信息安全管理
先锋论坛

跟我学信息安全管理

浅谈CISA　　陈淑敏

信息安全管理专家委员会发布
2016年8月

信息安全管理论坛（http://www.iso27001cn.com）成立于2014年9月，为国内目前最专业的信息安全管理学习和实践交流平台。是学习信息安全管理方法、分享实战经验、提升实践水平的好地方！

关于我们

我们提供

- 最全的信息安全管理资料
- 信安经理高薪工作机会推荐
- 每周专家讲堂（ 每周四晚上8点半YY频道89519382 ）
- 物美价廉的ISO27001课程团购

- 信息安全管理学习实践QQ群 207723402
- 微信 IT管理精英圈 itilxf_(记得有下划线)

欢迎关注

授课专家

陈淑敏

大数据治理国家标准编制组成员， 电子商务司《跨境商品电子商务经营服务规范》和《移动商品电子商务经营服务规范》行业标准编制组成员，多年来为各大银行、证券、互联网金融公司做咨询相关工作，具有14年丰富的IT行业工作经验，在国外500强和国内知名企业担任过PMO经理、项目经理、高级咨询顾问，创业公司副总等职务，涉及领域包括：ISO20000及ITIL运维体系咨询、ISO27001信息安全管理体系咨询， 全球供应商管理体系咨询，数据化运维咨询等。

部分项目经验如下：

辽宁农信ISO20000、ISO27001认证咨询项目，	项目经理
北京银行ISO20000认证咨询项目，	项目经理
国泰君安大数据运维规划项目，	项目经理
交通银行全球供应商管理及风险管控项目，	项目经理
上海农商行ISO20000认证咨询项目，	项目经理
上交所ISO20000续证咨询项目，	项目经理
银天下科技ISO20000、ISO27001认证咨询项目，	项目经理
东方证券ISO20000 认证咨询项目，	项目经理
美国银行OpenView BP4SC ITIL实施项目,	项目经理
英孚石油BP OpenView BP4SM ITIL实施项目,	项目经理
联邦快递 FedEx OpenView BP4SC ITIL实施项目,	项目经理

资质证书：

- CISA、 COBIT
- ITIL V3 Expert认证、ITIL V2 Service Manager认证
- ISO9000、 ISO20000、 ISO27001主任审核员
- 项目管理（PRINCE2）从业者认证、项目管理PMP认证
- 敏捷SCRUM Allianc（CSM）认证
- 6 Sigma Green Belt/Lean + 6 Sigma
- TTT、 CCNA、 MCSE…

浅谈CISA

提纲

1. 信息系统审计过程
2. IT治理与管理
3. 信息系统的获取、开发与实施
4. 信息系统的运行、维护与支持
5. 信息资产的保护

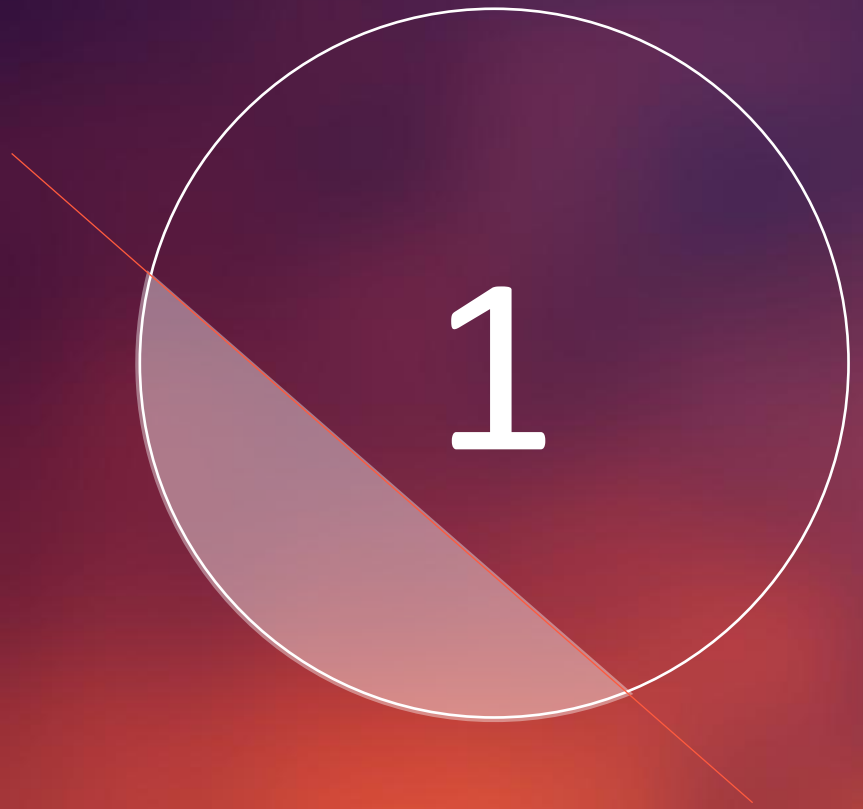
ISACA 简介

- 国际信息系统审计委员会（ISACA）：
“信息系统审计是一个获取并评价证据，以判断计算机系统是否能够保证资产的安全、数据的完整以及有效率利用组织的资源并有效果地实现组织目标地过程。

- 信息系统审计及控制协会，创始于1969年。在信息技术治理、审计、控制、保障和安全等方面，ISACA是全球公认的领导者
- 目前已有超过86，000名会员分布在160多个国家。
- 已有超过175个分会分布在70多个国家。
- 自 1978 年以来，由 ISACA 组织的信息系统审计师 (CISA) 考试已为全球公认的信息系统 (IS) 审计、控制和安全专业人员的成就标准。

CISA 认证要求

- 顺利通过CISA考试（考试包括200道多项选择题，考试时间4小时，国内每年考试6月，9月，12月）
- 提供从事信息系统审计、控制与安全工作5 年以上经验的证明。
- 提交CISA申请表并得到正式批准
- 遵守ISACA职业道德规范
- 遵守ISACA采用的信息系统审计标准
- 遵守持续职业教育规划



信息系统审计过程

第一章 信息系统审计过程

- 实施IS审计
- 内部控制
- 风险分析
- 控制自评估
- ISACA 审计准则和指南
- 审计职能管理

倒后镜的作用

我们开车的时候，关注更多

- 前方？
- 仪表盘？
- 倒后镜？

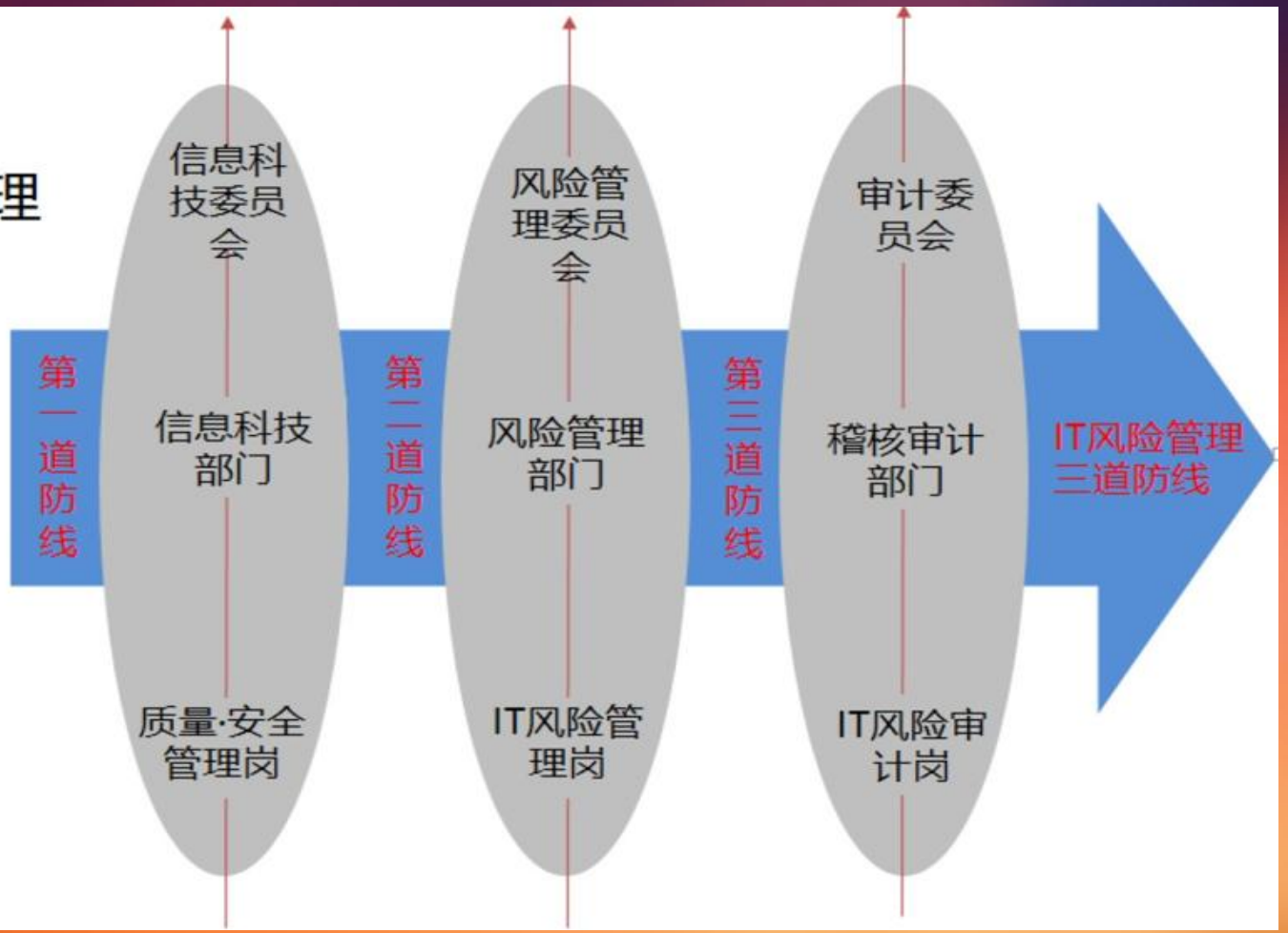
三道防线

- 明确信息科技风险管理的三道防线

✓ 第一道防线：自身遵从

✓ 第二道防线：提前预防

✓ 第三道防线：事后审计



Risk based Audit 风险为基础的审核

审核类型	自我评估	第一方审核	第二方审核	第三方审核
ISO标准要求（自愿）				客观、有效 较高成本
客户要求（特定）				
法规要求（强制）				
组织要求（规定）	主观、合规、低投入			

