解决方案实践

Thoughtworks DevSecOps 服务解决方案实践

文档版本 1.0

发布日期 2024-01-16

华为技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

安全声明

漏洞处理流程

华为公司对产品漏洞管理的规定以“漏洞处理流程”为准，该流程的详细内容请参见如下网址：
https://www.huawei.com/cn/psirt/vul-response-process
如企业客户须获取漏洞信息，请参见如下网址：
https://securitybulletin.huawei.com/enterprise/cn/security-advisory

目 录

1 方案概述

应用场景

DevSecOps的概念最早于2012年被Gartner分析师首次提出。最近几年，随着对软件研发质量与效能的重视，大型企业对DevSecOps引入占比逐年递增。然而，企业在引入DevSecOps时候，往往遇到以下的挑战：

- 缺乏明确的软件研发目标，并没有明确的优先级和战略规划；
- 需求不明确、导致团队在开发过程中频繁变更需求，增加了开发时间和成本，并降低了交付的质量；
- 缺乏有效的绩效度量和反馈机制，无法准确评估和改进软件研发效能。

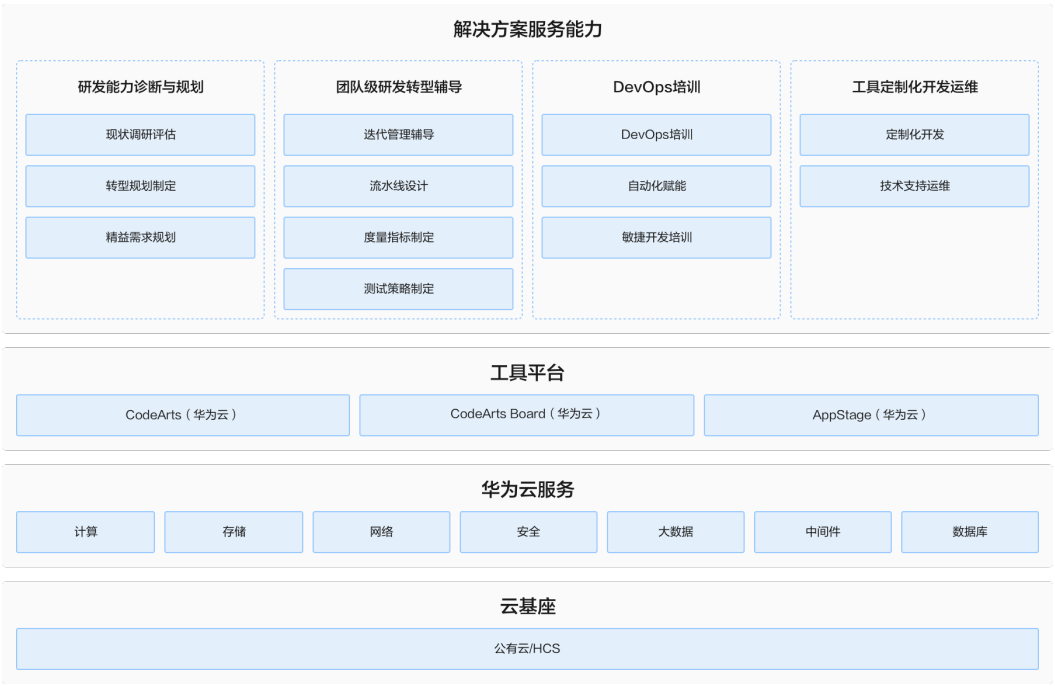
围绕这些挑战， DevSecOps服务解决方案，以华为云基座为基础，结合华为云工具平台，提供专业的DevSecOps咨询服务，指导落地DevSecOps，助力企业转型。

方案架构

方案主要由华为云计算底座+工具平台+专业咨询服务形成面向企业DevSecOps转型全流程的专业服务方案：

- 华为云计算底座作为方案的核心组成部分，提供了强大的云计算基础设施和先进的工具支持；
- 工具平台提供需求管理、代码管理、持续集成、持续交付、自动化测试、安全审计等能力，企业可以快速响应市场需求，提供高质量的软件产品；
- 专业服务结合工具平台提供的能力，为企业提供全方位的咨询支持，帮助企业制定符合实际情况的DevSecOps转型策略和规划，并实施落地。

