COBIT模型培训

叶佑林

2011/10/21

内容安排

1.IT审计介绍

2.IT治理介绍

3.COBIT概念

4.COBIT体系框架

5.Q&A

IT审计介绍

- 信息系统审计(ITA)是以企业或政府等组织的信息系统为审计对象，通过现代的审计理论和IT管理理论，从信息资产的安全性、数据的完整性以及系统的有效性和效率性等方面出发，对其是否能够有效可靠的达到组织的战略目标进行全面的监测和评估，并为改善和健全组织对信息系统的控制提出详细的建议。

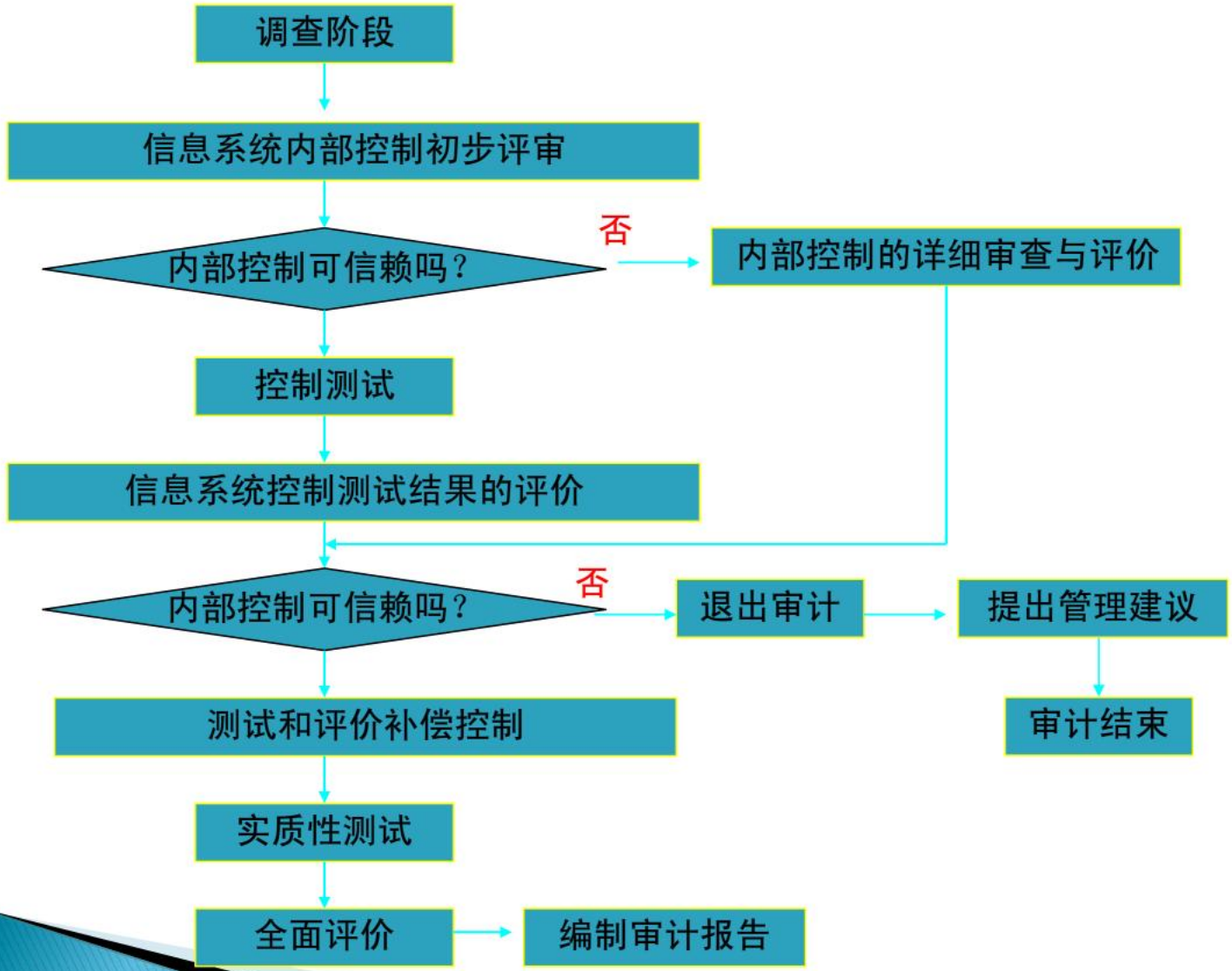
- IT审计对象是信息系统，审计内容是计算机资源管理、硬件、软件获取、系统软件、数据库、网络、应用系统开发、系统维护、操作、安全等审计

IT审计目标

- Asset Security（资产安全性）
- Effectivity（系统有效性）
- Efficiency（系统效率性）
- Data Integrity（数据完整性）

IT审计流程

- 信息系统调查
- 信息系统内部控制测试
- 信息系统初步评价
- 信息系统实质性测试
- 信息系统综合评价



计算机信息系统审计流程

信息系统调查

- 信息系统调查是对被审计单位信息系统的管理体制、总体架构、规划设计、管理水平等进行全面、深入地了解，是进行信息系统审计的基础。
- 了解管理体制，从总体上把握被审计单位信息系统管理的基本情况。
- 了解总体架构，完成对被审计单位有什么类型的信息系统，每个系统有多少子系统，信息系统分布在哪些部门，信息系统之间有什么关系的调查。
- 了解规划管理，对信息系统建设、使用、管理情况的调查。

IT内部控制

- IT内部控制的类型：根据控制的范围，信息系统内部控制分为
  - 一般控制
  - 应用控制

一般控制

是指对整个计算机信息系统及环境要素实施的，对系统所有的应用或功能模块具有普遍影响的控制措施。划分成五类控制：

- 组织控制：为实现组织的目标而进行的组织结构设计、权责安排和制度设计。包括职责分离、授权、监督、人事管理等
- 系统开发与维护控制：包括需求定义、开发规划、系统设计、编程实现、测试、运行维护、文档管理等控制

一般控制

- 安全控制：保持良好的运行环境，包括访问接触、环境安全、防病毒、安全保密、安全教育等控制
- 硬件及系统软件控制

（1）硬件控制

（2）软件控制

- 5、操作控制

信息系统的使用操作应有一套完整的管理制度，包括上机守则与操作规程、上级日志记录、保密制度和操作工作计划等。

应用控制

应用控制是为适应各种数据处理的特殊控制要求，保证数据处理完整、准确地完成而建立的内部控制。

分成三类控制

- 输入控制：保证只有经过授权批准的业务才能输入计算机信息系统；保证经批准的数据没有丢失、遗漏和篡改；保证被计算机拒绝的错误数据能改正后重新提交。包括数据采集、数据输入控制

应用控制

- 处理控制：对信息系统进行的内部数据处理活动的控制措施，这些控制措施往往被写入计算机程序，包括数据有效性检测、错误纠正控制。
- 输出控制：主要是保证交付给用户的数据是符合格式要求的、可交付的，并以一致和安全的方式递交给用户，包括输出错误处理、输出报告管理、报告接收确认

内容安排

1.IT审计介绍

2.IT治理介绍

3.COBIT概念

4.COBIT体系框架

5.Q&A

IT治理提出的背景

- IT的应用越来越广泛，业务依赖程度越来越高
- IT投资规模巨大，ROI无法有效量化
- IT风险加剧
- IT与业务之间的沟通“代沟”
- 外部监管越来越严

