

一个重要研究方向。人机混合智能旨在将人的作用或认知模型引入到人工智能系统中，提升人工智能系统的性能，使人工智能成为人类智能的自然延伸和拓展，通过人机协同更加高效地解决复杂问题。

(2) 从“人工+智能”向自主智能系统发展。当前人工智能领域的大量研究集中在深度学习，但是深度学习的局限是需要大量人工干预，比如人工设计深度神经网络模型、人工设定应用场景、人工采集和标注大量训练数据、用户需要人工适配智能系统等，非常费时费力。因此，科研人员开始关注减少人工干预的自主智能方法，提高机器智能对环境的自主学习能力。

(3) 人工智能将加速与其他学科领域交叉渗透。人工智能本身是一门综合性的前沿学科和高度交叉的复合型学科，研究范畴广泛而又异常复杂，其发展需要与计算机科学、数学、认知科学、神经科学和社会科学等学科深度融合。借助于生物学、脑科学、生命科学和心理学等学科的突破，将机理变为可计算的模型，人工智能将与更多学科深入地交叉渗透。

(4) 人工智能产业将蓬勃发展。随着人工智能技术的进一步成熟以及政府和产业界投入的日益增长，人工智能应用的云端化将不断加速，全球人工智能产业规模在未来10年将进入高速增长期。“人工智能+X”的创新模式将随着技术和产业的发展日趋成熟，对生产力和产业结构产生革命性影响，并推动人类进入普惠型智能社会。

(5) 人工智能的社会学将提上议程。为了确保人工智能的健康可持续发展，使其发展成果造福于民，需要从社会学的角度系统全面地研究人工智能对人类社会的影响，制定完善人工智能法律法规，规避可能的风险，旨在“以有利于整个人类的方式促进和发展友好的人工智能”。

2.2.6 虚拟现实

自从计算机创造以来，计算机一直是传统信息处理环境的主体，这与人类认识空间及计算机处理问题的信息空间存在不一致的矛盾，如何把人类的感知能力和认知经历及计算机信息处理环境直接联系起来，是虚拟现实产生的重大背景。如何建立一个能包容图像、声音、化学气味等多种信息源的信息空间，将其与视觉、听觉、嗅觉、口令、手势等人类的生活空间交叉融合，虚拟现实的技术应运而生。

1. 技术基础

虚拟现实（Virtual Reality, VR）是一种可以创立和体验虚拟世界的计算机系统（其中虚拟世界是全体虚拟环境的总称）。通过虚拟现实系统所建立的信息空间，已不再是单纯的数字信息空间，而是一个包容多种信息的多维化的信息空间（Cyberspace），人类的感性认识和理性认识能力都能在这个多维化的信息空间中得到充分的发挥。要创立一个能让参与者具有身临其境感，具有完善交互作用能力的虚拟现实系统，在硬件方面，需要高性能的计算机软硬件和各类先进的传感器；在软件方面，主要是需要提供一个能产生虚拟环境的工具集。

虚拟现实技术的主要特征包括沉浸性、交互性、多感知性、构想性（也称想象性）和自主性。随着虚拟现实技术的快速发展，按照其“沉浸性”程度的高低和交互程度的不同，虚拟现实技术已经从桌面虚拟现实系统、沉浸式虚拟现实系统、分布式虚拟现实系统等，向着增强式

虚拟现实系统（Augmented Reality, AR）和元宇宙的方向发展。

2. 关键技术

虚拟现实的关键技术主要涉及人机交互技术、传感器技术、动态环境建模技术和系统集成技术等。

1) 人机交互技术

虚拟现实中的人机交互技术与传统的只有键盘和鼠标的交互模式不同，是一种新型的利用VR眼镜、控制手柄等传感器设备，能让用户真实感受到周围事物存在的一种三维交互技术，将三维交互技术与语音识别、语音输入技术及其他用于监测用户行为动作的设备相结合，形成了目前主流的人机交互手段。

