KPMG

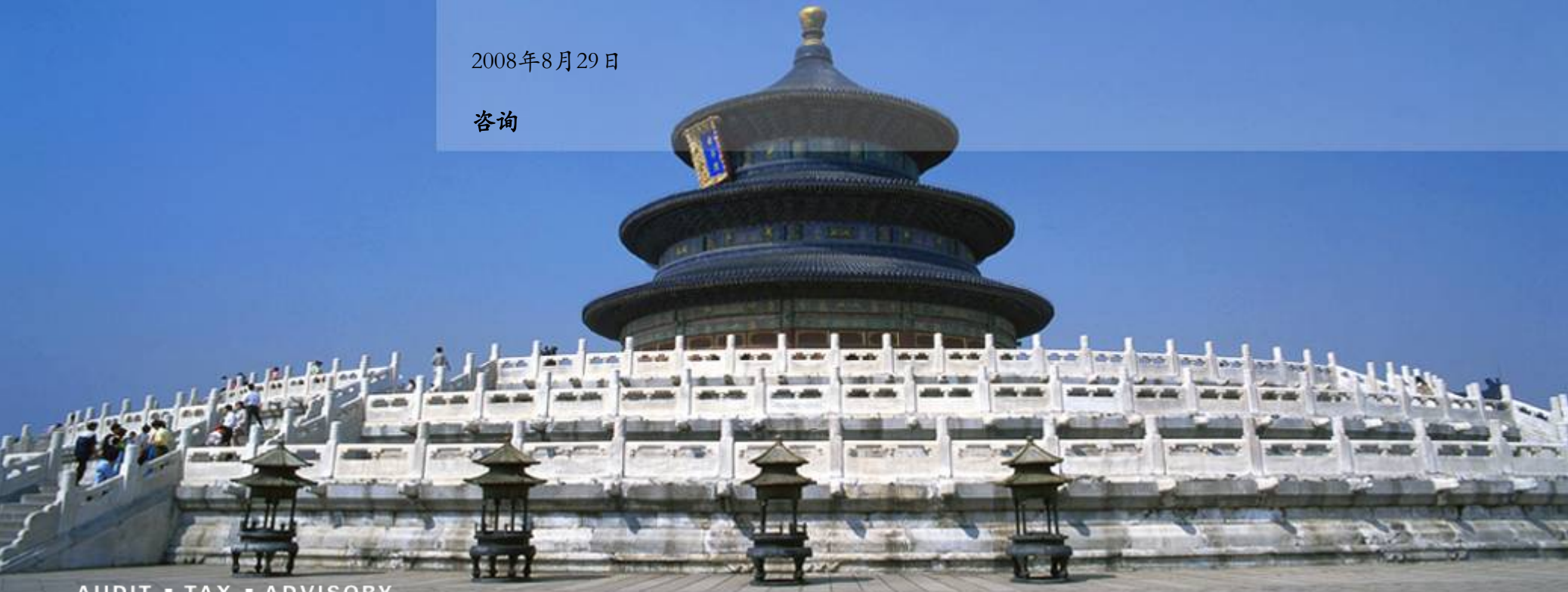
风险咨询服务

山东省农村信用社联合社

信息技术内部审计培训

2008年8月29日

咨询



AUDIT ▪ TAX ▪ ADVISORY

主要内容

主要内容

第一部分 IT审计概述

1、金融风险案例

2、内部控制与内部审计

3、IT审计的起源和基本概念

4、IT审计的特点和意义

金融风险案例

- 1995年，由于旗下的新加坡期货公司前台交易员兼后台结算主管里森越权违规交易，造成约**合十四亿美元的损失**，导致具有两百三十多年历史的英国巴林银行**倒闭**。巴林银行集团内部控制机制的不健全、高级管理层漠视缺乏实行岗位制约的严重性等管理和控制上的缺陷都是导致严重问题的根源。同时，内审部门和外部审计也都没有及时发现该公司长期以来使用“88888”账户进行越权违规交易以及严重亏损的问题，也暴露了审计执行中的漏洞。

- 日本大和银行纽约分行交易员兼内部业务负责人井口俊英从1984年起，在长达11年的时间为弥补国债交易带来的损失，私自卖掉该分行保有的国债券等有价证券以及为顾客保管的证券，并伪造账簿，造成**损失约11亿美元**。由于内部控制制度的缺陷，当事人可以身兼数职，一个人独立完成证券的交易、确认、会计记录和核对的整个流程，并且，由于缺乏有力的内部审计，交易亏损长期没有暴露出来。

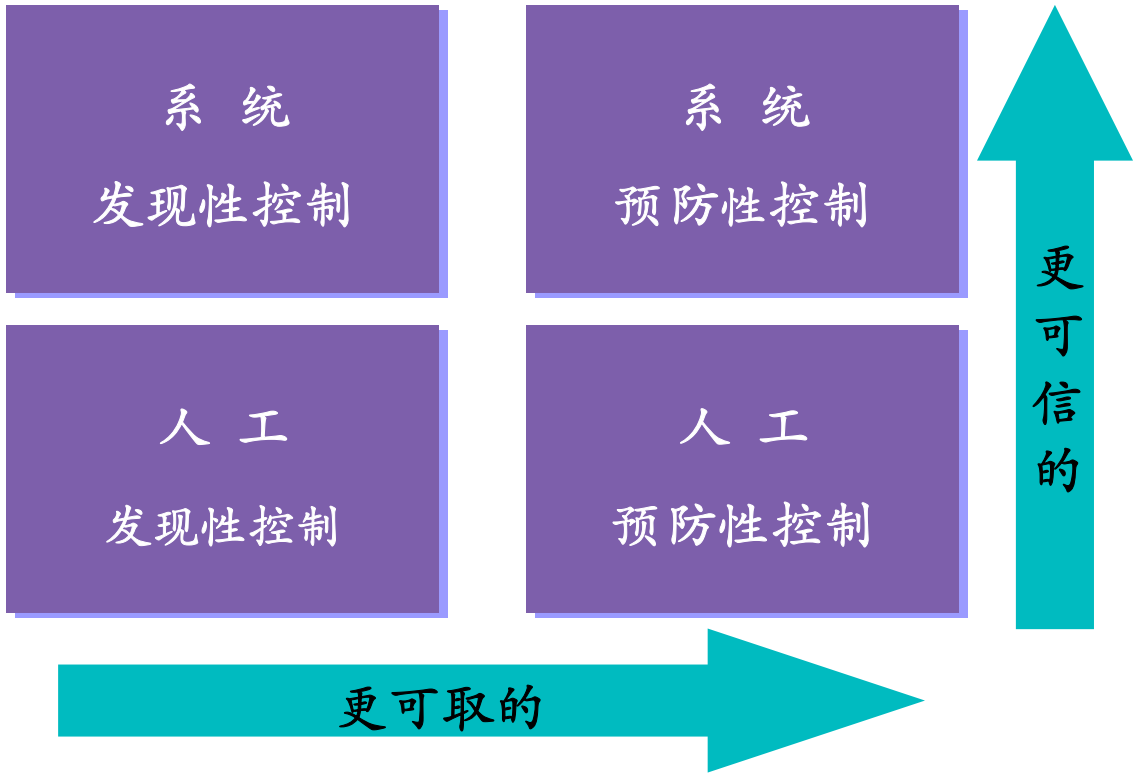
什么是内部控制

- 内部控制是企业为控制经营风险、实现经营目标而制定的各项政策与程序。

- COSO报告指出：内部控制是一个过程，受企业董事会、管理当局和其他员工影响，旨在保证财务报告的可靠性、经营的效果和效率以及现行法规的遵循。它认为内部控制整体架构主要由控制环境、风险评估、控制活动、信息与沟通、监督五项要素构成。

注：COSO是指美国反对虚假财务报告委员会所属的内部控制专门研究委员会——发起机构委员会（Committee of Sponsoring Organizations of the Treadway Commission， 简称COSO）。它包括美国注册会计师协会，内部审计师协会，财务经理协会，美国会计学会，管理会计协会。

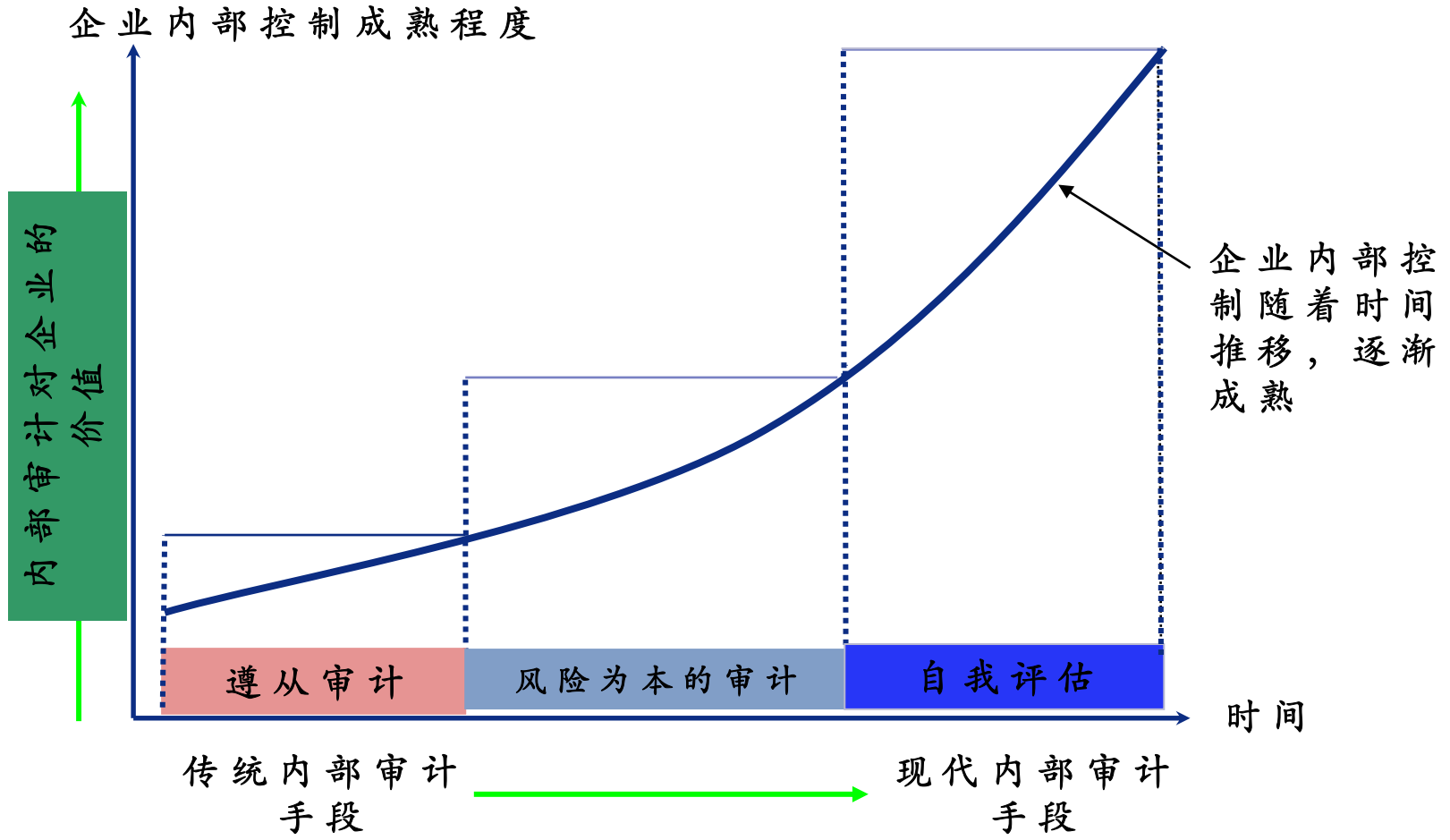
内部控制程序的种类



内部控制的种类

- 按控制内容分类
  - ⇨ 一般控制
  - ⇨ 应用控制
- 按控制地位分类
  - ⇨ 主导性控制
  - ⇨ 补偿性控制
- 按控制功能分类
  - ⇨ 预防性控制
  - ⇨ 发现性控制
- 按控制时序分类
  - ⇨ 输入控制
  - ⇨ 处理控制
  - ⇨ 输出控制

内部控制与内部审计的关系

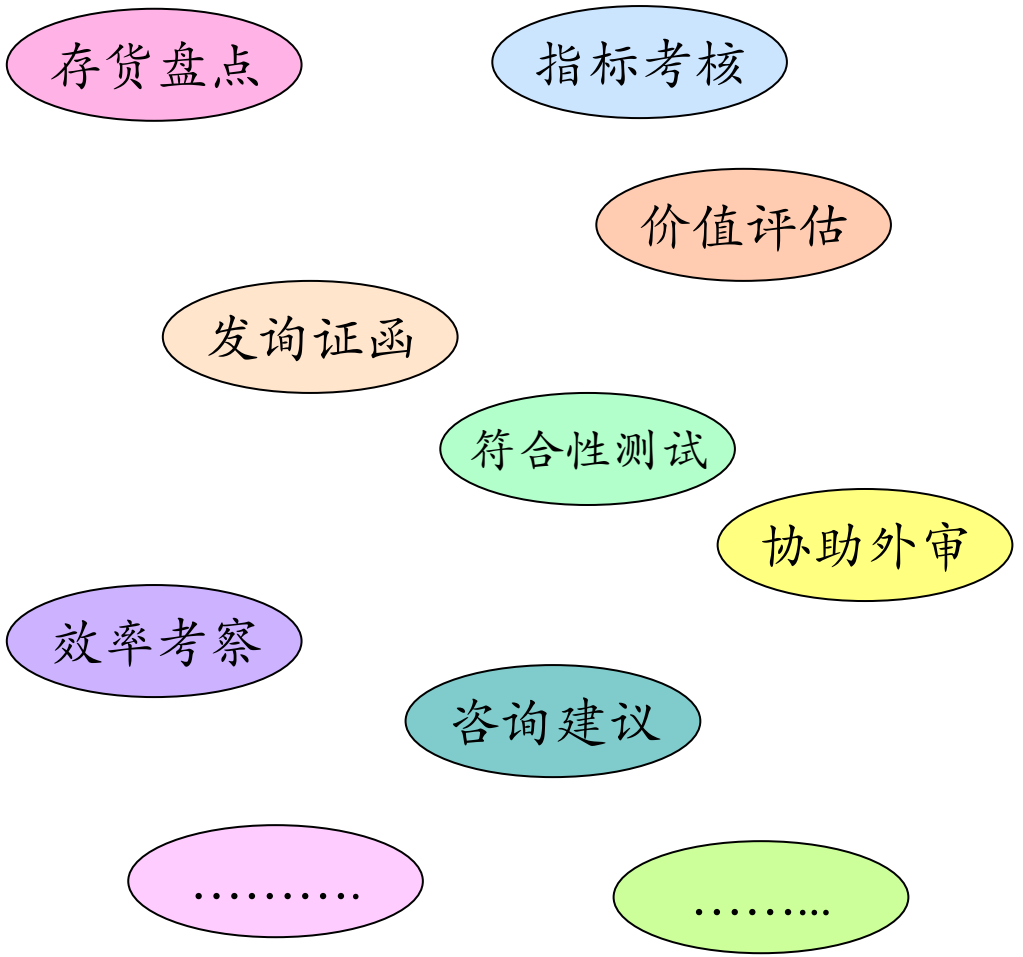


内部审计的演变历史

第一代（1980之前）	第二代（80年代）	第三代（90年代）	第四代（21世纪）
控制	控制结构	企业风险	企业风险管理流程
• 出发点是已有的流程、程序和控制	• 出发点是财务风险和符合性风险	• 出发点是对企业和各种风险的充分理解	• 出发点是对企业和各种风险的充分理解
• 以符合性测试为主	• 确定应该存在的控制	• 确定应该存在的控制	• 确定应该存在的能有效控制风险的企业风险管理流程
	• 审计目的是评估控制的设计、运行效果和合规性	• 审计目的是评估控制的设计、运行效果和合规性	• 评估在各个企业风险管理流程的设计、运行效果和合规性

