

# 项目实施管理方案

- 项目实施方案
- 项目实施准备
- 双方事项与责任

XX 项目方成立项目组并指定项目经理监督协调整个项目的执行并指派人员在项目开始后参与配合项目的各项任务。

本项目中开发/生产环境所涉及的其它由 XX 项目方直接采购的设备，由 XX 项目方保证安排其采购、到货日程，保证在我公司的项目日程安排的规定日期前能够及时完成就位，并须负责协调相关硬件供应商安排足够的安装、调试及连接实施技术力量，参与整体系统集成连接、调试过程。如果该部分任务延误或供应商集成技术支援问题，则本项目的实施日程将受影响。

XX 项目方应按项目计划日程，及时提供相关业务资料，如业务手册、作业流程等。

在本项目作业期间，XX 项目方应安排人力参与并配合项目作业，以便日后的管理和维护。为使项目顺利进行，XX 项目方参与作业人员，应按我公司所列日程，完成所负责的交付任务。若因 XX 项目方负责的工作未能按时完成或因非我公司责任的状况发生延误，则本项目的实施日程将受影响。

本项目在开发和测试期间，XX 项目方应保证项目建设、开发和测试环

境的独立性，如果在此期间由于其他本项目以外的项目开发 and 测试导致本项目开发和测试环境宕机，则本项目的实施日程将受影响。

以上配合事项根据项目不同阶段而有所不同，根据项目实际情况酌情调整，并秉着精诚合作态度，积极相互配合。

### ● 交付的文件验收

以本项目规定的交付文件为验收内容。若有验收不合格项目 XX 项目方应于验收期间内书面通知我公司，逾期视同验收通过。验收期为各交付项目交付日起算的五个工作日内。针对不合格的项目，我公司负责改正，并再次对该改正项目提出复验申请，XX 项目方应于三个工作天内进行复验，否则视同复验无误。

如遇特殊情况。经双方书面确认后可以适当延长复验期。

### ● 应用系统功能验收

以双方确认的“应用系统功能清单”所定义的功能为验收内容，参考我公司提供的测试计划及本章中“验收准则”实施。若有验收不合格项目，XX 项目方应于验收期间内书面通知我公司，逾期视同验收通过。验收期为我公司完成“交付项目”所述项目的交付日起算 20 个工作日内，针对不合格的项目，我公司负责改正，并再次对该改正项目提出复验申请，XX 项目方应于 5 个工作日内进行复验，否则视同复验无误。

如遇特殊情况，经双方书面确认后可以适当延长复验期。

### ● 交付件的验收依据

递交的技术文件验收依据是前一个阶段递交的并经双方确认的相关文件。如果前一阶段有变更请求，则本阶段的递交文件仅包含了双方同意必须在本次递交文件中完成的变更内容。

- **验收复查程序**

以上“交付的文件验收”和“应用系统功能验收”，应按计划进行，并以双方项目经理认可的书面签章为验收通过的凭据。考虑到工作效率，以上所述“书面通知”，可以备忘录方式由项目经理代行之。

- **测试资料的准备**

验收测试的测试资料由 XX 项目方准备，测试环境由 XX 项目方提供，我公司负责协助 XX 项目方完成验收测试。

- **开发测试方案**

最终验收测试前，要求对系统进行多种测试（如黑箱、白箱等），保证代码的正确性。其中要求开发过程中对各方法、模块、功能点等必须通过单元测试，并且是 100%覆盖。开发活动必须使用回归测试，并允许在 12 小时内重新进行完整的测试。

- **开发测试意义**

在开发大型软件系统的漫长过程中，面对着极其错综复杂的问题，人的主观认识不可能完全符合客观现实，与工程密切相关的各类人员之间的通信和配合也不可能完美无缺，因此，在软件生命周期的每个阶段都不可

避免地会产生差错。我们力求在每个阶段结束之前通过严格的技术审查，尽可能早地发现并纠正差错。

经验表明审查并不能发现所有差错，此外在编码过程中还不可避免地会引入新的错误。如果在软件投入生产性运行之前，没有发现并纠正软件中的大部分差错，则这些差错迟早会在生产过程中暴露出来，那时不仅改正这些错误的代价更高，而且往往会造成很恶劣的后果。测试的目的就是在软件投入生产性运行之前，尽可能多地发现软件中的错误。

目前软件测试仍然是保证软件质量的关键步骤，它是对软件规格说明、设计和编码的最后复审。软件测试在软件生命周期中横跨两个阶段。通常在编写出每个模块之后就对它做必要的测试(称为单元测试)，模块的编写者和测试者是同一个人，编码和单元测试属于软件生命周期的同一个阶段。在这个阶段结束之后，对软件系统还应该进行各种综合测试，这是软件生命周期中的另一个独立的阶段，通常由专门的测试人员承担这项工作。

大量统计资料表明，软件测试的工作量往往占软件开发总工作量的40%以上，在极端情况，测试那种关系人的生命安全的软件所花费的成本，可能相当于软件工程其他开发步骤总成本的三倍到五倍。因此，必须高度重视软件测试工作，绝不要以为写出程序之后软件开发工作就接近完成了，实际上，大约还有同样多的开发工作量需要完成。仅就测试而言，它的目标是发现软件中的错误，但是，发现错误并不是我们的最终目的。软件工程的根本目标是开发出高质量的完全符合用户需要的软件。

- 开发测试目标

做好软件开发测试，我们将确定以下目标：

(1) 测试是为了发现程序中的错误而执行程序的过程；

(2) 好的测试方案是极可能发现迄今为止尚未发现的错误的测试方案；

(3) 成功的测试是发现了迄今为止尚未发现的错误的测试。

综上，测试的正确定义是“为了发现程序中的错误而执行程序的过程”。正确认识测试的目标是十分重要的，测试目标决定了测试方案的设计。如果为了表明程序是正确的而进行测试，就会设计一些不易暴露错误的测试方案；相反，如果测试是为了发现程序中的错误，就会力求设计出最能暴露错误的测试方案。

## ● 开发测试小组

本项目将根据实际需求以及开发测试时间要求，成立专门的开发测试小组，测试小组成员将由技术过硬的开发工程师与测试工程师组成，其职责是在项目开发过程中负责开发成果测试工作，主要包含的角色以及工作职责如下：

1、测试组长，由测试经理或项目经理指定项目组成员其他人员担任测试组长负责：

分析需求并进行细化可用于执行测试的需求

制定测试计划

参与、跟踪测试过程

对测试活动和结果进行分析，撰写测试分析报告。

2、测试人员，由项目组成员担任，负责：

根据测试计划编写测试用例

搭建测试环境，准备测试脚本

执行测试，记录测试结果和缺陷

执行回归测试

3、开发人员，由项目组成员担任，负责：

单元测试

功能开发完毕之后，提交测试之前的确认测试

## ● 开发需求理解

开发测试小组全程参与本项目开发实施过程，首先了解前期的需求调研报告、XX 项目提出的系统业务需求功能点，以及实施工程师对需求的理解及说明，其次全程参加需求评审、设计评审。通过对文档分析，分解各功能模块，各功能点，为测试用例设计提供数据依据。

反复检查并理解各种信息，与 XX 项目工作人员保持深入交流，理解他们的要求。可以按照以下步骤执行：

1) 确定本项目的功能需求。

2) 对每个开发任务，确定完成该任务所要进行的交易。

3) 确定从数据库信息引出的计算结果。

4) 对于对时间有要求的交易，确定所要的时间和条件。这些条件包括数据库大小、机器配置、交易量、以及网络拥挤情况。

5) 确定会产生重大意外的压力测试，包括：内存、硬盘空间、高的交易率。

6) 确定应用需要处理的数据量。

7) 确定需要的软件和硬件配置。

通常情况下，不可能对所有可能的配置都测试到，因此要选择最有可能产生问题的情况进行测试，包括：最低性能的硬件、几个有兼容性问题的软件并存、客户端机器通过最慢的 LAN/WANF 连接访问服务器。

8) 确定其他与应用软件没有直接关系的商业交易。包括：

管理功能，如启动和推出程序

配置功能，如设置打印机

操作员的爱好，如字体、颜色

应用功能，如访问 email 或者显示时间和日期。

9) 确定安装过程，包括定置从哪安装、定制安装、升级安装。本次项目开发将基于 XX 项目专有云服务基础架构。

10) 确定没有隐含在功能测试中的户界面要求。大多界面都在功能测试时被测试到。还有写没有测到，如：操作与显示的一致性，如使用快捷键等；界面遵从合理标准，如按钮大小，标签等。

## ● 测试策略

测试策略用于说明某项工作的测试方法与目标。系统测试策略主要针对系统测试需求确定测试类型及实施的测试方法与技术。测试策略一般包括下列内容：

确定系统测试策略首先要清楚地所实施系统测试的类型和测试目标。

系统测试类型一般包括：

- 功能测试
- 性能测试
- 负载测试
- 强度测试
- 安全性测试
- 配置测试
- 故障恢复测试
- 文档测试
- 用户界面测试

其中，功能测试，配置测试，安装测试在一般情况下是必需的，其它类型的测试可根据需求进行裁剪。

采用的技术：系统测试主要采用黑盒测试技术来设计测试用例来确定软件是否满足需求规格说明中的要求。

用于测试评估结果和测试是否完成的标准

对测试策略所述的测试工作存在影响的特殊事项

## ● 测试计划

根据测试的种类，测试计划分为功能测试和性能测试计划。

测试计划旨在说明各测试阶段任务、人员分配、时间安排、测试要点、工作规范等。测试计划在策略和方法方面说明如何计划、组织和管理测试

项目。

测试计划包含足够的信息使测试人员明白项目需要做什么是如何运作的。

测试计划不包括测试用例的细节和系统功能的详细信息。

测试计划应附有测试功能点矩阵、测试性能点矩阵。

测试计划应在项目组内进行评审。参与测试计划评审的人员包括：项目经理、测试组长、开发组长、测试组员。

## ● 测试用例

测试用例是为实施测试而向被测试系统提供的输入数据、操作或各种环境设置以及期望结果的一个特定的集合。解决要测什么、怎么测和如何衡量的问题。

从测试结构上面划分分为黑盒测试、和白盒测试 2 种，他们各自有不同的测试方式，目前本公司只考虑黑盒测试，以下设计方法以黑盒方法为例

## ● 测试用例设计方法

黑盒测试用例设计方法有等价类测试、边界值分析、基于因果图的测试、基于猜错的测试、基于场景的测试、基于随机的测试。其中常用的设计方法有等价类测试、边界值分析、因果图三种方法，以下分别介绍这几种方法：

## ● 等价类划分

等价类划分是一种典型的黑盒测试方法。等价类是指某个输入域的集合。它表示对揭露程序中的错误来说，集合中的每个输入条件是等效的。因此我们只要在一个集合中选取一个测试数据即可。

等价类划分的办法是把程序的输入域划分成若干等价类，然后从每个部分中选取少数代表性数据当作测试用例。这样就可使用少数测试用例检验程序在一大类情况下的反映。

在考虑等价类时，应该注意区别以下两种不同的情况：

#### (1) 有效等价类

有效等价类指的是对程序的规范是有意义的、合理的输入数据所构成的集合。在具体问题中，有效等价类可以是一个，也可以是多个。

#### (2) 无效等价类

无效等价类指对程序的规范是不合理的或无意义的输入数据所构成的集合。对于具体的问题，无效等价类至少应有一个，也可能有多个。

确定等价类有以下几条原则：

如果输入条件规定了取值范围或值的个数，则可确定一个有效等价类和两个无效等价类。例如，程序的规范中提到的输入条包括“……项数可以从1到999……”，则可取有效等价类为“ $1 \leq \text{项数} \leq 999$ ”，无效等价类为“ $\text{项数} < 1$ ”，及“ $\text{项数} > 999$ ”。

输入条件规定了输入值的集合，或是规定了“必须如何”的条件，则可确定一个有效等价类和一个无效等价类。如某程序涉及标识符，其输入条件规定“标识符应以字母开头……”则“以字母开头者”作为有效等价类，“以非字母开头”作为无效等价类。

如果我们确知，已划分的等价类中各元素在程序中的处理方式是不同的，则应将此等价类进一步划分成更小等价类。

输入条件	有效等价类	无效等价类
.....	.....	.....
.....	.....	.....

根据已列出的等价类表，按以下步骤确定测试用例：

为每个等价类规定一个唯一的编号；

设计一个测试用例，使其尽可能多地覆盖尚未覆盖的有效等价类。重复这一步，最后使得所有有效等价类均被测试用例所覆盖；

设计一个新的测试用例，使其只覆盖一个无效等价类。重复这一步，使所有无效等价类均被覆盖。

这里强调每次只覆盖一个无效等价类。这是因为一个测试用例中如果含有多个缺陷，有可能在测试中只发现其中的一个，另一些被忽视。等价类划分法能够全面、系统地考虑黑盒测试的测试用例设计问题，但是没有注意选用一些“高效的”、“有针对性的”测试用例。后面介绍的边值分析法可以弥补这一缺点。

## ● 边值分析法

边值分析法是列出单元功能、输入、状态及控制的合法边界值和非法边界值，设计测试用例，包含全部边界值的方法。典型地包括 IF 语句中的判别值，定义域、值域边界，空或畸形输入，未受控状态等。边值分析法不是一类找一个例子的方法，而是以边界情况的处理作为主要目标专门

设计测试用例的方法。另外，边值分析不仅考查输入的边值，也要考虑输出的边值。这是从人们的经验得出的一种有效方法。人们发现许多软件错误只是在下标、数据结构和标量值的边界值及其上、下出现，运行这个区域的测试用例发现错误的概率很高。

用边值分析法设计测试用例时，有以下几条原则：

如果输入条件规定了取值范围，或是规定了值的个数，则应以该范围的边界内及刚刚超出范围的边界外的值，或是分别对最大、最小及稍小于最小、稍大于最大个数作为测试用例。如有规范“某文件可包含 1 至 255”个记录……“，则测试用例可选 1 和 255 及 0 和 256 等。

针对规范的每个输出条件使用原则 (a)。

如果程序规范中提到的输入或输出域是个有序的集合(如顺序文件、表格等)就应注意选取有序集的第一个和最后一个元素作为测试用例。

分析规范，尽可能找出可能的边界条件。一个典型的边值分析例子是三角形分类程序。选取  $a, b, c$  构成三角形三边，“任意两边之和大于第三边”为边界条件。边值分析相等价类划分侧重不同，对等价类划分是一个补充。如上述三角形问题，选取  $a=3, b=4, c=5, a=2, b=4, c=7$  则覆盖有效和无效等价类。如果能在等价类划分中注入边值分析的思想。在每个等价类中不只选取一个覆盖用例，而是进而选取该等价类的边界值等价类划分法将更有效，最后可以用边值分析法再补充一些测试用例。

## ● 因果图

等价类划分法并没有考虑到输入情况的各种组合。这样虽然各个输入

条件单独可能出错的情况已经看到了，但多个输入情况组合起来可能出错的情况却被忽略。采用因果图方法能帮助我们按一定步骤选择一组高效的测试用例，同时，还能为我们指出程序规范的描述中存在什么问题。

利用因果图导出测试用例需要经过以下几个步骤：

分析程序规范的描述中哪些是原因，哪些是结果。原因常常是输入条件或是输入条件的等价类。结果是输出条件。

分析程序规范的描述中语义的内容，并将其表示成连接各个原因与各个结果的“因果图”。

由于语法或环境的限制，有些原因和结果的组合情况是不可能出现的。为表明这些特定的情况，在因果图上使用特殊的符号标明约束条件。把因果图转换成判定表。把判定表的每一列写成一个测试用例。

## ● 猜错法

猜错法在很大程度上是凭经验进行的，是凭人们对过去所作的测试工作结果的分析，对所揭示的缺陷的规律性作直觉的推测来发现缺陷的。

一个采用两分法的检索程序，典型地可以列出下面几种测试情况：

- 被检索的表只有一项或为空表；
- 表的项数恰好是 2 的幂次；
- 表的项数比 2 的幂次多 1 等。

猜错法充分发挥人的经验，在一个测试小组中集思广益，方便实用，特别在软件测试基础较差的情况下，很好地组织测试小组(也可以有外来人员)进行错误猜测，是有效的测试方法。

- **随机数法**

即测试用例的参数是随机数。它可以自动生成，因此自动化程度高。使用大量随机测试用例测试通过的程序会提高用户对程序的信心。但其关键在于随机数的规律是否符合使用实际。

- **测试用例操作步骤**

在设计编写测试用例时，首先要从测试用例库中选择相应功能的测试用例，在原有测试用例的基础上依据系统需求文档对测试用例的进行修改、更新，评审通过后将使用该测试用例测试被测系统。

在测试项目结束后，统计分析所使用过的测试用例，进行分类放到相应的测试用例库中。为以后测试用例的设计编写提供数据基础。

- **测试用例选择准则**

测试用例的代表性：能够代表各种合理和不合理的、合法的和非法的、边界和越界的, 以及极限的输入数据、操作和环境设置等；

测试结果的可判定性：即测试执行结果的正确性是可判定的或可评估的；

测试结果的可再现性：即对同样的测试用例, 系统的执行结果应当是相同的。

- **测试软/硬件环境**

根据需求文档提供的内容，和开发部沟通确定测试项目所需的软硬件环境，完成对测试项目所需软硬件资源的准备工作，使软硬件资源得到满

足。

完成对硬件资源的配置后，要进行对测试项目的软硬件环境进行评审，确认对硬件资源配置的有效性。

### ● 测试数据准备

完成对测试项目基本数据的准备操作，包括数据库连接、用户信息、用户角色权限、单位组织等信息和测试相关的测试数据。

### ● 测试执行过程绩效考核

为促进测试人员积极主动做好测试执行工作，对测试人员进行测试执行过程进行考核。

序号	测试准备内容	考核评分标准
1	测试组长工作安排	待定
2	测试组长风险评估	待定
3	测试人员设计用例	待定
4	测试人员执行用例	待定
5	开发组长配合度	待定
6	开发人员回归次数	待定
7	开发人员处理问题情况	待定

以上统计数据由项目经理提供给部长。

### ● 测试执行

## ● 项目测试周期

测试项目的测试周期可分为：单元测试、接收测试、集成测试、系统测试、回归测试、性能测试等。

## ● 项目测试启动

软件项目测试活动的正式启动，是在确认软件可测试性后展开的。开发人员需要对产品进行单元测试，单元测试效果通过接收测试验证。

## ● 项目测试阶段

测试人员依据测试计划和测试用例进行测试活动。

测试一般分为两个阶段：

1、集成测试、系统测试阶段：该阶段测试人员每天提交缺陷，并跟踪缺陷，验证缺陷，直到提交的缺陷被关闭或被保留。开发人员周期性提交修改过缺陷的新版本，测试人员在新版本上验证缺陷。

2、回归测试阶段：在集成测试、系统测试阶段完成后，产品将进入回归测试阶段。测试人员对修改后的产品进行重新功能验证，确保修改的正确性，验证在修改缺陷的同时没有引入新的问题。回归缺陷是指开发人员标示已修改的缺陷，经测试后发现仍未修改正确，或引入其他缺陷，或在前一个版本中未发现的缺陷，在后一个版本中出现。

如产品进行性能测试，则需要在性能测试后，进行一轮回归测试，确保功能的正确性。

## ● 项目测试结束

项目测试结束时应达到测试质量目标所规定的标准。通过评审后结束该项目测试。

- **测试变更**

当需求变更，功能变化，测试人员根据变更情况，评估测试变更所需时间，提出变更风险。如变更情况被项目组通过，测试组长要修改相应的测试计划，测试人员要从新设计测试用例。

- **缺陷管理**

- **缺陷基本属性**

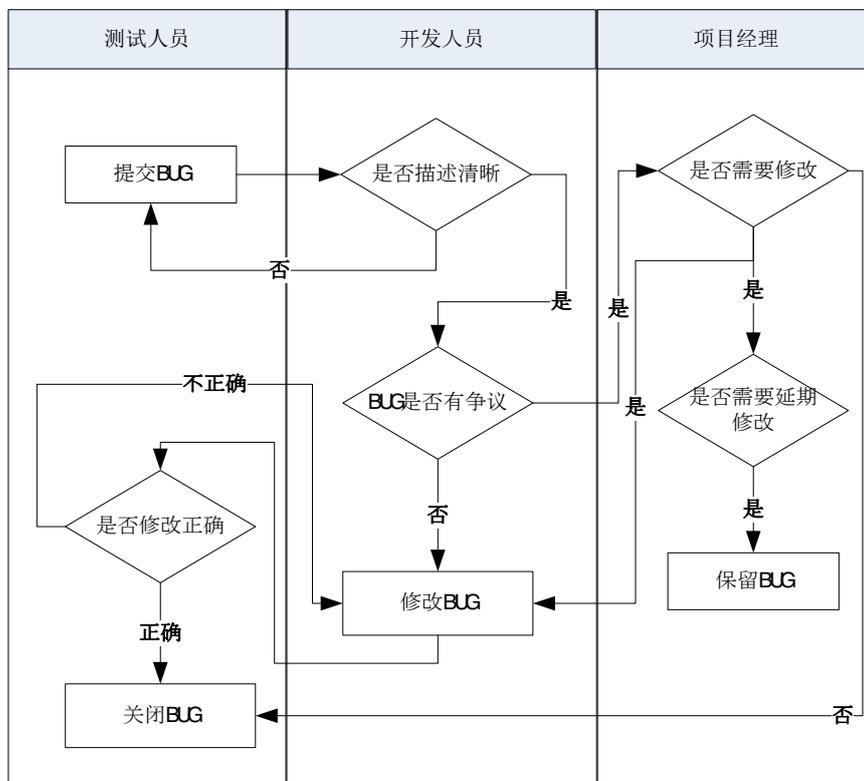
缺陷是指在软件开发过程中的针对软件产品和开发过程中的问题，这些问题已经影响或可能会影响软件产品的质量。

缺陷应该具备以下属性，也就是往缺陷管理库或者缺陷列表中提交的缺陷应该具备以下属性：

属性名称	描述
缺陷标识	标记某个缺陷的一组符号，每个缺陷必须有一个唯一的标识
缺陷类型	根据缺陷的自然属性划分的缺陷种类
缺陷验证程度	因缺陷引起的故障对软件产品的影响程度
缺陷所处的模块或子系统	缺陷分步的模块或子系统
缺陷出现几率	指发现错误的几率

缺陷的重现步骤	详细的缺陷重现步骤
附件	与缺陷相关的附件（截图、附件、用例等）
备注	对缺陷的其他描述

## ● 缺陷管理流程



### 1. 提交缺陷

测试人员将缺陷填写到管理工具中，选择指派人为开发组长或相应的开发人员。

### 2. 分配缺陷

开发人员分别对自己收到的缺陷进行评审。评审后如果对提交的缺陷有疑问，可以与提交人协商。对未能达成一致的缺陷由项目经理组织项目

组成员评审。评审人员可以是项目组人员。

如果缺陷初次分配的开发人员无法修改该缺陷，初次分配的开发人员可以将缺陷再次分配给其他开发人员。但为避免缺陷被多次分配，项目经理应跟踪 3 天以上未修改的缺陷。

### 3. 修改缺陷

开发人员对已确认的缺陷进行修改，填写修改记录，修改缺陷状态为“已修改”或其他状态。

### 4. 关闭缺陷

测试人员对已修改的缺陷进行验证。如果已修改完成，测试人员将缺陷状态设置为关闭。如果没有修改或引起回归问题，将修改缺陷状态为“重新开启”或新增缺陷，由开发工程师继续修改。

### 5. 保留缺陷

对于有争议的缺陷进行，将有项目经理最终决定是否修改。如果缺陷是由于技术原因、版本原因不能修改，则保留该缺陷。

## ● 缺陷分类

根据缺陷的定义，将缺陷分为如下列：

文档缺陷：是指对文档的静态检查过程中发现的缺陷。检查活动包括同行评审、产品审计等。评审的缺陷要根据被评审对象的类型来确定，被评审的对象包括最终出产物和中间过程产出物，比如需求文档、设计文档、计划、报告、用例等

缺陷分类	描述
------	----

描述不完整	文档内容缺失，或文档应该包括的范围没有涵盖
不一致	一致性问题有两类： 一是与源头说明书不一致，比如需求和客户业务需求不一致、设计与需求不一致等 二是上下文或者与前提不一致
描述错误	文档描述是错误的，不可实现或导致错误的输出或结果
功能问题	该缺陷将会导致用户功能的错误、不满足、不可用
不清楚或有歧义	内容的描述不清楚、不能准确表达、或表达的意思有歧义
逻辑错误	内容组织逻辑不清楚、逻辑错误
接口问题	与最终用户接口问题、与外部系统的接口问题、内部子系统或模块的接口问题
输入输出问题	输入输出不完整、不正确、不可测试或验证
不细化	内容还需要进一步细化
性能问题	文档的设计或实现方式存在性能问题
安全性问题	文档的设计或实现方式存在安全性问题