图 1-1 业务架构



方案优势

- **成功的商业实践：**持续为多个业界头部客户提供服务，项目规模达千万级，涵盖零售、金融、汽车等核心领域
- **团队专业能力：**经过华为云认证的专业人员50多位，DevSecOps咨询服务团队超过100人，专业的售前团队成员超过15人。各团队具备深入行业的洞察力和技术知识，能够与客户紧密合作。
- **服务场景完整：**熟练掌握华为云CodeArts、Board等关键平台产品，支持包括研发诊断、转型规划、实施，赋能等，全面满足研发转型的诉求。

2 资源和成本规划

以某行业客户为例，客户下单一套标准的DevSecOps服务，设计以下的资源与成本清单。实际收费应以账单为准：

表 2-1 云服务清单

资源类型	规格	数量
CodeArts	专业版： 代码仓总存储容量100GB 代码仓单仓存储容量20GB 代码检查并发10个 代码检查执行时长不限 构建并发10个 构建执行时长不限 构建依赖缓存大小20GB 部署并发10个 部署执行时长不限 制品仓存储容量100GB 制品仓下载流量50GB/月 流水线并发10个 流水线执行时长不限 流水线资源型任务执行时长6,000分钟/月 接口测试并发2个 接口测试时长不限 知识库存储容量100GB	10人/包周期（年）

本案例所涉及的上云专业服务报价项如下，实际以收费账单为准：

表 2-2 专业服务清单

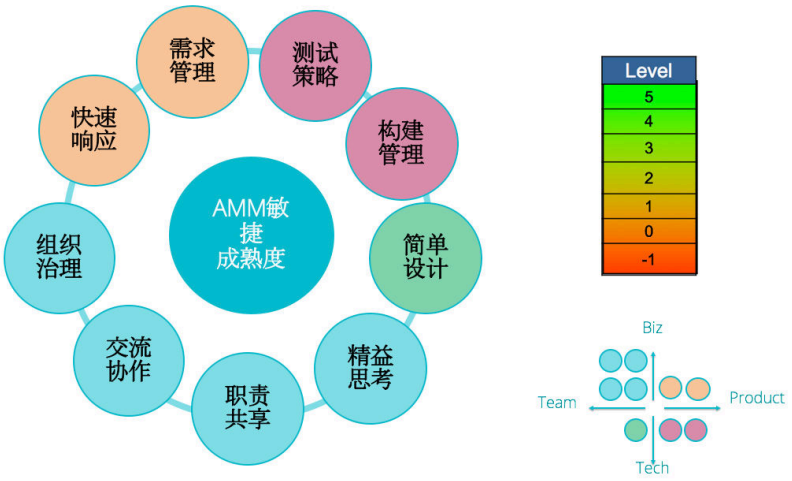
服务项	报价项	量纲
转型规划与培训实施服务	研发能力诊断与规划	套
	团队级研发转型辅导基础包	套
	团队级研发转型辅导增量包	套
集成开发与技术支持	工具定制化开发	元/人天
	技术支持与运维	元/人天
DevSecOps培训	DevSecOps培训	套

3 实施步骤

3.1 研发能力调研与诊断

使用ThoughtWorks特有的敏捷成熟度的体系框架，对客户IT现状进行多维度的评估，并定制转型方案及实施计划。

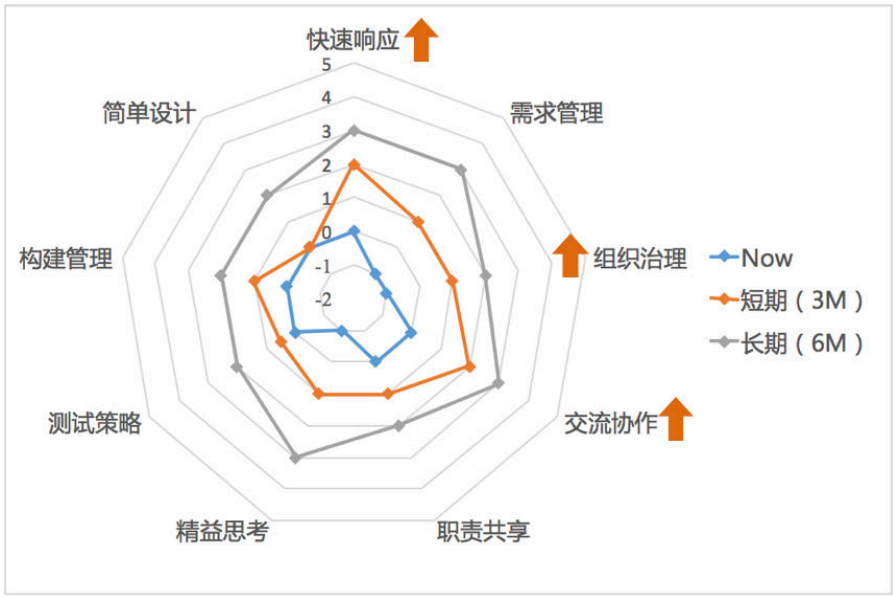
图 3-1 ThoughtWorks AMM（Agile Maturity Model）敏捷成熟度评估



