# 上海翰纬信息管理咨询有限公司

# 翰纬 IT 治理

# 白皮书

SinoServiceONE
上海翰纬信息管理咨询有限公司
地 址：上海市张江高科毕升路 289 弄 8 号 101
电 话：021 3393 2855/2856/2849
传 真：021 3393 2850
邮 编：201 204
电 邮：info@sinoserviceone.com
网 址：www.sinoserviceone.com

## 文档信息

| | | | |
|---|---|---|---|
| 项目名称： | | 项目编号： | |
| 项目经理： | | 项目阶段： | |
| 文档名称： | | 文档编号： | |
| 文档起草人： | | 起草日期： | |
| 当前版本编号： | | 版本日期： | |
| 相关文档： | | | |

## 分发名单

| 来自 From | 日 期 | 电话/传真/Email |
|---|---|---|
| | | |
| | | |

| 给 To | 行 动* | 截止日期 | 电话/传真/Email |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

*：*行动类别：批准，复审，通知，存档，修改，其它（请指明）*

## 版本记录

| 版本号 | 版本日期 | 修改者 | 说 明 | 文件名 |
|---|---|---|---|---|
| | | | | |
| | | | | |
| | | | | |
| | | | | |



Web: www.sinoserviceone.com Email: Info@sinoserviceone.com

# 目 录





Web: www.sinoserviceone.com Email: Info@sinoserviceone.com

# 上海翰纬信息管理咨询有限公司

# 翰纬 IT 治理白皮书

## 1. 什么是 IT 治理

国际信息系统审计与控制协会 ISACA（Information system Audit and Control Association）成立于 1969 年，最初称为 EDP 审计师联合会，总部设在美国的芝加哥，是一个非盈利组织。目前在世界上 100 多个国家设有 160 多个分会，现有会员两万多人，是全球公认的在 IT 的管理、控制和保证领域的权威。

ISACA 的任务是：通过发展促进对信息、系统、技术的有效管理与控制的研究、实施及标准、权限的制定来支持企业实现其目标。这说明该协会的存在就是为了帮助 IT 的管理控制及保证利益相关者妥善处理 IT 的管理、IT 的风险、IT 的运作过程及协作控制、协作管理、协作风险和协作程序的相互作用。ISACA 通过提供各种有价值的服务（如：研究、标准、信息、教育、认证、专业的远景）实现以上作用。协会帮助从事信息系统审计、控制、安全工作的人员，使之不仅注意 IT、IT 的风险与安全主题而且更要关注 IT 与商业、商业运作及商业风险的关系。其主要工作内容如下：

- 设定标准——一般作为世界范围内的 IT 审计、控制的指导方针。
- 一个令人尊敬的认证项目 CISA ——在 IS 审计、控制、安全领域内国际上承认的认证。
- 一个关于关键的管理和技术主题的专业的发展项目。
- 提供备受赞誉的技术出版物，包含最新的研究、案例学习、信息知识入门等。
- 指导会员专业的活动和操行的职业道德准则。

通过 ISACA 会员共同的努力，ISACA 超越了地理、文化和职业界限，他们代表各种不同的企业团体，包括金融银行协会、会计审核公司、政府公共部门、公共事业及制造业等，通过选举或指定一个由全球的志愿者组成的团体管理这个协会，把他们独特的专业的见解带到协会中并用来作出组织的决定，这就是国际信息系统审计与控制协会的国际委员会。

1999 年下半年，ISACA 成立了 IT 治理研究院，专门研究 IT 治理的概念，并提出 COBIT 模型和最佳实务，帮助企业领导层认识有效实施 IT 治理的必要性与益处，从而保证长期的可持续的成功，并且增强利益相关者的价值。

国际信息系统审计与控制协会（ISACA）定义：IT 治理是一个由关系和过程所构成的体制，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。

可见，IT 治理必须与企业战略目标一致，IT 对于企业非常关键，也是战略规划的组成，影响战略竞争；IT 治理和其它治理主体一样，是管理执行人员和利益相关者的责任；IT 治理保护利益相关者的权益，使风险透明化，指导和控制 IT 投资、机遇、利益、风险；信息技术治理包括管理层、组织结构、过程，以确保 IT 维持和拓展组织战略目标；应该合理利用企业的信息资源，有效地集成与协调；确保 IT 及时按照目标交付，有合适的功能和期望的收益，是一个一致性和价值传递的基本构



Web: www.sinoserviceone.com Email: Info@sinoserviceone.com

建模块，有明确的期望值和衡量手段；引导 IT 战略平衡系统的投资，支持企业，变革企业，或者创建一个信息基础架构，保证业务增长，并在一个新的领域竞争；对于核心 IT 资源做出合理的决策，进入新的市场，驱动竞争策略，创造总的收入增长，改善客户满意度，维系客户关系。