代码缺陷：是指对代码进行同行评审、审计或代码走查过程中发现的缺陷

缺陷分类	描述
------	----

常量变量定义问题	
不满足设计或需求	
编写代码不符合规范	
条件判断处理	
循环处理错误	
异常处理	
算法逻辑问题	
注释问题	
代码冗余	
性能问题	

测试缺陷：是指由测试活动发现的测试对象（被测对象一般是指可运行的代码、系统，不包括静态测试发现的问题）的缺陷，测试活动包括单元测试、集成测试、系统测试、性能测试等

过程缺陷：有称为不符合项问题，是指通过过程审计、过程分析、管理评审、质量评估、质量审核等活动发现的关于过程的缺陷和问题。过程缺陷的发现者一般是测试人员、项目经理等

缺陷类型	描述
功能错误	影响了重要的特性、用户界面、产品接口或全局数据结构，并且设计文档需要争取的变更。如逻辑、循环、递归、功能等缺陷
结构错误	Web 应用程序结构化页面无法显示，或者显示错误

脚本错误	Web 应用程序当中出现脚本错误，包括客户端对数据进行校验和运算的各种情况下产生的错误
页面链接错误	Web 应用程序页面出现空链接、错误链接、死链接
页面文字错误	Web 应用程序页面出现的中外文拼写、使用、以及不同语种页面的编码错误
页面图形错误	Web 应用程序页面出现图片内容使用不当，或者无法显示
ALT 错误	Web 应用程序页面当中超文本标识语言、文本标签解释错误
排版错误	Web 应用程序页面排版不符合要求或者不符合使用习惯
业务逻辑不合理	应用程序的实现流程和规定业务流程不一致，或者实现流程无法正确完成。包括流程数据的部分并行、争用、同步等操作，引起的流程断裂、死锁、以及其他异常情况
业务逻辑不方便	应用程序实现流程在实际情况下虽然可以完成，但是存在不必要的反复、等待、冗余等影响使用效率的情况
其他错误	其他未分类错误
建议	系统改进建议

## ● 缺陷定义

### 缺陷等级定义

缺陷的严重程度对以上所述的缺陷类型都是适合的，缺陷的严重程度反映的是对缺陷的发现对象可能造成的影响或后果来定义的。

缺陷等级	缺陷性质	系统中对应的错误分类	描述
一级	致命错误	系统崩溃系统死锁	导致对被描述的主要对象的理解错误、不可行、不可运转、对业务和整个系统造成重大损失或损害；对使用、维护或保管人员有危险或不安全，以及对产品的基本功能有致命影响的缺陷
二级	严重缺陷	严重错误	对被描述的部分对象的理解或实现错误，部分的模块或系统不可行或不能运转或部分模块和系统缺失，对整个系统有重大影响或可能造成部分的损失或损害；严重影响使用安全
三级	一般缺陷	次要错误布局不合理文字错误	系统中部分单元模块或单个功能描述和实现有错误、有偏差、不一致或有缺失，不影响模块的正常运行，或有影响，但可以有替代的办法

			或避免办法
四级	微小缺陷	微不足道	基本不影响系统的运行和功能的实现。但是与标准、规范和定义不一致
五级	建议缺陷	新特性	不在定义、标准、范围的定义和约束之内,但是从提出者来看是需要完善的建议

#### 缺陷优先级定义

缺陷优先级	描述
特急	需要立刻进行修改
加急	一天到两天之内必须修改
高	介于中和加急之间
中	缺陷需要正常排队等待修复或列入软件发布清单
低	留到组后解决, 如果项目的进度跟紧张可以在产品发布以前不解决

#### 缺陷状态定义

缺陷状态	描述
初始状态 (New)	测试或开发人员提交一个新的缺陷, 等待开发人员或项目经理分配修改负责人
打回 (FeedBack)	要求缺陷的报告者再次对缺陷进行说明
已分配 (Assigned)	是指已经分配给属主, 等待修改。

已解决 (Resolved)	缺陷被属主修改，等待测试人员验证
关闭 (Closed)	测试人员验证缺陷已经修复
重新打开 (Reopen)	测试人员验证，缺陷没有修改正确
遗留 (Later)	经项目经理和技术经理验证此缺陷在本版本中不用修改

### 缺陷完成度

缺陷完成度	描述
打开 (Open)	缺陷没有被解决
已解决 (Fixed)	缺陷已经修改
遗留 (Suspended)	此缺陷步骤本阶段解决
重新打开 (Reopen)	重新打开某个缺陷
不做修改 (Won't fix)	不对这个缺陷进行修改
重复 (Duplicate)	与某个缺陷重复
需求如此	经理和开发人员经过需求和设计的核实后决定不需要修改
不可重现	被指派的开发人员想要再现缺陷进行修改的时候，发现缺陷始终不能再现

- 处理机制

#### 退回机制

若在测试过程中发生如下情况，将系统退回到申请部门：

(1) 经过测试后，发现与需求说明规格说明书中定义的功能项存在较大的差异。

(2) 单一模块，测试过程中发现缺陷输了较多或者无法继续进行系统其它功能模块的测试，继续测试无意义。

(3) 测试过程中，频繁死机或系统崩溃主业务流程出现断点异常情况处理机制非正常情况下，需要进行特别处理的情形，此情况需要主管领导签字确认：

上线时间紧急的情况下，未经测试部充分测试就需要部署到用户现场作为总包时，子商进度明显延迟，尚未进行验收测试就需要上线报告机制

若出现以下情况，需要及时向部门领导和项目经理汇报的情况：

- (1) 测试后期出现重大逻辑错误，修改测试影响上线时间
- (2) 测试过程中用户需求出现重大变更
- (3) 测试负责人定期汇报测试情况

## ● 测试结果分析

## ● 测试完成的标准

被测试出的、在软件错误级别分类中定义的：

- 一级缺陷，致命错误，100%得到修改并且复测通过
- 二级缺陷，严重错误，100%得到修改并且复测通过
- 三级缺陷，较大错误，100%得到修改并且复测通过

- 四级缺陷，一般错误，95%得到修改并且复测通过
- 五级缺陷，轻微错误，95%得到修改并且复测通过
- 允许保留的缺陷

测试超过了预定时间表，由项目经理决定是否停止测试

测试结论及评价标准

测试结论	评价标准
拒绝发布	遗留了一级、二级缺陷
测试通过版本	不能遗留以一、二类缺陷 三类一般缺陷 95%得到修改并且通过复测 四类轻微缺陷 85%得到修改并且通过复测
推荐使用版本	不能遗留以一、二类缺陷 三类一般缺陷 95%得到修改并且通过复测 四类轻微缺陷 90%得到修改并且通过复测
可以证实发布版本	不能遗留以一、二类缺陷 三类一般缺陷 97%得到修改并且通过复测 四类轻微缺陷 90%得到修改并且通过复测

测试结果分析是对测试结果的一个综合评估，主要描述有测试中各个等级的缺陷数量，缺陷分布情况，缺陷修改情况、回归测试提交缺陷数量，性能测试指标情况。

测试报告由测试组长编写并提交给项目经理。测试报告需要经项目组评审通过。

## ● 测试输出文档

测试工作完成之后，开发测试小组将出具以下文档作为交付物：

- 软件系统测试计划(方案)
- 系统测试用例
- 系统测试过程（缺陷跟踪与管理）
- 测试脚本（可选）用于回归测试、性能测试
- 系统测试报告
- 性能测试报告

## ● 系统集成方案

### ● 集成原则

能够清晰描述第三方业务系统的主体功能，详述集成场景中的数据流程，形成集成概要设计，尽可能减少现有系统改造工作量和降低对现有系统稳定性影响。

### ● 系统集成概述

#### 1. 系统集成概念

所谓系统集成，就是通过结构化的综合对接系统和计算机网络技术，将各个分离的软件、硬件、功能和信息等集成到相互关联的、统一和协调的系统之中，使资源达到充分共享，实现集中、高效、便利的管理。

系统集成应采用功能集成、网络集成、软件界面集成等多种集成技术。系统集成实现的关键在于解决系统之间的互连和互操作性问题，它是一个

多厂商、多协议和面向各种应用的体系结构。这需要解决各类设备、子系统间的接口、协议、系统平台、应用软件等与子系统、建筑环境、施工配合、组织管理和人员配备相关的一切面向集成的问题。系统集成作为一种新兴的服务方式，是近年来国际信息服务业中发展势头最猛的一个行业。系统集成的本质就是最优化的综合统筹设计，一个大型的综合计算机网络系统，系统集成包括软件、硬件、操作系统技术、数据库技术、网络通讯技术等的集成，以及不同厂家产品选型，搭配的集成，系统集成所要达到的目标整体性能最优，即所有部件和成分合在一起后不但能工作，而且全系统是低成本的、高效率的、性能匀称的、可扩充性和可维护的系统。

广义上讲，系统集成包括人员的集成、组织机构的集成、设备的集成、系统软件的集成、应用软件的集成和管理方法的集成等多方面的工作。狭义上讲，系统集成就是系统平台的集成。系统集成应用功能集成、网络集成、软件界面集成等多种集成技术。系统集成实现的关键在于解决系统之间的互联和互操作性问题，它是一个多厂商、多协议和面向各种应用的体系结构。这需要解决各类设备、子系统间的接口、协议、系统平台、应用软件等与子系统、建筑环境施工配合、组织管理和人员配备相关的一切面向集成的问题。

## 2. 系统集成特点

[1]系统集成要以满足用户对需求为根本出发点。

[2]系统集成不是选择最好的产品的简单行为，而是要选择最适合用户的需求和投资规模的产品和技术。

[3]系统集成不是简单的设备供货，它体现更多的是设计，调试与开

发，是技术含量很高的行为。

[4]系统集成包含技术，管理和商务等方面，是一项综合性的系统工程。技术是系统集成工作的核心，管理和商务活动是系统集成项目成功实施的可靠保障。

[5]性能价格比的高低是评价一个系统集成项目设计是否合理和实施成功的重要参考因素。

### 3. 典型的系统集成技术

#### (1) 数据库与数据仓库技术

传统的数据库以单一的数据源即数据库为中心，进行事务处理、批处理、决策分析等数据处理工作，主要有操作型处理和分析型处理两类。

操作型处理也称事务处理，指对联机数据库的日常操作，通常是对数据库中记录的查询和修改，主要为企业的特定应用服务，强调处理的响应时间、数据的安全性和完整性等；

分析型处理则用于管理人员的决策分析，经常要访问大量的历史数据。

数据仓库（DataWarehouse）是一个面向主题的、集成的、相对稳定的、反映历史变化的数据集合，用于支持管理决策。可从两个层面理解数据仓库：

首先数据仓库用于决策支持，面向分析型数据处理，不同于企业现有的操作型数据库；

其次数据仓库是对多个异构数据源的有效集成，集成后按主题重组，且放在数据仓库中的数据一般不再修改。

数据仓库系统结构包含四个层次：

- 数据源，数据仓库系统的基础；
- 数据的存储与管理，核心；
- 联机分析处理（OLAP），服务器对分析需要的数据进行有效集成，按多维模型组织，以便进行多角度、多层次的分析并发现趋势；
- 前端工具。

## （2）WEBServices 技术

web 服务定义了一种松散的、粗粒度的分布式计算模式，使用标准的 HTTP(S) 协议传送 XML 表示和封装的内容；

webservices 技术使得运行在不同机器上的不同应用无需借助附加的、专门的第三方软件或硬件，可相互交换数据或集成。根据 webservices 服务规范来实施的应用与应用之间无论它们使用什么语言、平台或者内部协议，都可以互相交换数据。

XML，可拓展性标记语言，类似 HTML，设计宗旨是传输数据，而非显示数据；XML 标签没有被预定义，需要自行定义，是 W3C 的推荐标准。

## 4. JavaEE

JavaEE（JavaPlatformEnterpriseEdition）即 Java 的平台企业版，是 Sun 公司为企业级应用推出的标准平台，用来开发 B/S 架构软件，JavaEE 是一个框架，也可以说是一种规范。

## 5. .NET 架构

.NET 是微软新一代技术平台，为敏捷商务构建互联互通的应用系统。它的执行机制与很多编程语言都不同，先将高级语言（C#、VB）编译成为

中间语言（IL），然后在编译为机器语言。

## 6. 软件引擎技术

软件引擎通常是系统的核心组件，目的是封装某些过程方法，使得在开发的时候不需要过多关注具体实现，从而可以将关注点聚焦在与业务的结合上。

## 7. 组件在系统集成项目中的重要性

组件是实现了某些功能的、有输入输出接口的黑盒子，它将一些人们所关心的，但不便让最终用户去直接操作的细节进行封装，同时实现各种业务逻辑规则，用于处理用户的内部操作细节。

常用的组件标准有：微软的 COM/DCOM/COM+、OMG 的 CORBA、Java 的 RMI/EJB。

## ● 系统集成原则

根据目前计算机网络现状和需求分析以及未来的发展趋势，系统设计应该遵循以下几个原则。

### 1. 开放性和标准化原则

首先采用国家标准和国际标准，其次采用广为流行的、实用的工业标准。只有这样，系统内部才能方便地从外部网络快速获取信息，同时还要授权后，保证网络系统适度的开放性。在进行系统设计时，在有标准可执行的情况下，一定要严格按照相应的标准进行设计。采用开放的标准，就可以充分保障物流系统设计的延续性，即使将来最初设计人员不在现场，后来人员也可以通过标准轻松地了解整个网络系统的设计，保证互连

简单易行。

## 2. 实用性与先进性兼顾原则

在系统设计时应该以注重实用为原则，紧密结合具体应用的实际需求。在选择具体的网络技术时，要同时考虑当前及未来一段时间内主流应用的技术，不要一味地追求新技术和新产品。

一方面新的技术和产品还有一个成熟的过程，立即选用新的技术和产品，可能会出现各种意想不到的问题；

另一方面，最新技术的产品价格肯定非常昂贵，会造成不必要的资金浪费。另外一定要选择主流应用的技术。

## 3. 可用性原则

服务器的“四性”之一是“可用性”，系统集成也一样需要遵循。它决定了所设计的系统是否能满足用户应用和稳定运行的需求。系统集成的“可用性”主要体现在系统的“可靠性和稳定性”，这要求系统能长时间稳定运行，而不能经常出现这样或者那样的问题，否则会给用户带来的损失可能是非常巨大的

## 4. 安全性原则

系统集成安全涉及许多方面，最明显、最重要的就是对外界入侵、攻击和检查与防护。现在的网络几乎无时无刻不受到外界的安全威胁，稍有不慎就会被病毒感染、黑客入侵，致使整个网络陷入瘫痪。在一个安全措施完善的计算机网络中，不但部署了病毒防护系统、防火墙隔离系统，还可能部署了入侵检测、木马查杀系统、物理隔离系统等，所选用系统的等级要根据相应网络规模大小和安全需要而定，并不一定要求每个网络系统

都全面部署这些防护系统。

除了病毒、黑客入侵外，系统集成的安全性需求还体现在用户对数据的访问权限上。根据对应的工作需求为不同用户、不同数据配置相应的访问权限，对安全级别需求较高的数据则要采取相应的加密措施。同时，对用户账户，特别是高权限账户的安全更要高度重视，要采取相应的账户防护策略（如密码复杂性策略、账户锁定策略等），保护好用户账户，以防被非法用户盗取。

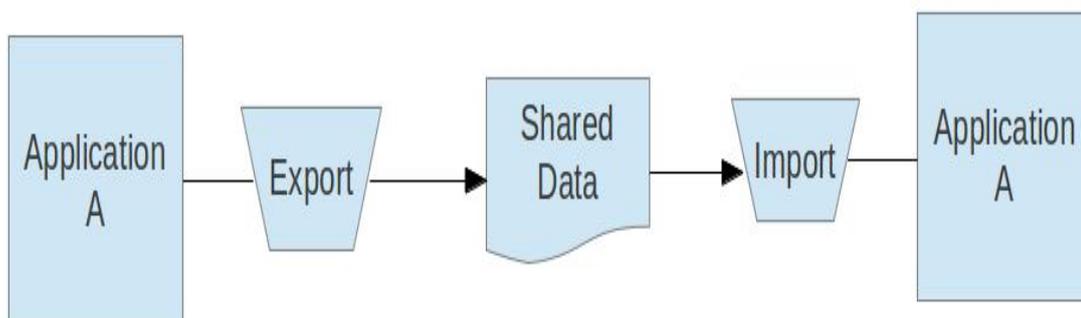
安全性防护的另外一个重要方面就是数据备份和容灾处理。数据备份和容灾处理，在一定程度上决定了企业的生存与发展，特别是以电子文档为主的电子商务类企业数据。

在设计系统集成时，一定要充分考虑到为用户数据备份和容灾部署相应级别的备份和容灾方案。

## ● 系统集成方法

### （1）文件传输（共享）

文件共享传输的方式是一种简单直观的办法。它的典型交互场景如下：



在这种场景下，XX 项目物流系统产生包含需要提供信息的文件，然后

再由相关集成系统来通过访问文件获取信息。集成部分主要作用是将文件根据应用的不同需要做格式的转换。

采用文件传输的方式，需要关注文件的格式，考虑到不同应用系统传递消息的具体样式不一致，XX 项目物流系统应用产生的文件不一定能够给相关集成应用。一些常见的方法是传递 XML 或者 JSON 格式的文本，在一些 UNIX 系统里面也可以通过纯 TXT 文本传递信息的。

文件共享传输方式的缺点：

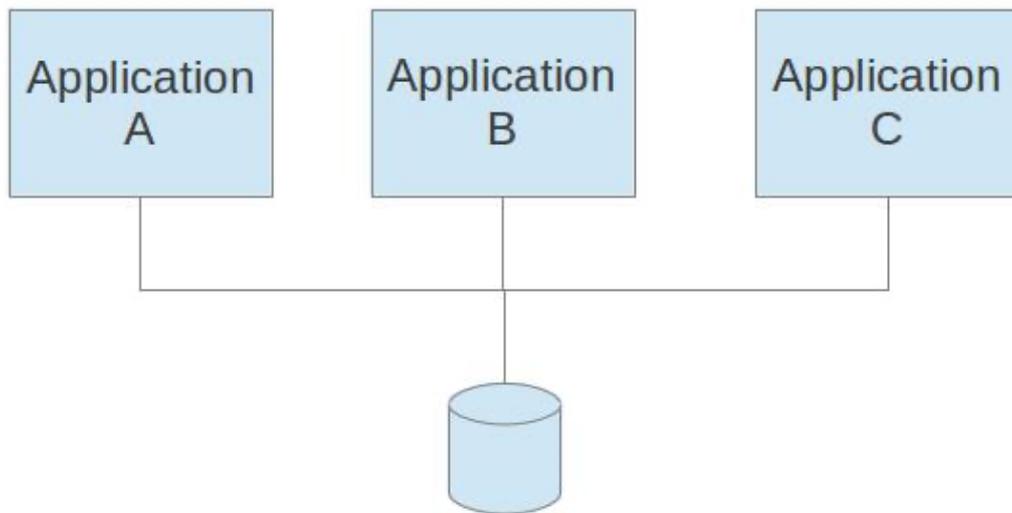
- 1、无法避免物流系统与其他系统同时修改该文件，即在物流应用产生文件的时候无法保证集成应用不去修改；
- 2、通信问题，即文件产生后怎么通知集成应用的问题；
- 3、集成系统之间信息不同步。

文件共享传输方式的优势：

- 1、在信息交换不是很频繁，而且对于信息的及时性要求不太高的情况下，文件传输方式简单直接。
- 2、可以采用一些 timerjob 的方式来产生和消费文件。保证两者不产生冲突和他们正确的执行顺序。
- 3、对于集成的系统来说它比较完美的屏蔽了集成的细节。每个系统只要关注符合标准格式的文件内容，具体实现和数据交换他们都不需要关心。

## (2) 共享数据库

将数据库作为相对独立提供服务的一部分。对于其他集成系统的对接比较容易，这种集成的方式如下图：



共享数据库的优势：

可以保证数据的一致性。共享数据库里所有的数据都是统一存储在公共的数据库里，可以保证数据的同步和一致性。对于任何一个系统产生的数据或者变化，另外一个系统马上可以看到。

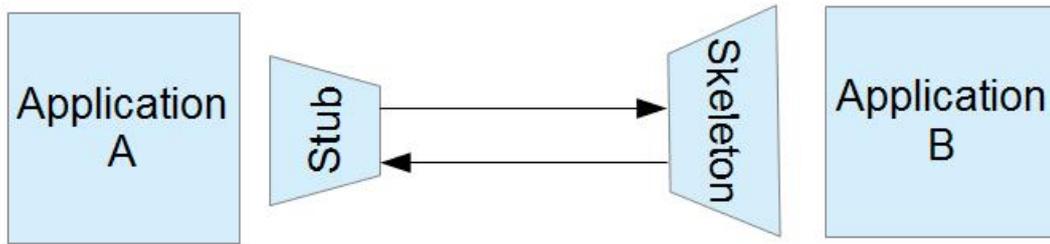
共享数据库的缺点：

1、对于多个应用来说，这个共享数据库需要能够适应他们所有的场景。不同的应用考量的点是不一样的，要能适应所有的需求对于数据库这一部分就显得尤其的困难。

2、性能方面。不同的应用可能会同时访问相同的数据导致数据访问冲突，因此也会带来如死锁等问题。所以说，共享数据库方案出现问题的根源在于用一种统一的数据模型来解决各种不同的应用需求是并不现实的。

### (3) RPC（远程过程调用）

远程过程调用的方法典型的如 Java 的 RMI。典型的应用场景如下：

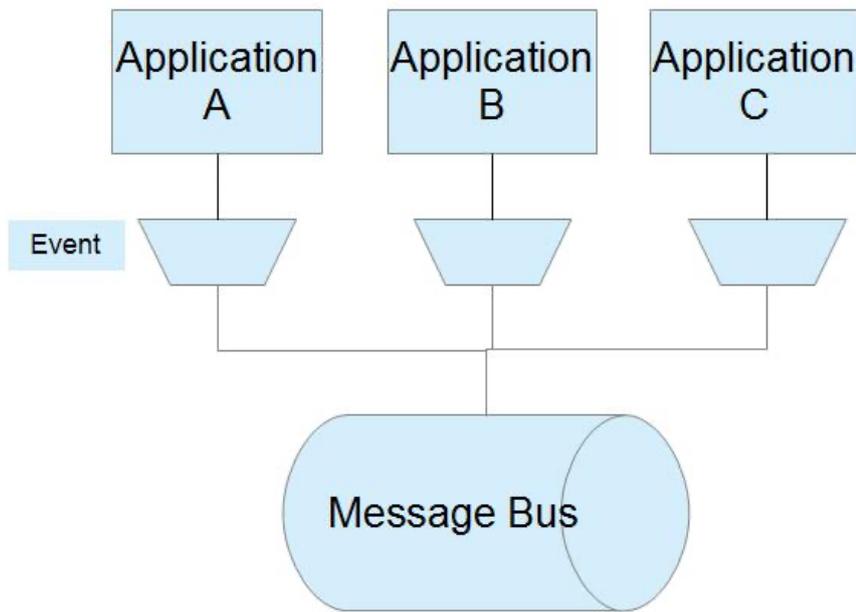


以典型的 javaRMI 为例，当需要访问远程方法的时候，需要定义访问的接口，然后通过相关工具生成 skeleton 和 stub。然后一端通过 stub 给另外一端发送消息。在物流系统本地的代码中访问 stub 看起来还是和调用本地方法一样，这些细节都由 stub 给屏蔽了。其他的技术如 COM，CORBA，.netRemoting 都采用了 RPC 的思路。RPC 的这种思路能够很好的集成应用开发。

RPC 机制也会带来一定的问题，比如说 javaRMI 或者.netremoting 都局限于一个平台，如果物流系统是用 java 做的，那么要和相关系统通过 RMI 集成，对应系统也必须是 java 做的。另外，集成系统间是一种紧耦合。RPC 调用是用的一种类似于系统 api 的同步调用，当一端发出调用请求的时候会在那里等待返回的结果。如果另外一个系统出现故障也会对调用方产生很大影响。而且用 RPC 调用的时候默认期望消息是按照发送的顺序给接收方的。但是由于各种环境的影响会使得接收的结果乱序，这样也可能导致系统执行出现问题。所以从可靠性来说还是存在着一定的不足。

#### (4) 消息队列

消息队列的集成方式如下图：



所有应用之间要通信的消息都通过消息队列来传输，由消息队列来保证数据传输的异步性、稳定性等。总的来说，所有数据通过一条可靠的链路来进行通信。

#### 消息队列集成方式的特征

- 更好的应用解耦

采用文件传输或者共享数据库的方式需要知道文件或者数据库的位置。对于 RPC 的方式来说需要知道对方的 IP 地址才能进行方法调用。且开发运行平台也有依赖。消息队列则是双方规定好通信的消息格式，各自都只要发消息给消息队列就可以了。可以保证不同开发语言开发的系统之间的通信。