2) 传感器技术

VR技术的进步受制于传感器技术的发展，现有的VR设备存在的缺点与传感器的灵敏程度有很大的关系。例如VR头显（即VR眼镜）设备过重、分辨率低、刷新频率慢等，容易造成视觉疲劳；数据手套等设备也都有延迟长、使用灵敏度不够的缺陷，所以传感器技术是VR技术更好地实现人机交互的关键。

3) 动态环境建模技术

虚拟环境的设计是VR技术的重要内容，该技术是利用三维数据建立虚拟环境模型。目前常用的虚拟环境建模工具为计算机辅助设计（Computer Aided Design, CAD），操作者可以通过CAD技术获取所需数据，并通过得到的数据建立满足实际需要的虚拟环境模型。除了通过CAD技术获取三维数据，多数情况下还可以利用视觉建模技术，两者相结合可以更有效地获取数据。

4) 系统集成技术

VR系统中的集成技术包括信息同步、数据转换、模型标定、识别和合成等技术，由于VR系统中储存着许多的语音输入信息、感知信息以及数据模型，因此VR系统中的集成技术显得越发重要。

3. 应用和发展

(1) 硬件性能优化迭代加快。轻薄化、超清化加速了虚拟现实终端市场的迅速扩大，开启了虚拟现实产业爆发增长的新空间，虚拟现实设备的显示分辨率、帧率、自由度、延时、交互性能、重量、眩晕感等性能指标日趋优化，用户体验感不断提升。

(2) 网络技术的发展有效助力其应用化的程度。泛在网络通信和高速的网络速度，有效提升了虚拟现实技术在应用端的体验。借助于终端轻型化和移动化5G技术，高峰值速率、毫秒级的传输时延和千亿级的连接能力，降低了对虚拟现实终端侧的要求。

(3) 虚拟现实产业要素加速融通。技术、人才多维并举，虚拟现实产业核心技术不断取得突破，已形成较为完整的虚拟现实产业链条。虚拟现实产业呈现出从创新应用到常态应用的产业趋势，在舞台艺术、体育智慧观赛、新文化弘扬、教育、医疗等领域普遍应用。“虚拟现实+商贸会展”成为后疫情时代的未来新常态，“虚拟现实+工业生产”是组织数字化转型的新动

能，“虚拟现实+智慧生活”大大提升了未来智能化的生活体验，“虚拟现实+文娱休闲”成为新型信息消费模式的新载体等。

(4) 元宇宙等新兴概念为虚拟现实技术带来了“沉浸和叠加”“激进和渐进”“开放和封闭”等新的商业理念，大大提升了其应用价值和社会价值，将逐渐改变人们所习惯的现实世界物理规则，以全新方式激发产业技术创新，以新模式、新业态等方式带动相关产业跃迁升级。

2.3 本章练习

1. 选择题

(1) 关于信息技术的描述，不正确的是_____。

- A. 信息技术是研究如何获取信息、处理信息、传输信息和使用信息的技术
- B. 信息技术是信息系统的前提和基础，信息系统是信息技术的应用和体现
- C. 信息、信息化以及信息系统都是信息技术发展不可或缺的部分
- D. 信息技术是在信息科学的基本原理和方法下的关于一切信息的产生、信息的传输、信息的转化应用技术的总称

参考答案: D

(2) _____关键技术主要涉及传感器技术、传感网和应用系统架构等。

- A. 物联网
- B. 云计算
- C. 大数据
- D. 人工智能

参考答案: A

(3) _____关键技术主要涉及机器学习、自然语言处理、专家系统等技术。

- A. 物联网
- B. 云计算
- C. 大数据
- D. 人工智能

参考答案: D

(4) 关于云计算的描述，不正确的是_____。

- A. 云计算可以通过宽带网络连接，用户需要通过宽带网络接入“云”中并获得有关的服务，“云”内节点之间也通过内部的高速网络相连
- B. 云计算可以快速、按需、弹性服务，用户可以按照实际需求迅速获取或释放资源，并可以根据需求对资源进行动态扩展
- C. 按照云计算服务提供的资源层次，可以分为基础设施即服务和平台即服务两种服务类型
- D. 云计算是一种基于并高度依赖 Internet，用户与实际服务提供的计算资源相分离，集合了大量计算设备和资源，并向用户屏蔽底层差异的分布式处理架构