内部审计在现代企业中的角色和职能

- 企业内部活动的监督者
- 防错纠弊的检察员
- 监控企业运作和资源使用的效率和效果
- 协助外部审计人员
- 风险管理咨询



内部审计与被审计单位管理层的关系

- 独立
- 合作、帮助，而非对立
- 发现事项、改进建议须得到管理层的同意，而非命令
- 内审的价值不仅是发现问题还要提出可行的建议，协助管理层解决问题

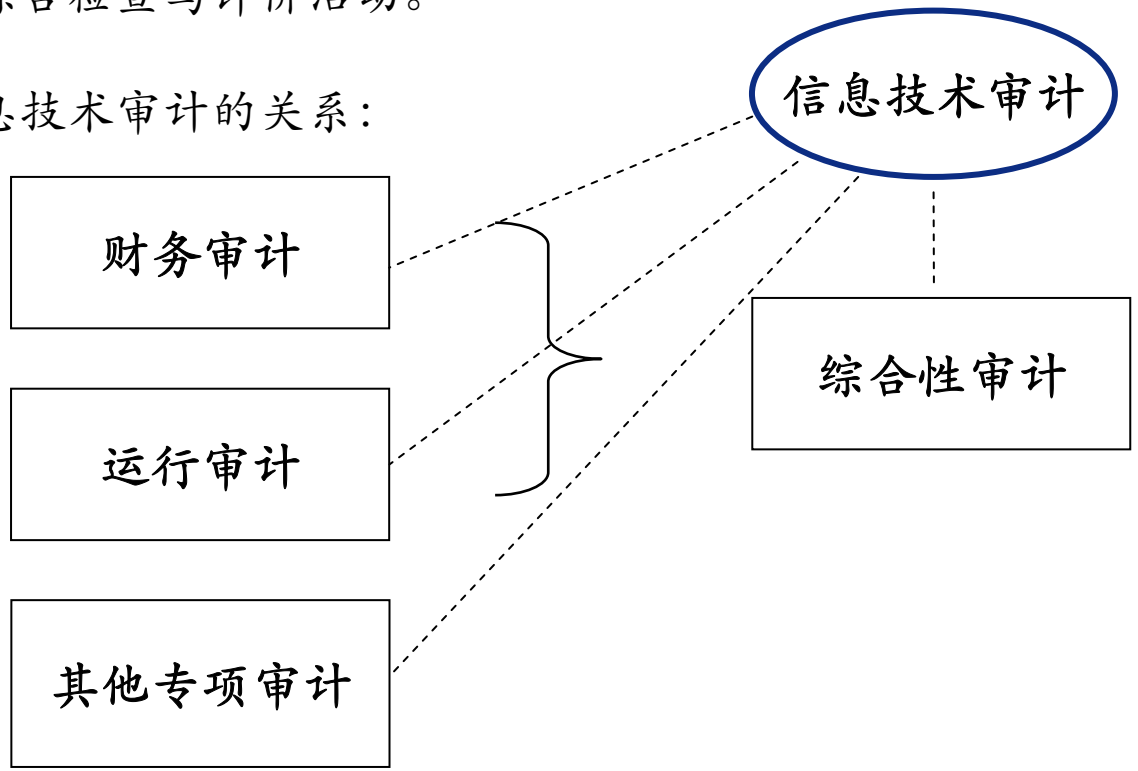
IT审计的起源

- 信息化社会的到来是IT审计起源的根本原因
- 现代社会对信息系统（Information System）的依赖越来越强，而信息系统本身结构、功能复杂性越来越高，信息系统的安全、稳定、可靠性越来越重要
- 对信息系统的误操作、不正当使用、信息技术滥用等带来的危害影响事件层出不穷
- 应对信息系统的建设需要引入一种新的管理机制来对信息系统的安全性、投资效果、实施进程和实施效果等进行评估、指导和改进—IT审计

IT审计的基本概念

为了确保组织的信息技术战略充分反映该组织的业务战略目标，提高组织所依赖的信息系统的可靠性、稳定性、相关信息资产的安全性及数据处理的完整性和准确性，提高信息系统运行的效果与效率，确保财务报告的可靠性及信息系统的运行符合法律法规的相关要求，而由信息技术审计人员对信息技术内部控制和流程以及利用信息技术对系统和数据进行的一系列综合检查与评价活动。

审计的分类及与信息技术审计的关系：



IT审计的主要特点

- 从狭义上讲，IT审计的范围是信息系统本身及其相关环境，涉及整个信息系统的生命周期，包括基础设施、系统开发、软硬件管理、信息安全、网络管理和通信等。而广义上IT审计则不仅仅针对信息系统及其环境本身，同时还包含使用信息技术作为手段对业务流程的审计，以对业务活动和财务数据的有效性、完整性、准确性等作出评估。
- 与非IT审计相比，IT审计提出了更多的审计方法与审计程序，比如对某软件进行审计时，要采用技术含量相当高的测试，对网络安全审计时要采用渗透性测试等。
- IT审计不仅仅是事后审计，同时还包含对信息系统建设过程中和运行过程中的监督和咨询，使信息系统更准确和有效的满足业务需求。

IT审计的意义

随着信息系统在企业运营中的支持地位越来越突出，信息技术审计对企业有着重要的意义：

- **满足外部监管的要求**：外部监管机构对企业的信息系统风险管理存在着明确的要求，特别是金融业，例如中国银监会发布的《银行业金融机构信息系统风险管理指引》，指引中明确对信息系统审计提出了要求，同时IT审计可以帮助企业了解现状、找出与监管要求的差距、促进企业信息系统建设符合外部监管机构的要求。
- **满足企业业务和管理对信息系统建设的要求**：现代企业的业务和管理的快速发展需要信息系统的有效支持，IT审计在信息系统建设过程中能够提供必要和客观的评估和咨询意见，协助维护信息系统开发建设的规范性，以确保信息系统满足需求、有效地为企业业务和管理提供支持。
- **为企业的运营承担内部咨询顾问的角色**：信息技术审计不但可以协助管理层发现系统建设及运营中的问题，还可以针对发现的问题提出公正客观的改进建议。

IT审计的发展

- 20世纪60年代
  - IBM出版的《Audit encounters Electronic Data Processing》有关在EDI环境下进行审核和组织的论述被认为是IT审计的出处
  - 早期被称为计算机审计，主要关注对被审计单位电子数据的取得、分析、计算等数据处理业务
- 20世纪70－80年代
  - 美国、日本先后成立了IT审计方面的协会组织。从事对IT审计规则的制定和实施指导
  - 计算机审计所关注的内容也从单纯的对电子的处理，延伸到对计算机系统的可靠性、安全性进行了解和评价
- 20世纪90年代
  - 由于互联网的普及，计算机犯罪的涌现及日益严重的软件项目失败等引发了对信息系统的投资和开发进行审计的深思，IT审计步入普及期
  - 我国在1999年颁布了《独立审计准则第20号——计算机信息系统环境下的审计》，我国的IT审计步入起步阶段

主要内容

第二部分 内部审计方法论

1、战略分析

2、企业风险评估

3、制定内审计划

4、内审项目执行

5、报告

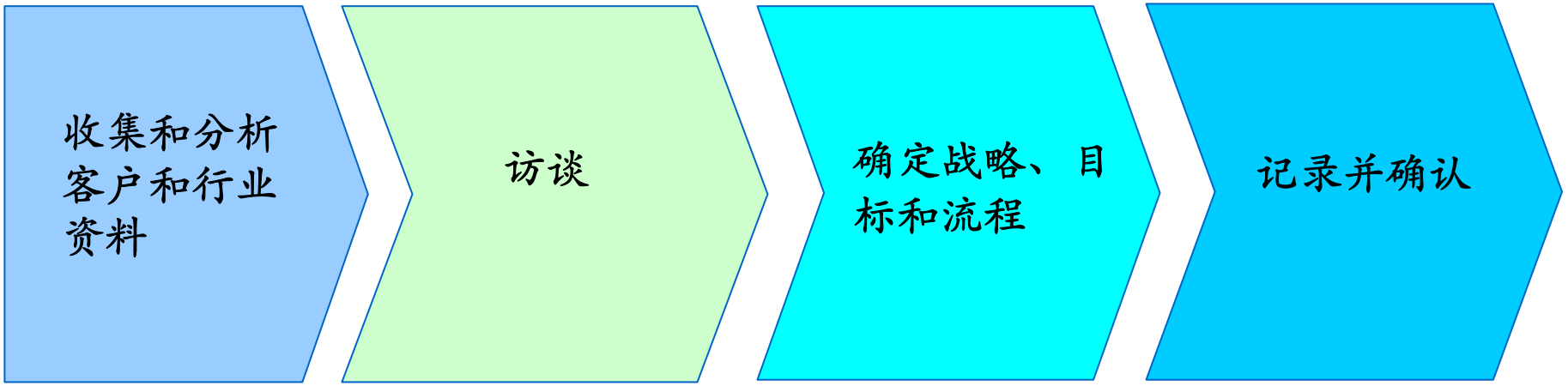
6、问题的解决和跟踪

内部审计方法－IAM

战略分析

- 以从上到下的角度，初步了解公司业务；
- 帮助识别与客户及其所属行业相关的问题；
- 获得对客户业务和外部影响力的宏观的认识；
- 定义战略目标，了解公司如何应付阻碍实现战略目标的挑战，并提出建议。

战略分析的步骤



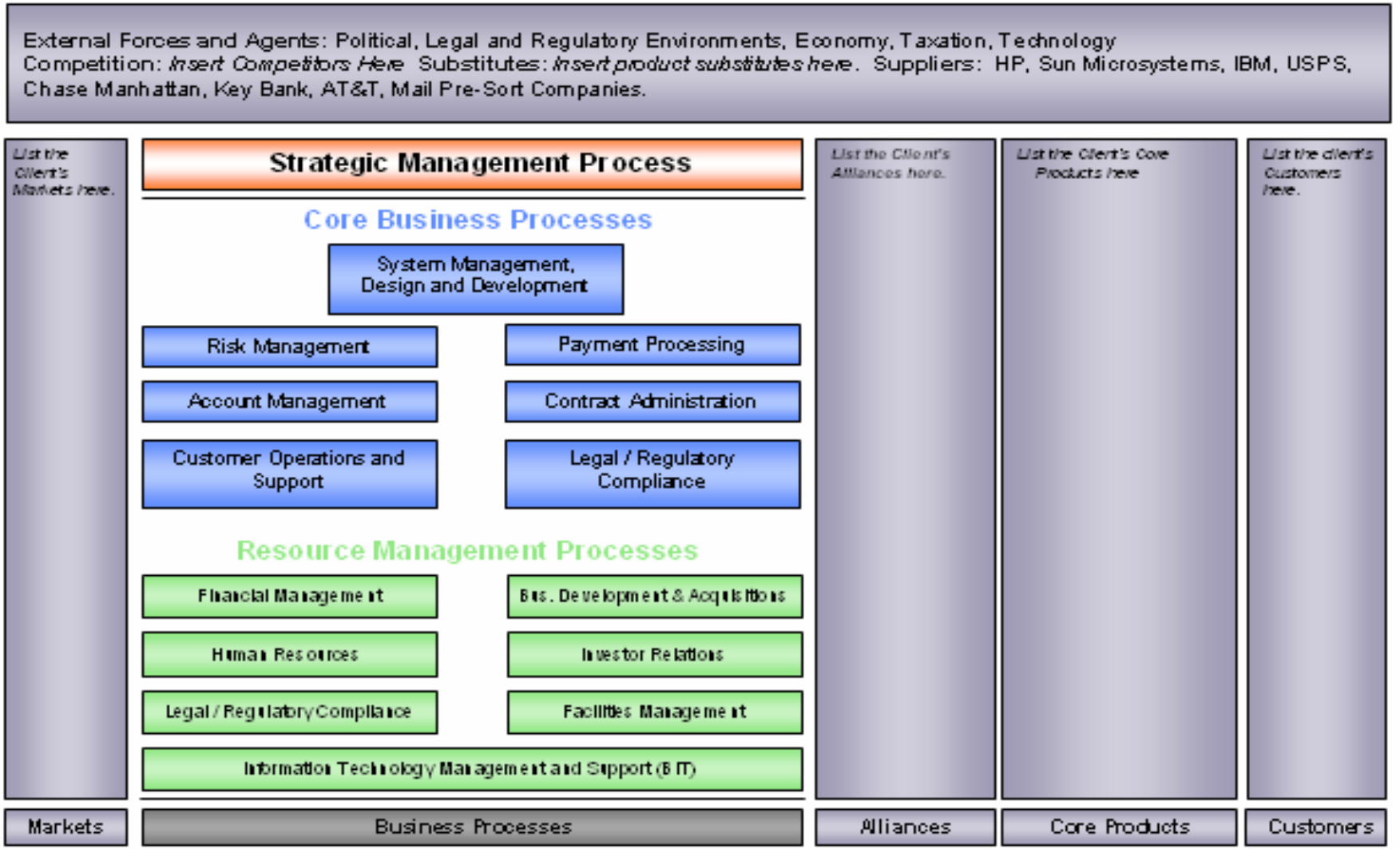
战略分析—任务

收集并分析客户和行业信息

- 行业: 运用一些工具进行初步分析，例如：业务模型、行业手册、行业数据和资料、分析报告、新闻等。

- 客户: 公司网站、公司历史和大事件、章程、财务报表、组织架构图、公司结构、会议纪要、KPI、战略规划等。

战略分析—业务模型



See the Business Model Template for additional information.