IT治理

- 公司治理就是为所有股东创造和呈现价值的企业道德行为
- 公司治理包括组织中管理层、董事会、股东和其他利益相关法之间的一系列关系，它为制定公司目标、确定实现目标和监督绩效的方式提供了框架。

IT治理

"IT治理是公司治理的一个有机组成部分，它包含领导力、组织结构和流程等制度和机制，其确保IT维续和扩展组织的战略和目标。"

(来源: IT Governance Institute)

"IT治理是为了在使用IT的过程中得到我们所期望的结果而特别设计的决策权力和责任。"

(来源: MIT CISR)

IT治理

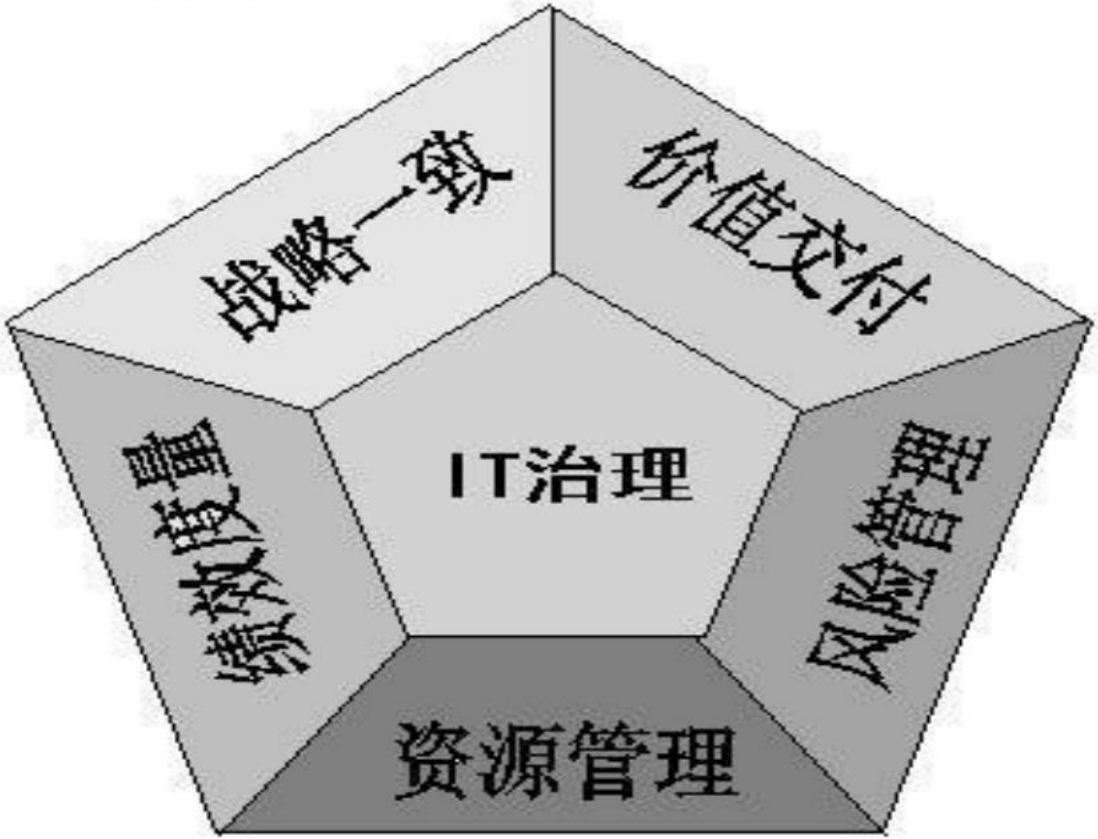
- IT治理是一个综合术语，它包括信息系统，技术和通讯，业务，法律相关事务，所有利益相关方，董事会，高级管理层，流程所有人，IT供应商，用户和审计师。IT治理有助于确保IT和企业目标保持一致。
- IT治理是组织中的一种制度安排，目的是为了提高IT绩效、降低IT风险，有效地利用资源。

- IT治理采用最佳实践来确保组织信息及相关技术支持其业务目标和价值交付，确保资源得到合理使用，风险得到适当管理、绩效得到测评。

IT治理

- IT治理在根本上关注以下两方面的问题：
  - IT向业务交付价值 ： 由IT和业务的战略一致驱动
  - IT风险得到管理： 通过向企业分配责任来驱动

IT治理领域



内容安排

1.IT审计介绍

2.IT治理介绍

3.COBIT概念

4.COBIT体系框架

5.Q&A

COBIT是什么？

- Control Objectives for Information and related Technology
- COBIT是一个在国际上得到公认的、先进的和权威的安全与信息技术管理和控制标准，它在业务风险、控制需要和技术问题之间架起了一座桥梁，它可以辅助管理层进行IT 治理，指导组织有效利用信息资源，有效地管理与信息相关的风险。

- 面向业务是COBIT的主题，它不仅是为用户和审计师而设计，而且更重要的是它可以作为管理者及业务过程的所有者的综合指南。

- COBIT真正关注的问题是，企业是否具备适当的控制力，以确保符合相关的管理规定。它帮助企业确定他们是否正在做他们表示要做的事，以及他们是否可以证明这一点

COBIT 发展历程

- COBIT第一版由信息系统审计与控制基金会（ISACF）于1996年发布。
- COBIT第二版于1998年出版，修订了高层控制目标与详细控制目标，增加了实施工具集（Implementation Tool Set）
- 信息系统审计与控制协会（ISACA）及其相关的基金会在1998年创立 IT治理研究院(ITGI)，由ITGI制定并发布了COBIT第三版，加入了管理指南，以及扩展和加强了对IT治理的关注；
- COBIT基于ISACF的建立的IT控制目标，参照了其他控制框架、行业标准；
- ITGI于2005年底发布了COBIT第四版，这一版对IT某些过程进行了调整，强调了IT控制与IT治理五个领域的对应关系。

COBIT 发展历程

- 早期第1、2版以控制目标和审计指南为主。
- 2000年推出第3版，重点突出了“管理指南”。
- 2006年推出第4版，精简了控制目标，并完善了管理指南
- 2007年推出第4.1版，将审计指南改为“签证指南”，并提出ValueIT等理念，与IT治理联系更紧密。

IT资源

- COBIT中定义的IT资源如下。
- (1)数据：是最广泛意义上的对象(如外部和内部的)、结构化及非结构化的、 图形、声音等。
- (2)应用系统：手工的以及计算机程序的总和。
- (3)技术：包括硬件、操作系统、数据库管理系统、网络、多媒体等。
- (4)设备：包括所拥有的支持信息系统的所有资源。
- (5)人员：包括员工技能、意识，以及计划、组织、获取、交付、支持和监控信息系统及服务的能力。