参考答案: C

(5) 区块链有以下几种特性：多中心化、多方维护、时序数据、智能合约、开放共识、安全可信和_____。

- A. 可回溯性
- B. 不可篡改
- C. 周期性
- D. 稳定性

参考答案: B

(6) 虚拟现实技术的主要特征包括：沉浸性、交互性、多感知性、构想性和_____。

- A. 自主性
- B. 抗否认性
- C. 可审计性
- D. 可靠性

参考答案：A

2. 思考题

(1) 请概述云计算的主要服务模式有哪些。

参考答案：略

(2) 请简述大数据的技术架构是什么。

参考答案：略

(3) 请简述区块链的共识机制。

参考答案：略

第3章 信息系统治理

信息系统治理（IT治理）是组织开展信息技术及其应用活动的重要管控手段，也是组织治理的重要组成部分，尤其在以数字化发展为重要关注点的新时代，组织的数字化转型和组织建设过程中，IT治理起到重要的统筹、评估、指导和监督作用。信息技术审计（IT审计）作为与IT治理配套的组织管控手段，是IT治理不可或缺的评估和监督工具，重点承担着组织信息系统发展的合规性检测以及信息技术风险的管控等职能。

3.1 IT治理

新时代的信息技术与各领域发展进入到了深度融合的发展新阶段，成为各类组织实现治理体系与能力现代化，构建敏捷运行管理体系，打造高质量的生产与服务系统，洞察社会与市场变化等高质量发展的必要过程。组织如何从其信息系统投资中获得真正的价值；如何将信息技术战略与组织战略相融合；如何从组织治理的高度，对组织数字化能力做出制度安排；如何从战略投资、组织管理变革的角度，降低IT的风险；如何利用国内外信息技术开发利用的最佳实践和重要成果，加快组织的信息化、数字化工作推进等。这些都是IT治理所关注的问题。

3.1.1 IT治理基础

IT治理是描述组织采用有效的机制对信息技术和数据资源开发利用，平衡信息化发展和数字化转型过程中的风险，确保实现组织的战略目标的过程。

1. IT治理的驱动因素

组织信息系统建设和运行需要制订总体规划，但制订IT资源统一规划存在很多问题：①信息系统应用已有相当的基础，但多年来分散开发或引进的信息系统，形成了许多“信息孤岛”，缺乏共享的、网络化的信息资源，系统集成难题一直无法解决；②信息资源整合目标空泛，没有整合“信息孤岛”的措施，数据中心建设和数据集中管理等规划缺乏可操作性，尤其是缺少数据标准化建设方面的建设规划。这些问题的出现，表明组织在IT资源方面没有做到有效统一规划，如何解决这些问题成为了组织发展的一个重要课题。

IT资产作为组织资产的重要组成部分，IT治理自然就是组织治理结构中不可分割的一部分。IT治理是指组织在开发利用信息技术过程中，为鼓励组织所期望的组织行为而明确决策权归属和责任担当的框架，其目标是通过IT治理的决策权和责任影响组织所期望的组织行为。随着新时代的发展，数字特征成为组织发展的一项关键特征，组织的高质量发展对IT的依赖越来越强，IT治理对组织愈发重要，为确保IT治理的有效，组织高层管理者需要投入越来越多的时间和精力。

