDL信息，也可以调用查询可用服务列表接口获取可以访问的服务列表。

* + 1. **统一监控管理**

对用户进行增加、修改、删除以及查询。只有成为平台用户，才有可能访问平台提供的各应用系统。

每个用户都应该具有一种以上的角色，角色不同意味着具有的操作权限不同，管理职责不同。

角色管理支持增加角色、修改删除角色、查询角色，建立角色与用户之间的对应关系。

每个角色都需要赋予一定的操作权限，权限管理通过增加权限、修改权限、删除权限实现对角色权限的调整。

* + 1. **逻辑节点管理**

逻辑节点是组件、服务及业务流程的运行环境，它包含了实现J2EE1、4规范的应用服务器。平台基于标准的J2EE1、4规范，因此在其上开发的组件、服务及相应的业务流程，最终要打包成标准的J2EE相关组件和应用，部署到相应的J2EE应用服务器上运行，逻辑节点管理包括：

* 查看逻辑节点详细信息，包括该逻辑节点的IP，端口等信息。
* 修改逻辑节点的别名。
* 配置整个逻辑节点的日志相关属性，逻辑节点日志的相关属性可以包括设置日志的类型、级别，日志文件的大小、备份等。
* 获取逻辑节点日志，在显示日志内容页面，可以通过查找关键字，快速浏览日志信息。

1. 项目监控管理

主要是针对整个项目的一个管理监控功能，包括该项目下合成应用，及合成应用相应的部署名称和运行状态等信息的查看及相应的启、停等功能。

* **项目**：查看此项目下所有的部署文件自身信息及运行状态等信息，同时可以对权限管理范围内的部署文件进行启、停控制。
* **项目警告信息处理：**可以通过过滤条件查看项目的警告信息，同时也可以手工清理相关警告信息。
* **部署管理：**查看该部署下的服务运行情况，可以对权限管理范围内的部署进行启动、停止操作。
* **合成应用：**显示该合成应用的服务连接关系图。

1. 服务监控管理

（一）服务基本信息

在服务信息中，可以查看到服务如下信息：

* 服务名：监控项目下服务的名称，与在集成开发工具中该项目下创建的适配器和服务名称一致。
* 合成应用名称：监控项目下，该服务所属的合成应用名称，与在集成开发工具中该项目下创建的合成应用名称一致。
* 容器名：监控项目下，该服务在合成应用中容器的名称，与在集成开发工具中该项目下创建的该服务容器名称一致。
* 逻辑节点IP：该服务所在的逻辑节点的IP地址。
* 逻辑节点端口：该服务所在的逻辑节点的端口号。
* 服务名：监控项目下服务的名称，与在集成开发工具中该项目下创建的适配器和服务名称一致。
* 类型：该服务的类型。
* 状态：该服务的当前活动状态，状态分为：

suspend：暂停状态；

active：正常运行状态；

unkown：非正常运行状态。

* 接口信息：该服务所用接口的名称。
* 警告数：该服务产生的警告信息数量。

（二）服务参数设置

参数设置，是根据该服务所涉及的适配器属性，显示适配器的属性设置。与集成开发工具中该项目下，在合成应用中，为每个适配器设置属性一致。当前版本，用户只能通过“参数设置”，了解适配器的属性设置内容，不可以进行修改。

（三）服务日志管理

服务日志设置

可以针对服务的日志类型、日志级别，组件名深度、保存模式等日志相关信息进行设置。

服务的日志获取

在日志查看是，可以设置需要获取日志的起始时间和终止时间，需要获取日志的条数，每页日志显示行数。

在显示日志内容页面，可以通过查找关键字，快速浏览日志信息。

（四）服务交易状况管理

服务交易状况统计可以实时监控一个业务流程在一定时间内处理业务流程的情况分析，成功处理业务多少笔，失败多少笔等信息。

（五）服务负载信息管理

在“服务信息”列表中，选中一个服务，通过设置查看该服务的负载信息统计，也可以删除一些负载信息。

* **服务负载信息统计**

1. 统计总计调用次数：服务的调用次数统计。
2. 根据时间段统计调用次数：设置某段时间内的调用次数，可以设定起始和终止时间。
3. 根据年份统计每月调用次数：统计某一年内，每个月对该服务的调用次数，可以设定年份。
4. 根据月份统计每天调用次数：统计某一年的某个月份内，每一天对该服务的调用次数，可以设定年份和月份。
5. 根据天统计每小时调用次数：统计某一年的某个月份的某一天内，对该服务的调用次数，可以设定年份，月份和日期。
6. 统一监控管理

监控管理是对平台自身的交换管理、用户认证授权和基础信息资源共享系统的工作状态、交换节点、交换流程运行状态进行集中监控管理。

1. 交换信息查看

对平台、外系统接入适配器、交换流程的历史运行状态以及Web服务的历史使用日志等进行按关键或日期查询。

1. 系统运行信息查看

系统运行信息是指平台各服务的运行信息（如数据服务器、交换服务器等）、平台运行日志信息（如，数据插入数据库失败、文件传输中断等）以及用户操作日志信息等，支持按照关键字或者日期查看系统运行信息。

1. 交换情况统计分析

对日志信息按照业务系统进行分类统计分析，得到各系统使用平台的综合情况，如数据交换的次数和数据量、用户认证次数和点击量等，实现对系统交换业务访问情况的展现和统计。

1. 信息告警通知

对节点、流程运行过程中的异常情况如，节点停止、传输中断等，以邮件的方式及时通知给相关负责人，帮助相关人员迅速了解平台的运行情况，诊断、发现并及时解决平台的各类故障问题。

1. 日志管理

日志管理模块主要实现对系统自动记录的用户操作日志进行查看、查询、删除等操作，该模块主要提供给审计用户使用。

* + 1. **集成接口管理**

定义编码对外部系统开放的WebService服务的地址、方法等。提供两类服务：编码生成服务于编码查询服务。

1、编码生成服务：

* 1. 按数据规范接收外部系统传入的某一数据对象的数据。
  2. 按元数据模型提取该元数据的编码规则。
  3. 解析编码规则使用到的元数据元素数值。
  4. 按码段逐一生成编码规则，拼装产生完整的数据编码，返回调用服务的接口。
  5. 编码发生异常，返回异常信息。

2、编码查询服务：

* 1. 第三方系统调用服务，按数据规范传入数据对象。
  2. 按元数据模型解析传入数据。
  3. 将传入的数据项作为查询条件执行数据查询，如果查询结果只有唯一的一条生效数据，则返回该数据编码，如果没有对应生效数据或有多条生效数据，返回异常，提示传入的数据不足以查询唯一的编码。

3、连接测试：可对配置的接口进行连通性测试。

* + 1. **安全管理**

1. 网络接入层

* 客户端非法接入控制

保证接入ESB系统的合法性，提供应用系统和ESB系统之间的双向身份认证，采用基于证书的认证模式，系统使用的数字证书由第三方CA或者采用自运行维护的CA提供。CA证书采用离线下发的方式，以PKCS#12文件的格式安装到ESB系统和应用接入系统。身份认证完成后，双方得到一个64个字节的随机数，通讯双方使用的对称密钥都是基于这一组随机数产生，对称密钥的选取规则双方使用相同的策略。对称密钥和对方的公钥信息存放在系统主机的共享内存，方便应用系统加密使用

1. 网络传输层

* 支持SSL（包含国密算法）

数据通信采用128位的SSL技术（包括SSLv3和TLSv1）提供尖端的高安全保证，确保连接的合法性、私有数据的保密性。

数据传输通过使用身份证书，来建立具有强安全性的SSL连接。只有通过双方身份验证的连接才允许建立，并进行数据传输，在此连接上传输的数据都将被加密，保证传输机密性的安全需求。

支持的加密算法和摘要算法列表如下（包含国密算法）：

表 0‑1支持的加密算法和摘要算法

| **加密算法** | **摘要算法** | **备注** |
| --- | --- | --- |
| NULL | MD5 | SSLv3 / TLSv1 |
| NULL | SHA | SSLv3 / TLSv1 |
| RC4 | MD5 | SSLv3 / TLSv1 |
| RC4 | SHA | SSLv3 / TLSv1 |
| IDEA-CBC | SHA | SSLv3 / TLSv1 |
| DES-CBC | SHA | SSLv3 / TLSv1 |
| DES-CBC3 | SHA | SSLv3 / TLSv1 |
| AES128 | SHA | TLSv1 |
| AES256 | SHA | TLSv1 |
| SM4-ECB | SM3 | 国密算法；非对称算法使用SM2 |
| SM4-CBC | SM3 | 国密算法；非对称算法使用SM2 |

1. 应用层

* 加密接口

ESB提供了加密和解密接口，使用的算法是RC5，应用程序在发送消息之前调用加密接口，在接收消息之后调用解密接口，可以有效保证传输过程中私有数据的保密性。另外，应用程序在发送消息之前、接收消息之后，可以调用第三方提供的加密库，包括与第三方加密设备（如加密机）配合使用的加密库。

1. 管理层

配置文件加密、管理权限、用户审计

* 1. 配置文件加密

对配置文件的加密功能，加密后的配置文件以密文形式存在。加密后的配置文件只能通过管理控制台这个唯一入口进行查看和编辑，保证了对服务器管理的安全性。

* 1. 管理权限

ESB管理控制台提供了用户权限管理功能，对系统的使用者进行了角色划分，并对不同使用者对不同管理功能拥有的访问权限进行定义，从而保证系统的不同使用者只能访问被授权的系统和进行规定的访问操作。

* 1. 用户审计

用户操作审计功能，详细记录了每个用户对节点的所有操作，包括登录信息，对配置信息的查看、修改、删除等操作，为后续问题查找提供了技术支持。

* 1. **数据备份和恢复**
  + 数据备份

依托机房的集中数据存储和备份存储实现平台的本地数据存储、备份与恢复，系统数据和业务数据可联机备份、联机恢复，恢复的数据必须保持其完整性和一致性；系统应具备自动或手动恢复措施，以便在发生错误时能够快速恢复正常运行；系统支持异地备份的拓展。

数据存储与备份将采取以下策略：

1、将数据库数据存储路径定义至专用磁盘阵列存储介质；

2、采用全备份和差分备份相结合的方式进行数据备份；

3、每周进行一次全备份，每天进行一次业务数据差分备份；

4、在具备条件时，对备份数据进行异地保存管理。

* + 双机热备

实现无单点故障的全冗余双机热备方式。这种方式的特点在于：

1、存储之间的数据复制不经过网络，而是由存储之间进行复制。

2、两个存储之间的复制是完全实时的，不存在任何时间延时。

3、主备存储之间的切换时间小于500ms，以确保系统存储时不产生延时。

4、硬盘盘符及分区不因为主备存储之间的切换而改变。

5、服务器的切换，不影响存储之间的初始化，增量同步及数据复制。

6、某一存储设备的计划性停机，不影响整个服务器双机热备系统的工作。

7、存储设备之间使用重复数据删除技术，完成增量同步工作。

8、真正的7X24小时或切换的全冗余方案。

* + 灾备优化

建议充分提供数据备份与安全、系统恢复与软件应用、灾难恢复以及异地灾备四大保障来充分保障系统的业务连续性。

在数据备份与安全方面，基于磁盘“块”级别的备份，实现了实时的文件、数据库、应用程序、操作系统、逻辑卷和裸设备等的持续数据备份，可以立即对备份的数据进行查验，并且持续数据备份又实现了三个“‘0’的突破”：零停机备份、零窗口备份和零冲击备份；

在系统恢复与软件应用方面，实现了病毒、应用程序错误、人为误操作、系统瘫痪等软故障下的任意时间点的一分钟数据恢复、5分钟系统恢复以及无需停止业务的在线系统恢复；

在灾难恢复上则实现前端主机磁盘等硬件损坏故障时的操作系统远程启动，实现快速灾难恢复；

为了应对地震、火灾等自然灾害，将来将对接北京市政府密云灾备中心实现提异地容灾。

* 1. **系统处理和响应能力**

（1） 最大支持1000用户同时在线使用，高峰时支持50个用户并发访问。

（2） 对于处理不超过20个数据项的普通维护操作，要求平均响应时间在1秒以内，峰值响应时间控制在3秒内；对于处理不超过50个数据项的普通维护操作，要求平均响应时间在2秒以内，峰值响应时间控制在5秒内；对于处理超过50个数据项的维护操作，如果数据项为X，则要求平均响应时间小于（X/50）×2 秒，峰值响应时间控制在；（X/50）×4秒内，最高不超过8秒。

（3） 对于单表信息的精确查询，要求平均响应时间在1秒内；对于跨表的精确查询，平均响应时间要小于（2×相关联的表的个数）秒，峰值响应时间控制在（4×相关联的表的个数）秒内，并且最高不能超过20秒。

（4） 系统平均无故障率不低于99.5%，若发生故障，恢复时间的要求是：

* 一般故障，恢复系统正常运行所需时间不超过30分钟；
* 严重故障，不超过4小时；
* 特别严重的故障，一般不超过24 小时。

第四部分安全保障方案

* 1. **安全设计原则**

在对本系统规划设计过程中，充分考虑用户业务应用的需求，使用目前成熟、稳定且先进的技术来规划和设计整个平台的安全系统结构。本次安全的整体思想是要构建一个集安全技术体系、安全管理体系和安全运维服务体系三个体系为一体的信息安全保障体系；形成集防护、检测、响应、恢复于一体的安全保障体系，从而实现物理安全、网络安全、系统安全、数据安全、应用安全和管理安全，以满足信息系统全方位的安全保护需求。同时，由于安全的动态性，还需要建立安全风险评估机制，在安全风险评估的基础上，调整和完善安全策略，改进安全措施，以适应新的安全需求，满足等级保护以及自身安全运维的要求，保证长期、稳定、可靠运行。

本设计方案将遵循以下整体建设原则：

1、统一规划、分步实施

根据实际工作需要，从业务应用系统、信息服务系统、网络体系等方面的安全需求考虑，制定平台项目安全保障体系的整体目标和规划，并根据需求的轻重缓急情况，制定出分阶段的计划，突出重点、分步实施，确保在分步实施的过程中，避免盲目建设和低效建设。

2、需求、风险、代价平衡的原则

对信息系统建设进行切合实际的分析与设计，对系统可能面临的威胁或可能承担的风险提出定性、定量的分析意见，并制定相应的规范和措施，确定系统的安全策略。

3、综合性、整体性原则

采用适当的技术手段分析网络的安全，并制定具体措施。安全措施主要包括：行政法律手段、各种管理制度以及专业技术措施，如访问控制、加密技术、认证技术、攻击检测技术、容错、防病毒、综合审计等。

4、一致性原则

针对系统平台安全问题与整个网络的工作周期（或生命周期）提出分析意见，并保证制定的安全体系结构必须与网络的安全需求相一致。

5、易操作性原则

所采用的安全措施应保证易于操作，并保证不影响系统的争产运行。

6、适应性及灵活性原则

所采用的安全措施必须保证实现随着系统平台性能及安全需求的变化而变化，易适应、易修改。

7、多重保护原则

所建立的安全系统要确保是一个多重保护系统，各层保护相互补充，当一层保护被攻破时，其它层保护仍可保护信息的安全。

安全系统的建设目标是根据系统结构和应用模式，针对可能存在的安全漏洞和安全需求，在不同层次上提出安全级别要求，并提出相应的解决方案，制定相应的安全策略，编制安全规划，采用合理、先进的技术实施安全工程，加强安全管理，保证系统的安全性。

1、统筹规划，分步实施：明确整体安全策略，规划本系统平台信息安全保障体系并制定实施计划，结合本系统平台应用实际情况和发展需要，分阶段、分步骤，不断推进和完善信息安全保障体系；

2、统一协调，各负其责：抓好安全工作，构筑本系统平台信息安全保障体系；

3、综合防范，整体安全：在本系统平台安全体系建设中，坚持管理与技术并重，从人员、管理、安全技术手段等多方面着手，建立综合防范机制，实现整体安全；

4、分级保护、务求实效：从实际出发，综合评估信息的价值和系统所面临的风险大小等因素，科学划分网络与信息系统安全等级。依据安全等级进行安全建设和管理，综合平衡安全成本和风险，优化信息安全资源的配置，提高信息安全保障的有效性。

* 1. **安全保障体系框架**

本项目将参照国家信息化建设三级等级保护标准建设本项目工程及应用服务系统，主要从物理安全、网络安全、主机安全、应用安全以及数据库安全五个方面着手，采用当今先进而成熟的安防技术与产品，设计部署信息安全防护体系，并树立规范信息安全管理体系，完善管理机构与管理制度，全方面实现信息安全的整体要求，最终达到安全防护的目标。



图 0‑2安全保障体系框架示意图

* 1. **物理安全**

对于本系统而言，物理安全保障业务系统正常运转的基础。因此，对于承载业务系统的物理运行环境应从以下几方面予以考虑，防止意外的物理风险的发生：

* 意外事故（如自然灾害、火灾）造成的系统破坏；
* 电源故障造成的设备损坏或数据丢失；
* 设备失窃造成数据丢失或信息泄漏；

电磁辐射可能造成数据信息被窃取或偷阅。

* 1. **应用安全**
     1. **用户身份认证**

根据《信息安全技术信息系统等级保护安全设计技术要求》，对于信息系统需建立网络接入认证机制，可采用由密码技术支持的可信网络连接机制，通过对连接到网络的设备进行可信检验，确保接入网络的设备真实可信，防止设备的非法接入。

互联网云已通过各种防护措施实现安全域的划分与边界控制，但是在网络的接入认证与控制措施上前存在一定的不足，无法对接入到网络中设备进行识别及控制和记录。为规避上述风险，建立基于网络的接入认证控制措施，即部署网络接入认证网关系统来实现对通过政务外网及内网接入网络核心的实体的身份识别、安全策略检查和权限进行控制及行为记录，增强对网络资源的使用保护。

为防止对平台信息资源的非授权访问，需建立有效的身份认证措施。将结合采用北京市CA认证管理系统登录身份鉴别机制和基于数字证书的用户身份鉴别机制，实现系统强身份认证登录。强身份认证登录将采取以下安全策略：