# 2. IT 治理的目标

- 与业务目标一致

IT 治理要从组织目标和信息化战略中抽取信息需求和功能需求，形成总体的 IT 治理框架和系统整体模型，为进一步系统设计和实施奠定基础，保证信息技术跟上持续变化的业务目标。

- 有效利用信息资源

目前信息化工程超期、IT 客户的需求没有满足、IT 平台不支持业务应用等问题较为突出，通过 IT 治理可以对信息资源的管理职责进行有效管理，保证投资的回收，并支持决策。

- 风险管理

由于企业越来越依赖于信息技术和网络，新的风险不断涌现，例如，新出现的技术没有管理，不符合现有法律和规章制度、没有识别对 IT 服务的威胁等。IT 治理强调风险管理，通过制定信息资源的保护级别，强调关键的信息技术资源，有效实施监控，事故处理。IT 治理使企业适应外部环境变化，为企业内部实现对业务流程中资源的有效利用，从而达到改善管理效率和水平的重要手段。

IT 治理的目标将帮助管理层建立以组织战略为导向，以外界环境为依据，以业务与 IT 整合为中心的观念，正确定位 IT 部门在整个组织中的作用。最终能够针对不同业务发展要求，整合信息资源，制定并执行推动组织发展的 IT 战略。

对于最高管理层而言，IT 治理可以解决以下三个方面问题：

- 发现信息技术本身的问题

例如 IT 项目未能实现期望价值的概率；终端用户是否满意 IT 服务的质量；是否有足够的 IT 资源、基础设施、竞争力来满足战略目标；信息技术平均操作失误的原因；IT 没有推动业务改善而是阻碍业务的次数。

- 帮助管理者处理 IT 问题

例如，IT 和组织战略目标的一致性程度怎么样；怎样衡量 IT 的交付价值；执行管理人员采取什么样的战略动机来管理 IT；与企业的运营与成长管理相关的问题；企业是否清楚其商业目标与技术的关系:领先、跟随者还是滞后者；企业对风险（风险规避和风险承担）是否清楚；有没有最新的企业相关 IT 风险的清单，采取哪些行动处理这些风险。

- 自我评估 IT 管理的效果

例如，是否经常向最高管理层定期汇报 IT 风险；IT 是否是最高管理层议程中的一个常用的术语，它是否以结构化形式表达；最高管理层是否就商业目标与信息技术一致性进行阐明和沟通；最高管理层对主要 IT 投资是否有清楚的观点，包括风险和回报；最高管理层是否定期得到主要 IT 过程的报告；最高管理层在获取 IT 目标和限制 IT 风险时是否得到独立的保证。



Web: www.sinoserviceone.com Email: Info@sinoserviceone.com

# 3. IT 治理的范围

IT 治理体系保证总体战略目标能够从上而下贯彻执行。IT 治理和其它治理活动一样，集中在最高管理层（董事会）和执行管理层。然而，由于 IT 治理的复杂性和专业性，治理层必须强烈依赖企业的下层来提供决策和评估活动所需要的信息。为保证有效的 IT 治理，下层应用要和企业总体目标采用相同的原则，提供评估业绩的衡量方法。因此，好的 IT 治理实践需要在企业全部范围内推行。

最高管理层的主要职责是：

- 证实 IT 战略与企业战略一致；
- 证实 IT 通过明确的期望和衡量手段交付；
- 指导 IT 战略、平衡支持企业和使企业成长的投资；
- 恰当决策信息资源应着重使用的地方。

最高管理层通过下述指标衡量业绩:定义和检查衡量手段以及管理，证实目标已经达到，并且衡量业绩，减少不确定性。

管理者的焦点主要是成本-效益比，增加收入，构建竞争力，这些都由信息、知识、信息技术体系推动。由于信息技术作为实现企业目标的一个集成部分，其解决办法越来越复杂（外包，第三方合同，网络化等），因此，善治成为成功的一个关键因素。

管理者的职责是：

- 将 IT 风险管理的责任和控制落实到企业中，制定明确的政策和全面的控制框架；
- 将战略，策略，目标等由上至下落实到企业，并使信息技术的组织与企业目标一致；
- 提供治理结构支持 IT 战略的实施，制定 IT 基础设施加快商业信息的创造与共享；
- 通过衡量公司业绩和竞争优势来测度信息技术的效果（KPI，KGI）；
- 使用平衡计分卡，弥补行政管理的不足；
- 关注 IT 必须支持的商业竞争力，如增加客户价值的业务过程，在市场上差异化的产品和服务，通过多产品和服务来产生增值；
- 关注重要的增值的信息技术过程；
- 关注与规划和管理 IT 资产、风险、工程项目、客户和供应商相关的核心竞争能力。