战略分析－任务

访谈

主要受访者 –

- CEO、CFO和其他的高级管理人员
- 董事会主席、审计委员会和其他主管
- 外部第三方，例如：分析师、供应商等。
- 其他人员，例如：参与业务重要决策的人员、业务模块管理者、法律顾问、风险管理人员、股东和权益拥有人。

战略分析—任务

确定业务目标、战略和业务流程

- 业务目标 – 在公司、业务模块、职能或者流程层面的远景和目标;
- 战略 – 公司计划怎样实现远景、目标和目的.
- 业务流程 – 在一个组织内部通过有序的活动来产生具体的结果 （战略管理流程、 核心业务流程、资源管理流程=> 业务模型）

企业风险评估

- 识别与战略目标相关的战略风险；
- 帮助客户理解阻碍公司达到战略目标的风险；
- 协助客户确认能规避战略风险的关键业务流程，并进行流程层面的评估；
- 为内部审计计划提供根据和基础。

企业风险评估的阶段

企业风险评估－任务

项目规划

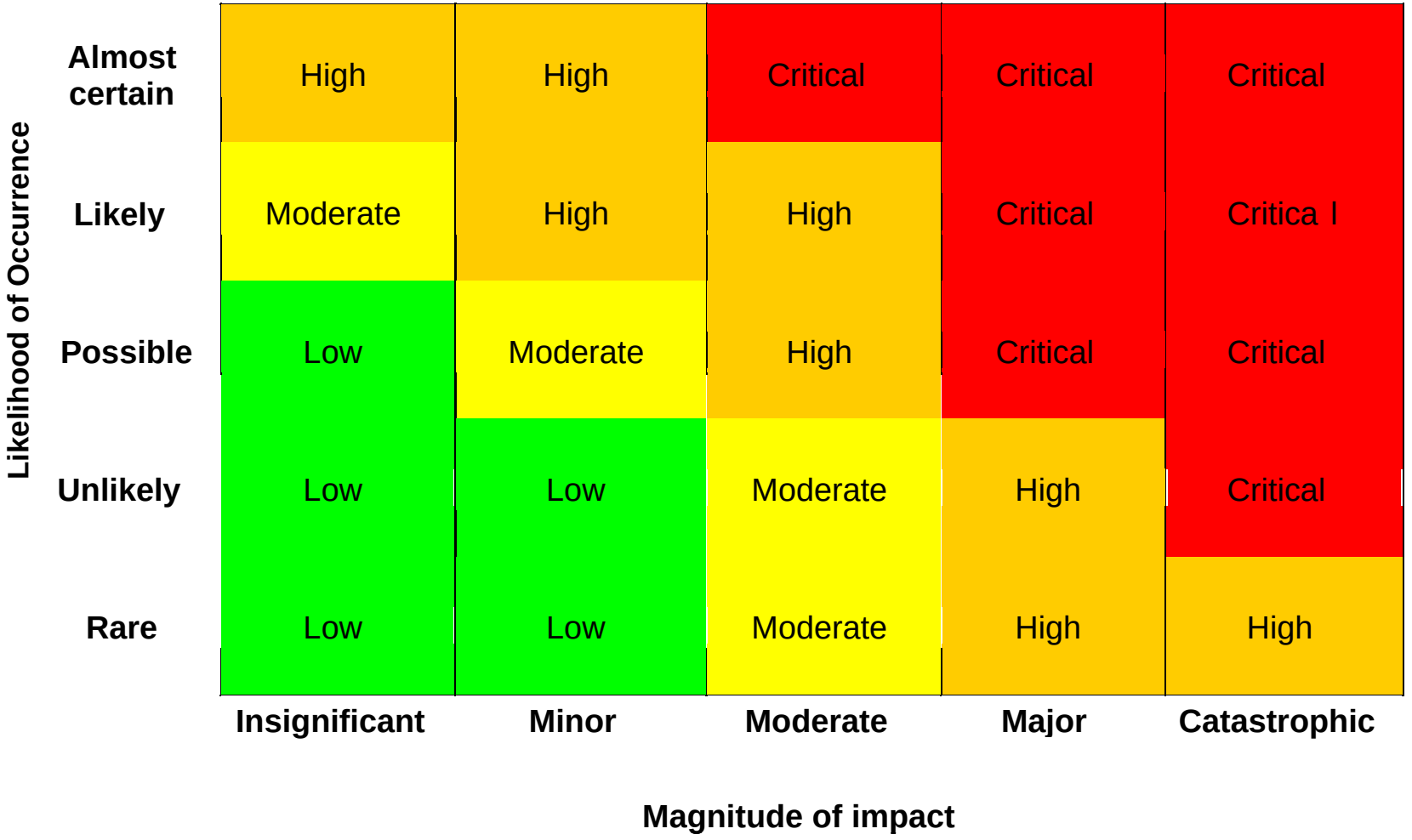
- 确定收集风险的方法 – 访谈、研讨会或者调查问卷;
- 确定风险标准 - 可能性/ 发生的概率、影响级别;
- 确定项目范围;
- 确定项目细节和访谈时间表。

企业风险评估－影响和可能性描述

重要性	
无关重要	▪ 对收益的影响< $X 百万 ▪ 对市场份额没有潜在影响 ▪ 对品牌价值没有影响
较少的	▪ 收益会有$X到 $X 百万的损失 ▪ 在正常操作条件下，结果唯一 ▪ 对市场份额和品牌价值有潜在影响 ▪ 问题会指派给中层管理者解决
中等的	▪ 对收益有$X 到 $X百万影响 ▪ 市场份额和/或品牌价值在短期内将会受影响 ▪ 事件将需要高级和中层管理层干涉
较多的	▪ 对收益有$X 到 $X百万影响 ▪ 市场份额和品牌价值严重减少 ▪ 主要的战略联盟受到威胁 ▪ 事件和问题需要董事会和高级管理层注意
灾难性的	▪ 对收益的影响> $X 百万 ▪ 失去主要战略联盟 ▪ 持续不断的严重损失市场份额

发生的概率	
几乎确定	▪ 事件在大多数情况下会发生
很可能	▪ 事件有可能在大多数情况下发生
一般的	▪ 事件应该在某时发生
不太可能	▪ 事件有可能在某时发生
极少可能的	▪ 事件仅在特殊情况下可能发生

企业风险评估－风险等级标准



企业风险评估－任务

识别风险

- 风险定义 – 总体风险、剩余风险、风险来源、战略风险、流程层面风险
- 汇总和分类（风险分类）
- 确定可能性和影响
- 制定企业风险矩阵

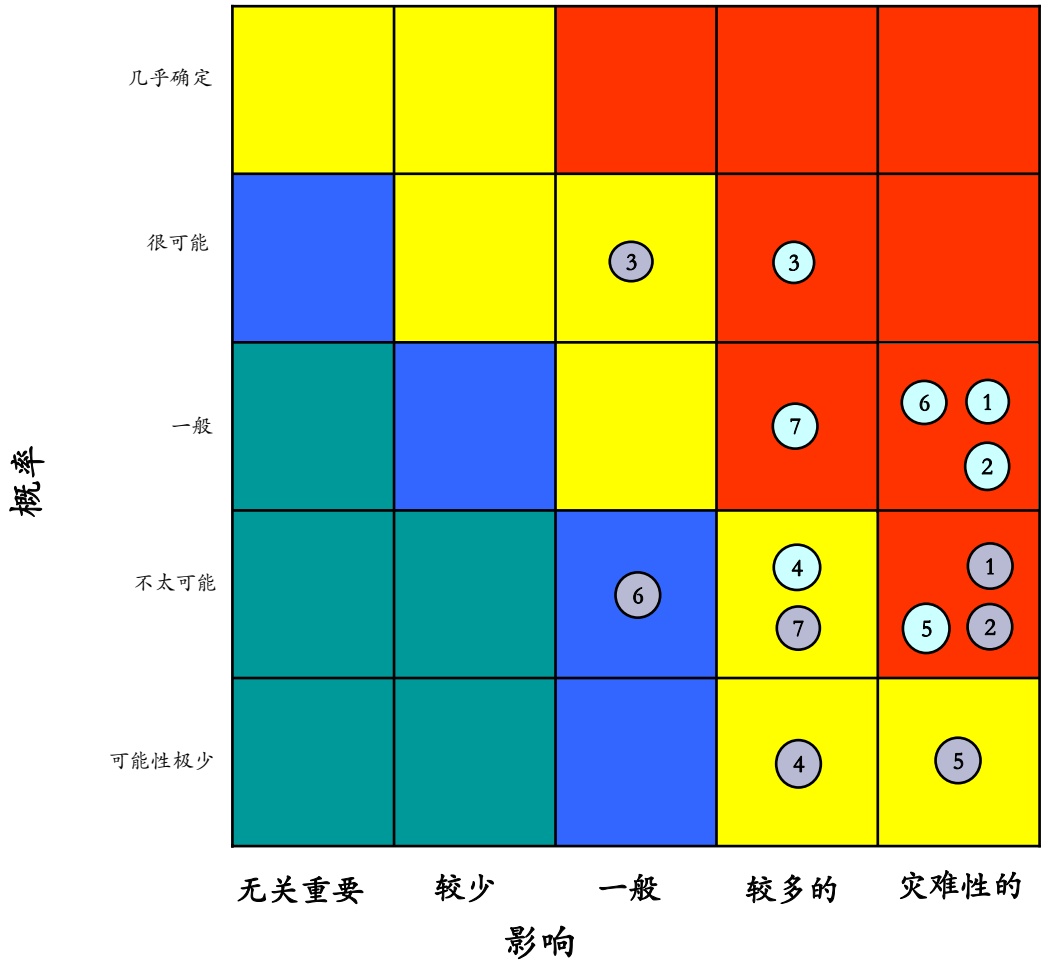
企业风险评估－任务

记录和分析风险信息

- 汇总和分类（风险分类）
- 确定可能性和影响
- 建立企业风险矩阵
- 按顺序排列识别的风险
- 识别和确定关键业务流程

企业风险矩阵的实例

下图详细说明了每一个风险的总体风险和剩余风险等级，说明了风险评级在控制汇总后是如何收到影响的。在矩阵中所示，定义了7个主要风险，在考虑管理这些风险的现有控制后，其中四个被重新划分在“一般”或者“低”的区域中。



序号	总体风险	剩余风险
1	高	高
2	高	高
3	高	一般
4	一般	一般
5	高	一般
6	高	低
7	高	一般

注：无关 低 一般 高

剩余风险 (RR)　总体风险 (GR)

流程风险评估－任务

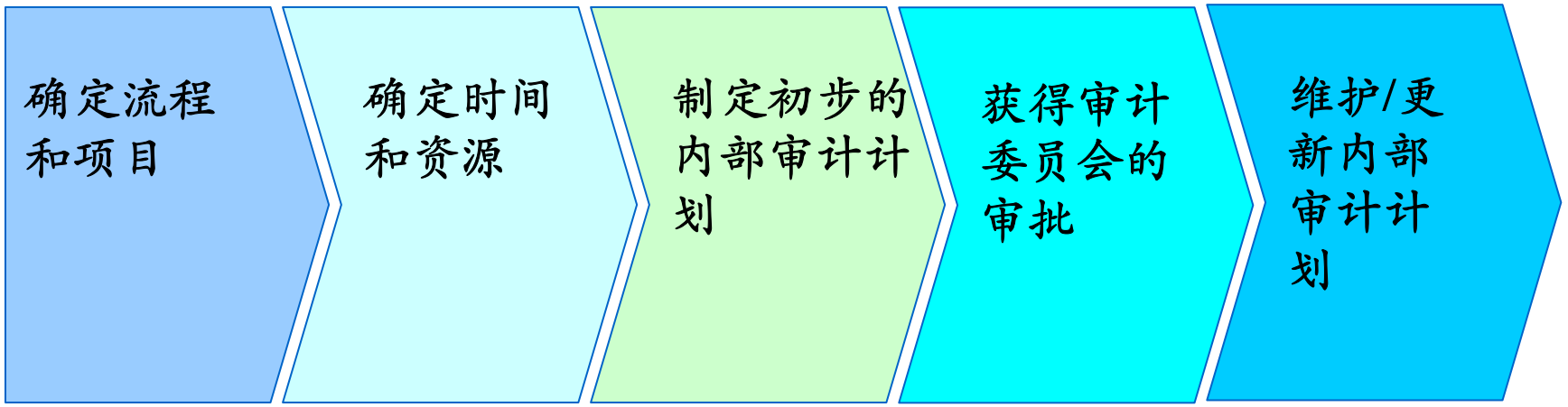
流程层面风险评估

- 使用企业风险评估框架来评估流程风险；
- 流程层面风险评级标准；
- 集中在某具体流程而不是集中在公司的整体层面；
- 文档：流程分析文档、流程图、风险记录表和必需的补充描述 => 帮助识别和评估流程层面的风险以及相关内部控制的设计有效性。

制定内部审计计划

- 确定内部审计部门的工作范围；
- 根据客户的需求、预算和细节程度，确定何时制定内部审计计划；
- 总体的和详细的内部审计计划；
- 最终由客户的审计委员会同意并采用。

制定内部审计计划的步骤



制定内部审计计划－任务

确定流程和审计项目

- 通常着重于已经建立好的、管理最重要风险的业务流程;
- 管理层或者审计委员会的具体要求
- 过去问题的跟进检查
- 其他有顾虑的方面 （例如，欺诈舞弊事件、新业务/产品、法律法规的要求）

制定内部审计计划－任务

确定时间和资源

- 审计计划、范围和协调工作
- 向管理层和审计委员会报告
- 不同业务流程的集中/分散程度
- 人员组合
- 需要特殊专业人员参与的程度

内部审计计划案例

Ref	Company Name	Location	Principal Business	Year of Audit	Manweeks	# of weeks on site per assignment - Assume 2 staff per assignment	Total Hours Required	Audit Preparation Time	Sales Order Management (from sales order processing to shipping)
1	ABC International Holdings Limited	Singapore	Holding Company	Year 1	2	1	80	16	
3	ABC Manaufacturing Pte Ltd	Singapore	Manufacturer, importer and exporter of upholstered furniture	Year 1	4.8	2.4	192	24	24
4	ABC Leather Sdn Bhd	Malaysia	Manufacturer of upholstered furniture	Year 1	3.6	1.8	144	24	
5	ABC Furniture (China) Co Ltd	China	Manufacturer of upholstered furniture	Year 1	3.6	1.8	144	24	
8	ABC Manufacturing Sdn Bhd	Malaysia	Manufacturer and retailer of leather furniture	Year 1	4.8	2.4	192	24	24
21	XYZ Leather (Yangzhou) Co., Ltd	China	Leather tanning and finishing and provision of cut and sew services	Year 1	3.6	1.8	144	24	
	Information Technology Audit			Year 1	3	1.5	120	24	
16	ABC Leather Pte Ltd	Singapore	Leather tanning and finishing	Year 2	3.6	1.8	144	24	
19	ABC International Pte Ltd	Singapore	Wholesaler of leather, fabrics and other furnishing materials	Year 2	3.4	1.7	136	24	24
6	XYZ Leather (Kunshan) Co Ltd	China	Manufacturer of upholstered furniture	Year 2	3.6	1.8	144	24	
7	XYZ Leather (Changshu) Co Ltd	China	Manufacturer of upholstered furniture	Year 2	3.6	1.8	144	24	
12	ABC (UK) Limited	UK	Sale and distribution of leather sofa products	Year 2	2.6	1.3	104	24	24
20	ABC Leather (China) Co., Ltd	China	Leather tanning and finishing	Year 2	3.6	1.8	144	24	
9	Noosag Industries Sdn Bhd	Malaysia	Manufacturer of foam	Year 2	3.6	1.8	144	24	
17	XYZ Leather Pte Ltd	Singapore	Wholesaler of leather	Year 2	3.4	1.7	136	24	24
2	Hwa Tat Lee Japan Co Ltd	Japan	Wholesaler of home and office furnishings	Year 3	2.6	1.3	104	24	24
14	H.T.L. Furniture Inc	USA	Sales and distribution of upholstered furniture	Year 3	2.6	1.3	104	24	24
15	XYZ Leather Inc	USA	Sale and distribution of leather products	Year 3	3.4	1.7	136	24	24
11	Hwatalee G.M. (Taiwan) Co., Ltd	Taiwan	Retailer of furniture	Year 3	2.6	1.3	104	24	24
13	ABC International GmBH	Germany	Commission agent for upholstered furniture	Year 3	2.6	1.3	104	24	24
22	ABC Leather (HK) Ltd	Hong Kong	Wholesaler of leather and fabrics	Year 3	3.4	1.7	136	24	24