1、在系统层面，制定系统登录错误锁定、会话超时退出等安全策略；

2、在应用层面，采用 “数字证书＋USBKEY”认证方式来实现用户对本期项目登录访问的身份鉴别。

* + 1. **访问权限控制**

本期项目将面向北京市各校园学院、事业单位提供服务，为进一步加强对本期项目内数据信息资源访问的可控性，防止信息资源被非授权访问，建议在身份有效性识别的基础上，对不同角色人员采取授权访问措施。

系统将从系统级访问控制和资源级访问控制两方面进行设计：

1、系统级访问控制

通过账户权限最小化配置、边界并发会话阈值限制、单一资源最大化（或最小化）使用限度等方式实现，将本期项目纳入市共享交换平台进行统一认证授权管理。

2、资源级访问控制

在本期项目过程中实现细粒度的资源授权和字段级授权，以实现资源级访问控制。

* + 1. **应用软件安全**

应用软件安全保证是指在应用软件的设计、开发、测试、分发和升级等整个生命周期中通过安全的运作方式保证软件的安全性。具体包括：

1、软件的安全设计评估

任何一套软件都可能存在安全隐患，这也是被大家广为接受的概念。而针对本期项目而言，应拥有一套良好的策略和手段针对业务软件本身的安全设计进行有效的评估。

2、版本控制

在软件开发过程中，制订版本控制制度，并采用有效的版本控制或配置管理软件。对版本进行必要的访问控制。

3、测试

应用系统开发应具有完善的测试文档，对应用软件进行多样的测试，例如白箱测试、黑箱测试和压力测试等。

4、软件分发和操作

新的软件发布的时候，应按照安全策略中的有关流程进行分发，不应对现有安全策略产生影响或者违背。

* + 1. **Web应用程序安全设计**

针对Web应用程序的攻击不容易在网络边界处进行防范，并且攻击形式多样，难于完全杜绝。防止针对Web应用程序的攻击最有效的方法是在软件设计时进行安全编程考虑，从代码本身杜绝被攻击的可能性，从而做到未雨绸缪、主动防御。

针对Web程序的攻击主要分为跨站脚本攻击和SQL注入攻击两大类，以下分别从这两种攻击的攻击手段考虑，提出解决方案。Web应用程序软件开发时应根据以下建议进行安全开发。

* XSS跨站脚本攻击

1、漏洞成因

原因很简单，就是因为WEB程序没有对用户提交的变量中的HTML代码进行过滤或转换。

2、漏洞形式

这里所说的形式，实际上是指WEB输入的形式，主要分为两种：

显示输入；

隐式输入；

其中显示输入明确要求用户输入数据，而隐式输入则本来并不要求用户输入数据，但是用户却可以通过输入数据来进行干涉。

显示输入又可以分为两种：

输入完成立刻输出结果；

输入完成先存储在文本文件或数据库中，然后再输出结果；

而隐式输入除了一些正常的情况外，还可以利用服务器或WEB程序处理错误信息的方式来实施。

3、漏洞危害

比较典型的危害包括但不限于：

获取其它用户Cookie中的敏感数据；

屏蔽页面特定信息；

伪造页面信息；

拒绝服务攻击；

突破本期项目网络不同安全设置；

与其它漏洞结合，修改系统设置，查看系统文件，执行系统命令等；

其它。

一般来说，上面的危害还经常伴随着页面变形的情况。而所谓跨站脚本执行漏洞，也就是通过别人的网站达到攻击的效果，这种攻击能在一定程度上隐藏身份。

4、解决方法

要避免受到跨站脚本执行漏洞的攻击，需要程序员和用户两方面共同努力，程序员应过滤或转换用户提交数据中的所有HTML代码，并限制用户提交数据的长度；而用户方则不要轻易访问别人提供的链接，并禁止浏览器运行JavaScript和ActiveX代码。

* SQL INJECTION数据库注射攻击

1、SQL Injection定义

所谓SQL Injection ，就是通过向有SQL查询的WEB程序提交一个精心构造的请求，从而突破了最初的SQL查询限制，实现了未授权的访问或存取。

2、S2QL Injection原理

随着WEB应用的复杂化，多数WEB应用都使用数据库作为后台，WEB程序接受用户参数作为查询条件，即用户可以在某种程度上控制查询的结果，如果WEB程序对用户输入过滤的比较少，那么入侵者就可能提交一些特殊的参数，而这些参数可以使该查询语句按照自己的意图来运行，这往往是一些未授权的操作，这样只要组合后的查询语句在语法上没有错误，那么就会被执行。

3、SQL Injection危害

SQL Injection的危害主要包括：

暴露敏感信息

提升WEB应用程序权限

操作任意文件

执行任意命令

4、SQL Injection 技巧

利用SQL Injection的攻击技巧主要有如下几种：

逻辑组合法：通过组合多种逻辑查询语句，获得所需要的查询结果。

错误信息法：通过精心构造某些查询语句，使数据库运行出错，错误信息中包含了敏感信息。

有限穷举法：通过精心构造查询语句，可以快速穷举出数据库中的任意信息。

移花接木法：利用数据库已有资源，结合其特性立刻获得所需信息。

5、预防手段

要做到预防SQL Injection, 数据库管理员（MS SQL Server）应做到：

应用系统使用独立的数据库帐号，并且分配最小的库，表以及字段权限；

禁止或删除不必要的存储过程；

必须使用的存储过程要分配合理的权限；

屏蔽数据库错误信息。

WEB程序员则应做到：

对用户输入内容进行过滤；

对用户输入长度进行限制；

注意查询语句书写技巧。

* 网页防篡改

网页防篡改系统是黑客入侵防范体系的一个重要组成部分和最后一道防线。目前国内网页防篡改产品生产厂商相对较少，产品研发采用的技术主要可以分为二类：扫描技术、核心内嵌技术。下面从二种技术的实现原理上分析一下两种技术的优缺点：

扫描技术采用的方式是周期性的访问监控的网页，来判断网页的真实性。这种技术的优点是实现的技术门槛比较低，厂商能够快速的开发出网页防篡改产品。缺点是：一、不能保证被篡改网页的实时恢复，被篡改的文件存在一定的存活期；二、周期性的访问监控网页势必会加重服务器的负载，影响应用系统的正常运行。扫描技术是网页防篡改产品在初期采用的一种技术。

核心内嵌技术采用将其篡改检测模块嵌入Web服务器软件内部运行，与Web服务器无缝结合。这种技术的优点是每次Web服务器对外发送网页时，网页防篡改系统都进行检测，从而能够实时地确保每个网页的真实性。缺点是：一、被篡改文件的恢复依赖于用户的访问请求，被篡改文件存在一定的存活期，并且增加了服务器的负载；二、需要针对于不同的Web服务器提供不同版本的产品。核心内嵌技术是比扫描技术更科学、更先进的一种技术。

* 1. **数据安全**

从数据传输过程和数据存储过程两方面保障本期项目的数据的完整性和保密性。具体防护策略如下：

1、数据传输过程：通过部署和配置SSL安全通讯协议服务，确保关键数据的传输保密性和完整性；

2、数据存储过程：采用密码机制所支持的完整性校验机制，检验在系统安全计算环境中存储数据的完整性；采用密码机制所支持的保密性保护机制，对安全计算环境中的存储数据进行保密性保护。

* + 1. **传输安全与抗抵赖**

开启系统、设备的日志审核策略功能，建立网络安全审计系统，同时将系统记录的日志信息统一提交给安全管理中心的集中日志审计系统，实现关联性统计分析。

部署SSL安全传输协议信道，数显数据传输交换过程中的完整新和保密性；统一认证服务提供安全认证凭证的安全传输和校验。

* + 1. **数据存储与备份恢复**

依托新建机房的集中数据存储和备份存储实现本期项目的本地数据存储、备份与恢复，同时在中环等有条件的机房选择部署异地灾备存储环境，利用政务外网网络，实现异地数据备份。

数据存储与备份将采取以下策略：

1、将数据库数据存储路径定义至专用磁盘阵列存储介质；

2、采用全备份和差分备份相结合的方式进行数据备份；

3、每周进行一次全备份，每天进行一次业务数据差分备份；

4、在具备条件时，对备份数据进行异地保存管理。

* 数据备份

依托机房的集中数据存储和备份存储实现平台的本地数据存储、备份与恢复，系统数据和业务数据可联机备份、联机恢复，恢复的数据必须保持其完整性和一致性；系统应具备自动或手动恢复措施，以便在发生错误时能够快速恢复正常运行；系统支持异地备份的拓展。

数据存储与备份将采取以下策略：

1、将数据库数据存储路径定义至专用磁盘阵列存储介质；

2、采用全备份和差分备份相结合的方式进行数据备份；

3、每周进行一次全备份，每天进行一次业务数据差分备份；

4、在具备条件时，对备份数据进行异地保存管理。

数据层安全措施主要有数据库安全审计、数据盗窃安全防护系统等。

1、数据库安全审计

数据库对于本项目是一个复杂而又关键的系统，数据库在管理和技术上存在风险，若这些风险变为事实，则数据中心数据将遭受经济损失和法律风险。当数据库产生安全问题时很难追查和定位，因为无法查找问题发生的痕迹和证据。因此，数据库的安全审计成为数据库安全的重要组成部分，它可以通过对数据库操作的痕迹进行详细记录和审计，使数据的所有者对数据库访问活动一目了然，有据可查，及时掌握数据库的使用情况，并可对安全隐患进行调整和优化。

数据库安全审计要求支持分布式部署结构，能够同时管理多个审计引擎，并对审计引擎的审计结果信息进行集中查询、分析；集用户身份认证、基于角色的授权访问及网络内容审计三位一体；提供会话监控功能对正在进行的连接会话内容进行实时监视并可以进行手工阻断；支持对敏感行为的阻断功能，包括基于策略和手工两种方式。能够根据制定的策略对违规行为进行实时自动阻断，支持将正在发生的违规行为通过操作系统显示界面以手工方式阻断当前会话连接。发现安全隐患，并对网络活动的相关信息进行存储、分析和协议还原，并对网络中的可疑网络行为实施记录、告警和阻断。

2、数据存储安全

在信息系统中存储的信息主要包括纯粹的数据信息和各种功能文件信息两大类。以数据库信息的保护最为典型，对应用终端数据安全保护也很重要。

数据库安全：提供多级数据库的安全机制，并能支持数据加密存储和传输及冗余控制。对数据库系统所管理的数据和资源提供安全保护，一般包括：物理完整性，即数据能够免于物理方面破坏的问题，如掉电等；逻辑完整性，保持数据库的结构，如对一个字段的修改不影响其它字段；元素完整性，包括在每个元素中的数据是准确的；用户鉴别，确保每个用户被正确识别，避免非法用户入侵；可获得性，可访问数据库和所有授权访问的数据。

应用终端的数据存储安全：主要解决计算机信息的安全保护问题，一般的安全功能有：基于口令或（和）密码算法的身份验证，防止非法使用机器；强制存取控制，防止非法访问文件；多级权限管理，防止越权操作；存储设备安全管理，防止非法拷贝和硬盘启动；数据和程序代码加密存储，防止信息被窃；预防病毒，防止病毒侵袭；严格审计跟踪，便于追查责任事故。

* 双机热备

实现无单点故障的全冗余双机热备方式。这种方式的特点在于：

1、存储之间的数据复制不经过网络，而是由存储之间进行复制。

2、两个存储之间的复制是完全实时的，不存在任何时间延时。

3、主备存储之间的切换时间小于500ms，以确保系统存储时不产生延时。

4、硬盘盘符及分区不因为主备存储之间的切换而改变。

5、服务器的切换，不影响存储之间的初始化，增量同步及数据复制。

6、某一存储设备的计划性停机，不影响整个服务器双机热备系统的工作。

7、存储设备之间使用重复数据删除技术，完成增量同步工作。

8、真正的7X24小时或切换的全冗余方案。

* 灾备优化

建议充分提供数据备份与安全、系统恢复与软件应用、灾难恢复以及异地灾备四大保障来充分保障系统的业务连续性。

在数据备份与安全方面，基于磁盘“块”级别的备份，实现了实时的文件、数据库、应用程序、操作系统、逻辑卷和裸设备等的持续数据备份，可以立即对备份的数据进行查验，并且持续数据备份又实现了三个“‘0’的突破”：零停机备份、零窗口备份和零冲击备份；

在系统恢复与软件应用方面，实现了病毒、应用程序错误、人为误操作、系统瘫痪等软故障下的任意时间点的一分钟数据恢复、5分钟系统恢复以及无需停止业务的在线系统恢复；

在灾难恢复上则实现前端主机磁盘等硬件损坏故障时的操作系统远程启动，实现快速灾难恢复；

为了应对地震、火灾等自然灾害，将来将对接北京市政府密云灾备中心实现提异地容灾。

* + 1. **数据保护**

为了对那些必须保护的记录提供足够的保护，而对那些不重要的记录不提供多余的保护，应该对所有记录给予评价，并作出分类。

1类（关键性的）记录：对设备的功能来说是最重要的，不可替代的，火灾或灾害后立即需要但又不能再制的那些记录。如关键程序、主记录、设备分配图表、加密、并法、密钥等秘级很高的记录。

2类（重要的）记录：这类记录是很重要的，可以在不影响系统最主要功能的情况下进行复制，但比较困难和昂贵。如某些程序、存贮及输入输出数据等属于该类。

3类（很有用的）记录：其丢失可能引起极大的不便，但可以很快复制。已留有拷贝的程序、扫描的影像数据等属此类。

4类（不重要的）记录：在调动时很少需要的记录

* + 1. **数据脱敏脱密**
* 数据脱敏

数据脱敏是指对某些敏感信息（如：账号、身份证号、电话、地址、密码）通过脱敏规则进行数据的变形，实现敏感隐私数据的可靠保护。这样，就可以在开发、测试和其它非生产环境以及外包环境中安全地使用脱敏后的真实数据集

数据脱敏是为了确保在非生产环境下使用生产数据更加安全，但是其又与纯粹的数据加密不同，数据加密可能是将数据库中有意义的字符通过加密后转变成了无意义字符，而脱敏是将数据通过一定的算法变成另一种样式，而这种样式是可读的，并且与元数据是同一类的。

一个好的数据脱敏过程必须具备以下特点：可用性、数据关联关系、业务规则关系、数据分布、易用性和可定制。从而在针对不同系统进行数据脱敏时，制定良好的脱敏方法，是整个数据脱敏关键所在，本项目中数据脱敏目标如下：

1.防止生产库中敏感数据泄露

通过对生产库中的身份信息、地址信息、银行卡号信息、电话号码信息等敏感数据进行混淆、扰乱后再提供给第三方使用，防止生产库中的敏感数据泄露；

通过对生产中或扰乱后的数据进行局部数据抽取，实现非生产环境下数据集合使用的最小化。

2.提升测试、开发和培训数据质量

在数据漂白和数据子集的过程中，通过内置的策略和算法，保证脱敏后数据的有效性（保持原有数据类型和业务格式要求）、完整性（保证长度不变化、数据内涵不丢失）、关系性（保持表间数据关联关系、表内数据关联关系），以提升在测试、开发和培训环节的真实有效性。

3.提高数据维护和数据共享安全性

通过对生产数据库访问者的用户名、IP、工具类型、时间等多个访问者身份维度，控制对生产数据访问结果的差异化，返回结果可以为真实数据返回、数据掩码，同时可以进行数据阻断、行数限定。

脱敏功能设计如下：

1.静态数据脱敏

支持全流程的静态数据脱敏：

1）数据漂白

通过高效的数据脱敏算法，能够针对不同数据类型进行数据脱敏及掩码扰乱，支持的脱敏算法包括屏蔽、变形、替换、随机、格式保留加密（FPE）和强加密算法（如AES）。

2）数据装载

可将脱敏后的数据按用户需求，装载至不同环境中。按照场景不同，可提供文件至文件，文件至数据库，数据库至数据库，数据库至文件的不同装载方式。

2.动态数据脱敏

对需要共享的生产数据或时效性很高的数据测试、培训场景，提供基于网络代理模式的动态脱敏技术；动态脱敏可实现对业务系统数据库中敏感数据进行透明、实时脱敏。

1）动态脱敏可以依据数据库用户名、IP、客户端工具类型、访问时间，甚至业务用户身份等多重身份特征进行访问控制；

2）动态脱敏对生产数据库中返回的数据可以进行放行、屏蔽、加密、隐藏、返回行控制等多种脱敏策略。

3.数据子集

提供多种的数据子集抽取方式：

1）基于事实表发起的百分比抽取方式；

2）基于基础信息表中的身份信息或商品类别发起的向下延展的数据抽取方式；

3）针对多表的灵活条件设定的抽取方式。

4.敏感数据管理

实现全面的敏感数据管理功能，帮助组织实现有序、一致的可视化脱敏数据管理。

1）敏感数据发现

能够按照用户指定的一部分敏感数据或预定义的敏感数据特征，在执行任务过程中对数据进行自动识别，发现敏感数据。与此同时，既可发现数据之间的主外键关系，也可以智能分析出用户赋予数据间的依赖关系、同类数据间的联动关系，为数据子集管理、脱敏数据关联性保留等功能提供了保障。

2）敏感数据字典管理

以敏感数据为中心，对数据库字段进行分类管理；对同库多表、多库多表的同一类敏感数据实施统一的脱敏算法和策略，保证同一单位或行业内跨系统、跨库之间的数据脱敏后一致性；并支持敏感数据字典导入、导出等功能。

3）脱敏方案管理

针对每一脱敏项目，在基础性脱敏算法的基础上，可以配置专门的脱敏策略，或者实现脱敏算法的扩展；

可实现脱敏策略的导入导出，以帮助脱敏策略的复用，保障在同一组织架构内脱敏策略的一致性。

4）脱敏任务管理

可对任务数据进行停止、启动、重启、暂停、继续，并且支持任务并发，充分利用系统资源，提高脱敏效率。脱敏过程中可跳过异常数据，持续执行任务。

* 数据脱密

本项目所存储的信息涉及到涉密数据，需要对开发环境和测试环境中的数据建立统一的管理规范，对于必须使用生产数据的系统开发、测试、维护项目，生产数据必须经过脱密，才能被加载到开发、测试或维护环境。此脱密过程称做“数据漂白”。