内控控制

- 预防性
- 检测性
- 纠正性

审计风险

- 固有风险
- 审计风险

审计测试

- 符合性测试
- 实质性测试

审计抽样

- 停-走抽样
- 发现抽样

信度 vs效度

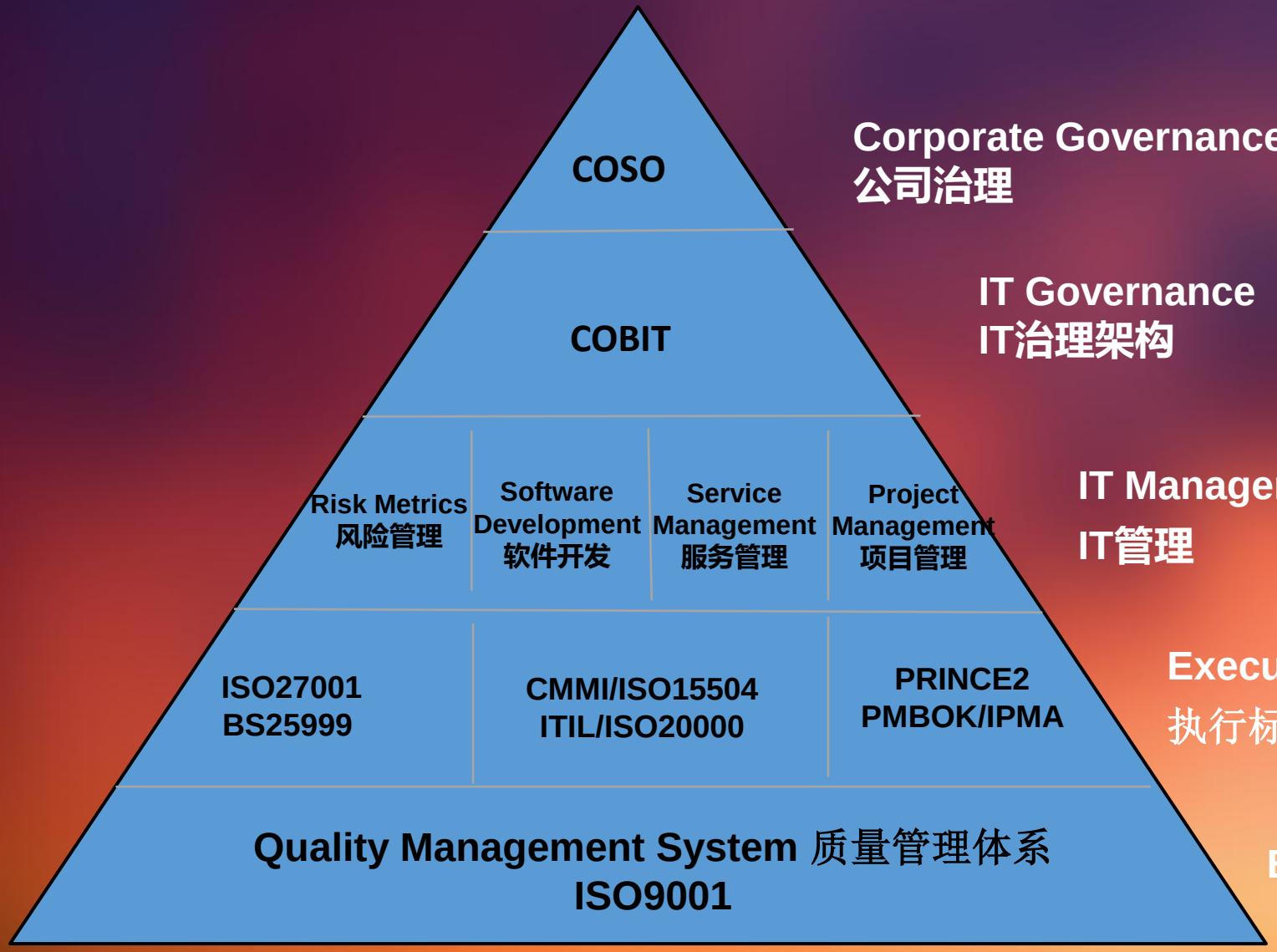
2

IT治理与管理

第二章 IT治理和管理

- 风险管理
- IS管理实务
- IS组织结构和职责
- 业务连续性计划和灾难恢复计划
- 政策和程序
- 投资和分配实践
- 成熟度以及过程改进模型
- 信息系统战略
- IT治理