IT 治理使得最高管理层（董事会）和执行经理的一系列活动成为可能。这些活动主要包括：IT 的目标，新技术的机遇和风险，关键过程与核心竞争力。如指导信息技术的职能和对企业的影响，分配责任，定义操作，衡量业绩，管理风险和获得保证的约束等。

# 4. IT 治理相关工具

## 4.1 COSO ERM 风险管理

2001 年，COSO（Committee ofSponsoring Organization of the Treadway Committee）委托



Web: www.sinoserviceone.com Email: Info@sinoserviceone.com

普华永道设计一种能被企业管理层用来评估和改善企业风险管理的框架。COSO 于 2004 年发布了《企业风险管理———整体框架》（简称 ERM）的报告。COSOERM 企业风险管理框架中，企业的风险管理框架包括四类目标和八要素。四类目标分别是战略目标、经营目标、报告目标和合法性目标，八要素是内部环境、目标制定、事项识别、风险评估、风险反应、控制活动、信息和沟通、监控,是企业实现各类目标的保证，相互之间存在直接的关系。风险管理框架还强调在整个企业范围内实行风险管理，COSOERM 的管理层次比较高，但是目的却在于“能够向一个主体的管理当局和董事会提供合理保证”,出发点和终点都是围绕审计和会计的观点。COSOERM 把风险分为总和风险和单一目标（或事项风险）两个层次，作为总和风险与组织使命相关，是组织使命实现过程中障碍或促进，是一种综合而不确定性。风险管理在于把这种不确定性控制于组织的风险偏好，或者吸收风险（或利用机遇）。作为单一目标和单一事项而言，存在事项识别、应对和控制,风险管理把风险控制在组织的风险容忍度的范围之内。所有事项或目标构成组织的使命，所有事项和目标的风险构成的综合风险，主体风险控制是使综合风险在主体的风险偏好之内。但是综合风险不是总和风险，而是风险的组合。

## 4.2 ITIL

ITIL（Information Technology Infrastructure Library，信息技术基础架构库）是英国中央计算机和电信局 CCTA（现在已并入英国商务部）开发的一套针对 IT 行业的服务管理标准库，是服务管理的最佳实践标准。

自 20 世纪 80 年代中期英国商务部（OGC）发布 ITIL 以来，已于 2007 年 5 月 30 日最新推出第三版。不论是应用相对成熟的 ITIL v2，还是应时推出的 ITIL v3，ITIL 体系架构中服务管理功能都是其核心模块，是 ITIL 与其它 IT 管理方法最不同的地方，即以一系列典型流程的方式把大部分 IT 管理内容进行合理划分和管理。

ITIL 为企业的 IT 服务管理实践提供了客观、严谨、可量化的标准和规范，企业的 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不同服务水平，参考 ITIL 来规划和制定其 IT 基础架构及服务管理，从而确保 IT 服务管理能为企业的业务运作提供更好的支持。ITIL 是基于流程的方法论，这些流程方法可用于检查是否用一种可控的和可训练有素的方法为最终用户交付所需的 IT 服务。ITIL 合并了一套最佳的实践惯例，可适用于几乎所有 IT 组织，无论其规模大小或采取何种技术。ITIL 已经成为 IT 行业服务管理的理论基础，在全球 IT 服务管理领域得到了广泛的认同和支持。

## 4.3 COBIT

COBIT 美国信息系统审计与控制协会（ISACA）从 1967 年成立时起,就开始研究信息技术的安全控制问题，提出了信息及相关技术的控制目标（COBIT）。该标准为 IT 的治理、安全与控制提供了一般适用的公认标准,以辅助管理层进行 IT 治理。该标准体系已在世界多个国家的重要组织与企业中运用，指导这些组织有效利用信息资源，有效地管理与信息相关的风险。COBIT 是 COSOERM



Web: www.sinoserviceone.com Email: Info@sinoserviceone.com

的补充，目的是使 COSOERM 具有可操作性，提供一种可用于管理的有逻辑性的结构。COBIT 架构由 34 个高层控制目标和 318 个细节控制目标组成,并归集为四个控制域：IT 规划和组织、系统获得和实施、交付与支持以及信息系统运行性能监控。

