IT治理与风险管理

- 陈忠阳教授
- 中国人民大学财政金融学院

一、治理与风险的基本关系

- 治理的本质
- 治理与风险
- IT治理的内容与目标

治理的本质

- 形式上：一整套据以对公司进行管理和控制的体系，具体包括流程、习惯、政策和机构设置等。（OECD）
- 本质上：是对公司利益相关方（Stakeholder）责权利关系的一种安排
- 目的：企业实现价值目标

治理与风险

- 风险是治理关系安排的核心，即所谓风险治理
- 有效治理的关键在于明确风险的所有者（RISK OWNER）：谁是风险的所有者？
- 风险管理者和风险所有者之间的问题：委托代理、信息不对称、监督管理、激励机制
- 承担和管理风险的责权利是什么？事前观和事后观
- 可见，风险治理是围绕公司范围内风险承担和风险管理的决策权（事前）、问责（事后）和激励制度安排

IT治理的内容与目标

- 根据国际信息系统审计与控制协会(ISACA)的定义: IT治理是一个由各种关系和活动过程组成的治理结构，用以指导和控制企业的IT活动，其目的是为了在平衡IT和IT活动所产生的风险与回报的过程中，通过增加商业价值来实现企业的目标。
- 商业银行实施IT治理的目的是要使IT应用最大限度地满足以下目标：
  - 确保银行的IT战略目标和银行整体战略目标一致
  - 促进银行业务的发展，并使银行收益最大化
  - 负责任、可靠地利用各种IT资源
  - 管理和控制与IT相关的各类风险

二、IT风险治理体系的内容

- IT风险治理的利益相关方
- IT风险的内涵和范围
- IT治理活动：对风险的治理关系安排行为

IT治理利益相关方

- 股东、董事会和大小股东
- 管理层：IT使用部门、IT科技部门、风险管理部门、审计部门，等等
- 客户和银行服务使用者
- 供应商
- 监管部门
- 等等

IT相关风险

- 业务风险
- 声誉风险
- 法律合规风险
- 战略风险
- 数据风险
- 模型风险

IT治理相关活动

- 治理模式定位 （见后一张幻灯片）
- 组织架构、职责分配、报告线路
- 风险文化建设
- 内部控制
- 风险管理（操作风险管理、法律合规管理）： 政策和评估
- 薪酬机制（如RAROC的引入）
- 审计 活动

IT 治理：几种模式

- 彼得.维尔和珍妮.罗斯 ：《IT治理》

模式	谁拥有决策权
业务君主制	一群业务主管或者单个主管，包括高级业务主管委员会（可能包括CIO），不包括IT主管
IT君主制	一个或一群IT主管
封建制	业务单位领导，关键流程负责人或其代表
联邦制	核心级主管和业务团队，可能也包括作为额外参与者的IT主管，相当于中央政府和州政府的协同工作机制
IT双寡头制	IT主管和其他团队（如业务主管或业务单位负责人）
无政府制	每一个单独的使用者

三、结论

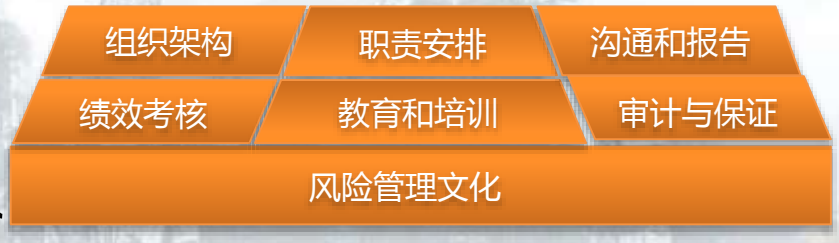
- IT治理的核心内容在于IT风险治理
- IT风险治理的本质在于围绕公司范围内IT风险承担和风险管理的决策权（事前）、问责（事后）和激励制度的安排
- IT治理是有效IT风险管理的基石
- IT风险管理也是IT治理成功的标志

IT风险管理：体系建设

策略层面

管理层面

治理层面



多谢！
请批评指正。