IT治理 vs 公司治理



Corporate Governance/SOX
公司治理

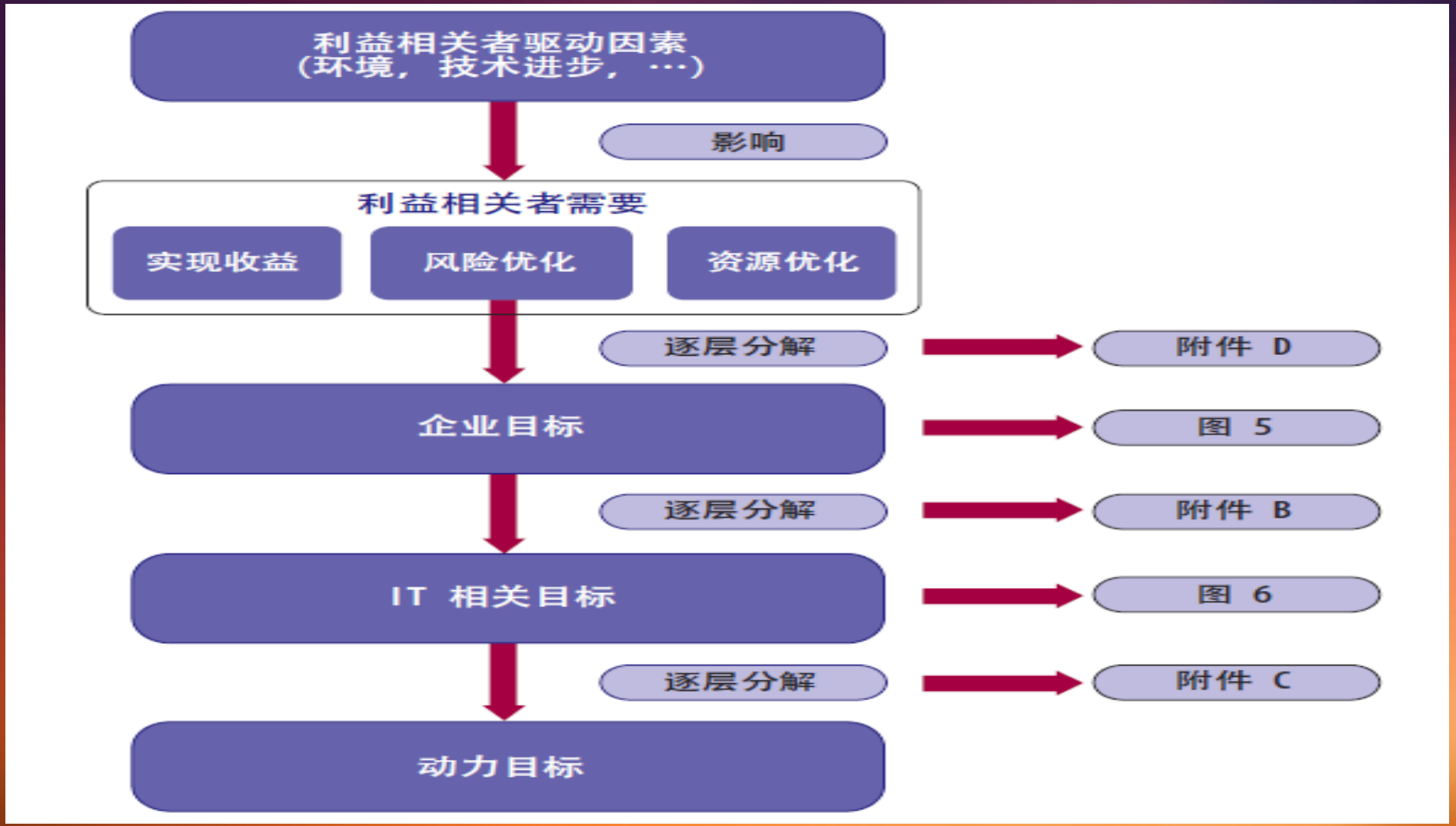
IT Governance
IT治理架构

IT Management
IT管理

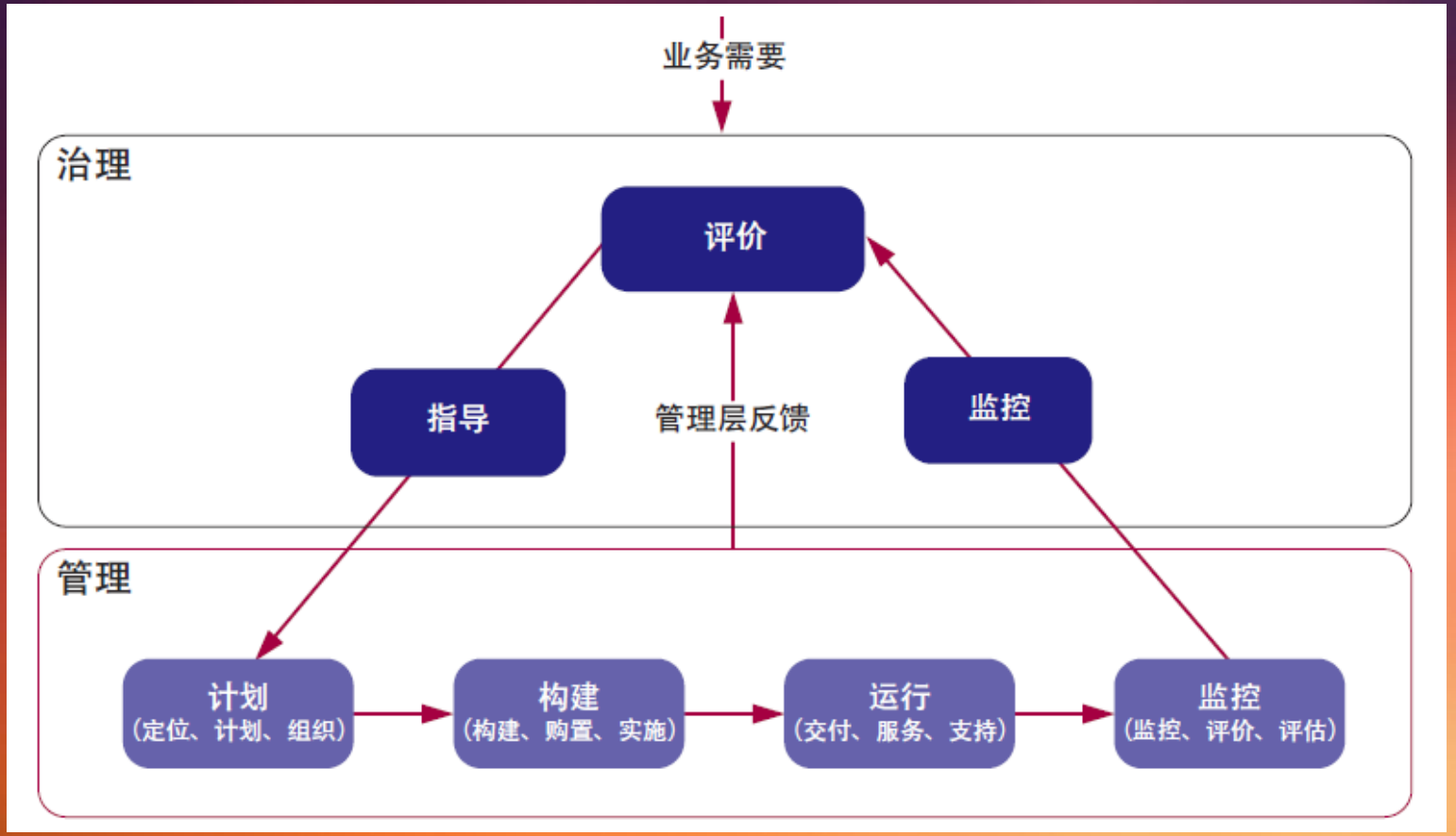
Execution
执行标准

Basic 基础管理

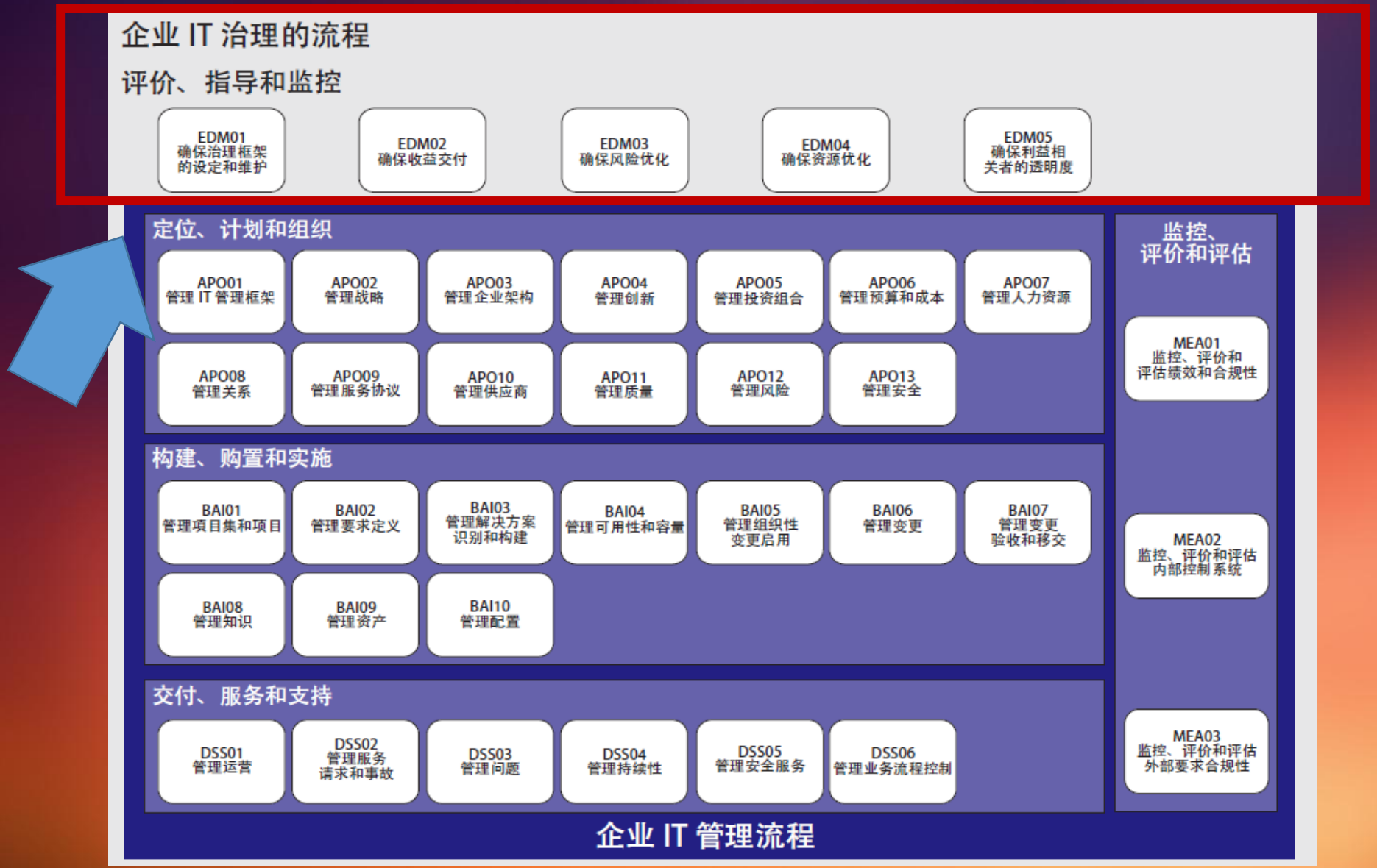
满足干系人的需求


利益相关者驱动因素
(环境，技术进步，…)
影响
利益相关者需要
实现收益
风险优化
资源优化
逐层分解
附件 D
企业目标
图 5
逐层分解
附件 B
IT 相关目标
图 6
逐层分解
附件 C
动力目标