- 消息的可靠性

所有系统之间提交的消息有消息队列里的 messengerouter 来投递。根据一个发送方指定的地址并转发到另外一个地方。同时，消息队列也根据不同的需要将消息进行持久化，这样保证消息在投递的过程中不会被丢

失。

- 系统可靠性

集成系统中有一方出现故障，不影响系统之间的通信，保证了有效信息的传递。保证了系统的异步执行，从某种角度来说也提升了系统性能。消息队列算是一种兼顾了性能、可靠性和松耦合的一种理想集成方式。目前实现消息队列的产品有很多，比如微软的 MSMQ，开源产品 ActiveMQ，RabbitMQ，ZeroMQ 等。

#### (5) 系统接口标准

采用 SOA 体系架构，通过服务总线技术实现数据交换以及实现各业务子系统间、外部业务系统之间的信息共享和集成，因此 SOA 体系标准就是我们采用的接口核心标准。

主要包括：

##### [1] 服务目录标准

服务目录 API 接口格式参考国家以及关于服务目录的元数据指导规范，对于 W3CUDDIv2API 结构规范，采取 UDDIv2 的 API 的模型，定义 UDDI 的查询和发布服务接口，定制基于 Java 和 SOAP 的访问接口。

除了基于 SOAP1.2 的 Webservice 接口方式，对于基于消息的接口采用 JMS 或者 MQ 的方式。

##### [2] 交换标准

基于服务的交换，采用 HTTP/HTTPS 作为传输协议，而其消息体存放基于 SOAP1.2 协议的 SOAP 消息格式。

SOAP 的消息体包括服务数据以及服务操作，服务数据和服务操作采用

WSDL 进行描述。

### [3]Web 服务标准

用 WSDL 描述业务服务，将 WSDL 发布到 UDDI 用以设计/创建服务，SOAP/HTTP 服务遵循 WS-IBasicProfile1.0，利用 J2EESessionEJBs 实现新的业务服务，根据需求提供 SOAP/HTTPorJMSandRMI/IIOP 接口。

### [4]业务流程标准

使用没有扩展的标准的 BPEL4WS，对于业务流程以 SOAP 服务形式进行访问，业务流程之间的调用通过 SOAP。

### [5]数据交换安全

与外部系统对接需考虑外部访问的安全性，通过 IP 白名单、SSL 认证等方式保证集成互访的合法性与安全性。

### [6]数据交换标准

制定适合双方系统统一的数据交换数据标准，支持对增量的数据自动进行数据同步，避免人工重复录入的工作。

### (6)接口规范性设计

项目接口众多，依赖关系复杂，通过接口交换的数据与接口调用必须遵循统一的接口模型进行设计。接口模型除了遵循工程统一的数据标准和接口规范标准，实现接口规范定义的功能外，需要从数据管理、完整性管理、接口安全、接口的访问效率、性能以及可扩展性多个方面设计接口规格。

### (7) 接口定义约定

客户端与系统平台以及系统平台间的接口消息协议采用基于 HTTP 协

议的 REST 风格接口实现，协议栈如图所示：

业务消息
会话数据
HTTP/HTTPS
TCP/IP
底层承载

系统在 http 协议中传输的应用数据采用具有自解释、自包含特征的 JSON 数据格式，通过配置数据对象的序列化和反序列化的实现组件来实现通信数据包的编码和解码。

在接口协议中，包含接口的版本信息，通过协议版本约束服务功能规范，支持服务平台间接口协作的升级和扩展。一个服务提供者可通过版本区别同时支持多个版本的客户端，从而使得组件服务的提供者和使用者的根据实际的需要，独立演进，降低系统升级的复杂度，保证系统具备灵活的扩展和持续演进的能力。

#### (8) 业务消息约定

请求消息 URI 中的参数采用 UTF-8 编码并经过 URLEncode 编码。

应答消息根节点为“response”，每个响应包含固定的两个属性节点：“status”和“message”。它们分别表示操作的返回值和返回消息描述，其他的同级子节点为业务返回对象属性，根据业务类型的不同，有不同的属性名称。

当客户端支持数据压缩传输时，需要在请求的消息头的“Accept-Encoding”字段中指定压缩方式(gzip)，如消息可以被压缩传输则平台将应答的数据报文进行压缩作为应答数据返回，Content-Length为压缩后的数据长度。

#### (9) 响应码规则约定

响应结果码在响应消息的“status”属性中，相应的解释信息在响应消息的“message”属性中。解释消息为终端用户可读的消息，终端应用不需要解析可直接呈现给最终用户。响应结果码为6位数字串。根据响应类型，包括以下几类响应码。

- 0：成功；
- 1XXXXX：系统错误；
- 2XXXXX：输入参数不合法错误；
- 3XXXXX：应用级返回码，定义应用级的异常返回；
- 4XXXXX 正常的应用级返回码，定义特定场景的应用级返回说明。

#### (10) 数据管理

##### 1、业务数据检查

接口应提供业务数据检查功能，即对接收的数据进行合法性检查，对非法数据和错误数据则拒绝接收，以防止外来数据非法入侵，减轻应用支撑平台系统主机处理负荷。

对于接口，其业务数据检查的主要内容有以下几个方面：

- 数据格式的合法性：如接收到非预期格式的数据。包括接收的数据长度，类型，开始结束标志等。

- 数据来源的合法性：如接收到非授权接口的数据。

- 业务类型的合法性：如接收到接口指定业务类型外的接入请求。

- 对于业务数据检查中解析出非法数据应提供以下几种处理方式：

- 事件报警：在出现异常情况时自动报警，以便系统管理员及时进行处理。

- 分析原因：在出现异常情况时，可自动分析其出错原因。如是数据来源非法和业务类型非法，本地记录并做后续管理，如是数据格式非法，分析网络传输原因或对端数据处理原因，并做相应处理。

- 统计分析：定期对所有的非法记录做统计分析，分析非法数据的各种来源是否具有恶意，并做相应处理。

## 2、数据压缩/解压

接口根据具体的需求应提供数据压缩/解压功能，以减轻网络传输压力，提高传输效率，从而使整个系统能够快速响应并发请求，高效率运行。

在使用数据压缩/解压功能时，应具体分析每一类业务的传输过程、处理过程、传输的网络介质、处理的主机系统和该类业务的并发量、峰值及对于所有业务的比例关系等，从而确定该类业务是否需要压缩/解压处理。对于传输文件的业务，必须压缩后传输，以减轻网络压力，提高传输速度。

在接口中所使用的压缩工具必须基于通用无损压缩技术，压缩算法的

模型和编码必须符合标准且高效，压缩算法的工具函数必须是面向流的函数，并且提供校验检查功能。

### (11) 完整性管理

根据业务处理和接口服务的特点，应用系统的业务主要为实时请求业务和批量传输业务。两类业务的特点分别如下：

#### 1、实时请求业务：

- [1]采用基于事务处理机制实现
- [2]业务传输以数据包的方式进行
- [3]对传输和处理的实时性要求很高
- [4]对数据的一致性和完整性有很高的要求
- [5]应保证高效地处理大量并发的请求

#### 2、批量传输业务：

- [1]业务传输主要是数据文件的形式
- [2]业务接收点可并发处理大量传输，可适应高峰期的传输和处理
- [3]要求传输的可靠性高

根据上述特点，完整性管理对于实时交易业务，要保证交易的完整性；对于批量传输业务，要保证数据传输的完整性。

### (12) 接口双方责任

1、消息发送方：遵循本接口规范中规定的验证规则，对接口数据提供相关的验证功能，保证数据的完整性、准确性；消息发起的平台支持超时重发机制，重发次数和重发间隔可配置。提供接口元数据信息，包括接口数据结构、实体间依赖关系、计算关系、关联关系及接口数据传输过程中的各类管理规则等信息；提供对敏感数据的加密功能；及时解决接口数据提供过程中数据提供方一侧出现的问题；

2、消息响应方：遵循本接口规范中规定的验证规则，对接收的数据进行验证，保证数据的完整性、准确性。

及时按照消息发送方提供的变更说明进行本系统的相关改造。

及时响应并解决接口数据接收过程中出现的问题。

3、异常处理：对接口流程调用过程中发生的异常情况，如流程异常、数据异常、会话传输异常、重发异常等，进行相应的异常处理，包括：

- 对产生异常的记录生成异常记录文件。
- 针对可以回收处理的异常记录，进行自动或者人工的回收处理。
- 记录有关异常事件的日志，包含异常类别、发生时间、异常描述等信息。
- 当接口调用异常时，根据预先配置的规则进行相关异常处理，并进行自动告警。

### (13) 接口的可扩展性规划与设计

各个系统间的通信接口版本信息限定了各个系统平台间交互的数据

协议类型、特定版本发布的系统接口功能特征、特定功能的访问参数等接口规格。通过接口协议的版本划分，为客户端升级、其他被集成系统的升级、以及系统的部署提供了较高的自由度和灵活性。

系统可根据接口请求中包含的接口协议版本实现对接口的向下兼容。系统平台可根据系统的集群策略，按协议版本分别部署，也可多版本并存部署。由于系统平台可同时支持多版本的外部系统及客户端应用访问系统，特别是新版本客户端发布时，不要求用户强制升级，也可降低强制升级安装包发布的几率。从而支持系统的客户端与系统平台分离的持续演进。

#### (14) 接口安全性设计

为了保证系统平台的安全运行，各种集成的外部系统都应该保证其接入的安全性。接口的安全是平台系统安全的一个重要组成部分。保证接口的自身安全，通过接口实现技术上的安全控制，做到对安全事件的“可知、可控、可预测”，是实现系统安全的一个重要基础。根据接口连接特点与业务特色，制定专门的安全技术实施策略，保证接口的数据传输和数据处理的安全性。

系统应在接口的接入点的网络边界实施接口安全控制。接口的安全控制在逻辑上包括：安全评估、访问控制、入侵检测、口令认证、安全审计、防(毒)恶意代码、加密等内容。

##### 1、安全评估

安全管理人员利用网络扫描器定期(每周)/不定期(当发现新的安全

漏洞时)地进行接口的漏洞扫描与风险评估。

扫描对象包括接口通信服务器本身以及与之关联的交换机、防火墙等，要求通过扫描器的扫描和评估，发现能被入侵者利用的网络漏洞，并给出检测到漏洞的全面信息，包括位置、详细描述和建议改进方案，以便及时完善安全策略，降低安全风险。

安全管理人员利用系统扫描器对接口通信服务器操作系统定期(每周)/不定期(当发现新的安全漏洞时)地进行安全漏洞扫描和风险评估。在接口通信服务器操作系统上，通过依附于服务器上的扫描器代理侦测服务器内部的漏洞，包括缺少安全补丁、词典中可猜中的口令、不适当的用户权限、不正确的系统登录权限、操作系统内部是否有黑客程序驻留，安全服务配置等。系统扫描器的应用除了实现操作系统级的安全扫描和风险评估之外还需要实现文件基线控制。

接口的配置文件包括接口服务间相互协调作业的配置文件、系统平台与接口对端系统之间协调作业的配置文件，对接口服务应用的配置文件进行严格控制，并且配置文件中不应出现口令明文，对系统权限配置限制到能满足要求的最小权限，关键配置文件加密保存。为了防止对配置文件的非法修改或删除，要求对配置文件进行文件级的基线控制。

## 2、访问控制

访问控制主要通过防火墙控制接口对端系统与应用支撑平台之间的相互访问，避免系统间非正常访问，保证接口交互信息的可用性、完整性和保密性。访问控制除了保证接口本身的安全之外，还进一步保证应用支

撑平台的安全。

为了有效抵御威胁，应采用异构的双防火墙结构，提高对防火墙安全访问控制机制的破坏难度。双防火墙在选型上采用异构方式，即采用不同生产厂家不同品牌的完全异构防火墙。同时，双防火墙中的至少一个应具有与实时入侵检测系统可进行互动的能力。当发生攻击事件或不正当访问时，实时入侵检测系统检测到相关信息，及时通知防火墙，防火墙能够自动进行动态配置，在定义的时间段内自动阻断源地址的正常访问。

系统对接口被集成系统只开放应用定义的特定端口。

采用防火墙的地址翻译功能，隐藏系统内部网络，向代理系统提供翻译后的接口通信服务器地址及端口，禁止接口对端系统对其它地址及端口的访问。

对通过/未通过防火墙的所有访问记录日志。

### 3、入侵检测

接口安全机制应具有入侵检测(IDS)功能，实时监控可疑连接和非法访问等安全事件。一旦发现对网络或主机的入侵行为，应报警并采取相应安全措施，包括自动阻断通信连接或者执行用户自定义的安全策略。

实施基于网络和主机的入侵检测。检测攻击行为和非法访问行为，自动中断其连接，并通知防火墙在指定时间段内阻断源地址的访问，记录日志并按不同级别报警，对重要系统文件实施自动恢复策略。

### 4、口令认证

对于需经接口安全控制系统对相关集成系统进行业务操作的请求，实行一次性口令认证。

为保证接口的自身安全，对接口通信服务器和其它设备的操作和管理要求采用强口令的认证机制，即采用动态的口令认证机制。

## 5、安全审计

为了保证接口的安全，要求对接口通信服务器的系统日志、接口应用服务器的应用日志进行实时收集、整理和统计分析，采用不同的介质存档。

## 6、防恶意代码或病毒

由于 Internet 为客户提 WEB 服务，因此，对于 Internet 接口要在网络分界点建立一个功能强大的防恶意代码系统，该系统能实时地进行基于网络的恶意代码过滤。建立集中的防恶意代码系统控制管理中心。

## 7、安全加密

为了提高接口通信信息的保密性，同时保证应用支撑平台的安全性，可以对系统平台与接口集成系统间的相关通信实施链路加密、网络加密或应用加密，保证无关人员以及无关应用不能通过网络链路监听获得关键业务信息，充分保证业务信息的安全。

- 系统集成方案
- 系统集成架构

本项目建设过程中，需要和外围系统对接实现集成服务。

1、整体开发项目采用微服务的技术架构，各微服务中心之间的接口调用采用 RPC 调用，消息传输格式为 json。

2、整体开发项目对外提供的能力，如对各销售渠道前端产品提供的商品、订单、库存等能力服务，通过 API 网关封装为 HTTP 接口，消息传输格式为 json。

3、整体开发项目也可以集成的外部第三方平台及能力，通过集成平台进行集成，由集成平台屏蔽外部接口的版本变更或不同外部平台供应商接口的差异。集成平台对外接口为 HTTP，对内根据业务场景不同，可采用 RPC、HTTP 或消息队列 MQ 等不同的接口方式。对外消息传输格式采用第三方平台的消息格式类型，如 XML 或 SOAP 等，对内消息格式尽量转换为 json。

4、跟外部第三方平台的集成根据业务场景也会采用文件传输的方式，数据提供方生成文件放入指定的文件目录，数据消费方下载文件进行处理。

5、统一工作台提供的部分页面功能由各微服务中心提供或来至 BI 数据分析，采用页面挂载方式集成，点击页面跳转至页面功能提供方，系统间通过统一工作台提供的 SSO 解决单点登录和权限控制。部分页面功能也可由统一工作台进行页面开发，微服务中心或 BI 系统提供 HTTP 接口能力。

6、整体开发项目跟 BI 系统的数据对接方式为 BI 系统通过 ETL 工具对新企业的读库进行数据抽取。

## ● 系统接口方案

## 1、接口原则

接口提供方提供接口方案，包括接口形式、传输协议及消息格式，接口调用方进行接口适配。

为便于统一监控和接口管理，原则上建议内部接口采用 RPC，外部接口采用 HTTP，对实时性要求不高或下游接口可异步处理的接口调用采用 MQ。

## 2、接口方式

### 1) 消息接口

同步请求/应答方式：客户端向服务器端发送服务请求，客户端阻塞等待服务器端返回处理结果。

异步请求/应答方式：客户端向服务器端发送服务请求，与同步方式不同的是，在此方式下，服务器端处理请求时，客户端继续运行；当服务器端处理结束时返回处理结果。

会话方式：客户端与服务器端建立连接后，可以多次发送或接收数据，同时存储信息的上下文关系。

### 2) 文件接口

### 3) 消息队列

广播通知方式：由服务器端主动向客户端以单个或批量方式发出未经客户端请求的广播或通知消息，客户端可在适当的时候检查是否收到消息并定义收到消息后所采取的动作。

事件订阅方式：客户端可事先向服务器端订阅自定义的事件，当这些事件发生时，服务器端通知客户端事件发生，客户端可采取相应处理。事

件订阅方式使客户端拥有了个性化的事件触发功能，方便客户端及时响应所订阅的事件。

### 3、消息接口消息格式

✓ json

✓ xml

✓ SOAP

以上接口消息格式尽量采用 json。

## ● 系统接口监控方案

TraceInsight 负责链路追踪，针对现有的分布式系统开发，实现了从 web 或 service 入口到数据库类中间件调用全链路记录，支持采样统计，并记录链路中各阶段的性能指标，定时发送追踪数据到数据中心供监控分析及告警。

- 追踪数据支持分模块、时间、接口与类实时查询。
- 追踪记录每次调用的依赖关系、持续事件甚至参数和异常。

应用监控提供了有关 Web 应用程序在性能方面的实时监控信息，帮助开发、运维团队快速分析程序性能瓶颈以及应用潜在的问题。应用监控总共分为“拓扑”，“web 事务”，“数据库”，“缓存”和“JVMs”五个类别，并且支持选择固定时间段查看数据统计。

通过应用的追踪数据，可以计算出应用间调用关系，应用与数据库中间件的拓扑结构，如下所示，其中 EU（EnderUser）代指用户，每个节点

代表一个应用或者数据库、中间件，连接 2 个节点的线条代指调用关系与调用次数。

web 事务展示了 Web 应用的事务详情，以接口维度展示调用明细，访问应用的 web 请求的响应时间分析，耗时前五的 API 性能趋势，总体吞吐量统计，慢事务追踪。

Web 事务明细：平均响应时间、响应时间占比、吞吐量分别展示了每个事务接口在可选的固定时间段内的平均响应时间 75%分位数、每个接口占用总体调用时间的百分比，与每个接口的每分钟调用次数。

响应时间 Top5：展示了可选的固定时间段内将调用时间 75%分位数排列后前五的事物接口与性能趋势。

吞吐量 Top5：展示了事务接口可选的固定时间段内每分钟被请求的次数与趋势的前五位。

慢事务追踪 Top10：展示了一可选的固定时间段内响应时间超过 250ms 并且排列前十的事务接口的发生次数与平均响应时间等信息。

数据库事物展示了数据库事物详情，以 Web 应用中 DAO 方法维度（mybatis）统计调用明细，耗时前五的查询性能趋势，总体吞吐量，与慢数据库追踪。

数据库明细：平均响应时间、吞吐量分别展示了一小时内（可选）每个查询方法的平均执行时间 75%分位数、每个查询的每分钟调用次数。

响应时间 Top5：展示了最近一小时内（可选）数据库查询时间 75%分

位数排列后前五的数据库事物与性能趋势。

吞吐量 Top5: 展示了最近一小时内 (可选) 每分钟被请求数据库查询排列前五位的次数与趋势。

慢数据库追踪 Top10: 慢事物列表展示了一小时内 (可选) 响应时间超过 250ms 并且排列前十的数据库请求次数与平均响应时间等信息。

缓存事务主要包括 redis 调用明细, 耗时前五的查询性能趋势, 总体吞吐量统计分析。

缓存明细: 平均响应时间、吞吐量分别展示了一小时内 (可选) 每次 redis 查询的平均执行时间 75%分位数、每个查询的每分钟调用次数。

响应时间 Top5: 展示了最近一小时内 (可选) 数据库查询时间 75%分位数排列后前五的 redis 查询与性能趋势。

吞吐量 Top5: 展示了最近一小时内 (可选) 每分钟被请求 redis 查询排列前五位的次数与趋势。

JVMs 主要包括 Web 应用的各个模块的各个 Java 容器实例状态

Heapmemoryusage: JVM 堆内存使用情况。

NonHeapmemoryusag: JVM 非堆内存使用情况。

PS-Eden-Space, PS-Old-Gen, PS-Survivor-Space: 分别表示 jvm 堆内存中伊甸园, 老年代区, 幸存者区。

GCMarkSweep, GCScavenge: 分别表示 JVMfullGC 和增量 GC 次数。

Classcount: 展示 JVM 从启动开始加载和卸载的类的个数。

Thread: JVM 加载线程。

浏览器监控为浏览器端、移动端 H5 性能监控产品。它提供了直接面向用户的浏览器应用的性能追踪，包括响应加载时间，页面错误，异步调用，地理追踪等等。

浏览器监控总共分为“访问域名”，“访问页面”，“定位分析”，“Ajax 接口”，“脚本错误”，“浏览器性能”，“摘要”，“地理”八个维度。

访问域名

一个应用可以配置多个子域名，BI 的访问域名性能监控根据域名的维度统计性能数据，主要包括页面加载性能趋势、响应时间趋势、吞吐量与慢加载。

白屏时间: 从准备加载页面到浏览器开始显示内容的时间。

首屏时间: 指用户看到第一屏，即整个网页顶部大小为当前窗口的区域，显示完整的时间。

网页加载: 从接收到页面文档第一个字节到接收到最后一个字节的时间。

资源加载时间: 页面内 js、css、image 等资源加载时间。

慢加载追踪: 加载时间超过 8000ms 的访问。

从 Ajax 维度，统计每条 Ajax 请求的平均响应时间，时间百分比，吞

吐量，并且从响应时间 TOP5，吞吐量 TOP5，发送数据，接收数据四个方面统计请求性能趋势。

## ● 系统平台集成能力

系统接口服务规范化管理：发布基于 Webservice 的常用业务接口；具备系统接口服务的管理工具，可查看、维护、测试接口的 WSDL 文件。

系统平台的构件可区分为客户端构件和服务端构件，对于服务端构件，可以通过“发布”功能，发布为标准的 WebService 服务接口。

同时，系统平台提供“常用业务接口”功能，可以查看当前系统里所有的 WebService 服务接口，并可以联查每个 WebService 服务的 WSDL 描述信息。

平台预置常用业务数据接口：平台预置常用业务数据的接口，包括：凭证信息、应收单、应付单、预算数。

在本项目产品中，所有的业务数据接口，是以数据交换包的形式体现的，系统预制了大量的常用业务数据接口，包括凭证接口、审计接口、应收应付、主数据等，如下图所示：

Portal 支持：平台已具有成熟的 Portal 集成框架，能与业务流程无缝集成。

本项目企业信息门户平台是参考国外先进门户解决方案，结合国内实际应用设计研发而成的一套企业门户系统，即是一套门户开发框架，也是一套门户应用系统。

本项目企业信息门户平台包含门户管理、站点管理、内容管理、门户

应用 4 大部分，提供了多站点管理、数据连接服务、部件与展现服务、开发与扩展工具、展现布局设计、个性化设置、单点登录、文档管理、信息集成、审批中心、全文搜索、社区服务等几十种服务和工具，提供企业信息门户、企业集成门户、企业业务门户等多种门户方案，通过简单配置即可快速实现各类门户应用。

本项目企业信息门户平台具有优秀的跨系统信息集成能力，通过一套信息集成与展现模型，把与异构系统的接口屏蔽在数据连接层面，通过预置各种常见数据连接器及信息描述规范，能够快速实现系统集成；本项目企业信息门户平台具有高度可扩展性，系统对门户展现、通讯、事件等进行了统一封装，内置各种配置管理工具和开发工具，通过这些工具，可快速实现系统功能扩展；本项目企业信息门户平台还具有强大的内容管理能力，对企业的各种结构化和非结构化信息都能够进行良好的支持，能够为这些信息提供的统一呈现和检索服务。

ESB 支持：平台提供企业服务总线的实现，能进行不同接口协议的适配、数据映射、转换，可靠的消息传输。

我公司企业服务总线（Ent 企业 riseServiceBus，简称 ESB）是一款基于 SOA 架构的服务集成平台。实现了可构建基于面向服务的、松耦合的、灵活拆分的信息交换平台，完成了动态链接、智能路由、信息流转等服务总线核心功能，并提供了协议转换、安全控制等基础服务。同时，企业服务总线通过服务配置管理中心完成对总线服务的部署与管理，通过服务注册中心实现对总线服务的注册与定位，并通过监控中心获得总线服务性能的实时监控，为用户快速便捷的完成 SOA 整合环境下总线的搭建工作提供

了架构支持。

主要功能特征如下：

支持如 FILE、HTTP/SOAP、TCP/IP、FTP、JMS、POPS、SMTP 等多种协议的适配器。

### 1. 具有强大的数据转换能力

- 支持消息格式转换
- 支持数据映射
- 支持数据合并与拆分
- 支持各种表达式的定制
- 支持数据转换逻辑的扩展
- 提供强大的消息路由功能
- 支持硬编码实现的静态路由
- 基于消息内容的、可配置的动态路由
- 服务注册的动态服务绑定和调用