ThoughtWorks有一套已被行业验证的敏捷成熟度体系（Agile Maturity Model – AMM），这套成熟度模型能够测量团队不同维度的能力，包括：

- **需求管理：**在软件开发过程中，需求是对客户价值的明确定义。最大化满足客户价值的软件开发过程依赖于实际用户参与开发和以即时制（JIT）为基础的价值排序。
- **快速响应：**“敏捷”本意是具备快速响应客户需求变化的能力，响应的度量从速度和质量两个维度，需求的变更被高响应力淡化。
- **交流协作：**通过促进在项目利益相关者之间高效沟通和协作，使得项目可以快速、准确地传递客户价值。协同开发过程是通过配置、工具和技术的系统性支持。在最高层面上，用户和企业赞助者都会持续参与。
- **职责共享：**团队灵活和相互协调创造出积极氛围和不断提高效率。不存在知识或技能的潜在单点故障，由团队而不是个人对问题负责。
- **精益思考：**敏捷开发实践是对精益管理目标的很好补充。 软件开发中的浪费在端到端业务价值流中无处不在。系统性地识别、跟踪、消除浪费来提高组织的生产率。
- **测试策略：**测试是为敏捷项目小步快走保证，提供行之有效的安全网。测试承诺通过大量的测试套件能够及时预警任何修改导致已有功能的出错。
- **构建管理：**敏捷团队中，多人快速提交是一种日常行为。构建管理系统应该支持快速并发提交构建而不破坏现有构建。

图 3-2 敏捷成熟度评估结果实例



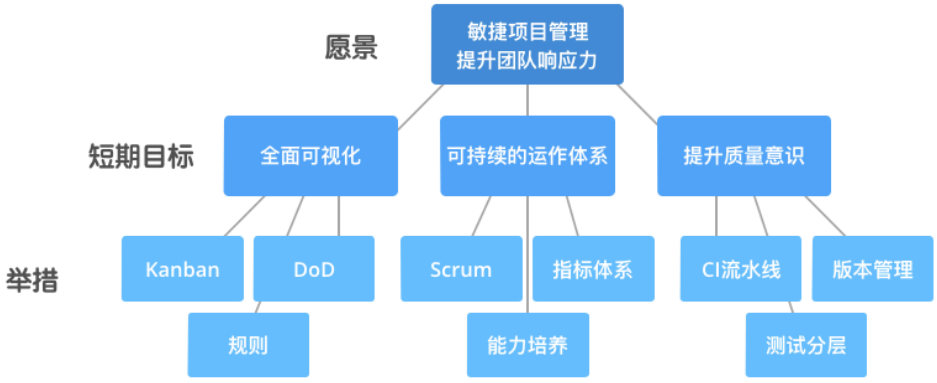
ThoughtWorks咨询团队和客户一起通过对上述维度的分析，形成敏捷成熟度评估报告。

3.2 研发能力评估与规划

使用精益价值树(Lean Value Tree, LVT)的方法规划敏捷转型，使得各个层级目标统一，通力协作，实现高效转型。

精益价值树是一种用来促进捕捉和共享组织级愿景和战略的工具。它是一种树型结构，因为一切都源于企业高层商业愿景。树型结构上的一切都是根据成效来表达的，所以它都将给组织提供价值。