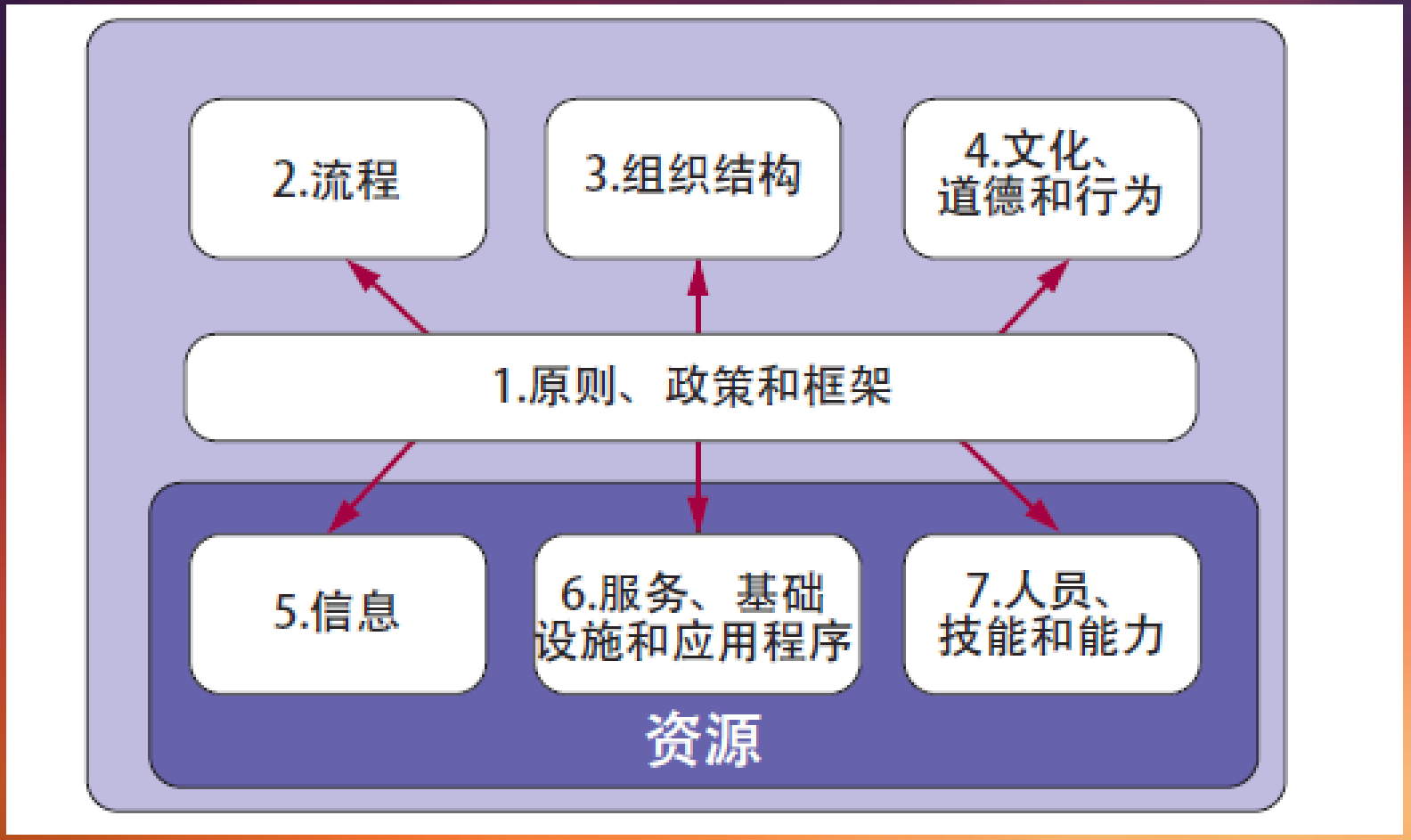
治理和管理的定义


业务需要
治理
评价
指导
管理层反馈
监控
管理
计划
（定位、计划、组织）
构建
（构建、购置、实施）
运行
（交付、服务、支持）
监控
（监控、评价、评估）

COBIT 5 流程参考模型



动力要素



数据中心成熟度国标


战略发展
战略规划
战略规划管理
商业论证管理
战略执行
项目组合管理
项目群管理
项目管理
传承创新
知识管理
创新管理
稳健发展
财务管理
人才管理
持续运营
例行管理
监控管理
值班管理
作业管理
技术管理
技术生命周期管理
技术评审管理
服务支持
服务请求管理
突发事件管理
问题管理
变更管理
发布管理
资产与配置管理
服务交付
服务级别管理
可用性管理
性能与容量管理
IT服务连续性管理
关系管理
公共关系管理
业务关系管理
供应商管理
安全管理
合规管理
信息安全风险管理
安全策略管理
安全措施管理
质量管理
文档管理
质量审计管理
报告管理
持续改进管理
组织治理
组织架构
组织设置管理
职能协同管理
驱动机制
领导力管理
执行力管理
绩效管理
人员绩效管理
组织绩效管理
组织文化
组织文化管理

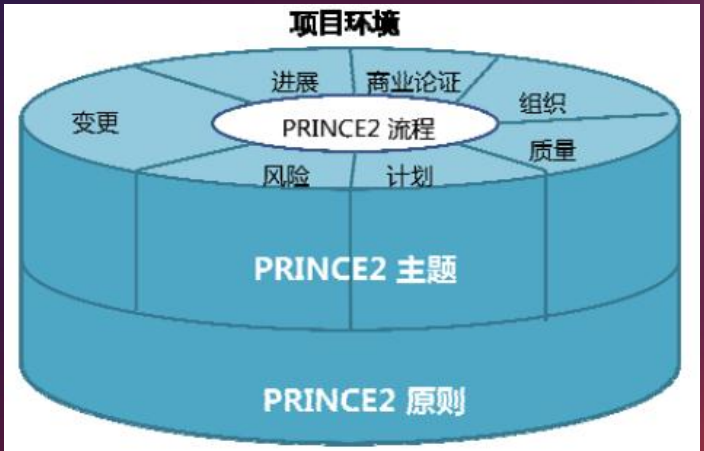
3

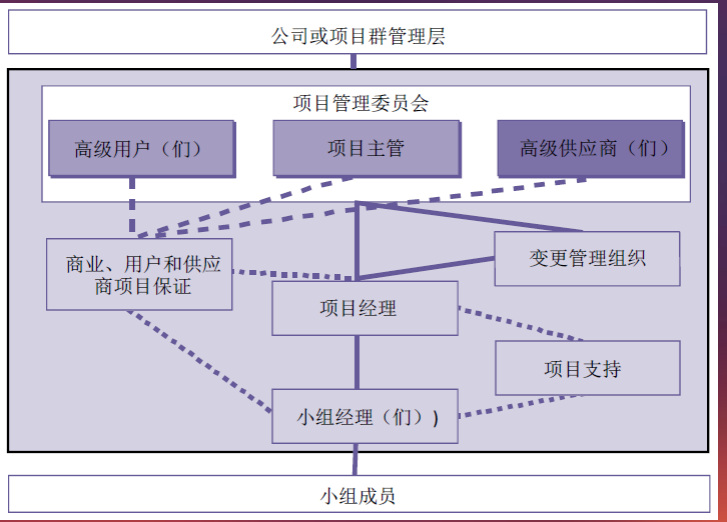
信息系统的获取、开发与实施

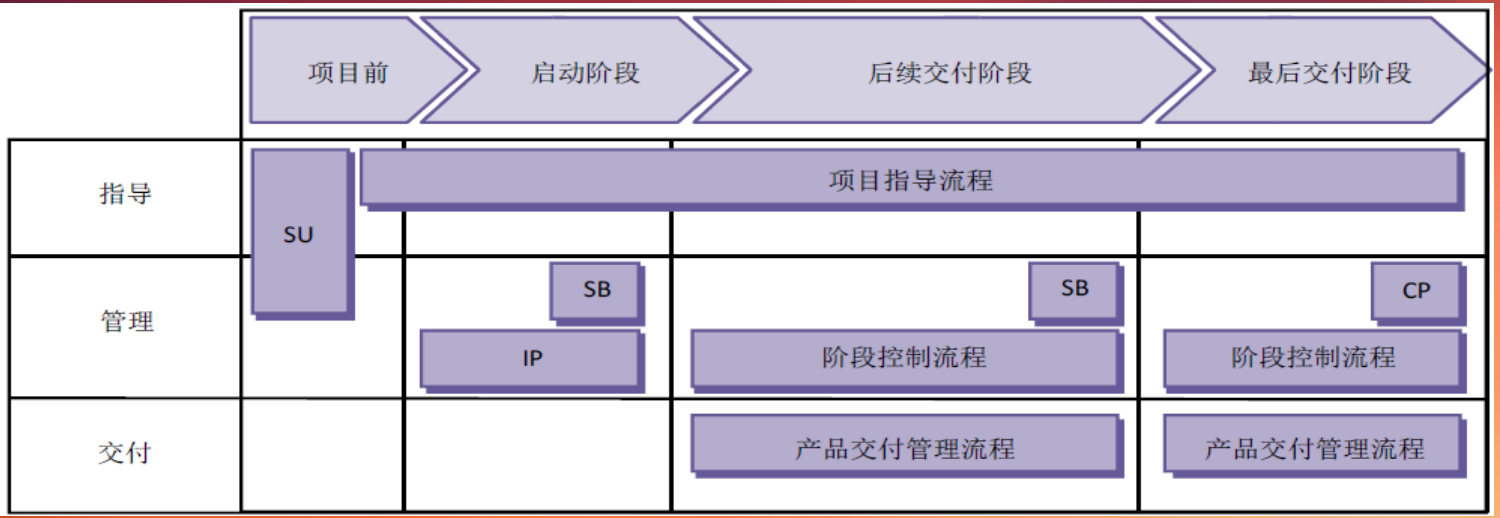
第三章 信息系统获取、开发与实施

- 业务实现
- 项目管理结构
- 项目管理实务
- 业务应用系统的开发SDLC
- 开发方法
- 业务应用系统
- 基础设施开发与获取实务
- 信息系统维护实务
- 过程改进实务
- 系统开发工具和辅助工具
- 应用控制

PRINCE2

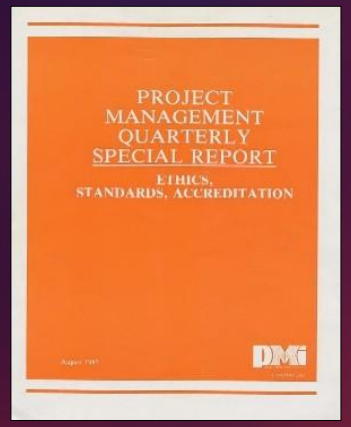






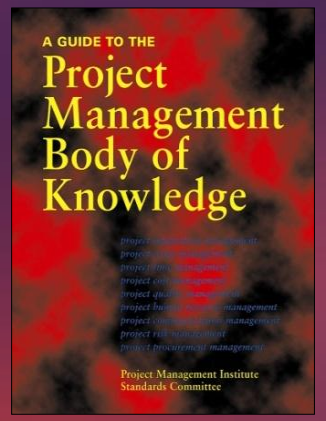
注：PRINCE2（Project IN Controlled Environment，受控环境下的项目管理）是一种结构化的项目管理方法论，由英国政府商务办公室（OGC）开发，在英联邦和欧洲国家的公共服务部门和私营企业中得到广泛应用。