随着组织在IT方面的投资越来越大，组织的IT战略要与组织战略相一致，才能确保组织核心竞争力的建设与保持；要尽可能地保持开放性和长远性，以确保系统的稳定性和延续性；

要认真分析组织的战略与 IT 支撑之间的影响度，并合理预测环境变化可能给组织战略带来的偏移，在规划时留有适当的余地。组织目标变化太快，很难保证 IT 与组织目标始终保持一致，因此需要多方面的协调，保证 IT 治理继续沿着正确的方向走，这也是 IT 投资者真正关心的问题。IT 治理要从组织目标和数字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，保证信息技术开发应用符合持续变化的业务目标。

高质量的 IT 治理能够使组织的 IT 管理和应用决策与组织期望的行为和业务目标相一致，这就需要组织 IT 治理机构对组织 IT 发展进行科学规划并确保其有效实施。驱动组织开展高质量 IT 治理因素包括：①良好的 IT 治理能够确保组织 IT 投资有效性；②IT 属于知识高度密集型领域，其价值发挥的弹性较大；③IT 已经融入组织管理、运行、生产和交付等各领域中，成为各领域高质量发展的重要基础；④信息技术的发展演进以及新兴信息技术的引入，可为组织提供大量新的发展空间和业务机会等；⑤IT 治理能够推动组织充分理解 IT 价值，从而促进 IT 价值挖掘和融合利用；⑥IT 价值不仅仅取决于好的技术，也需要良好的价值管理，场景化的业务融合应用；⑦高级管理层的管理幅度有限，无法深入到 IT 每项管理当中，需要采用明确责权利和清晰管理去确保 IT 价值；⑧成熟度较高的组织以不同的方式治理 IT，获得了领域或行业领先的业务发展效果。

IT 治理的内涵主要体现在 5 个方面：①IT 治理作为组织上层管理的一个有机组成部分，由组织治理层或高级管理层负责，从组织全局的高度上对组织信息化与数字化转型做出制度安排，体现了治理层和最高管理层对信息相关活动的关注；②IT 治理强调数字目标与组织战略目标保持一致，通过对 IT 的综合开发利用，为组织战略规划提供技术或控制方面的支持，以保证相关建设能够真正落实并贯彻组织业务战略和目标；③IT 治理保护利益相关者的权益，对风险进行有效管理，合理利用 IT 资源，平衡成本和收益，确保信息系统应用有效、及时地满足需求，并获得期望的收益，增强组织的核心竞争力；④IT 治理是一种制度和机制，主要涉及管理和制衡信息系统与业务战略匹配、信息系统建设投资、信息系统安全和信息系统绩效评价等方面的内容；⑤IT 治理的组成部分包括管理层、组织结构、制度、流程、人员、技术等多个方面，共同构建完善的 IT 治理架构，达到数字战略和支持组织的目标。

2. IT 治理的目标价值

组织治理驱动和调整 IT 治理。同时，IT 治理能够提供关键的输入，成为战略计划的一个重要组成部分，是组织治理的一个重要功能。IT 治理将帮助组织建立以组织战略为导向、以实现 IT 与业务匹配为重心、以价值交付为成果、以绩效管理为控制手段的 IT 管理体制，正确定位 IT 团队在整个组织的作用，最终能够针对不同业务发展要求，统一规划 IT 资源、整合信息资源、有效规避风险、制定并执行组织发展战略。IT 治理就是要明确有关 IT 决策权的归属机制和有关 IT 责任的承担机制，以鼓励 IT 应用的期望行为的产生，以联接战略目标、业务目标和 IT 目标，从而使组织从 IT 中获得最大的价值。组织实施 IT 治理的使命通常包括：保持 IT 与业务目标一致，推动业务发展，促使收益最大化，合理利用 IT 资源，恰当理清与 IT 相关的风险等。

IT 治理主要目标包括：与业务目标一致、有效利用信息与数据资源、风险管理。

(1) 与业务目标一致。IT 治理要从组织目标和数字战略中抽取信息与数据需求和功能需求，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，保证信息技术开

