# 7 实施保障方案

根据《政务信息系统密码应用与安全性评估工作指南（2020版）》、《GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求》，结合信息系统的实际情况，项目预算及拟采购的密码产品，落实第5章密码应用技术方案和第6章密码安全管理方案，从实施内容、实施计划、保障措施三个方面设计实施保障方案，保障目标信息系统顺利、成功进行密码应用改造。

## 7.1 实施内容

目标信息系统密码应用的实施内容包括软硬件开发及改造、系统集成、综合调试、试运行、最终验收、风险点及应对措施六个方面。

### 7.1.1 软硬件开发及改造

按照采购内容和目标信息系统密码应用改造要求，对采购的密码软硬件进行定制开发和改造，以符合实现项目需求。

表7.1 定制开发任务表

|  |  |  |  |
| --- | --- | --- | --- |
| 指标要求 | 开发任务 | 信息系统模块 | 对接密码产品 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

### 7.1.2 系统集成

目标信息系统，通过集成密码产品中间件，业务应用系统提供密码服务和身份认证服务。

密码安全应用贯穿业务始终，即从传输链路、身份鉴别、数据加密、电子签名、数据完整性保护等方方面面。例如在用户在与服务端之间通信时，通过安全网关建立加密通道、数据进行存储时以密文的形式存储、对访问控制策略信息进行HMAC运算和校验、对用户操作行为使用用户的证书进行签名/服务端发出的数据可以由应用系统自身的数字证书进行签名等，充分保证了应用系统的使用安全。

### 7.1.3 综合调试

系统集成完成后，密码软硬件产品上架部署后，进行统一的综合调试，串通整体业务流程和密码应用流程。

### 7.1.4 试运行

系统移交买方后即进入试运行阶段，试运行时间为1个月，试运行期间卖方负责解决问题清单中的遗留问题，进一步完善系统，并且在此过程中，卖方应提供完善的监护服务。

试运行结束后，由卖方负责起草《试运行报告》，经双方确认并签署。

### 7.1.5 最终验收

系统在试运行期结束后进行工程终验，需由卖方提出终验书面申请，且买方需在收到卖方终验申请后10个工作日内组织工程终验。若10日内买方没有响应或无正当理由推迟，则视为系统通过终验。

测试项目一般同初步验收测试相同，考虑到测试进度的因素，系统终验可以只对对初验遗留的问题进行测试验证，对初验通过的免予测试。验收通过后，卖方应提供相应的工程文档，工程文档应包括：系统详细配置说明书、软件安装测试记录、使用及维护说明书、所有软件的文档等。

终验通过后，由卖方负责起草《系统终验合格证明》，经双方确认并签署。

### 7.1.6 风险点及应对措施

风险管理贯穿于整个项目实施过程，通过制定项目实施过程的风险管理计划，并在项目各生命周期阶段开始时进行相应的评估，在项目实施过程中持续进行风险识别、监控、处理，最终把实施阶段的风险控制在可以接受的范围。本项目实施和运行过程中主要存在的风险包括：

1. 外部风险分析及对策

外部风险主要是由于外部不可控因素造成的风险。一般将不可控制的“不可抗力”不作为风险因素处理，这些事件往往采用灾难防御措施。对于此项目，要做好在政策法规、外部资源、技术等方面的风险防范。

项目中的外部风险主要包括如下几类：

* 1. 外部资源风险

**外部资源风险：**由于外部资源因某种原因无法按计划配置，导致总体进度受到影响，如承包商无法按原计划完成项目软硬件建设、项目实施时与原应用开发商无法对接等情况。

**风险对策：**尽早识别关键性的外部资源，与资源的提供方进行沟通，并提前配置或增加足够的备份方案。通过招标方式，选择具备资质、有类似项目实施经验的软硬件承包商，深入了解各个软硬件建设方案的优缺点及应急措施；对于关键性数据，需明确其来源，并尽快安排与应用开发商进行沟通协调。