制定内部审计计划－任务

制定初步的内部审计计划

- 额外信息，例如计划流程和方法、风险矩阵、内部审计项目范围、预算和时间安排；
- 与内部审计协调人讨论和确定工作范围；
- 按客户要求进行变更；
- 审计委员会最终决定内部审计计划。

制定内部审计计划－任务

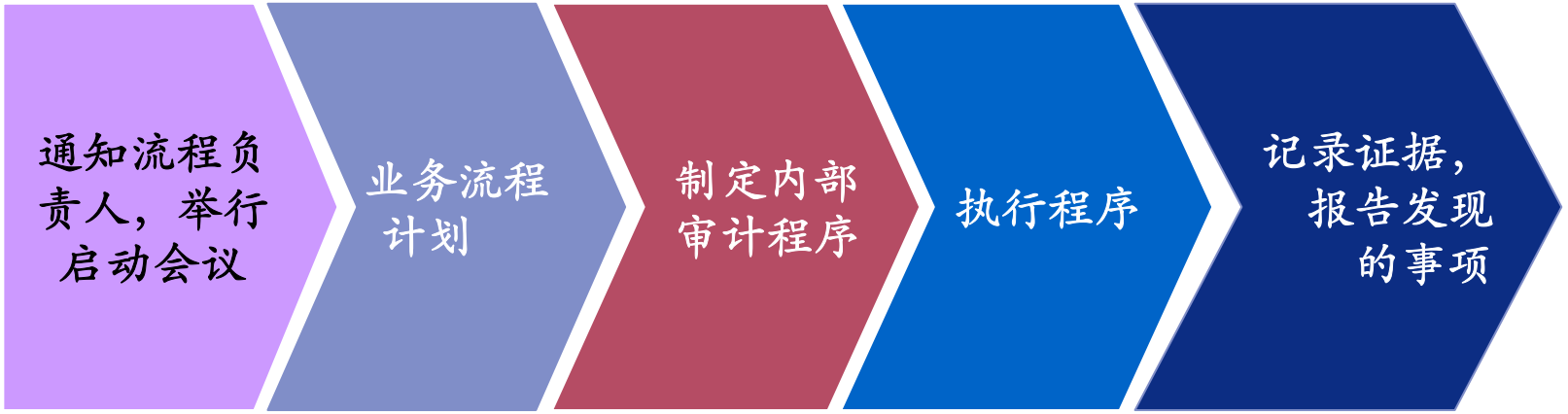
获得审计委员会的审批

- 提交初步的内部审计计划给审计委员会研究和采用；
- 指出不包括在内部审计计划范围内的重要流程。

内部审计执行

- 获得对内部审计计划的审批后开始执行；
- 致力于向客户提供发现事项和提高经营业绩的机会。

内部审计执行流程



内部审计执行－任务

通知流程负责人，举行启动会议

- 在内部审计现场工作之前
- 通知信 （或其他形式）
- 启动会议 – 向管理层阐述相关计划的范围，获得管理层的支持，将项目小组成员介绍给被审计人员。

内部审计执行—任务

业务流程分析

- 主要目的是用来建立审计程序的内容和着重点
- 获得对流程的了解
- 通过访谈和讨论
- 叙述或者流程图
- 确定流程层面风险、控制、设计差距和跟进的机会
- 与流程负责人确认

内部审计执行—任务

业务流程分析（续）

- 评估现有流程和控制，并进行比较；
- 将流程情况与一些标准进行适当的比较，进而帮助客户评估流程和控制的合理性，以及他们的管理情况。

内部审计执行—任务

设计内部审计程序

- 需要识别流程层面的风险和控制用来测试设计及执行有效性；
- 战略分析、企业风险评估、业务流程分析来可以帮助确定审计程序的重点；
- 需要考虑哪些因素来确定需要测试哪些控制：总体风险、控制强度、剩余风险；
- 审计程序应该详细说明测试步骤和控制目标；
- 测试步骤的类型：观察、询问、重新操作、检查、确证询问和知识评估；
- 测试步骤应该包括：总数的定义、测试数量和测试属性。

内部审计执行－任务

执行程序

- 内部审计测试－样本选择，包括统计抽样、CAATs、判断抽样（某些特定情况下比较适合用统计抽样；但判断抽样也是可以接受的。）
- 工作文档－工作文档必须拥有足够的信息和内容，让另外一个独立方能重新执行同样的测试，并能得到同样的结论；
- 支持文档－全部保存还是只保存有异常的文档?

内部审计执行—任务

记录证据和报告发现事项

- 发现：记录控制的不存在或者没有按照预设的情况执行；
- 流程改进建议：不算控制弱点的改进建议；
- 在结束会议之前，获得被审计人员和管理层对发现的确认；
- “发现事项总结” — 详细记录观察到的事实、影响、建议和管理层回应。

报告

- 沟通内部审计工作的结果;
- 整个审计过程中会出现多次正式的/非正式的报告，不仅仅局限于最后的报告;
- 报告格式应该符合客户或公司统一的要求。

报告－任务

战略层面报告

- 沟通战略分析/企业分析评估/内部审计计划的结果
- 工作成果：业务模型、企业风险矩阵、风险记录表、内部审计计划

流程层面报告

- 沟通流程层面工作的结果
- 工作成果：流程风险矩阵、流程层面的风险矩阵、流程风险记录表、内部审计报告、对以前审计发现事项的跟进报告。

报告—任务

撰写内部审计报告

- 一致同意的发现和管理层的行动计划；
- 避免有惊无喜的情况出现；
- 工作成果：流程风险矩阵、流程层面风险；
- 在审计报告概述部分重点指出不同意的地方；
- 高级管理层和审计委员会根据情况自己进行判断。

问题的解决和跟踪

跟踪和监控管理层答应的行动计划的实施情况，并将实施情况报告给高级管理层和审计委员会。

问题的解决和跟踪－任务

将解决问题的活动与行动计划作对比

- 确定哪些发现事项应该跟进
- 确定报告中的管理层回应是否实际发生
- 评估管理层行动计划的合理性
- 评估实施的活动是否是针对最初的发现事项
- 将所有的行动汇总并更新行动的实施情况
- 总结并报告

问题的解决和跟踪－任务

- 向管理层和审计委员会报告
- 输出：
  - 问题跟踪/跟进报告

主要内容

第三部分 IT审计的内容和方法

1、IT审计的框架和内容

（1）公司层面控制的审计

（2）信息技术一般性控制的审计

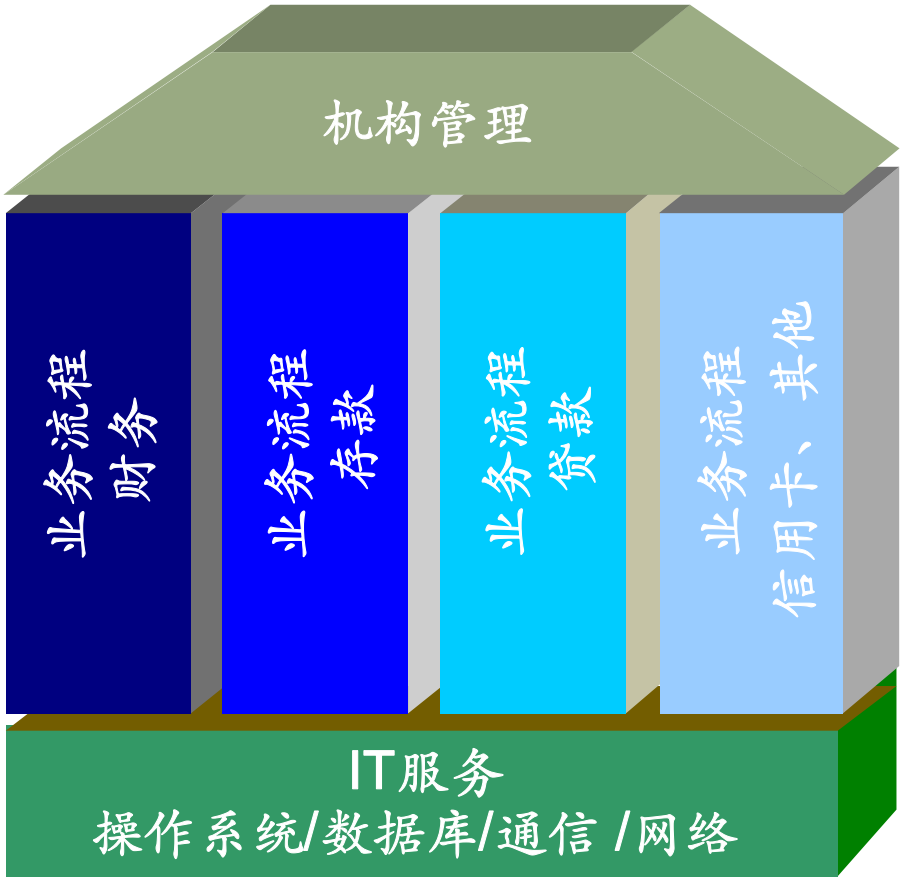
（3）业务流程层面应用系统控制的审计

2、IT审计的方法

（1）控制类型

（2）审计方法

信息技术审计的框架



公司层面信息技术控制

业务流程层面应用系统信息技术控制

信息技术一般性控制

人员

流程

技术

国际信息系统审计协会ISACA关注的主要内容在公司层面信息技术控制和信息技术一般性控制范畴

IT控制嵌入在机构三大控制领域内

公司层面控制中所关注的内容

公司层面控制中与信息科技相关的关注内容:

- 战略规划
- 组织架构
- 管理架构
- 规章制度

公司层面控制——战略规划

- **战略规划：**

  信息科技战略规划为如何发展、管理和考核信息科技的基础架构提供指引，以支持业务的发展目标。信息科技战略规划应该与业务发展战略规划保持一致性。

  信息科技战略规划可以确保信息化建设的步伐、重点、方向与业务发展战略保持一致，提高银行充分驾驭信息科技的能力，提升竞争力。信息科技战略规划有利于高级管理层和各级部门对信息化建设的指导思想、工作原则、重点应用领域、关键成功因素等形成统一共识。

公司层面控制——组织架构

❖**组织架构：**

信息科技组织架构是信息科技部门在银行业务运行和管理实施中的地位和作用，其主要内容包括：信息科技部门的设置及其功能和权限、信息科技与其他部门之间的相互关系等实施管理的模式。组织架构涉及考核及晋升流程、人员培训、汇报机制、总体的风险评估体系等。

组织架构是银行经营和管理的极为重要的基础性制度因素，是银行核心竞争力的主要构成因素之一。组织架构不合理会严重阻碍的业务的正常运作。

公司层面控制——管理架构

- **管理架构：**

  管理架构是指信息科技管理的决策机构和管理结构的设置，以及机构内的沟通及汇报流程，包括风险评估和应对、内部沟通等几个方面，有效的管理架构的设置是实现信息科技战略的有效保障。

  合理的信息科技管理架构的设立应确保信息技术的管理职责被明确的分配到部门和岗位。信息科技管理架构是信息科技管理的基础，确保信息系统的安全、稳定、有效的运行，以支持业务的发展。

公司层面控制——规章制度

❖**规章制度：**

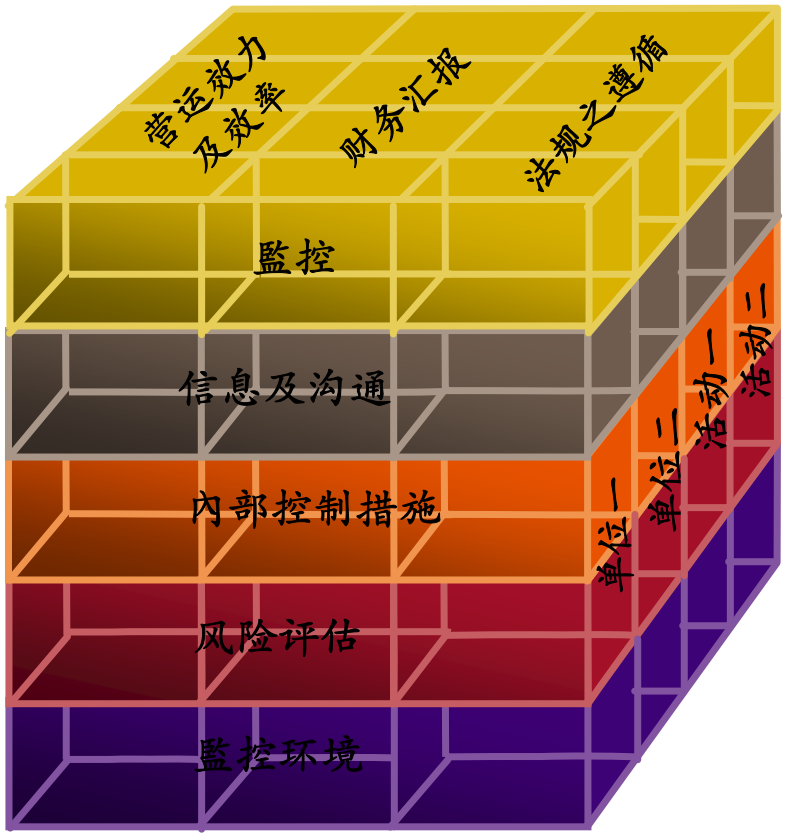
规章制度为信息科技管理提供清晰的指引和管理支持，帮助实现信息科技发展战略和业务目标。 规章制度管理包括：管理制度体系的建设情况，管理制度规章和管理办法的制定、审批和修订流程等。