图 3-3 精益价值树实例



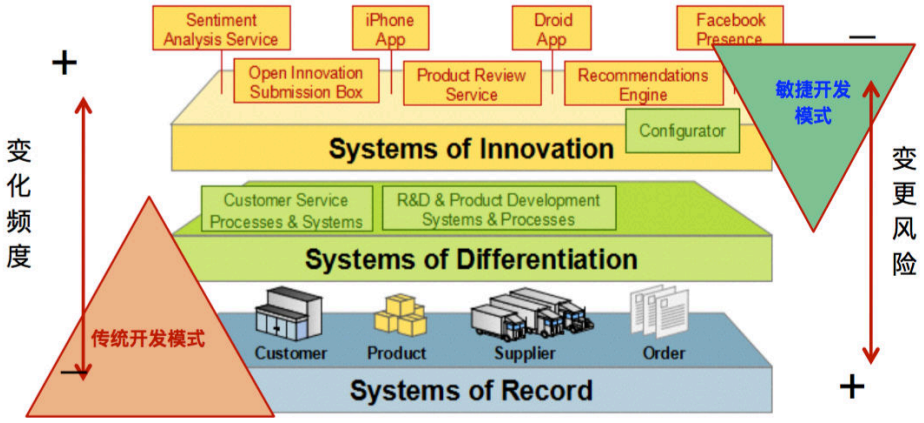
3.3 转型方案设计

结合客户自身的业务及IT的特点（敏捷评估的结果），以及ThoughtWorks在金融领域的经验，补充建立敏捷类应用开发项目实施流程

传统开发模式：强调高度安全、稳定、可靠，适用于中后端核心系统的开发。

敏捷开发模式：强调响应、速度，兼顾稳定性，适用于前端客户交互体验相关系统或创新业务系统的开发。

图 3-4 双模模型



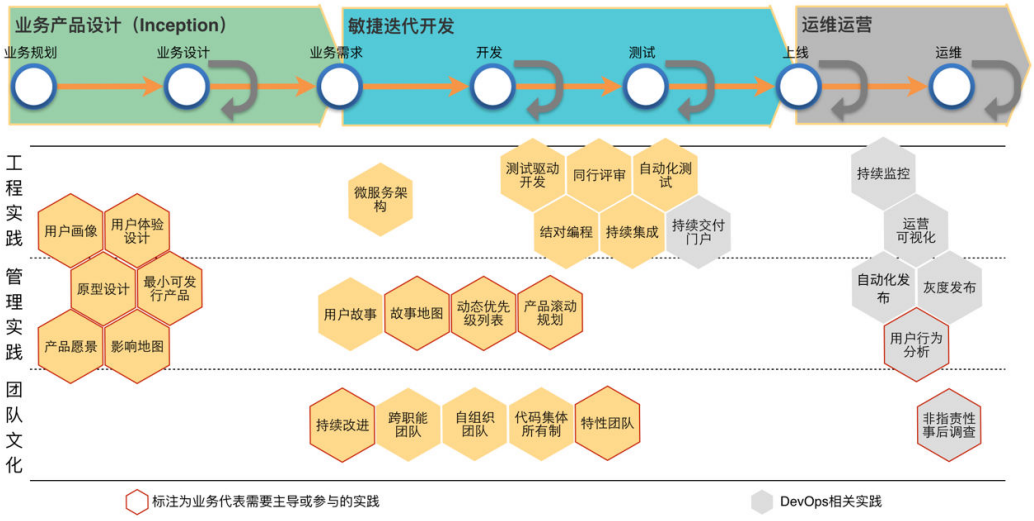
在现有过程管理体系和流程工具的基础上，构建研发和工程管理框架，补充敏捷类项目的实施流程。重点在于：以Kanban和Scrum作为基础管理工具，以持续集成实践集作为基础工程工具，支持传统和敏捷两种开发模式，适用于不同类型系统的项目研发。

图 3-5 支持敏捷开发模式的双模模式

一般来讲，组织在经历了最初敏捷尝试（包括相关专题）之后，通常都会面临敏捷实践的团队级向项目级扩展的问题，在团队级（通常是敏捷实践局限在开发团队内部）无法交付完整的业务价值，也使得敏捷所倡导的业务价值驱动交付较难得以实现。所以，成功的试点很自然会考虑进行端到端扩展的试点（让前端的业务和后端投产运维能与开发团队有效进行协作），也就是项目级的敏捷实施。

ThoughtWorks公司是打造端到端敏捷开发过程的行业领导者，从2007年开始在中国提供敏捷咨询服务至今，已经为数十家客户进行了成功的敏捷转型，并形成了众多的端到端敏捷转型成功实践。下图为端到端实践全集合。ThoughtWorks会根据客户现状为客户组合最佳实践，达到最佳的转型效果。

图 3-6 端到端敏捷实践图谱



3.4 转型方案实施

通过试点项目落地敏捷实践，探索出一套适合客户的敏捷运作指南，指南内容包括：需求管理、可视化管理、迭代管理、持续集成、分支管理等，并在过程中结合运作指南探索工具的使用。