发利用跟上持续变化的业务目标。

(2) 有效利用信息与数据资源。目前信息系统工程超期、IT客户的需求没有满足、IT平台不支持业务应用、数据开发利用效能与价值不高、信息技术与业务发展融合深度不够等问题突出，通过IT治理对信息与数据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。

(3) 风险管理。由于组织越来越依赖于信息网络、信息系统和数据资源等，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治理重视风险管理，通过制定信息与数据资源的保护级别，强调对关键的信息与数据资源，实施有效监控和事件处理。

3. IT 治理的管理层次

IT治理要保证总体战略目标能够从上而下贯彻执行，治理层主要集中在最高管理层（如董事会）和管理执行层。然而，由于IT治理的复杂性和专业性，治理层必须依赖组织的基层来提供决策和评估所需要的信息。基层依据组织总体目标采用相关的原则，提供评估业绩的衡量方法。因此，好的IT治理实践需要在组织全部范围内推行。管理层次大致可分为三层：最高管理层、执行管理层、业务与服务执行层。

最高管理层的主要职责包括：证实IT战略与业务战略是否一致；证实通过明确的期望和衡量手段交付IT价值；指导IT战略、平衡支持组织当前和未来发展的投资；指导信息和数据资源的分配。执行管理层的主要职责包括：制定IT的目标；分析新技术的机遇和风险；建设关键过程与核心竞争力；分配责任、定义规程、衡量业绩；管理风险和获得可靠保证等。业务及服务执行层的主要职责包括：信息和数据服务的提供和支持；IT基础设施的建设和维护；IT需求的提出和响应。

3.1.2 IT治理体系

IT治理用于描述组织在信息化建设和数字化转型过程中是否采用有效的机制使得信息技术开发利用能够完成组织赋予它的使命。IT治理的核心是关注IT定位和信息化建设与数字化转型的责权利划分，如图3-1所示。IT治理体系的具体构成包括IT定位：IT应用的期望行为与业务目标一致；IT治理架构：业务和IT在治理委员会中的构成、组织IT与各分支机构的IT权责边界等；IT治理内容：投资、风险、绩效、标准和规范等；IT治理流程：统筹、评估、指导、监督；IT治理效果（内外评价）等。

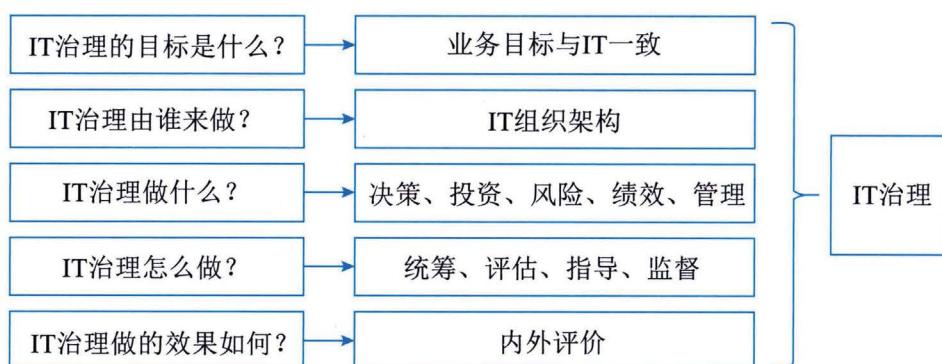


图3-1 IT治理体系的构成

1. IT 治理关键决策

有效的 IT 治理必须关注五项关键决策，如图 3-2 所示，包括 IT 原则、IT 架构、IT 基础设施、业务应用需求、IT 投资和优先顺序。IT 原则驱动着 IT 整体架构的形成，而 IT 整体架构又决定了基础设施，这种基础设施所确定的能力又决定着基于业务需求应用的构建，最后，IT 投资和优先顺序必须为 IT 原则、整体架构、基础设施和应用需求所驱动。然而，这些决策中又有独特问题，即 IT 治理需要确定每个决策由谁来负责输入，以及由谁来负责做出决策。

