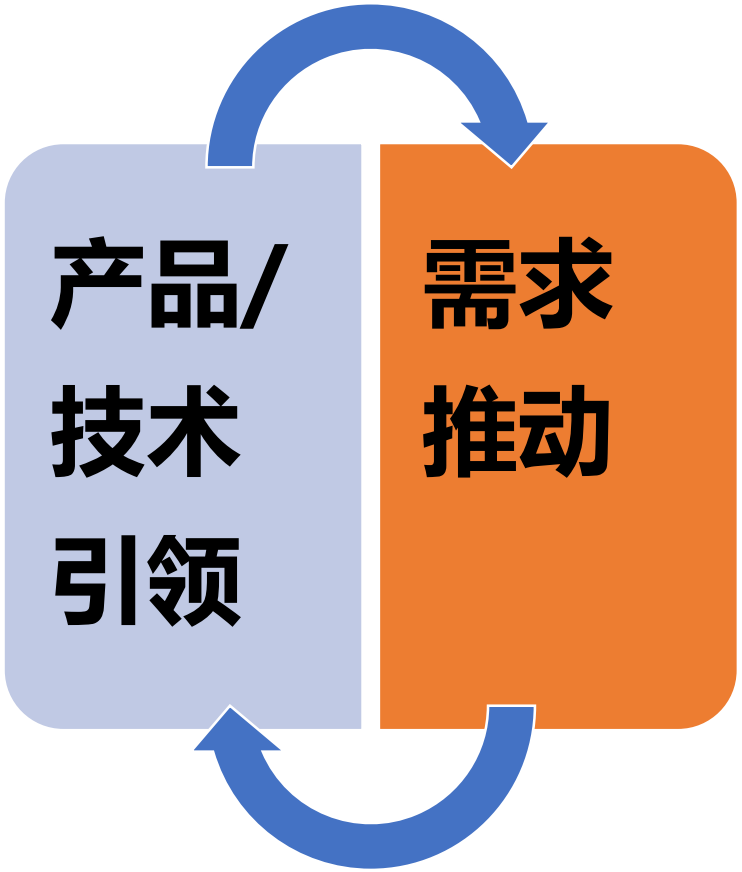
CSO怎么做

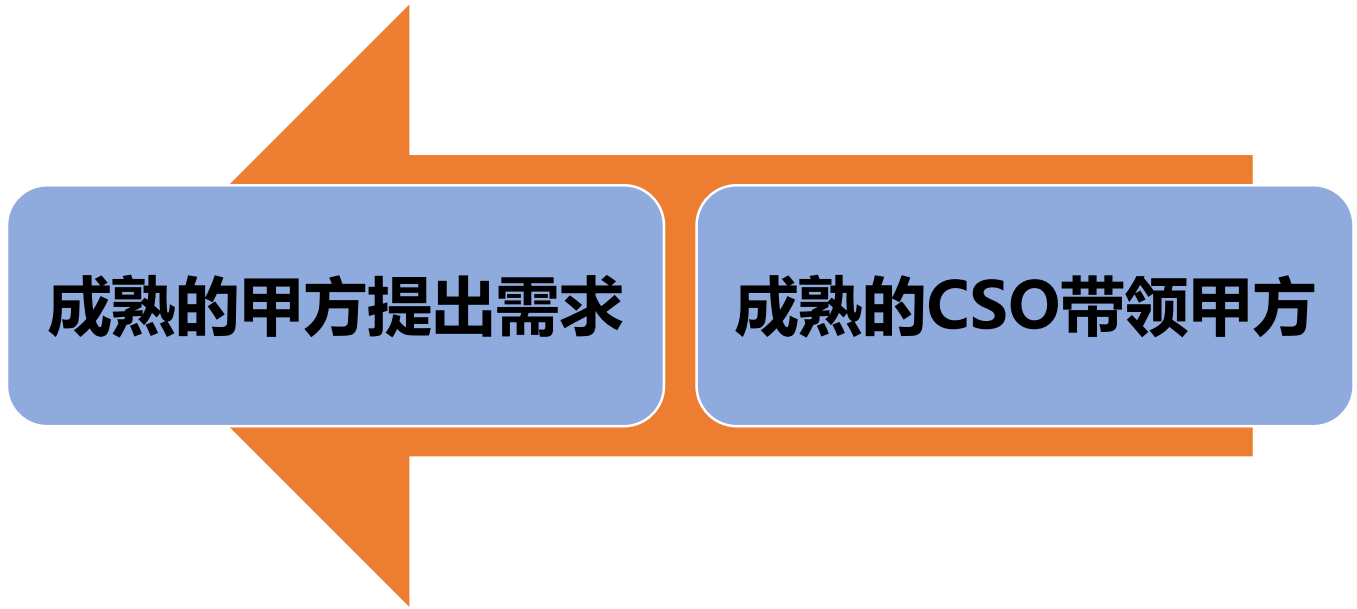
truebasic

自我介绍

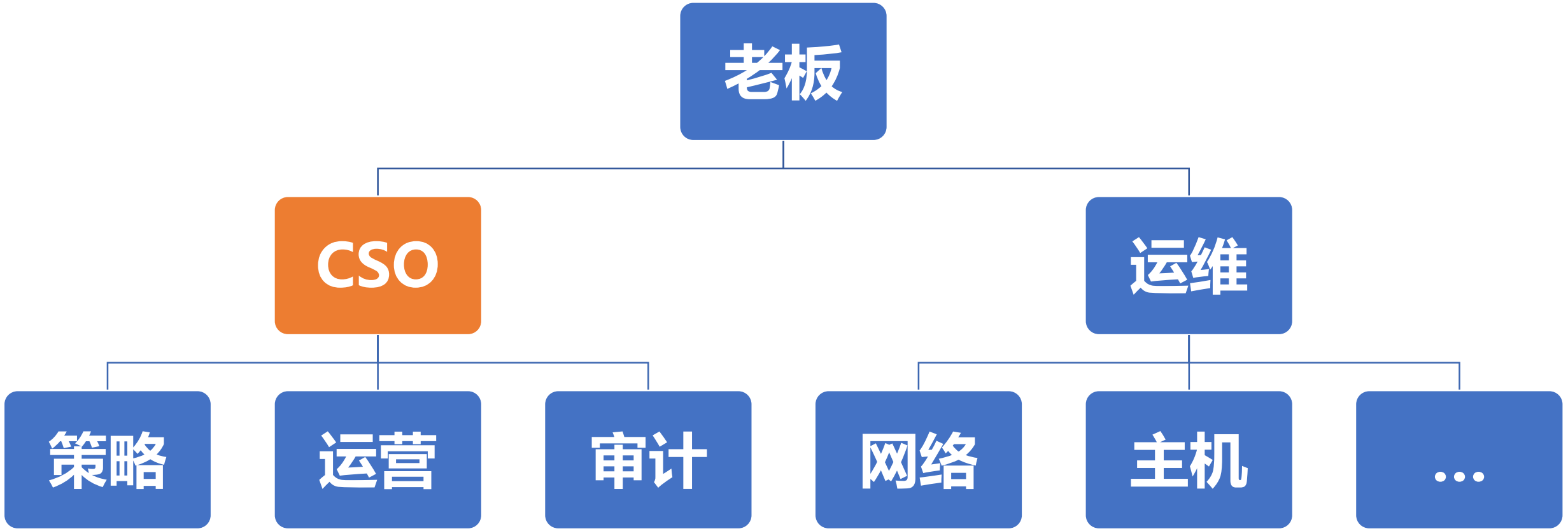
- 经历复杂，做过开发、项目经理、创业者、大学老师
- “误入”信息安全行业12年，科技创新型企业甲方经历为主，证券行业新兵
- 期待甲乙方同行多交流、共成长、多指正
- truebasic@outlook.com