试点团队的选取

ThoughtWorks咨询团队和客户一起基于以下几个原则条件选择试点团队：

- 团队主动意愿强烈
- 业务风险较低
- 产品属性比较强
- 专职的人员配备（例如：业务、需求、研发、测试等）

试点项目也将成为客户敏捷试点优选项目，建立端到端的敏捷开发和运作流程。

敏捷改进小组的建立

用敏捷的方式管理敏捷转型，改进工作本身就是一个敏捷项目，需要团队协作及适应性地去制定改进目标、计划和实施方案。

敏捷改进小组为敏捷转型项目的特性团队，包含领导层与各个角色的种子选手。建立敏捷改进工作圈迭代运作，建立敏捷转型工作坊持续总结与改进，建立敏捷改进工作墙，实时可视化敏捷转型的状态及进度。在管理敏捷转型的同时，让敏捷改进小组对敏捷转型本身有更加深入的理解。

图 3-7 现场实践示例

改进工作圈

改进工作墙

让改进小组在战斗中学会战斗！

改进工作坊

试点项目的敏捷实践

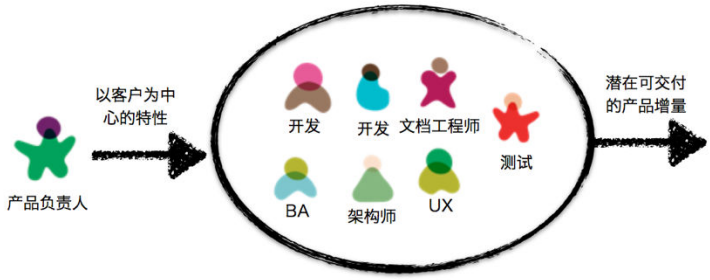
ThoughtWorks会依据AMM敏捷成熟度评估结果，为客户试点团队定制敏捷实践的导入，敏捷实践包括但不限于：全功能团队，需求管理，迭代规范化，可视化管理，持续集成，分支管理等。

1. **全功能团队**

试点团队打造围绕价值的全功能团队，优化快速反馈。

全功能团队——长期、跨功能逐个完成端到端客户特性的团队。

图 3-8 全功能团队



全功能团队的特征：

- 授权：在开发工作最前线的专家们是最精通该领域的人，理当找到一种方法让专家掌控自己熟悉的工作。
- 责任：如果一个团队的成员一起对设计、开发、调试、质量保证、产品交付等全方面负责，那么大家就能找到相互提出批评意见的方法。因为团队成员对产品都负有责任。
- 归属感：在跨功能的全功能团队中，每个人逐渐开始与部分产品密切结合，而不是锁定在某一很窄的专业技能上。
- 共识：团队因为有共同的交付目标而走到一起，并且 共同承担每项特性的责任，所以一定程度的开放是必须的。很多团队 重新组织、规划远景、再分配资源、改变计划都没有遇到棘手的分歧。
- 均衡：全功能团队中的均衡指的是不同技能、不同任务、不同观点的均衡。

全功能团队的优势：

- 推动增量和迭代的思维方式
- 促进学习
- 全局优化（价值驱动）
- 计划和协调工作量降低
- 励代码整洁

2. **需求管理**

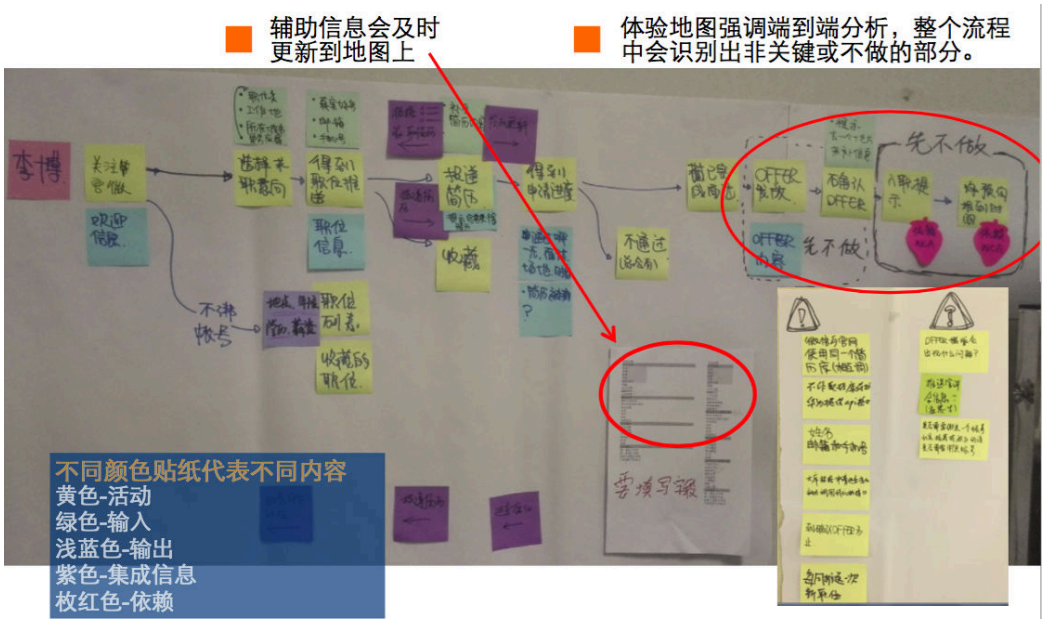
需求管理方法和工具：通过培训、工作坊、实例需求执行等方式，培养PO人员能力，掌握价值分析模型、用户故事地图、用户画像等方法，并进行实践操作，提升业务需求的分析和管理能力。