* 1. 标准风险

**标准风险：**国家和行业出台了新的业务标准或技术标准，与项目所执行的标准不一致，导致前期的规划失效。

**风险对策：**严格按照国家出台的相关标准制定系统建设框架，制定项目的业务标准和技术标准，符合密码发展的趋势。

**在标准设定时：**严格按照调研、需求分析、审核、征询建议、整合、征询建议、审核、标准制定、备案、更新现有标准体系、产生新版本的标准规范、对旧版本的标准规范存档、发布新标准的流程进行。

1. 内部风险分析及对策

内部风险主要是项目实施过程中，由于组织管理缺失、项目管理不当所导致的项目无法顺利开展的风险。充分地认识、正确地处理内部风险将会是保证项目最终成功的关键。

项目中的内部风险主要包括如下几类：

* 1. 组织风险

**组织风险：**组织风险主要指组织内部成员对目标未达成一致，管理高层对项目不重视，加上工程参与人员知识与技能欠缺、团队合作精神不足、人员激励机制不当等因素导致建设队伍不稳定，与其它项目存在资源冲突等。

**风险对策：**本次项目充分考虑到了项目中的组织风险，根据信息化系统的建设要求，在充分论证的基础上完善信息化建设项目的完整架构，保证信息化建设项目的正常运转，包括部门设置、岗位确定、职责落实、人员配备、制度建立等内容，将有效地保障目标信息系统项目建设中避免组织风险的发生。

* 1. 管理风险

**管理风险：**管理风险主要包括项目管理的基本原则使用不当，如计划草率、质量差、进度和资源配置不合理等。

**风险对策：**为确保项目管理的高效率，本项目建设领导小组将对项目建设方案进行有效策划，制定并落实严格的项目实施具体计划，应用先进管理工具和方法论提高进度计划管理、跟踪水平。借鉴同行业项目管理的实际经验，合理估算项目工作量，明确项目间依赖关系和先后顺序，突出关键项目，进一步分解项目工作任务，使每个里程碑阶段均应有工作量估算、时间进度，以及可操作、可管理、可检查的阶段性交付物。

为了避免在项目建设过程中对实施方的管理、协调不力，项目建设领导小组将制订统一的标准、流程和规范，并加强全过程的质量控制，在招标书、合同等文件中明确服务商应遵循的质量管理体系，明确项目工作范围，明确系统边界、需求、约束等前置条件。选择具备资质的监理单位，对项目实施过程中的工程招标、工程设计、工程实施、工程验收等项目建设全过程的进度、质量、投资、变更等行为进行监督和管理。

## 7.2 实施计划

目标信息系统密码应用的实施计划包括实施路线图以及进度计划两个方面。

### 7.2.1 实施路线图

根据本项目的需求，编制《项目建设实施方案》，组织专家进行评审论证，并报领导小组备案，报请用户批准；在《项目建设实施方案》被批准后，将严格按照实施方案、时间进度要求，组织工程建设，完成工程建设任务，组织工程验收，系统投入运行。

本项目具体实施主要包括以下几个步骤：

1. 组建项目实施团队；
2. 制定实施计划、编制《项目建设实施方案》；
3. 项目实施安装，进行软硬件的安装与调试；
4. 项目培训；
5. 系统试运行与交付；
6. 系统正式运行；
7. 日常运维。