一、CSO在企业信息安全中的作用和地位





一、CSO在企业信息安全中的作用和地位



二、CSO的道（1）理解安全的驱动方式

- 由于内外部信息安全事件而开展安全建设和改进动作

- 根据外部规范、要求建立自身的信息安全管理体系，以达到规范要求为主要目的

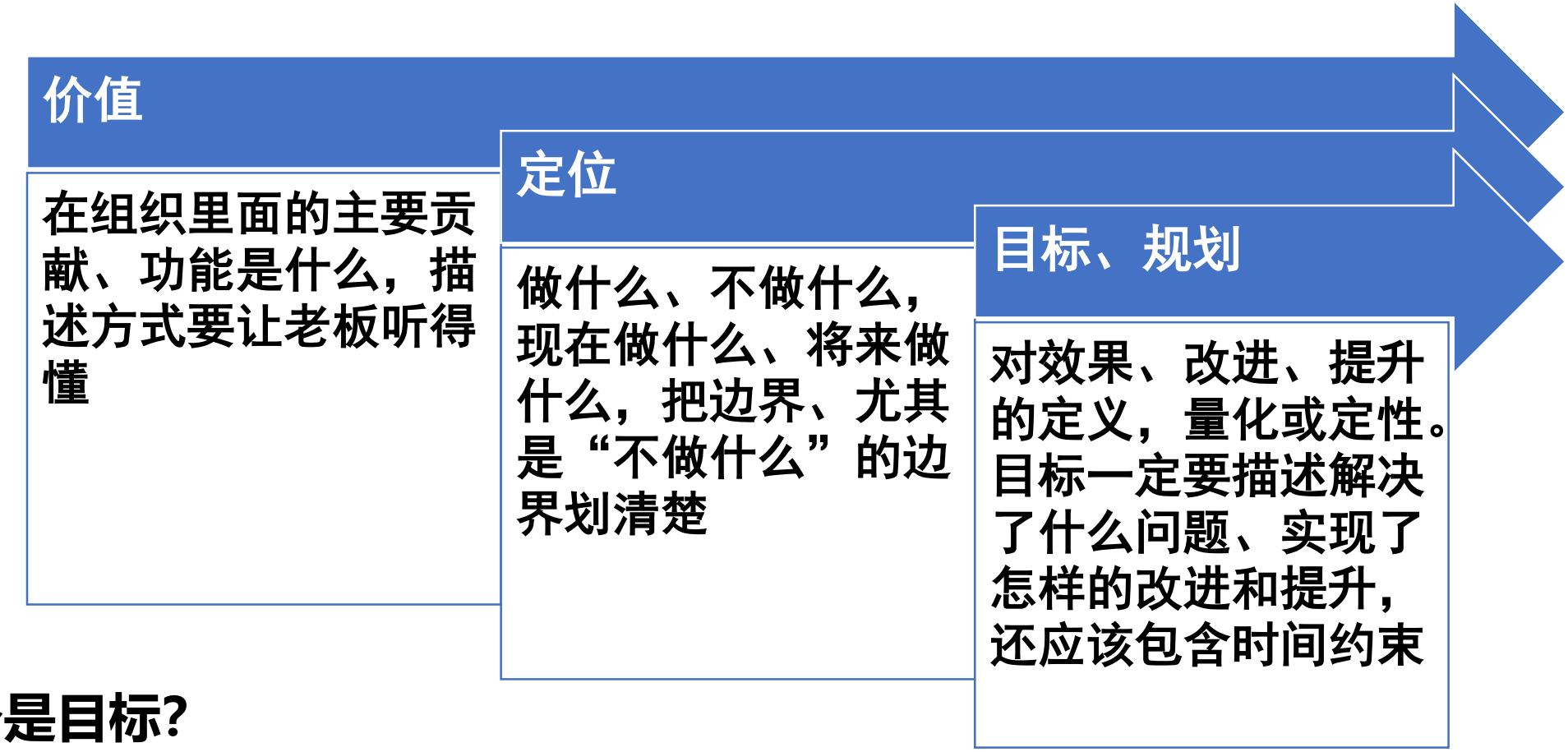
- 由内部业务部门驱动信息安全建设和改进的工作方式，旨在保护和提升企业竞争力

- 根据内外部规范、最佳实践和供应商推荐，制订年度规划和预算，开展信息安全建设。花预算为主。

二、CSO的道（2）4个核心工作

定目标	带团队	获取资源	评价
• 什么是目标 • 了解业务、梳理现状 • 价值、定位、目标、规划	• 组建团队 • 提升能力 • 引入外部力量 • 树正气 • 主动承担	• 人、财、物、政策、内部支持者、供应商&合作商资源 • 向上管理	• 团队成果 • 团队成员 • 供应商&合作商