敏捷实践：用户故事地图

用户故事地图将用户面对一个品牌或一款产品时的关键接触点描述出来。跟随一个典型的有序“生命周期”，通常从一个典型用户行动的 “触发点”开始，从而帮助团队明确产品的需求。

用户故事地图是根据真实用户来建模的，应该基于严谨的用户研究。这项活动通常在用户画像建立及场景定义之后。

图 3-9 用户故事地图



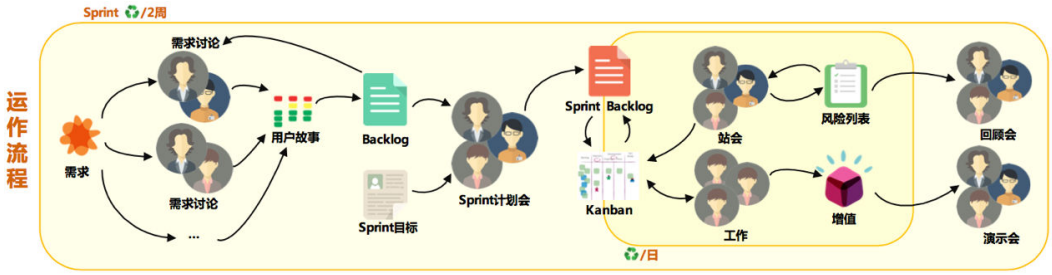
3. **迭代规范化**

迭代规范化：通过教练引导，优化Scrum活动，指导Scrum Master有效引导计划、回顾等活动，帮助团队进行DoD涌现等活动，尝试Scrum和看板融合，对项目进行预测和有效管理。

敏捷实践：Scrum活动规范。

团队通过实施Scrum，可以加强团队成员的协作，使得开发及交付变得有“节奏感”，提高团队的响应速度。

图 3-10 定制的运作流程



4. **可视化管理（Kanban与Scrum融合）**

通过看板可以透明团队现状，找到团队的瓶颈并进行改进。

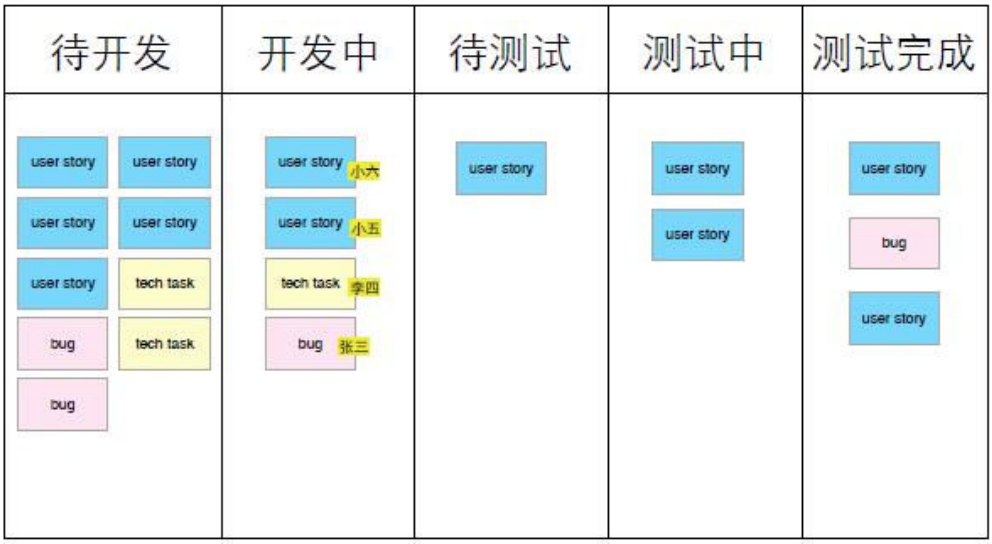
敏捷实践：Kanban

搭建看板：

- 价值流程（任务墙的列）
- 卡片类型及颗粒度（任务墙的卡片）

- 范围（时间）
- 任务负责人
- 各阶段的准入条件
- 移动卡片

图 3-11 看板示例



5. **持续集成**

敏捷实践：持续集成流水线（CI）

根据现有持续集成流水线水平，然后根据各团队产品特点给出具体的方案。业界有一些良好的工具和CI实践将作为参考。咨询师会根据方案，进一步协助搭建CI流水线，包括培训、技术答疑等方式。