### 7.2.2 进度计划

本项目主要阶段实施工作分解如表7.2所示：

表7.2 阶段实施工作分解表

|  |  |  |
| --- | --- | --- |
| 时间计划 | 工作阶段 | 工作内容 |
|  | 需求调研分析 | 根据需求调研计划，结合前期需求调研情况，针对信息系统的国产密码应用情况进行详细调研，并形成关于国产密码应用的《需求规格说明书》和《需求确认书》。 |
|  | 安全方案设计 | 基于用户单位建设方案及实际情况，设计密码系统部署、密码系统与应用对接、网络拓扑、安全防护机制和备份恢复机制等，确定设备配置，拟定详细建设方案。 |
|  | 项目准备启动 | 熟悉项目前期所形成的资料，制定项目实施计划，确定项目组织架构及人员，成立项目管理办公室，制定项目启动会议计划，召开项目启动会议。 |
|  | 项目研发 | 项目详细方案评审通过后，密码厂商即刻展开密码系统功能详细设计，按系统功能，进行相应模块的开发，并形成《详细设计说明书》。 |
|  | 项目测试 | 针对项目实施内容，编制产品测试方案、密码系统产品与改造后信息系统的联调测试、编制测试评估报告  项目试运行：测试完成通过进入项目试运行阶段，在试运行阶段遇到问题密码厂商需及时解决并对问题进行记录，形成问题知识库。 |
|  | 培训与交付 | 为项目用户单位编写技术参数手册和工程安装手册。编写培训方案，对试点信息系统相关人员进行全面的技术和运维培训，并生成培训记录和反馈。 |
|  | 密码测评 | 在建设完成后，通过密码测单位进行密码测评，并出具测试报告 |
|  | 项目试运行 | 进行系统试运行 |
|  | 项目验收 | 制定验收方案并完成系统验收工作 |