规章制度建设是基础管理工作的重点，规章制度所涉及的范围非常广，非常分散，涉及职能管理的各个方面；规章制度所涉及的管理关系复杂，存在执行的难度；规章制度具有时效性，在一定时间段内是有效的，但是随着外部环境变化和企业的不断发展，规章制度有时候会滞后，甚至会阻碍业务的发展。

公司层面控制——审计内容

❖战略规划 ❖组织架构 ❖管理架构 ❖规章制度

- ❖控制环境反映了管理层及其它人员对企业内部控制的重要性的整体看法、认识和行动
- ❖识别和管理相关风险的流程，以实现企业所定的目标
- ❖所采用的政策及程序可协助保证已经开展针对风险的管理行动
- ❖所采用的确定、收集和互通信息的形式和时间框架有助于员工履行职责
- ❖评估所设定的内部控制构成的效用和在适当时作出修订



信息技术一般性控制

信息技术一般性控制的主要内容:

- 系统和基础建设生命周期管理
- IT服务的交付与支持
- 信息资产的保护
- 灾难恢复和业务连续性计划

信息技术一般性控制

- 系统和基础建设生命周期管理：系统的开发、采购、测试、实施（交付）、维护和（配置）使用，与基础框架，确保实现组织的目标。
  - 系统开发
    - 可行性研究、需求定义、系统设计、程序开发、测试、培训、数据转换、上线
  - 项目管理过程
    - 项目计划管理流程、汇报流程、变更控制流程、项目风险管理/成本管理方法
  - 环境和职责分离
    - 开发环境、测试环境、生产环境的分离
    - 开发人员、测试人员、维护人员的职责分离

信息技术一般性控制

- IT服务的交付与支持：IT服务管理可确保提供所要求的等级、类别的服务，来满足组织的目标。
  - 硬件
    - 硬件的获取
    - 硬件的能力/性能的监督，系统容量管理
  - 操作系统
    - 系统软件的获取、安装、维护、变更控制
  - 数据库
    - 数据库的设计、访问、管理、接口和可移植性

信息技术一般性控制

- 问题管理
  - 记录、跟踪、解决、上报
- 调度作业
  - 批处理作业的准确性、完整性、及时性
- 变更管理
  - 变更的授权与审批
  - 测试
  - 移植到生产环境的流程控制

信息技术一般性控制

- 信息资产的保护：通过适当的安全体系（如安全政策、标准和控制），保证信息资产的机密性、完整性和有效性。
  - 信息安全的书面策略、流程和标准
    - 制定并保持信息安全政策，确保对程序和数据访问的控制措施得到了一贯地执行。
  - 逻辑访问安全策略
    - 身份识别和认证机制
    - 职责分离控制
  - 物理访问安全策略

信息技术一般性控制

- 安全意识的培训及养成
  - 终端用户知悉自己在信息资产保护方面的角色与责任
- 数据的访问书面授权
  - 用户帐号的增加、修改和删除
- 离职员工的访问控制
  - 离职员工的访问权限的及时清理或收回
- 安全基准
  - 防病毒管理、密码管理、补丁和漏洞管理

信息技术一般性控制

- 网络安全
  - 远程访问的管理
  - 渗透测试、系统漏洞扫描
  - 网络变更
- 环境风险（系统物理环境控制）
  - 消防设施
  - 温度湿度监控
  - UPS
  - 机房的防火墙、地板和天花板

信息技术一般性控制

- 灾难恢复计划（DRP）和业务持续性计划（BCP）：一旦连续的业务被（意外）中断（或破坏），灾难恢复计划确保（灾难）对业务影响最小化的同时，及时恢复（中断的）IT 服务。
  - 灾难恢复计划
  - 业务持续运行计划
  - 根据组织规模与需求的不同还可能包含危机通信计划、场所紧急计划等

业务流程层面信息技术控制

- 嵌于流程之中
- 更多预防性控制
- 控制有效性高
- 自动与人工的综合控制
- 控制可能被篡改
- 受制于信息技术一般性控制
  - 系统安全控制
  - 程序和参数变更控制
  - 系统开发控制
  - 系统运行维护控制

控制类型

控制类型可以归结为以下几种，适用于不同层面的控制点的审计：

- 管理层审阅
- 系统设置/科目映射
- 核对
- 授权及批准
- 职责分工
- 接口/数据转换
- 系统访问权限
- 例外情况报告
- 关键绩效指标
- 报表及关键计算

控制类型

控制类型	类别	需要关注的信息
授权及批准	预防性	❖授权人员做出授权及审批的依据是什么? ❖授权人的能力及在组织中的地位是否能够做出正确的授权及批准?
职责分工	预防性	❖职责分工是否根据不相容职责进行了定义? ❖系统是否能够自动实现定义的职责分工? ❖如果系统无法实现，是否有手工控制作为补偿性控制? ❖职责分工是否有定期审阅?
接口/数据转换控制	预防性	❖接口/数据转换是否对传输内容制定了核对控制? ❖核对的结果是否能够将异常情况记录? ❖异常情况是否被及时跟踪解决? ❖如何确保数据只被传输了一次? ❖核对结果是否被审阅?

控制类型

控制类型	类别	需要关注的信息
系统访问权限	预防性	❖权限分配的合理性及审批的权威性? ❖访问是否留有记录，并被监控? ❖访问权限是否被定期审阅?
例外情况报告	发现性	❖例外情况报告是否涵盖了例外情况主要的类型? ❖例外情况是否被适当记录并被及时跟踪解决? ❖例外情况是否被汇总并被审阅?
系统设置/科目映射	预防性	❖科目映射/系统设置是否经过合理审批? ❖设置是否有复核?
关键绩效指标	发现性	❖对KPI的定义是否有定期审核? ❖KPI的考核机制是怎样的? ❖对于KPI考核中发现的问题的跟踪解决机制是什么?

控制类型

控制类型	类别	需要关注的信息
管理层审阅	发现性	❖对审阅内容的定义是否明确，如审阅的内容及判断标准? ❖审阅的结果是否有明确记录? ❖审阅人员的能力及在组织中的地位是否能够有效履行该控制点? ❖审阅中的异常是否被及时跟进处理?
核对	发现性	❖核对是否明确定义了核对的内容? ❖当发生异常时，系统是否能够及时体现差别的内容? ❖核对的结果是否被及时跟踪解决? ❖核对的报告是否有汇总并提交管理层审阅?
报表及关键计算	发现性	❖报表及关键计算的数据源的准确性 ❖报表逻辑的完整性及准确性

控制测试方法

应用控制测试可以通过以下测试手段来获得证据:

- 观察 - 观察相关人员流程或控制的操作

  例如: 观察内部控制运行的实际情况; 例如观察盘点。

  例如: 观察金融市场部人员在重估远期结售汇时, 对远期汇率的维护和审核情况;

- 询问 - 从有相关专业知识/技能的人员获得信息

  例如: 向适合的人员询问有关控制运作的资料 (例如向负责应收账款回收的人员询问其认为可收回的应收账款的金额、账龄、及将会采取的措施) 。

  例如: 向资产负债部门人员询问不同种类债券的剩余期限计算方式, 了解流动性分析报表的统计口径。

控制测试方法

- 检查 - 检查纸质或电子或其他介质的记录或文件

  例如：检查内部控制生成的记录和文件 (例如银行余额调节表)，即作为内控有效实施的证据。

  例如：检查贷款业务系统记录的关键操作记录，如贷款审批记录，确认是否经过适当的人员审批。

- 重新履行 – 重新履行流程和控制

  例如：重新履行某些内部控制程序，以证明其运行是正确的 (例如重新进行供应商选择的分析) 。

  例如：依据担保方式和逾期天数，重新计算零售类贷款的五级分类结果。

控制测试方法

上述标准的测试手段，经常被综合运用

- 能力评估：综合运用询问、文件检查、重新履行等手段，可以测试某个管理人员在某一领域的知识及其实施某项控制程序的胜任能力。

  例如：与资金交易后台操作人员面谈，来评估其是否了解不同种类债券折溢价部分的摊销方式，检查某支债券的摊销结果。

- 确证询问：除实施适当测试手段外，通过询问企业内其它人员，验证控制的执行情况。这个过程的目的在于确认控制使用的有效性及一致性。

  例如：分别向两个营业柜台人员询问提现的操作流程，以证明大额提现需要主管授权。

- 系统查询：测试信息系统中的自动化控制的有效性。例如测试系统预定义的控制或逻辑权限设置。具体范围可包括：科目余额对帐报告的自动生成、贷款减值迁徙率的自动计算，总分帐科目映射及通过逻辑权限设置来实现职责分工等。

主要内容

第四部分 Cobit介绍

1、Cobit的产生背景

2、Cobit框架

3、Cobit的产品及应用

（1）控制目标

（2）管理指引

（3）审计指引

CobiT的产生背景

- 利用技术来实现企业战略的压力越来越大
- 越来越复杂的信息技术环境
- 信息技术基础设施分散
- 业务经理和信息技术经理不能有效地沟通
- 内部信息技术部门或外包的信息技术提供商不能提供满意的信息技术服务
- 信息技术成本好像已经不受控制了
- 技术方面的投资回报和产能非常少
- 企业失去了灵活性而不能应付转变
- 用户的失望直接导致不成熟解决方案的采用

CobiT的产生背景（续）

- 更加依赖信息和传输这些信息的系统；
- 越来越多的安全隐患和来自不同层面的威胁，例如网络入侵和信息战；
- 信息和信息技术上的投资规模和大小；
- 遵循法规的要求；
- 利用技术来改变企业组织架构和业务操作的潜力，创造新的机会和降低成本；
- 越来越被多的企业认识到技术可以产生的潜在收益

成功的企业能够非常有效的理解和管理在实施新技术时的相关风险。

CobiT的产生背景（续）

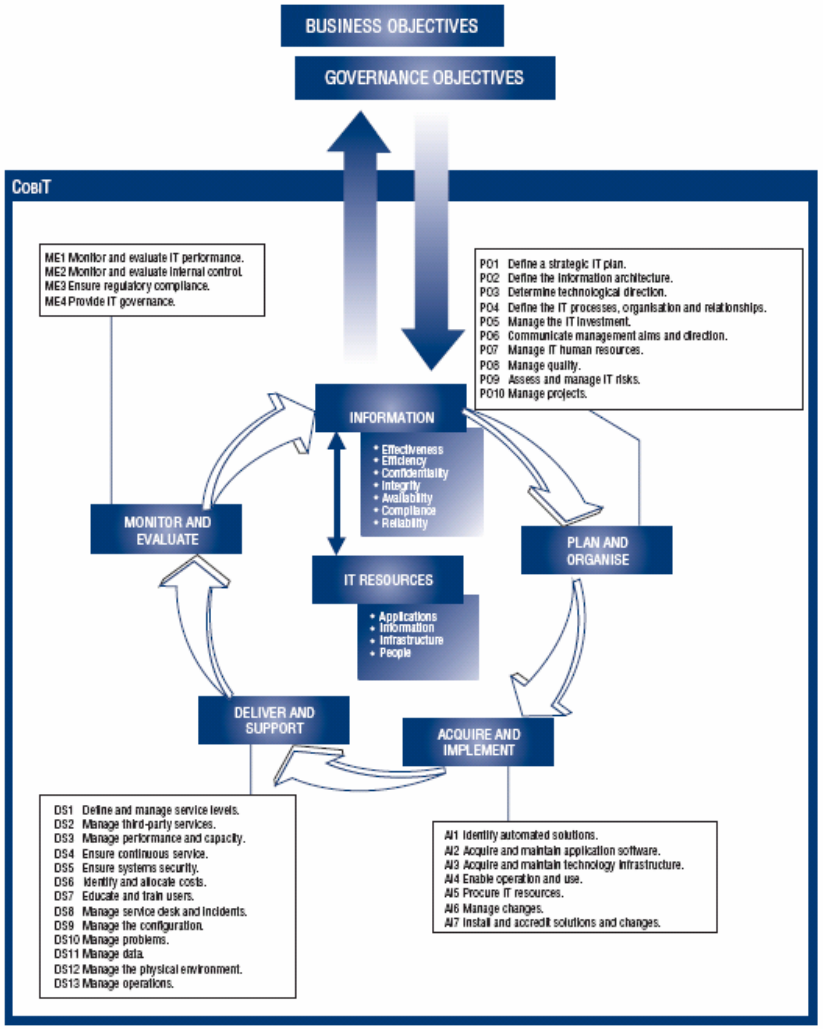
CobiT 可以满足各种需求

- 结合了主要的国际标准
- 已经成为信息技术控制领域毋容置疑的标准
- 以业务需求为起点
- 以流程为导向

CobiT框架

CoBIT把IT分成四个领域

- 策划和组织
- 获取和实施
- 交付和支持
- 监控和评价



CobiT 信息技术控制框架

- 以信息技术传递信息来满足企业需求为前提
- 提高流程的针对性和流程的所有权
- 将信息技术按照四个领域划分为34个流程，为每一流程提供高层次的控制目标
- 根据企业对质量和安全的要求，提供七种信息标准来定义企业业务对信息技术的要求
- 由详细的216个控制目标来支持