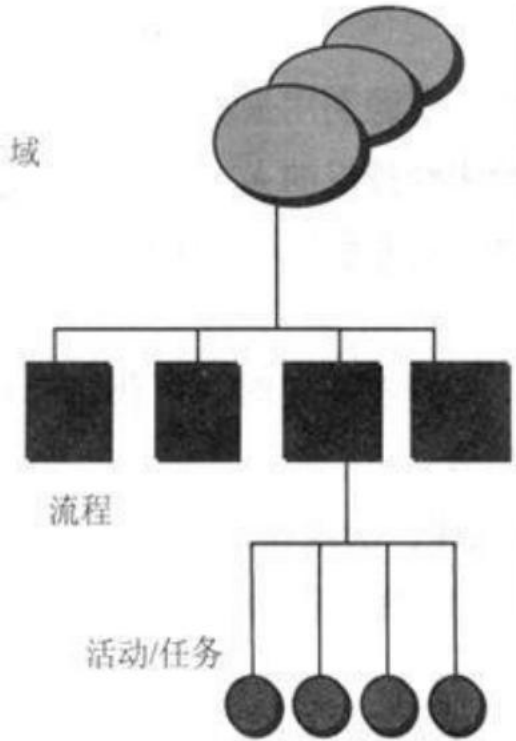
IT准则

- COBIT定义了7方面的信息标准：
  - 效果性（Effectiveness）：信息系统提供对业务处理来说“有效”的信息
  - 效率性（Efficiency）：“有效率”地使用资源，提供信息
  - 保密性（Confidentiality）：保护敏感信息，避免泄漏信息
  - 一致性（Integrity）：保证信息的“真实可信”，即信息准确、完整，并且从业务价值和业务需要的角度来说是正确有效的
  - 可用性（Availablity）：当业务需要时，信息可随时获得
  - 可靠性（Reliability）：为管理层维持组织运转和履行所赋予职责提供适当的信息
  - 合规性（Compliance）：符合相关法律、规定、合同对业务过程的规定

活动、过程、域

- 活动：企业的信息系统是由一个个功能组成的，它们对应于企业经营领域的一个个活动。
- 过程：这些活动可以按照彼此之间关系的紧密程度或者目标的一致程度归结为一些过程，例如，定义IT战略规划、定义信息体系结构、管理IT投资、风险评估，等等。
- 域：过程之间的自然组合形成企业的域，与企业结构的职责域相对应。