COBIT 的目标是建立 IT 与经营目标之间的连接，使 IT 与企业的经营目标一致。通过定义这些目标可以帮助维护企业业务对 IT 的有效控制。COBIT 使 IT 与企业经营一致，即经营目标为 IT 目标。其原理在于企业经营有需求，这种需求要依靠 IT 资源通过 IT 流程来实现。为了实现这一目标，COBIT 制定了相应的信息标准：效果、效率、保密、完整、实用、合规和可靠。用信息支持企业经营目标的制定，是经营目标制定需求的一种信息标准。IT 战略是企业经营战略的组成部分，服务并且服从于企业的经营战略，IT 目标介于企业战略目标和企业 IT 基础之间。COBIT 的作用在于，使 IT 活动成为一种一般化的过程模型，IT 风险能够常规化管理；识别主要 IT 资源的作用和功能，最大化实现 IT 的价值；定义管理控制的目标，风险有效控制，IT 能够正常和正确被使用。COBIT 应用成熟度模型,使 IT 能力改善得以度量；用平衡记分卡衡量 IT 流程与企业目标的匹配程度和一致性程度。从内容上看，COBIT 覆盖了从分析和设计到开发和实施到运营、维护的整个过程。需要指出的是，COBIT 可具体应用到几乎所有企业信息系统中。目前，ISACA 也提供相关专业人士的认证服务，经认证的专家可在一百多个国家执行信息系统审计业务。

## 4.4 Sysperanto

Steven Alter 通过对信息技术著名期刊 MISQ、ISR 和 JMIS1 等文献进行了分析研究，发现关于信息系统研究领域和核心概念非常零散，不利于基本概念的基础的形成和 IT 职业人员的应用。从 1992 起，开始对信息系统的概念进行了本体论（Ontology）研究，Steven Alter 命名其研究为 Sysperanto2，研究类似于应用于信息系统的 Esperanto（世界语）。目的在于用商务术语解释和理解信息系统，而不是用 IT 专家的解释和说明。一方面为了实践人员对信息系统的沟通，另一方面有利于研究人员在理论界统一概念。首先，Steven Alter 提出工作系统（Work system）的概念。无论 IT 在组织内应用如何，必须先假设组织内的系统应该被视为工作系统。工作系统是（Steven Alter 2003 p367）：“人和/或机器参与的利用信息、技术和其他资源厉行工作，生产产品或提供服务给组织内部或外部客户的系统。”任何组织都可以被视为一个工作系统，也可以被分解成为工作系统的子系统。S.Alter 工作系统的风险模型，是在工作系统理论模型基础之上的一般化工作系统的风险管理。工作系统权变管理模型描述为：“目标和期望”影响“风险”和“不确定性源”,同时影响系统工作人员和管理者的热情;系统不确定性包括系统内部的生变、灾祸和内部或外部的或然事件。风险管理的目的在于使了解和吸纳不确定性,使其与企业的目标和期望一致或得以满足。不确定性源与工作系统是相互作用和相互影响的。信息系统、项目和任何其他工作系统不会独立存在,而是一直处在影响和被影响。相对于最初的目标和期望而言,后果可能是有利的也可能是不利的。或然事项可能被考虑到也可能被忽略,但当事件发生过后总会对其结果进行评估。对于企业而言,最终归结为财务成果,可能是正的,也可能是负的。S.Alter 关于风险分析和管理基于一种科研文献的统计,试图找到一种在理论上的共识,消除沟通和合作的障碍,并不是给出一种方法或一种具有操作性的框架供用户使用。其理



Web: www.sinoserviceone.com Email: Info@sinoserviceone.com

论还是出于发展研究阶段,有待进一步的工作。

## 4.5 CMM

1993 年，卡耐基梅隆大学为美国国防部开发了一种能力成熟度模型（CMM），目的是为了软件开发管理。该标准基于众多软件专家的实践经验，侧重于软件开发过程的管理及工程能力的提高与评估，是国际上流行的软件生产过程标准和软件企业成熟度等级认证标准。CMM 认证已经成为世界公认的软件产品进入国际市场的通行证。模式是真实世界的简化表示，CMM 不仅是一个模型和工具，更代表了一种管理哲学在软件工业中的应用。其管理思想来源于已有 60 多年历史的产品质量管理，用成熟度衡量企业的流程。组织可以利用 CMM 模式，设定流程改善的目标和优先顺序、改善流程及提供指引，以确保流程的稳定度、能力度及成熟度。CMM 最为重要的概念是流程——在模型方法中可实施的活动的集合。活动可对应流程领域一个或多个执行方法，使得模式有效地对流程改善和评价。CMM 通过管理流程的成熟度已达到组织的能力度管理的目的。CMM 作为软件过程改善的指导框架，用于确定一个组织当前的软件工程过程状态及组织所面临的软件过程的优先改善问题，为组织领导层提供报告以获得组织对软件过程改善的支持。软件过程改善是一个持续的、全员参与的过程。CMM 建立了一组有效地描述成熟软件组织特征的准则。该准则清晰地描述了软件过程的关键元素,并包括软件工程和管理方面的优秀实践。