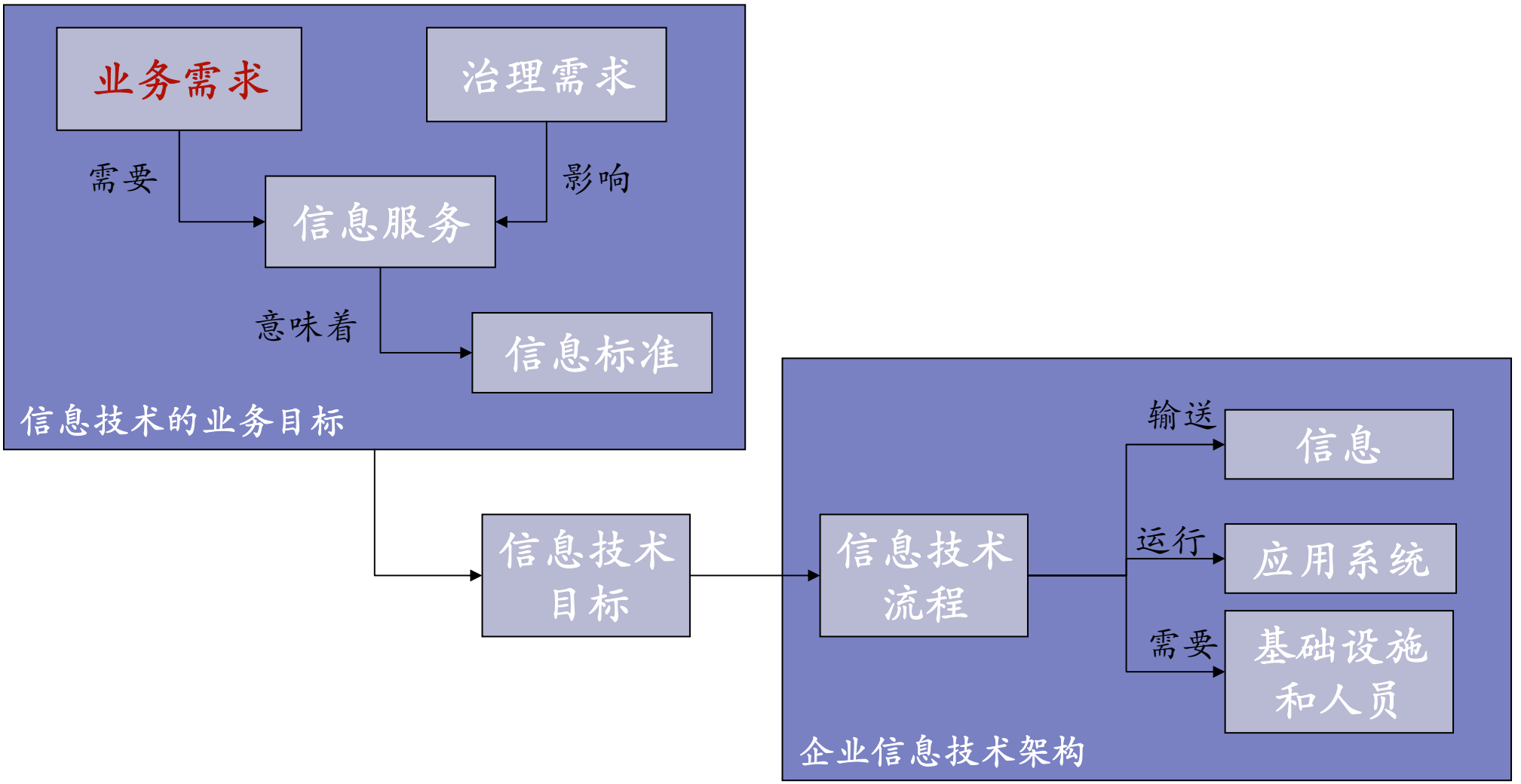
- 策划
- 实施
- 交付 & 支持
- 监控 & 评价

- 效率
- 效果
- 可用性
- 完整性
- 保密性
- 可靠性
- 合规

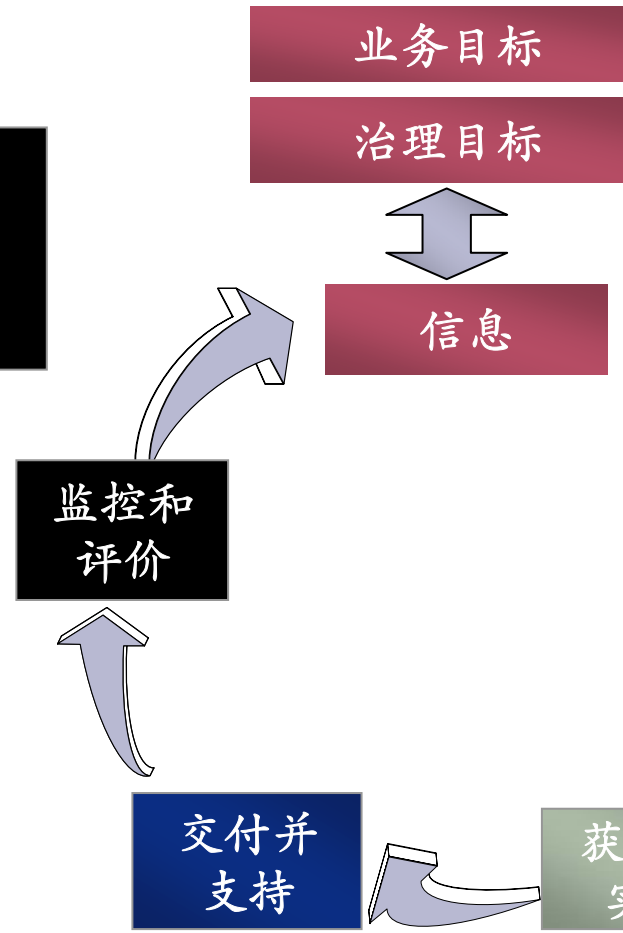
CobiT的主要属性

- 以业务为中心
- 以流程为导向
- 以控制为基础
- 以衡量为驱动

以业务为中心



以流程为导向



PO1 定义战略性的IT计划
PO2 定义信息架构
PO3 确定技术方向
PO4 定义IT流程、组织和关系
PO5 管理IT投资
PO6 沟通管理目标和方向
PO7 管理IT的人力资源
PO8 管理质量
PO9 评估和管理IT风险
PO10 管理项目

AI1 定义自动的解决方案
AI2 采购并维护应用软件
AI3 获得并维护技术架构
AI4 确保运行和使用
AI5 获得IT资源
AI6 管理变更
AI7 安装并授权解决方案和变更

DS1 定义和管理服务水平
DS2 管理第三方服务
DS3 管理性能和容量
DS4 确保服务的连续性
DS5 确保系统的安全性
DS6 确定并分配成本
DS7 教育和培训用户
DS8 管理服务台和事件
DS9 管理配置
DS10 管理问题
DS11 管理数据
DS12 管理物理环境
DS13 管理运行

ME1 监控和评估IT性能
ME2 监控和评估内部控制
ME3 确保规则的执行
ME4 提供IT管理

以控制为基础

业务控制 & 信息技术控制

- 高级管理层
- 业务流程层面
- 业务支撑层面 (信息技术)

信息技术整体控制

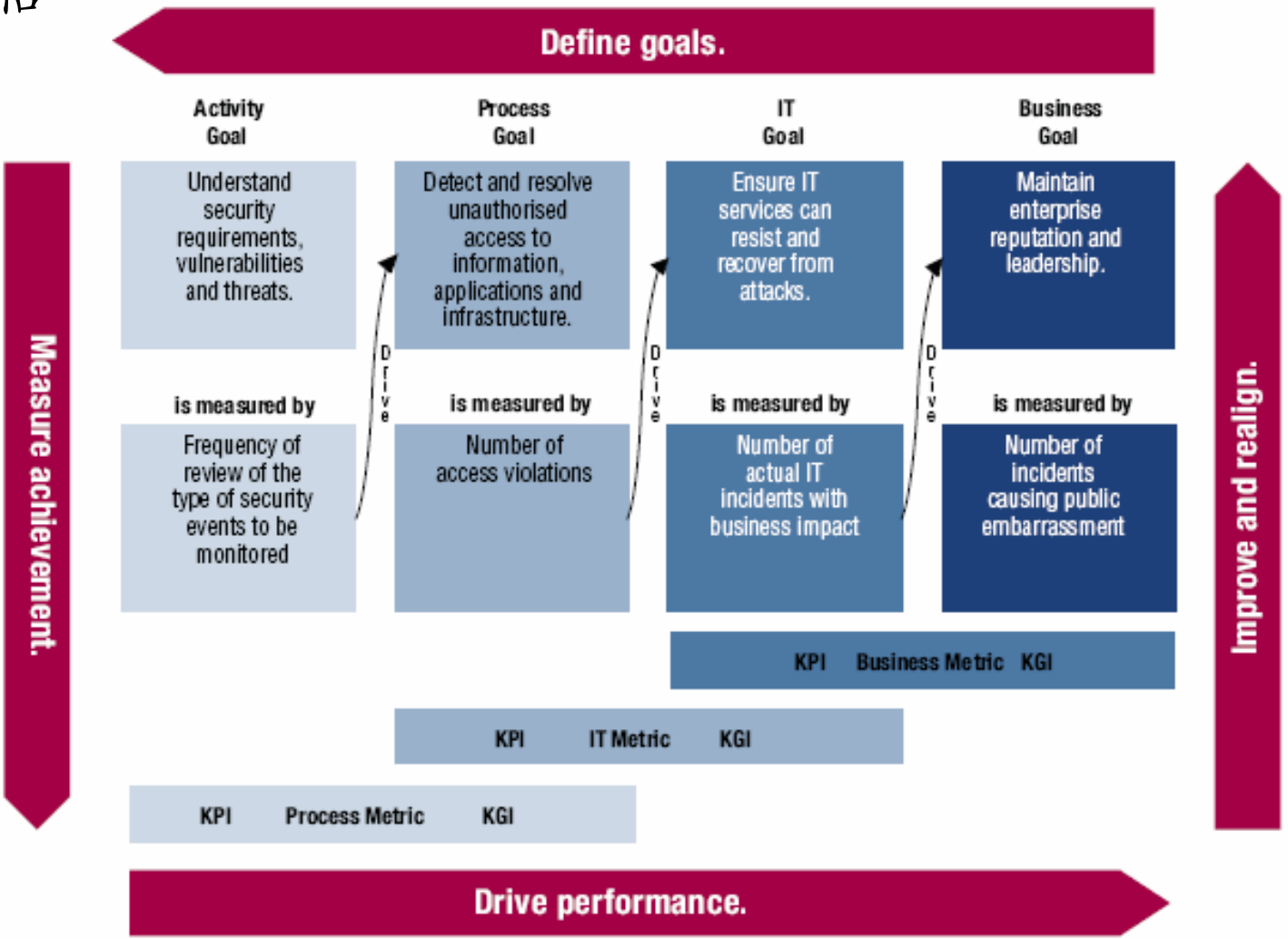
- 系统开发
- 变更管理
- 系统安全
- 系统运行

应用系统控制

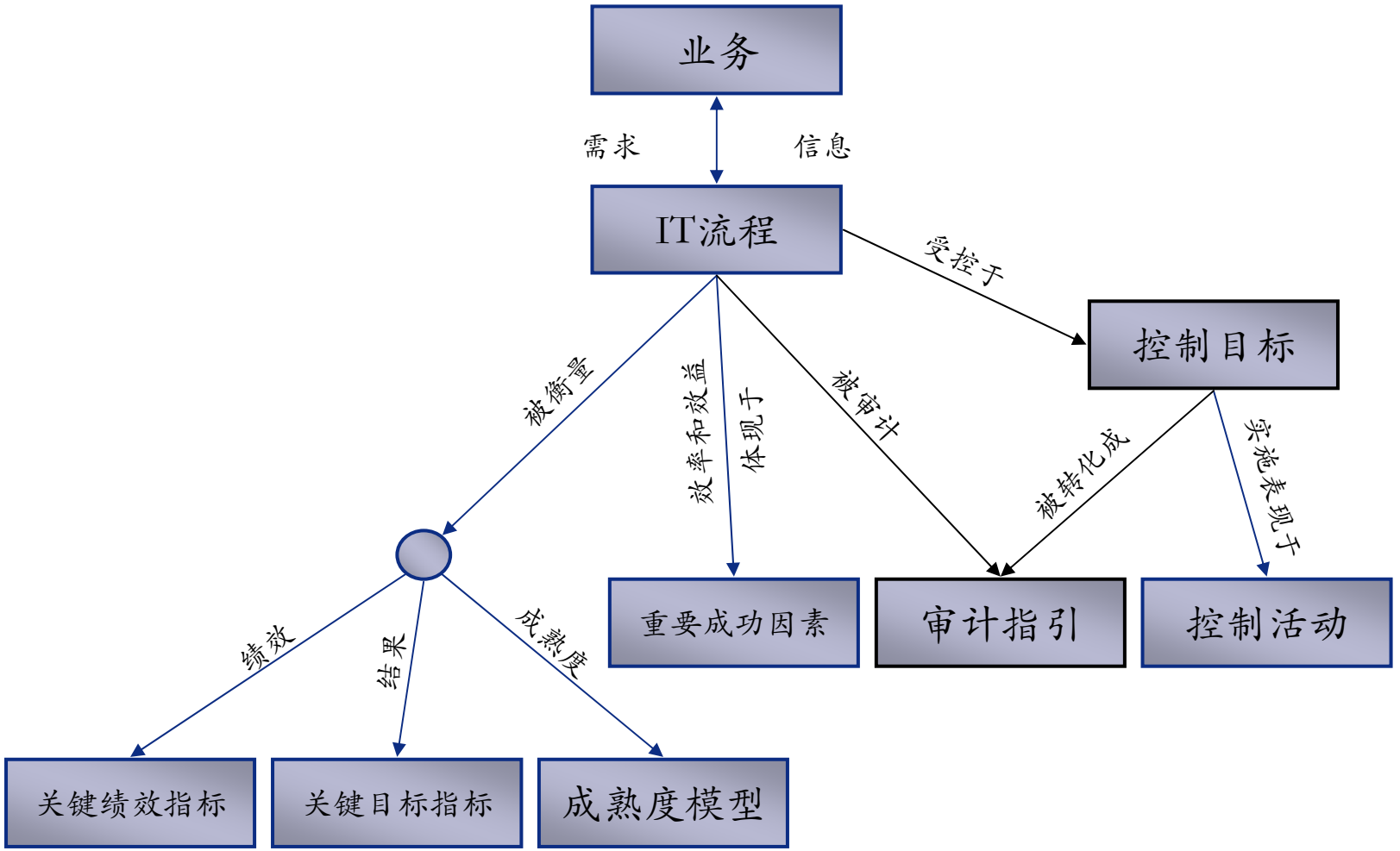
- 数据源/授权控制
- 数据输入控制
- 数据流程控制
- 数据输出控制
- 范围控制

以衡量为驱动

绩效评估


Define goals.
Activity Goal
Process Goal
IT Goal
Business Goal
Understand security requirements, vulnerabilities and threats.
Detect and resolve unauthorised access to information, applications and infrastructure.
Ensure IT services can resist and recover from attacks.
Maintain enterprise reputation and leadership.
Drive
Drive
Drive
is measured by
is measured by
is measured by
is measured by
Frequency of review of the type of security events to be monitored
Number of access violations
Number of actual IT incidents with business impact
Number of incidents causing public embarrassment
Measure achievement.
Improve and realign.
KPI Business Metric KGI
KPI IT Metric KGI
KPI Process Metric KGI
Drive performance.

