CIO 知识（2）：IT 治理

信息化是企业管理的重要组成部分，为充分发挥 IT 系统的价值，企业必须确保 IT 战略和企业战略的匹配、IT 系统运行的效率、IT 投资的效益以及控制 IT 运行风险。在这方面，企业需要引进 IT 治理的观念，建立和完善 IT 决策体系、决策流程，从而优化 IT 治理架构，规范信息化规划、选型、实施和维护流程，完善 IT 服务体系，从组织、制度和流程上确保信息化建设的成功，规避投资和运行风险。

根据国际信息系统审计与控制协会(ISACA)的定义，IT 治理是一个由关系和流程所构成的体制，用于指导和控制企业，通过平衡信息技术与过程的风险、增加价值来确保实现企业的目标。

IT 管理有广义和狭义之分，广义的 IT 治理还包括 IT 价值管理、IT 服务管理、IT 风险管理等内容。

需要指出的是，IT 治理与 IT 管理是两个不同的概念。IT 治理是企业从董事会等最高决策层面解决 IT 战略决策的结构、流程等问题，确保 IT 建设的正确方向，属于 IT 效益最大化即“做什么”的范畴。IT 管理是企业信息系统的运营，确保 IT 目标实现和 IT 运营效率，属于 IT 效率最大化即“如何做”的范畴。两者相辅相成。

为实现有效的 IT 治理，企业需要参考国际通行的 IT 治理最佳实践和标准，从而建立和完善自身的 IT 治理体系。

目前国际 IT 治理的主要体系是 COBIT 和 ITIL。

1、COBIT(Control Objectives for Information and related Technology 信息和相关技术的控制目标)

COBIT 是目前国际上通用的信息系统审计的标准，由信息系统审计与控制协会在 1996 年公布，目前最新的版本是 4.1。

COBIT 这个框架包括四个过程域，即规划和组织(PO-Planning and Organization)、获取和实施(AI-Acquisition and Implementation)、交付和支持(DS-Delivery and Support)以及监控和评价(ME-Monitor and Evaluate)。在这四个过程域之下，再细分为 34 个流程。

“规划和组织”包括：PO1-IT 战略规划的确定、PO2-信息结构的确定、PO3-技术方向的确定、PO4-IT 组织及关系的确定、PO5-IT 投资管理、PO6-沟通管理的目标和方向、PO7-人力资源管理、PO8-遵守外部要求的保证、PO9-风险评估、PO10-项目管理、PO11-质量管理。

“获取和实施”包含：AI1-确定自动解决方案、AI2-获取和维护应用软件、AI3-获取和维护技术设施、AI4-开发和维护程序、AI5-安装和验收系统、AI6-变更管理。

“交付和支持”包括：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-确保不间断服务、DS5-确保系统安全、DS6-确定和分配成本、DS7-教育和培训用户、DS8-对客户的协

助和建议、DS9-配置管理、DS10-管理问题和意外事件、DS11-数据管理、DS12-设施管理、DS13-运营管理。

“监控和评价”包含：M1-监视过程、M2-评估内部控制充分性、M3-获得独立保证、M4-提供独立的审计。

为有效进行 IT 治理的实施，COBIT 采用关键目标指标（KGI-Key Goal Indicators)来描述过程要达到哪些标准。对于 34 个治理过程，COBIT 设置关键成功因子（ CSF-Critical Success Factors），描述实现 KGI 所必须进行的一系列重要工作。同时，COBIT 设置了关键绩效指标”（ KPI-Key Performance Indicators）用于衡量每个过程达到 KGI 的程度。每个过程达到的 KPI 的程度则用成熟度(CMM-Capability Maturity Model)级别来表示，它们是：

0- 不存在

1- 初始级

2- 可重复级

3- 可定义级

4- 可管理级

5- 可优化级。

通过参照成熟度模型，组织可以对每个过程进行对照，确定本单位的能力成熟度，并根据成熟度的改进路径，采取纠正和改进措施。

2、ITIL（信息技术基础架构库 Information Technology Infrastructure Library, ITIL）

ITIL 由英国政府部门在 20 世纪 80 年代末制订，现由英国商务部 OGC 负责管理，主要适用于 IT 服务管理（ITSM）。2001 年，英国标准协会在国际 IT 服务管理论坛（ITSMF）上正式发布了以 ITIL 为核心的英国国家标准 BS15000。2005 年国际标准化组织及国际电工委员会以 BS15000 为核心，批准通过了 ISO20000 的标准决议，正式发布了 ISO20000 标准，成为国际 IT 服务管理体系建设和评估的标准方法。