通过与服务注册信息的集成，在服务请求过程中实时查询服务注册和更新情况，完成服务的动态绑定和调用。

### 2. 可视化的集成配置工具

支持适配器规则配置、组件流程编排、数据映射设置、消息格式转换、路由规则配置。

支持建模、开发、部署、测试、调试及监控等面向服务。

提供完备的系统容错与监控处理机制。

支持集群部署与负载均衡。

分布式部署支持：平台支持多套系统间的拓扑结构的定义及维护；支持服务器集群部署及扩展。

系统部署架构设计需要考虑企业组织架构、管理要素、网络状况等因素，建议对于涉密网单位用户，根据业务需求采取企业集中部署和以院级单位为中心的二级集中部署方式；对于非涉密网单位用户采取企业集中部署方式，为综合管理提供统一服务。

分布式部署网络拓扑结构中各个站点相互连接，实现涉密网和非涉密网的文件服务器、工作站和电缆等的连接。现在最主要的拓扑结构有总线型拓扑、星型拓扑、环型拓扑、树形拓扑（由总线型演变而来）以及它们的混合型。把这三种最基本的拓扑结构混合起来运用自然就是混合型了。

平台、主数据、应用系统部署在服务器物理单元；

涉密网以院级为单位进行二级集中部署；

非密网在企业非密中心集中部署；

密网、非密网数据通过数据安全交换集中到企业；

安全方面同设置了镜像库，保障数据写入的安全性；

系统支持分布式部署服务器集群，集群能将很多服务器集中起来一起

进行同一种服务，在客户端看来就象是只有一个服务器。集群可以利用多个计算机进行并行计算从而获得很高的计算速度，也可以用多个计算机做备份，从而使得任何一个机器坏了整个系统还是能正常运行。

集群系统可解决所有的服务器硬件故障，当某一台服务器出现任何故障，如：硬盘、内存、CPU、主板、I/O板以及电源故障，运行在这台服务器上的应用就会切换到其它的服务器上。

集群系统可解决软件系统问题，在计算机系统中，用户所使用的是应用程序和数据，而应用系统运行在操作系统之上，操作系统又运行在服务器上。这样，只要应用系统、操作系统、服务器三者中的任何一个出现故障，系统实际上就停止了向客户端提供服务，比如我们常见的软件死机，就是这种情况之一，尽管服务器硬件完好，但服务器仍旧不能向客户端提供服务。而集群的最大优势在于对故障服务器的监控是基于应用的，也就是说，只要服务器的应用停止运行，其它的相关服务器就会接管这个应用，而不必理会应用停止运行的原因是什么。

集群系统可以解决人为失误造成的应用系统停止工作的情况，例如，当管理员对某台服务器操作不当导致该服务器停机，因此运行在这台服务器上的应用系统也就停止了运行。由于集群是对应用进行监控，因此其它的相关服务器就会接管这个应用。

## ● 相关系统集成

我公司承诺按照系统适、对接、完善等工作。自行协商或开发本项目所需的对接的数据接口，不以任何理由降低建设标准、延长建设时间，并

在项目期内按照行业要求进行系统更新、升级、优化等后续服务，数据接口开发、对接系统改造、后续服务的费用已包含在本次投标中。

本项目基于经管平台、移动工作平台建设，按照标准进行集成对接，实现信息推送、数据抽取、数据展示等功能。

#### 1、与 XX 项目专有云资源集成

由 XX 项目专有云提供计算资源、存储资源和网络资源，本项目需符合 XX 项目专有云部署要求以及管理要求。

#### 2、与营销管理平台各应用系统集成

与 XX 项目经管平台中各应用子系统之间存在功能的调用关系，需要提供相互之间的集成服务。

### ● 系统测试验收

### ● 项目验收方案概述

验收测试的测试资料由 XX 项目方准备，测试环境由 XX 项目方提供，我公司负责协助 XX 项目方完成验收测试。

验收测试原则上由 XX 项目主导，由我公司项目组实施测试。我公司项目组根据 XX 项目的测试要求，编写必要的测试代码，提供相应的验收测试用例，XX 项目根据双方共同评审后的验收测试代码、测试用例，根据项目验收标准来逐一检验系统的安全性、功能性、非功能性及各项要求等是否满足需求。测试过程技术上由我公司项目组负责，我公司项目组根据 XX 项目要求，需对验收项目设计具体可行的测试方案，XX 项目全程参与确保测试的真实性、有效性。

当 XX 项目与我公司项目组对测试结论产生争议时，可由 XX 项目指定第三方软件评测机构对争议项进行评测（费用由 XX 项目承担），当第三方软件评测机构结论与我公司项目组验收测试结论不一致时，需进一步论证验收结论的真实性，原则上以 XX 项目指定的有资质的第三方软件评测机构出具的正式测试报告为准。

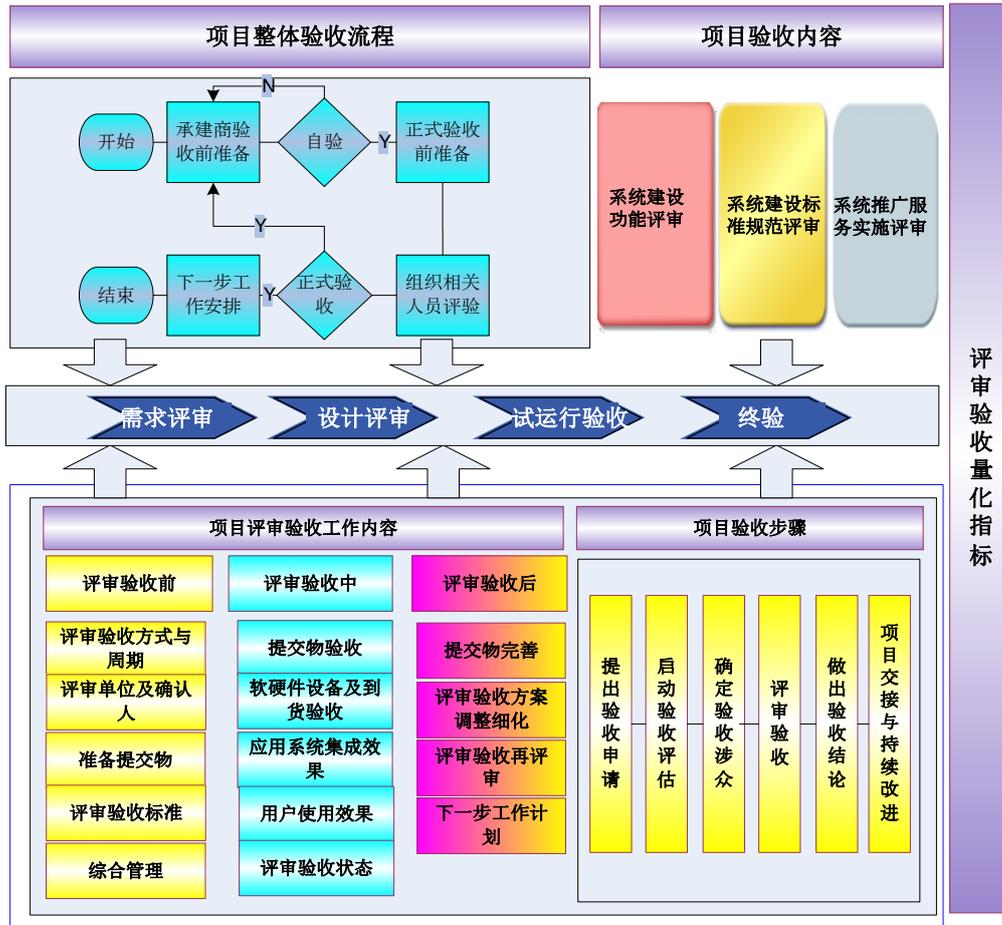
当验收测试结果不满足要求时，我公司项目组需对系统进行优化、修改、完善，确保验收测试全部通过。

项目验收测试结束，我公司将提供包括但不限于本项目所有开发文档（包含需求分析文档、技术分析文档、概要设计文档、详细设计文档、数据库设计文档、接口文档、软件测试文档等）、产品文档（包含安装手册、用户操作手册、系统维护手册、问题管理文档、软件修改文档等）。

针对本项目的实际情况，我们认为系统的测试验收包括了系统的需求评审，详细设计评审，系统试运行验收与系统终验。在每一个验收过程中制定了标准的验收流程：我公司首先需要进行自验，自验的标准除去常规的技术、业务、需求等要求外，我们还将遵从多年从事项目建设的经验总结出来的项目验收评价标准，自验通过后将提请监理和甲方进行系统的正式验收。

系统的正式验收分为系统的初验、试运行和终验阶段。在每个验收的阶段，我们都会从评审前、评审中和评审后三个阶段进行工作内容的准备。

系统的评审验收贯彻项目的全过程，对于过程中的重要过程和提交物我们将根据实际情况将进行正式和非正式的评审活动，以便于从项目过程中就确保项目质量，确保项目验收的顺利进行。



## ● 项目验收准则

终验时, 我公司将向项目办提交终验申请并进行技术交底, 同步提交实施结果与《需求规格说明书》和《总体设计报告》的差异表、用户测试报告、后续问题列表、验收方案、运维方案等。技术交底包括以培训形式进行的技术转移, 含证书、书籍、影像视频等。

我公司将根据测试方案提出验收方案和验收文档清单, XX 项目根据验收方案对系统每个模块进行逐一验收。

我公司负责在项目验收前将系统的全部各种相关的系统软件, 各阶段开发文档, 运行稳定可靠的本系统及其安装程序, 注释清晰明了的、能够编译生成目前正在运行的应用程序的源代码, 以及有关产品说明书、安装

手册、技术文件、资料、及安装、测试、验收报告等文档汇集成册交付 XX 项目。

我公司承诺，项目验收届时提供完整的项目系统源代码、必要的系统测试源代码、必要的源代码说明、必要的安装介质、验收测试报告、以 XX 项目为主体的软件著作权（以 XX 项目与我方评审后能够申请软件著作权的子系统为准，本项包含在投标总价中）、项目相关技术和管理标准规范。

按照实际情况，按需提供数据实体与接口服务说明书、系统部署说明书、项目资产变更清单（含软硬件及授权文件、专利版权等）、配置信息、相关产品质保证书等。

验收测试问题分类表：

严重程度	描述
A	整个系统不能继续运转
B	关键业务功能模块不能继续运转或错误
C	非关键业务功能模块不能继续运转或错误
D	某种状态下交易结果不对但有其他现成取代方案

系统升级扩容、客户化应用增加的验收测试

本项目的系统验收期中，XX 项目方应负责完成依据既定的“用户系统测试方案”进行的应用系统测试，并需按时向我公司方提交该用户测试报告。

“用户系统测试方案”需由 XX 项目方制定，在我公司项目组进行系统整体测试方案制定前提供给我公司方。

● 验收合格标准

## ● 软件验收合格标准

如果用户整体系统功能测试/用户系统验收测试结果分别如下表所述则视为测试合格，我公司将依规范时间对错误进行修改，以进行再测试。

严重程度	关系	用户系统验收测试
		发生个数
A	=	0
B	<=	0
C	<=	5
D	<=	10

当系统用户验收测试按照上述标准合格时，则由 XX 项目方和我公司双方签署书面的“应用系统验收报告”。

### 文档验收方式及错误限制

文档验收以抽样方式进行，抽样率为 50%。如果在验收的文档中，错误的总字数超过抽样文档总字数的 0.5%，或描述某一独立完整的功能/章节错误，则视为验收失败。

验收内容包括但不限于以下内容：

- （一）完成应用开发并已经上线运行；
- （二）完成项目相关技术和操作培训；
- （三）项目招标文件、项目投标书、开标现场承诺、正式合同以及项目过程中形成的需求规格说明书、详细技术方案。

## ● 项目验收步骤

- **提出验收申请**

根据每个阶段的验收要求，在自验通过后需要由系统承建商提出验收申请，经监理公司和甲方批准后，方可启动评估。

- **启动验收评估**

对于每一个验收阶段，验收前都需要进行验收准备工作，确定验收方法，验收范围，验收标准，细化验收方案等。

- **确定验收涉众**

启动验收后，需要细化哪些组织、人员需要参与到验收工作中，需要定义验收组织中的基本角色和各自的职责。

其中，需要确定关键人员是否需要全职进行评估工作，并保证全体参与人员能够正确全面地理解评估流程。

参与评估人员一般包括：

- 评估方：业务骨干；技术骨干
- 监理方：项目经理；
- 专家组：技术专家业务专家
- 被评估方：业务人员；项目经理；项目总监；开发人员；测试人员；  
管理维护人员。

- **评估、验收**

由验收人员根据验收方法、验收原则和验收方案对评估范围内的项目进行评估，并对评估结果进行记录和分析。

## ● 验收结论

根据评估结果，确认本次评估是否通过，并对通过 / 未通过的原因进行总结，做出评估报告。验收结果分为：验收通过、整改两种。

符合信息化项目建设标准、系统运行安全可靠、任务按期保质完成、经费使用合理的，视为验收合格；由于提供材料不详难以判断，或目标任务完成不足 80%而又难以确定其原因等导致验收结论争议较大的，视为不通过需要整改。

1. 项目凡具有下列情况之一的，按验收不合格处理：

(1) 未按项目考核指标或合同要求达到所预定的主要技术指标的；

(2) 所提供的验收材料不齐全或不真实的；

(3) 项目的内容、目标或技术路线等已进行了较大调整，但未曾得到相关单位认可的；

(4) 实施过程中出现重大问题，尚未解决和做出说明，或项目实施过程及结果等存在纠纷尚未解决的；

(5) 没有对系统或设备进行试运行，或者试运行不合格；

(6) 项目经费使用情况审计发现问题的；

(7) 违反法律、法规的其他行为。

## 2. 验收结论确认和处理

由项目验收组根据验收意见和相关资料得出结论，形成书面意见，提请监理公司审查，并经甲方确认。

## 3. 项目验收结论的处理

(1) 验收结论为验收合格的，系统承建商将全部验收材料统一装订成册并连同相应的电子文档，正式提交甲方存档。

(2) 验收结论为验收不合格的，系统承建商根据要求，限期整改，整改后试运行合格的，重新申请验收。

## ● 项目交接与持续改进

对于通过验收的项目，我公司承诺将相关文档、规范以及其他内容等正式提交 XX 项目。

在本项目全部功能试运行结束后，我公司提出验收申请，项目领导小组在接收到我公司提出的验收申请后一周之内组织验收人员准备验收工作，项目领导小组在验收结束后需要提出验收报告，确定验收合格与否。

我公司完成交付项目所述交付物品的交货及安装后，XX 项目方应于验收期内完成验收手续。验收内容含：交付的文件验收。

以“合同正式交付文档”的交付文件为验收内容。若有验收不合格项目 XX 项目方应于验收期间内书面通知我公司，逾期视同验收通过。验收期为各交付项目交付日起算的五个工作日内。针对不合格的项目，我公司负责改正，并再次对该改正项目提出复验申请，XX 项目方应于三个工作天

内进行复验，否则视同复验无误。

如遇特殊情况。经双方书面确认后可以适当延长复验期。

## ● 应用系统功能验收

以双方确认的“应用系统功能清单”所定义的功能为验收内容，参考我公司提供的测试计划及本章中“验收准则”实施。

根据项目验收标准对本项目各系统入口程序的终端类型进行逐一验收，确认需求的终端类型是否全部开发完毕。如 web 系统必要的双版本（PC 与移动端）、微信小程序版、支付宝小程序版、钉钉小程序版、独立 APP 版（IOS 和安卓平台）等。

若有验收不合格项目，XX 项目方应于验收期间内书面通知我公司，逾期视同验收通过。验收期为我公司完成“交付项目”所述项目的交付日起算 20 个工作日内，针对不合格的项目，我公司负责改正，并再次对该改正项目提出复验申请，于 5 个工作日内进行复验，否则视同复验无误。

如遇特殊情况，经双方书面确认后可以适当延长复验期。

## ● 交付件的验收收据

递交的技术文件验收依据是前一个阶段递交的并经双方确认的相关文件。如果前一阶段有变更请求，则本阶段的递交文件仅包含了双方同意必须在本次递交文件中完成的变更内容。

## ● 验收复查程序

以上“交付的文件验收”和“应用系统功能验收”，按计划进行，并

以双方项目经理认可的书面签章为验收通过的凭据。考虑到工作效率，以上所述“书面通知”，可以备忘录方式由项目经理代行之。

- **项目培训方案**

- **培训目标**

我公司提供相关用户培训，以帮助用户学习充足的专业知识，使其能有效使用系统资源。

我公司将保证提供最有经验的教员，使各类人员在培训后能够独立地对系统进行操作、管理、维护。

1、培训计划及大纲：我公司在项目建设过程中须提供相关用户培训（含培训所需的讲义、资料、教学设施等）。我公司将对培训计划和培训主要内容在建议书中进行说明。

2、培训对象：包括系统管理员和各级最终系统用户。

3、培训类别：包括原厂培训和应用系统培训。

4、培训时间：培训课程应安排在整个项目计划的合适时间段内。

5、培训费用：培训费用纳入项目总体报价。

- **项目培训的重要性**

项目培训工作是信息系统工作的基础性工作，是知识转移的开始，是系统实施的重要组成部分，也是系统应用的第一步。通过对不同角色的培训，能够提前分析与控制项目的实施风险，统一思想，正确理解和应用我公司实施方法论。通过培训，XX项目的技术人员将深入了解软件技术的先

进性、软件的开发理念及管理思想等，使应用人员能得心应手的应用好软件系统，使技术人员能够很好为系统应用提供技术支持，保证系统的安全运行。

通过培训，XX 项目的操作人员可以正确理解相关的业务流程，熟练掌握各个子系统的详细操作，从而为实现项目总体目标打下坚实的基础。

## ● 项目培训的步骤

培训工作要贯穿整个项目实施的全过程，依据我公司实施方法论的指导，在每一个阶段针对不同的角色提供不同的培训内容。因为项目涉及的范围较广，培训的人员也非常多，提供所有人员的一次性培训很困难，也不够合理，为了取得理想的培训效果，按照有利于项目实施的原则：

首先：我们为所需培训人员先按角色划分，为不同的人员制定不同的培训计划，按照项目实施的进度对相关人员进行培训；

其次：对相同角色的人员，也要分期分批的进行培训。

## ● 项目培训的内容

针对 XX 项目的实际情况，结合我公司在行业相关系统建设项目丰富的项目成功培训经验，我们将为 XX 项目制定一整套的培训制度与培训方案。

培训计划按照实施进度每期分为系统建设前、系统建设中、系统建设后等部分，力求通过培训使用户掌握规范的工作方式和业务流程，深入了解系统成功实施的关键因素，从而为顺利实施和运行 XX 项目本项目作好准备。

XX 项目本项目的培训包括业务管理培训和实际操作培训两大主要内容。

管理培训要求各级业务部门负责人、相关管理人员及各相关部门负责人参与，管理培训的主要目的在于明确管理思路，因此，相关责任人员需要共同参与管理培训。

XX 项目本项目的操作培训的参与人包括全部需要操作该系统的人员。通过操作培训，使全部系统参与人员对系统从感性上产生直接的认识。

培训的重点在于：通过整个 XX 项目本项目的实施，来帮助 XX 项目实现现有计算机和手工业务流程的优化，在优化的过程中，逐步实现 XX 项目管理流程的规范和工作质量的实质性改进。

根据 XX 项目本项目的要求，结合实施的进度，培训工作将分阶段地按照简明、实用、层次性原则开展。

培训分为五类培训：

(1) XX 项目本项目应用的各级领导。

这部分用户是 XX 项目本项目的使用者，也是最终的支持者，没有这部分用户的支持和推动，整个系统将在实施和推广阶段就面临失败的风险。

主要培训内容为企业系统为企业带来的管理价值提升；

(2) XX 项目本项目的各级中层领导和业务骨干

这部分用户可以认为是整个 XX 项目本项目的关键用户，他们直接担负着项目的推动和具体实施工作，可以说整个项目的成败，有很大程度将依赖这部分用户的参与程度和应用效果。对于这部分用户的培训也将是整

个项目进行培训的重点。

这部分培训的主要内容是项目管理理论，XX 项目本项目的平台架构，各业务模块的业务流程和详细功能。

### (3) XX 项目本项目的系统管理员

系统管理员是一个信息化系统持续稳定运行的基础，对该部分用户的培训将主要侧重于技术层面，同时兼顾部分业务流程的讲解。

主要培训内容为 XX 项目本项目技术架构，整个系统的业务流程和具体模块操作等内容。

### (4) XX 项目本项目纳入实施范围的所有操作人员。

这部分用户是最终用户，系统最终体现为他们在终端的操作。

主要培训内容为系统的框架介绍，业务流程介绍，分岗位分职能的软件操作。

### (5) XX 项目本项目验收前的答疑培训。

这部分培训主要针对系统应用中经常遇到的问题进行集中消灭式的答疑培训。

## ● 项目培训的对象

A—XX 项目本项目领导小组。

定义：由 XX 项目决策人员和相关业务高级管理人员组成的项目领导小组。

B—XX 项目本项目工作组成员。

定义：项目工作组成员包括关键用户、系统管理员、软件维护人员和

其他人员。

C—XX 项目商品、销售、服务管理等相关部门成员。

定义：商品、销售、服务管理等相关部门中的主要业务处理者和承担者。

D—XX 项目本项目的使用人员。

定义：XX 项目本项目使用所涉及的下属单位所有业务处理操作人员。

## ● 项目培训的方式

### 1、逐级培训

采用逐级培训的方式：首先在项目实施小组中，我公司的咨询顾问将会在实施小组中培养专业的培训讲师。然后，这些内部培训师与我公司的咨询顾问一起分头到各区域服务机构和应用部门进行操作培训。

具体安排如下：

在理念导入期间将进行省级单位中高层服务主管的理念培训，让企业上下充分了解 XX 项目开展企业项目的目标和意义；

在实施期间重点培养项目小组中的 2-3 名人员，他们将有机会了解到系统的初始化配置、协助制定数据收集规范、并有机会获得特殊培训，成为内部培训讲师，具备指导他人进行规范的数据录入的能力；

本方案优势：节约费用，并可培养 2-3 名有内部系统应用高级人员，便于以后长期的数据录入指导和数据录入规范的后期调整。多地培训可同时进行。

本方案条件：需要 2-3 名员工配合。

## 2、集中培训

采用集中培训的方式：集中把各机构、各办公单位业务人员组织成各个片区,在 XX 项目进行统一的培训，再由他们回到自己的岗位，直接上岗操作。

具体如下：

- 在理念导入期间将进行中高层服务主管以上人员的理念培训。
- 各个应用部门对指定的数据录入人员集中进行理念及操作培训。
- 如当地的操作人员离职或需要多人录入，由接受培训者负责对本应用部门内其他数据录入者进行培训。

### ● 项目培训的效果保障

#### 1. 理念培训

理念培训不仅仅是作为一个理念的介绍，更重要的是让员工知道自己为什么要采用这样的系统，对 XX 项目有什么帮助，对自己的工作会带来什么帮助及指导，目的是要让员工对系统产生主动的兴趣，以便更主动的应用系统。

#### 2. 培训教材

我公司提供针对角色的操作教材，帮助学员更好的理解自己角色在系统中的操作范围及角色权限，了解自己需要应用的功能的作用，并可以随时通过教材来解决具体的使用方法。

#### 3. 知识管理

我公司系统提供知识管理规范，可以描述企业操作规范，详细介绍不

同的角色应该如何在系统中进行操作，为员工提供操作层面的参考。

并可根据操作应用状况，随时调整数据录入规范和要求。

#### 4. 考试认证

我公司应用培训完全采用上机实地培训的方式，我公司将在培训前配置模拟的应用环境，仿真模拟每天/周/月所要输入的数据，并进行上机测试，通过考试认证者方能上岗。

#### 5. 培养讲师

我公司将在实施过程和内训中培养内部培训讲师，对此系统有着更全面的理解和深入的认识，不仅能充分掌握系统的功能，并能帮助 XX 项目提供持续后继的培训支持。

#### 6. 培训主体课程

我公司为 XX 项目本项目开设的主要培训课程如下：

- 实施准备阶段：信息系统规划培训；
- 实施准备阶段：计算机基础课程培训；
- 数据准备阶段：基础数据规范培训；
- 原型测试阶段：业务流程规范培训、软件结构和功能操作培训；
- 系统验收阶段：业务流程规范培训、软件结构和功能操作培训；
- 系统维护阶段：系统维护培训、数据库维护培训、网络知识培训；