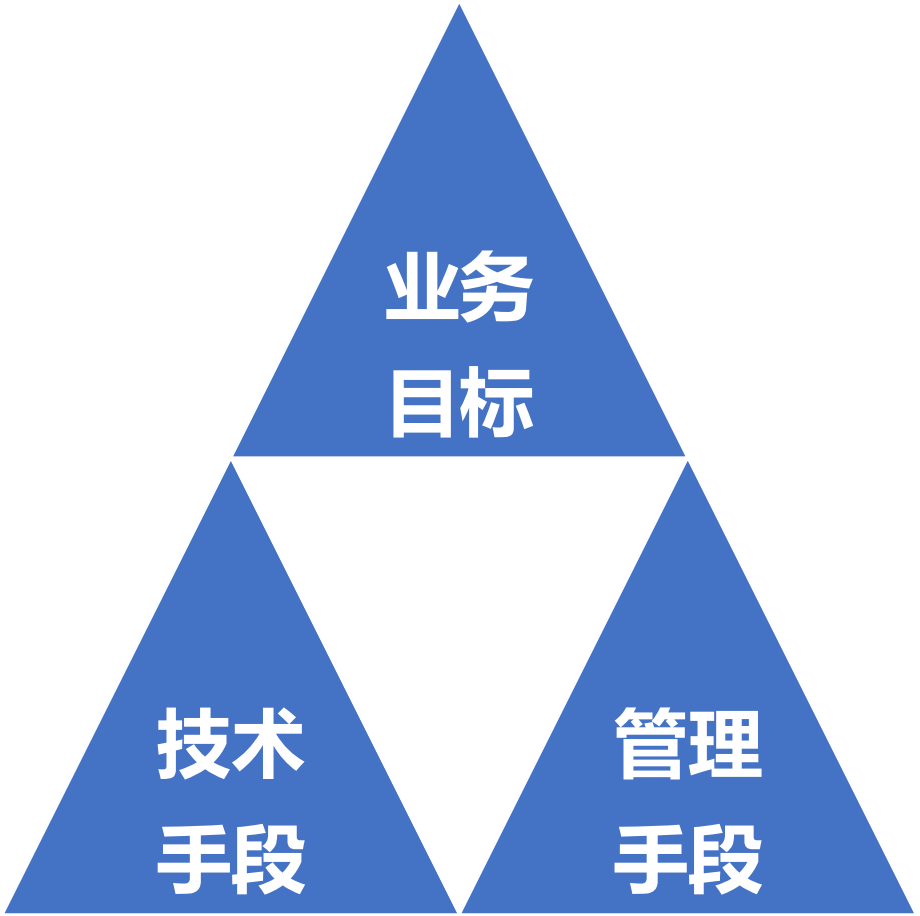
二、CSO的道（3）价值、定位和目标



以下哪个是目标?

- **不让坏人进来，或者坏人进来了、干不了坏事；**
- **不让攻击者对交易所造成任何负面影响，或攻击者、信息泄露者每年对我司业务造成（客户、声誉、业务）损失小于100万；**