## 4.6 UML

UML（统一建模语言）是一种面向对象的建模语言，在软件工业化方面做出了杰出的贡献。UML 实质上是一种沟通方法。UML 的目标是以面向对象图的方式来描述任何类型的系统，具有很宽的应用领域。其中最常用的是建立软件系统的模型，但同样可以用于描述非软件领域的系统，如机械系统、企业机构或业务过程，以及处理复杂数据的信息系统、具有实时要求的工业系统或工业过程等。UML 是一个通用的标准建模语言，可以对任何具有静态结构和动态行为的系统进行建模。UML 适用于系统开发过程中从需求规格描述到系统完成后测试的不同阶段。UML 的概念包括了 UML 语义和 UML 表示符两个部分，UML 语义定义了结构模型和行为模型。结构模型（又称为静态模型）强调系统的对象结构，如对象的类、接口、属性和关系；行为模型（动态模型）关注的是系统对象的行为动作，如对象的方法、交互、协作和状态。以此为基础，为 UML 表示符提供了完整的语义定义。UML 的表示符包括了类图、用例图、顺序图、协作图、状态图、活动图、部署图等几种主要的图。标准建模语言 UML 适用于以面向对象技术来描述任何类型的系统，而且适用于系统开发的不同阶段，从需求规格描述直至系统完成后的测试和维护。软件开发方法学相对于风险控制和内部控制是超前的，软件工程学的生命周期方法已经有几十年的历史，但是在需求分析这一环节，至今没有一个成熟的方法，因此人们对 UML 寄予厚望。



Web: www.sinoserviceone.com Email: Info@sinoserviceone.com

## 4.7 六种工具的比较

COSO ERM、ITIL、Sysperanto、COBIT、CMM 及 UML，各自出发点不同，服务对象也不同。但这并不影响其作为工具应用于信息系统风险管理，事实上这些理论框架有着内在的联系，并且必须将其结合起来应用才能真正发挥作用。同时，由于各自出于不同的目的、不同的版本、不同的时间和不同的侧重，因此也存在差异，这些差异也会引发问题和风险。

通过表 4-1 可以了解到，从 COSO ERM 到 UML，每种理论模型都有自己不同的听众、不同的目标、不同的应用领域，也是由不同的理论结构，当然也被不同的团体所采用，并且不同的研发者在不断地完善和更新。共同点是在现代信息技术背景下，对信息化密集型的组织有着深远的影响。我们用图 4-1 表示 COSOERM 等在组织系统中的作用域。

**表 4-1　六种 IT 治理工具的比较**

| 比较项 | COSO ERM | ITIL | Sysperanto | CMM | COBIT | UML |
|---|---|---|---|---|---|---|
| 目标听众 | 管理层、内控人员 | IT 部门和用户 | 学术界 | 软件用户和开发商 | 企业管理层、用户、审计 | 软件开发商 |
| 作用 | 风险管理 | 实施和服务标准 | 信息系统基础理论 | 流程研发支持 | 信息系统 | 系统模型化工具 |
| 目标 | 主体目标的实现提供合理保证 | 标准化服务 | 概念和术语的统一 | 系统改进和完善 | 信息有效、效果、保密、合规、完整等 | 为软件工程服务，有效地开发软件 |
| 组成要素 | 内部环境等 8 要素 | 业务管理等 6 个部分 | 目标和期望，不确定性源，风险管理，后果和可能性，财务结果 | 流程领域，执行方法，工作产品等要素 | 34 个高层控制目标和 318 个细节控制目标组成 | UML 语义和表示符体系 |
| 应用域 | 企业风险控制层 | 信息系统 | 工作系统 | 流程 | IT | 软件 |
| 应用度 | 普遍应用于内部控制和审计 | 普遍用于 IT 服务标准 | 理论研究 | 软件行业用户和开发商 | IT 审计 | 软件开发人员 |
| 操作性 | 弱 | 良 | 弱 | 良 | 良 | 强 |
| 采用度 | 普遍 | 普遍 | 很少 | 普遍 | 普遍 | 普遍 |
| 研发发行 | 普华永道 COSO | CCTA | Steven Alter | Carnegie Mellon Software | ISACA | OMG |



Web: www.sinoserviceone.com Email: Info@sinoserviceone.com

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | Engineering Institute | | |
| 版本 | 2004 | 2.0 | 2005 | CMM V1.1 | COBIT 4.0 | 2.0 |