### ● 项目培训教师的组成及要求

培训教师的组成为我公司认证顾问教师与 XX 项目关键用户结合的模式。

对于所有培训，我公司将派出具有相应专业的实际工作和教学经验的教师和相应的辅导人员进行培训，主要培训教员均具有二年以上的教学经验。培训所使用的语言和教材都是中文。

## ● 项目培训的地点选择

培训地点是培训效果与培训成本考虑的重要因素：

- XX 项目单位级培训：XX 项目专卖局办公现场。
- 最终用户培训：结合实际情况选择。

## ● 项目培训的双方角色

培训工作将是我公司方与 XX 项目本项目关键用户（包括项目组成员）共同进行，双方的角色与责任如下：

### 1、我公司项目经理

- 制定培训计划；
- 确认培训总结报告；
- 咨询培训教师
- 制定培训教材及课件
- 培训关键用户成为授课教师；
- 提交培训总结报告；
- 拟定考核策略和题目；

### 2、XX 项目本项目经理

- 协调并落实最终用户培训；
- 确认培训计划；

- 确认培训总结报告；
- 进行应用培训；
- 分岗位操作手册、练习题的准备；
- 进行培训考勤、考核。

● 项目培训的服务

XX 项目本项目的培训工作不仅是保证实施成功的一项重要工作，更是一项长期的工作，在后期应用过程中，由于应用功能的调整、应用系统的升级、应用人员的变化，应用人员的能力提高等需求，我公司将提供持续培训服务，我公司将与 XX 项目紧密合作，定期为 XX 项目本项目提供专项培训，培训采用集中专题培训方式进行。

● 项目培训的文档

编号	提交文档名称	备注	
项目培训文档	1	系统培训组织要求	
	2	项目培训计划	
	3	项目系统培训人员签到表	
	4	项目培训出勤统计表	
	5	项目培训考试试题	
	6	项目培训情况反馈表	

	7	项目培训考试成绩统计表	
	8	项目系统培训总结报告	

- 项目管理方案

- 项目管理策略

本着长期合作，共同发展的宗旨，我公司将不遗余力调动内部资源，运用丰富的信息化成功经验和行业经验为客户项目尽心尽力。

我们坚信在客户的领导下，在业务部门、技术部门的配合下，通过科学的管理和应用先进的开发工具，必能充分发挥我公司实施团队的丰富经验、熟练技能，从而按时高效高质地完成好项目的建设实施及系统开发工作。

- 系统规划原则

根据企业的战略发展要求，借鉴国内外大型企业的发展经验，电商平台功能众多，架构复杂，为保证项目目的的成功达成，我们认为系统的架构规划需按照以下原则进行。

- 1、管理面考虑：

- 统一领导

大的原则是由 XX 项目统一领导，组建项目领导小组，统一对整个项目的规划、建设和部署负责，形成统一的组织领导，确保总体方向的正确，符合企业的总体战略。

- 统一规范

统一制定建设的标准和共享的编码体系，建立共用的基础信息库和书面沟通模式，形成统一的资源开发与管理模式；各个系统在建设过程中，必须坚持统一标准，统一接口，统一运行平台的原则。

- 统筹考虑

统筹考虑项目执行部门、运营部门和内部用户部门的实际需要和核心诉求，统一思想，一起朝着项目成功上线这一目标前进。

- 逐级规划

按照总体架构和优先级规划，各运营单位应根据业务和运营特点，分别制定适合自身发展的战略和具体的运营策略，由此来展开具体的系统规划和需求调研。

## 2、技术面考虑：

- 先进性

技术上采用当前稳定网络计算技术和分布式处理模式，符合国际、国内标准的硬件和软件技术规范，保证技术上的先进性和前瞻性。系统支持大型数据库，面向 Internet/Intranet；硬件系统选择具有先进性、成熟性、稳定性，并拥有优良性能价格比的设备；软件系统在满足业务需求的基础上具有易改造、易升级、易操作、易维护等特性。

- 投资保护原则

充分考虑企业对投资的保护，并考虑业务框架和技术框架的前瞻性和先进性，为后续系统的接入预留接口和弹性，可以较低的成本重复利用已有系统功能。

- 持续优化原则

系统建设是迭代和局部升级的，建成后的系统可以持续优化。

- 灵活性原则

支持异构分布的系统和网络平台，系统之间可以协调运作。

- 扩充性

系统体系结构和硬件配置方面在考虑当前需求的前提下，为今后的扩展预留了空间。系统采用开放型的应用接口，具有灵活的扩充性，满足未来的业务系统发展需求。

- 前瞻性

系统体系架构和软件体系结构具有前瞻性，考虑了未来业务的发展和管理的变化，方便新业务和新需求的扩展。

- 开放性

为了充分利用现有资源，系统具有良好的开放性，实现与第三方系统的无缝对接。

- 灵活性

系统提供较好的灵活性，满足不同用户的个性化需求；在对业务系统进行数据采集时，提供灵活、多样的接口配置。

- 阶段性

系统充分考虑了系统建设内容与工程实施时间的辩证关系，分期实现，即保证总体目标的最终实现，又符合阶段性目标的合理性。

- 可靠性

系统采用大型关系型数据库，有严格的安全控制和数据备份机制，可

以确保数据安全可靠；拥有一套切实可行的质量保证体系，可以确软件的质量。

- 安全性

在网络上，保证内部系统的数据不被非法用户所获取。在应用软件的设计上，强化权限管理功能，具有多级安全机制。通过对各级人员及不同岗位人员的权限分配，做到所有人员只能查看与自己相关的数据，并建立完善的日志管理，做到所有操作都有据可查。

- 易用性

结合使用人员文化习惯，界面友好、方便使用。前台网站符合目标客户的使用习惯，后台操作让操作、维护、管理人员能够迅速掌握、简单易用。

- 集成性

系统应充分考虑与外部系统之间的接口，特别是本次规划的系统与原来已经存在的业务系统的接口问题，实现系统的集成应用，保障了不同业务系统之间的数据交换和资源共享。

- 质量控制原则

- 1) 系统应运行稳定，并具有较强的容错能力。
- 2) 尽量从用户角度出发，以方便使用系统：操作简单；界面表达清晰、美观。
- 3) 软件功能应全面、实用，技术先进，专业性强，满足各类不同需求。

4) 软件应具有较强用户个性化定制能力、迁移能力和后续开发能力，能够容易根据用户需求进行功能组合及调整。

5) 系统数据安全，应该能够记录系统运行时所发生的所有错误，包括本机错误和网络错误。这些错误记录便于查找错误的原因。

6) 系统的所有功能都应该进行功能权限、部门权限的判断和控制。

7) 系统能够对必须录入的项目进行控制，使用户能够确保信息录入的完整。

8) 系统安装方便，易于维护。

## ● 项目实施管理

项目周期需求分析阶段开始，包括需求分析、系统设计、开发及单元测试、系统测试、验收测试、上线演练等阶段，至系统正式提交投产。

我公司将派出强大技术实施队伍，本项目由 XX 项目项目实施团队技术总监总体负责，负责项目总体技术方案及项目总体协调，同时指派至少一名项目经理，负责拟定本项目的项目实施日程，并依据实施日程对本项目系统集成和客户化应用开发进行有效地管理、监控工作，领导我公司所属项目成员和 XX 项目方实施项目相关人员协调配合下如期完成项目。

## ● 项目实施阶段

### 1、实施前期准备

确立项目组织结构，成立实施开发团队；

项目启动会议，讨论项目目标，确定计划和安排，定义职责和分配资

源，形成文档项目实施方案，包括项目里程碑、活动和每个人的职责；

(1) 需求分析及方案制定：

我公司项目组和客户项目组进行充分交流，深入了解、细化、确认项目的建设的需求，编写详细的《项目需求说明书》。制定项目具体的开发步骤、实施计划和各方的《工作计划书》，项目实施相关技术文档规范的编写等。根据制定的开发步骤和实施计划，落实各方的工作职责、工作具体内容、实施时间、前提条件等。

(2) 建立独立的开发环境，进行系统的开发和测试：

在确定了具体《项目需求说明书》和各方的《工作计划书》后，我公司配合客户建立独立、完整的开发环境。客户项目组、我公司项目组在开发环境上按照《项目需求说明书》的要求对电子商务系统进行设计、开发、测试等具体开发工作。

(3) 生产硬件运行环境的检测：

如有必要时，在服务器等设备运抵安装现场前，我公司项目组和硬件厂家将派遣工程师对硬件运行环境进行全面的检测，确保机房的温度、湿度，电源等指标符合主机系统运行的要求。

(4) 硬件设备运输路径确认：

如果存在特殊硬件，在硬件设备运抵安装现场前，我公司项目组和硬件厂家将派遣工程师对主机系统硬件设备的运输路径进行现场勘察，制定运输路径及具体办法，确保主机系统硬件设备顺利进场。

## 2、主机系统软件的安装、开发和调试及现场培训

协助相关产品厂家人员、项目组成员将根据客户的实施开发环境（OS、WEB、DB 等）及设备情况进行安装及配置、调试相关的软硬件。

## 3、系统平台的安装、调试及试运行

当系统平台的主要设备就位、调试完毕后，我公司项目组及设备厂商负责在此环境上进行开发、测试，并在测试通过后正式部署，并且确保相关子系统的正常运行和相互之间的协同工作顺畅。

## 4、开发计划阶段

用户需求采集（需求面谈或用户需求调查问卷）；

建立工作分解结构（WBS），形成文档项目工作分解结构报告；

建立整体的项目计划：如范围定义；资源分配；费用结算；任务安排；初步项目计划；计划审核审批；形成文档项目计划；

发布详细的工作描述（SOW），形成文档项目实施工作手册（WorkBook）。

## 5、需求分析阶段

用户调查；

确立并文档化整体的系统结构；

数据分析并建立数据模型；

结构化功能分析定义；

界面分析定义，确立并文档化应用视图；

定义用户和用户权限需求；

审核数据模型，发布应用蓝图；

定义并文档化需求设计规则；

以调研和访谈记录为基础，编写并形成文档用户需求分析报告；

## 6、系统设计阶段

系统层：系统架构定义，数据库定义，形成文档 PRD 图，形成系统设计文档。

系统要求进行系统设计。

## 7、定制开发阶段

组件层：I. 功能设计；II. 界面设计；III. 系统管理设计；编码；开发；编码预排；内部单元、系统测试、系统集成；

## 8、评估、系统、用户测试阶段

用户运行环境测试；

业务功能测试；

项目组的质量管理小组进行回归测试，形成最终测试文档；

建立问题跟踪系统进行跟踪管理；

## 9、试运行及培训阶段

系统运行环境软硬件安装配置；

系统初始化数据整体与转换；

用户及权限设置，初始化数据设置；

进行用户应用测试；

建立用户初始化标准库，发布应用；

系统实施方案、项目测试报告、验收报告等文档

用户维护培训。

用户培训，发布用户操作手册；

技术培训，发布系统安装手册和系统管理员手册；

10、系统正式上线阶段

清理最初用户和试运行数据；

移交系统以及管理员密码；

系统验收，正式上线；

## ● 项目组织管理

项目规划阶段的第一个活动是项目组织建立，以保证整个项目有合理高效的组织机构保证，任何一项工作都是可以通过项目组织被快速有效地执行。

项目组成员要正式的互相介绍，同时要回顾技术规范，以确保服务商和客户对于项目的目标和目的能够达成共识。所有的决定，包括成本，进度计划，工作范围变更都要正式的以书面形式提交，这样所有参与项目的

人都同意要做什么工作，怎么做，何时做，它的费用是多少，有什么可以替换的方法，咨询顾问和客户项目组中的哪一位负责，以确保一个高质量的项目能够按时的在预算范围内完成。我们采用一次设计联络会来完成该过程。

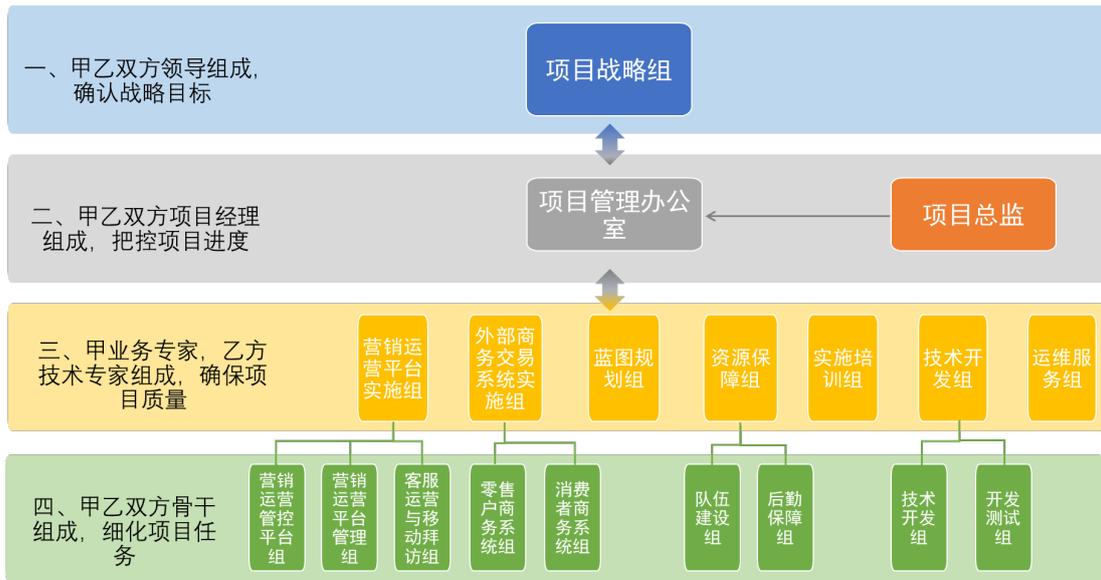
一套健全有效的组织和领导机构是贯彻项目意图并顺利进行工程实施的重要条件和保证。在项目规划之初，建议客户和我公司共同成立工程项目组。采用项目领导小组领导下的项目组负责制。

该组织结构是在多个大型软件工程项目中采用并被验证为是行之有效的组织方案。

## ● 项目组织架构

项目日常管理工作的由项目管理组承担，项目管理组由客户项目经理、业务经理和 XX 项目项目经理组成，对上向信息科技部领导和该项目业务主管部门负责，下辖需求工程组、开发组、测试组、架构组、系统环境组，由于本项目为大型项目，不存在一人兼职多项职责。项目开发管理组负责项目实施过程中的质量监督和质量控制，项目质量经理由 XX 项目方开发管理组指定一名人员兼任。

本项目实施组织架构：



### ● 小组职责总体分工

小组	组成	职责
项目战略组	甲乙双方高层领导组成	监督项目的实施；协调客户内部与各XX项目的资源，包括人力资源、设备资源及财力资源等；定期听取并审核项目经理的工作汇报；对项目存在的重大问题进行协调解决，做出相应的决策。
项目管理办公室	甲方项目经理、技术经理、业务经理及乙方协调人	制定和落实项目计划；随时解决项目中出现的各种问题；对项目的总体实施负责；对项目中的问题做决策；重大的问题由项目管理组上报项目领导组；协调项目组和客户内部其他部门的沟通和联系。负责项目组的文档编写的支持工作；整理各阶段文档，进行文档的版本控制；负责安

		<p>排项目组的住宿，饮食，交通，通讯，活动等一切后勤工作。</p> <p>乙方指定一名高级开发人员兼任乙方协调人，主要职责配合甲方进行项目管理，协调乙方内部事务的沟通与管理工 作。</p>
质量控 制组	甲方质量控 制人员组成，甲 方担任组长	<p>制定项目提交物的质量规范；按各提交物的质量标准，检查各阶段提交物的质量；配置管理方法的制定；对项目实施质量控制；配合客户内部质量控制机构对项目进行质量监督；配合各阶段的测试和验收工作。</p>
蓝图架 构组	由甲方技术 经理或者指定人 员担任组长	<p>负责对整个系统的技术方向的把握；负责本次开发的系统设计；对重大的技术问题进行评估和决策；参与制定开发规范，并参与对项目成功实施有重大影响的技术问题的讨论；对有争议的问题的上报 项目管理组</p>
业务组	由甲方人员 担任组长	<p>业务负责人或联系人具体负责：提出业务需求，完成业务需求说明书；确认并签收需求分析说明书；在开发阶段，及时回答开发组提出的与业务相关的问题；参</p>

		<p>与系统的验收测试。</p> <p>这里的业务组长负责项目组的需求管理工作。</p>
开发组	<p>由甲方技术经理或者指定人员担任组长,甲、乙方技术人员组成</p>	<p>负责根据业务需求,进行符合用户需求的逻辑设计,编写出符合用户需求的需求分析说明书;进行系统设计,并根据系统设计,完成编程和单元测试;完成系统的联调测试;在开发阶段,负责对需求的变更进行分析,评估。</p> <p>负责应用开发版本控制;开发环境与测试环境的建立;测试环境维护;对联调测试和系统内部测试做支持与管理;对系统中的操作系统、数据库、中间件等系统软件方面进行支持。</p>
测试组	<p>由甲方人员担任组长,双方测试人员组成</p>	<p>根据需求分析说明书,制定测试计划,准备测试案例及数据,并且负责进行项目测试;</p>
资源保障组	<p>由双方技术人员组成</p>	<p>提供人力资源以及后勤保障,技术资源协调,保障支持服务,7*24小时支持。</p>

● 双方协调机制

为保障项目有序进行,项目启动后将第一时间确认项目协调沟通机

制。

- 每周例会及工作周报

由我公司项目经理在周五下班前提交本周工作周报，分发给项目领导小组及 XX 项目方项目经理。周一召开项目例会，例会内容：检讨本周的工作情况、核实进度、研究本周的问题并落实问题的解决方案和责任人。

- 重要会议纪要

对于项目过程中重要的会议纪要由我公司项目经理整理后双方项目经理进行签字确认。

- 定期开展工作回顾

定期召开项目成员会议，促进项目成员对项目的了解，能对项目达成共识。

- 分歧处理机制

本着相互理解的原则，基于项目按质按期完成的共同目标协商处理  
协商无法解决，采用逐级提交的机制处理

- 项目风险管理

- 风险管理方案

风险管理技术是识别和度量风险，选择、拟定并实施风险处理方案的一种有组织的手段。

风险管理是按照装备研制项目的风险管理政策，对资源进行系统地 and 反复地优化的过程。

风险管理是在所有项目范围内，将任务和责任落实到工作中，能辅助项目管理进行管理、工程实践和做出判断。

风险管理技术涉及风险管理规划、风险的早期识别和分析、风险的连续跟踪和评估、纠正措施的尽早实施、沟通、文件编制和协调等。

风险管理方法由四部分组成：规划、评估、处理和监控。

风险管理的四要素形成联锁的闭环，并从初始规划之后相互依赖。风险管理要求由每个部门共同承担责任，并明确由上至下的职责和职责权限。风险管理是项目管理的内容之一。

风险管理是不断迭代的过程，要尽可能地利用现有项目管理过程的要素。

### 1) 风险规划

风险规划是确立有组织的、综合性的风险管理途径的持续策划的过程，策划的结果编制风险管理计划。

#### 1、风险规划的主要内容

确定风险管理的目的和目标；

确定风险管理使用的方法、工具和数据资源；

明确风险管理活动中各类人员的任务、职责及能力要求；

规定评估过程和需要考虑的区域；

规定选择处理方案的程序；

规定监控衡量标准和监控程序；

确定报告和文档的需求，规定报告的要求。

## 2、风险管理计划

风险规划过程的输出是编制风险管理计划。风险管理计划的内容可包括：

引言：说明计划的目的是目标；

项目的概述：简要的介绍项目、项目管理方法；

定义：确定项目风险定义范围，例如技术、进度、费用等方面风险定义、风险等级的定义及其他事项；

风险管理的策略和方法：综述风险管理的方法，包括风险管理现状和项目的风险管理策略、方针、政策和方法；

组织机构：说明风险管理的组织，逐个列举参与人员的职责；

风险管理过程和程序：说明风险管理需经历的必要过程，即风险规划、评估、处理、监控、记录文档，并对这些过程环节作基本解释；

风险规划：规定风险规划过程、持续的风险管理计划、计划的修改更新问题及批准等指导意见；

风险评估：规定风险评估过程和程序，概述风险识别、风险分析的过程，以确定风险等级和需制定应对措施的风险；

风险处理：阐明用于确定和评定风险处理方案的程序，对各种风险处

理方案如何用于具体风险提出指导意见；

风险监控：规定监控风险的过程和程序，规定准则以明确什么样的风险需要提出报告、报告的频次是多少；

风险文档和报告：规定风险管理信息系统的结构、需要编写的文档和报告，规定报告的格式、频度及编写的职责。

## (2) 风险评估

风险评估是装备研制项目风险管理过程中最重要的阶段之一，“风险评估”是对项目各个方面的风险、关键性的技术过程的风险进行识别和分析的过程，其目的是促进项目更有把握地实现其性能、进度和费用目标。风险评估过程包括三个步骤：风险识别、风险分析和风险排序。

### ● 风险识别

是指对项目的各个方面、各个关键性技术过程进行考察研究，从而识别和记录有关风险的过程。风险识别活动包括：

- a) 识别风险源/不确定因素源和主要因素；
- b) 通过风险分析技术，将不确定因素转化为确定的风险；
- c) 确定风险发生概率和发生后果的危害程度；
- d) 依据风险评估准则，量化风险；
- e) 确定风险项目的优先顺序(风险排序)。

### ● 风险分析

是指对已识别的风险事件（项目）进行具体的详细研讨、分析，判定可能出现的情况以及关键过程对预期目标偏离的程度，确定每一风险事件发生概率和后果，从而评定其风险的大小；同时通过分析确定促成风险的原因，找出风险致因，以便为确定规避风险策略提供依据。

风险分析的方法通常有：

- a) 故障模式影响及危害度分析（FMECA）；
- b) 故障树分析（FTA）；
- c) 建模和仿真；
- d) 可靠性预计；
- e) 专家的评估；
- f) 类推比较/经验教训法。

#### ● 风险排序

是指依据风险分析的方法所得到的风险大小或不同的风险等级，按其高低、大小顺序排列的方法。风险排序可以风险类别（如进度、费用、技术）、风险区域、风险过程分别进行，也可综合排序。不论采取那种形式排序，都要充分利用风险识别、风险分析过程中得到的定性和定量的数据或信息，在专家的评判中排出风险次序，并确定关键风险区域和关键风险过程。

### （3）风险处理

风险经过评估后，必须对确定了的风险规定规避策略，制定处理重大风险的方法。风险处理包括处理已知风险的具体方法和技术，完成各项任务的时间安排，明确各风险区域的责任者及估计费用和进度影响。其主要目的之一是将风险控制在可接受的水平上。

风险处理包括确定应当做些什么，由谁负责，何时完成，需要多少经费等。从可行性、可望获得的效果、资源需求是否可承受、制定和实施方案的时间长短以及方案是否对系统的技术性能造成影响等方面，评价各种风险处理供选方案，从中选取最恰当的处理方法。

风险处理的方法有：风险避免、风险控制、风险转移、风险接受、

#### （4）风险监控

是指按既定的衡量标准对风险处理的效果进行持续跟踪和评价的过程，必要时还包括进一步提出风险处理备选方案。监控结果可以为判定新的风险处理方法奠定基础，也可能识别新的风险。风险监控是一个连续的过程，风险监控过程的关键在于能对潜在问题及早报警，以便采取管理措施。

风险监控的方法可有：试验和评定、获得值管理、技术性能度量、项目的衡量标准、进度执行情况监控。

风险管理过程如下：



1. 召集项目组各方人员，开展头脑风暴活动，识别项目组存在的各类风险。
2. 根据列出来的风险内容，权衡利害关系，规整形成风险描述。
3. 针对已列入的风险，制定风险跟踪计划、预防风险措施，以及风险责任人。
4. 定期持续跟踪风险。
5. 在跟踪过程中，实行风险控制。对已规避掉的风险，从风险列表中去除，对风险内容的变化，进行更新。而一旦风险触发或预警时，必须启动风险应对预案，来降低风险带来的影响。

#### 项目潜在风险和预防手段

风险	降低风险的方法
项目时间紧，任务重，项目执行的效果有可能会受到影响	多方位多重手段保证，项目之初，需成立精兵强将的项目队伍，制定明确计划，任务分解细致，并严格

风险	降低风险的方法
	推进和即时跟踪
系统上线后，反映系统提升或变化不明显	项目之初，应和业务部门充分沟通，设立明确的可感知的目标，界面操作原型尽早和业务部门以及一线操作人员沟通。点击次数、时间需要设立可量化的指标。
项目推广牵涉多个单位或与其它多个系统有依赖关系，致使协调配合复杂	建立项目管理办公室 PMO，需要分管副总牵头成立项目组进行横向协调，相关业务部门参与项目组进行纵向协调。明确分工职责。建立 KPI 考核体系
业务需求无法得到有效控制，多头提出来的需求，缺乏专人来进行确认，从而导致需求发散。	需要在组织上保证需求的归口单位，确定和放权给专门的组织或人员来统一管控需求，保证需求的闭环管理
项目建设时间安排较紧，需要在短时间内，保质保量完成项目要求，没有冗余时间。	建立有效的风险管控体系，提前暴露问题隐患，设立预警机制和应对措施
新系统牵涉面较广，业务流程复杂，个性化需求较	需要站在全局的视角站在企业全局的视角，和局方共同在业务流