数据漂白后的要求：

1.去掉隐私信息。

2.保持数据脱密后的数据构成、合法性标准（如果目标系统需要对该数据字段进行校验的话。

3.保持数据库的数据一致性和参考完整性。

4.应用系统间关联使用的有效性。

5.保持聚合字段、行/列计算字段有效性。

6.脱密算法不可破解。

针对于本项目，数据加/脱密处理的主要流程设计如下：

1）对数据库命令进行语法分析，如果语法正确，转下一步；如不正确，则转6），直接将SQL命令交数据库服务器处理。

2）是否为数据库加/脱密引擎的内部控制命令？如果是，则处理内部控制命令，然后转7）；如果不是则转下一步。

3）检查数据库加/脱密引擎是否处于关闭状态或数据库命令是否只需要编译？如果是则转6），否则转下一步。

4）检索加密字典，根据加密定义对数据库命令进行加脱密语义分析。

5）数据库命令是否需要加密处理？如果是，则将数据库命令进行加密变换，替换原数据库命令，然后转下一步；否则直接转下一步。

6）将数据库命令转送数据库服务器处理。

7）数据库命令执行完毕，清除数据库命令缓冲区。

* 1. **系统安全和监控体系**
     1. **安全监控总体框架**

为了有效防范和化解风险，保证信用数据的安全，实现信息系统的平稳运行以及业务应用的持续稳定进行，必须按照统一规划、统一建设、统一管理和统一服务的原则，建立可靠的安全保障体系，增强信息安全风险防范能力。

系统的安全监控体系设计将建立纵深防御体系：包括“人”、技术”和“操作”三个方面入手，对系统的信息安全进行全方位的安全管理，并且作为实际的安全措施来实行，构建系统的安全监控体系。其中“人”即指管理安全措施；技术”指保护网络和基础设施、保护网络边界、保护计算环境及支撑性基础设施；“操作”指运行安全措施。

* + 1. **事前防护安全设计**

1、安全管理

对于信息安全，除了配置较为完善的技术设备外，还必须制定好相应的规章制度：

（1）成立信息安全小组。主要任务是贯彻执行和完善信息安全的规章制度，对日常工作进行认真检查、监督、指导和教育。

（2）制定安全规范。根据各应用系统的建设情况和对信息资源的需求，将在安全领域制定一系列的标准规范，以进一步加强信息安全。该规范主要包括安全管理措施、安全技术标准、运行安全措施。

2、安全域划分

通过安全域划分，形成清晰、简洁、稳定的 IT 组网架构，实现系统之间严格访问控制的安全互连，更好的解决复杂系统的安全问题；安全域划分后，安全域间的信息流控制遵循如下原则：

* 跨安全域的数据流须经过定义好的边界控制组件控制。
* 在边界控制组件中，缺市情况下，除了明确被允许的流量，所有的流量都将被阻止。
* 边界控制组件的故障将不会导致跨越安全域的非授权访问。
* 所有来自互联网的流量需要被严格控制和监控，每个连接必须被授权和审计。

3、链路负载均衡

在互联网出口部署两台链路负载均衡设备对互联网接入线路进行链路负载均衡。对于外部用户访问“基础支撑平台”应用的入站访问，链路负载均衡设备可以通过智能 DNS 解析功能，动态选择最佳链路，将外部用户导向到内部站点中的资源。同时链路负载均衡设备会随时监测每条链路的状况，当发现任何一条 ISP 链路故障时，都不会再把该 ISP 的 IP 地址解析给用户，从而保证用户可以 7\*24 小时的访问到内部应用并且提高用户的访问速度。

4、Web 防火墙

在“支撑平台”DMZ 区域部署两台 Web 防火墙，主要是对 Web特有入侵方式的加强防护，如 DDOS 防护、SQL 注入、XML 注入、XSS 等。WEB 应用防火墙部署于门户网站服务器群的前端，通过抗扫描、防注入、防跨站脚本、防后门攻击等安全策略加强门户网站的安全防护能力，最大限度的杜绝网站被黑客入侵的可能。

5、网页防篡改系统

为保证Web 前端服务器的安全性，系统需部署网页防篡改系统，防止对外提供服务的信用北京网被非法、恶意篡改。网页防篡改系统分为三个相对独立的子系统，分别是监控代理Monitor Agent（简称 MA）、同步代理 Synchronization Agent（简称SA）和管理中心 Management Center（简称 MC）。监控代理 MA 部署于网站服务器，负责实时监控保护网站文件，发现篡改企图或篡改操作实时发送恢复请求，并及时提交告警信息。同步代理 SA 部署于同步服务器，负责实时监控备份文件变更，以及监控代理提交的恢复请求，并根据请求执行向网站服务器的文件同步。管理中心 MC 逻辑上部署于管理服务器，作为用户与系统之间的接口，负责将操作指令传达给监控代理和同步代理；同时，负责实时接收来自代理端的各种告警信息并及时通知用户。

6、防火墙方案设计

本项目需要采用双层异构防火墙防护技术，在互联网外部部署安全网关，在内部网络部署异构防火墙，从网络安全方面提供整体防护能力。安全网关集成防火墙、IPS、防病毒等功能，加强整个内外网网络边界的区域安全性及服务器区域安全性；通过防火墙有效隔离和阻断来自互联网的非授权访问，阻断和处理来自互联网的攻击，防范从互联网流入流到内部网络的病毒、间谍软件、木马等攻击行为。

7、防病毒方案设计

根据国家信息系统安全等级保护中“主机系统安全--恶意代码防范、入侵防范”的要求，方案设计中采用集成基于主机 IPS 防范的网络防病毒技术，对服务器、工作站进行全面的安全保护。在“基础支撑平台”包括的所有主机上安装防病毒客户端，接受防病毒服务器的统一管理。

8、服务器虚拟化安全设计

采用服务器虚拟化提供的虚拟化安全整体解决方案，可针对数据中心内的网络威胁提供基本的防护,提供采用基于基本流量信息的策略的应用程序防火墙, 按主机进行部署。对虚拟机之间的流量进行基本的防火墙保护，这样便能够根据 5 元组（源 IP 地址、目标 IP地址、源端口、目标端口、协议）对连接进行筛选和分组，根据网络、应用程序端口、协议类型（TCP、UDP）、应用程序类型强制实施安全保护。

9、CA 证书体系安全设计

充分利用市级法人一证通平台，提供在线证书状态认证服务（基于在线证书状态协议，即 OCSP 协议），签名、验签服务和加密、解密服务。设计以 CA 证书体系为核心的信用数据的管理系统，这个系统的核心是信用数据管理中心，提供信用数据管理系统的认证、授权、审计等功能。由于证书的发放、使用有严格的登记、管理流程，此系统有较强的审计、追溯能力，以及防抵赖能力。

* + 1. **事中监控安全**

1、系统运行监控

通过部署业界先进的 IT 监控软件，采用集中统一的监控平台，通过全局、直观的监控展现，保障业务系统平台稳定、高效的运行，实现业务应用、基础架构与网络架构集中监控，实时掌握核心关键业务应用、主机服务器、中间件、数据库、网络设备等关键指标运行状况，及告警信息及时预警机制。通过 IT 监控软件的部署，可将被动式服务转换为主动式服务，提升运维服务质量、服务能力与服务水平，提高系统的可用性，减少系统问题的发生，实现系统安全稳定健康的运行。

2、日志集中管理

本项目通过日志集中管理系统，对该平台中包括的所有服务器、网络设备进行集中日志审计管理，日志集中管理系统包括管理（审计）中心和可选的日志采集器两个部分。日志集中管理系统支持同时采集多个不同网段的日志信息，适用于逻辑隔离的多个网络。

3、运维审计管理

本项目需要一台运维审计系统（堡垒机），对所有运维人员的 IT 操作行为进行监控、审计，实现 IT 运维操作的集中认证、授权、审计。通过在运维审计系统上配置所有服务器的开放资源以及所有需要访问服务器的运维管理人员的帐号，并利用运维审计系统的访问控制和授权功能，实现对所有访问服务器进行运维操作的行为进行控制与监控，从而达到运维审计的要求。

* + 1. **事后恢复安全**

1、备份软件及磁带库安全设计

在本方案中选用业界领先的备份管理软件作为本系统备份的核心软件，使用物理磁带库，作为备份介质。数据备份方式有：LAN 备份、LAN-Free 备份和Server-Free 备份三种。LAN 备份针对所有存储类型都可以使用， LAN-Free 备份和 Server-Free 备份只能针对 SAN 架构的存储。本系统采取 LAN 备份，LAN-FREE 备份和 SERVER-FREE 相结合的手段，对重点主机中数据读写要求速度快的做 LAN-FREE 备份，特大数据做SERVER-FREE 备份，其他普通主机做 LAN 备份。

以下详细描述针对不同应用系统所做的不同备份策略：

（1）基于 LAN 的数据备份方式--针对 IP 网络的普通服务器：传统数据备份方式需要在每台主机上安装磁带机备份本机系统，采用 LAN 备份策略，在数据量不是很大时候，可采用集中备份。一台中央备份服务器将会安装在 LAN 中，然后将应用服务器和工作站配置为备份服务器的客户端。中央备份服务器接受运行在客户机上的备份代理程序的请求，将数据通过 LAN 传递到它所管理的、与其连接的本地磁带机资源上。这一方式提供了一种集中的、易于管理的备份方案，并通过在网络中共享磁带机资源提高了效率。本系统中的归集服务器、清洗服务器、比对服务器和应用服务器等机器，运行在 IP 网络，服务器中保存的内容主要包括网页、源代码、文档、配置文件等，备份数据量不是太大，可采用 LAN 备份方式，以较低的投入达到较为理想的效果。

（2）LAN-Free 数据备份方式：由于数据通过 LAN 传播，当需要备份的数据量较大，备份时间窗口紧张时，网络容易发生堵塞。在 SAN 环境下，可采用存储网络的 LAN-Free 备份，需要备份的服务器通过 SAN 连接到磁带机上，在 LAN-Free 备份客户端软件的触发下，读取需要备份的数据，通过 SAN 备份到共享的磁带机。这种独立网络不仅可以使 LAN 流量得以转移，而且它的运转所需的CPU 资源低于 LAN 方式，这是因为光纤通道连接不需要经过服务器的 TCP/IP 栈，而且某些层的错误检查可以由光纤通道内部的硬件完成。此时，需要一台主机来管理共享的存储设备以及用于查找和恢复数据的备份数据库。本系统中运行在互联网的信用北京网数据库，由于备份数据量较大，备份时间较长。因此，可以考虑采用 LAN -Free 的备份方式。

（3）Server-Free 数据备份方式：Server-Free 对需要占用备份主机的 CPU 资源，如果备份过程能够在 SAN 内部完成，而大量数据流无需流过服务器，则可以极大降低备份操作对生产系统的影响。SAN Server-Free 备份就是这样的技术。本系统中政务外网的本期项目核心数据库，由于备份数据量非常大，备份时间长，备份时不能对主机有较大影响。因此，可以考虑采用 Server-Free 的备份方式。

以上三种数据备份方式中，LAN 备份数据量最小，对服务器资源占用最多，成本最低；LAN-free 备份数据量大一些，对服务器资源占用小一些，成本高一些；Server-free 备份方案能够在短时间备份大量数据，对服务器资源占用最少，但成本最高。

2、容灾方案设计

系统运行支撑环境为用户提供应用访问服务时，当主数据中心遭遇自然灾害而不可用时，将带来不可预计的严重后果。通过建立容灾数据中心，可以大大提高整体平台的业务连续性。容灾数据中心的主要建设内容如下：

——磁带数据容灾：通过备份系统将业务系统数据备份至磁带，实现数据离线异地保存。

——数据级容灾：利用存储的同步复制技术，将主数据中心的数据实时同步至容灾中心，实现数据级容灾。

——通过容灾软件组件，将主数据中心的所有虚拟机复制到容灾中心，实现应用级容灾。系统容灾数据中心将交由市政务信息资源中心统筹建设。

* 1. **项目主要风险及防范措施**
  2. **项目风险管理机制**

项目风险是客观存在的，主要包括技术风险、管理风险和系统风险。技术风险包括项目的技术结构、项目的规模以及项目实施方的技术能力和经验。管理风险主要来自于项目人员组织的有效性，项目时间、资源计划的确定性和可控性，以及项目质量监控的力度和立场。系统在这里指的是由信息化相关要素组成的动态联系的有机体系。主要指的是用户自身的组织规范化、组织的观念转变、组织责任与控制体系的适应性等。所以，建立风险管理机制是降低和化解风险的有效手段。

* + 1. **风险监督机构**

借助于专业人员，建立内部监督机构，对该应用系统的实施进行风险分析和跟踪，并提出防范措施。

* + 1. **长期合作关系**

要实行对项目的有效监督，不仅要对项目的实施进行监控，而且对甲方的长期发展战略有全面、深刻的了解。这样，监督人员才能站在战略的高度，分析应用系统的发展方向，把握系统建设的目标。

* + 1. **全过程风险管理**

对本项目风险的管理，不能只停留在实施完成后对项目的评估上，更重要的是防范和化解风险。监督分为定期阶段评估和终审评估，它们贯穿于项目的全过程，从规划、准备、实施到系统运行。定期评估是监督人员根据项目的实施进度，制定计划，在现场做实际分析，通过分析来发现潜在的问题和风险，及时提出修改建议。各实施小组采取相应的措施加以改进。终审评估是在实施完成后，对运行系统所做的全面评价。定期评估是预防性监督，全过程监督的内容不仅是对各项风险进行专项跟踪，更包括对工作质量的跟踪；审核项目实施计划，确认计划的完整；跟踪实施进展，判断项目实施是否得到有效的控制；审核实施的阶段性成果，如系统的分析报告、设计报告、测试报告等，确认实施是否达到阶段目标。

* 1. **项目主要风险及防范措施**

针对本项目来说，项目风险主要包括进度、技术、管理、质量和人员等五个主要部分。

* + 1. **进度风险**

1、风险识别

项目实施周期为半年，从2017年1月初至2017年6月初。项目整个实施工作大体划分为如下的6个主要阶段。

* 1. 前期准备和需求调研
  2. 系统需求分析
  3. 系统概要设计和详细设计
  4. 系统开发和测试
  5. 系统试运行
  6. 系统正式运行和验收

商务合同签订后的1个月内，完成项目需求调研、系统初步设计、系统整体设计和系统详细设计工作，并进行专家论证和确认。2个月内，完成项目的开发、测试、安装、部署工作。软件集成测试通过后，1个月内进入系统试运行。系统试运行合格后，1个月内完成项目的系统初步验收以及用户上线。培训工作完成后，进行系统终验。终验合格后，工程建设完工，进入质量保证期。即在此期间完成从需求分析到软件集成测试，并包括整个项目培训、试运行前的所有工作。项目对时间进度的要求较高。

2、风险分析

可能造成进度风险的因素包括：

1）项目承担单位工作任务分解时，考虑到的主要工作进度主线，各分解工作最早开始时间完成时间、最迟开始时间完成时间以及契合、交叉工作任务划分不尽合理，或考虑不够周全。

2）项目承担单位对分解的工作任务配备的人员和人员组成结构不能保证该工作任务的按时完成。

3）项目承担单位主要里程碑中，尤其是完成项目的需求分析、设计并通过审至完成开发、集成和测试，有两点需要注意，一是开发工作须以需求分析、系统设计通过评审为前置条件；二是开发、集成和测试工作需要在2个月内完成。时间较紧，如果项目承担单位不在需求分析和系统设计阶段，不在可能范围内预先开展开发的准备工作，则很有可能造成进度延误。

4）业主单位为共同开展项目建设配备的相关业务协调人员和业务协同部门，如果不全力指导、配合项目建设，则需求分析和系统设计进度难以保障。

5）业务较大变更和项目涉及各方有效沟通存在问题等，也会对项目进度带来重大影响。

3、风险规避

针对以上主要风险因素，可以采取的风险规避措施主要包括：

1）合理进行工作任务分解。目承担单位在明确项目范围后，应在各实施组充分参与条件下，共同制定WBS。

2）根据工作任务统筹考虑参与任务的人员和人员结构组成。

3）在需求分析和系统设计阶段，采用原型迭代法，开发原型系统，以更好了解业务单位需求，缩短评审通过后的编码开发时间。

4）对于确认后需求分析和系统设计，在不影响业务主要使用前提下，在编码开发阶段尽量不作变更。必要的变更可在项目应用软件系统编码、集成、联调、测试并通过第三方测评后进行。

5）在项目涉及各方间建立有效的沟通机制。

* + 1. **技术风险**

1、风险识别

项目涉及个人隐私信息，能够对工作主管部门、其他政府部门、服务评级机构和社会公众等各类用户提供查询、统计分析等项内容。另外，在系统建设中需要统一考虑的还有系统整体框架、数据库建设、应用支撑平台以及标准规范等。项目涉及的技术内容较多，存在一定风险。

2、风险分析

本建设项目的技术风险主要包括：

1）数据存取、调用等数据层操作方法和接口等在多个系统中不一致导致的风险。

2）应用支撑平台中各基础组件的结构化和一致性较差可能导致的风险。

3）应用系统专业组件封装方法和提供接口不一致或灵活性较差导致的复用度不够造成的风险。

4）系统间互调用、互操作设计不合理导致的联通性较差的风险。

5）系统对于大量多并发访问以及性能等方面要求不能满足，而造成的使用风险。

6）业务系统中的多维分析、计算、统计的实现可能存在技术风险。

7）在系统的开发、使用和运维中，没有明确统一的标准规范和要求，而造成的风险等。

3、风险规避

针对以上主要技术风险，可以采取的风险规避措施主要包括：

1）采用原型迭代法进行前期系统开发，识别关键技术和主要解决方法。

2）利用项目承担单位已有的应用软件构件库和类似项目开发技术，最大程度解决可能出现的技术风险。

3）在项目编码开发前，完成标准规范特别是技术标准规范的制定，指导规范应用软件开发、集成工作。

* + 1. **管理风险**

管理风险主要来自于项目人员组织的有效性，项目时间、资源计划的确定性和可控性，以及项目质量监控的力度和立场。项目共分五类角色：用户方的业务人员、用户方的决策人员、集成商的技术人员、集成商的项目管理人员以及项目的监管者如何有效组织，并协同发挥积极因素是一个项目组织的课题，存在很多的不确定性。而项目进度的计划和项目预算是否具有确定性直接影响项目的可控程度。最后，项目监控的力度和立场在实际过程中会面临来自各方面的干扰和阻力。