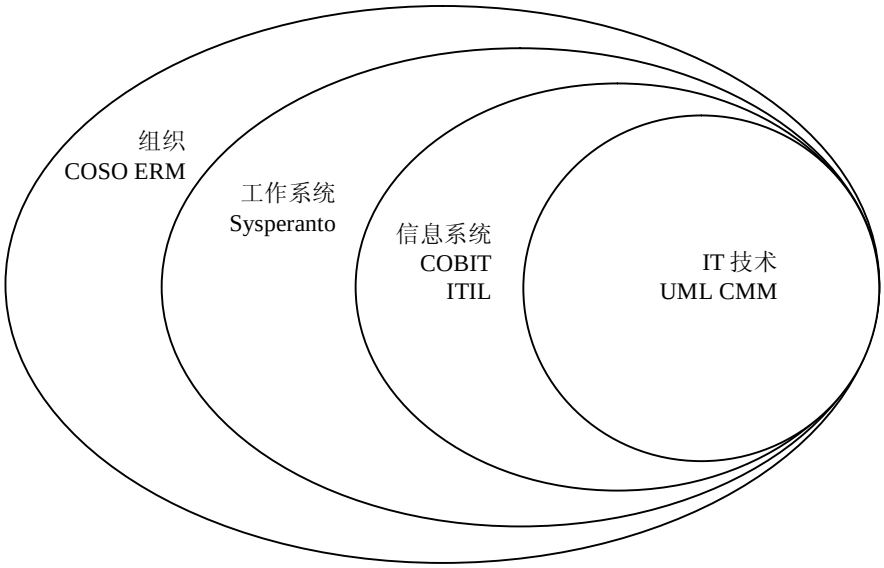



**图 4-1　六种工具不同理论的作用域**

COSO 报告自从问世以来，已经得到企业内部控制普遍采用，尤其是由于普华永道等开发和支持，不论在实践和理论领域都具有普遍的影响，当然企业应用信息技术也不例外。COSOERM 成为企业规避风险的一般性准则，给出了风险控制的管理模型，但是对模型产生的理论并没有提及。从会计或审计的视角看企业的风险管理，COSO ER 由八个要素组成，但是相互之间的关系不是很清晰，很难构造和理解八个要素之间的有机关系。ITIL 为企业的 IT 服务管理实践提供了一个客观、严谨、可量化的标准和规范。组织内的信息系统管理部门和最终用户可以根据自身的能力和需求定义所需的不同服务水平，参照 ITIL 来规划和制定其 IT 基础架构及服务管理。对企业来讲，实施 ITIL 的最大意义在于把 IT 与业务紧密地结合起来了。COBIT 接受并遵循 COSO 内部控制的有关框架内容，COSO 内部控制框架是 COBIT 的目标和基础。COBIT 使 COSO 内部控制框架在 IT 治理领域具有可操作性和逻辑性，COBIT 实现了企业目标与 IT 治理目标之间的桥梁作用。但 COBIT 并不只是用到了 COSO 框架作导引，在 COBIT 中 CMM 被用来作为“基准”，以此衡量 IT 控制和绩效水平是否满足监控，Robert Kaplan 的平衡记分卡作目标分析，应用关键目标指标理论作为导向。COBIT 以企业经营目标实现的合理保证为目标，控制 IT 目标的实现。CMM 不单成为企业软件开发和流程改善的指南，而且成为一种类似于国际 ISO 9000 的一种认证体系。CMM 制定的能力成熟度级别已



Web: www.sinoserviceone.com Email: Info@sinoserviceone.com

经是衡量软件企业水平的标准。CMM 的应用领域远不只是软件行业,其应用领域是流程改善和规范化,范围相当广。规范化和制度化对防范风险意义重大,是最为有效的方式和方法。UML 解决了软件如何获取和开发,即软件系统模型化。由于软件开发方法和软件工程的历史很长,相对于企业范围的其他应用而言,软件开发比较超前。当然会这引发问题,IT 人员和他们的合作者使用不同的沟通工具。Sysperanto 出于学者发现的问题和提出解决问题的方法,但是目前并没有得到发展和推广。

综上所述，COSOERM 各自有自己理论和实践背景，互相很难代替，沟通也有一定困难，这也正是 S.Alter 研究一种通用的理论模型的原因。COSOERM、COBIT、CMM、UML 及 Sysperanto 之间有各自研究和服务的对象，也有其内在的联系。但是由于各自产生的背景不同，在理论和概念上都有区别，这些差别会给用户带来沟通和实施的困难。在这些理论中最重要的概念是“流程”,对于这个概念都有各自的解释。类似于“流程”的概念，还有“环境”、“基础设施”等概念都不同，在某种意义上而言，需要对这些理论进行纵向整合。

# 5. IT 治理与公司治理

## 5.1 公司治理的基本概念

按照经济合作及发展组织（Organisation for Economic Co-operation and Development，简称 OECD）的定义，公司治理是一种据以对工商业公司进行管理和控制的制度体系，它明确规定了公司各参与者的责任和权力分布，诸如董事会、经理层、股东和其他利益相关者，并且清楚说明了决策公司事务时应遵循的规则和程序，同时，它还提供了一种结构，使之用以设置公司目标，也提供了达到这些目标和监控运营的手段。