风险	降低风险的方法
多，并会带来管理和流程的改变	程、功能、数据、系统集成多个层面，全方位进行规划、设计以及对应实现。
数据准备工作量大，而且系统割接比较复杂，可能对生产运行运行有负面影响	<p>业务部门做为系统的主要使用者，也是数据完备性和一致性以及割接上线的主要责任者，因此需要业务部门的大力配合。</p> <p>指定熟悉专业人员负责数据割接工作，并准备详细的数据迁移方案，进行多轮次的数据校验</p>
项目涉及面广，实施周期长，对系统集成商的管控非常困难，由于沟通、诚信等各方面问题，造成实施障碍。	<p>建立面向系统集成商的考核机制，将一个大的项目，按照不同纬度，以及不同的时间阶段，建立相关的KPI 考核，确保系统集成商或应用提供商得到有效的管控和激励。</p>

● 其它主要风险防范工作

1. 加强项目监控

双方共同对项目进行管理，采取的主要监控措施为：

2. 项目计划

利用 project 项目管理工具，在项目各小组采取自下而上，上下结合的原则，按阶段制定详细项目计划。该计划按每周六个工作日制定，周日作为项目成员的机动日，提高计划的可操作性。

### 3. 进度跟踪

项目常务管理组每周两次与各小组长根据项目计划，核对工作进度，对发现的进度问题，及时查找原因，采取相应措施（如：调整工作、调整资源、确认有疑问的业务或技术问题）。

定期形成进度报告。

### 4. 人员沟通

项目组内形成畅通的沟通渠道（组员间日常非正式沟通，小组间定期正式沟通），沟通以文档为基础。重要文档经过项目常务管理组的审核。

项目组与局方的日常沟通，通过参与项目全程设计开发的局方组员进行；对于重要事项，由项目常务管理组确认。

根据项目需要，举行项目会议：项目会议的议题、参加人员、相关文档在会前准备妥当，会后形成纪要，明确会议成果或需采取的措施、相关责任、行动时间表等。

项目常务管理组成员每周定期沟通，并形成相应的项目进度及状态报告。

不定期形成项目状态报告，报送相关部门和领导。

### 5. 质量检查

严格实行工作过程和工作结果的文档化。

工作过程和结果通过组内互查、质量管理与配置组检查，尽可能消灭质量隐患。

## 6. 内部评审

在项目的各阶段组织内部评审，在评审前几天，将有关文档递交参加评审的人员。通过评审验证软件的需求、发现任何形式的软件功能、逻辑或实现方面的错误。

## 7. 加强测试工作

测试组在概要设计阶段完成测试方案的编写和评审。在详细设计和编码阶段完成测试用例的设计和评审。

项目小组负责完成现场的单元测试，提交单元测试报告。

集成测试以测试组为主完成，通过反复测试改进，形成稳定的软件版本。

局方各相关部门的主要业务人员均参与接受性测试。

## ● 系统性能及其他保障

项目设计应综合考虑 XX 项目的现状及未来的发展，要求遵循统一标准、总体规划、分阶段实施、先易后难、效果驱动，逐步完善的总体建设原则，根据 XX 项目的实际情况并结合业务开展情况，详细制定出业务的总体目标和分阶段目标，并同步明确相关建设内容，业务成熟一块推广一

块，最终实现总体项目目标。

我公司方案将基于 XX 项目基础资源云开展建设，我对专有云应用解读如下：

系统设计要遵循以下原则：

本项目符合技术先进性、稳定性、高可用性、易管理性、易维护性、安全性、开放性的要求。以便于适应国家、行业和企业后续制定的标准规范。

- **基础要求设计**

- **响应性保障**

1. 简单网页、接口、服务等（如首页、功能页、低数据量查询等）的请求响应时间。从业务功能数量上来看，80%的业务功能的平均响应时间控制在 2 秒内，并且单个业务功能 98%的请求都在 2 秒内；20%的业务功能的平均响应时间控制在 3 秒内，并且单个业务功能 98%的请求都在 3 秒内；特殊情况下，最长时间不超过 5 秒。

2. 复杂网页、接口、服务等（如高数据量查询、数据分析等）的请求响应时间。从业务功能数量上来看，80%的业务功能的平均响应时间控制在 4 秒内，并且单个业务功能 98%的请求都在 4 秒内；20%的业务功能的平均响应时间控制在 10 秒内，并且单个业务功能 98%的请求都在 10 秒内；特殊情况下，最长时间不超过 20 秒。

- **兼容性保障**

系统需对各类常见浏览器进行兼容性优化，保障系统能在各类浏览器下正确打开与使用，支持国产化生态软、硬件。包括但不限于：IE11 及以上，Chrome、360（极速模式）等主流浏览器；其涉及的外接控件等应用运行环境应同时通过国产化生态的兼容性验证，确保国产化终端适配。应支持国产主流、国内主流打印机等外设。

系统支持 web 类系统根据业务需要，需对移动与 PC 端进行双端支持，保证各设备不同屏幕尺寸下、不同系统下能够合理、正确的展示与使用各项功能。

## ● 稳定性保障

系统在一定的业务压力情况下，持续运行一段时间（一般为 24 小时），确保系统能够稳定运行，要求各个子系统各项功能点正常打开的几率  $\geq 99.95\%$ 。

系统支持 7×24 小时持续可用，可在每日特定时间段内对系统进行维护，稳定性要求达到 99.95%，稳定性计算规则  $(1 - \text{服务不可用时间} / \text{总服务时间}) * 100\%$ 。传输数据服务要求准确，不能丢失数据。系统需达到输入有提示，数据有检查，防止数据异常，能够处理系统运行过程中出现的各种异常情况。

系统需提供错误处理机制，当系统运行过程中发生错误时，系统可以明确提示错误信息并指导用户按照错误处理指引进行处理。

系统提供运行监控机制，应有详细的系统日志，记录系统运行的状态及所有操作痕迹，可追踪系统的历史使用情况。系统应提供数据备份、故

障恢复机制，定期对系统的数据、运行状态等进行备份，由于系统的错误或其他原因引起系统的数据丢失或系统的数据被破坏时，能够及时恢复和还原数据。

## ● 易用性保障

系统用户界面友好，使用操作便捷，用户对照使用说明书或者略经培训就可快速掌握使用；通过提供批量处理、便捷功能、下拉菜单、弹出页面等多种方式，以及更多的快捷方式（快捷键、右键菜单等），减少用户机械、重复操作，尽可能支持导入功能，使用户能够方便快速的将数据传入系统。

对于常用不变的数据项、重复数据项、可枚举的数据项、可自动产生的数据项，设置为缺省值或自动提供，以减少用户录入操作。系统需注重产品体验，对于页面数据量大，导致加载时间长，给用户提供加载进度条，预计加载时间，减少用户焦虑；查询数据量很大时，采用分页加载、懒加载。

## ● 扩展性保障

系统应采用模块化、组件化、面向对象的体系结构。在技术架构和设计模式上保证技术的延续性，灵活的扩展性和广泛的适应性，确保系统能够根据技术发展、用户在数据及业务功能方面需求的增加不断升级扩展。在选择技术实现时尽量做到可配性强、配置灵活，以适应不同情况下用户的需求。

在规定的业务规范范围内，能够机动、灵活地更改业务内容，增删业

务处理程序，改变相关报表及统计信息，并能够为后续系统扩展和功能完善增加组件设置接口，使得数据更新简便、系统升级容易。

充分考虑现有应用以及今后业务的可能扩展，随着数据量的增加和运行节点的扩展，应用系统能够随着硬件和系统软件的升级或增加，具有良好的可扩展性。

应用软件应具有良好的开放性，遵循业界相关标准，支持开放的标准接口，使整个系统成为一个统一的整体。

## ● 可维护性保障

系统各业务功能模块可单独创建、更新、移除，改动过程中不可影响系统其他业务功能的运行。

开发过程中，从接到修改请求后，对于普通修改应在 1 至 2 天内完成；对于评估后为重大需求或设计修改应在 1 周内完成。90%的 BUG 修改时间不超过 1 个工作日，其他不超过 2 个工作日。

任何对象的任何方法都不允许超过 200 行代码。一个模块或方法的最大圈复杂度不能超过 15。系统代码可读性要强，每个类、接口、方法、属性等命名要有意义且要求尽可能进行中文注释，确保能够帮理解代码，注释率 $\geq 60\%$ ，注释率计算规则（类、接口、方法、属性等已添加注释的个数/类、接口、方法、属性等总个数） $*100\%$ 。

## ● 关键技术路线

## ● 基于 SOA 架构

SOA (ServiceOrientedArchitecture, 缩写 SOA), 即面向服务的体系架构, 它提供了一种构建 IT 组织的标准和方法, 并通过建立可组合、可重用的服务体系来减少 IT 业务冗余并加快项目开发的进程。SOA 允许一个企业高效地平衡现有的资源和财产, 这种体系能够使得 IT 部门效率更高、开发周期更短、项目分发更快, 在帮助 IT 技术和业务整合方面有着深远的意义。

企业服务总线 (EnterpriseServiceBus, 缩写 ESB), 是面向服务架构的骨干, 在完成服务的接入, 服务间的通信和交互基础上, 还提供安全性、可靠性、高性能的服务能力保障。采用 SOA 架构, 基于 ESB 总线进行企业应用集成, 应用系统之间的交互通过总线进行, 这样可以降低应用系统、各个组件及相关技术的耦合度, 消除应用系统点对点集成瓶颈, 降低集成开发难度, 提高复用, 增进系统开发和运行效率, 便于业务系统灵活重构, 快速适应业务及流程变化需要。

基于 SOA 架构的应用集成开发方法, 与传统的软件开发方法略有不同, 角色分工更加明确。就整个项目开发周期来讲, 首先由业务分析员进企业务及流程定义, 然后由架构师和设计人员利用 SOA 方法将业务和复杂系统进行分割, 抽象出对应的业务服务及流程服务; 再由开发人员使用不同的开发技术, 基于选定的 SOA 基础架构, 进行组件和服务的开发实现、服务的组装与合成, 并打包部署和运行调试; 最后移交管理人员对服务和业务流程的运行系统进行监控和管理, SOA 系统运行中, 还可能会涉及操作人员参与业务流程的处理和使用。

## ● WebService 技术

从表面上看，WebService 就是一个应用程序，它向外界暴露出一个能够通过 Web 进行调用的 API。这就是说，你能够用编程的方法通过 Web 调用来实现某个功能的应用程序。例如，创建一个 WebService，它的作用是查询某 XX 项目某员工的基本信息。它接受该员工的编号作为查询字符串，返回该员工的具体信息。你可以在浏览器的地址栏中直接输入 HTTPGET 请求来调用罗列该员工基本信息的 ASP 页面，这就可以算作是体验 WebService 了。

从深层次上看，WebService 是一种新的 Web 应用程序分支，它们是自包含、自描述、模块化的应用，可以在网络(通常为 Web)中被描述、发布、查找以及通过 Web 来调用。

WebService 便是基于网络的、分布式的模块化组件，它执行特定的任务，遵守具体的技术规范，这些规范使得 WebService 能与其他兼容的组件进行互操作。它可以使用标准的互联网协议，像超文本传输协议 HTTP 和 XML，将功能体现在互联网和企业内部网上。WebService 平台是一套标准，它定义了应用程序如何在 Web 上实现互操作性。可以用任何语言在任何平台上写 WebService。

WebService 平台需要一套协议来实现分布式应用程序的创建。任何平台都有它的数据表示方法和类型系统。要实现互操作性，WebService 平台必须提供一套标准的类型系统，用于沟通不同平台、编程语言和组件模型中的不同类型系统。目前这些协议有：

## ● XML 和 XSD

可扩展的标记语言 XML 是 WebService 平台中表示数据的基本格式。除了易于建立和易于分析外，XML 主要的优点在于它既与平台无关，又与厂商无关。XML 是由万维网协会(W3C)创建，W3C 制定的 XMLSchemaXSD 定义了一套标准的数据类型，并给出了一种语言来扩展这套数据类型。

WebService 平台是用 XSD 来作为数据类型系统的。当你用某种语言如 java 来构造一个 WebService 时，为了符合 WebService 标准，所有你使用的数据类型都必须被转换为 XSD 类型。如想让它使用在不同平台和不同软件的不同组织间传递，还需要用某种东西将它包装起来。这种东西就是一种协议，如 SOAP。

## ● SOAP

SOAP 即简单对象访问协议(SimpleObjectAccessProtocol)，它是用于交换 XML 编码信息的轻量级协议。它有三个主要方面：XML-envelope 为描述信息内容和如何处理内容定义了框架，将程序对象编码成为 XML 对象的规则，执行远程过程调用(RPC)的约定。

SOAP 可以运行在任何其他传输协议上。如可以使用 SMTP，即因特网电子邮件协议来传递 SOAP 消息，在传输层之间的头是不同的，但 XML 有效负载保持相同。

WebService 希望实现不同的系统之间能够用“软件-软件对话”的方式相互调用，打破了软件应用、网站和各种设备之间的格格不入的状态，实现“基于 Web 无缝集成”的目标。

- **WSDL**

WebService 描述语言 WSDL 就是用机器能阅读的方式提供的一个正式描述文档而基于 XML 的语言，用于描述 WebService 及其函数、参数和返回值。因为是基于 XML 的，所以 WSDL 既是机器可阅读的，又是人可阅读的。

- **UDDI**

UDDI 的目的是为电子商务建立标准；UDDI 是一套基于 Web 的、分布式的、为 WebService 提供的、信息注册中心的实现标准规范，同时也包含一组使企业能将自身提供的 WebService 注册，以使别的企业能够发现的访问协议的实现标准。

- **WS-Security 技术**

WS-Security 定义了一个用于携带安全性相关数据的 SOAP 标头元素。如果使用 XML 签名，标头可以包含由 XML 签名定义的信息，其中包括消息的签名方法、使用的密钥以及得出的签名值。

同样，如果消息中的某个元素被加密，则 WS-Security 标头中还可以包含加密信息（例如由 XML 加密定义的加密信息）。WS-Security 并不指定签名或加密的格式，而是指定如何在 SOAP 消息中嵌入由其他规范定义的安全性信息。WS-Security 主要是一个用于基于 XML 的安全性元数据容器的规范。

- **非对称加密技术**

1976 年，美国学者 Dime 和 Henman 为解决信息公开传送和密钥管理问题，提出一种新的密钥交换协议，允许在不安全的媒体上的通讯双方交换信息，安全地达成一致的密钥，这就是“公开密钥系统”。相对于“对称加密算法”这种方法也叫做“非对称加密算法”。

与对称加密算法不同，非对称加密算法需要两个密钥：公开密钥（Publickey）和私有密钥（Privatekey）。公开密钥与私有密钥是一对，如果用公开密钥对数据进行加密，只有用对应的私有密钥才能解密；如果用私有密钥对数据进行加密，那么只有用对应的公开密钥才能解密。因为加密和解密使用的是两个不同的密钥，所以这种算法叫作非对称加密算法。

贸易方利用该非对称加密算法实现机密信息交换的基本过程是：贸易方甲生成一对密钥并将其中的一把作为公用密钥向其他贸易方公开；得到该公用密钥的贸易方乙使用该密钥对机密信息进行加密后再发送给贸易方甲；贸易方甲再用自己保存的另一把专用密钥对加密后的信息进行解密。贸易方甲只能用其专用密钥解密由其公用密钥加密后的任何信息。

非对称加密算法的保密性比较好，它消除了最终用户交换密钥的需要，但加密和解密花费时间长、速度慢，它不适合于对文件加密而只适用于对少量数据进行加密。

在微软的 WindowNT 的安全性体系结构中，公开密钥系统主要用于对私有密钥的加密过程。每个用户如果想要对数据进行加密，都需要生成一对自己的密钥对（Keypair）。密钥对中的公开密钥和非对称加密解密算法是公开的，但私有密钥则应该由密钥的主人妥善保管。

使用公开密钥对文件进行加密传输的实际过程包括四步：

发送方生成一个自己的私有密钥并用接收方的公开密钥对自己的私有密钥进行加密，然后通过网络传输到接收方；

发送方对需要传输的文件用自己的私有密钥进行加密，然后通过网络把加密后的文件传输到接收方；

接收方用自己的公开密钥进行解密后得到发送方的私有密钥；

接受方用发送方的私有密钥对文件进行解密得到文件的明文形式。

因为只有接收方才拥有自己的公开密钥，所以即使其他人得到了经过加密的发送方的私有密钥，也因为无法进行解密而保证了私有密钥的安全性，从而也保证了传输文件的安全性。

实际上，上述在文件传输过程中实现了两个加密解密过程：文件本身的加密和解密与私有密钥的加密解密，这分别通过私有密钥和公开密钥来实现。

## ● 统一标准规范设计

项目标准规范体系是由一定范围内的具有内在联系的标准组成的科学的有机整体，它包括现有的、正在制定的和应着手制定的各类标准，是促进一定范围内的标准组成趋向科学化和合理化的手段，通常用标准体系框架和明细表的方式来表达。

标准一旦制定，将对整个企业产生广泛的影响，并且将持续较长一段时间，项目标准和规范的建设是一项复杂而艰巨的任务，它的工作量很大，并且需要协调的方面很多。因此在建设的过程中要必须遵循以下原则：

### 1. 大局着眼，急用先行

全面分析项目需求，结合项目信息化标准体系，从信息化建设的高度着眼，完善信息化标准体系框架，本着急用先行的原则制定编制计划和标准经费概算，明确在本项目中需要完成的标准以及需要引用的标准，配合本项目的实施进度。

### 2. 结构合理、前瞻性强

标准体系是支撑本项目实施质量的标准规范框架，其设计过程必须充分考虑标准之间的互补关系，以合理的结构，全面地体现本项目的建设需要，以规范本项目的建设并完善我国的信息化标准体系。同时，信息化建设日新月异，标准体系设计必须有一定的前瞻性，充分考虑未来企业的发展趋势。

### 3. 充分利用现有标准

标准体系设计要充分继承现有 XX 项目客户端现有标准，对于 XX 项目现有标准可以满足项目需求的，要尽量引用，减少标准的新编任务。

### 4. 统一标准，保障安全

统一标准，保障安全是项目建设必须坚持的重要原则之一。

### 5. 切实可行，准确实用

标准和规范必须根据实际情况而制订和修改，这样才能使标准符合实际。标准的制订和修订要求准确实用，使执行者易于理解和执行，具有较强的可操作性。

### 6. 遵循电子政务的国家标准、企业标准、国际标准

标准和规范的制订应遵照、继承和贯彻国家标准、企业标准，避免重

复建设，参考国际标准和国外先进标准。标准和规范的采用顺序是：先国家标准，后企业标准，最后是国际标准。

#### 7. 前瞻性强，易于扩展

由于项目建设是一个跨部门、复杂的系统，各个业务部门都有其特点，因此标准的制订和采用应具有前瞻性并成熟可用，满足易于扩展的需求，使之能适应企业的变化。

#### 8. 统一组织，各级参与

标准和规范建设涉及面广，不是一个单位、一个部门所能解决的。因此，在标准的制订过程中必须调动各部门的积极性，吸收尽可能多的单位参与。特别是业务处理规范和业务数据标准的制订，必须有各业务部门的业务人员的参与。

在标准和规范的执行过程中，也需要各级业务部门的配合。在统一采集数据的基础上，建立系统的、分层次的管理指标规范。

### ● 系统性能设计

### ● 客户端快速访问响应设计

在设计原则中一种常见主题是适度原则。例如，任何页面似乎都有多个项并且请求多个连接。重要的是，页面设计者首先考虑的是每个页面项的实用价值，然后才是它们的大小和复杂度。页面设计者可以控制页面项的大小和复杂度，并且必须确保项的商业价值、大小和复杂度对每个因素向总下载时间所贡献的时间进行调整。页面设计者还能影响连接的数量和类型，并且必须了解他们做出的选择如何影响下载时间。

同样，还要考虑到准备页面的人们很少像最终用户那样查看自己的作品。考虑到效率，客户端设计者和开发者大多将自己置于靠近他们工作的 Web 服务器附近。大多数人设法与服务器处于同一个 LAN。相比之下，Web 站点访问者大多却处于很远的地方，并可能用速度相当慢的拨号连接。他们认为，Web 设计者可能看不到响应时间的显著差别。但是站点访问者却能看到经过深思熟虑的组装所能带来的益处。可以考虑把这种方法当成一种策略——让开发者在开发调试过程中多使用目标用户使用的典型连接来查看页面。

Web 页面中有很多公共组件和特征，我们对它们进行处理，以缩短下载时间。虽然并不是所有的事都行的通，而且有些组件或特征可能不在页面设计者的控制之下。

每个对站点性能感兴趣的人仍应该了解这些因素以及与它们相关的折衷办法。主要包括项的数量、大小和复杂度、连接数量、被访问的服务器数量、空白的使用、装入顺序、数据安全性。

### 1、管理项的数量、大小和复杂度

页面项的数量、大小和复杂度是促成页面大小、页面复杂度以及页面下载所需时间的唯一重要因素。十分简单，拥有少量简单项的页面装入最快并能赢得最满意的访问者。

#### (1) 管理项的数量

要想统计出精确的项数是不可能的。在选择所需项之后，使用有助于缩短下载时间的技巧：

发送作为浏览器或客户端热点图的菜单，而不是带有单独图形元素的

表格。因为传输表格本身就很慢，特别是那些带有图形元素的表格。

将项结合起来，这样 Web 服务器只需用较少的机器周期就能检索和传输内容了。

避免使用鼠标滑过时产生效果的 GIF 格式的图片。使用动态改变外观的 GIF 鼠标滑过效果图似乎很有趣，不过为实现这种操作效果，需要下载额外的 GIF 图片。不使用鼠标滑过效果的 GIF 图片可以减少页面中项的总和。

虽然大多人为减少项的数量削弱了界面的一些功能，但还是有其它的技巧存在。

## (2) 管理项的大小

根据功能或信息内容，平衡每项的大小。大些的项的装入总是要花费更多时间，但它不是提供更多的信息或更佳的功能所必需的。

## (3) 管理项的复杂度

页面的复杂度影响页面呈现的速度。在选择具有增加复杂度特性的项时，请考虑所涉及的延迟。决定页面复杂度的因素包括大表格、动态计算大小的表格单元、Java 脚本和 Java 小应用程序。动画 GIF、图像颜色管理和图像抖动也造成了延迟。延迟因浏览器的不同而不同，还因浏览器中级别的不同而不同；幸好有了新的级别，它们将趋于更快，但并不总是如此。

粗制滥造或描述蹩脚且不完整的项会造成浏览器到套接字通信挂起。一些表可能太复杂了，浏览器资源全部用来对它们进行操作，不能够再为它的套接字连接服务了。虽然时间在流逝，但处于运行状态的任何事都没

有完成。出现挂起情况时，粗制滥造的项或许已经在浏览器中并正在被处理。服务器和网络也会挂起，但是浏览器的挂起几乎总可以再生。这种挂起会造成丢失连接，就需要资源再次连接，从而使全部装入时间增加并让访问者更加不满。

HTML 文件的数量和大小是页面复杂度的指示器。虽然 HTML 编码超出了小组的分析范围，但我们的确知道像 GZIP 之类的实用程序能够压缩 HTML 文件。我们曾经看到 GZIP 将一个 HTML 文件的大小缩小至原有的 80%到 90%。一个较小的 HTML 文件能减少下载时间并使浏览器得以立刻开始呈现页面。

## 2、控制连接数量

从 Web 服务器到达 Web 浏览器的信息通过 TCP/IP 套接字连接。在页面信息能够流动之前，两端的连接必须是打开的。每个连接为建立和断开花费了时间，而且有些连接本来就需要比别的连接多花费些时间。请为每个所需连接的考虑以下因素：

(1)、如果必须传输多个项，持久的连接可减少连接设置开销

(2)、安全连接需要更多时间来建立

(3)、Web 站点可以在传输完一项后，对保持打开套接字连接或关闭进行控制。如果一个 Web 站点关闭了连接，浏览器必须为每一项建立一个新的连接。在装入页面时，这种连接开销会显著扩大访问者感觉到的延迟。大多数浏览器试图在它们这一端保持连接的打开状态，但两端必须都同意让连接保持在打开状态。是否保持连接开启的选项通常取决于 Web 服务器端，服务器上有个配置选项，这个选项决定了在浏览器有持久连接能力时，服务器是否支持持久连接的使用。