ITIL 为组织的 IT 服务管理提供了一个系统、客观、严谨、可量化的标准和规范，IT 部门和最终用户可以根据自己的能力和需求定义自己所要求的服务水平，参考 ITIL 来规划和制定 IT 基础架构及服务管理，从而确保 IT 服务为组织的各项业务运作提供良好的支持。

ITIL 的核心是“服务管理”，包括了十个流程和一项职能，这些流程和职能又被分为两组，即“服务提供”流程组和“服务支持”流程组。

服务提供”流程组包括事故管理、问题管理、配置管理、变更管理和发布管理；“服务支持”流程组包括服务级别管理、IT 服务财务管理、能力管理、IT 服务持续性管理和可用性管理。

服务台是 IT 部门和 IT 服务用户之间的单一联系点。它通过

提供一个集中和专职的服务联系点促进了组织业务流程与服务管理基础架构集成。服务台的主要目标是协调用户和 IT 部门之间的联系，为 IT 服务运作提供支持，从而提高客户的满意度。

事故管理负责记录、归类和安排专家处理事故并监督整个处理过程直至事故得到解决和终止。事故管理的目的是在尽可能最小地影响客户和用户业务的情况下使 IT 系统恢复到服务级别协议所定义的服务级别。

问题管理是指通过调查和分析 IT 基础架构的薄弱环节、查明事故产生的潜在原因，并制定解决事故的方案和防止事故再次发生的措施，将由于问题和事故对业务产生的负面影响减小到最低的服务管理流程。

配置管理是识别和确认系统的配置项，记录和报告配置项状态和变更请求，检验配置项的正确性和完整性等活动构成的过程，其目的是提供 IT 基础架构的逻辑模型，支持其它服务管理流程特别是变更管理和发布管理的运作。

变更管理是指为在最短的中断时间内完成基础架构或服务的任一方面的变更而对其进行控制的服务管理流程。变更管理的目标是确保在变更实施过程中使用标准的方法和步骤，尽快地实施变更，以将由变更所导致的业务中断对业务的影响减小到最低。

发布管理是指对经测试后导入实际应用的新增或修改后的配置项进行分发和宣传的管理流程，目的是要保障所有的软件组件的安全性，以确保只有经过完整测试的正确版本得到授权进入正式运行环境。

服务级别管理是为签订服务级别协议（SLA）而进行的计划、草拟、协商、监控和报告以及签订服务级别协议后对服务绩效的评价等一系列活动所组成的一个服务管理流程。服务级别管理旨在确保组织所需的 IT 服务质量在成本合理的范围内得以维持并逐渐提高。

IT 服务财务管理是负责预算和核算 IT 服务提供方提供 IT 服务所需的成本，并向客户收取相应服务费用的管理流程，它包括 IT 投资预算、IT 服务成本核算和服务计费三个子流程，其目标是通过量化服务成本减少成本超支的风险、减少不必要的浪费、合理引导客户的行为，从而最终保证所提供的 IT 服务符合成本效益的原则。

IT 服务持续性管理是指确保发生灾难后有足够的技术、财务和管理资源来确保 IT 服务持续性的管理流程。IT 服务持续性管理关注的焦点是在发生服务故障后仍然能够提供预定级别的 IT 服务，从而支持组织的业务持续运作的能力。

能力管理是指在成本和业务需求的双重约束下，通过配置合理的服务能力使组织的 IT 资源发挥最大效能的服务管理流程。能力管理流程包括业务能力管理、服务能力管理和资源能力管理三个子流程。

可用性管理是在正确使用资源、方法及技术的前提下保障 IT 服务的可用性和实践可用性要求。目标是确保 IT 服务的设计符合业务所

需的可用性级别。

ISO20000 包括五个过程域，共十三个管理流程。ISO20000 在 ITIL 基础上新增了业务关系管理、供货商管理和服务报告，实际上已经包含在 ITIL 中。