CobiT 各个组成部分之间的关系



重要的CobiT产品

控制目标—
“最起码应该有这些控制…”

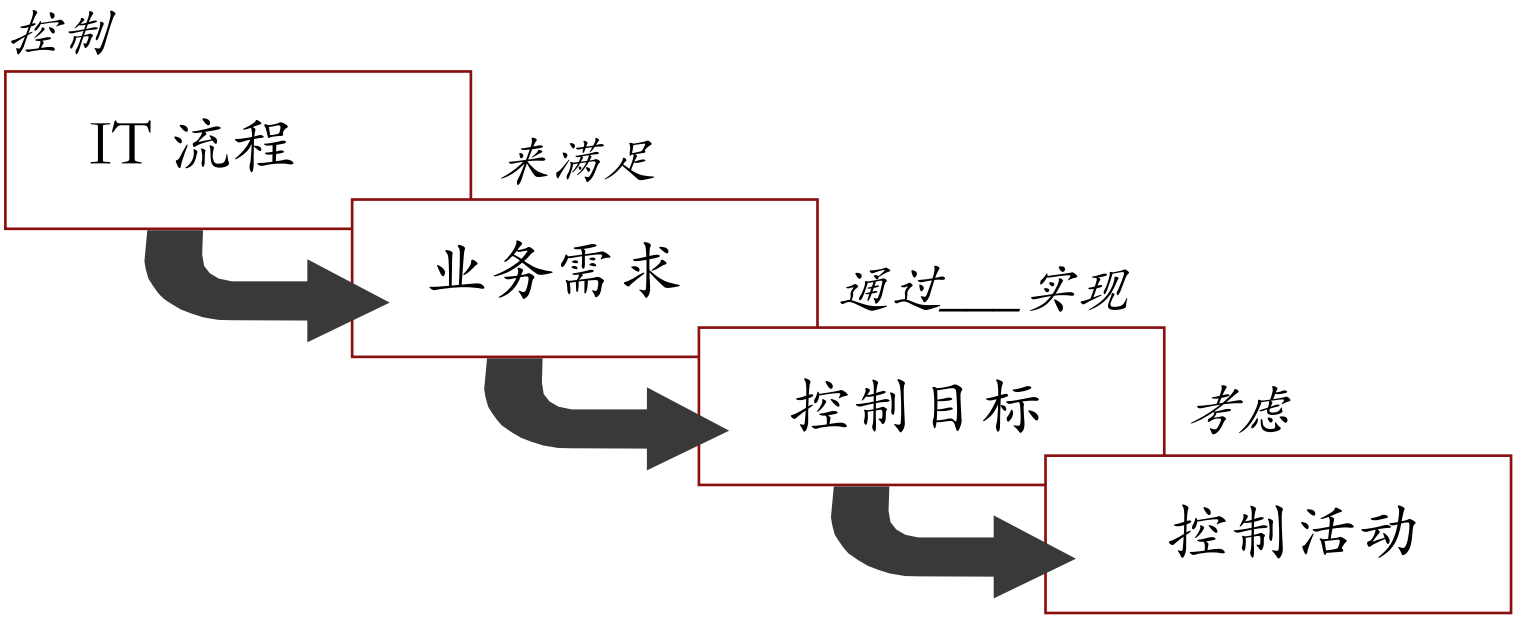
管理指引—
“这些是可以衡量的…”

审计指引—
“你可以这样进行审计…”

CobiT控制和控制目标定义

- 高层次控制目标
  - 每个流程一个
- 详细的控制目标
  - 每个流程3到30个
- 控制活动
  - 每个控制目标5到7个

瀑布模式



4 个领域- 34 个流程 – 216个控制目标

高层次控制目标

AI6 管理变更

Managing changes to computer programs is required to ensure processing integrity between versions, and for consistency of results period to period. Change must be formally managed via change control request, impact assessment, documentation, authorisation, release, and distribution policies and procedures.

详细的控制目标

AI6 变更管理

AI6.1 变更标准和流程

Set up formal change management procedures to handle in a standardised manner all requests (including maintenance and patches) for changes to applications, procedures, processes, system and service parameters, and the underlying platforms.

AI6.2 影响评估、排序和授权

Ensure that all requests for change are assessed in a structured way for impacts on the operational system and its functionality. This assessment should include categorisation and prioritisation of changes. Prior to migration to production, changes are authorised by the appropriate stakeholder.

AI6.3 紧急变更

Establish a process for defining, raising, assessing and authorising emergency changes that do not follow the established change process. Documentation and testing should be performed, possibly after implementation of the emergency change.

AI6.4 变更状态跟踪和报告

Establish a tracking and reporting system for keeping change requestors and relevant stakeholders up to date about the status of the change to applications, procedures, processes, system and service parameters, and the underlying platforms.

AI6.5 变更关闭和归档

Whenever system changes are implemented, update the associated system and user documentation and procedures accordingly. Establish a review process to ensure complete implementation of changes.

控制活动

将CobiT的控制目标转化成详细的、可以实施的活动，从价值和风险角度来提供业务根据。

- 控制活动是支持下点的关键控制机制：
  - 控制目标的实现
  - 防止、发现和纠正不希望发生的事件
- 控制活动实现以上目标通过：
  - 负责任的使用资源
  - 合适的管理风险
  - 将IT和业务相对应

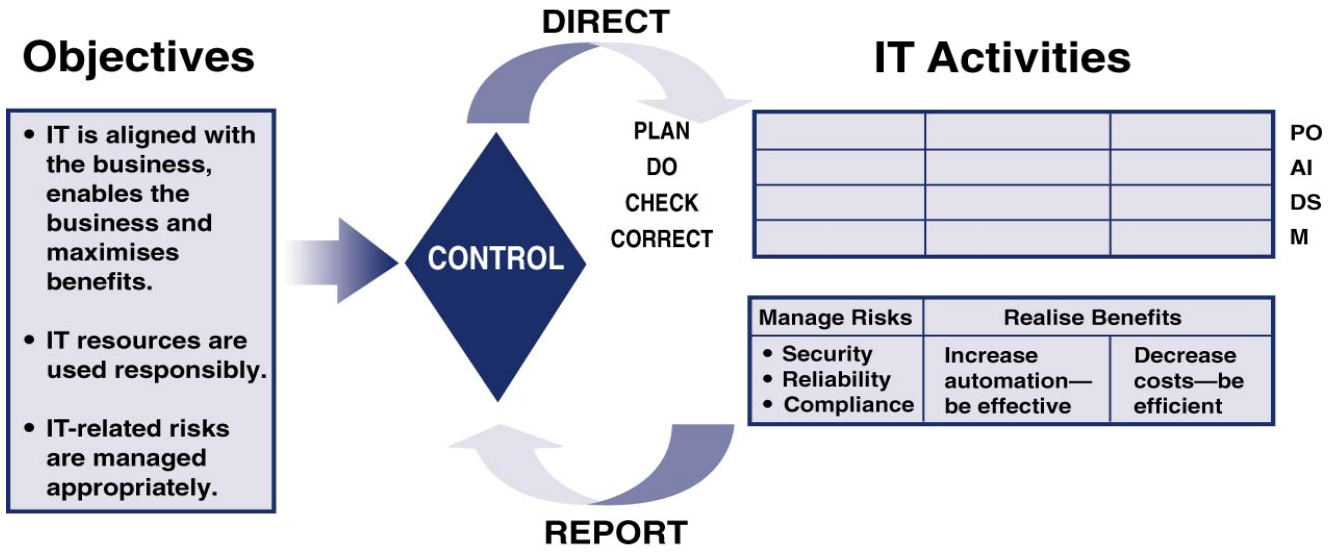
重要的CobiT产品

控制目标—
“最起码应该有这些控制…”

管理指引—
“这些是可以衡量的…”

审计指引—
“你可以这样进行审计…”

IT 治理模式

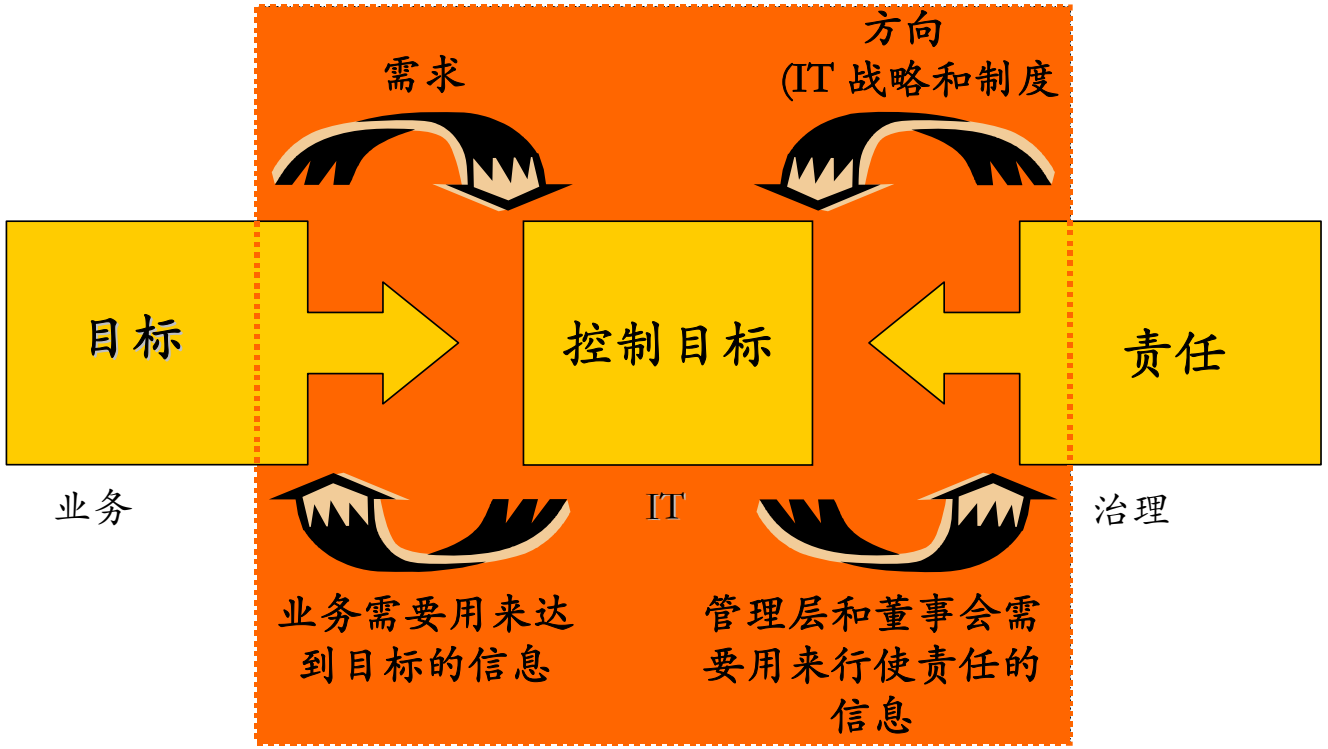


IT 治理帮助确定自动化系统如何:

- 将运营简单化
- 降低成本
- 增加收入

需要有一个IT控制框架

CobiT 如何与IT治理联系起来?



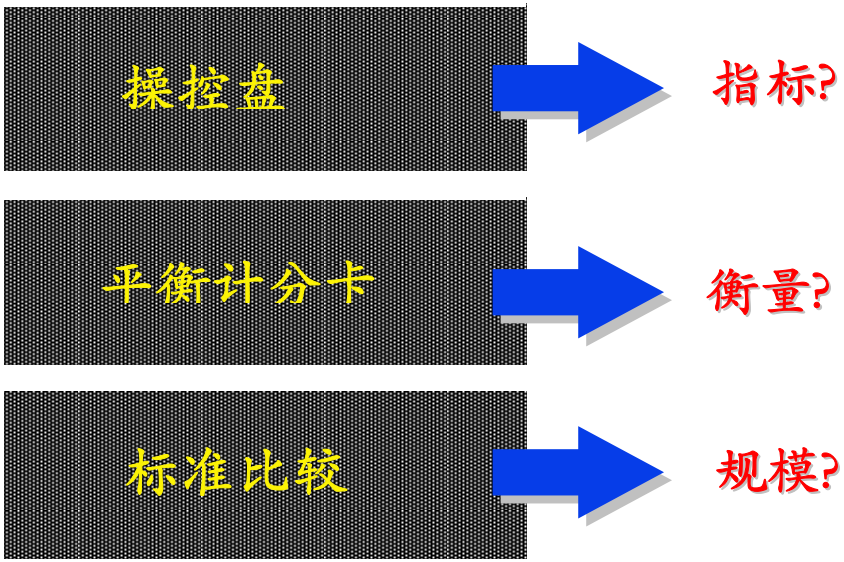
管理指南

但是，管理层还有除了控制框架以外的问题:

负责的管理人员如何保证“船的正确方向”？

如何最大限度的完成权益人要求达到的目标?

如何在企业环境的发展下及时转变企业的行为?



管理指南框架

IT KGI

-
-
-

流程 KGI

-
-
-

KPI 关键绩效指标

-
-

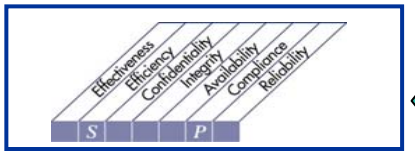
RACI 图和职能

RACI Chart

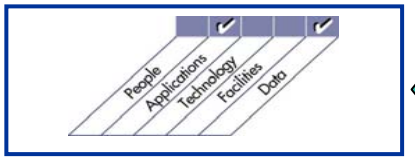
Functions

Activities	CEO	CFO	Business Executive	CIO	Business Process Owner	Head Operations	Chief Architect	Head Development	Head IT Administration	PMO	Compliance, Audit, Risk and Security
Create and maintain corporate/enterprise information model.		C	I	A	C		R	C	C		C
Create and maintain corporate data dictionary(ies).				I	C		A/R	R			C
Establish and maintain data classification scheme.	I	C	A	C	C	I	C	C			R
Provide data owners with procedures and tools for classifying information systems.	I	C	A	C	C	I	C	C			R
Utilise the information model, data dictionary and classification scheme to plan optimised business systems.	C	C	I	A	C		R	C			I

A RACI chart identifies who is Responsible, Accountable, Consulted and/or Informed.



信息标准



资源

流程输入和输出

PO2 Define the Information Architecture

From	Inputs
PO1	Strategic and tactical IT plans
AI1	Business requirements feasibility study
AI7	Post-implementation review
DS3	Performance and capacity information
ME1	Performance input to IT planning

Outputs	To						
Data classification scheme	AI2						
Optimised business systems plan	PO3	AI2					
Data dictionary	AI2	DS11					
Information architecture	PO3	DS5					
Assigned data classifications	DS1	DS4	DS5	DS11	DS12		
Classification procedures and tools	*						

* Outputs to outside CoeIT

成熟度模型

0 - Management processes are not applied at all.
1 - Processes are *ad hoc* and disorganised.
2 - Processes follow a regular pattern.
3 - Processes are documented and communicated.
4 - Processes are monitored and measured.
5 - Best practices are followed and automated.