本项目的顺利实施离不开相关部门和单位的密切配合，本项目建设将涉若干政府部门，重点在于参与案件转办的单位与其他职能单位的沟通协调，存在的风险较小。

* + 1. **质量风险**

1、风险识别

本建设项目要求在规定的进度范围内，采用合理先进的技术实现项目要求，更重要的是，必须满足质量的要求，达到立项和系统使用要求。

2、风险分析

项目质量风险主要包括：

1）项目相关提交物的质量风险。其中需求分析规格说明书、系统概要设计、系统详细设计、系统集成设计等交付物需要得到评审通过，以指导项目后续工作。这方面的质量风险是由业务单位和项目承担单位共同承担。其他阶段和过程，重点是编码开发质量需要由项目承担单位严格控制、监督检查的。

2）项目管理过程的风险。本项目涉及范围广、内容多，规范性强。必须采用严格的项目管理规定和制度。在项目整体开发进度要求下，项目管理的实施需要对实施过程各阶段各要素进行严格规划、定义、检查监督，也就是说，项目管理会带来时间、费用、人力等的成本，可能会对项目的进度造成影响。

3）项目质量实际上包括项目管理的各主要要素，有时间、费用、人力、沟通、采购等，这些因素同样会影响到项目质量。

3、风险规避

针对以上主要质量风险，可以采取的风险规避措施主要包括：

进行项目全过程的监督。对本项的质量管理，不能只停留在实施完成后对项目的评估上，更重要的是防范和化解质量风险。监督分为定期阶段评估和终审评估，它们贯穿于项目的全过程，从规划、准备、实施到系统运行。定期评估是质量管理人员根据项目的实施进度，制定计划，在现场做实际分析，通过分析来发现潜在的问题和风险，及时提出修改建议。各实施小组采取相应的措施加以改进。终审评估是在实施完成后，对运行系统所做的全面评价。定期评估是预防性监督，全过程监督的内容不仅是对各项风险进行专项跟踪，更包括对工作质量的跟踪；审核项目实施计划，确认计划的完整；跟踪实施进展，判断项目实施是否得到有效的控制；审核实施的阶段性成果，如系统的分析报告、设计报告、测试报告等，确认实施是否达到阶段目标。

* + 1. **人员风险**

1、风险识别

本建设项目涉及内容较多、时间进度要求较紧。如果没有充足的人员保障，没有合理的人员结构分析，要在进度规定下完成项目是不可能的。

2、风险分析

项目人力资源风险包括：

1）投入项目的总的实施人数、实施人员的素质能力和实施团队结构的安排如果不合理，不能满足人力资源计划和项目计划，则项目存在巨大风险。

2）足备合格的实施人员不能同分解的工作任务有机结合，即制定的工作任务对应的人员、人员结构组成和目标不能合理匹配，则项目存在风险。

3）人员分配和人员费用计划不能有效结合，不能在进度规定范围内，在一定费用匡算下，完成项目工作任务要求的目标，则项目存在风险。

4）项目承担单位制定人员计划时，可能现有人力资源不能全部满足项目实施需要，而在人力组织时没有考虑到解决方法，则项目存在风险。

3、风险规避

针对以上主要人力资源风险，可以采取的风险规避措施主要包括：

1）本项目投入使用人员全部定岗、定职，精力全部投入本项目建设。

2）在项目启动阶段，结合项目范围要求，制定项目工作计划，完成工作任务分解，必须完成人员计划制定，并根据实际工作开展情况适当变更。

3）根据人员计划，明确组织结构和岗位分配，进行人员配置管理。

4）根据配置管理要求，选派单位内部合格人员参与项目建设，进行必要的现有工作交接和针对项目的前期沟通、培训。

5）制定合理的外聘人员计划和合作计划，选择适当外聘人员。

6）项目人员适当的复用和合理沟通是确保项目成功的要素之一，如需求分析人员适当参与系统设计工作、培训人员应由项目主要开发集成人员组成等。

7）结合项目范围管理、时间管理、质量管理等要求，进行团队绩效考核和个人绩效考核。

第五部分应用系统方案设计

* 1. **设计依据**
     1. **在国家和北京市政策法规的指导下进行建设**

国家政策法规是本工程的基础保障环境，具有约束、威慑以及不得已情况时的非常手段，保证项目顺利施行与最终目标的达成。本次建设应遵循国家、北京市、信息化建设领域的各种标准、规范和制度。

* + 1. **符合国际开放技术标准与规范**

系统设计和建设要符合国际开发技术标准，系统设计的各种接口在遵循规范性原则的基础上，保证其可以继承不同设备的厂商、系统或平台供应商、软件供应商的产品，保证系统的设备管理、系统扩容和业务维护不依赖于单一设备厂商、系统或软件供应商的产品。

同时，为了使系统具有较强的生命力和开放性，系统建设应遵循当前业界认可的、先进的技术思想和国际标准。系统开发应严格遵照国家软件工程规范进行，根据开发进度及时提供有关开发文档，包括软件需求说明书、系统设计说明书、数据库设计说明书、测试计划、用户手册、测试分析报告、系统维护手册、操作手册等。

* + 1. **政策与法规**

1. 《国家电子政务工程建设项目管理暂行办法》（发改委令55号〔2007〕）；
2. 《北京市信息化工作领导小组关于加强信息安全保障工作的实施意见》（京办发〔2004〕3号）；
3. 《北京市电子政务建设管理办法（试行）》(京信息办发〔2004〕39号）；
4. 《北京市电子政务总体技术框架》；
5. 《北京市政务与公共服务信息化工程建设管理办法》（市政府第67号令）。
6. 《国务院办公厅关于政府向社会力量购买服务的指导意见》(国办发〔2013〕96号)
   * 1. **安全性原则**

系统应该保证不同权限级别的人访问不同级别的信息，任何非法的访问都被杜绝。保证信息的有效性、机密性、完整性、可靠性和标识，系统在网络、数据库、应用操作权限和身份认证方面，加载全面的信息安全保护措施。

本平台对安全要求较高。平台设计将安全可靠性作为首要的先决条件，确保系统能够长期、高效和安全可靠运行。系统采用流行、成熟、稳定、先进的操作系统、数据库等，保证系统的稳定性。

* + 1. **标准与规范**

1. 《计算机软件需求说明编制指南》（GB9385-1988）；
2. 《功能建模方法IDEF0》（IEEE 1320.1-1998）；
3. 《信息建模方法》（IEEE 1320.2-1998）；
4. 《信息安全技术信息系统灾难恢复规范》（GB20988-2007-T）
5. 《信息技术安全技术信息安全管理体系要求》（GBT22080-2008）
6. 《计算机软件产品开发文件编制指南》（GB/T 8567-1988）；
7. 《计算机信息系统安全保护等级划分准则》（GB/T 17859-1999）；
8. 《信息技术开放系统互联高层安全模型》（GB/T 17965-2000）；
9. 《信息技术开放系统互联基本参考模型》（GB/T 9387）；
10. 《信息技术开放系统互联应用层结构》（GB/T 17176-1997）；
11. 《信息技术开放系统互联开放系统安全框架》（GB/T 18794）；
12. 《信息技术开放系统互联通用高层安全》（GB/T 18237）；
13. 《电子信息系统机房设计规范》（GB 50174-2008）；
14. 《计算机信息系统设备电磁泄漏发射限值》（GGBB1-1999）；
15. 《计算机信息系统设备电磁泄漏发射测试方法》（GGBB2-1999）；
16. 《电子信息系统机房建设规范》（GB50174-2008）；
17. 《电子信息系统机房施工及验收规范》（GB50462-2008）。
    1. **总体设计原则** 
       1. **先进性原则**

系统应当采用当今国内、国际上先进和成熟的技术，使新建立的系统能够最大限度地适应今后技术发展变化和业务数字化发展的需要。

本项目选择先进的计算机网络、信息存储、信息处理等高新技术手段，合理设计、规划与配置系统的整体结构，实现系统结构合理、技术先进、性能稳定的整体设计目标。

* + 1. **实用性原则**

系统总体设计要充分考虑各用户层当前的不同层次应用要求，对各级用户来说，业务应用操作简便、易用；能够最大限度地满足实际工作要求，使系统始终与用户的实际需求紧密结合，增加系统的实用性。

* + 1. **可靠性原则**

系统应采用成熟的信息化技术和软硬件设备，关键部分要求有备份措施；系统业务软件应能长期稳定运行，并具有较强的容错和自动恢复能力。

* + 1. **兼容性原则**

系统要求能够平滑接入平台目前已建的业务体系中，以保证中心呼叫业务系统运行的完整性。平台设计时，所采用的技术手段遵循相关标准，保证各应用系统间的无缝连接，并具有较高的灵活性，适应后续的升级或引进新技术的需要。

* + 1. **可扩展性原则**

系统设计要求具备良好的开放性和高弹性化结构。系统应采用结构化、模块化的设计理念，可根据业务需要修改某个模块、增加新功能或重组系统结构，以达到程序可重用的目的；数据结构设计合理、规范，同时具有可维护性，对数据库表的修改维护可在很短时间内完成。

系统设计将充分保证系统容量、处理能力和业务范围具有良好的扩展能力；满足项目未来发展的需要，保护投资，避免重复建设；因此系统设计时必须采用当前先进设计思想和主流技术，既要考虑软硬件支撑环境的先进性，更要考虑系统结构、应用设计、网络、硬件的扩展、数据结构和系统二次开发的需要，并支持未来可能出现的新业务的需要。系统网络结构易于扩充，以适应今后的较大任务负载；硬件平台可升级，当需要时可以通过新的设备同原有设备一起工作以提高系统的处理能力，从而保护原有投资。

* + 1. **可维护性原则**

系统应具有较好地可维护性，能够对网络、设备故障、系统配置、系统性能和安全等系统基础环境设备进行管理。设备出现故障时能及时告警并定位，实现运行和维护工作的有效的运维展示。便于系统管理员管理，要能有效辅助系统管理员诊断排除故障，采取有效的措施，使得系统时刻处在良好运行的状态。

* + 1. **实用性与易管理性原则**

系统功能充分满足用户的实际需求，人机界面友好，易于使用、管理、维护、扩展；系统的建设将采用成熟、稳定、完善的产品和技术，满足当前应用需求，使整个系统具有灵活的权限管理机制，系统管理员可以根据使用系统的不同角色对用户进行权限分配，日常维护工作简单、易操作，无需高级计算机用户即可进行系统的日常维护工作。

* + 1. **总体规划、分步实施原则**

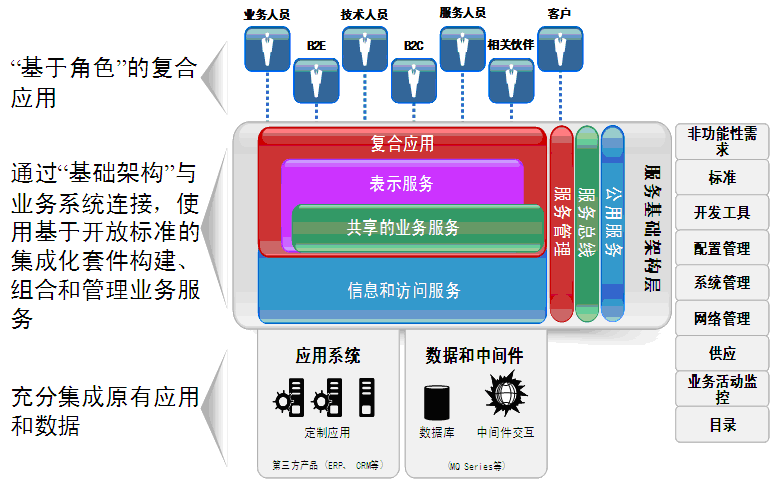
项目建设遵循“总体规划、分步实施”的原则推进，通过设定阶段目标，保证平台建设能够稳步扩展，使平台服务内容和范围能够更为广泛。

* 1. **系统技术线路**
     1. **采用基于SOA框架**

面向服务的架构（SOA）是一种创新思维，它是一种不局限于任何特定技术或厂商的架构方法，屏蔽了不同平台、编程语言、操作系统和硬件架构之间的差异，将企业应用系统中的分散功能组合成可互操作的、基于标准的服务，使其能被重新组合和重用，从而快速满足业务的需求，帮助弥合业务需求与企业IT支持能力之间的鸿沟。采用SOA架构实现应用服务运行管理框架的设计。通过SOA技术实现了服务的注册、查找、管理、监控。通过研究，我们认为服务分为2种，一种由内部组件提供，成为内部服务，包括组织身份服务、访问控制服务等。另一种由外部注册到服务仓库的服务构成，例如会议系统提供的会议室查询服务，此类称之为外部服务。

参考SOA架构的系统将不同的服务通过服务之间定义良好的接口和契约联系起来。服务独立于实现服务的操作系统和编程语言之外，接口采用中立的方式进行定义。构架在各种系统中的服务通过统一且通用的方式进行交互，保证了业务系统的互联互通。采用SOA技术构建的应用系统可以非常方便地实现业务整合、接口整合、信息整合、UI整合。SOA具有松耦合、标准化服务调用、跨平台等灵活特性，很好的规避了系统信息孤岛的产生。

SOA架构模型如下图所示：



图表0‑1SOA架构模型图

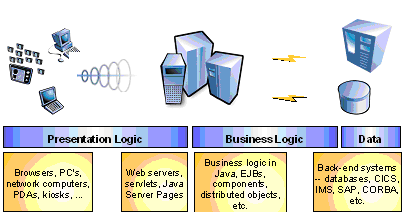
1. 应用系统采用SOA架构的优点

| **特点** | **描述** | **优点，应用性能以及注解** |
| --- | --- | --- |
| 松散耦合 | 服务提供者和消费者可以用定义良好的接口来独立开发。服务实现者可以更改服务中的接口、数据或者消息版本，而不对消费者造成影响。 | 松散耦合消除了对系统两端进行紧密控制的需要。就系统的性能、可伸缩性以及高可用性而言，每个系统都可以实现独立管理。它并没有消除任何的运行时依赖性。它可以划分众多服务提供者的依赖性，但如果该运行时系统需要 24x7 的可用性以及每秒 50000 的吞吐量的话，那么对服务提供者的这些需求必须得到满足。  实现的改变被隐藏了起来。松散耦合给服务提供者和消费者提供了独立性，但要求基于标准的接口和中间物来积极地管理和代理终端系统之间的请求。 |
| 基于行业标准 | 真正的行业标准是由技术旗舰如BEA、IBM、Microsoft、Sun、Oracle、W3C 以及 Oasis 所认可的。SOA 由于其可以用基于标准的技术来实现，所以它被广泛接受。消除了拥有私有客户的需要。 | 使用基于标准的技术可打破行业垄断并促进供应商产品的最优组合。松散耦合层的概念依赖于在内部和外部对标准的广泛支持。 |
| 可重用的服务 | 由于服务是在目录中发布并且在整个网络中都可用，所以它们变得更加容易被发现和重用。如果某个服务不能被重用，那么它可能根本不需要服务接口。为了不同的目的再次将服务组合，这种方式也可以实现服务的重用。 | 服务重用避免了重复开发之苦，同时提高了实现中的一致性。服务的重用比起组件或者类的重用更容易实现，在过去曾尝试过组件和类的重用，但很少成功。 |
| 同步服务调用 (RPC 方式) | 在同步服务调用中，调用方进行调用、传递所需的参数、中断并等待响应。 | 如果服务提供者可用，那么同步服务调用可为请求提供立即响应。同步服务对于要求实时响应的应用程序来说是至关重要的。 |
| 异步服务调用(文档方式) | 在异步服务调用中，调用方向消息收发服务发送一个包含完全上下文的消息，收发服务将该消息传递给接收者。接收者处理该消息并通过消息总线向调用方返回响应。在消息正在处理的过程中，调用方不会中断。 | 由于粗粒度消息和消息收发服务的使用，可以对服务请求进行排队并以最合适的系统速度来处理它们。这种方法具有高度可伸缩性，原因是队列允许的长度是多少，消息收发系统就能够对多少请求进行排队。调用方并不在处理过程当中保持网络连接，并且由于调用方并不会中断，所以它们不会受处理延迟的负面影响，也不会受异步服务执行中所存在问题的负面影响。  本实现采用回调的支持，这本身并不是 Web 服务标准的一部分。 |
| 无干扰开发（通过使用现有的软件组件来开发服务） | 现有的软件组件并不需要修改就可以将其功能作为服务提供出来。服务是用组件的接口定义开发或生成的。 | 消除了修改、测试以及维护现有软件的需要。有了组合服务，来自现有投资的功能可以被重用并重新组合来为企业创造新的价值。 |
| 策略管理 | 当把共享的服务应用于应用程序中时，针对每个应用程序所特有的规则被外化为策略。在设计和运行时，必须就每个服务进行策略的管理和应用。 | 基于策略的计算可以促进普通的可重用服务的创建。随着特定应用程序服务定制的外化，应用程序实现的变化被减少到了最低限度。  通常实施策略的是一个组织的操作和支持小组，并非开发小组。如果不使用策略的话，应用程序的开发人员以及操作和支持小组不得不在应用程序开发过程中并肩工作来实现并测试策略。策略的使用使得开发人员能够集中精力于应用逻辑，而使操作和支持小组专注于规则。 |
| 数据访问服务 | 数据访问、集成、转换以及重用服务。 | 隐藏数据源的复杂性，同时加强跨数据源的一致性、完整性以及安全性。 |
| 组合服务 | 组合服务将新的现有的应用程序逻辑和事务处理进行了合并。 | 充分利用现有的 IT 投资。适用于绿地和遗留实现。装配或者编排产品简化了异构系统的集成。 |
| 共享的或企业的基础架构服务 | 基于 SOA 构建的所有应用程序所使用的公共服务称为共享的基础架构服务。使用共享的基础架构来提供公共服务可以避免每一个应用程序构建类似的服务。 | 使用共享的基础架构服务可提供一致性，并允许单点管理。  其他的共享服务（例如与安全相关的服务）可以通过将现有的产品作为服务直接提供出来的方式创建。 |
| 细粒度服务 | 细粒度服务实现最小的功能，同时消耗并返回最小量的数据。  细粒度服务可以用 Web 服务来实现，也可以利用基于RMI、 .Net 或者 CORBA 的分布式对象来实现。 | 细粒度服务的优点是可在粒度级实施严格的安全和访问策略。  实现和单元测试很简单，而且相互独立。 |
| 粗粒度服务 | 粗粒度服务比细粒度服务实现更多的功能，并消耗不同数量的结构化数据或者消息。它们返回类似的数据或者消息，可能还含有内嵌的上下文。 | 粗粒度服务不需要通过网络多次调用来提供有意义的业务功能。 |