## 7.3 保障措施

目标信息系统平台密码应用的保障措施包括组织保障、人员保障、经费保障、质量保障四个方面。

### 7.3.1 组织保障

1. 组织架构

本项目实施过程中，组织一整套的开发、工程人员，组建专业的研发、工程施工和服务队伍，力求为该项目提供最为完善的工程支持，项目的组织架构如图 7.1所示。

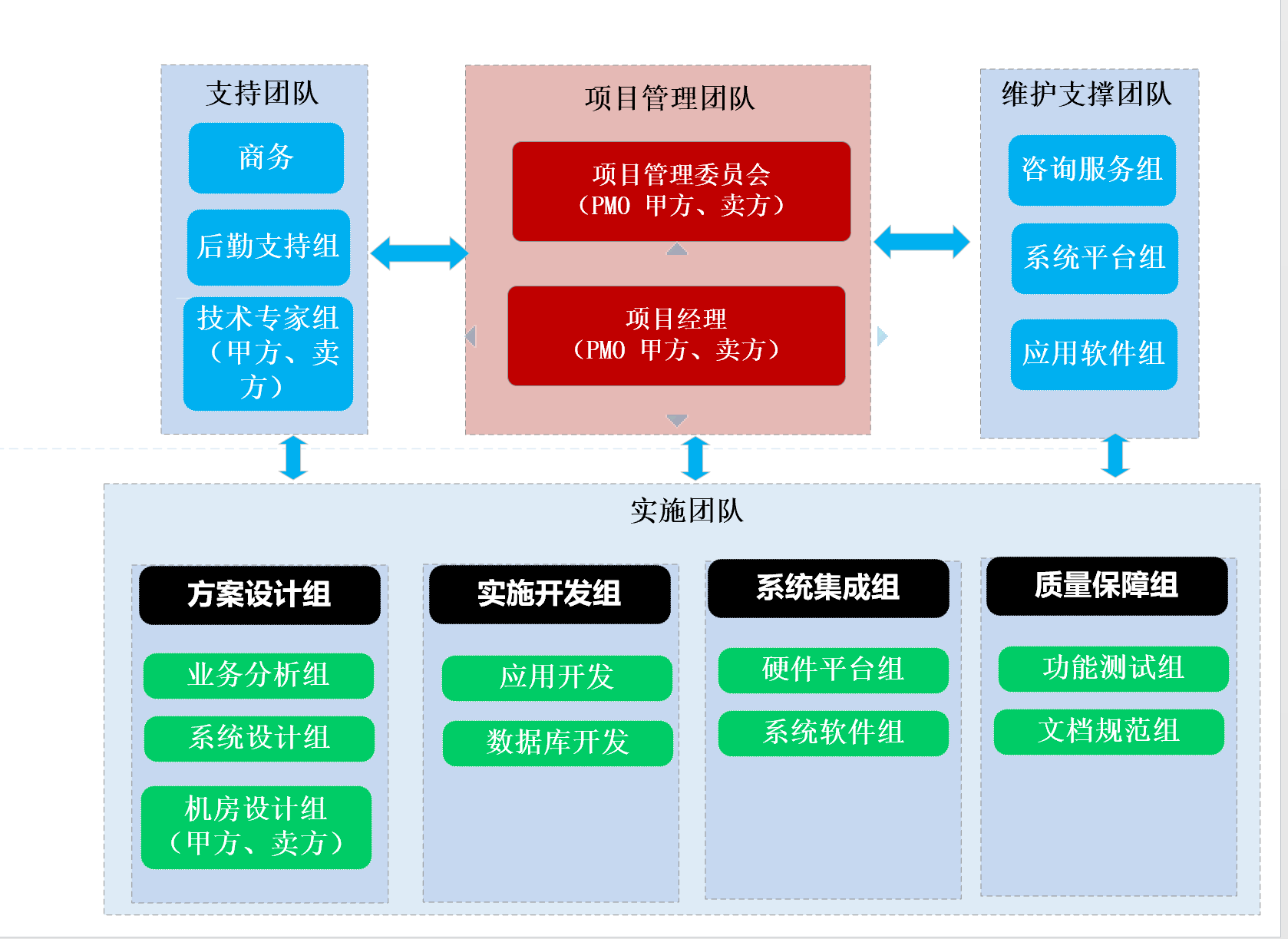


图 7.1 组织架构图

1. 项目管理团队

项目管理团队负责对项目进度、工程质量进行宏观管理，提供对项目出现的重大问题进行协调和指导，完成重要阶段评审，与项目内外部人员及合作方进行沟通，确保项目顺利成功实施。

项目管理团队包括以下角色：

* 1. 项目管理委员会：负责从商务角度对项目发展方向、管理策略、资源调配等进行决策，并有权任免以下层次人员组成。管理委员会成员由甲方、卖方人员组成；
  2. 项目经理：负责从项目运作角度协调管理，支持项目实施团队工作，向管理层汇报，对项目成败负责。项目经理成员由甲方、卖方人员组成。

1. 实施团队

实施团队负责系统平台集成和建设实施，对于项目最终产出提交物负责。

实施团队包括以下角色：

* 1. 方案设计组：对系统的建设进行设计规划，包括了业务分析设计和系统分析设计两部分。
  2. 业务分析组：负责收集、分析、汇总用户需求，与系统设计组及实施开发组配合工作；
  3. 系统设计组：负责从系统架构和技术选型角度进行分析设计，建立系统逻辑模型，从而指导实施开发组工作；
  4. 机房设计组：配合买方负责对整体机房做整体建设设计，输出建设图纸。
  5. 实施开发组：负责从系统实施角度进行代码开发，完成软件模块的开发、修改和整合。
  6. 应用开发组：负责除数据库开发外的代码开发内容，包括界面操作逻辑、业务逻辑和接口等；
  7. 数据库开发组：负责对数据库操作部分的开发实施工作，对应用开发组予以技术支持。
  8. 系统集成组：负责设备平台的架设、安装、调试，同时将开发完成的软件有效的集成发布在测试、生产环境，并确保调试通过。
  9. 硬件平台组：负责设备平台的架设安装及调试工作；
  10. 系统软件组：负责系统软件及第三方软件的发布和调试，并配合实施开发组对开发完成的应用在测试和生产环境进行发布，并确保调试通过；
  11. 机房建设组：配合买方对机房建设提供必要的支持。
  12. 质量保障组：负责从质量管理角度，定制适合本项目应用的工作流程，同时定期实施质量审核，以确保整个项目的质量水平。
  13. 功能测试组：负责对整个系统进行软硬件测试，完成测试文档，并及时将所发现的问题向有关的部门通报；
  14. 文档规范组：负责汇总并整理相关工程技术文档，提交有关责任人审核通过，同时管理各类技术规范和资料库，支持项目其他团队工作。