活动、过程、域



过程被自然归组成域。过程的自然组合被作为组织结构的职责域相匹配

一系列具有自然(或有控制的)间隔的活动和任务的组合

包含可测量结果的活动或任务，活动有一个生命周期而任务是离散的，不连续

内容安排

1.IT审计介绍

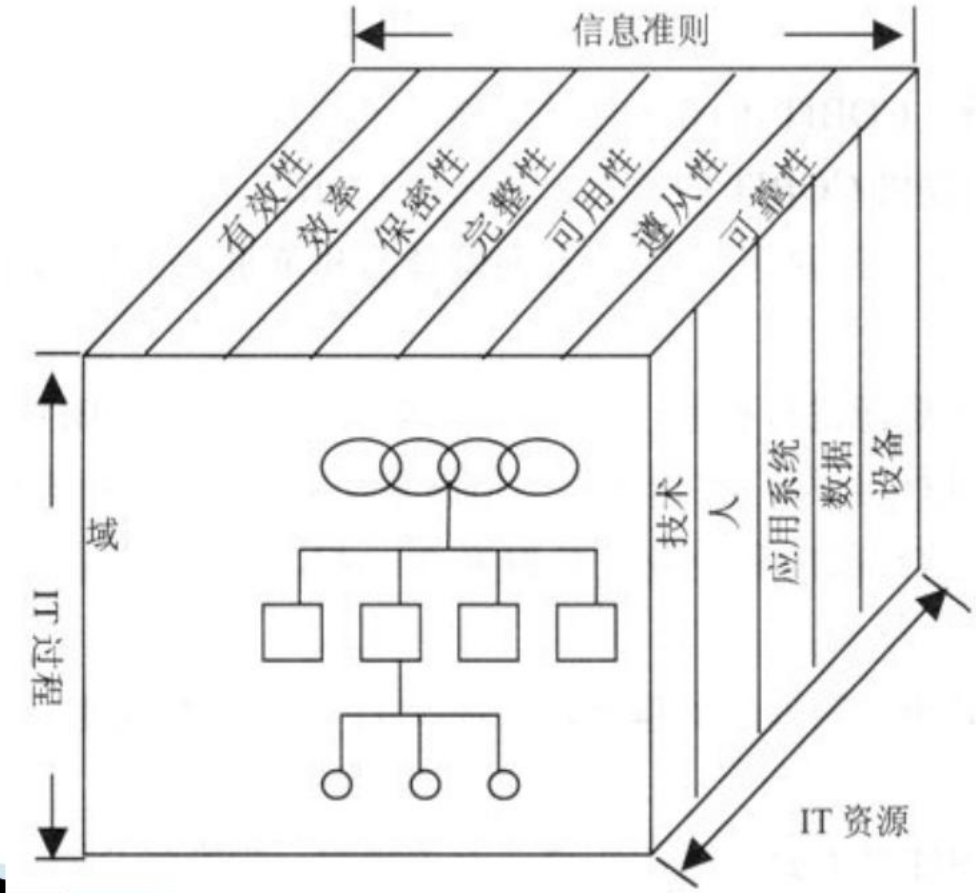
2.IT治理介绍

3.COBIT概念

4.COBIT体系框架

5.Q&A

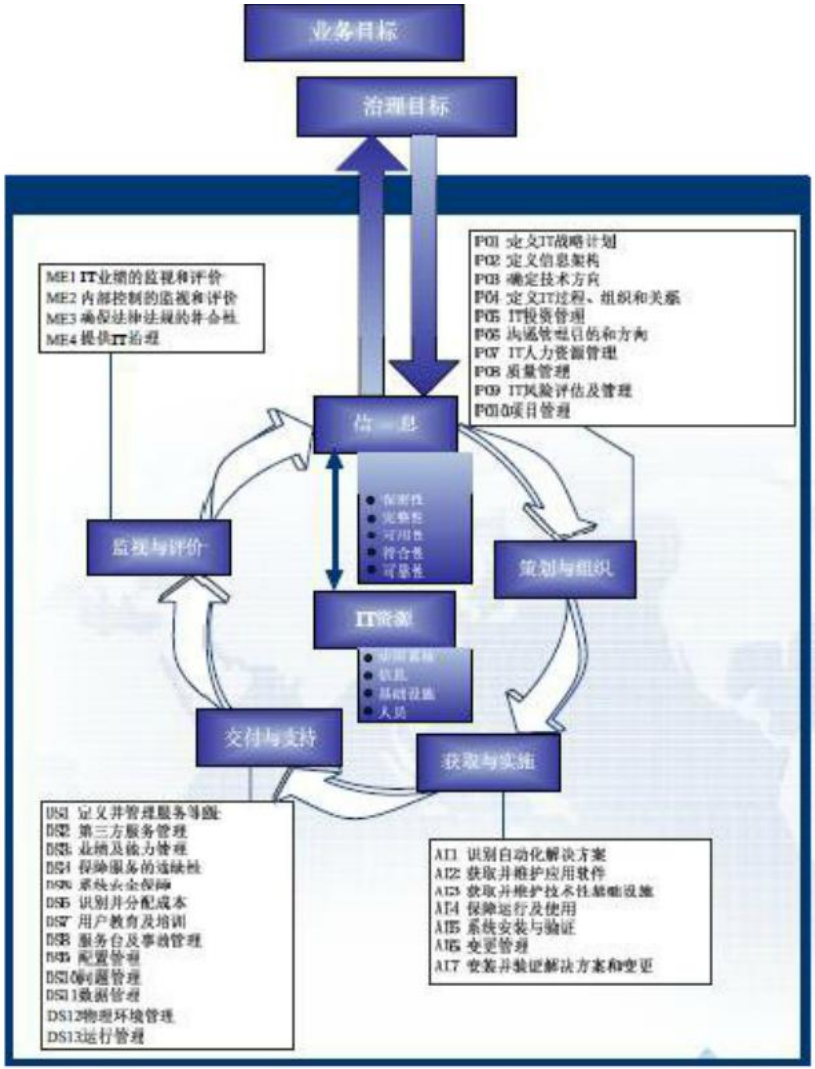
COBIT框架模型



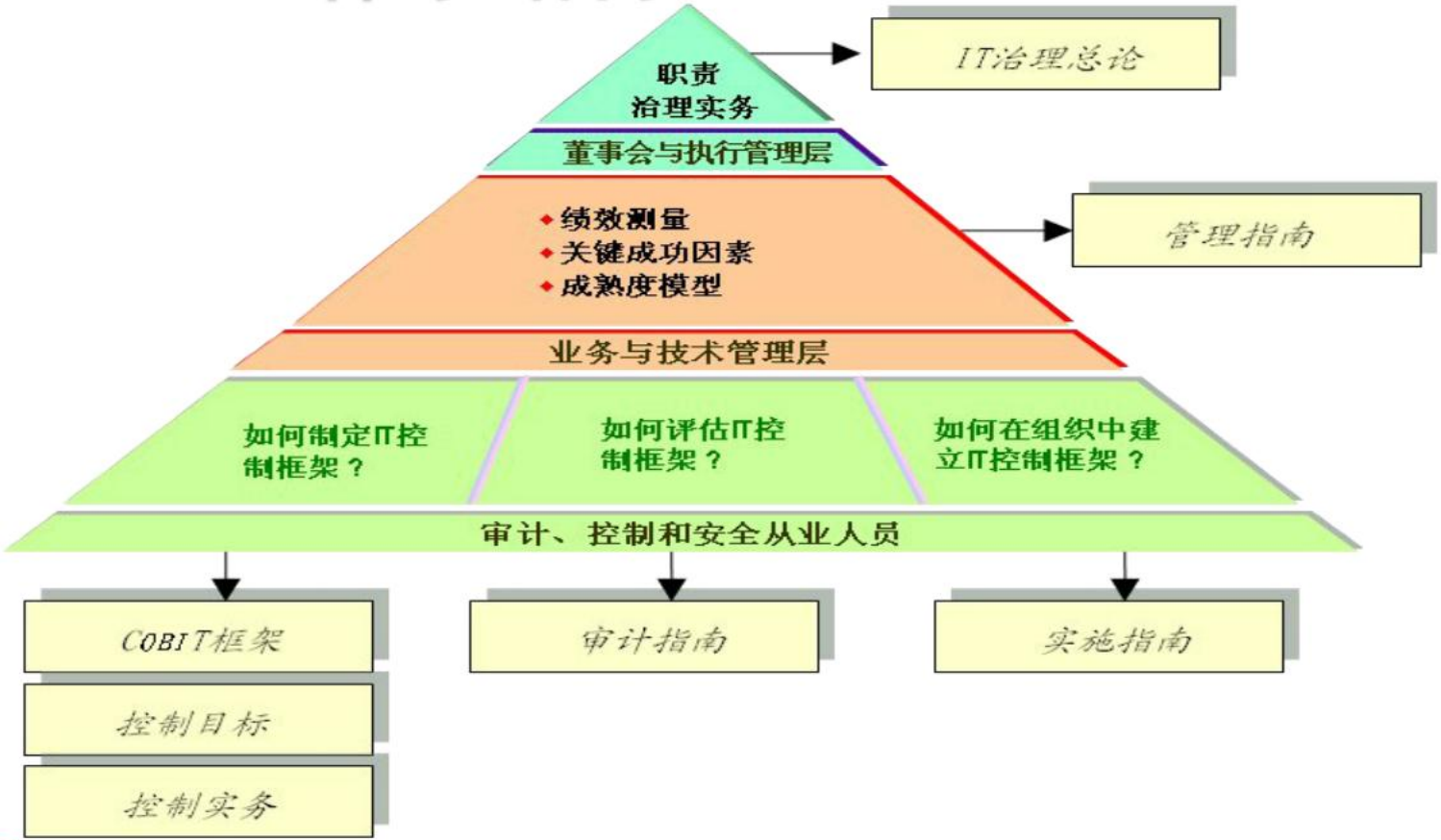
CoBit框架模型

Cobit可细化为34项高层控制目标，318个细化控制目标

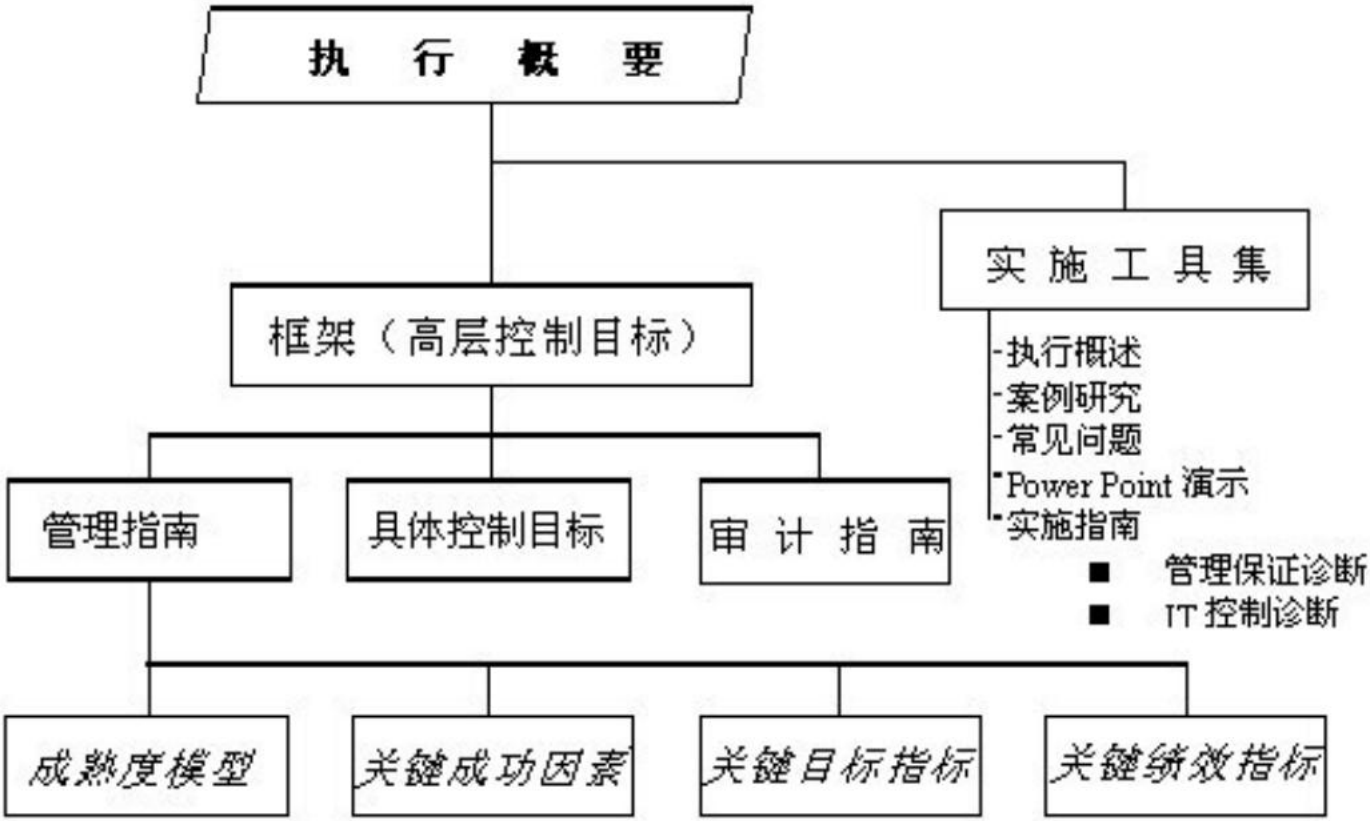
。每个目标都针对特定的IT过程；这些高层控制目标又可组合为策划与组织、采购与实施、交付与支持、监控四大领域。