图表0‑2SOA架构的优点表

* + 1. **基于B/S/D三层结构开发应用系统**

采用Browser/WebServer/DataBaseServer三层结构进行应用系统的开发。

* ****

图表0‑3三层结构应用开发图

Browser/WebServer/DataBaseServer三层结构如上图所示，下面对B/S/D三层结构作详细的阐述。

1、数据与应用逻辑分离的特征

Browser/WebServer/DataBaseServer结构指硬件的体系结构，也有相应的逻辑的体系结构相对应。在Browser / Web Server / Data Base Server计算模型中，要完成的功能在浏览器、Web应用服务器和数据库服务器之间进行划分。

硬件的Browser/WebServer/DataBaseServer结构，通常是指某项请求任务在浏览器或Web应用服务器和数据库服务器之间进行分配，其中浏览器用来发送请求和前端表示处理，Web应用服务器处理来自浏览器的请求，数据库服务器处理数据查询逻辑处理。

对逻辑系统体系来说，分为表示层、商业逻辑处理层、和数据处理层三层客户\服务器结构。

鉴于两层结构(C/S)在设计和应用的局限性，将复杂的业务数据处理提出，将复杂的业务数据处理提出，将系统的逻辑结构和物理结构分离，形成三层结构的客户\服务器结构，运用基于组件的分布式技术，从结构上就避免两层结构的局限性.三层结构具体内涵如下：

2、用户服务(客户层)

用户服务层是应用的用户接口部分，是用户与系统间交互信息的窗口。它的主要功能是检查用户输入的数据，显示系统输出的数据。

如果用户服务层需要修改时，只需改写显示控制和数据校验程序，而不影响其他两层。检查的内容也只限于数据格式和取值范围，不包括有关业务本身的处理逻辑。该层是浏览器。

3、商业服务(中间层)

崭新的一层是商业服务层，它是应用的主体，它包括了应用中全部的业务处理程序。除了输入/输出在用户服务层、数据库在数据服务层外，全部的统计、汇总、分析、打印功能全部封装在商业服务层。

他的一方面起传递数据作用，一方面进行强大的数据处理。该层还承担安全性检查的任务。

4、数据服务（数据库）

数据服务层就是数据库管理系统（DBMS），负责管理对数据库数据的读写。DBMS能迅速执行大量的数据的更新和检索。一般商业服务层通过发送SQL命令来操作数据库的数据。

5、采用B/S/D架构的优势

浏览器Browser/WEB服务器Server/数据库服务器Database是解决公共信息服务以及交互相应动态服务最适用的一种应用模型。实现了真正意义上的瘦客户，大大简化了应用系统的分发、配置管理和版本管理工作。

6、分布式

C/S技术的出现，给系统集成方案带来了集中的信息和本地的PC环境，但其数据的共享程度是很不够的。当今的信息技术需要新的解决方案，它提供以客户为中心的用户界面和Web的分布结构，它带有IT环境的个人特征，如数据存取、安全性能等，这就是我们通常所说的三层结构。

7、Web结构的优势

在Web结构中，事务层和数据逻辑层放在中间组件层，这是关键，是与C/S结构的最大区别，它能解决以下几个问题：

客户端很瘦小，并且很容易在运行时自动升级；

事务层可在跨平台的客户端上共享；

不同逻辑组件的分离意味着图形设计人员、事务逻辑开发人员和数据库分析人员可以独立地设计他们各自的部分；

统一的、抽象的用户界面可使用户更有效地从同一数据源中存取数据；

8、开放性

Web是一个开放的环境，应用由复用组件集成，通过标准语言汇编、跨平台的统一协议发布，用标准用户界面显示，它与硬件平台和操作系统无关。

1）充分利用现有IT资源

由于系统必须适应不断变化的业务需求，利用已有的资源系统方面的投资，而不是重新制定全盘方案就变得很重要。这样，一个以渐进的方式建立在已有系统之上的服务器端平台机制是系统所必需的。

2) 高效的开发

这样开发人员可以把精力集中在如何创建逻辑上，相应地缩短开发时间。由中间件提供复杂的中间件服务。

状态管理服务—让开发人员写更少的代码，不用关心如何管理状态，这样能够更快地完成程序开发。

持续性服务—让开发人员不用对数据访问逻辑进行编码就能编写应用程序，并且生成更轻巧，与数据库无关的应用程序，这种应用程序更易于开发与维护。

分布式共享数据对象CACHE服务—让开发人员编制高性能的系统，极大提高整体部署的伸缩性。

* + 1. **全面应用XML技术及Web Service技术**

系统全面采用XML、Web Service技术进行数据、服务描述及数据交换。

XML（eXtensible Markup Language,可扩展标记语言）是Internet上数据表示和数据交换的新标准。它是ISO（International Organization for Standardization，国际标准化组织）的SGML（Standard for General Markup Language，通用标记语言标准）的一个简化子集。XML关注信息本身，是Web上表示结构化信息的一种标准文本格式。与传统的注重页面信息显示的HTML（Hypertext Markup Language, 超文本链接标示语言）相比，关注于内容的XML具有诸多优点：良好的可扩展性，语言简单有效，可自行定义标记；内容与形式的分离，主要刻画数据内容，不考虑显示效果；有严格的语法要求，便于分析统一和与数据库信息转换；便于传输，为纯文本形式，可通过Http协议直接传输，可跨越防火墙；等等。

在XML基础上发展起来的Web服务（Web Service）使用基于XML的消息处理作为基本的数据通讯方式，消除使用不同组件模型、操作系统和编程语言的系统之间存在的差异，使异类系统能够作为计算网络的一部分协同运行。开发人员可以使用像过去创建分布式应用程序时使用组件的方式，创建由各种来源的Web服务组合在一起的应用程序。由于Web服务是建立在一些通用协议的基础上，如HTTP（Hypertext Transfer Protocol, WWW服务程序所用的协议），SOAP（Simple Object Access Protocol，简单对象访问协议），XML，WSDL（Web Services Description Language，Web服务描述语言），UDDI（Universal Description，Discovery，and Integration，通用描述发现和集成协议）等，这些协议在涉及到操作系统、对象模型和编程语言的选择时，没有任何倾向，因此Web服务有很强的生命力。

* + 1. **基于UML 2.0进行系统建模**

整个系统将采用UML2.0 “41”视图进行系统建模。广义地看UML，它已经不仅仅是一种建模语言，而是一个可以用于定义语言家族的元元核心和一个通用建模元语言的结合体；作为狭义的UML，UML 2.0较之以前的版本，在基于构件的软件工程、实时和嵌入式系统、业务过程的描述能力等方面都有很大的增强。 OMG的UML修订任务组和分析设计组的联合主席Cris Kobryn表示，UML 2.0已经变成一个基础更坚实的规范，可以为未来的软件工程、测试和业务规则建模提供更强大的支持。

* + 1. **面向构件技术及方法论**

面向构件技术整合了传统的构件技术、模型驱动技术和面向服务技术。构件的意义超越了技术层面的代码集合，而是真正做到与业务层面的内容相映射。构件将成为表达业务需求的最小单元，在特定行业中，通过积累可以形成相对完备的客户业务需求构件库，以构件组装的形式快速搭建客户的应用；以构件修改和构件增减的方式快速满足客户业务需求的变化。其次，从构件的技术实现角度来说，可以用四个要素来陈述软件构件模型：构件本身、该构件的插口、构件与其他构件协作的能力、以及构件的使用者。

面向构件的开发是一种软件开发手段，在开发周期的不同阶段和不同方面，包括需求分析、结构、设计、建立、测试、上线、支撑性技术架构、项目管理等，都以构件为基础，同时为了使构件可随时用于组装，这些构件必须作为项目的零件来建造。

本系统将采用面向构件的系统分析与设计方法。

* + 1. **基于组件模型的系统内核结构**

组件模型是系统架构的一种形式，软件开发过程从过程功能模型、面向对象模型、到组件模型。广义上讲，组件就是实现一类业务功能的、可重用的、可独立部署和设计的程序集合，这些程序有明确和完善的接口定义，通过接口完成功能请求，具体实现则通过封装机制屏蔽，而内部通过多种设计模式，保证组件的合理性。

采用组件模型可以通过业务功能封装在不同的组件中，实现功能分解，降低系统的耦合度，保证系统中的各个组件能够独立地修改和扩展。同时，组件模型还支持通过组件扩展系统功能，保证系统能够可持续的进行扩展。

在本系统的设计过程中，通过提炼业务功能需求和系统需求，分解业务处理流程，把系统划分为若干通用组件和若干业务功能组件。通过系统平台提供的组件管理工具实现组件的配置和管理，通过流程和功能把组件整合成相应的系统功能，这样，可以从两个方面保证系统的可持续扩展能力：

1、充分利用已有的成熟通用组件，加快系统的开发速度，通过更换这些通用组件，可以实现基本功能层面的功能扩展；

2、抽象并实现业务功能组件，实现业务功能的快速搭建，通过扩展业务组件，可以实现业务功能扩展。

通用组件和业务组件是应用系统稳定、持续、高效运行的核心组成部分。总的来说是将逻辑及应用的同类或相似的概念和方法抽象出来，以类的形式加以约束和实现，并定义相应的接口，也即定义数据的输入输出的规范；再将逻辑或功能相关的类集合在一起构成一个组件（类包），来完成一个或一组功能的实现；最后是将各个组件统一进行封装，给表示层提供清晰明确的接口，并通过自身相对数据层的访问接口与其进行通信。

* 1. **系统功能设计**
     1. **数据中心升级改造**

1.数据仓库

统计分析系统的真正关键是数据仓库的存储和管理。数据仓库的应用目标和数据的组织管理方式决定了它有别于传统数据库。要决定采用什么产品和技术来建立数据仓库核心，则需要从数据仓库的技术特点着手分析。

数据仓库中的数据是来源于联机事务处理系统长期积累的历史数据，

数据仓库所涉及的数据量比传统事务处理大得多,而且随时间的推移，其数据量还在不断的增加。从现有技术和产品来看,只有大型关系数据库系统能够担当此任，关系数据库经过近30年的发展,在数据存储和管理方面已经非常成熟, 非其他数据管理系统可比。目前不少关系数据库系统已支持数据分割技术,能够将一个大的数据库表分散在多个物理存储设备中,进一步增强了系统管理大数据量的扩展能力。采用关系数据库管理数百个GB甚至到TB的数据已是一件平常的事情。目前交大学院数据中心使用了ORACLE数据库，可满足此重任。

数据仓库中的数据存储首先涉及到数据缓存区。数据缓存区区域是临时数据存放区，其数据模型完全按照原始系统的数据格式。

ODS为操作性数据存储区，它基本保持业务源系统的数据结构不变，由数据缓存区提供每天增量数据加载到ODS。ODS根据具体需要，一般保存3-6个月的历史数据，为历史交易查询和操作性报表和操作性应用等提供数据支持。

DWD是整个系统的核心，依据逻辑数据模型划分10大数据模型主题存储和管理来自各种源数据系统的数据（包括当前及长期的历史数据），并为访问用户提供数据服务。

数据转换和存储层还包含从属数据集市，应用数据区就是一系列从属数据集市（DM），这些数据集市的数据来自DWD或DWA，可以确保其数据质量和数据一致性。对于某些特定的应用，例如某些业务报表其实时性要求非常高，那么也可以通过数据缓存区区域为其提供数据。

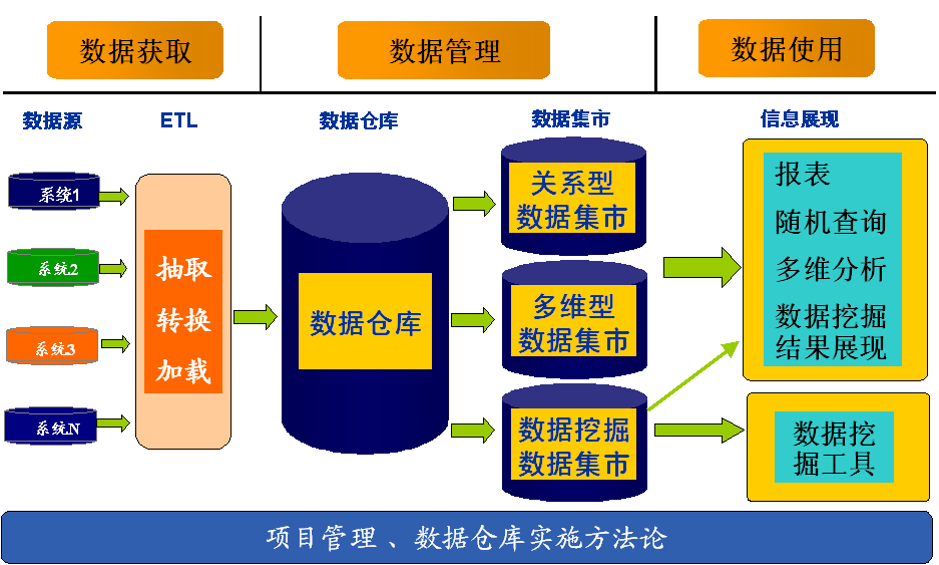


图 2 数据仓库逻辑结构图

基于交大学院数据中心信息构建的微型数据库存储，主要是将案件、服务商等的基础数据按照数据标准化进行清洗、转化，为OLAP分析模型提供数据支撑。

数据仓库为所有用户服务，具备极高的扩展性和性能，提供完整的、即时的数据，强化BI和分析能力。

2.数据ETL

针对分析模块中的数据进行数据的清洗以及抽取等。ETL过程，完成将业务源系统的数据，进行抽取、转换、（清洗）、加载到数据仓库的过程（同理，数据仓库的数据向数据集市的流转也需经过ETL过程）。通常，ETL过程的具体内容包括，将分布的、异构的数据源中的数据如关系数据、平面数据文件等抽取到临时中间层后进行清洗、转换、集成，最后加载到数据仓库或数据集市中，成为联机分析处理、数据挖掘的基础。

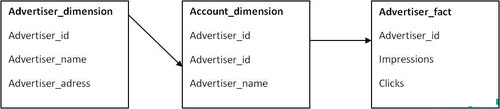
ETL是数据中心建设过程中的非常重要的一环。它是承前启后的必要的一步。在技术上，ETL主要涉及到关联、转换、增量、调度和监控等几个方面。数据仓库系统中，数据不要求与联机事务处理系统（业务系统）中数据实时同步，所以ETL可以定时进行。但多个ETL的操作时间、顺序和成败对数据仓库中信息的有效性至关重要。ETL过程、实现方式（设计）与质量，最终影响数据仓库与数据集市加载数据的准确性、完整性、一致性、完备性、有效性、时效性和可获取性等几个特性。

ETL过程中，通常处理的内容包括：空值处理、规范化数据格式、拆分数据、验证数据正确性、数据替换、Lookup等。

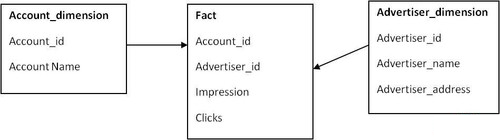
3.OLAP模型

根据多维模型建设原则，将DM层的数据按照前端展现的要求进行业务模型、物件模型等的星型或雪花型构建，满足即席查询、报表分析的需求。

雪花模型使用的是规范化数据，也就是说数据在数据库内部是组织好的，以便消除冗余，因此它能够有效地减少数据量。通过引用完整性，其业务层级和维度都将存储在数据模型之中。



相比较而言，星形模型实用的是反规范化数据。在星形模型中，维度直接指的是事实表，业务层级不会通过维度之间的参照完整性来部署。



雪花模型使得维度分析更加容易，比如：交大学院数据中心某特定加盟服务商，有哪些区域潜在客户或者客户在某日寻求此类服务商的服务。

星形模型用来做指标分析更适合，比如：交大学院数据中心某类型型的案件，接单率、派单率、满意率是多少。

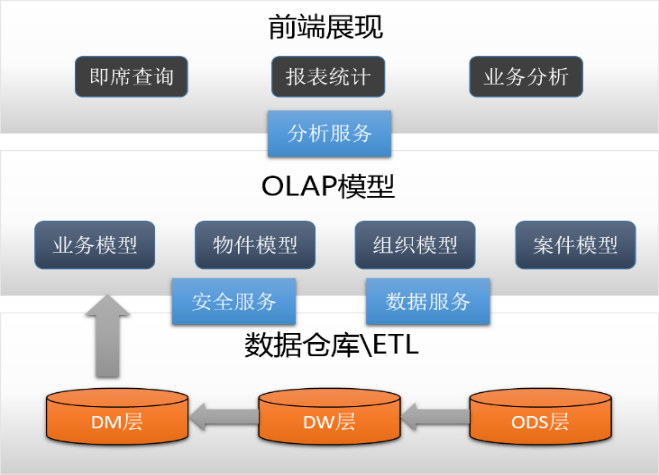


图 3 数据模型示意图

OLAP提供多维数据管理环境，典型的应用是对案件办理的建模与数据分析。

OLAP展现在用户面前的是一幅幅多维视图。

维（Dimension）：是人们观察数据的特定角度，是考虑问题时的一类属性。

维的层次（Level）：观察数据的某个特定角度（即某个维）还可以存在细节程度不同的各个描述方面（时间维：日期、月份、季度、年）。

维的成员（Member）：维的一个取值，是数据项在某维中位置的描述。（“某年某月某日”是在时间维上位置的描述）。

度量（Measure）：多维数组的取值。（例如：2014年12月1日，大峪街道，案件，10）。

OLAP的基本多维分析操作有钻取（Drill-up和Drill-down）、切片（Slice）和切块（Dice）、以及旋转（Pivot）等。

4.数据展现

数据分析和表现是数据仓库的门面，必须借助专业厂商的专业工具。它们主要集中在多维分析、数理统计分析、图表等。

数据仓库通过OLAP技术，能完成即席查询和动态报表的生成。数据仓库赋予数据多维的概念，使得用户可以从多种角度来观察数据，可以对数据进行任意的旋转、切分和钻取。这使得用户可以随机的查询数据仓库中的数据，获得数据仓库中的任意的数据。这就使得用户在完成特殊的查询时不需要编写程序，而仅仅通过简单的人机交互即可完成。