公司治理是一种对公司管理和运营进行监督和控制的体系。它不仅规定了公的各个参与者，例如董事会、经理层、股东和其他利害相关者的责任和权利分布，而且明确了决策公司事务时所应遵循的规则和程序，既要遵从《公司法》、《证券法》会计准则、工商和和税务规定，又要执行公司的章程、规则、程序和制度。公司理的核心是在所有权和经营权分离的条件下，需要解决好所有者和经营者的利益不一致而产生的委托-代理关系。公司治理的目标是降低代理成本，使所有者不干预公司的日常经营，同时又保证经理层能维护股东的利益，实现公司价值和利益的大化。

虽然公司治理结构没有单一的模式，但从公司发展的实践上看，国际社会认为，比较好的公司治理结构应具备一些共同的要素：

- 问责机制和责任（Accountability & Responsibility）

内容包括明确董事会职责，强化董事的诚信与勤勉义务，确保董事会对经理层的有效监督。建立健全绩效评价与激励约束机制。

- 公平性原则（Fairness）

主要指平等对待所有股东，如果他们的权利受到损害，他们应有机会得到有效补偿。同时，公司治理结构的框架应确认公司利益相关者(债权人、雇员、供应商、客户)的合法权利。

- 透明度原则（Transparency）



Web: www.sinoserviceone.com Email: Info@sinoserviceone.com

一个强有力的信息披露制度是对公司进行市场监督的典型特征，是股东具有行使表决权能力的关键。信息披露也是影响公司行为和保护投资者利益的有力工具。强有力的披露制度有助于公司吸引资金，维持对资本市场的信心。良好的治理结构要求信息披露中采用高质量会计标准一一国际会计准则，提高国家之间信息的可比性。良好的治理结构要求可靠的信息审计，以确保信息披露的真实性和准确性。

## 5.2 IT 治理与公司治理的关系

公司治理主要关注利益相关者权益和管理，包括一系列责任和条例，由最高管理层和执行管理层实施，目的是提供战略方向，保证目标能够实现，风险适当管理，企业的资源合理使用。

公司治理，驱动和调整 IT 治理。同时，IT 治理能够提供关键的输入，形成战略计划的一个重要组成部分，这是 IT 治理影响企业的战略竞争机遇。如图 5-1 所示。

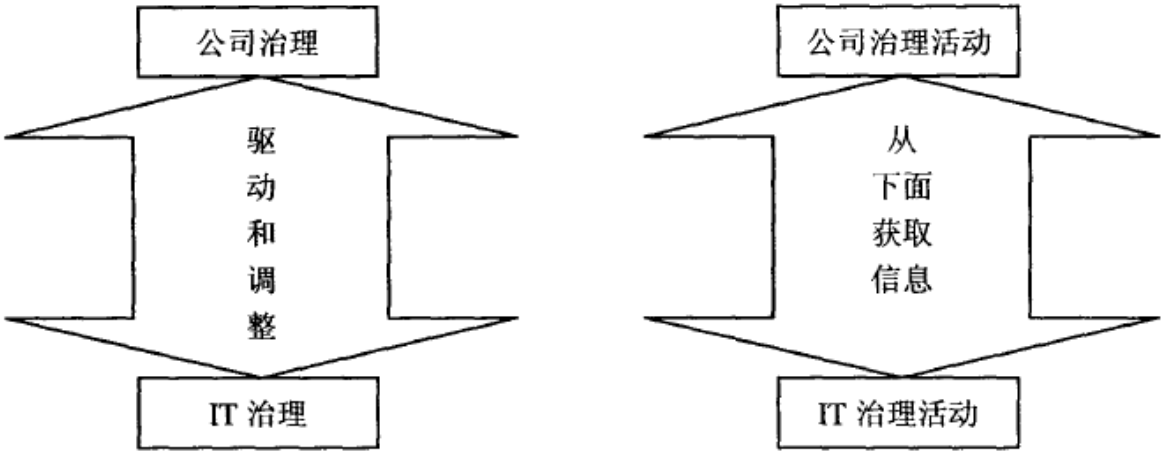
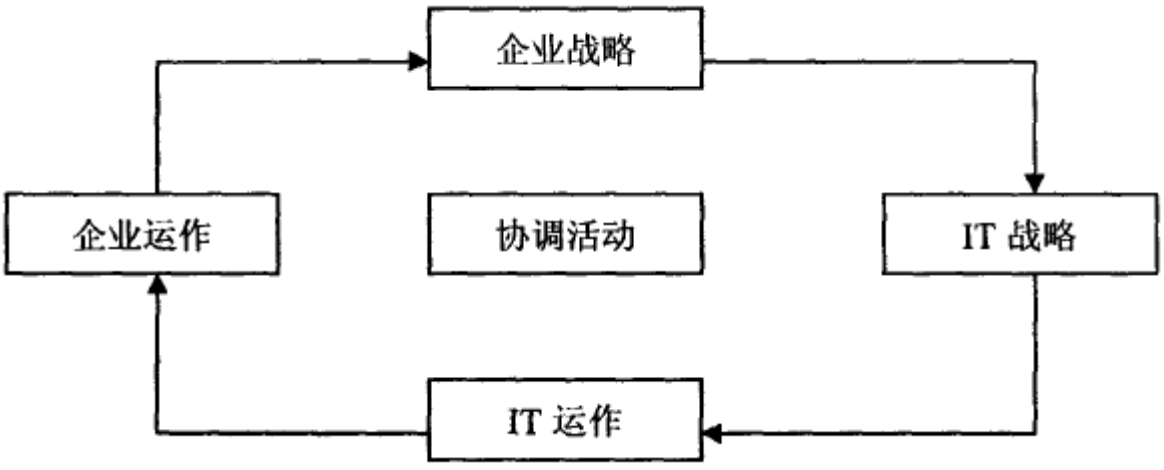