COBIT体系结构


职责
治理实务
董事会与执行管理层
绩效测量
关键成功因素
成熟度模型
业务与技术管理层
如何制定IT控制框架？
如何评估IT控制框架？
如何在组织中建立IT控制框架？
审计、控制和安全从业人员
IT治理总论
管理指南
COBIT框架
控制目标
控制实务
审计指南
实施指南

COBIT产品簇


执 行 概 要
框架（高层控制目标）
实 施 工 具 集
-执行概述
-案例研究
-常见问题
-Power Point 演示
-实施指南
管理指南
具体控制目标
审 计 指 南
管理保证诊断
IT 控制诊断
成熟度模型
关键成功因素
关键目标指标
关键绩效指标

COBIT体系结构

- 控制目标（Control Objectives）
- 在34个高层控制目标的基础上，为每个IT过程定义了更为详细的控制目标（detail objectives，共计318个），用以指导IT控制工作、保证该过程的成功实施。

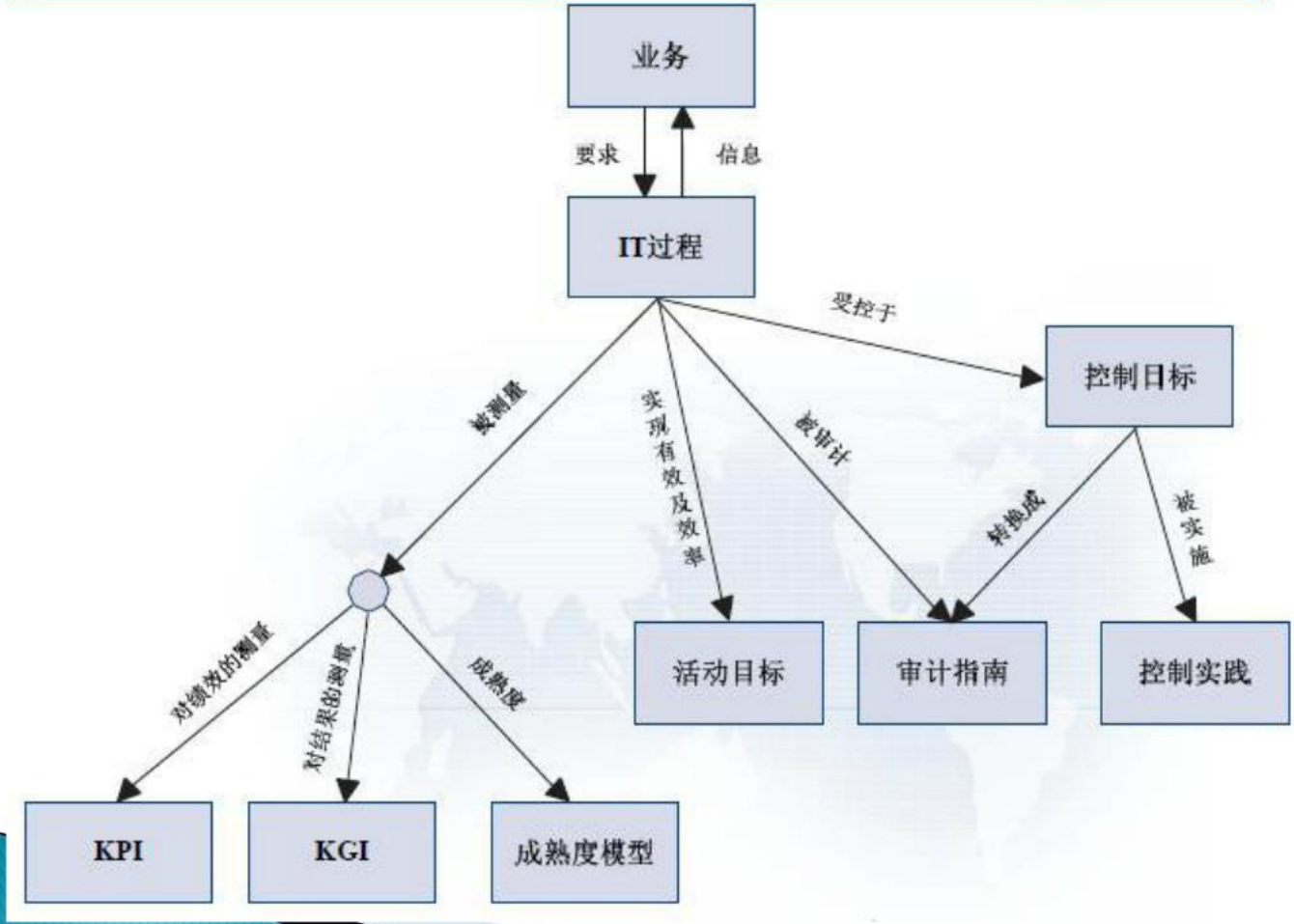
COBIT体系结构

- 审计指南（Audit Guideline）
- 针对每个IT过程分别提出了审计方法，通过对照审查相应的控制目标实现对IT过程的评价和建议。
  - 内容：
  - 如何了解该过程相关内控，包括应面询的对象、问题、应查阅的文档
  - 如何评价该过程的控制，包括具体要核查的项目
  - 该过程中常规的符合性测试项目
  - 该过程中常规的实质性测试项目