从人机界面来说，目前的工具都支持多种类型的常用图表，如报表、直方图、饼图、折线图等；另外，基于展现应用服务器的系统还可以为用户提供基于WEB的访问方式，大大提高的系统的易用性和易维护性。

5.统一用户

用户管理系统的建设目标是，统一管理交大学院智能统计分析系统的用户及其权限分配等管理功能；实现与交大学院系统无缝对接，实现统一用户登录。应用系统实现统一认证和单点登录提供基础的数据服务。

用户管理系统负责对平台的多类用户进行管理，主要包括以下部分：

1、用户管理：在系统中对用户采用分级分类管理的方式，即系统管理员可以管理所有用户，为所有用户分配操作使用权限，而拥有“组管理”权限的用户也可以管理与自己同组织的用户。具体功能模块包括用户注册、用户审核及授权、用户信息及状态修改、察看用户资料。

2、用户组管理：用户组是用户的集合体，类似于现实工作中的组织结构。注册用户可以隶属于用户组。用户组采用树型结构进行管理和显示，同时可以通过查看用户信息，了解用户所属组织和角色。

3、组织机构配置：用户组就是反映的用户隶属的组织机构，采用树型结构显示和管理，通过改变其父节点的位置，整体的移动组织机构节点和子节点的隶属关系。

4、角色管理：角色是具有相同职能的用户集合。管理员可以自由定义角色以及角色所拥有的权限。

5、权限分配：针对角色的权限进行分配组合，形成该角色的具体权限列表。

6、资源访问控制：针对细粒度的访问控制，提供资源项的定义，进而配置ACL访问控制列表，达到细粒度的数据访问控制管理

7、日志管理：记录用户的操作轨迹和系统的状态，如用户登录、非授权访问、敏感操作等。系统管理员可以利用日志管理提供的信息作为系统的监视、诊断和维护的依据。日志信息包括三种类型：信息、告警和错误。

* + 1. **决策辅助分析系统**

1.数据仓库设计

* 面向主题

操作型数据库的数据组织面向事务处理任务，各个业务系统之间各自分离。而数据仓库中的数据是按照一定的主题进行组织的。

* 集成

数据仓库中的数据是在对原有分散的数据库数据抽取、清理的基础上经过系统加工、汇总和整理得到的，必须消除源数据中的不一致性，以保证数据仓库内的信息是关于整个系统的一致的全局信息。

* 相对稳定

数据仓库的数据主要供决策分析之用（本项目用于Oracle BI系统以及呈现各种报表之用），所涉及的数据操作主要是数据查询，一旦某个数据进入数据仓库以后，一般情况下将被长期保留，也就是数据仓库中一般有大量的查询操作，但修改和删除操作很少，通常只需要定期的加载、刷新。

* 反映历史变化

数据仓库中的数据通常包含历史信息，系统记录了从过去某一时点（如，开始应用数据仓库的时点或业务系统起用的时点）到目前的各个阶段的信息，通过这些信息，可以对交大学院的发展历程和未来趋势做出定量分析和预测。

数据仓库从业务处理系统获得数据，主要以星型模型和雪花模型进行数据组织，并为用户提供各种手段从数据中获取信息和知识。

2.数据集市设计

数据集市是一个从集合数据中，为满足面向某个主题更专业分析而提供数据的平台。其数据组成是从数据仓库中抽取、再加工出来的。那么，数据集市就是企业级数据仓库的一个子集。数据集市可以分为两种类型：独立型数据集市、从属型数据集市。独立型数据集市直接从操作型环境获取数据，从属型数据集市从企业级数据仓库获取数据，带有从属型数据集市的体系结构。

3.元数据库设计

元数据是描述数据仓库内数据的结构和建立方法的数据。可将其按用途的不同分为两种，信息资源目录元数据和指标元数据。

指标元数据是数据仓库的设计和管理人员用于开发和日常管理指标数据仓库使用的数据。包括：数据源信息；数据转换的描述；数据仓库内对象和数据结构的定义；数据清理和数据更新时用的规则；源数据到目的数据的映射；用户访问权限；数据备份历史记录；数据导入历史记录；信息发布历史记录等。

信息资源目录元数据从决策服务业务的角度，描述了数据仓库中的信息资源目录的原数据。包括：决策分析主题的描述包含的数据、查询和报表。

4.基础数据库设计

1、数据层次划分

在基础数据库的存储层次划分上，逻辑上可划分以下几个层次：

 静态字典数据

 动态字典数据

 基础字典数据

各层次的存储内容如下：

表 1存储内容

| **层次** | **对象** | **内容** |
| --- | --- | --- |
| 静态字典 | 系统运行参数 | 组织机构、角色、资源等 |
| 动态字典 | 行业标准、规范 | 标准、电子政务规范等 |
| 基础字典 | 安全信息 | 系统ACL访问控制设计等 |

2、数据规范

基础数据库的建设必须遵循严格的标准规范进行，以避免数据的歧义以及使用混乱。建设规范重点考虑以下两个方面：

（1）编码规则

对于各类字典的代码编码需要统一定义，明确编码组成含义；对于需要关联的基础数据建立外键进行关联；编码的本身的组成以定长的数字或者字符组成。通过编码规则的统一，实现将唯一信息存储在一个地方，唯一性调用。

（2）数据项定义

各类数据对象的数据项根据交大学院相关单位用户确定，并在此基础上进行适当的项目扩展，以适应未来业务发展需要。

3、数据管理

为确保基础数据库数据的唯一性和可靠性，数据管理方面，需要注意三个方面：

（1）角色授权

对于各类角色与基础数据的操作需要严格的授权，授权形式可按照组织结构分级授权，实现集中与分布的多级管理模式。

（2）操作授权

在角色授权的基础上，对数据的增加、删除、修改、查询进行细化授权，原则上不允许对基础数据库的数据删除；对于增加、修改操作根据数据保密性质进行操作授权，修改时不允许对主键进行修改。

（3）数据安全

基础数据中类似口令、核心参数等数据采用加密算法进行数据加密存储，防止数据被篡改，此外也可通过校验算法增加校验位来确保数据的安全。

（4）数据监控

对所有的基础数据的改动系统提供日志记录（包括修改人、修改时间、修改项目等信息），关键数据提供历史修改记录。

5.智能分析

专题分析是高级的BI分析页面，根据交大学院的具体情况设定，可设置为老服务专题、志愿服务专题、便民服务专题等，供领导使用。通过仪表板对同类业务中的重点业务、关键维度、关键度量进行分析展现，以共享维度为基础，展现当前最新的业务数据，为领导提供最关心的业务分析结果；让用户一眼就大概明了自己要重点了解那一部分信息。仪表盘包含各种图表，初始粒度大，同时支持很深的下钻，可以钻取到相关的明细报表当中查看问题的疑点所在。仪表盘主要通过饼图、柱状图、趋势图、散点图、预警信息、记分卡等较为直观的展现形式表达业务信息。

提供用户自主在线动态分析功能，提高了决策系统的自主应用性。

6.阀值管理

通过设置阀值制定KPI的合理范围，对于超过范围的异常显示。

通过KPI（Key Performance Index ，关键性能指标）可以监控关键数据的发展趋势和状态。

7.报表视图

提供了两种以企业常见的报表格式为基础的分析控件：分析树、表格控件和图表控件、选取元数据查询的维度树，构建报表初始查询。通过设置报表参数生成参数化报表从而能够生成新报表。

8.动态分析

通过访问系统功能模型利用BI工具实现上钻、下钻、展开、转轴等分析操作，得到有用的数据结果报表。

报表的条件定制非常灵活。将固定或通用的报表条件定义在参数化报表中，并作为报表模板存储，再生成报表时，只需在报表模板基础上进行特殊的再定制，减少了重复定制条件的工作量，保证了定制的灵活性。

包括：

* 连接数据源
* 使用维度树选取维度和成员，构建查询
* 使用图表和表格视图显示数据
* 图表中的其它查看操作
* 基础分析操作
* 排序数据、过滤、标明异常值、时间智能等高级分析操作
* 设置报表参数，制定参数化报表

9.综合仪表板

用户还可以把自己相关的报表、图片、以及其他系统页面连接等信息资源联合组织进入综合仪表板，以得到关于某个主题相关指标的综合显示。

**1、添加窗口**

用户可以添加窗口显示已存报表到综合仪表板。

**2、添加标签**

用户可以添加标签主题显示特定主题的报表到综合仪表板

**3、综合仪表板管理**

用户可以对综合仪表板进行添加、删除操作，对名城以及其中标签 、窗口修改，设定用户访问权限等。

10.监控预警

定义和选取预警指标，监测绝对差异和相对差异的变化，不同领域的发展高低值之间的差异，设定预警指标临界值。

11.周期报告

周期报告是交大学院对一段时间内中心业务数据的统计汇总以及发展分析的总结与共享。通过对数据进行整理，按照默认模板，系统化输出文字性描述、数据报表，并按照菜单选项定义输出简单的饼图、柱状图或趋势图。同时，可在平台界面选择添加文本框，定义文本标题，用户可在界面进行文本编辑。

支持以Word、PDF等格式导出。

12.信息日报

用户编写《信息日报》上报，分类统计当日求助件数量。通过选择时间段，出具平台日受理案件总体情况。包括总体情况介绍、重点工作介绍，按照案件类型对案件进行分类统计。提供文字性叙述模板，确定报表格式，以饼图或柱状图的形式输出。用户可根据权限进行编辑修改。

包括时间定义、数据查询、图形选择、内容添加、模板修改、报告导出、历史查询等，根据权限不同，设置报告提交与报告审核功能。

13.信息周报

信息周报是对上一周（以日为单位进行划分）的案件、服务商等数据进行汇总统计，并进一步分析。用户对周报时间进行设置之后，系统根据模板对数据进行输出，并以柱状图或饼状图的形式进行直观展示。同时提供空白文本框，供执行部进行文本描述或模板设置。

包括时间定义、数据查询、图形选择、内容添加、模板修改、报告导出、历史查询等，根据权限不同，设置报告提交与报告审核功能。

14.信息月报

信息月报是对上一月（以周为单位进行划分）的案件、服务商等数据，进行汇总统计，并进一步分析，同时对上一月的诉求办理情况、加盟企业服务情况进行统计，为考核分析提供数据基础。用户对月报时间进行设置后，系统根据模板对数据进行输出，并以饼图或柱状图的形式进行直观展示。同时提供空白文档，供用户进行文本描述或模板设置。

包括时间定义、数据查询、图形选择、内容添加、模板修改、报告导出、历史查询等，根据权限不同，设置报告提交与报告审核功能。

15.即席查询

除了中心报表和仪表盘这一类固定报表，智能统计分析系统还将设计后台对相关人员进行开放，设计后台以报表设计区域为主，模型区域中的各种维表和事实表字段均按照业务人员能够理解的方式进行命名，将模型字段拖拽到设计区域很容易就能做出用户希望的报表，同时还可以将报表保存到个人文件夹下，方便重复利用和查看。

用户根据自己的需求，灵活的选择查询条件，轻松快速地创建、修改和编制报告、图表、数据透视表和信息仪表盘，系统能够根据用户的选择生成相应的统计报表。

即席查询的用户可分为三类：

1、决策用户：可使用的信息为面向全区所有信息；

2、执行部：决策用户信息应用的实现者，同时负责信息的主动挖掘、总结和发布；

3、其他部门业务用户：可使用的信息为部门业务相关信息。

16.综合统计

对行政管理中各类数据和相关业务数据的处理、统计、分析，提供数据的整合能力。

* + 1. **教师肖像数据表支持**

需要与原有学校MIS系统进行数据接口对接，添加教师个人科研教学数据信息及学院各系平局值对比功能，以图表的形式展现。做到教师个人数据与系统数据同步类比功能。

* + 1. **学校肖像数据表支持**

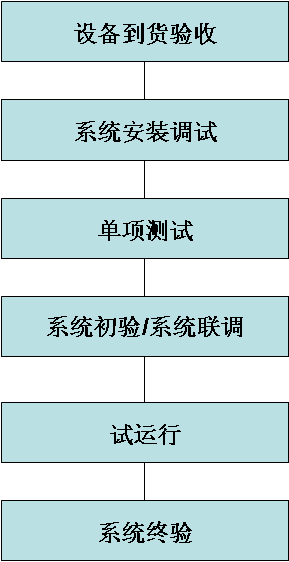
需要与原有学生管理系统对接，增添学院学生活动表单，建设录入、修改、删除等管理功能。通过学生成绩等信息数据的同步，扩展学生个人信息标的维度。对于超出指标的数据进行跟踪预警，增加消息提示和并通过手机向学生发送短信。

* + 1. **完善校友数据库**

增添校友信息数据库表单，开发校企合作信息功能模块包含：企业基本信息、企业来访及拜访记录、阶段性记录成果、教职工研究方向和科研项目与企业的发展相关性分析、校友企业拜访记录等。

* 1. **设备到货验收方案**
     1. **设备验收流程**

设备的验收流程如下所示：



图表4设备的验收流程图

* + 1. **设备到货验收**

设备由我公司运输至最终客户机房，开箱验货需由最终用户、代理商，以及设备原厂商的系统维护工程师三方共同进行。

我公司首先和最终客户确认机房条件安装条件。机房安装条件应符合设备安装要求。设备到达最终客户现场后，首先由我公司清点外包装箱的个数。同时系统维护工程师将协助进行外包装箱运输受损情况的检查，（主要检查在运输的过程中是否有碰撞及倾斜以及是否为原设备包装箱）。

设备开箱应该在最终用户、我公司、设备原厂商系统维护工程师三方到场的情况下进行，在产品维护工程师的协助和监督下进行开箱工作，开箱后需按照随箱所带的设备装箱单进行设备及配件的清点。如有与装箱单不符的情况需要在开箱/安装检查表上进行详细的纪录。并返回产品提供商的客户服务部门进行核查。

清点设备及配件完成并无误后，产品维护工程师将对负责安装的设备进行相应的安装工作，该工作需要最终用户及代理商进行相应的配合。安装完成后，产品维护工程师将按照设备安装手册的规定进行加电测试，如果系统加电正常，无任何报错代码和信息则设备验收和安装工作完成。如有相关设备报错信息，则致电产品技术支持中心进行相应的报修。

设备验收和安装工作完成后，产品维护工程师将在装机报告单上进行详细的纪录并请最终客户进行签字确认。

* + 1. **系统安装调试**

根据工程实施方案以及具体要求对到货设备进行调试安装，并按照合同要求，对系统进行集成。

我公司在对项目涉及的设备进行安装、配置与调试时，应对整个安装、配置与调试的每一步骤以及在安装调试过程中出现的各种问题及解决方法详细地记录到现场安装调试记录中，同时对系统中可能出现的问题及其解决方法形成注意事项向业主的技术工程师进行详细讲解。

安装、调试完成之后，按照建设方对工作环境恢复的要求，恢复工作环境，梳理机柜内和设备之间的连接线缆，使之美观、整齐，利于维护。

我公司在系统安装调试完毕后，向业主提交《工程实施手册/操作手册》（一式两份），验收完毕双方代表签字后各执一份。

* + 1. **系统联调测试/工程初验**

完成安装调试、单项测试检验后，进行整个系统的联合调试检验。我公司根据技术规范中的要求负责系统的联调，之后即进行系统初验工作，以检验系统是否可以投入试运行，改进并完善在联合调试检验中发现的问题。

在项目实施前，根据系统安装调试记录的有关要求，我公司工程师将与业主协商集成工作的测试时间、测试组组成人员、测试内容以及测试步骤和接收条件等，制定《工程初验测试方案》，《工程初验测试方案》需经用户方项目负责人签字认可并作为项目测试的测试依据，同时形成测试记录。

测试组成员按《工程初验测试方案》中要求的测试时间进入测试现场，根据计划中规定的测试内容及测试步骤对系统性能指标进行逐项测试，得出测试结果，形成《工程初验测试记录》并由测试组成员签字确认。

根据《工程初验测试记录》得出的测试结果和合同书中规定的功能及性能指标要求及系统接收准则，由测试组出具《工程初验报告》，并由测试组成员会签认可。

* + 1. **试运行**

在工程初验合格后，整个项目将进入系统试运行期。试运行期将进行以下工作：

1．试运行调查记录

在系统试运行期间，我公司的项目执行人员要对系统的功能、性能、稳定性以及系统的运行效果等各项关键因素进行全面的监测与记录，对出现的问题及时处理并形成系统试运行记录。

同时进行项目培训、文档整理等收尾工作。

2．得出试运行结论

试运行期满后，项目经理根据系统试运行记录得出的系统试运行结果，写出系统试运行报告，做出系统试运行结论，并经甲乙双方签字确认。

3．提交终验申请

各系统均通过测试与试运行后，项目经理根据《工程初验报告》及《系统试运行报告》向建设方提出项目验收申请。

* + 1. **工程终验**

“系统试运行”期满后，检验业主审计信息系统是否可以投入正式运行而进行的验收。

1．项目终验

建设方同意项目验收申请后，根据合同的要求组织项目验收。验收的时间及安排需经用户方、和我公司协商确定。

在项目实施前，根据系统安装调试记录的有关要求，我公司工程师将与业主协商集成工作的测试时间、测试组组成人员、测试内容以及测试步骤和接收条件等，制定《工程终验测试方案》，《工程终验测试方案》需经用户方项目负责人签字认可并作为项目测试的测试依据，同时形成测试记录。

测试组成员按《工程终验测试方案》中要求的测试时间进入测试现场，根据计划中规定的测试内容及测试步骤对系统性能指标进行逐项测试，得出测试结果，形成《工程终验测试记录》并由测试组成员签字确认。

根据《工程终验测试记录》，按照合同的要求对项目中设备的到货情况、系统功能的实现、项目文档的完整性以及项目的系统培训等重要项目进行验收并得出终验结论，业主与我公司签署《系统终验报告》，自三方签字之日起系统进入售后服务期。

2．顾客满意度调查

验收后要请用户协助填写《顾客满意度调查表》，了解顾客对项目的满意程度和存在的问题及顾客进一步的希望，以便不断改进我们的工作。

* + 1. **文档的验收**

我公司在整个工程的实施前、实施中、实施后向用户提交项目的整个文档，文档共分六类，分别为：技术文件类文档、安装计划类文档、网络配置计划类文档、安装结构类文档、系统测试类文档、系统验收类文档。