IT 原则的决策		组织高层关于如何使用 IT 的陈述
IT 架构的决策	业务应用需求决策	IT 投资和优先顺序决策
组织从一系列政策、关系以及技术选择中捕获的数据、应用和基础设施的逻辑，以达到预期和商业、技术的标准化和一体化	为购买或内部开发 IT 应用确定业务需求 IT 基础设施决策 集中协调、共享 IT 服务可以给组织的 IT 能力提供基础	关于应该在 IT 的哪些方面投资以及投资多少的决策，包括项目的审批和论证技术

图 3-2 关键的 IT 治理决策

IT 决策过程中，需要关注各类关键问题，如图表 3-1 所示。

表 3-1 IT 决策的关键问题

关键决策	关键问题
IT 原则	组织的运行模型是什么？IT 在业务中的角色是什么？IT 期望行为是什么？如何投资 IT
IT 架构	组织的核心业务流程是什么？它们之间有什么样的关系？哪些信息在驱动着这些核心流程？数据必须如何整合？哪些技术性能应当在组织范围内得到标准化，以支持 IT 效率，方便流程标准化和整合？哪些行为应当在组织范围内标准化以支持数据整合？哪些技术选择能够指引组织 IT 新计划的方法
IT 基础设施	哪些基础设施对实现组织的战略目标来说是最关键的？对于每个能力集，哪些基础设施服务应该在组织级实现，这些服务的水平需求是什么？应当如何定价基础设施服务？如何保持基础技术的不断更新？哪些基础设施服务应当外包
业务应用需求	新业务应用的市场和业务流程机会是什么？如何设计实验以评估业务应用成功与否？如何在架构标准上满足业务需求？应当在什么时候将一个业务需求从例外转换为标准？谁拥有每个项目的成果并且发起组织变革以确保其价值
IT 投资和优先顺序	哪些流程变革或者强化对组织来说在战略上是最为重要的？当前的以及在提议中的 IT 投资组合是如何分配的？这些投资组合同组织的战略目标一致吗？组织级的投资相对于业务单位的投资哪个更重要？实际投资情况会影响它们的相对重要性吗

2. IT 治理体系框架

IT 治理体系框架是实现组织 IT 治理的有效保障，缺乏良好的 IT 治理体系框架，IT 治理的过程将会变得盲目和无序。IT 治理体系框架以组织的战略目标为导向，架起了组织战略与 IT 的

桥梁，实现了 IT 风险的全面管理以及 IT 资源的合理利用。IT 治理体系框架具体包括：IT 战略目标、IT 治理组织、IT 治理机制、IT 治理域、IT 治理标准和 IT 绩效目标等部分，形成一整套 IT 治理运行闭环，如图 3-3 所示。