二、CSO的道（4）再谈技术与管理



管理思维

以客户为中心、达成目标、有体系框架和套路、会识人用人、先管理策略后技术手段

技术保障

用技术和工具保障管理策略落地

信息安全领域，“能用技术工具或系统实现的，尽量就用技术实现”这个观点你怎么看？

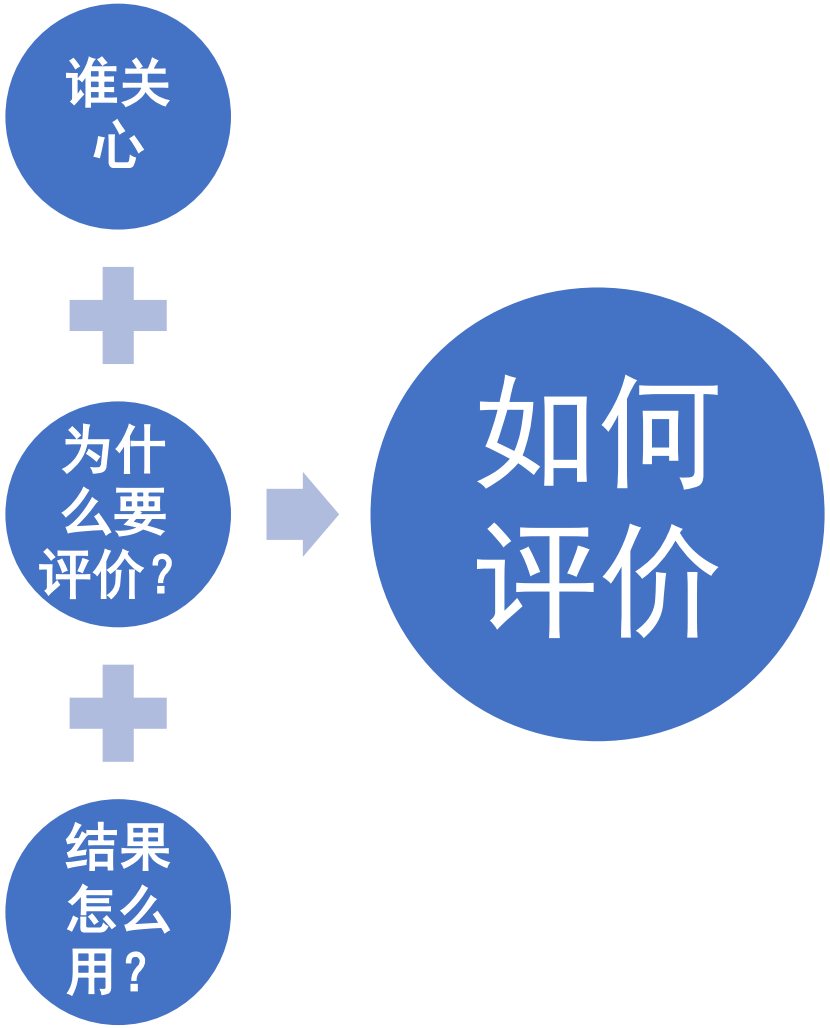
三、CSO的术（1）架构

三、CSO的术（2）评价

- 老板、CSO、对手？

- 为了评估工作成效、评估投资收益比、寻找需要改进的短板？

- 绩效考核、对标标杆、评估进攻风险…



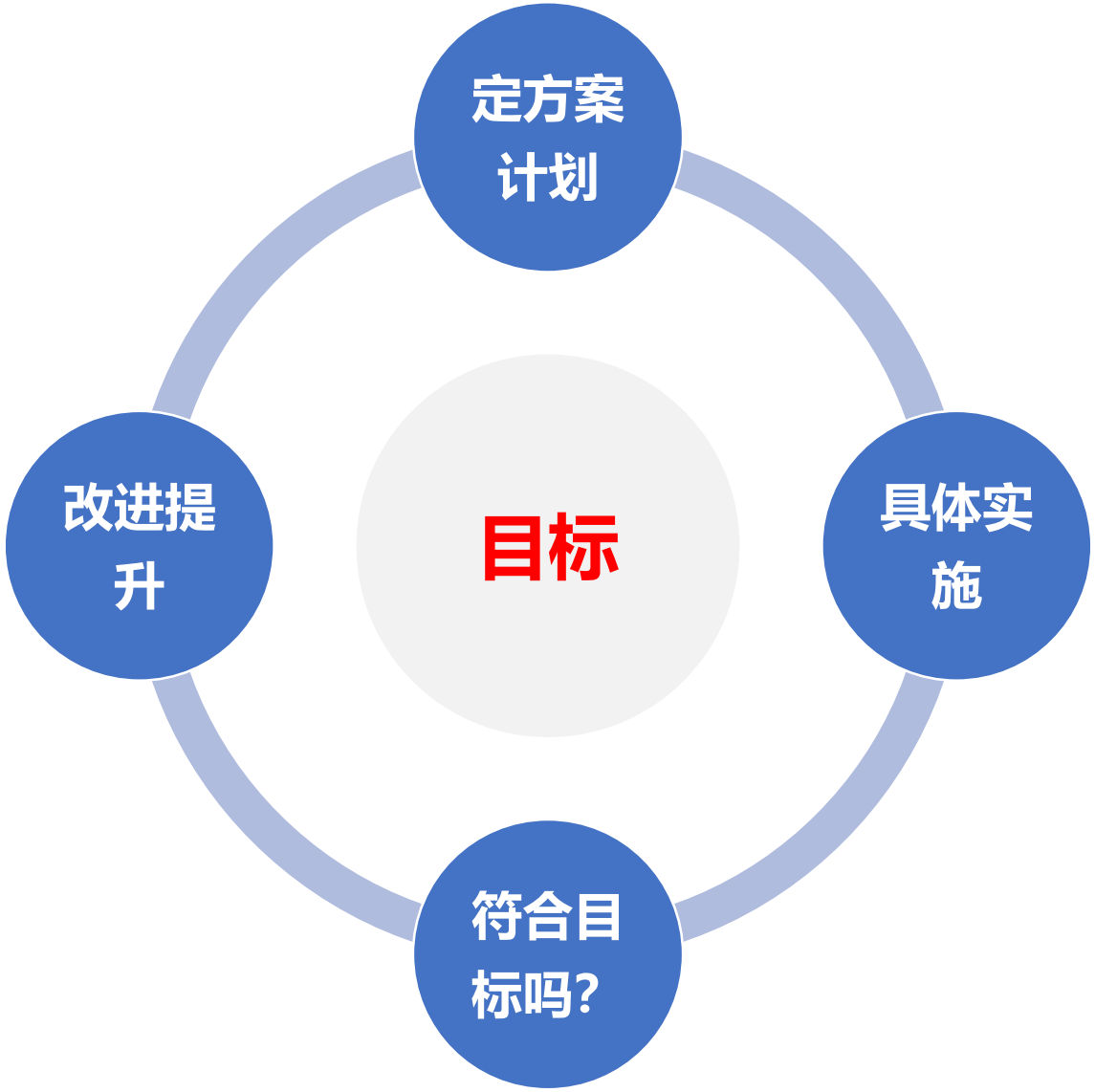
- 找到恰当的评价标准
- 评价
- 评价后的结果运用

三、CSO的术（3）运营与审计不可偏废

运营是通过持续地使用工具、优化策略、改进流程，达到或超过期望的目标。属于事中措施。

审计是通过检查、渗透或其他验证工作，检查安全策略有没有、做没做、是否达到了预期目标、是否引入其他的安全风险。属于事后措施。

三、CSO的术（4）PDCA



大到一个项目，小到优化一条WAF策略，都可以运用PDCA方法论。