第六部分实施及进度方案

* 1. **项目实施方法论** 
     1. **项目策划阶段**

提出概念性设想，就项目各个方面的任务进行策划，进行项目风险分析，并就项目可能存在的关键性技术问题进行专题研究。

项目前期准备

1、主要任务

* 项目启动会议
* 确认项目范围和主要目标
* 确认项目阶段性验收及总体验收标准
* 确认项目实施计划
* 成立项目组
* 确定各项目小组的成员及各自的工作职责
* 确定各项目小组的阶段性工作目标
* 确定服务流程及方式

2、输出内容

* 《项目组织机构》
* 《项目实施计划》
  + 1. **需求分析与设计阶段**

进行需求访谈，收集相关资源和样例数据，获得客户需求，对需求调研收集的资料进行分析，得到各项应用或整体系统需求。根据获得的应用或系统需求对平台功能模块和数据项进行分析，实现系统全部功能。

1、业务需求调研

1)主要任务

* 确定系统用户，即确定哪些人将是建成后平台的最终用户群
* 确定需求调研的单位、部门与人员
* 确定系统数据源的采集范围
* 结合合同约定、以及用户的具体需求确定最终的数据采集范围，此时的数据范围指系统级
* 进行用户需求调研、访谈与确认
* 用户需求和数据源的筛选和分析
* 对用户的需求进行分析与挖掘，并分析用户需求的数据源支撑情况，了解哪些需求是没有数据源支撑的或难以支撑的，以便最终确定可施的需求的范围。
* 对收集的大量用户需求进行整理、归并，形成用户的总体功能需求和具体功能需求列表
* 对用户需求的优先级进行排序

根据用户对业务需求的急迫状况、需求本身产生效益的、数据源的支撑状况、处理流程的复杂程度等，制定业务需求的实现顺序。

2)输出内容

* 《业务需求说明书》
* 《软件功能清单》

2、需求分析与功能定义

1)主要任务

* 用户需求概要分析

通过对用户需求的分析，确定用户需求所涉及的、详细的数据源情况，包括数据的来源、粒度的要求。

* 业务需求定义

对实现用户需求所要建设的应用功能进行定义，包括分析的指标、权限要求等进行详细的分析与定义。

* 应用功能分析

对应用功能需求进行分析，区分技术性需求和非技术性需求。

2)输出内容

* 《软件功能需求规格说明书》

3、概要设计

1）主要任务

* 应用体系结构设计
* 业务流程分析
* 对原始数据、单据、报表进行分析，了解并分析数据间固有的业务关系；对系统涉及的业务流程进行分析，了解数据之间的业务规则、数据流向
* 建立实体模型
* 建立实体间依赖关系
* 分析并定义实体的所有属性项和关系属性
* 建立过程模型，以及过程中每个步骤涉及的表单和角色
* 建立数据库结构视图
* 按照关系范式理论，结合业务流程分析结果、功能实现的便利性，设计数据库结构并进行优化，包括实体、属性、关系的优化、历史类实体的处理。
* 功能模块分析
* 根据IPO（输入/处理/输出）理论对所有功能点详细分析，确认所有的功能的输入/输出和处理逻辑

2）输出内容

* 《概要设计说明书》
* 《数据库设计说明书》
  + 1. **系统实现阶段**

按照概要设计进行编码和单元测试，实现系统功能，并进行模块的装配测试和模块之间接口测试。

1、应用开发与单元测试

1）主要任务

* 开发环境安装配置
* 为团队开发环境准备必要的开发工作站、文件服务器、数据库服务器和应用服务器，并安装必要的开发工具和开发辅助工具
* 创建数据库
* 根据《数据库设计说明书》生成数据库创建脚本，并在数据库服务器上执行脚本
* 编写测试用例和测试数据
* 测试人员根据《需求规格说明书》编写测试用例和测试数据
* 应用功能开发与单元测试
* 开发人员根据《概要设计说明书》和项目进度阶段计划中所分配的任务编写功能模块代码，并进行功能模块调试和单元测试。
* 项目经理定期组织项目组成员对开发的功能模块进行互测
* 撰写帮助文档和用户使用手册

2）输出内容

* 数据库创建脚本
* 应用程序代码
* 测试用例和测试数据
* 《用户使用手册》
* 集成测试

3）主要任务

* 建立系统测试计划
* 执行系统测试计划
* BUG记录、整理、汇总
* 修正应用功能中的错误（BUG）
* BUG跟踪
* 生成系统测试报告

4）输出内容

* 《系统测试计划》
* 《系统测试报告》
* 《BUG记录与跟踪表》
  + 1. **系统运行与收尾阶段**

对安装部署的系统确认在实际运行环境中运行的适用性，后续通过不断的系统调优，确认系统达到开发预定的各项目标和标准。

1、系统上线试运行

1）主要任务

* 应用程序编译打包、安装
* 编写系统上线试运行操作流程说明和操作手册，修订相关的管理规定，并与相关业务人员确认其内容
* 下发数据接口规范、操作流程说明和操作手册等文档
* 收集历史数据样本，了解历史数据特征、定义情况
* 编写历史数据导入接口
* 历史数据导入/录入
* 现场联网测试
* 执行系统割接计划
* 试运行跟踪与现场服务支持

2）输出内容

* 《系统操作流程说明》
* 《系统操作手册》
* 修订后的管理规范和管理制度
* 《试运行跟踪日志》

2、项目验收

1）主要任务

* 建立并执行系统验收测试计划
* 移植开发系统到生产系统
* 执行用户培训计划
* 项目实施完成
* 签署项目验收报告

2）输出内容

* 《项目验收报告》
* 《项目总结报告》
  1. **项目实施进度**

本项目工期要求：自签订合同起到项目交付运行6个月。在时间紧、任务重的情况下，我们会加大人员投入、加班加点，利用系统开发期间进行安装和实施工作。总体实施计划如下：

* 1. 调研、需求分析，1个月内；
  2. 系统概要设计、详细设计，1个月内
  3. 系统研发，2个月左右；
  4. 系统试运行，1个月；
  5. 系统正式运行及验收，1个月。

实际实施过程中，以合同签订日为项目启动日，其他时间点依次顺推

项目进度时间表如下：

|  |  |  |
| --- | --- | --- |
| **项目编号** | **项目内容** | **实施时间** |
| 1 | 前期准备、调研 | 2017年1月 |
| 2 | 需求分析 | 2017年1月 |
| 3 | 系统设计 | 2017年2月 |
| 4 | 系统研发 | 2017年3月-4月 |
| 5 | 系统试运行 | 2017年5月 |
| 6 | 正式运行和验收 | 2017年6月 |

图表5项目进度时间表

* 1. **工作阶段划分**

项目整个实施工作大体划分为如下的4个大阶段。

* + 1. **需求梳理、分析和确认**

公司专家团队将对调研后的需求进行梳理分析，并经过内部需求评审后最终形成可提交客户的《需求分析说明书》。

* + 1. **系统设计**
* 概要设计阶段

概要设计阶段主要是建立目标系统的逻辑模型，完成数据库设计、划分功能模块、建立各功能模块间的层次结构及调用关系、确定模块间的接口及人机界面等。

* 详细设计阶段

详细设计阶段是对概要设计的一个细化，主要任务是设计每个模块的实现算法、所需的局部数据结构。

* + 1. **系统的开发、测试工作**

1. **系统编码阶段**
2. 阶段目标（里程碑）

完成整个项目系统的研发及功能修改工作，提交可测试的版本。

1. 客户工作事项

积极配合公司进行开发功能的确认；为公司提供及时的反馈信息。

1. 公司（实施方）工作事项

根据系统需求报告、设计文档进行编码。

1. **系统测试阶段**
2. 阶段目标（里程碑）

完成整个项目研发的测试工作，提供合格的产品；形成《系统测试报告》。

1. 客户工作事项

为公司提供及时的反馈；对测试结果进行评审，并协助公司项目组完成系统测试的确认工作。

1. 公司（实施方）工作事项

进行系统的全面测试；测试结束，提供规定的测试阶段文档。

* + 1. **系统的验收和试运行工作**

1. **系统验收阶段**

系统验收阶段包括初验和终验。系统初验是按照双方约定的初验条件我方发起初验申请并提供初验阶段需要的各个文档，用户方相关人员进行初验工作。

验收通过，要完成各单位的培训工作。

1. **系统试运行阶段**
2. 阶段目标（里程碑）

* 完成软件安装部署工作。
* 开发完成后将使用系统的各用户进行软件的试运行使用。

1. 客户工作事项

* 各级参与试运行的业务部门设置系统的各类参数。
* 督促检查基层单位工作的进展情况，保证基层单位的工作进度。
* 收集下属单位的意见，定期汇总后转交给公司进行解决。

1. 基层单位工作事项

* 执行上级部门制定的任务，进行组织结构、基础数据等数据的初始化。
* 使用交大学院本期项目系统的各项功能进行日常管理。

1. 公司（实施方）工作事项

* 协助客户进行系统的初始化和数据的初始化。
* 系统环境搭建部署。
* 解决软件使用过程中的问题，提供及时的技术支持。
* 协助客户进行系统权限、参数的设置。
* 对其它运行过程中出现的问题进行解决、完善和优化系统。

系统的维护工作从系统试运行便开始，我们将以钻石般的品质为用户提供优质的服务，具体方案可参见技术支持服务章节。免费维护期从终验通过之日起算，提供1年免费维护期。并根据软件使用情况，在质量保证期内免费进行修改、完善，确保系统软件质量良好和运行稳定。

* + 1. **各阶段交付物**

在项目实施过程中，我们将按计划提交下列文档：

| **序号** | **文档类型** | **文档名称** |
| --- | --- | --- |
|  | 招投标文档 | 项目招标书 |
|  | 项目投标书 |
|  | 项目合同 |
|  | 项目管理文档 | 项目计划书 |
|  | 质量控制计划 |
|  | 配置管理计划 |
|  | 用户培训计划 |
|  | 质量总结报告 |
|  | 会议记录 |
|  | 项目需求变更单 |
|  | 实施计划 | 项目实施计划 |
|  | 需求文档 | 需求调研报告 |
|  | 需求分析说明书 |
|  | 设计文档 | 概要设计说明书 |
|  | 详细设计说明书 |
|  | 数据库设计说明书 |
|  | 测试文档 | 测试计划 |
|  | 测试用例 |
|  | 测试报告 |
|  | 用户手册 | 管理员手册 |
|  | 安装部署手册 |
|  | 用户操作手册 |
|  | 培训手册 | 培训手册 |
|  | 试运行文档 | 试运行计划 |
|  | 试运行总结报告 |
|  | 验收文档 | 项目验收申请 |
|  | 项目验收方案 |
|  | 项目实施总结报告 |
|  | 项目总结报告 |

图表6各阶段交付物表

第七部分技术支持与售后服务

北京北信智科科技有限公司通过了有关系统集成、软件开发业务ISO9001质量认证和CMMI4认证。在公司的ISO9001程序文件中，对于工作人员在工作中的每一个方面都有着严格的规定。我公司关于售后的ISO9001程序文件规定了售后服务（发货、安装、调试、培训、维护、维修）的质量控制方法和要求。在售后服务与技术支持的过程中，公司以ISO9001质量体系作为提供优质服务的标准和保障，一个项目从立项到实施，到最终提交给用户及提交后系统的维护和产品维修，都有非常严格的制度和规定。这样做，不但能确保我们的工作可以按步骤有计划地进行，最重要的是确实保证了用户的利益，保证了我们提供的产品与服务满足用户的需要。

* 1. **售后服务与技术支持体系**
     1. **服务承诺**

针对本项目，北信公司如果中标将承诺履行以下售后服务的承诺条款：

1. 承诺免费送货、安装，提供良好的技术支持
2. 对用户提供7\*24小时不间断电话收接，1小时内电话响应，2小时内免费上门服务的优秀服务机制。
3. 硬件承诺原厂保修，实行三包
4. 提供原厂承诺保修函，采购服务器等大型硬件设备提供三年保修承诺
5. 除满足厂家标准服务外，为用户提供本公司其他优质服务内容
6. 在北京市内设有常驻机构，并针对本期项目配有专业的技术工程师 定期进行常规维修维护服务
7. 北信公司承诺自验收合格并签署验收文件后提供12个月质量保证期。即在1年的质量保质期内承诺对所开发系统免费维护和免费升级。
8. 北信承诺提供对本项目全方位的、有效的、及时的技术支持和服务。

对于项目中提供的硬件设备承诺免费维护三年，软件产品免费升级及维护一年，并且提供技术设备安装、调试、使用、维护、升级和新技术推荐等方面的免费咨询服务。

1. 远程技术支持。当系统出现故障，经用户许可后，北信公司将利用远程登录用户系统，进行故障分析、问题定位并提供解决方案。但对系统进行的任何配置、数据改动及其它可能对系统和业务造成不良影响的操作，将会经用户确认后进行。
2. 定期跟踪。项目验收完毕后，北信公司承诺通过定期电话、现场巡检等方式跟踪系统使用情况，听取用户意见和建议，及时分析系统存在的问题，并随时给予解决。必要时，承诺派遣技术人员去现场解决存在的问题。
3. 系统软件升级。质量保证期内，北信公司承诺会及时向用户通报系统软件升级情况，若用户需要对系统软件升级，北信公司将尽量在不影响用户使用现有系统的情况下，科学安排升级步骤，确保提供最新升级版本和相应的系统升级技术服务。
4. 现场服务。自系统验收之日起一年内，提供至少一名具备三年以上相关平台技术支持与运维经验的技术人员常驻用户现场服务。在驻现场人员以及通过远程支持均不能及时解决问题的情况下，将派技术支持人员在4小时内赶赴现场，协助用户完成故障排除、升级或迁移操作，对系统进行完整性检查并跟踪运行。
5. 免费维护期后的服务。在质量保证期结束后，北信公司继续提供对产品故障处理、软件升级等的服务，不以任何借口拖延或中断对产品的售后服务。
6. 保修期结束检查。在保修期结束前，由北信公司工程师和用户代表进行一次全面检查，任何缺陷由北信负责，再修理之后，北信将缺陷原因、修理内容、完成修理及恢复正常的时间和日期等报告给用户负责人。
   * 1. **服务理念**

北信公司依据ISO9001规范，以其在信息技术支持与服务领域丰富的实践经验和良好的信誉，以及雄厚的技术资源，与客户共同解决所面临的问题，为客户在IT运营管理方面提供一种高素质、高效率，全方位的服务。

“一切价值由专业化服务创造”，我们的服务理念是通过对IT系统(软/硬件)提供专业、标准和高效的运维支持和管理服务，通过提高IT系统的运营效率和可靠性、安全性，最终创造可靠的在线业务环境，提供优质的网络应用服务。

* 1. **售后服务组织机构设置** 
     1. **服务组织架构**

北信公司建立人员稳定、有业务素养的技术支持与服务队伍，不断跟踪业务需求的变化，进行系统的完善，提供全面的技术支持服务。北信公司系统开发项目客户服务体系组织结构包括：管理支持部、技术开发部、运维服务部。

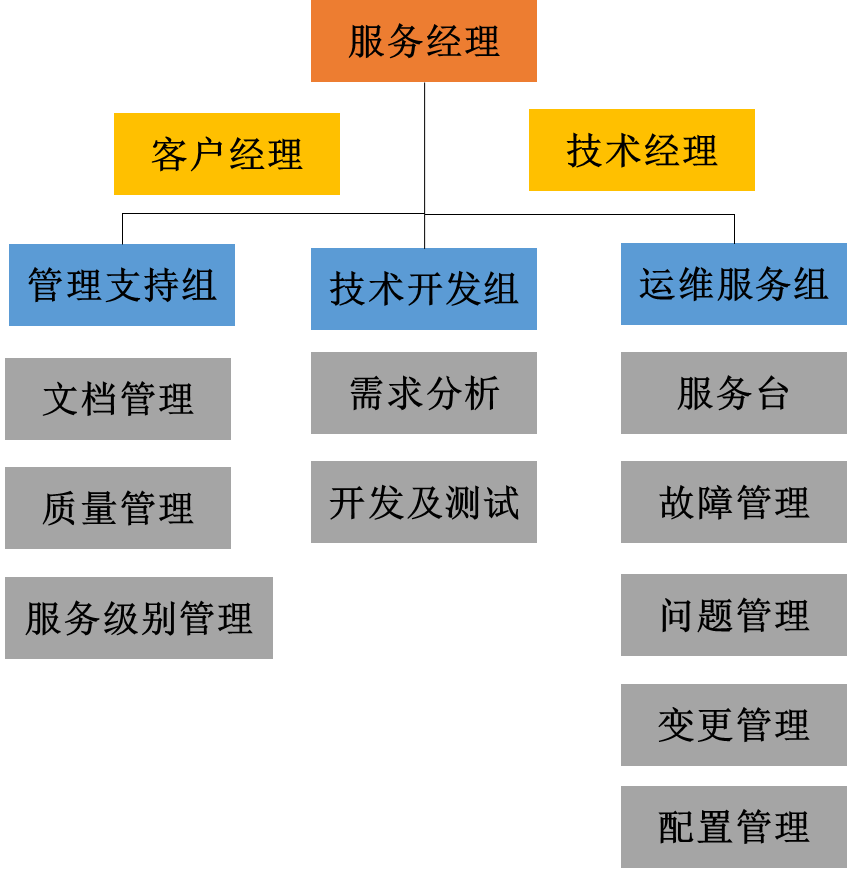


图 26售后报务组织架构图

1）服务经理，总体负责售后服务和技术支持工作，确保售后服务和支持功能能够达到向业主方承诺要求。

2）客户经理，与业主方进行必要的商务沟通。

3）技术经理，负责售后服务和技术支持的总体技术工作，负责服务团队的技术管理，协调解决各类技术问题。

4）管理支持部，按照公司管理要求，对售后服务和技术支持过程进行管理，确保各项工作规范有序，并对各类技术文档进行管理。

5）技术支持部，根据用户需求，进行相应的设计、开发、测试和集成调试工作，以及技术升级服务。

6）运维服务部，提供日常的技术支持和系统维护服务、系统巡检、性能调优、对潜在的故障点进行预防、技术升级、应急保障等工作。

* + 1. **人员保障措施**

对于项目负责人变更对本项目带来的风险的规避，一方面尽量保持项目组成员的稳定性，另一方面采用完善的文档管理制度，尽可能做到某个工作任务情况以文档为准绳，做到不完全依赖于该项目实施人员。项目组成员在工作的每个阶段都提交一定的工作文档，设专人监督和管理项目文档。