(4)、如果运行一个海量网站，还是不要保持持久连接，因为这种连接会造成所有端口或其它受限的服务器资源（如线程）都被占用。可以在服务器端分配额外资源，从而支持持久连接。

(5)、我们的目标是每页只有四个连接。随着服务器和 HTTP 服务器软件的发展，它们打破了使资源受限制的局限。当服务器端的连接保持打开状态时，站点访问者会受益。

### 3、控制被访问的服务器数量

在数全齐美的情况下，少数简单的项将驻留在同一个服务器，产生可能的最快下载时间。但是，在真实世界中，页面项经常驻留在多个服务器。这些项可能来自一个站点的服务器或来自跨越多个站点的服务器。每当用户访问另一个服务器，浏览器必须连接通向新服务器的套接字。如果所有浏览器的连接正保持打开状态，为连接到新服务器，浏览器必须断开一个现有的连接。通常情况下，浏览器先请求第一个服务器中的附加项，接着必须重新建立连接。如果可能，把来自单个服务器的项组织起来，避免中断和重新打开连接这个时间开销。当您必须使用多个服务器的时候，把来自同一服务器的请求合并起来，以便利用打开的连接。

尽可能使用直接链接，避免中间页面这一开销。重定向是专用于一当一组新的页面从原有的书签中装入时，将浏览器指向它。

使用浏览器内存高速缓存，可以减少带有对同一项多次请求的页面的下载时间。例如，设计者使用空白 GIF 来定位页面项。与其对空白 GIF 连续请求，不如先请求一个空白 GIF，再请求其它项比较好。这就允许服务器时间用来将 GIF 装入浏览器高速缓存，这样 GIF 就能满足后续请求了。

因为从高速缓存中检索 GIF 比为每个请求返回服务器要快些。

#### 4、控制空白的使用

与其必需添加服务器，不如合理的控制空白更有助于达到可接受的下载时间，甚至更快。

页面设计者经常使用空白帮助他们使页面表现更形象。没有额外的空白，浏览器也可以工作的很好。在将页面放到产品 Web 服务器上之前，可以考虑使用可用的实用程序消除 HTML 源码中额外的空白。

避免在需要加密的页面使用额外的空白。虽然明文中额外空白可以在拨号线路中被很好压缩，但加密的空白却不能被很好的压缩，因为这已不再是一个重复字符符号的字符串。加密后，每个重复空白块通常以独特的字节字符串表示，这就使它们不大可能被调制解调器压缩。每个额外字节的传输也占用资源，而对站点访问者没有任何好处。

#### 5、管理装入顺序

设计者可以确定对页面项请求的顺序，以这种方法优化下载时间。其目的是：指定并发操作使页面得以平稳下载的顺序。提前请求项，特别是大项和那些导航需要的项，从而避免在装入过程结束时产生延迟。理想情况是，浏览器应该及时识别项，让它和服务器的连接保持忙状态。

#### 6、了解数据安全性的影响

SSL（私密性）握手和加密会消耗两端的时间。因为私密性为每一项增加了阻力，所以准确设计加密页面很重要。在您设计加密页面时，所有被推荐的设计方法的影响要加倍考虑。

加密页面上的 HTML 项没有很好的压缩，因为 HTML 被转化成长数字序

列，它们在拨号调制解调器压缩方案下运行的效果不大好。这样，在加密页面上避免使用不必要的空白就更加重要。

显然，私有信息必须保持私有。权衡之计在于，分配私有信息给私有页面，而公有信息给公有页面：不要混淆私有和公有数据。不要将为私有信息请求的开销浪费在公有信息上。

## ● 数据检索处理响应设计

### 科学运用表分区

数据库大表优化，表分区技术是在超大型数据库 (VLDB) 中将大表及其索引通过分区 (partition) 的形式分割为若干较小、可管理的小块，并且每一分区可进一步划分为更小的子分区 (subpartition)。而这种分区对于应用来说是透明的，通过对表进行分区，可以获得以下的好处：

- 1、减少数据损坏的可能性。
- 2、各分区可以独立备份和恢复，增强了数据库的可管理性。
- 3、可以控制分区在硬盘上的分布，以均衡 IO，改善了数据库的性能。

### 表分区类型

表分区主要以下类型：

- 1、范围分区：将表按某一字段或若干个字段的取值范围分区。
- 2、hash 分区：将表按某一字段的值均匀地分布到若干个指定的分区。
- 3、复合分区：结合了前面两种分区类型的优点，首先通过值范围将表进行分区，然后以 hash 模式将数据进一步均匀分配至物理存储位置。

### 分区键的选择

分区键的选择：让查询很快定位，但尽量避免数据库操作集中；使大数据表拆分成“小表”，并使数据库操作平均分散到表分区中。

分区在单节点数据库上，提高查询定位的速度，不提供查询并行性。

## ● 并发性能设计

为了有效支撑大用户并发访问的要求，本项目主要从采用高效率的 WEB 架构、数据访问性能优化、系统采用集群、CPU 和并行查询方式的利用和负载均衡等方面保证项目的并发性能要求。

### 1、采用高效率的 WEB 架构

本项目采用面向服务的架构（ServiceOrientedArchitecture - SOA）架构，SOA 是解决应用系统互联互通的一种新架构和新思想，SOA 采用了很多业界所共同遵守的标准或规范，能够将应用程序的不同功能单元通过服务之间定义良好的接口和契约联系起来。

支撑 SOA 的企业服务总线 ESB 是传统中间件技术与 XML、Web 服务等技术相互结合的产物，能有效实现系统应用不同消息和信息的准确、高效和安全传递，能有效提高系统的并发响应能力。

### 2、数据访问性能优化

在数据库处理中，资源花销最大的是建立数据库连接，而且用户还会有一个较长的连接等待时间。本项目将复用现有的 Connection，也就是使用 ConnectionPool 对象机制优化数据访问性能。

当一个用户访问时，直接在连接缓冲池中取得一个数据库连接，而不需重新连接数据库，因此可以大大地提高系统的响应速度。

### 3、CPU 和并行查询方式的利用

本项目将充分利用 CPU 和并行查询方式提高系统的并发响应能力。

#### (1)、尽量利用多个 CPU 处理器来执行事务处理和查询

CPU 的快速发展使得数据库越来越重视对多 CPU 的并行技术的应用，一个数据库的访问工作可以用多个 CPU 相互配合来完成，加上分布式计算已经相当普遍，只要可能，应该将数据库服务器和应用程序的 CPU 请求分开，或将 CPU 请求从一个服务器移到另一个服务器。对于多 CPU 系统尽量采用并行查询方式进行数据库操作。

#### (2)、使用并行查询方式进行数据查询

使用并行查询方式不仅可以在多个 CPU 间分配 SQL 语句的请求处理，当所查询的数据处于不同的磁盘时，一个个独立的进程可以同时进行数据读取。

#### (3)、使用优秀工具进行大数据量的装载

使用该方法进行数据装载时，程序创建格式化数据块直接写入数据文件中，不要求数据库内核的其他 I/O。

### 4、系统采用集群和负载均衡

本项目的应用服务器将采用集群和负载均衡技术实现对系统访问的连续运行以及系统之间的业务分流，减少单个服务器的运行压力，提高系统整体的并发响应能力。

## ● 敏捷迭代型基础建设

有效进行高层次的业务抽象，对所有业务进行横向、纵向拆解切分，

合并相同部分，独立不同部分。制定一系列标准，在业务逻辑之上能够提供统一流程编排服务，实现微服务化。

通过可视化、配置化、低代码的方式，降低对每个 API 学习域的熟悉成本，从而不抵消 API 复用的便利性。

实现可视化，有效降低使用方的学习成本；实现配置化，能够把各个业务使用的能力集中管理，让熟悉业务的人员直接控制应用中的业务逻辑，更好的执行标准；实现低代码，降低开发人员学习中台复杂技术框架的门槛，使其能忽略底层的技术实现，只关心业务逻辑部分。

同时，做好系统设计与中台化标准之间的平衡，在满足复用性的基础上，有效的实现快速低成本创新。

建立围绕运行域与管理域的中台整体应用架构，以页面、功能、能力和数据模型四个维度为标准，建立运行域八大中心共用库，同时开发元数据管理、能力管理、组件管理三个管理域基础功能，实现对八大中心的有效管理。

具体要具备以下几种能力：

元数据管理主要完成对数据模型的管理，包括对内置对象的数据结构进行扩展、部分字段的设定以及对应用中的定制对象进行定义等功能。

能力管理主要针对能力和功能的管理，主要包括：

（一）对中台预置的配置项进行注册和发现；

（二）中台预留抽象类，实现应用的定制化开发，通过机制进行注册和发现并提供给应用使用，具体需实现以下几种功能：

（1）在代码中使用统一注释，通过扫描可以自动把注释部分的代码

上报到能力管理实现注册；

(2) 在能力对应的代码进行修改后，扫描机制也能在一定的时机进行更新；

(3) 通过统一的编码规范，对某些类预留抽象类，可暴露给应用方自己进行实现；

(4) 应用方对抽象类进行实现后，可通过扫描机制发现，并让应用进行调用。

组件管理主要针对页面组件和服务组件的管理，页面组件在设计时需要区分面对不同用户的页面组件管理，如用户、商城、运营人员。前端的组件最终以页面编辑器的方式实现，后端的页面组件库，则需要实现与全局管理中的资源、菜单、角色管理配合，共同满足业务需求。

通过以上三种能力，实现对数据模型、能力、功能以及页面的统一管理需求。同时，还需要能够按照新系统开发迭代业务需求，通过配置化、低代码的方式，组装成新内容。

在以上业务逻辑中，还需要满足以下几点：

(1) 所有的模块均需在业务中台中进行定义，需要有统一的实体编号生成机制，且这个统一的机制能够与业务身份所需要的信息进行关联；

(2) 模块与组件由开发方生产，可以被任一消费方、开发方、运维方调用，而不需要进行代码上的重复开发；

(3) 业务中台的能力都是通过接口提供给上方的功能或者页面，所以所有应用对应的底层业务逻辑代码，都要使用业务中台的代码，并且在开发时要做好代码本地化部署。

- **项目服务方案**

- **项目实施工期**

自合同签订之日起 60 天内，完成项目中所有功能的上线运行工作，并确保所有功能上线试运行正常稳定。

试运行不少于 3 个月后，可完成项目终验工作，自项目终验之日起，进入项目运维服务期。

- **项目质保服务**

自项目完成终验合格之日起，我公司为本项目提供一年的免费运维服务。

- **服务要求理解**

- 1、项目实施

自合同签订之日起 60 天内，我公司将完成所有建设任务并提交初验报告，经他 XX 项目通过并盖章后，进行为期不少于 3 个月的上线试运行。

试运行结束若无问题，提供项目终验报告，完成项目终验盖章等相关手续。

- 2、服务人员

项目免费运维期（即质保期）内，有固定的维护技术支持团队，保障项目正常运行。

- **运维服务内容**

我公司将提供售后运维服务和技术支持，免费运维期（即质保期）内的服务包括但不限于：

#### 1. 升级服务

维护期内出现质量问题时，我公司提供软件升级服务、必要的相关应用系统改造支持和其它现场技术支持服务。

#### 2. 响应服务

我公司将提供 7×24 小时的技术支持，1 小时内响应，24 小时内解决问题（节假日可放宽至上班时间），以保证项目正常运行。

#### 3. 热线服务

我公司将提供热线电话、钉钉、微信等其它咨询服务渠道随时回答 XX 项目的各种问题。

#### 4. 质量跟踪

项目验收完毕后，我公司将定期跟踪，及时了解存在的问题，并给予解决。

### ● 运维服务质量管理

我公司设有专业的质量控制管理部，负责制定各项详细的考核指标，并接受用户的投诉，同时对内部各专业部门进行严格的监督考核，以保证向客户提供高质量的服务。

### ● 服务考核评估

我公司制定严格的服务考核评估体系，对运维服务质量进行考核，提高运维服务水平：

## ■ 系统运行的主要统计项目

- 系统可用率。
- 网络设备的可用率、CPU 利用率，内存占用率、磁盘空间占用率。
- 系统、设备发生故障的次数、类型和历时。
- 重大故障次数和历时。
- 用户申告次数和修复及时率。
- 发生安全事件的次数、类型和影响。

## ■ 维护质量指标

- 故障修复及时率——在规定时限内修复故障的次数与故障总次数之比。
- 重大故障、紧急故障发生次数——在统计时间内，重大故障发生的次数

## ● 故障申报及处理

### （一）故障受理

客户服务中心负责统一受理客户故障申告。

### （二）故障转派

客户服务中心在受理故障申告后，及时进行故障转派：根据机房计算机信息设备、机房基础设施、前端设备故障、光纤网络故障分类进行派单，由相应的维护人员接障。

### （三）故障解决

各类维护人员收到客户服务中心报障后，立即组织协调、解决故障。

若维护人员如遇到重大故障和疑难问题则向售后维护部提交，售后维护部负责进行技术支撑；售后维护部如遇到重大故障和疑难问题则向总经理助理提交，总经理助理负责进行技术支撑。

#### **（四）故障上报**

各单位遇到重大故障在积极处理的同时上报售后维护部，并由售后维护部统一处理。

#### **（五）故障通报**

当各类维护人员发现影响业务的系统平台故障时及时通报售后维护部；客户服务中心对相关故障进行拦截。

#### **（六）故障分析报告**

重大故障处理完毕后按相关维护管理规定向所属上级部门提交详细的分析报告。

#### **（七）故障维护考核**

各类维护人员及时判断故障段落，指挥故障的修复，并清楚记录故障处理情况，按要求及时通知用户，在故障通报过程中，各工序间要进行横评配合度考核。

### **● 客户满意度调查**

满意度调查是了解客户感受和预期的理想手段，客户满意度能否得以确保则是评价一切运维服务项目成功与否的标杆。

#### **（一）满意度调查内容**

我公司将会开展多方面的满意度调查，包括故障受理、故障处理、技

术支持等涉及到运维服务的多方面内容：

(1) 故障受理

- 报障方便性
- 受理人员的服务态度

(2) 故障处理

- 故障的处理速度
- 故障的处理结果
- 反馈的及时性
- 维护人员的服务态度
- 维护人员的技术能力

(3) 技术支持

- 联系技术人员的便捷程度
- 提供的技术支持的及时性
- 提供的技术支持的有效性
- 技术支持的广度和深度

**(二) 满意度调查的关键点**

成功的客户满意度调查应对若干关键点加以把握：

(1) 确定调查范围：

- 应覆盖运维项目提供的所有支持服务。
- 应覆盖设计相关服务属性

(2) 确定目标受众：

- 应涵盖全体客户

### (3) 我公司对满意度调查的态度

我公司在战略高度重视用户满意度的测评与改进用户满意度的测评与持续改进已纳入企业的运营管理体系，并持续采取有力的跟踪和改进措施。在用户满意度调查中，对于如何构建模型，如何设计问卷，如何采集数据，如何分析数据，都是有专业的团队和业务设计来实施。

企业实施用户满意度改进项目应有确定的组织和经费保证。

### (4) 我公司对满意度调查明确了组织和经费保障

通过运营制度体系有效推动用户满意度的测评与持续改进。我公司希望通过有效的监控影响用户满意度的各驱动要素的变化，并对其重要性指标和表现的结果作出深入分析，从而指导在生产经营中更好地配置资源，并有效地提高经营绩效。

## (三) 满意度调查的受众

- ① 本项目相关领导
- ② 本项目最终用户（使用用户、报障用户）
- ③ 本项目监理单位
- ④ 其他本项目重要干系人满意度调查的形式

## (四) 满意度调查的形式

我公司主要采用的客户满意调查的手段以电话、文本问卷、服务现场表格等。

顾客满意度调查表格式模板举例如下：

热线服务顾客满意度调查表
热线服务

热线服务时间	<input type="radio"/> 很满意 <input type="radio"/> 满意 <input type="radio"/> 一般 <input type="radio"/> 不太满意 <input type="radio"/> 很不满意
服务热线接通	<input type="radio"/> 很满意 <input type="radio"/> 满意 <input type="radio"/> 一般 <input type="radio"/> 不太满意 <input type="radio"/> 很不满意
热线服务人员的服务态度	<input type="radio"/> 很满意 <input type="radio"/> 满意 <input type="radio"/> 一般 <input type="radio"/> 不太满意 <input type="radio"/> 很不满意
热线服务人员的责任心	<input type="radio"/> 很满意 <input type="radio"/> 满意 <input type="radio"/> 一般 <input type="radio"/> 不太满意 <input type="radio"/> 很不满意
热线服务人员的专业知识水平	<input type="radio"/> 很满意 <input type="radio"/> 满意 <input type="radio"/> 一般 <input type="radio"/> 不太满意 <input type="radio"/> 很不满意
未解决问题回复的及时率	<input type="radio"/> 很满意 <input type="radio"/> 满意 <input type="radio"/> 一般 <input type="radio"/> 不太满意 <input type="radio"/> 很不满意

## ● 文档管理

### (1) 文档范围

文档范围是指本项目在运维过程中规定的项目交付成果中所涉及的文档，也包括在项目实施过程中所产生的不在规定之列的有关文档（包括临时过渡性文档）。

### (2) 文档管理员

文档管理员即是对文档的变化进行跟踪管理的专职人员。该专职人员由我公司委派。考虑到文档是重要的成果资料，在项目运维的生命周期内

其维护具有不断延续性，且是一个动态的跟踪过程。

### （3）文档状态

文档状态是在文档正式形成过程中即文档签发前文档所处的阶段。从对文档变化的动态跟踪和文档的标识角度来分析，文档状态（文档所处阶段）可以由一些关键点来体现。

### （4）文档备份

文档备份是文档管理的一个重要环节。万一文档库崩溃，备份是恢复文档库的唯一途径。其方式备份有两种：

配置管理工具服务器的库备份。如果库是以文件方式存储，则备份文件；库是以数据库方式存储则必须备份数据库，对数据库的备份可根据具体情况采用数据库的逻辑或物理备份，一般来说数据库中数据量较小时用逻辑备份即可。

## ● 业务管理

建立人员知识更新制度。包括能力的持续性培养，建立素质模型，明确岗位设置，全面掌握新产品新设备的特点、性能及维护要领，明确维护工作的任务、责任和质量要求。

为客户提供优质的服务，保持人员的稳定性十分重要。根据维护业务的性质并结合我公司的实际情况，在保持人员稳定性方面采取以下三方面的措施：

对参与本项目的人员签订补充协议，在本项目结束前不得由于个人原因离开。

适当的保持部分人员的本地化，是保持维护人员相对稳定的有力保证。

对部分骨干人员采取项目期满后给予一定的奖励措施。

## ● 进度和质量管理

按照项目管理要求，严格把控项目进度，从需求调研阶段、功能设计阶段、产品研发阶段、系统交付阶段及运维保障阶段，各阶段严格把控，按计划执行，对于出现偏差的情况，要分析研讨及时纠正、更新。

项目执行过程中严格把控项目进度和质量，确保项目顺利交付和成功实施。

- **售后服务能力**

- **售后服务方案**

针对本项目建设和实施，我公司将提供系统正常运行所需的软件、文档，并按照用户要求进行开发、安装实施、调试、优化、试运行，最终完成验收交付。

我公司将严格按照招标要求完成项目售后服务，包含：

我公司将为本项目提供更为全面、周到、细致、及时-的项目服务方案，并做出明确承诺。

基本售后服务要求包括：

- **项目质保期**

自本项目终验合格之日起，提供自终验合格之日起一年运维服务。

- **服务人员**

1. 服务时间及服务方式

项目质保期内，我公司提供 7×24 小时服务，保障项目系统正常运行。

2. 运维人员要求

运维人员应满足如下资质和能力要求：是项目实施的团队人员，应具有履行服务必要的技术能力、沟通能力和服务态度。

- **故障排除服务**

当系统故障发生时，我公司有责任诊断系统故障，对系统出现的问题进行及时的处理和故障排除，以保证系统的正常运行。

如果系统出现系统故障时且 XX 项目通过电话或传真方式通知的情况下，我公司的工程师应在 30 分钟内予以答复。

如果 XX 项目要求紧急处理，我公司在收到甲方通知后的 1 小时内赶到故障现场，4 小时内恢复系统正常运行。

## ● 系统优化服务

提出在正常条件下改进系统性能的各项建议，包括系统资源分配与效率改进建议、软件配置规划和性能优化建议、系统容量预测建议等。

## ● 数据备份服务

项目验收完毕后，在整个项目的运维过程中，实时做好系统的数据备份工作，确保经营数据和管理数据的安全可靠。

## ● 运维服务的定义

XX 项目平台涉及业务范围多，组织范围广、对系统稳定运行的要求高，因此售后服务和技术支持十分重要。如果对于上述标准运维服务模式需要深化界定，则采取服务定义的方式进一步细化服务内容、服务等级、服务周期等工作内容。

XX 项目本项目平台上线前一个月，我公司团队将会和 XX 项目内部支持团队一起讨论确定详细的系统技术支持计划，确定后续支持各项事宜的安排、人员部署等情况。这段时间的运维服务效果将是整体运维的增值价

值。

我们将从两个方面制定切实可行的运维支持计划：

1) 首先，明确服务水平和要求：

- 7\*24 小时响应
- 24 小时内问题应答
- 48 小时到达现场
- 每月定期客户回访并记录
- 技术交流平台问题 24 小时内回复
- 明确运维服务人员技能要求

2) 其次，制定增值的运维支持方式：

- 现场与远程的结合
- 每月用户体验访谈和讨论
- 组织用户研讨，互相参观，借鉴好的功能，好的应用推动方法
- 建立用户体验中心和交流中心

## ● 运维服务流程

技术支持阶段的任务将支持用户在新系统上完成所有的业务操作。记录出现的问题，并根据需要调整和优化系统，以下列出技术支持工作的内容及相关步骤。

### 1. 上线支持策略和流程

制定上线阶段的支持策略，落实现场支持人员和组织，确定支持工作的后勤准备（车辆、电话、传真等），落实上线过程中遇到问题的处理流

程。

## 2. 上线支持

依据 XX 项目信息化系统总体运维体系所需支持服务的特点构建本项目的运维支撑体系（包括支持模式、问题解决流程、建立支持团队等）。

## 3. 培训内部支持单位系统运维支持人员

解决内部支持单位一线/二线运维不能解决的问题，主要涉及配置问题、BUG 修复问题。

收集新增权限管理需求，并指导协助 XX 项目内部单位进行系统内调整或开发。

协助内部支持单位内部培训师组织用户再培训。

指导编写操作问题解决方法手册。

## 3. 系统维护计划

此流程包括系统的日常监测、系统备份及恢复策略、系统归档、系统用户创建/维护流程和系统安全管理等。

## 4. 长期维护和支持计划

用户在使用过程中会碰到各种各样的问题，这项计划为了使日常业务顺利进行，给用户提供一个寻求帮助机制。

## 5. 建立系统支持问题记录

对于系统支持阶段出现的问题，予以详细记录，为以后提高解决问题的速度和效率提供信息，为进一步的推广提供经验。

在质保期（支持维护期）内，我公司将提供以下的售后服务支持：

- （1） 进行系统缺陷修复；

- (2) 诊断并解决用户提出的问题或提供解决问题的方案；
- (3) 优化运维流程；
- (4) 传递运维知识；
- (5) 定位系统层面的问题；
- (6) 系统监控及运维报告编写；
- (7) 系统性能监控和调优建议编制

● **运维服务水平协议**

我公司对于 XX 项目提供售后技术支持的服务水平包括平均响应时间、平均问题解决时间、未关闭的事件数量、规定时限内解决问题的百分比等，这些指标的定义需要符合 XX 项目的 SLA 标准，而我公司将根据具体的 SLA 标准制定相应的 OLA。XX 项目对于服务水平的要求如下：

1) 我公司对系统问题进行以下几类级别的划分：

问题级别	级别描述及影响
问题级别 1	本项目系统的业务功能整体失效，或者某个模块体失效
问题级别 2	本项目系统部分关键业务功能失效
问题级别 3	本项目系统部分业务功能失效，其影响范围是 XX 项目或者部门（多于两家独立部门）
问题级别 4	本项目系统部分业务功能失效或者出现错误，其影响范围是个别 XX 项目或者部门（不多于两家）
问题级别 5	当前不影响应用环境或业务操作的问题，包括未

问题级别	级别描述及影响
	处理的潜在影响，或实际发生前已被解决问题

针对本项目系统新增功能及开发，将统一归入问题级别 5 的处理方式（反馈时间和方案提交时间）进行统计

## 2) 服务等级指标

服务等级	更新频率	建议指标
问题级别 1 - 反馈时间		100%问题 20 分钟内反馈
问题级别 2 - 反馈时间		100%问题 20 分钟内反馈
问题级别 3 - 反馈时间		100%问题 1 小时内反馈
问题级别 4 - 反馈时间		100%问题 2 小时内反馈
问题级别 5 - 反馈时间		100%问题 8 小时内反馈
问题级别 1 - 方案提交时间	1 小时	100%问题 1 小时内提交
问题级别 2 - 方案提交时间	2 小时	100%问题 2 小时内提交
问题级别 3 - 方案提交时间	4 小时	100%问题 4 小时内提交