PMBOK®指南的演变



1983，ESA

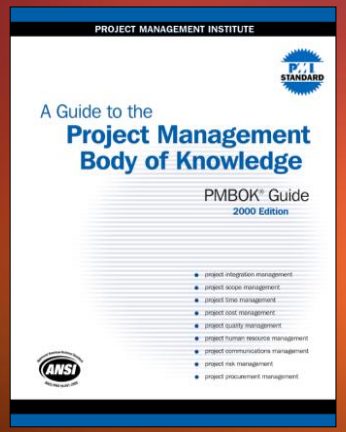
1987，修订



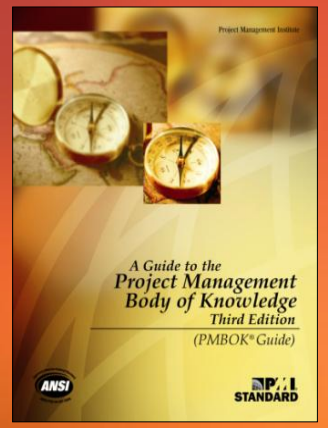
1996，第1版

2012，第5版

2000，第2版

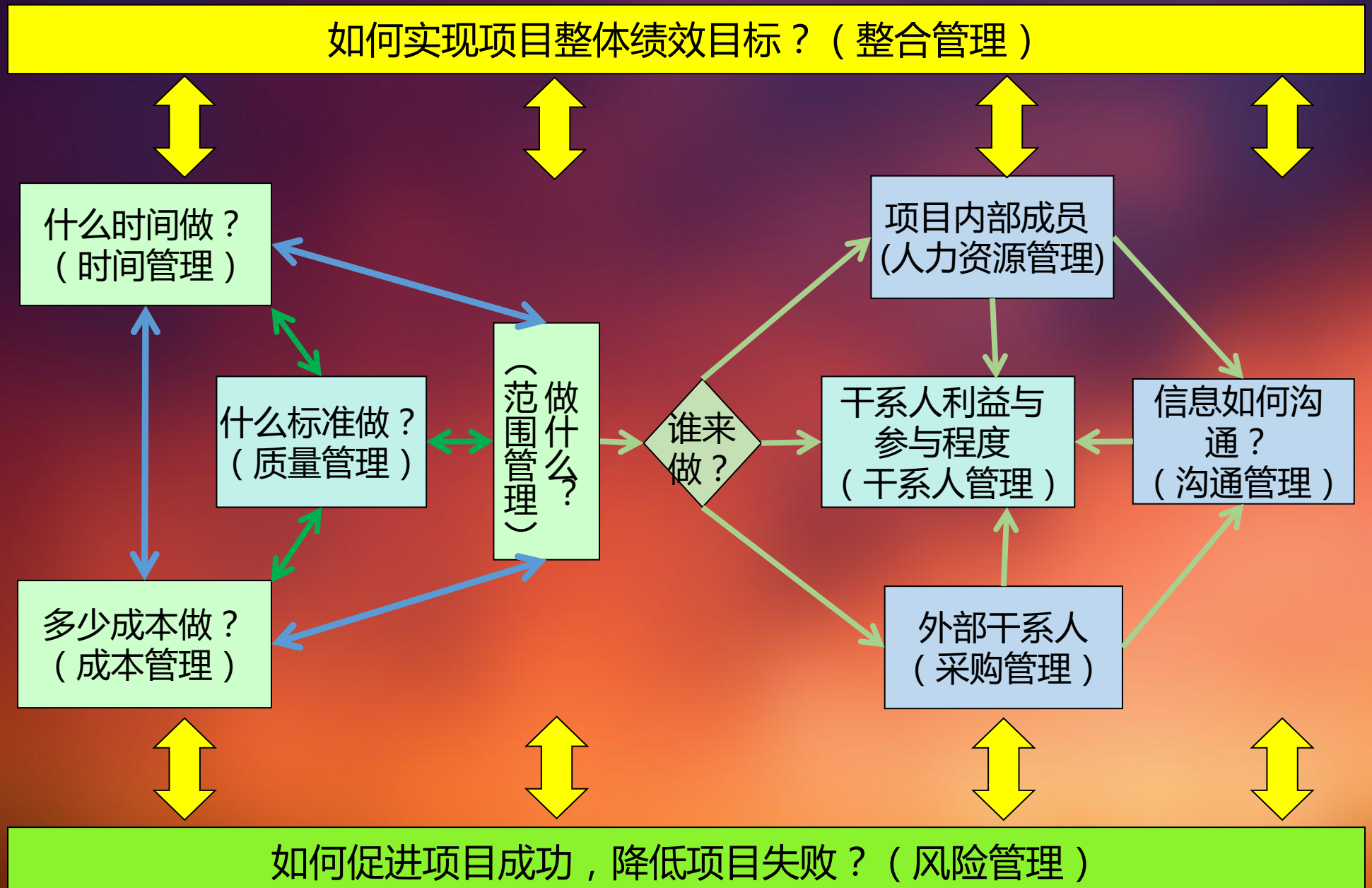


2004，第3版

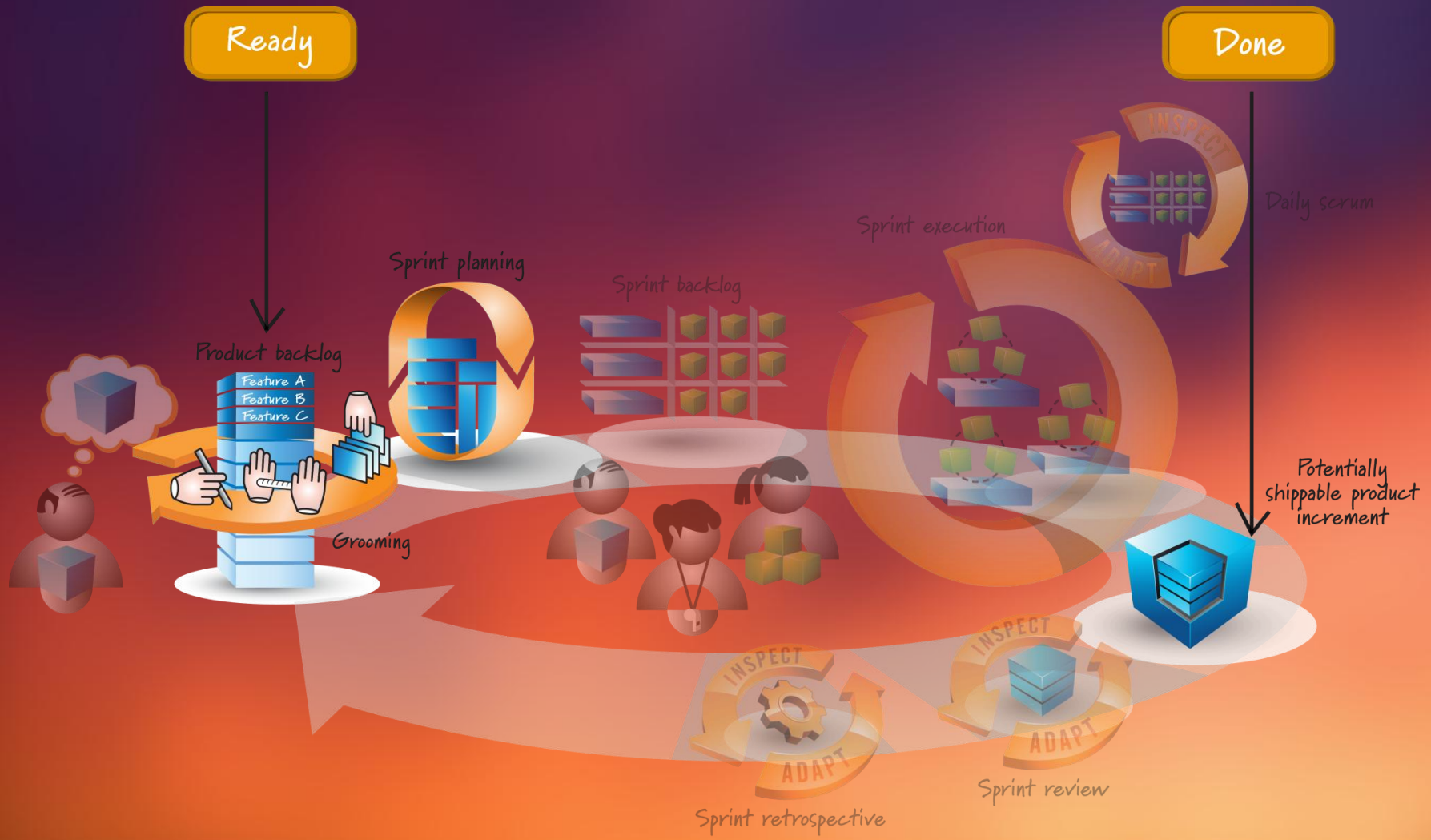


2008，第4版

PMP十大知识领域关系概要



敏捷项目管理



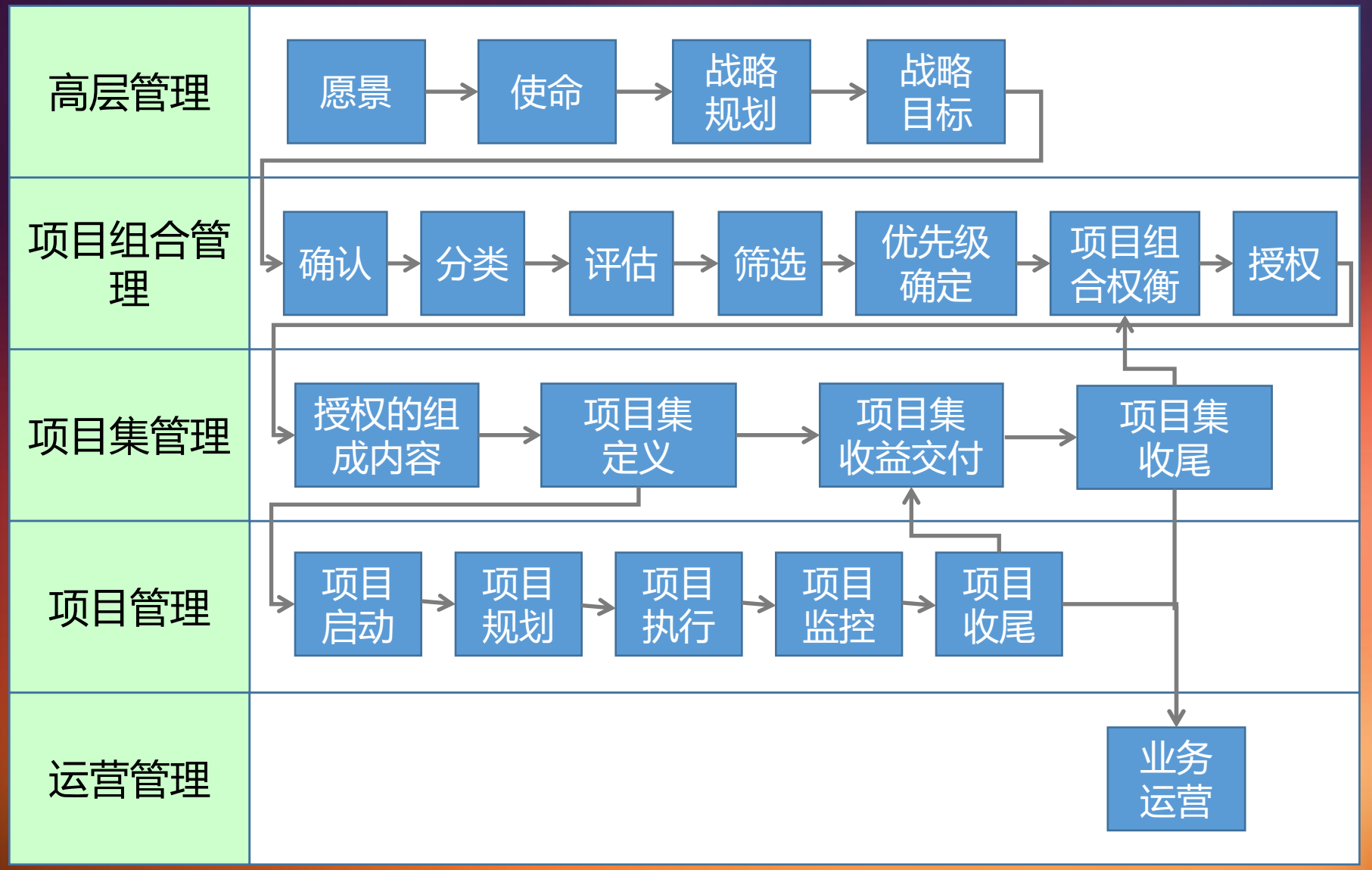
项目、项目集、项目组合