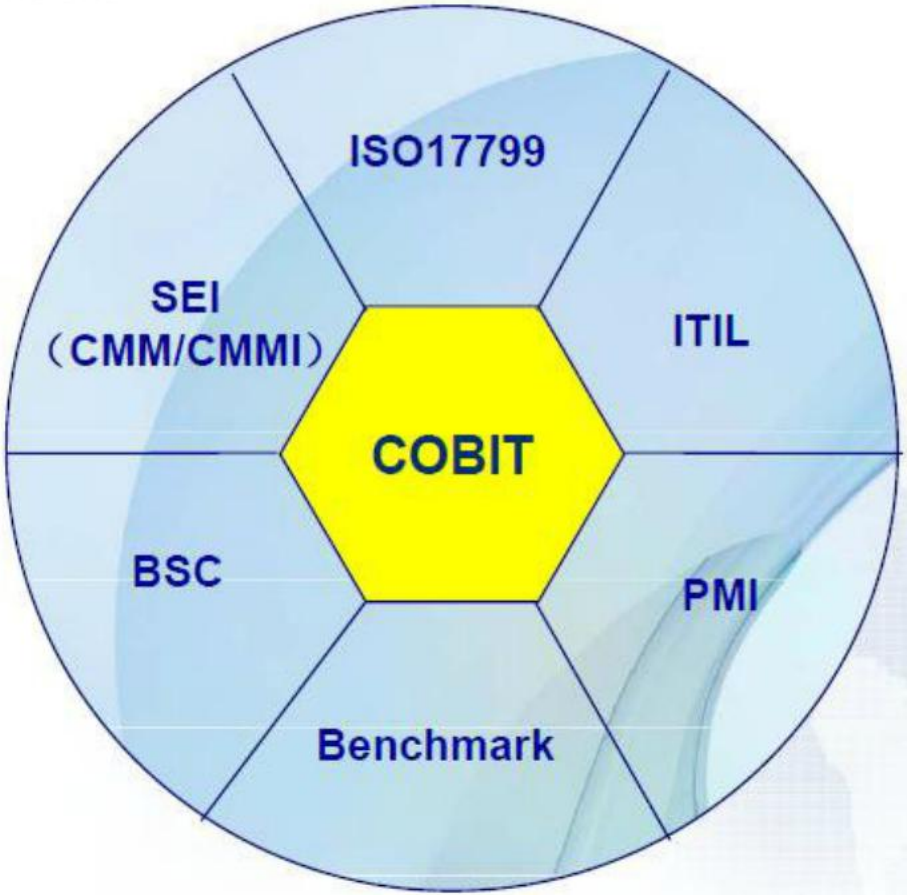
COBIT体系结构

- 管理指南（Management Guideline）
- 针对每个IT过程均为管理者详细定义了下列分析工具：
  - 关键成功因素（CSF）：管理者“应该作什么？”，即在每一个过程中最重要的因素或控制活动，可以作为IT投资的指导之一。
  - 关键目标指标（KGI）：IT过程“执行后的结果应该作到怎样”。若想实现业务目标，该过程执行后必须达到哪些指标。
  - 关键执行指标或关键性能指标（KPI）：怎样判断正在执行的IT过程当前的状态是否良好、是否需要调整。
  - 成熟度模型（CMM）：为每一个过程定义了六种成熟度级别，使管理者可以评价本组织在该过程控制上所处的级别，然后通过与同行业标竿企业相比较，判断自身所处的先进程度、竞争优势和改进方向。