服务等级	更新频率	建议指标
问题级别 4 - 方案提交时间	1 天	100%问题 1 天内提交
问题级别 5 - 方案提交时间	5 天	100%问题 5 天内提交

注：支持语言为中文

## ● 运维体系的组织

XX 项目需要建立适用于企业的运维机制以确保高质量的系统运行，在系统上线前，我公司就会为 XX 项目设计完整的系统运维体系，并在一年的运维期中帮助 XX 项目将体系逐步搭建和完善。

从我公司项目成功的运维经验来看，一个好的运维机制包括组织及人员、运维的流程和规章制度以及强大的运维管理工具和平台。

### 1) 组织及人员

通常由 IT 部门牵头建立项目的运维组织，由运维部门主管，精通技术的 IT 人员和既了解业务又对系统功能了解的关键用户组成，常见的组织及人员结构如下：

运维支持等级	运维角色	工作项
一级	技术支持客服	负责一线运维投诉电话，客户问题答疑和系统异常监控，创建问题工单并分配应用系统负责模块

运维支持等级	运维角色	工作项
一级	技术支持专家	负责提供一线运维客服专业技术解决方案支持
二级	关键用户	负责优化和维护实施方案, 维护系统中出现的功能问题
二级	运维主管	负责整体系统的运维管理和维护
二级	应用系统管理员	负责电子商务系统的管理和维护
二级	基础设施管理员	负责硬件、网络基础设施的管理
三级	技术人员	负责由问题工单产生的变更开发, 对应用系统进行的二次开发及维护
三级	技术测试人员	负责准备变更测试数据, 质量控制和管理

## 2) 流程及规章制度

建立完善严格的运维的流程及规章制度将大大提高运维的效率和运维的服务水平, 此部分内容需结合 XX 项目现有的 IT 管理的相关要求制定。常见的主要内容包括, IT 运维服务的质量指标, IT 基础设施运维服务、IT 应用系统运维服务、安全管理服务、网络接入服务、内容信息服务以及综合管理服务流程及制度。

## 3) 运维管理工具和平台

应用系统建设之后将转入运维阶段，在项目建设阶段就应该从应用软  
件系统整个生命周期去考虑。我公司提供的解决方案中提供用户一个全面  
的运维管理工具和平台。包括系统安装、系统配置、系统日常监控管理、  
系统诊断、系统复制、系统升级、技术基础平台管理、系统管理员技能培  
训。

系统厂商提供安装，自动化集成框架，应用部署管理器，应用程序响  
应度量众多管理工具和组件，提升整体运维的效果。

## ● 运维体系的人员安排

在 XX 项目本项目上线后，根据项目运维期的服务要求，我公司的实  
施顾问会免费提供为期一年的支持与服务。根据运维事件的等级和处理流  
程，必要时现场办公。

我公司会与 XX 项目在本项目的内部支持单位一起建立起技术支持体  
系，组织运维支持服务工作的交付，尤其在刚上线投产的阶段，将安排资  
源现场服务。

现场支持顾问的主要责任是：

1. 协同甲方的内部支持团队一起进行系统维护工作，并逐步移交工  
作职责；
2. 回答用户提出的关于系统功能和操作的问题；
3. 诊断系统错误和提出合适的解决方案；
4. 对系统出现的问题进行及时地解决，以保证新的系统能够在真实  
的运作环境下正常工作；

5. 对实施后的系统进行最终审核，以检查是否达到预计的目标。

- **项目应急方案**

- **突发事件应急措施**

一、突发事件应急流程

在日常运维中可能会出现突发事件，一旦出现如下问题我公司将遵循应急流程处理突发事件。

突发事件的来源，可能来自三个途径，第一巡检维护过程中发现、第二设备运行发生告警、业务部门反馈，一旦发生驻点工程师第一时间告知客户，并将具体的情况一同告知，以最快速度联系公司相关技术专家和公司相关高层领导，与专家进行充分沟通初步定为故障，并将故障定级，同时告知客户，如遇到驻点工程师无法解决的故障时，公司内相关领域技术专家会以最快速度赶到事故现场进行故障处理，直至问题解决，在问题解决之后。

由技术专家和驻点工程师共同完事件问题报告，将事故的发生原因，处理的方式，已及如何避免再次发生的方法进行详细记录，录入客户的运维管理文件中，同时由公司技术专家完成将此案例录入公司内部知识案例库，作为以后借鉴依据，当事故处理完毕后，由驻点工程师或技术专家讲结果告知客户和公司相关领导。

二、预防措施及处理办法

系统运维应急方案是对中断或严重影响业务的故障，如宕机、数据丢失、业务中断等，进行快速响应和处理，在最短时间内恢复业务系统，将

损失降到最低。在系统维护过程中，突发事件的出现将是很难完全避免的，针对这种情况，设计了完善的突发事件应急策略。

系统巡检人员要定期规范检查各硬件设备的运转情况和应用软件运行情况，同时做好日常的数据增量备份和定期全备份。对发现的问题在报各级负责人的同时，要协调相关资源分析问题根源，确定解决方案和临时解决措施，避免造成更大的影响。

问题得到稳定或彻底解决后，要形成问题汇报，避免以后类似重大紧急情况的发生。

对发现的问题在报负责人的同时，要协调相关资源分析问题根源，确定解决方案和临时解决措施，避免造成更大的影响。问题得到稳定或彻底解决后，要形成问题汇报，避免以后类似重大紧急情况的发生。

当获悉出现突发事件时，驻点工程师可以立即从知识库中获取相应的应急策略，并综合用户方的具体情况，与公司技术专家沟通，给出相关解决方案，然后在第一时间以电话、邮件支持或现场服务的方式帮助用户解决问题，尽最大努力减小突发事件对用户日常应用的影响。

## ● 运行服务应急方案

紧急故障应急措施应以快速恢复客户使用为目标，第一时间将客户使用状态恢复到正常，避免或尽量减少因故障而导致的损失。

### 一、启动应急流程

在问题管理流程中，当服务主管收到服务台人员或助理提交的《运维工作单》，并判断该问题属于重大事故时，则启动应急处理流程。

重大事故包括以下几种情况：

1. 大范围系统中断
2. 区域性系统崩溃
3. 关键业务中断
4. 大范围病毒爆发
5. 系统严重破坏
6. 数据严重破坏

根据重大事故的紧急程度和状态不同，服务主管可采取以下方式启动应急流程

（一）当紧急事件发生时，我公司的运行人员首先要进行故障分析，确定故障的范围和程度，确认为紧急故障的，在查找原因和解决问题的同时，要同步将故障解决情况通报给部门领导及向客服中说明事件发生的状况。如需其他部门协助的，需要请求相关部门共同尽快解决故障。

（二）对于病毒突发事件，当病毒大面积地感染终端，我公司的现场服务人员将已感染的终端从局域网中断开，我公司的运行人员将第一时间收集病毒信息，并向现场人员提供有针对性的应急方案；如果应急方案没有效果，要立即和杀毒软件厂方联络，由双方共同协同提供有效地应对措施。

（三）对于网络中断事件，我公司的运行人员首先要判断中断原因，如果是局域网本地设备或线路造成的，依网络运行处理流程优先快速处理；如果是电信服务提供商造成的，要立即联络电信技术部门解决问题。

（四）对于系统故障事件，我公司的运行人员首先要启用备用系统，

再判断故障类型：硬件损坏、操作系统故障、软件故障。硬件损坏的情况，首先向服务器供应商报障；操作系统故障多数情况都和硬件故障同时出现，处理方式相同；软件故障如果是购买的软件造成的，立即向软件厂商寻求技术支持；如果是公司自行开发的软件，立即向相关人员联系并排除故障。

（五）对于自然灾害性事件，运行管理人员要尽可能将设备转移到安全地带，将损失降低到最少。

（六）对于电力中断事件，由于机房多采用 UPS 防止断电带来的系统停机现象，在 UPS 还能供应电力期间恢复供电，对系统使用不会有影响；但遇到特殊情况导致供电部门在短期内不能恢复供电时，如有备用发电设备要启用备用发电设备供电，否则要关闭所有设备，确保突然断电造成设备损坏。

（七）在故障排除之后，运行管理人员要填写故障记录，如果故障是由于项目实施中存在的隐患造成的问题，具体操作请参见上层文件《网络系统维护管理指引》。故障记录汇总到“系统运行故障记录表”，重大事故由故障处理人填写故障报告。

## 二、成立应急小组

《启动应急流程申请单》获批准后（包括口头批准），由信息主管部门负责组建应急小组。

应急小组由多方人员组成，例如信息中心代表、运维部代表、服务主管、客户代表、供应商代表以及其他第三方人员等。

应急小组对发生的重大事故进行讨论分析并制定应急处理方案。

运维小组会根据实际人员需求情况从公司本部调配足够人员加入应急小组。

运维小组会根据实际需求情况从公司本部调配足够的资金以保障事件处理经费需求。

### 三、应急处理过程

1. 运维服务商根据应急小组制定的应急处理方案具体实施应急处理活动，并将实施过程和结果记录在《应急处理过程记录》中。涉及客户现场服务的应取得客户的签字确认。

2. 应急处理实施过程中涉及需要协调配合的工作由服务主管填写《资源申请单》，说明需要获得的资源、需要协调配合的工作等，经应急小组审批通过后由相关人员代表配合实施。

3. 应急处理实施过程中涉及需要采购的，由服务主管填写《资源申请单》，说明需要采购地产品名称、型号/规格/功能、厂商/供应商、费用等。《资源申请单》经应急小组审批通过后由运维工程师实施采购，并将采购过程和结果记录在《资源申请单》中，应急小组对采购结果进行确认。

4. 应急处理实施过程中涉及需要变更的，由服务主管填写《变更请求表》，说明变更内容、变更原因、变更方案等，经应急小组批准后直接由运维工程师根据《变更请求表》中的变更方案实施变更，并将变更过程和结果记录在《变更日志》中。

5. 所有应急处理活动均应记录在《应急处理过程记录》中。具体涉及网络紧急故障处置，我们以恢复使用为第一目标。

(1) 在确认设备故障情况下，将第一时间采用备机备件恢复网络功

能；

(2) 在链路故障情况下，启动备用链路进行通讯恢复，并积极配合链路运营商恢复链路；

(3) 在大面积病毒爆发情况下，利用趋势病毒爆发阻止功能，首先阻止网络病毒传播途径，阻止病毒源，并积极联系厂商获取最新病毒码对全网进行病毒处置。

#### 四、应急处理结果评估

应急处理过程完成后，服务主管向应急小组提交应急处理过程相关表单，包括《启动应急流程申请单》、《应急处理过程记录》、《资源申请单》、《变更请求表》、《变更日志》等。应急小组对应急处理结果进行评估和确认，并在《应急流程评估单》中填写评估意见。

如果应急小组评估意见为达到要求（即问题得到解决并恢复服务），则应急流程结束。

如果应急小组评估意见为未达到要求，则由应急小组讨论分析原因，根据分析结果可采取以下措施：

1. 如果需要继续进行应急处理，则由应急小组提出应急处理方案，进行应急处理过程；

2. 如果不需要继续进行应急处理：

(1) 如果有新的问题产生，则由服务主管填写《运维工作单》，转问题管理流程处理；

(2) 如果有新的变更需求，则由服务主管填写《变更请求单》，转变更管理流程处理；

(3) 否则应急流程结束。

应急流程结束时，由服务主管在《运维工作单》中记录应急处理结果及关联表单编号。配置管理员对应急处理结果进行检查，登记新的配置项或更改后的配置项。

## 五、统计和报告

由助理每月或每季度对应急流程情况进行统计，形成《应急流程管理报告》，并提交给服务主管。

《应急流程管理报告》内容包括：启动应急流程次数（不同类别的次数）、原因分析、影响分析、完成情况、所需时间、各项资源利用情况、费用情况、意见和建议等。

《应急流程管理报告》经服务主管确认后提交数据部。

## ● 组织体系与职责

应急组织体系由应急响应领导小组、应急响应调查处置小组、应急响应日常运行小组、应急响应协调小组及专家组组成。

### （一）应急响应领导小组

主要由公司网络安全与信息化领导小组部分成员、领导小组办公室主要负责人构成。

应急响应领导小组主要职能包括：

1. 启动和终止特别重大应急预案；
2. 组织、指导和指挥特别重大和重大安全事件的应急响应工作；
3. 审核安全事件处理和分析报告；

4. 指导应急预案的宣传和教育培训；
5. 外部媒体沟通及安全事件信息发布。

## （二）应急响应协调小组

主要由项目负责人、网络安全管理人员、机房管理人员、运维人员以及安全服务技术人员组成，由信息中心主要负责人任组长。

应急响应协调小组主要职能包括：

1. 启动和终止重大事件和较大事件应急预案；
2. 组织、指导和指挥较大事件的应急响应工作；
3. 传达应急响应领导小组信息指令，上报事件应急处理进度；
4. 组织、协调相关技术支持人员、关联单位和各应急小组及时到场开展应急处置工作；
5. 安全事件处理和分析报告以及其他发布资料的审核与上报；
6. 起草和修订应急预案，并定期组织专家对应急预案进行研究、评估；
7. 制订应急预案培训及演练方案，组织开展应急预案培训及应急演练；
8. 如有必要，在处理网络安全应急事件时配合 XX 项目和 XX 项目进行调查取证，为后期责任追查提供有力证据。

## （三）专家组

主要由网络安全与信息化领导小组成员、信息中心主要负责人以及网络安全行业专家组成，由网络安全与信息化的分管领导任组长。

专家组主要职能包括：

1. 提供安全事件的预防与处置建议；

2. 在制定网络安全应急有关规定、预案、制度和项目建设的过程中提供参考意见；

3. 定期对应急预案进行评审，及时反映网络安全应急工作中存在的问题与不足，并提出相关改进建议；

4. 对网络安全事件发生和发展趋势、处置措施、恢复方案等进行研究、评估，并提出相关改进建议。

5. 指导网络安全事件应急演练、培训及相关教材编审等工作。

#### （四）应急响应调查处置小组

主要由机房管理人员、业务应用运营人员、运维人员以及安全服务技术人员组成，由信息中心机房管理人员任组长。

应急响应调查处置小组主要职能包括：

1. 应急响应过程中技术问题的解决；
2. 及时向应急响应协调小组报告进展情况；
3. 制定信息安全事件技术应对表，明确职责和沟通方式；
4. 分析事件发生原因，提出应用系统加固建议；
5. 评估和总结应急响应处置过程，提供应急预案的改善意见。

#### （五）应急响应日常运行小组

主要由运维人员组成，由运维负责人任组长。

应急响应日常运行小组主要职能包括：

1. 对系统进行日常监控，及时预警，尽早发现安全事件；
2. 启动和终止一般事件应急预案；
3. 及时向应急响应协调小组汇报事件的发生时间、影响范围、事态发

展变化情况和处置进展等情况；

4. 现场参与和跟踪安全事件的应急处置过程；

5. 定期核查应急保障物资，特别是冗余设备的状态，保证事件发生时应急保障物资的正常使用。

## ● 预防工作

### （一）宣传、教育和培训

将突发信息网络事件的应急管理、工作流程等列为培训内容，增强应急处置能力。加强对突发信息网络事件的技术准备培训，提高技术人员的防范意识及技能。信息中心负责人每年至少开展一次信息网络安全教育，提高信息安全防范意识和能力。

### （二）应急演练

信息中心负责人每年定期安排演练，建立应急预案定期演练制度。通过演练，发现和解决应急工作体系和工作机制存在的问题，不断完善应急预案，提高应急处置能力。

### （三）重要活动期间的预防措施

在国家重要活动、会议期间，着重加强网络安全事件的防范和应急响应，及时预警可能造成重大影响的风险和隐患，确保网络安全。

## ● 应急响应

### （一）基本响应

网络安全事件发生后，应立即启动应急预案，实施处置并及时报送信息。

1. 控制事态发展，防控蔓延。先期处置，采取各种技术措施，及时控制事态发展，最大限度地防止事件蔓延。

2. 快速判断事件性质和危害程度。尽快分析事件发生原因，根据网络与信息系统运行和承载业务情况，初步判断事件的影响、危害和可能波及的范围，提出应对措施和建议。

3. 及时报告信息。在先期处置的同时要按照预案要求，及时向上级主管部门报告事件信息。

4. 做好事件发生、发展、处置的记录和证据留存。

## （二）事件上报

### 1. 上报原则

当判定为发生特别重大事件（Ⅰ级）和重大事件（Ⅱ级）时启动完整上报流程。

### 2. 上报流程

#### （1）事件认定

由应急响应日常运行小组和应急响应调查处置小组的专业技术人员确定发生信息安全事件的系统受影响的程度，初步判定事件原因，并对事件影响状况进行评估。

#### （2）事件上报

应急响应协调小组负责填写《重大网络安全事件报告表》后上报给应急响应领导小组。

应急响应领导小组组长按照事件级别决定是否向网络安全与信息化领导小组组长报告，并决定是否通知和协调国家安全局、公安厅网络安全

保卫总队、网信办或通信管理局协助妥善处理信息安全事件。

### （三）分级响应

#### 1. I 级响应

I 级响应由应急响应领导小组启动，并向网络安全与信息化领导小组组长报告，其他各应急响应小组在应急响应领导小组的统一指挥下，开展应急处置工作。

##### （1）启动应急体系。

应急响应领导小组组织专家组专家、应急响应协调小组、应急响应日常运行小组和应急响应调查处置小组的专业技术人员研究对策，提出处置方案建议，为领导决策提供支撑。

##### （2）掌握事件动态。

事件影响部门及时告知事态发展变化情况和处置进展情况，应急响应日常运行小组在全面了解信息系统受到事件波及或影响情况后，汇总并上报应急响应协调小组。

#### 2. II 级响应

II 级响应由应急响应协调小组启动，并报应急响应小组，其他各应急响应小组在应急响应领导小组的统一指挥下，开展应急处置工作。

##### （1）启动应急体系。

应急响应领导小组组织专家组专家、应急响应协调小组、应急响应日常运行小组和应急响应调查处置小组的专业技术人员研究对策，提出处置方案建议，为领导决策提供支撑。

##### （2）掌握事件动态。

事件影响部门及时告知事态发展变化情况和处置进展情况，应急响应日常运行小组在全面了解信息系统受到事件波及或影响情况后，汇总并上报应急响应协调小组。

### 3. III级响应

III级响应由应急响应协调小组启动，其他各应急响应小组在应急响应协调小组的统一指挥下，开展应急处置工作。

#### (1) 启动应急体系。

应急响应协调小组组织应急响应日常运行小组和应急响应调查处置小组的专业技术人员研究对策，提出处置方案建议。

#### (2) 掌握事件动态。

事件影响部门及时告知事态发展变化情况和处置进展情况，应急响应日常运行小组在全面了解信息系统受到事件波及或影响情况后，汇总并上报应急响应协调小组。

### 4. IV级响应

IV级响应由应急响应日常运行小组启动，并开展应急处置工作。

#### (1) 启动应急体系。

应急响应日常运行小组组织应急响应调查处置小组的专业技术人员研究对策，组织应急处置工作。

#### (2) 掌握事件动态。

事件影响部门及时告知事态发展变化情况和处置进展情况，应急响应日常运行小组全面了解信息系统受到事件波及或影响的情况。

#### (四) 现场应急处置

## 1. 处置原则

(1) 当发生水灾、火灾、地震等突发事件时，应根据当时的实际情况，在保障人身安全的前提下，首先保障数据的安全，然后保障设备安全。

(2) 当人为或病毒破坏信息系统安全时，按照网络安全事件发生的性质可采取隔离故障源、暂时关闭故障系统、保留痕迹、启用备用系统等措施。

## 2. 处置流程

(1) 事件认定。收集网络安全事件相关信息，识别事件类别，判断破坏的来源与性质，确保证据准确，以便缩短应急响应时间。

(2) 控制事态发展。抑制事件的影响进一步扩大，限制潜在的损失与破坏。

(3) 事件消除。在事件被抑制之后，找出事件根源，明确响应的补救措施并彻底清除。

(4) 系统恢复。修复被破坏的信息，清理系统，恢复数据、程序、服务，恢复信息系统。把所有被破坏的系统和网络设备还原到正常运行状态。恢复工作中如果涉及敏感数据资料，要明确数据资料保管责任人，资料接触人员要严格保密，做好敏感数据资料的防泄漏工作。

(5) 事件追踪。关注系统恢复以后的安全状况，特别是曾经出现问题的地方；建立跟踪档案，规范记录跟踪结果；对进入司法程序的事件，配合国家相关部门进行进一步的调查，打击违法犯罪活动。

### (五) 应急终止

#### 1. 应急终止的条件

现场应急处置工作在事件得到控制或者消除后，应当终止。

## 2. 应急终止的程序

(1) 应急响应领导小组决定终止应急，或其他应急响应小组提出，经应急响应领导小组批准；

(2) 应急响应领导小组向组织处置事件的各应急响应小组下达应急终止命令；

(3) 应急状态终止后，应急响应领导小组应根据 XX 项目统一安排和实际情况，决定是否继续进行环境监测和评价工作。

## ● 信息管理

### (一) 信息报告

各应急响应小组和部门根据各自职责分工，及时收集、分析、汇总本部门或本系统网络与信息系统安全运行情况信息，安全风险及事件信息及及时报告应急响应协调小组，由应急响应协调小组汇总后上报应急响应领导小组。

倡导社会公众参与网络、网站和信息系统安全运行的监督和信息报告，发现网络、网站和信息系统发生安全事件时，应及时报告。

发生 I 级、II 级网络安全事件后，应由应急响应协调小组及时填报《重大网络安全事件报告表》，并在应急事件终止后填报《重大网络安全事件处理结果报告》。

发生 III 级、IV 级网络安全事件并处置完成后，应由应急响应日常运行小组及时填报《网络安全事件故障分析处置报告》。

## （二）信息报告内容

信息报告内容一般包括以下要素：事件发生时间、发生事故网络信息系统名称及运营使用管理单位、地点、原因、信息来源、事件类型及性质、危害和损失程度、影响单位及业务、事件发展趋势、采取的处置措施等。

## （三）信息发布和新闻报道

发生 I 级网络安全事件后，需要开展情况公告时，应由网络与信息化领导小组负责外部媒体沟通及安全事件信息发布，正确引导舆论导向。

发生 II 级网络安全事件后，需要开展情况公告时，应由应急响应领导小组负责外部媒体沟通及安全事件信息发布，正确引导舆论导向。

## ● 后期处置

### （一）系统重建

在应急处置工作结束后，应制定重建方案，尽快抢修受损的基础设施，减少损失，尽快恢复正常工作。

### （二）应急响应总结

响应总结是应急处置之后应进行的工作，由应急响应调查处置小组负责，具体包括：

1. 分析和总结事件发生的原因；
2. 分析和总结事件发生的现象；
3. 评估系统的损害程度；
4. 评估事件导致的损失；
5. 分析和总结应急处置过程；

6. 评审应急响应措施的效果和效率，并提出改进建议；
7. 评审应急响应方案的效果和效率，并提出改进建议；
8. 评审应急过程中是否存在失职情况，并给出处理建议；
9. 根据事件发生的原因，提出应用系统加固改进建议。

## ● 保障措施

### （一）装备、物资保障

建立应急响应设备库，包括信息系统的备用设备、应急响应过程所需要的工具。由应急响应日常运行小组进行保管，每季度进行定期检查，确保能够正常使用。

### （二）技术保障

#### 1. 应急响应技术服务

技术保障由应急响应调查处置小组负责，该小组应制定信息安全事件技术应对表，全面考察和管理技术基础，选择合适的技术服务人员，明确职责和沟通方式。

#### 2. 日常技术保障

日常技术保障包括事件监控与预警的技术保障和应急技术储备两部分。

##### （1）事件监控与预警的技术保障

由应急响应日常运行小组采取监控技术对整个系统进行安全监控，及时预警，尽早发现安全事件。

##### （2）应急技术储备

由应急响应协调小组分析应急过程所需有的各项技术，针对各项技术形成培训方案或操作手册，定期进行交流、演练。确保各应急技术岗位人员分工清晰，职责明确。

### （3）应急专家储备

由应急响应协调小组定期组织和外部专家或技术供应商进行应急处理预案和技术的交流。

### （三）责任与奖惩

1. 网络安全事件应急处置工作实行责任追究制。

2. 对网络安全事件应急管理工作中做出突出贡献的先进集体和个人给予表彰和奖励。

3. 对不按照规定，迟报、谎报、瞒报和漏报网络安全事件重要情况或者应急管理工作中有其他失职、渎职行为的，依照相关规定对有关责任人给予处分；构成犯罪的，依法追究刑事责任。