- 项目组合（Portfolio）是指为了实现**战略目标**而组合在一起管理的项目、项目集、子项目组合和运营工作

- 项目集（Program）是一组**相互关联且被协调管理**的项目、子项目集和项目集活动，以便获得分别管理所无法获得的利益。

- 项目管理是将知识、技能、工具与技术应用于项目活动，以满足项目的要求

组织各层次管理流程关系

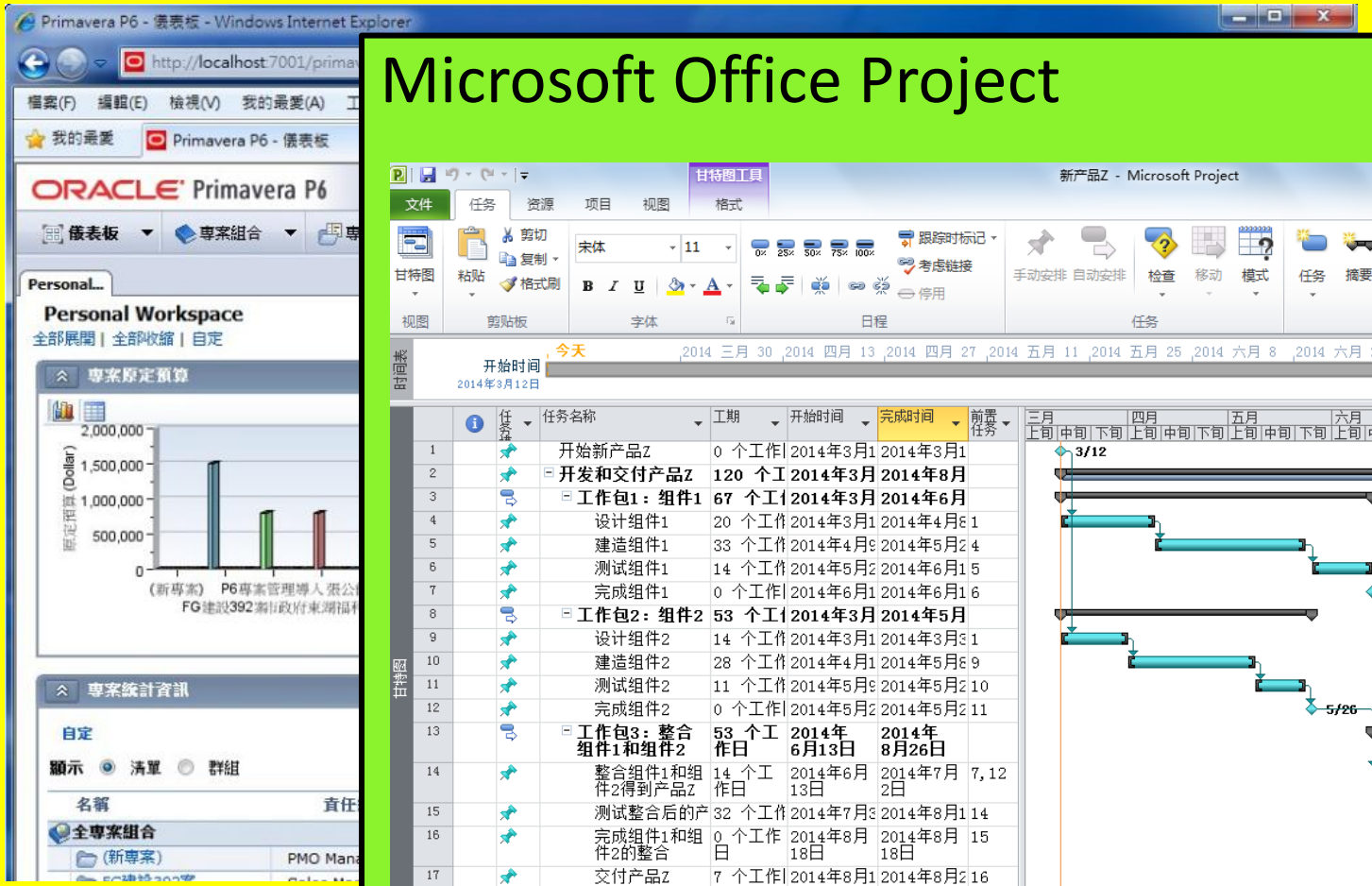


关键路径

- 关键路径是由一连串的任务组成，这条任务链在所有任务链中，**时间消耗最长**，所有的项目都有至少一条关键路径，一般只有一条。
- 它很重要，因为它代表了整个项目预计的**最短耗时**。
- 不在关键路径上的任务具有一定的**弹性**。

两款经典项目管理软件(甘特图)