**图 5-1　IT 治理和公司治理关系图**

IT 治理应该体现“以组织战略目标为中心”的思想，通过合理配置 IT 资源创造价值。公司治理侧重于企业整体规划，IT 治理侧重于企业中信息资源的有效利用和管理。

企业目标在于远景和商业模式，IT 目标在于商业模式的实施。如图 5-2 所示。






Web: www.sinoserviceone.com Email: Info@sinoserviceone.com

**图 5-2　企业目标与 IT 目标之间的关系**

IT 治理主要涉及两个方面：一方面 IT 要为企业交付价值，另一方面 IT 风险要降低。前者受 IT 与企业的战略一致性驱动，后者由责任义务落实到企业驱动。这两者都需要衡量，如使用平衡计分卡。这就可以看出 IT 治理的四个核心领域，都是由利益相关者价值驱动的，其中两个是成果：价值交付和风险降低，另外两个是驱动力:战略一致性和业绩衡量。

概括地说，公司治理和 IT 治理都是市场他律的机制，是如何“管好管理者”的机制，其目标也是一致的：达到业务永续运营，并增加组织的长期获利机会。无论大环境是好是坏，最高管理层均应以达成其目标为责任，而且管理阶层需有能力协助其达成目标，因此最高管理层必须常常监督管理部门对决策判断与政策实施的绩效。

企业设立目标，由通用的惯例来治理并保证目标实现。这些目标中渗透企业的发展方向，指导企业活动和使用资源。企业活动的结果被衡量及报告，为输入提供不断的修正和维护控制，从而开始下一轮循环。如图 5-3 所示。

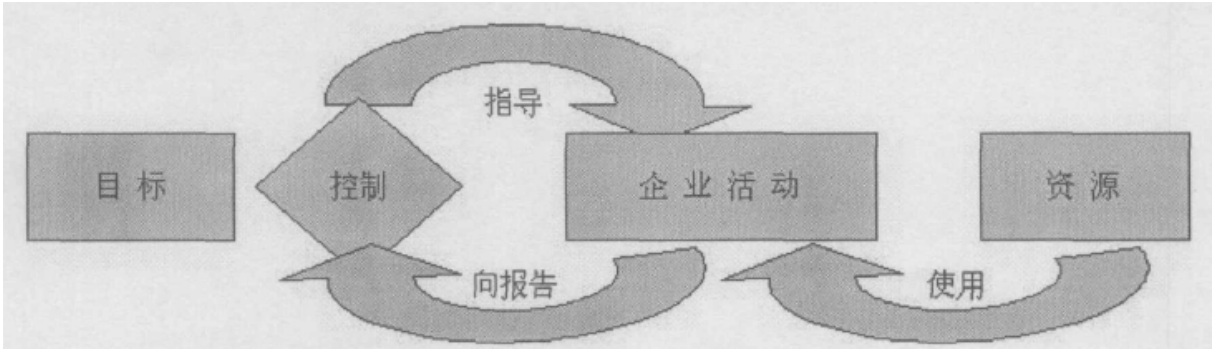



**图 5-3　公司治理与 IT 治理的循环**

公司治理问题一直是企业制度与组织的核心问题。近年来，因上市公司频频“惊曝黑幕”，“公司治理”成为全球性的问题。从美国的安然、世通舞弊案件，到我国出现的蓝田股份和银广夏的利润神话破灭事件，特别是 2002 年夏天美国颁布的萨班斯法案更是加强了对公司治理的要求，要求上市公司公告其内部控制制度体系，公司治理正在成为企业议事日程中最重要和最迫切的任务。但是目前企业内外环境都发生击打变化。网络在日常生活中普及化，企业管理信息化，信息技术与信息系统对企业组织形态、治理结构、管理体制、运作流程和商业模式的影响日益深化，原有的治理控制机制已经不适应，公司治理面临挑战。



Web: www.sinoserviceone.com Email: Info@sinoserviceone.com