敏捷实践：持续集成质量基线

- 在项目团队内部达成对软件质量标准的共识——项目软件的质量应该是什么水平
- 在项目团队内部达成对软件质量意识的共识——不允许项目软件质量低于基线
- 通过持续提高项目持续集成基线的水平，不断推动项目团队提升产出软件的质量
- 将项目的软件质量具象化为一组高度关联、可以通过CI技术手段无侵入式采集的指标

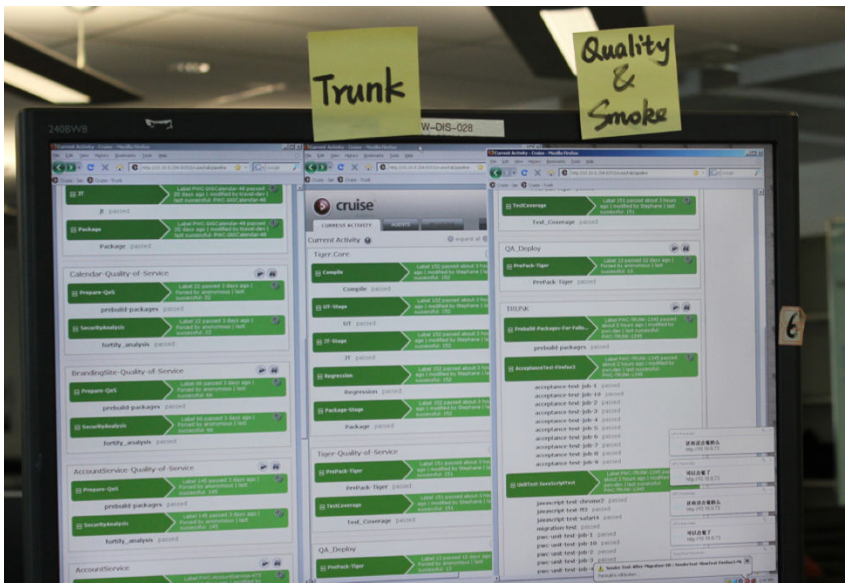
针对当前CI采集的统计指标，结合项目团队的实际情况，为每个项目团队制定特定的CI质量基线。一旦团队认可基线标准，CI流水线将只显示两种状态：红、绿，低于该基线即为红。不允许项目团队低于该基线。

敏捷实践：持续集成纪律

- 在项目团队内树立软件质量的认知意识，真正在日常的开发中内建质量
- 在项目团队内贯彻对软件质量的坚持意识，避免“破窗”的不良影响
- 保障软件产品的质量

图 3-12 七步提交法

图 3-13 持续集成可视化示例



6. **分支管理**

敏捷实践：分支管理

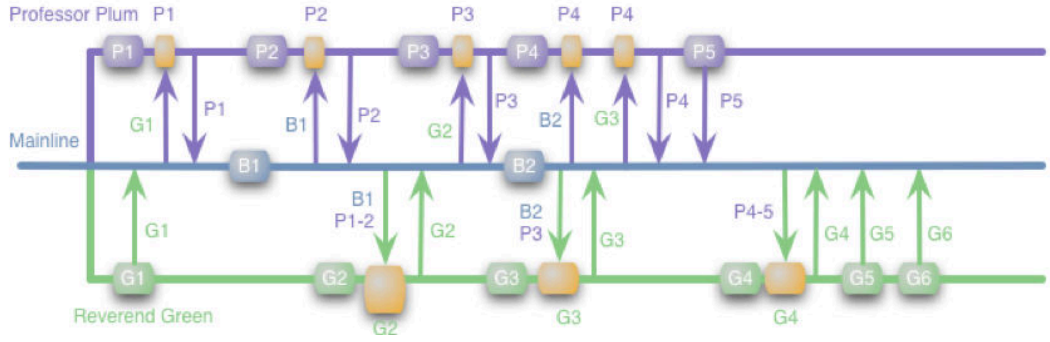
代码分支策略的目的在于解决如下问题：

- 项目团队往往使用多组并行的版本分支，分支何时才需要创建、分支的生命周期缺乏梳理和规范。
- 项目团队在使用版本分支时，未能使用正确的合并策略，导致不同的分支合并出现各种问题。
- 帮助团队尽量采用单一主干开发的方式