重要的CobiT产品

控制目标—
“最起码应该有这些控制…”

管理指引—
“这些是可以衡量的…”

审计指引—
“你可以这样进行审计…”

CobiT审计指南

一个通用指南和

34个以流程为导向的指南

- **通用指南**定义了评估任一流程中的控制目标所需执行的不同任务。该通用指南是所有控制目标的一个模型；
- 其他的指南是推荐的、非常具体的以**流程为导向**的任务，针对控制的存在和控制发动合理有效性给管理层提供一个保证。

通用审计指南（1/4）

获得了解

应该执行的审计步骤包括记录与控制目标相关的活动，识别存在的控制措施/流程。

- 与适当的管理层和员工访谈来取得对以下内容的了解：
  - 业务需求和相关的风险
  - 组织结构
  - 职责分工
  - 制度和流程
  - 法律法规
  - 存在的控制措施
  - 管理报告（现状、进行、行动）
- 记录影响流程的IT资源；
- 加强对所检查的流程和控制的了解，例如，通过一个流程穿行测试。

通用审计指南（2/4）

评价控制

执行的审计步骤包括评估控制的有效性或者满足控制目标的程度。

- 通过比较行业内标准做法和应用专业的判断，评价对所检查的流程控制措施的有效性。确定：
  - 所记录的流程是否存在；
  - 是否存在适当的交付成果；
  - 职责和责任是否清晰与有效；
  - 如有必要，是否存在补偿性控制。

- 总结控制目标的满足程度。

通用审计指南（3/4）

评估符合性

执行的审计步骤包括确保所述控制按照规定一致地和连续地运行。

- 获得针对所选审计单元/审计期间的直接或者间接证据来确保流程是遵循检查期间的规则来执行的；
- 有限度的对流程的交付成果进行审阅；
- 确定实质性测试和附加工作的多少来保证IT流程是否适当和合理。

通用审计指南（4/4）

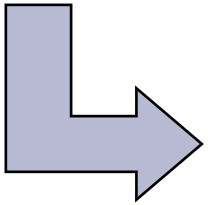
将风险具体化

执行的审计步骤包括运用分析技术和/或咨询手段来将没有满足控制目标的风险具体化。

- 记录控制弱点和导致的威胁和漏洞。
- 识别并记录实际的和潜在的影响。

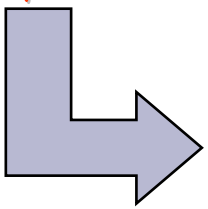
审计指南和控制目标如何关联?

- **获得了解**
  - 收集涉及业务环境、风险和基础设施的背景信息。
- **评价适当性**



控制目标被转化为：验证他们是否得到相应的处理，同时考虑企业和管理层宣称控制目标存在的适当性。

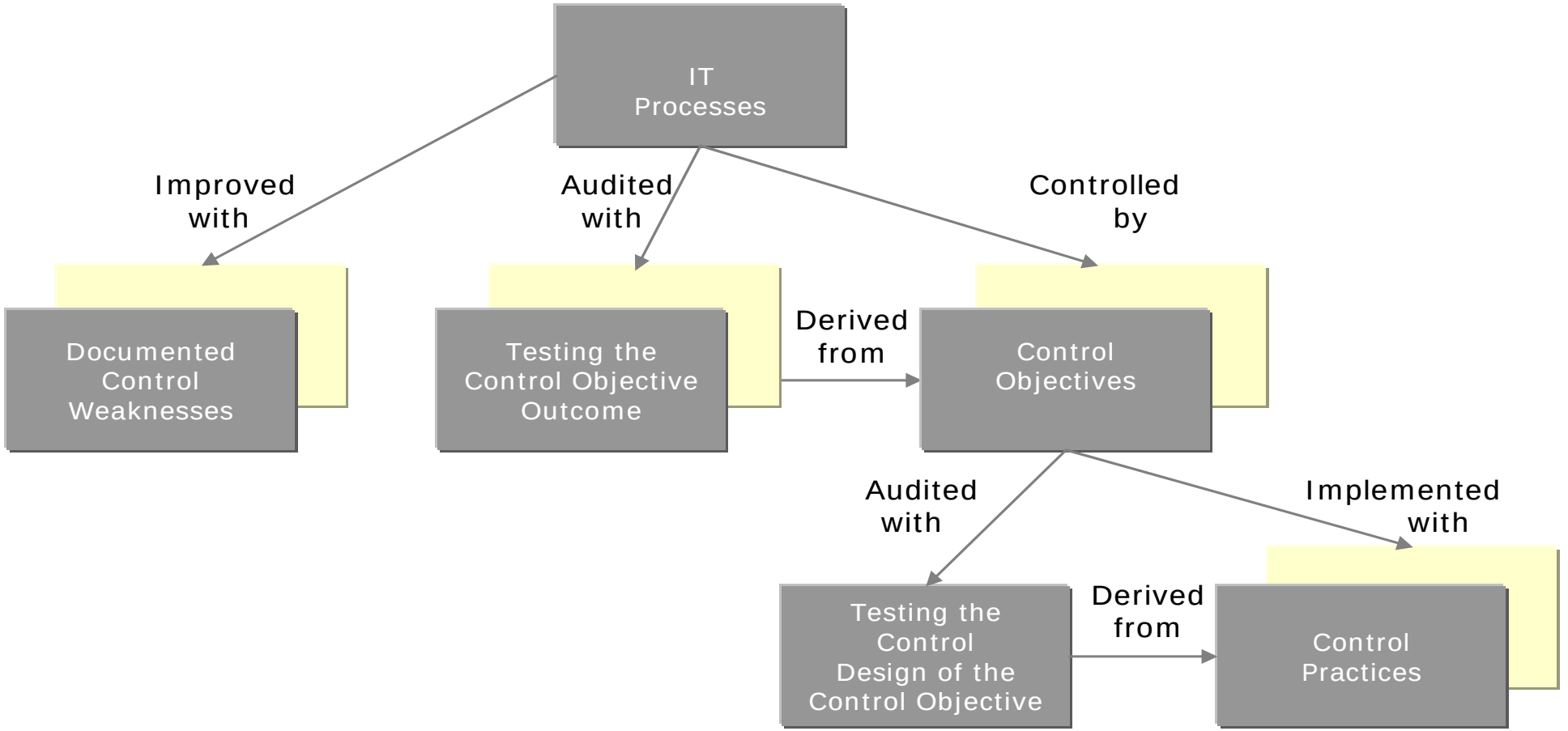
- **评估符合性**



控制目标被转化为：测试和/或测量满足控制目标的控制是否如同所讲述的一样存在，以及他们是否运行有效。

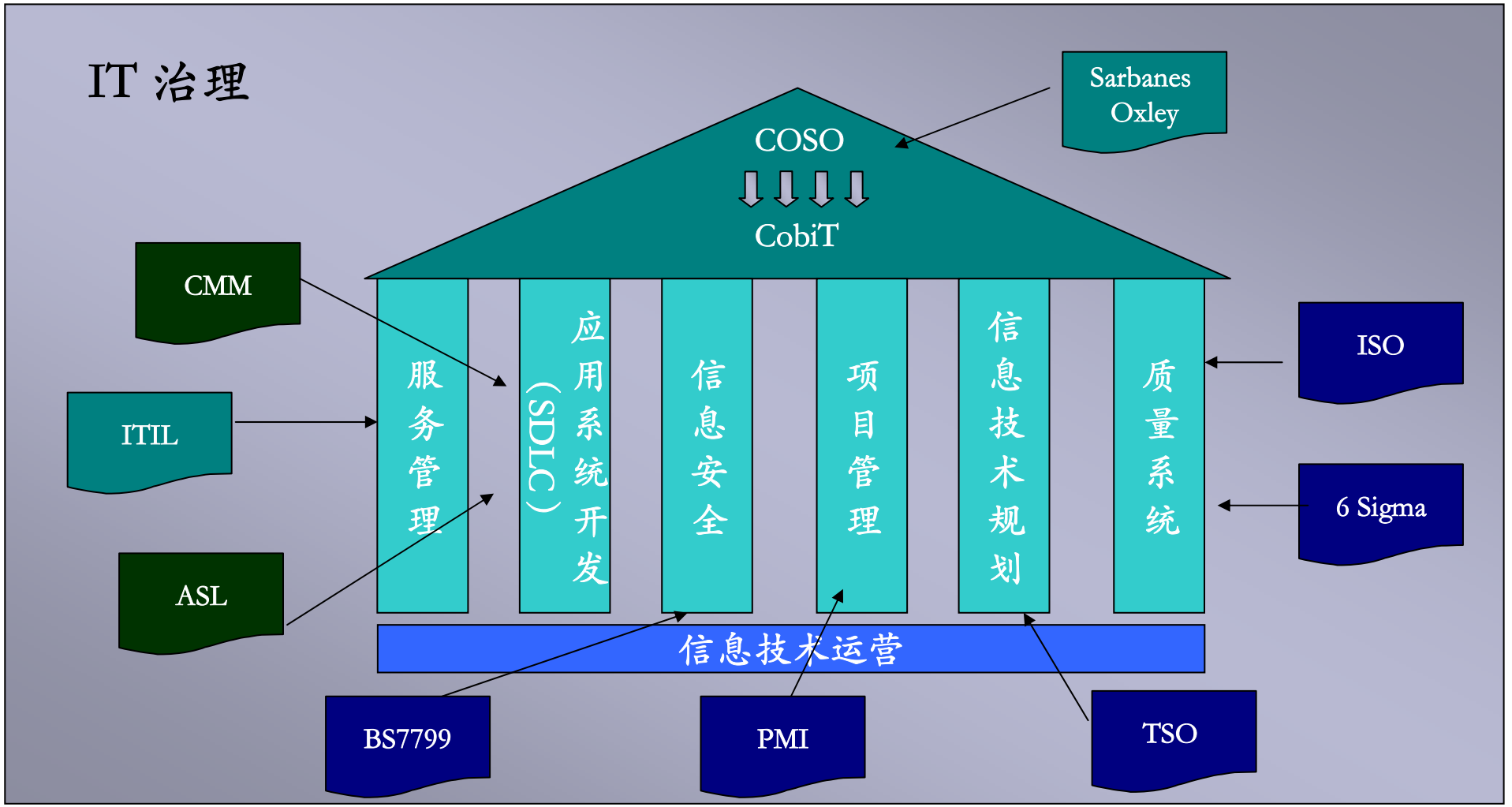
- **将风险具体化**
  - 阐明由于缺乏控制而引起的未能满足的业务目标、业务损失等。

审计框架



Generic ( ) and Specific ( ) Advise in the Assurance Guide

国内和国际的信息技术审计相关的标准



主要内容

第五部分 IT审计的辅助工具——CAATs

1、CAATs概述

2、使用CAATs

3、CAATs的收益

计算机辅助审计技术介绍

- 任何自动化技术，例如通用审计软件、功能软件、测试数据、应用软件跟踪/对应，以及审计专家系统都可以称为计算机辅助审计技术（**Computer Assisted Audit Technologies**）。

- 计算机辅助审计技术用于协助审计团队执行各项测试，包括数据抽取、分析重新计算和差异分析等。

- 对系统分析和记录、系统测试—控制和运营、数据测试及交易测试非常的有效。

CAATs的工作步骤

- 计划
- 测试CAATs
- 执行CAATs
- 记录工作过程及结果
- 报告

CAATs工作中需要注意的地方

- 明确审计目标
- 确认审计所用脚本的准确性和完整性
- 确认数据源的完整性和准确性
- 审计过程中数据的安全
- 审计结果的分析及判断
- 审计过程的记录

CAATs – 主要收益

审计团队从CAATs中获得的三大收益:

- **在最初一年节省大量审计时间**

  完成同样的工作，比手工测试花费更少的时间。自动测试一般可以节省40-60% 的时间。

- **审计覆盖面达到更高层次**

  CAAT方法测试所有交易，而不只是样本，在更少的时间内为审计队伍提供了保证。

- **为下一次审计节省了时间和金钱**

  在随后几年，同样的CAAT常规程序可以在最小时间内运行，达到更大效率。在第一年的6小时测试，在第2年可能只需要3小时!

主要内容

第六部分 信息技术审计案例

1、审计目标和范围

2、审计流程：

-战略分析

-风险评估

-制定计划

-实施审计

-审计报告

-问题解决与跟踪

审计案例 – 信息系统开发风险

- **审计目标和范围：**

信息系统开发流程审计的目标在于：通过审计信息系统开发过程中的风险和控制活动，评价信息系统开发管理的有效性，揭示信息系统开发管理中存在的问题和风险，提出改进建议，促进信息系统开发项目的风险管理水平建设，降低项目风险，提高项目的整体绩效。

信息系统开发审计是以整个信息系统开发生命周期为工作范围，覆盖项目从可行性研究以及立项开始，经过开发需求分析、系统设计和开发、系统测试和上线，直至项目验收的全过程，评估项目在系统开发流程、风险和控制方面的管理程度。

审计案例 – 信息系统开发风险

- **战略分析：**

  深入分析信息系统开发风险管理状况，包括内外部环境因素和信息科技战略，以及对信息系统开发风险管理的影响，以此作为信息系统开发风险管理稽核评价的出发点，制定信息系统开发风险管理审计的重点。

- **风险评估：**

  识别信息系统开发过程中关键流程，从项目风险管理的战略驱动风险、项目/项目群管理风险、流程风险、技术风险、人员风险、数据风险等六个风险领域以及系统开发生命周期的可行性研究、开发需求分析、系统设计开发、系统验收测试、系统上线切换和开发项目验收等六个阶段，对其相关风险进行识别，并根据关键固有风险可能带来的影响和发生可能性等因素对其进行风险评估。

审计案例 – 信息系统开发风险

风险评估矩阵：

风险领域	风险编号	主要风险	影响	发生可能性	固有风险评估
战略驱动	1	…	重大	很可能	高
	…	…	…	…	…
项目管理/项目群管理	3	…	较大	可能	中
	…	…	…	…	…
业务流程	15	…	重大	很可能	高
	…	…	…	…	…
技术	20	…	较大	可能	中
	…	…	…	…	…
人员	28	…	重大	很可能	高
	…	…	…	…	…
数据	33	…	重大	很可能	高
	…	…	…	…	低

审计案例 – 信息系统开发风险

❖ **审计计划：**

- 建立稽核矩阵。稽核矩阵是执行审计的核心工作内容。在稽核矩阵中，对选取的控制点逐一进行控制测试。

控制点信息			控制设计测试			控制执行测试			控制点总体结论
控制点编号	控制点描述	控制点负责人	测试步骤	测试结果	测试结论	测试步骤	测试结果	测试结论	

- 制定审计进度时间表：根据所审计项目的实际情况，估算审计过程的人员和时间投入，制定审计工作的整体进度。

- 确定审计里程碑及成果：即审计过程中的成果及产出物，如审计计划、工作底稿、问题发现清单、审计报告等等。

审计案例 – 信息系统开发风险

❖ **实施审计:**

根据确定的审计程序，通过人员访谈、项目相关文档审阅等手段对系统开发各环节的控制管理情况进行测试活动，根据审计结果评定各控制点的有效性。针对无效的控制点，归纳出问题发现清单，并对具体问题及其风险进行说明。

❖ **审计报告:**

审计报告是对稽核工作的汇总和总结，通常包括以下主要方面:

- 总结审计整体情况
- 汇总审计发现
- 评估剩余风险
- 提出改进建议

审计案例 – 信息系统开发风险

- **问题的解决与跟踪：**

  通过适当的方式，将审计结果与项目管理方进行沟通，针对发现的问题和风险探讨改进方案。审计人员要根据改进方案跟踪问题的解决情况。并根据需要进行问题的专项审计。

讨论

毕马威联系方式:

刘强
高级经理
风险咨询服务

毕马威华振会计师事务所
中国北京
东城区东长安街1号
东方广场东2座8层
邮政编码 100738

北京办公室电话: + 86 (10) 8508 5404
传真: + 86 (10) 8518 5111
邮件地址: sam.liu@kpmg.com.cn