1. 维护支撑团队

维护支撑团队负责系统的维护优化，并保证生产环境的正常工作。同时，维护支撑团队也面向用户提供咨询、培训和技术支持。

维护支持团队包括以下角色：

* 1. 咨询服务组：就系统运行维护相关的主题，提供各类咨询服务以及培训支持；
  2. 系统平台组：从设备平台的角度提供运行维护支持，以及有关系统的性能调优；
  3. 应用软件组：从应用软件的角度提供运行维护支持，以及相关功能的优化开发。

1. 支持团队

支持团队负责提供与本项目相关的外部支持，包括了商务合作、后勤保障、专家咨询等。支持团队包括以下角色：

* 1. 商务合作部：负责落实与项目相关的商务运作，主要包括设备订购。跟踪设备的到货情况，确保设备按期、准确、全部到达。同时，也可对客户提出的其他商务合作要求提供支持；
  2. 后勤支持组：负责整个项目的后勤支持，安排项目人员的工作环境和起居安排，减少项目组的无效投入；
  3. 技术专家组：从技术角度对整个项目提供支持，制定并审核本项目中的技术实施方案，解答技术问题，处理工程中出现的技术难点，必要时组织团队进行技术攻关。技术专家组成员由甲方、卖方人员组成。

### 7.3.2 人员保障

为确保项目的顺利开展、实施和运维，严格按照7.3.1设置的组织结构组织项目组人员，并按照一定的比例设置AB角。

### 7.3.3 经费保障

由项目建设方负责本项目资金的筹措和分配实施，详见7.4经费概算。

### 7.3.4 质量保障

1. 建立软件质量保证活动的实体

建立软件质量保证小组，软件质量保证小组在整个软件生命周期中应评审项目的活动并审计软件工作产品，使管理层能观察到软件项目是否遵从已建立的计划、标准和规程。并应指出在该软件项目中的问题：如果可能，则应及时解决；如果不能解决，则应提交到适当的管理层解决。

1. 制订软件质量保证计划

SQA计划应在整个项目的早期制订，并应与整个项目计划平行开发。 此计划包括：

* 1. SQA小组的职责和权利。
  2. SQA小组的资源需求（包括人员，工具及设施）。
  3. 该项目的SQA小组活动的进度安排和经费。
  4. SQA小组参与建立该项目的软件开发计划、标准和规程。
  5. 由SQA小组进行评估的内容。
  6. 由SQA小组指导的审计和评审。
  7. SQA小组在评审和审计时引用的项目标准和规程。
  8. 记录和跟踪不协调事项直至解决的规程。
  9. 要求SQA小组生成的文件。
  10. 为软件工程小组和其他软件相关小组提供SQA活动反馈信息的方法和频率。

1. 坚持各阶段的评审和审计，并跟踪其结果作合适处理
   1. 评审：包括里程碑活动评审、基线评审、SCM评审、SQA工作评审。
   2. 审计：包括基线审计、SQA审计。

有背离之处，则对其进行标识、记录、并跟踪直至其符合。

1. 监控软件产品的质量
   1. 对软件产品的验收
   2. 把握采购软件的质量
   3. 监控分承包商的软件质量保证工作
2. 采集软件质量保证活动的数据
   1. 记录不协调事项
   2. 跟踪不协调事项直至解决
   3. 收集各阶段的评审和审计情况
3. 度量软件质量保证活动
   1. 测量的目的是为了判断SQA活动的成本和进度状态；
   2. 与其计划相比，SQA活动完成的里程碑数；
   3. 在SQA活动中完成的工作，花费的工作量及支出的费用；
   4. 与其计划相比，产品审计和活动评审的次数。
4. 软件质量保证管理流程