Oracle Primavera P6



Microsoft Office Project

测试类型

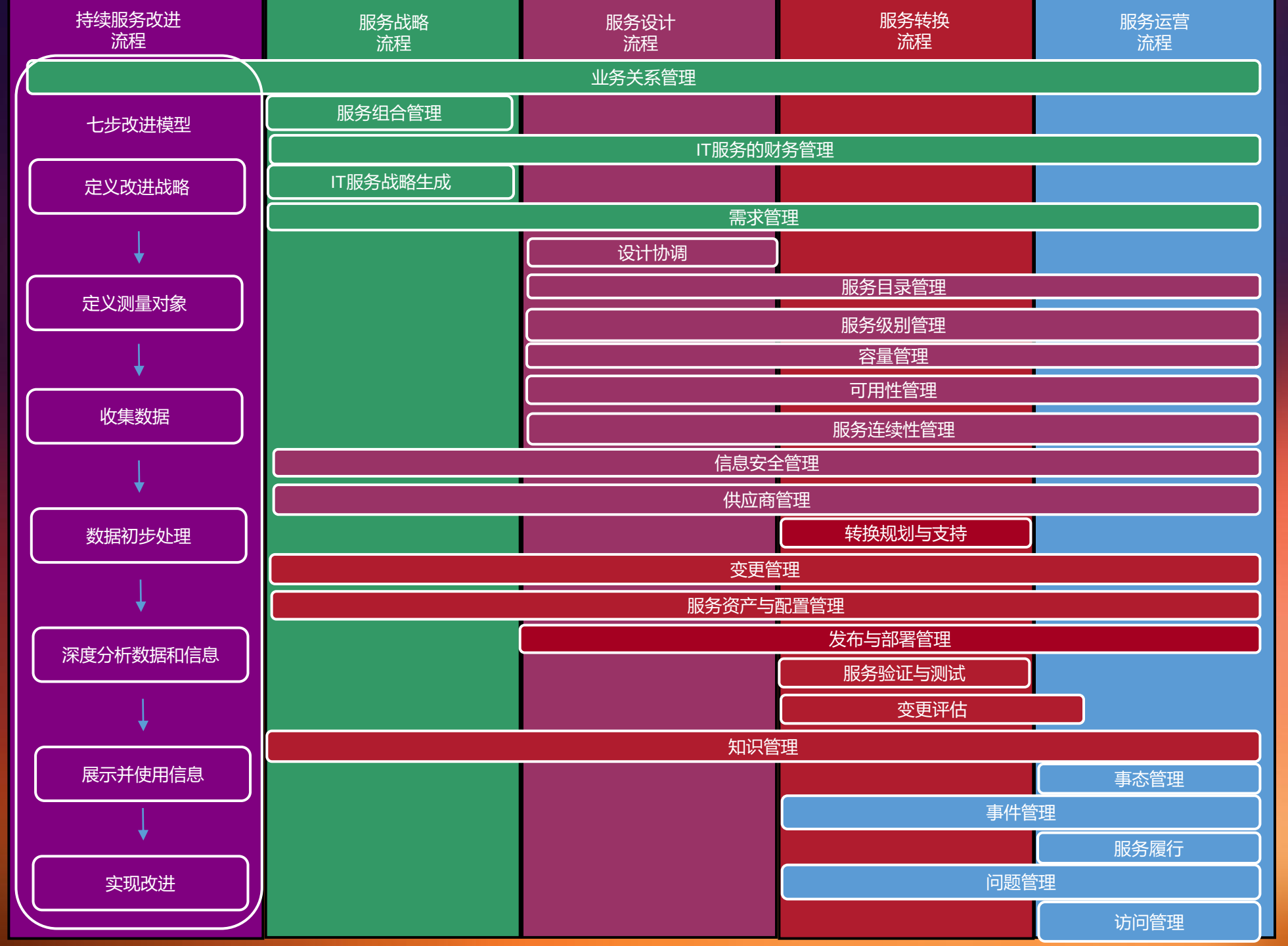
- 单体
- 集合/集成
- 系统
- 回归
- UAT
- 平行
- 灰度

4

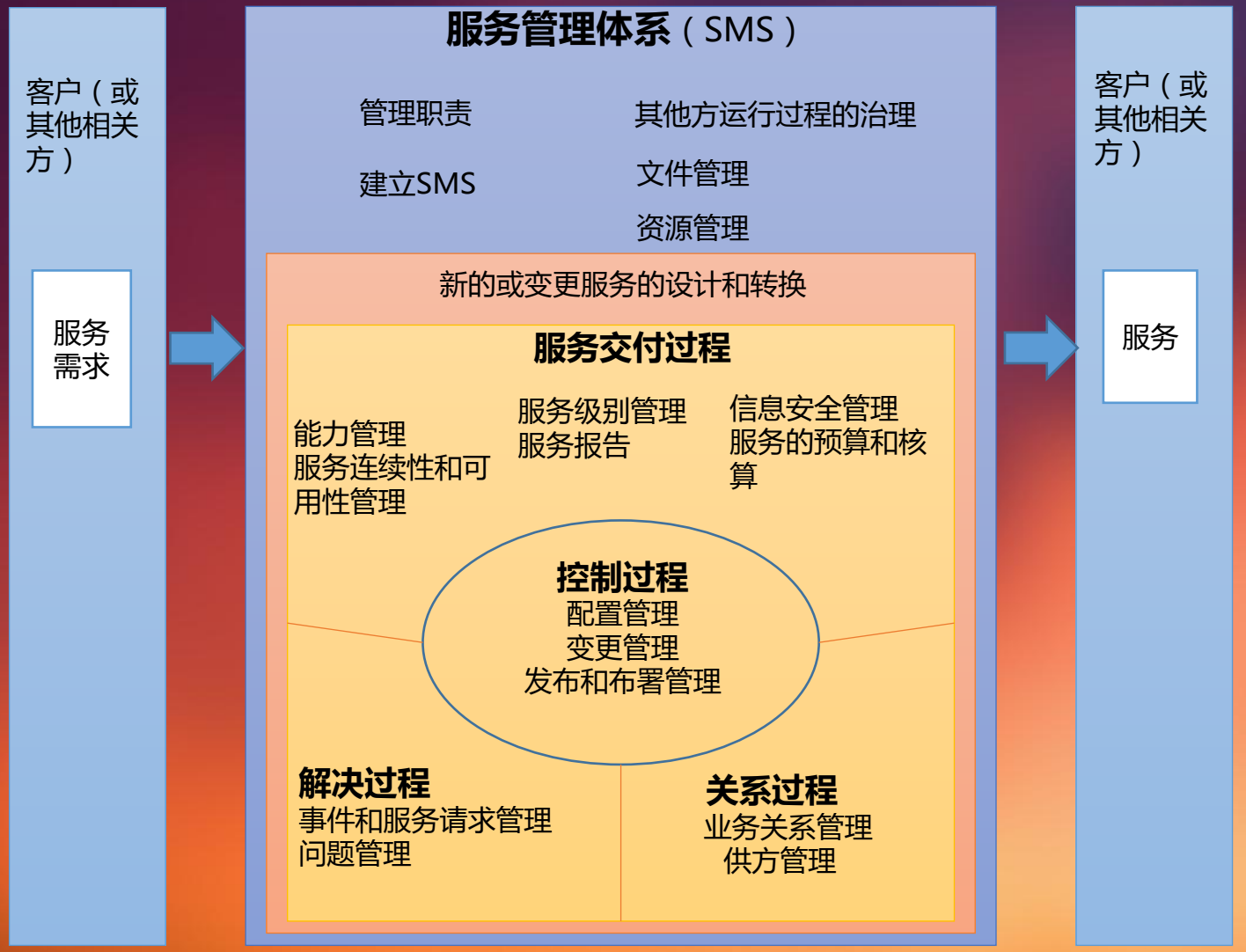
信息系统的运行、维护与支持

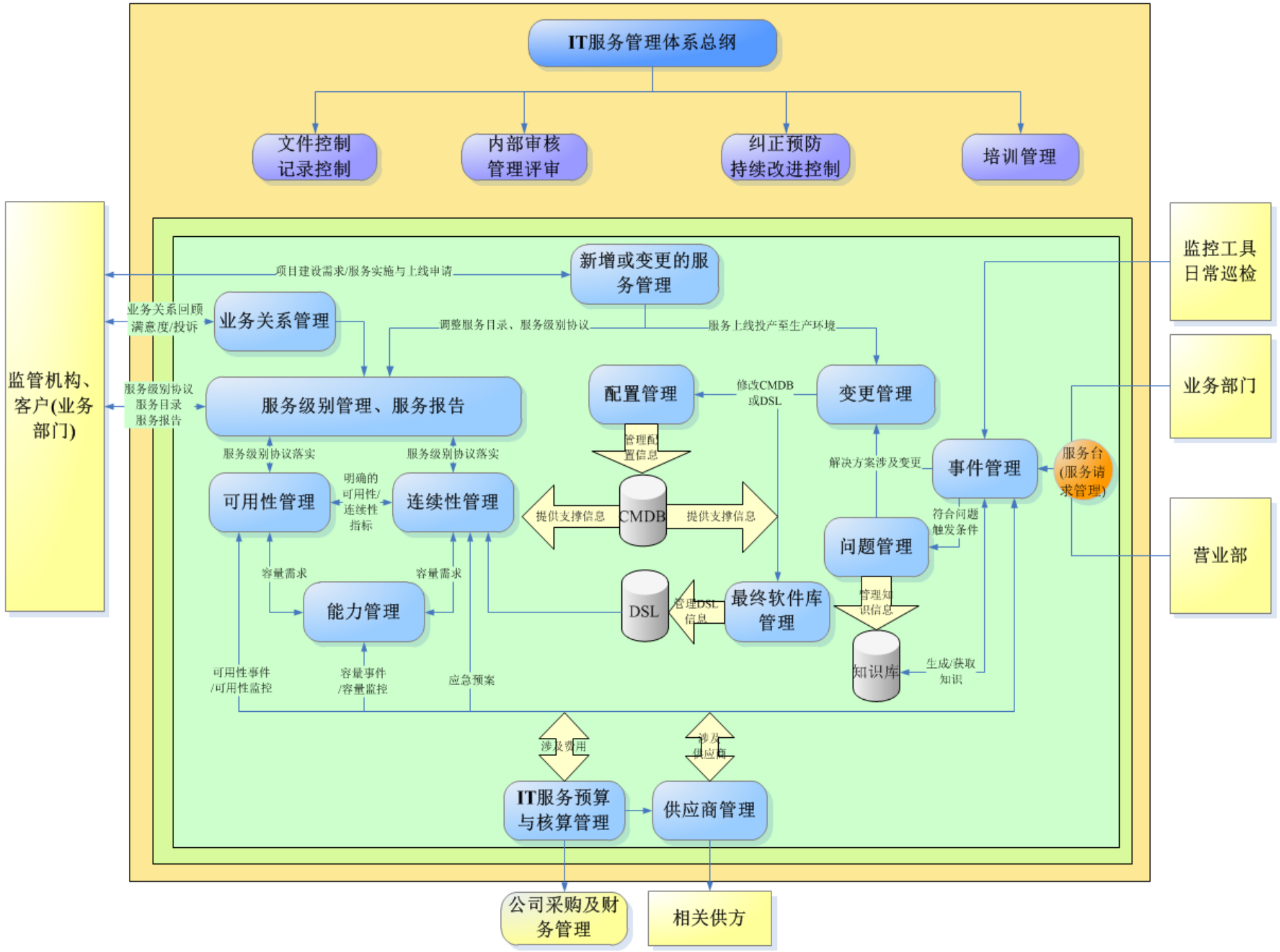
第四章信息系统运行、维护与支持

- 4.1综述
- 4.2信息系统运行
- 4.3 信息系统硬件
- 4.4信息系统结构和软件
- 4.5信息系统网络基础设施
- 4.6审计基础设施和运行
- 4.7灾难恢复计划


持续服务改进流程
服务战略流程
服务设计流程
服务转换流程
服务运营流程
业务关系管理
七步改进模型
服务组合管理
IT服务的财务管理
定义改进战略
IT服务战略生成
需求管理
设计协调
定义测量对象
服务目录管理
服务级别管理
容量管理
收集数据
可用性管理
服务连续性管理
信息安全管理
供应商管理
数据初步处理
转换规划与支持
变更管理
服务资产与配置管理
深度分析数据和信息
发布与部署管理
服务验证与测试
变更评估
知识管理
展示并使用信息
事态管理
事件管理
服务履行
实现改进
问题管理
访问管理