COBIT各组件之间的关系



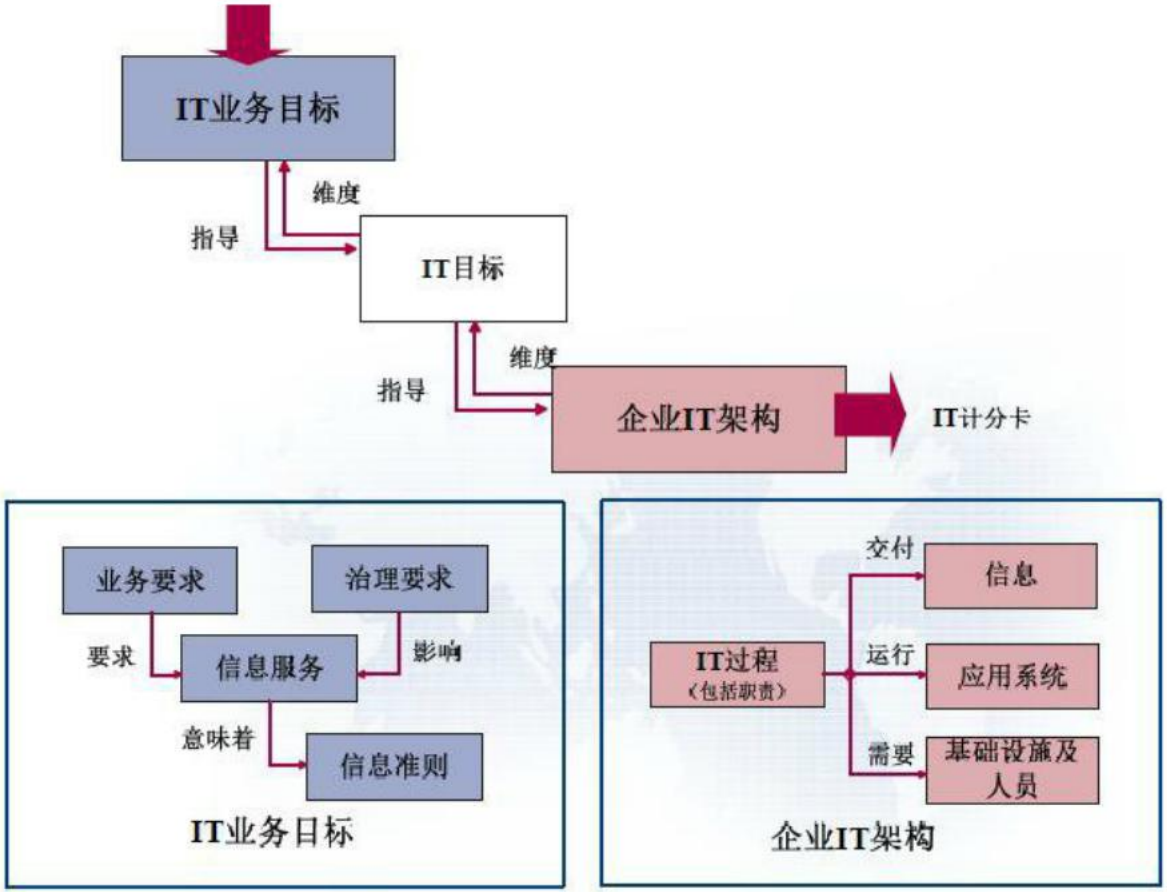
集大成者



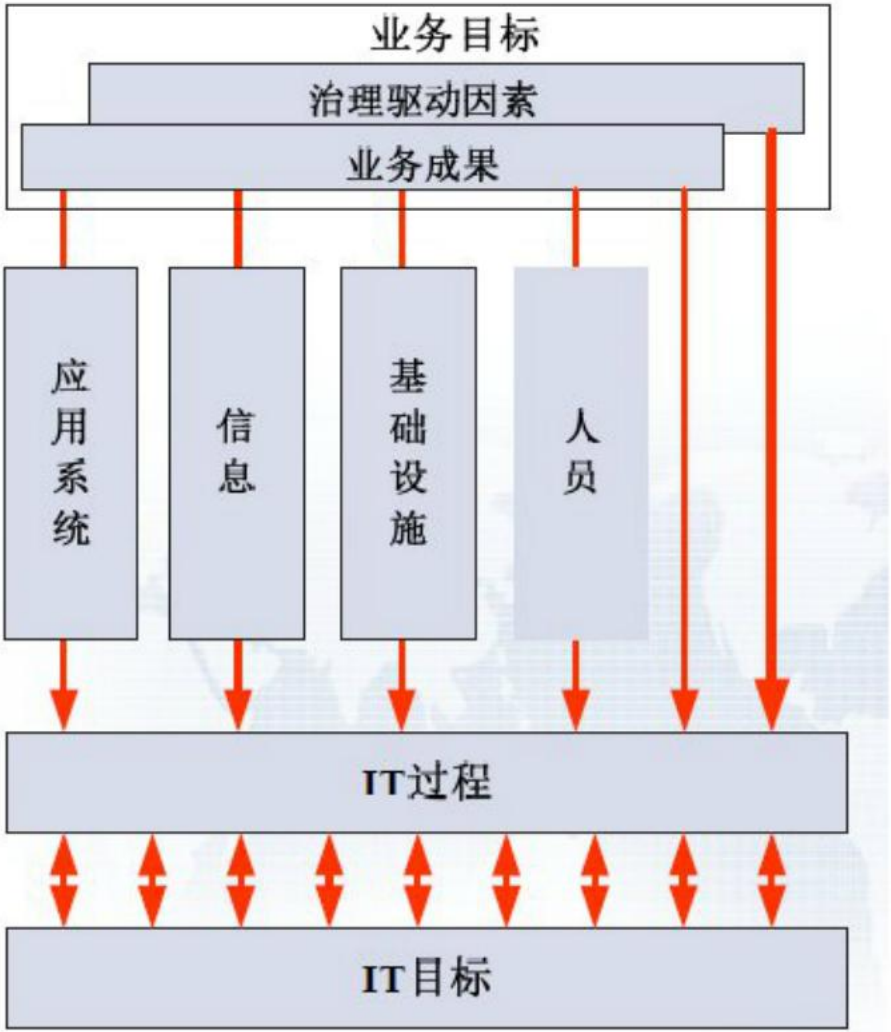
COBIT 特点


Business-focused
Measurement-driven
COBIT特点
Process-oriented
Controls-based

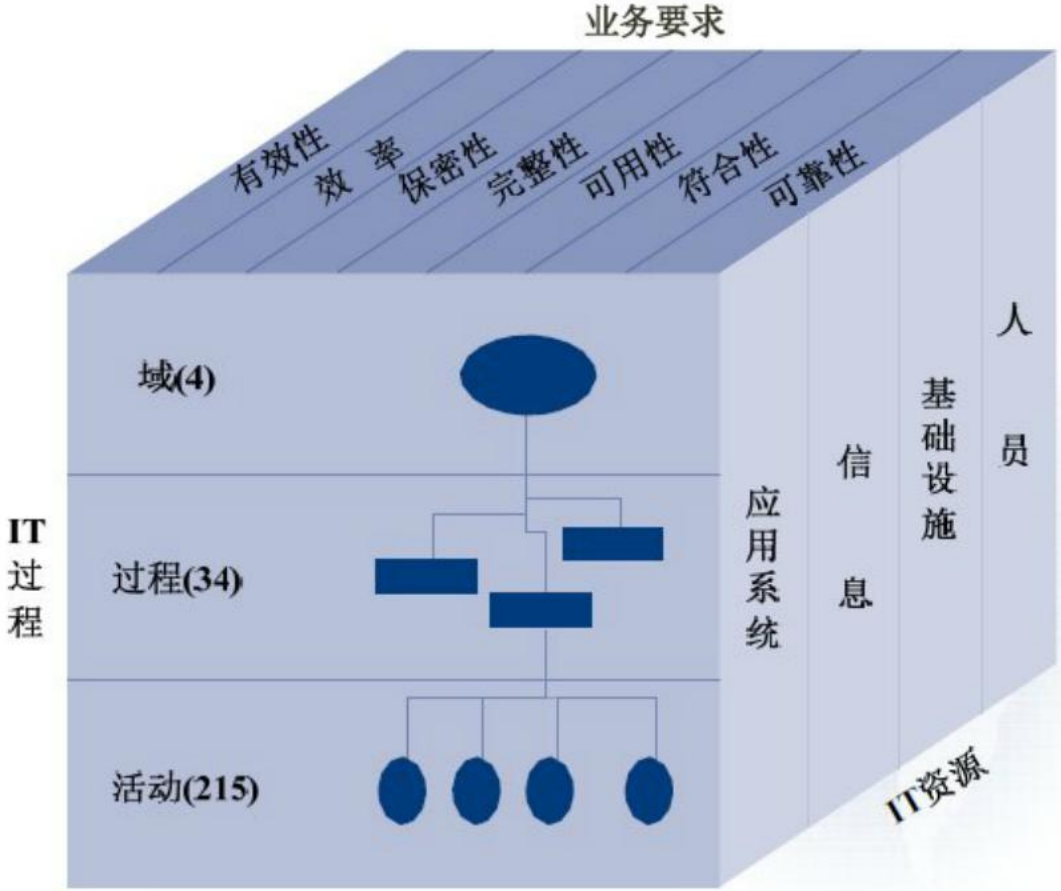
Business-focused



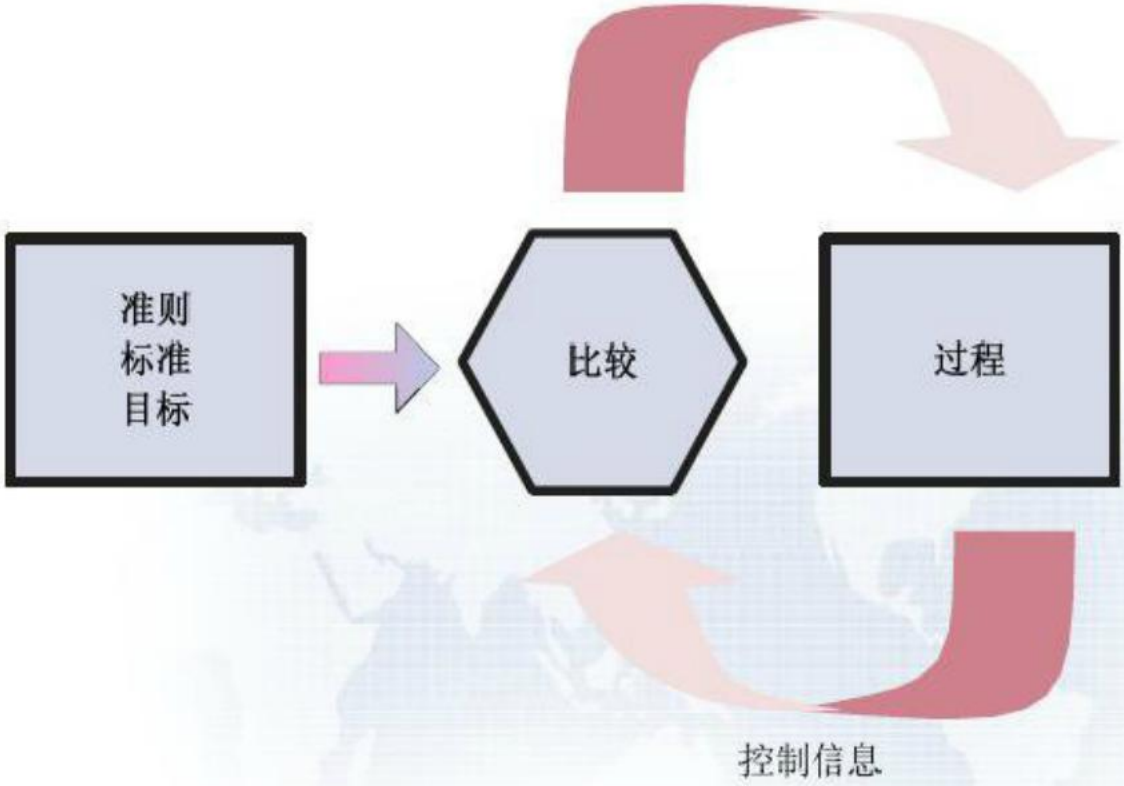
Business-focused



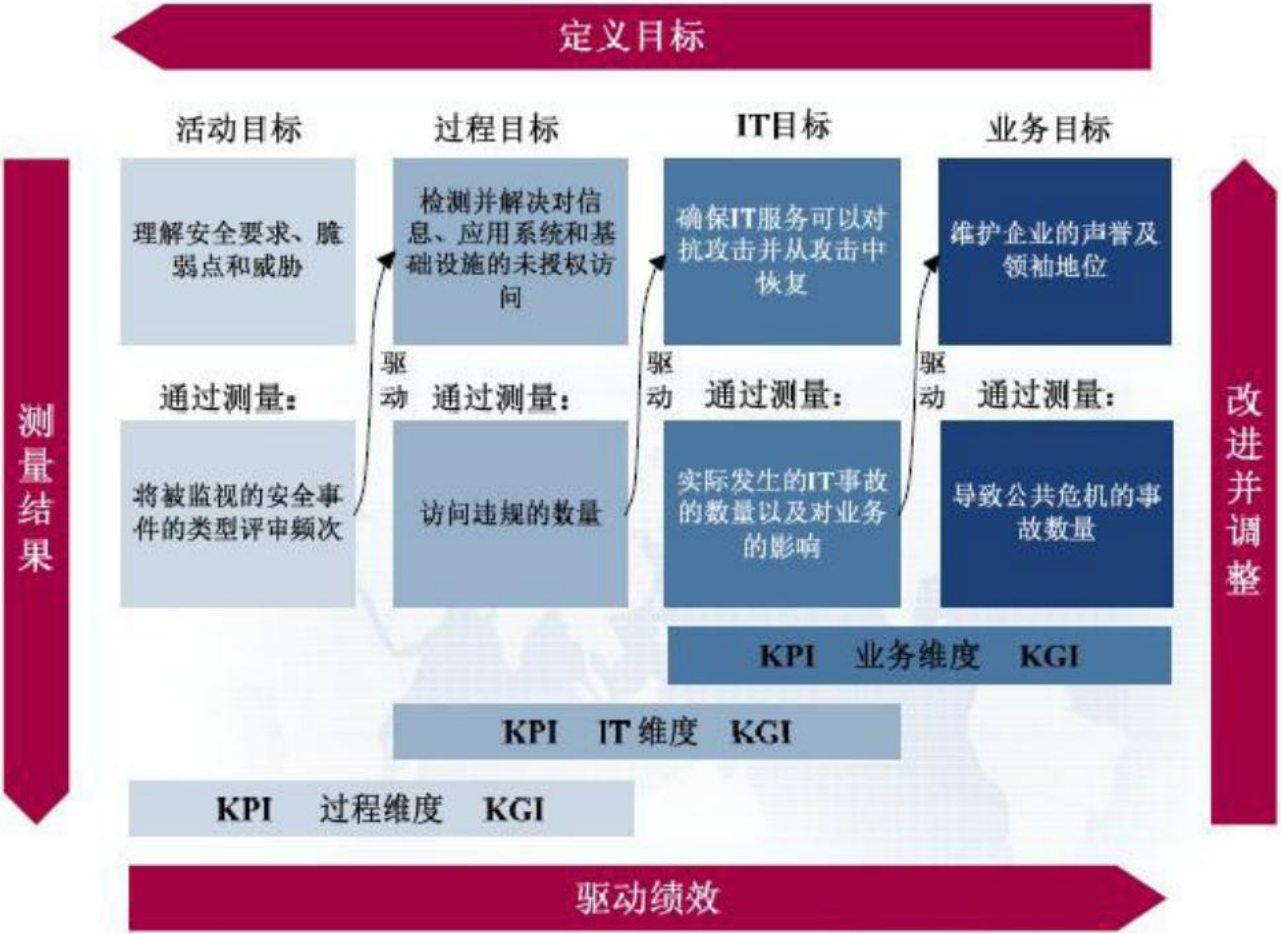
Process-Oriented