基本策略：

- 梳理各项目团队代码分支和合并的策略
- 梳理各项目团队对于版本管理的机制
- 与应用运维、数据中心等部门达成版本管理的策略

图 3-14 分支管理示例

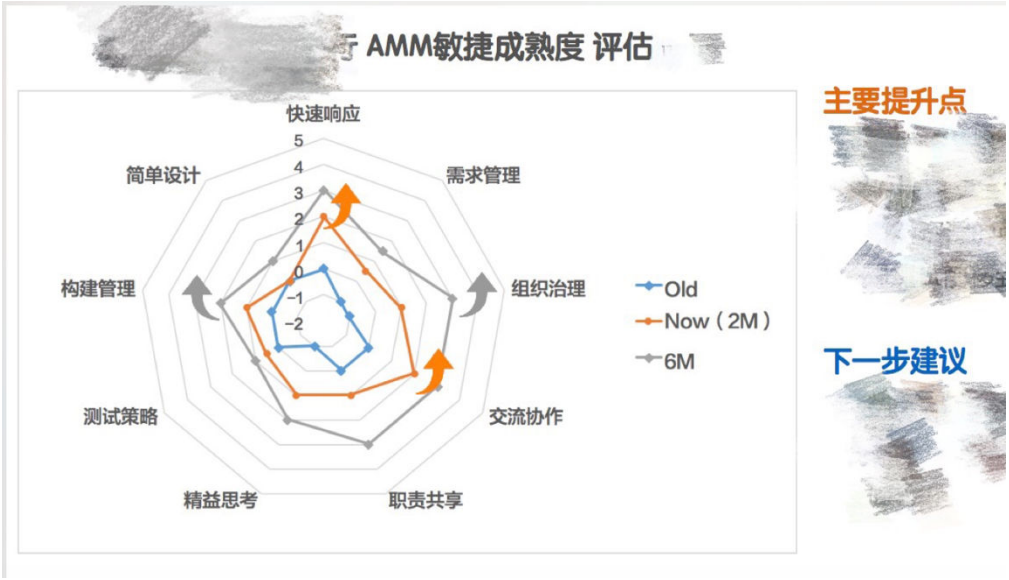


3.5 项目总结

在团队试点阶段，ThoughtWorks会持续总结改进运作方案（包括需求管理，运作管理，工具的尝试等），帮助客户打造自己合适的敏捷运作方案，便于之后的大规模推广。在项目总结阶段会把所有方案打包整理，并进一步细化其中的内容，ThoughtWorks拥有大量的金融行业定制化的敏捷运作方案的案例。

在项目总结阶段，ThoughtWorks将为试点团队再次进行AMM敏捷成熟度评估。从客观的体系总结出团队各个维度的现状、改进点、改进后仍然存在的问题，以及下一步的提升规划，并形成项目总结报告，以保证团队的持续敏捷运行。

图 3-15 总结 AMM 评估汇总实例



4 附录：常见问题

1. **如何保障专业服务中的人员投入**?

   答：ThoughtWorks拥有充足的后备专家资源池，为项目尽可能提供复合型顶尖专家人才，服务人员将按项目要求出勤到现场，保证方案和思路的前后一致性；在现场专家能力不能覆盖的情况下，可以通过调配资源方式，提供满足邀标方要求的专家到达现场开展工作。ThoughtWorks保证项目服务人员稳定，在未经过邀标方同意的情况下，不得随意更换人员，经邀标方同意并办理交接手续后方可更换，做好项目服务人员管理。

2. **如何保证项目进度?**

   答：ThoughtWorks对于本项目监控目的：提供对项目进展的理解，以便当项目的性能严重偏离计划时采取适当的纠正措施。

   项目例会：项目例会是项目组内进行信息交流的一种重要的机制，是项目管理例行过程的一部分。

   会议计划示例安排如下：

   - 项目上每两周设有计划会、成果展示会、回顾会议；
   - 项目上每个月设有客户沟通会，项目经理会专门收集客户反馈。
   - 本项目实施过程中，将在实施工作各阶段的关键节点召开相关会议，以达到对各关键节点进行管控、推进项目顺利实施的目的。

5 修订记录

发布日期	修订记录
2024-1-16	首次发布。