CSO做到了，团队成员自然就会做到。

- 以客户为中心
- 以价值创造者为本
- 较真
- 深入实际
- 必达目标

三、CSO的术（5）做好业务安全

定义：业务安全就是如何平安地赚钱。非传统意义的IT基础设施安全、信息资产安全。

原则：充分理解业务，做业务的朋友，在帮助业务解决难题的过程中解决安全问题

业务安全

做法：1快速学习，听懂；2看流程文件；3实地查看、体验业务需求和场景；4做朋友、找铁杆、掏心窝；5换位思考，琢磨既做好业务、又安全的措施；6把措施落实到位，双赢

资源：1自己主动学习业务；2安全和业务轮岗

四、目标管理、沟通能力是1后面的00000000

- 调研、分析需求
- 说服老板花钱
- 跟其他团队一起做项目
- 推动修复漏洞
- 跟供应商砍价
- 向老板展示业绩
- 表扬、批评、处罚、奖励
- 写周报月报总结计划
- 面试

我是技术人员，

我不喜欢沟通，我喜欢搞代码，

我喜欢搞工具，我喜欢搞系统，

我喜欢合作，不喜欢有人搞搞震，

我讨厌叽叽歪歪，我讨厌写报告，

我讨厌那个家伙，我没法推动工作，

我实战很强，表达不好...

沟通是为了达成一致。沟通≠表达、说服

谢谢