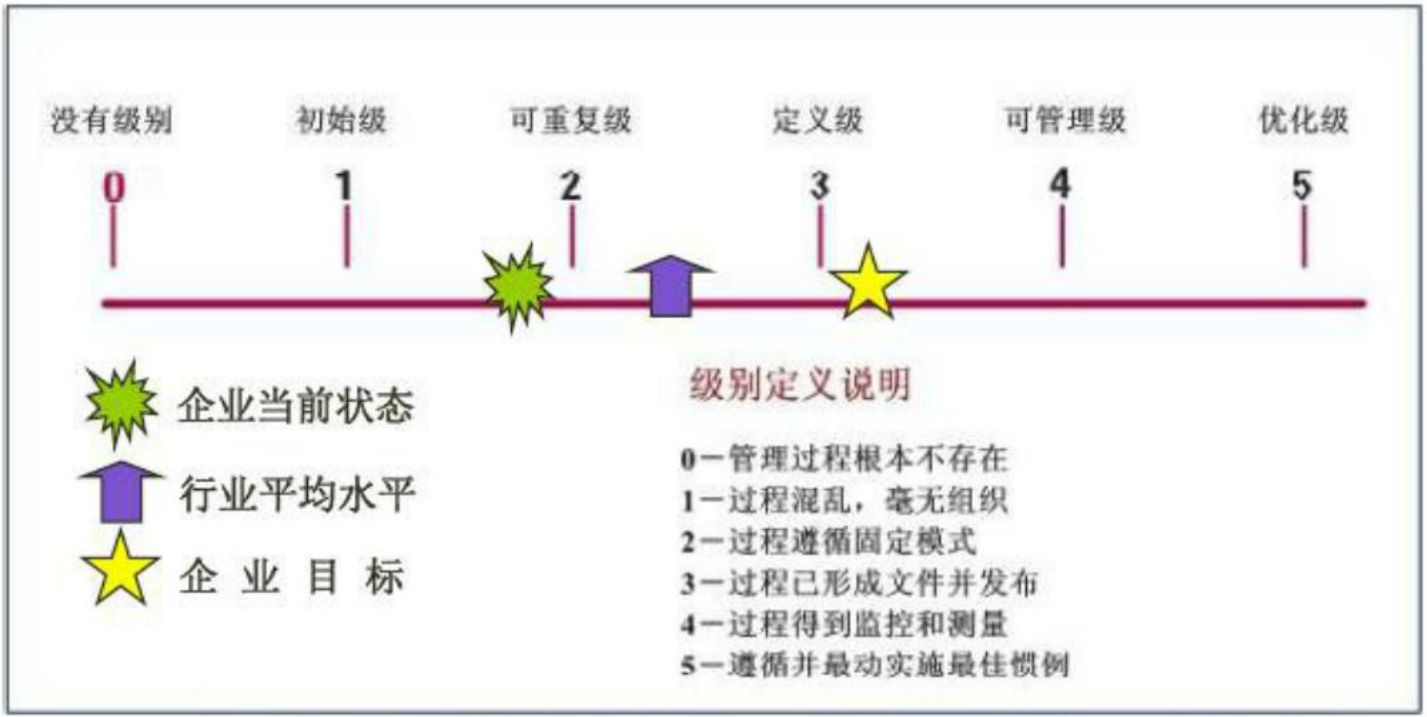
Controls-based



Measurement-Driven



Measurement-Driven



成熟度模型


5 Optimised
·遵循并最终实施最佳惯例
4 Managed
·过程得到监控和测量
3 Defined
·过程已形成文件并发布
2 Repeatable
·过程遵循固定模式
1 Initial
·过程混乱，毫无组织
0 Non-existent
·管理过程根本不存在

COBIT 组织方式


过程描述
信息准则
IT资源
IT治理关注领域
高级控制目标
详细控制目标
COBIT
框架
成熟度模型
MAP
过程输入、输出
RACI图
目标和维度
管理指南

内容安排

1.IT审计介绍

2.IT治理介绍

3.COBIT概念

4.COBIT体系框架

5.Q&A

Q&A

谢　谢！