ISO20000管理体系标准的结构




IT服务管理体系总纲
文件控制
记录控制
内部审核
管理评审
纠正预防
持续改进控制
培训管理
监管机构、客户(业务部门)
监控工具日常巡检
业务部门
营业部
项目建设需求/服务实施与上线申请
新增或变更的服务管理
业务关系回顾
满意度/投诉
业务关系管理
调整服务目录、服务级别协议
服务上线投产至生产环境
服务级别协议
服务目录
服务报告
服务级别管理、服务报告
配置管理
修改CMDB或DSL
变更管理
管理配置信息
服务级别协议落实
服务级别协议落实
解决方案涉及变更
事件管理
服务台(服务请求管理)
可用性管理
明确的可用性/连续性指标
连续性管理
提供支撑信息
CMDB
提供支撑信息
符合问题触发条件
问题管理
容量需求
容量需求
能力管理
DSL
管理DSL信息
最终软件库管理
管理知识信息
知识库
生成/获取知识
可用性事件/可用性监控
容量事件/容量监控
应急预案
涉及费用
涉及供应商
IT服务预算与核算管理
供应商管理
公司采购及财务管理
相关供方

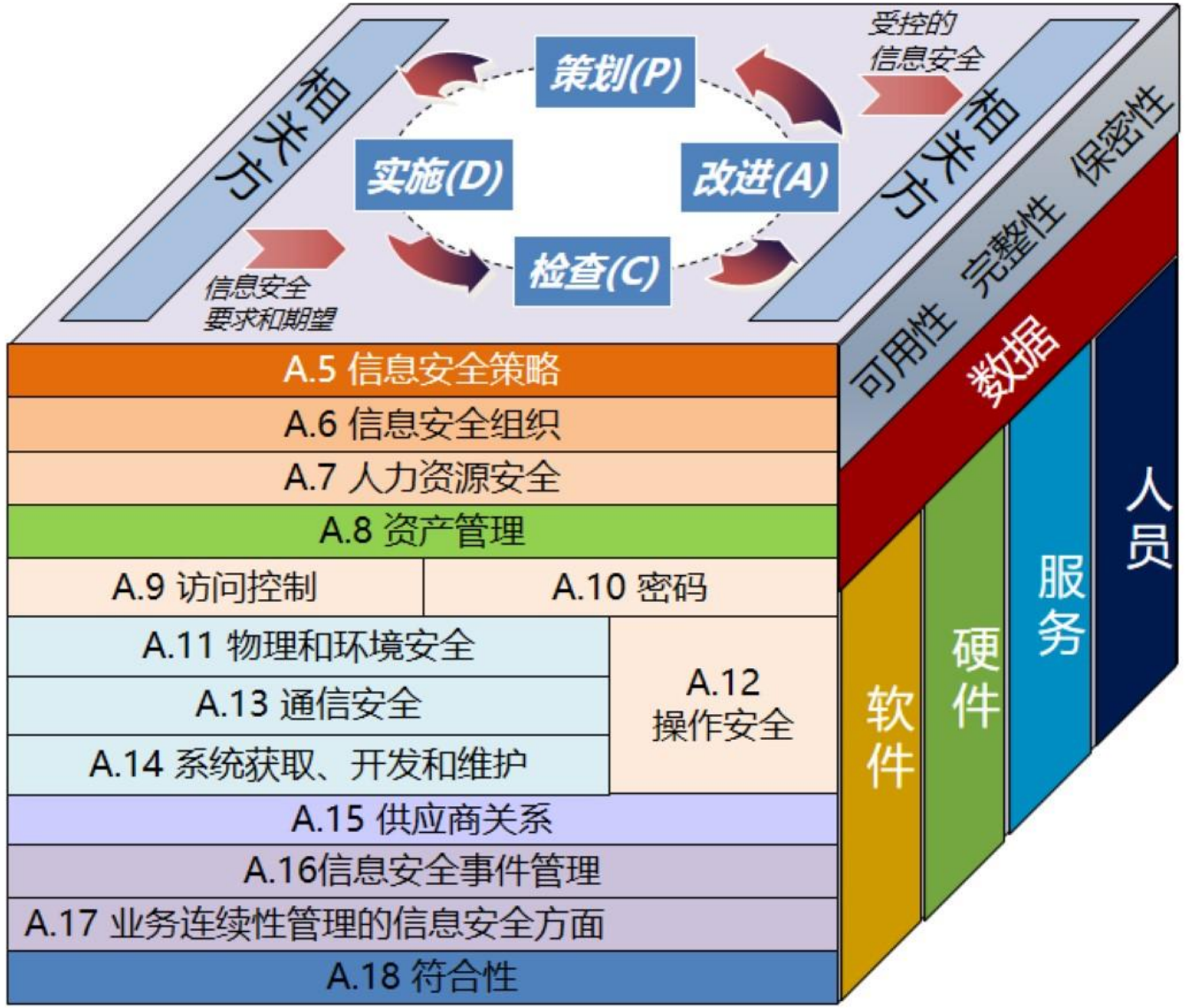
5

信息资产的保护

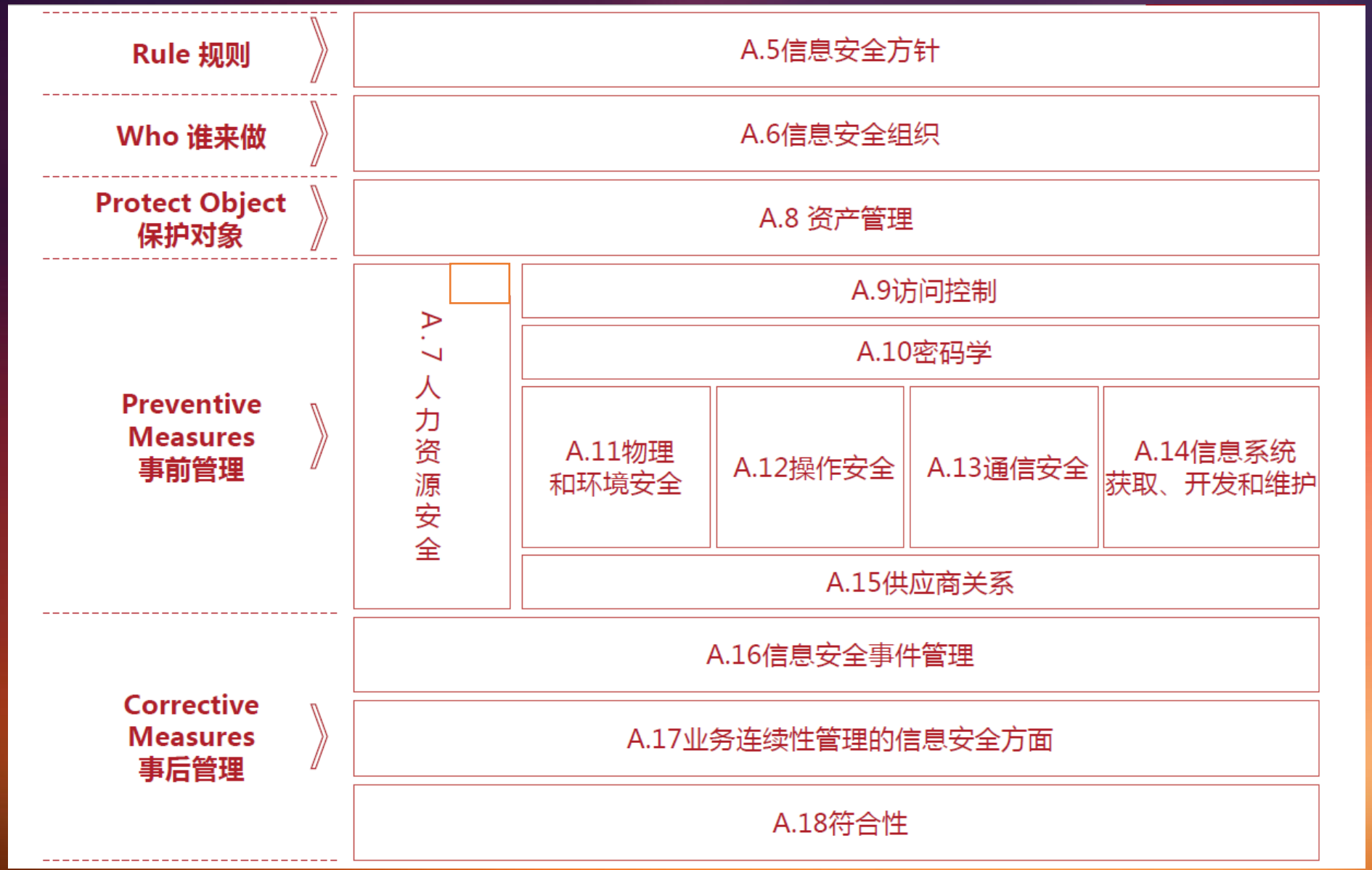
第五章 信息资产保护

- 5.1概述
- 5.2信息安全管理的重要性
- 5.3逻辑访问控制
- 5.4网络基础设施安全
- 5.5对信息安全管理框架进行审计
- 5.6网络基础架构的安全审计
- 5.7环境风险与控制
- 5.8物理访问风险与控制
- 5.9移动计算

ISO27001：2013版整体框架



ISO 27001的信息安全领域（2013版 附录A）



提问

Stay Hungry , Stay Foolish

Thank you

北宙咨询 North Universe

Trendsetting Consulting

特别鸣谢

艾拓咨询 AituoXianfeng Consulting