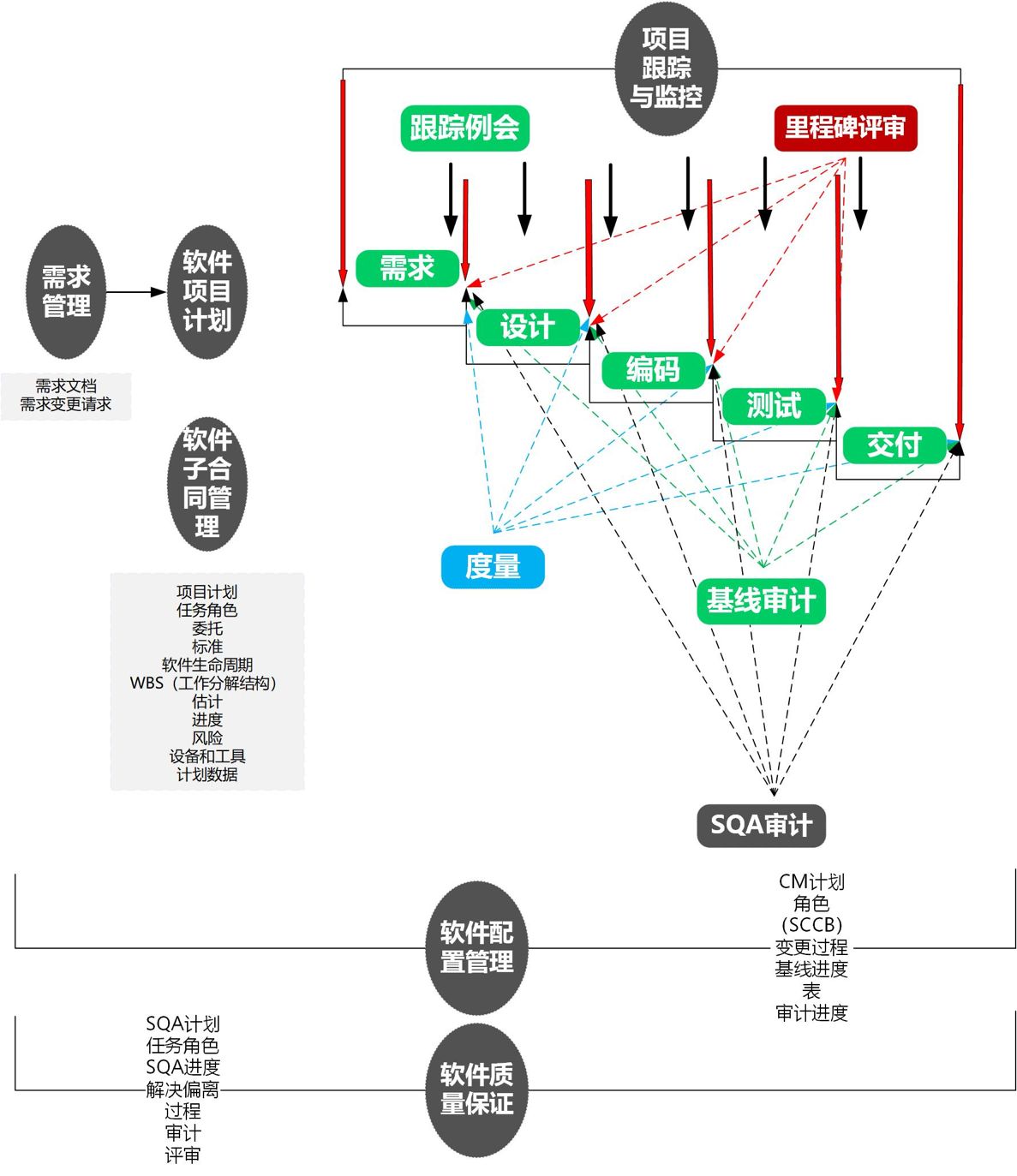


图 7.2 软件质量保证管理流程图

软件质量保证管理流程如图 7.2所示，首先设定需求管理和软件项目计划，依次从需求、设计、编码、测试、交付五个阶段展开项目跟踪与监控，监控软件产品的质量，采集软件质量保证活动的数据；同时坚持各阶段的评审和审计，并跟踪其结果作合适处理，有背离之处，则对其进行标识、记录、跟踪直至其符合。