* 1. **售后服务与技术支持计划**

北信公司将针对北京市交大学院信息系统安全防护建设向业主方承诺技术后援支持。承诺自双方签署最终验收文件之日起1年内为开发软件系统的质量保证期，其中承诺提供为期1年的软件产品升级服务，所开发系统1年免费维护服务，并提供质量保证期满后的调试、维护、升级和新技术推荐等方面的免费咨询服务。

* + 1. **服务方式**

北信公司为本项目提供现场服务、热线服务和在线服务三种服务方式。

* + 1. **现场服务**

本项目承诺在售后服务与技术支持过程中，除出现以下情况：1）需要到现场进行故障调查、诊断、解决时，提供现场支持服务；2）用户的扩展服务，包括用户培训等；3）用户需要现场咨询和指导；4）应用系统的安装、调试等，提供现场支持外，保证在系统验收之日起一年内提供至少一人，具备3年以上与相类似平台运维经验的技术服务人员常驻用户现场服务。

* + 1. **热线服务**

对售后服务与技术支持过程中，出现以下情况提供7×24热线支持：1）用户故障申报、服务请求时；2）可以通过热线支持解决的故障；3）通过热线提供的咨询和指导；4）软硬件设备服务目录查询；5）故障解决进展情况；6）服务投诉。

* + 1. **在线服务**

在线服务包括Email、QQ、远程登录等形式。对本项目售后服务与技术支持过程中，出现以下情况提供热线支持：1）用户故障申报、服务请求；2）可以通过在线支持解决的故障等；3）通过在线提供的咨询和指导；4）软硬件设备服务目录查询；5）故障解决进展情况；6）服务投诉；7）电子文档传输等。

* + 1. **响应时间**

售后服务和技术支持可以分为：设备故障申报、用户技术咨询、服务请求和投诉处理。这些服务受理的统一接口是服务台，服务台受理故障后，由现场服务工程师或专业技术支持小组处理这些相关的服务。下面分别讲述服务响应时间。

* + 1. **服务受理时间**

1）服务台提供7×24小时固定客户服务热线服务；

2）提供 7×24小时移动客户服务热线服务；

3）同时提供7×24小时的EMAIL/FAX/书面/口头/QQ/WEB等多种方式服务，保持与用户的沟通渠道通畅、有效。

* + 1. **故障申报响应时间**

对于如服务中断、数据丢失、主要功能不能正常工作等系统故障，北信公司提供快速的响应时间：

1）提供7×8小时固定电话热线支持，7×24小时的手机热线支持；

2）工作日1小时内响应，8小时内解决问题；休息日2小时内响应，8小时内解决问题。

* + 1. **技术支持与服务内容**

北信公司为项目提供1年的质量保证期，为系统提供免费维护服务，并根据软件使用情况，在质量保证期内免费进行修改、完善，确保系统软件质量良好和运行稳定。质量保证期自系统验收合格并签署验收文件后开始计算。

* + 1. **质量保证期内技术服务内容**

一、常规支持服务

在1年质量保证期内，北信协助业主方完成日常系统及应用的维护工作，保证系统的正常运行。

1）产品的安装和调试

北信公司派遣工程师现场进行系统的安装、调试和测试，并记录产品安装日志在用户和公司备案。

2）故障处理

系统用户可通过北信公司的热线服务和在线服务（EMAIL、QQ、远程登录）方式报告问题。正常工作日内，北信公司服务团队将在正式接到用户通知后4小时内进行有效响应，例如电话支持，远程解决问题等，如问题不能解决，我们将派有经验的技术人员到达现场进行系统调试，履行其维护义务，帮助处理紧急事故。

3）定期检测服务

北信公司为系统提供定期检测服务，用户也可根据系统运行情况提出检测要求，系统检测将对系统存在的潜在安全或故障隐患进行分析并提出相应的解决方案加以排除。

4）系统升级服务

在系统终验报告签订后2年内，如果本项目涉及的北信公司自有软件产品推出新的版本，将为用户提供产品升级方案及升级服务，如升级中涉及对第三方软件产品的升级要求，将为用户提供一年免费升级服务。系统升级后，公司将提供系统变更的全部技术资料并完成相应培训。

随着业务需求的变化，对于用户所提出的修改、优化原有系统和增加新功能的要求，售后服务小组将需求提交系统开发组，系统开发组进行工作量评估，对于工作量较小的部分，系统开发组将进行及时的修改，并为用户提供最新的补丁程序。对于一些工作量较大的功能或结构变化，北信将在下一个版本中进行修正。以上修改，如发生在项目终验之前，北信将提供免费的产品支持，如发生在保修期内和保修期后，会以优惠价格对系统进行相应的修改。

在保修期内，如果北信公司对合同系统行了技术改进（包括但不限于相关的软件和硬件），如果业主方认为有必要，北信公司免费向业主方提供与这些改进有关的详细技术资料，并对本合同系统进行免费改进。

5）技术咨询服务

北信公司为提供系统调试、维护、升级和新技术推荐等方面的技术咨询服务。

二、应急保障服务

紧急情况的反应和处理是服务质量的重要方面。当前，信息系统往往承担着用户的重要甚至关键的业务或管理系统。当严重的信息系统故障（如宕机）发生，或影响生产的较大故障较长时间不能得到有效处理时，对客户而言，该故障实际上就形成了紧急情况。

北信公司将对于对客户业务造成较大影响、较为复杂的紧急情况，启动危急情况处理体系。由专职服务经理负责，成立危急情况处理小组，调集相关的资源。该小组需每天向公司汇报处理进展，每小时更新紧急情况处理系统的相关记录。该小组具有高度权威，能快速调动相关资源，找到北信公司及原厂商、合作伙伴中最具经验的专家，防止问题处理的任何环节出现延迟，以尽快解决问题。

北信公司将结合多年的运维和重大活动应急保障经验，将为系统应急保障提供完整的解决方案。对于系统在8小时内（节、假日也不例外）未解决故障和问题，北信公司将采取紧急预案，使系统得以正常运行。

* + 1. **质量保证期外技术服务内容**

保修期过后，北信公司将继续为本项目提供多样的支持服务手段。

1）技术咨询服务。保修期后北信公司提供调试、维护、升级和新技术推荐等方面的免费咨询服务。

2）软件技术支持服务。在法定工作时间内，以优惠价格继续为用户提供与服务期内相同质量的技术支持。

* + 1. **技术支持与服务流程**

以下为典型的技术支持与服务流程：

1）故障受理

服务台负责接受用户的技术支持与服务请求，提供7×24小时的受理服务。服务台接受到用户服务请求后，认真填写《故障记录表》，并把问题转交指定的问题管理组。问题管理组直接和客户交流，协调公司内各种技术资源帮助用户解决问题，并分析系统运行过程的隐患和问题，并形成纪录报告，提交技术支持部备案。

2）远程处理

指定处理问题的工程师查询客户文档并与用户现场维护人员联系，根据掌握的故障现象，向用户维护人员提出问题处理指导或远程故障诊断。

（1）电话指导：判断故障由外部原因造成或者故障板件、软件设置等引起，则问题处理人可以电话指导用户做相应的处理措施。

（2）远程故障判断和处理：在掌握故障信息不足以对故障做定位，或者需要远程登陆设备后才能实施解决措施，同用户进行沟通了解必要信息后再进行相关的作业。

（3）现场技术支持准备：在对用户进行电话指导或实施远程登录手段的同时，将依据故障的性质作好必要的现场技术支持的准备工作。

准备备品、备件、维修或升级软件和相关设备。

查阅用户档案，了解设备组网、版本情况，关注其特殊设置或遗留问题。

人员联系信息的汇集：包括用户维护人员联系电话、公司相关技术支持工程师的联系电话。

工程人员解决问题后应将问题处理的结果记录在《问题记录表》中，记录详细的故障信息及处理过程，有无遗留问题等，回复问题的报告人，并将电子文档拷贝给客户代表并归档保存到FAQ库中以备后用。否则落实工程师到现场处理问题。

3）现场处理

如果需要现场进行解决的问题，故障处理组技术人员必须拟定现场解决方案。解决方案经客户同意后才能进行现场实施，双方的确认必须是书面形式，并传真给技术中心。成功实施后再通知客户进行维护。对未经过客户同意的解决方案绝对不允许实施于客户的系统。技术人员解决问题后应将处理的结果记录在《问题记录表》中，并将电子文档拷贝给客户代表归档保存到FAQ库中以备后用。如果现场实施失败，必须上报技术中心，由技术中心出面与客户协商问题解决时间并指定专门小组负责该问题。

如果问题无法按照普通解决方法予以解决，由故障处理研究是否需要并制定升级方案、替代方案，成立专门小组，和用户协商，对系统进行升级和替换。

4）回访

问题解决后，三天内责任工程师将对系统运行情况做进一步的跟踪了解，确保系统能正常稳定运行。

* + 1. **服务质量保证措施**

北信公司基于对客户及其业务驱动的理解，通过建立客户服务规范和用户满意度指标，进行项目客户满意度测评和现场服务满意度测评来了解并掌握客户对服务的感知，据此采取改进措施，提升服务水平与服务质量，不断提高客户的满意度。

* + 1. **客户服务规范**

北信公司根据自身业务特点，建立客户服务规范，规定提供客户现场服务的人员应遵守公司《现场服务守则》：

1）虚心接受客户批评与建议。处理好客户关系，在任何情况下不得以任何借口与客户发生冲突。

2）工作积极主动，谁接待谁负责，不相互推诿，实行“首问负责制”。

3）进房间前先敲门，经允许后方可进入；如客户不在，应在门外静候。

4）服务结束后，征得客户同意后方可离开，并保持环境整洁、干净。

5）主动归纳、汇总服务中出现的问题、经验和教训。

6）使用标准文明礼貌用语与客户交谈，见面要说“您好”。

7）举止大方得体、彬彬有礼，维护公司利益。

8）衣着整洁，仪表端庄，有良好的精神风貌。

* + 1. **服务报告制度**

为确保售后服务质量，并让客户更清晰地了解售后服务实施情况，北信再每一次安全服务完成后，将提供售后服务实施报告。内容包括实施服务的类型、时间、问题分析、解决方案或处理策略建议、实施步骤、实施内容等，使客户可以全面地了解系统运行状态、售后服务情况，便于客户做出正确的决策。

* 1. **其他优质服务**

为了保证本期安全系统等级保护测评的顺利有效进行，测评前参照附件1公安部颁发的系统安全等级保护测评评分标准，提前按照等保三级要求进行软件自测，涉及到的应用系统包括：门户网站，业务系统，呼叫中心相应系统，及时发现问题并整改，减少业主方时间成本与资金成本。

第八部分项目培训

* 1. **系统培训概述**

为了保证北京交通大学学院系统本期项目系统能够顺利移交用户方使用，我公司特为本项目制定了详细的培训方案，以便用户单位进一步明确系统操作细节，保证系统使用实效。

培训内容包括：系统应用培训、数据库管理培训和用户操作培训、系统整体日常运维培训、系统故障应急处理培训、系统使用人员安全意识培训。

通过培训可以使本系统的多级使用者从系统的结构、设备系统的性能、操作使用方法、维护管理技术、定制和升级等各个方面得到全面的掌握。

本方案适用于系统试运行阶段、正式推广阶段及系统长期使用过程中涉及的各个用户。

* + 1. **培训目标**

用户培训目的是让用户能够掌握相关软件操作、维护和管理工作，达到能进行独立使用、日常故障排除、日常维护等目的，保证我公司开发的系统能够正常、安全地运行，切实对用户业务带来帮助。

培训内容在专业化的基础上，将充分考虑用户对象和日常使用系统的内容不同，设定不同的课程，确保每个接受培训的人都能够顺利进行业务操作，完成本岗位工作，提高工作效率。

* + 1. **培训内容划分**

培训内容分为：日常运维培训、软件使用培训。

1．日常运维培训：

日常运维培训包括：系统整体日常运维培训、系统故障应急处理培训、系统使用人员安全意识培训、应用操作系统培训。

* 系统整体日常运维培训是指我公司针对本系统提交系统运行阶段日常维护工作方面的培训。
* 系统故障应急处理培训是指我公司针对本系统试运行阶段与其他类似信息化项目的系统故障处理办法方面的培训。
* 系统使用人员安全意识培训是指根据本项目系统安全建设要求结合客户要求对系统使用人员、系统维护人员进行安全操作方面常识的培训。

应用操作系统培训是指对本系统涉及的部分操作系统日常操作方法进行培训。

2.软件使用培训：

软件使用培训包括系统应用培训、数据库管理培训和用户操作培训。

* 系统应用培训是指我公司针对客户系统管理员进行系统访问、指标定义等定制开发方面的培训。
* 数据库管理培训指本系统日常数据备份、恢复等数据库管理方面的培训。
  1. **培训对象**

培训对象分为三个角色：一般使用人员、系统维护人员和管理（领导）人员。

* 1. **培训方式**

我公司经过多年的积累已经形成了完善的培训和知识转移体系，并由公司经验丰富的实施人员及培训讲师组建了一支实力强大的培训团队，专项完成北京交通大学学院系统本期项目系统用户培训及知识转移工作。

* 1. **个性化培训**

在上述培训方式的基础上，针对用户各使用单位提出的个性化培训需求，我们将会参照集中培训和分区域培训制定的培训目标及培训计划，派出培训教师并提供培训资料。具体的培训内容或方式也可根据具体的个性化要求双方沟通制定。

对于后续的培训需求，由于不属于事先约定免费培训的范围，我公司将按照规定收取相关的培训费用，费用由双方协商确定。

* + 1. **培训流程**

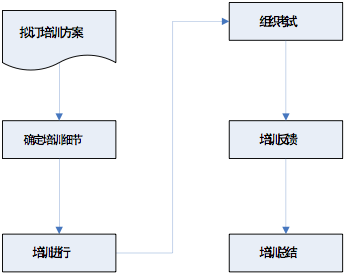


图 27培训流程

培训流程图说明：

* 根据项目需求，初步拟订培训方案，确定培训方法，培训人员组成等。
* 进一步确定培训时间，每期人数等细节
* 按照培训方案及确定的时间组织培训，合理安排培训课程。
* 培训结束后组织进行系统考核。
* 填写培训反馈表，搜集培训意见及建议，为完善后续培训提供参考资料。
  + 1. **培训教材**

我公司将为本项目编制专门的培训教材，培训教材全部为专门编写的实用性教材，我公司提供给参加培训人员人手一套，包括：

* 《培训大纲》
* 《培训计划及指南》
* 《信息系统安装、部署手册》
* 《信息系统运行维护手册》
* 《信息系统故障应急处理手册》
* 《信息系统涉及操作系统操作手册》
* 《信息系统数据库管理员手册》
  1. **培训课程**

根据北京交通大学学院系统本期项目系统的实际情况，我公司制订了详细的、富有针对性的培训课程计划。

* + 1. **培训课程介绍**

北京市交大学院信息系统安全防护建设项目使用培训：

|  |  |
| --- | --- |
| **技能要求和前提** | **课程描述** |
| 掌握计算机基本操作，熟悉浏览器、上网等基本操作，熟悉本单位的数据处理工作制度和流程 | 1.学会使用系统  2.掌握各种数据编辑录入、调整、审核、数据提交使用等实际操作  3.熟悉综合查询分析  4.掌握简单的系统应用技巧 |

表格 23平台系统使用培训表

北京市交大学院信息系统安全防护建设项目管理维护培训：

|  |  |
| --- | --- |
| **技能要求和前提** | **课程描述** |
| 掌握计算机基本操作，熟悉浏览器、上网等基本操作，熟悉本单位的业务制度和流程，有应用系统管理的经验 | 1.掌握系统的安装和配置  2.学习系统运行状态的监控方法  3.学会解决系统常见的故障或错误处理办法  4.掌握系统管理的各项功能  5.系统权限设置  6.日常的基本维护等 |

表格 24平台系统管理维护培训表

北京市交大学院信息系统安全防护建设项目领导使用培训：

|  |  |
| --- | --- |
| **技能要求和前提** | **课程描述** |
| 掌握计算机基本操作，熟悉浏览器、上网等基本操作，熟悉本单位的业务制度和流程。 | 1.软件功能基本操作。  2.掌握系统常用查询。  3.掌握系统查询分析功能使用。 |

表格 25平台系统领导使用培训表

* + 1. **培训风险控制**

针对以上可能出现的风险，在培训中需要注意以下几点，以最大限度减少在培训过程中风险发生的可能性：

* 项目双方确定培训工作负责人，以保证培训工作中双方有效沟通和责任明确。
* 严格按照计划控制项目进度，保证培训计划按时实施的充分可能性。
* 对于确定的培训需求及细节要有相关的文档确认，以保证需求不出现较大变化。
* 合理搜集集中培训结束后本系统使用单位的个性培训需求，由客户培训方面负责人要求系统使用单位上报培训需求，经汇总统计后将培训需求提交给培训负责人，由我公司负责具体培训工作的安排。我公司培训负责人在得到培训需求后，提交给具体的项目培训小组安排培训实施计划，双方确认。
* 我公司将全力保证培训计划的顺利实施。
  + 1. **培训承诺**

我公司向用户郑重承诺：将在北京交通大学学院系统本期项目系统实施完成后，由选派专业培训人员，严格按照项目要求，制定培训计划和培训内容，按照项目培训计划和培训规范，以及用户要求，圆满的完成项目的培训工作，保证系统培训能够高效、顺利、圆满的完成。

总结

根据以上分析，得出以下结论：

1. 北信公司从需求分析、技术架构、解决方案到实施安排、技术支持、售后服务各方面做好了充分准备，请各位专家放心地选用北信公司作为本次项目的合作伙伴。

2. 从项目系统安全、进度、扩展性、集成性出发，要选用稳定、成熟、能够持续服务的合作伙伴。

北京市交大学院本期项目系统招标书表达精准，路线明确。在此，深深感谢前期领导和专家提供的思路。