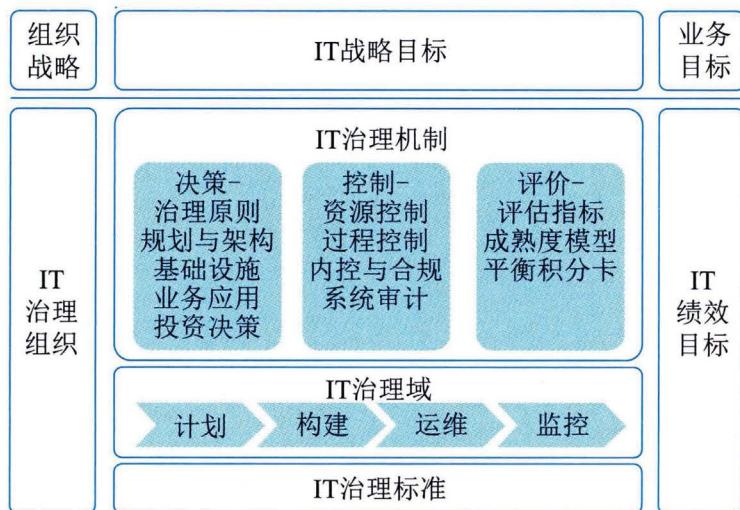


图 3-3 IT 治理体系框架

(1) IT 战略目标。IT 战略目标是指为实现 IT 价值和目标，使组织从 IT 投入中获得最大收益，而针对 IT 与业务关系、IT 决策、IT 资源利用、IT 风险控制等方面制定的目标。

(2) IT 治理组织。IT 治理组织是界定组织中各相关主体在各自方面的治理范围、责权利及其相互关系的准则，它的核心是治理机构（如 IT 治理委员会等）的设置和权限的划分。各治理机构职权的分配以及各机构间的相互协调，它的强弱直接影响到治理的效率和效能，对 IT 治理效率起着决定性的作用。

(3) IT 治理机制。IT 治理机制是 IT 治理决策机制、执行机制、风险控制机制、协调机制的综合体，各机制之间是相辅相成、相互促进的关系。有效的决策机制能保障 IT 决策与组织的业绩目标和战略目标相匹配；有效的执行机制能保证 IT 治理的良好运作，有效的风险控制机制能降低 IT 活动的风险，实现信息技术开发利用的价值效益；有效的协调机制能有力地发挥 IT 治理的协调效应。

(4) IT 治理域。IT 治理域是在 IT 治理的规则之下，对组织的 IT 资源进行整合与配置，根据 IT 目标所采取的行动。以科学、规范的做法交付面向业务的高质量 IT 服务，确保信息化“高效做事情”、数字化“敏捷的决策”。IT 治理域内容包括 IT 信息系统的计划、构建、运维与监控等。

(5) IT 治理标准。IT 治理标准包括 IT 治理基本规范、IT 治理实施参照、IT 治理评价体系和 IT 治理审计方法等方面，作为组织实施 IT 治理最佳实践和对标依据。

(6) IT 绩效目标。IT 绩效目标关注 IT 价值的实现，评价 IT 规划与 IT 构建过程中是否满足业务需求以及构建过程中的工期、成本、质量是否达到目标。

3. IT 治理核心内容

IT 治理本质上关心：①实现 IT 的业务价值；②IT 风险的规避。前者是通过 IT 与业务战略

匹配来实现的，后者通过在组织内部建立相关职责来实现。两者都需要相关资源的支持，并对其绩效进行有效度量。IT 治理的核心内容包括六个方面：组织职责、战略匹配、资源管理、价值交付、风险管理、绩效管理，如图 3-4 所示。

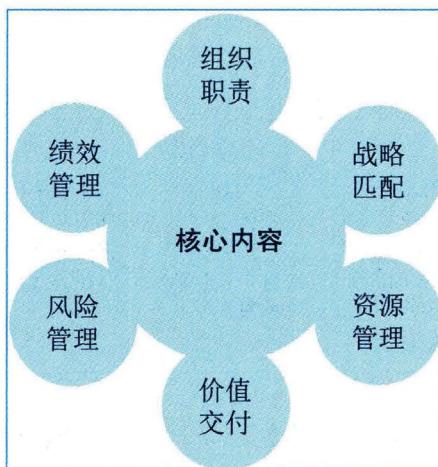


图 3-4 IT 治理核心内容

(1) 组织职责。组织职责指组织参与 IT 决策与管理的所有人员的集合，明确组织信息部门和业务部门之间的关系和责任，正确划分信息系统的所有者、建设者、管理者和监控者。

(2) 战略匹配。IT 治理的一个重要内容，是使组织的 IT 建设与组织战略相匹配，也就是通常所说的“战略匹配”。而战略匹配是 IT 为组织贡献业务价值的重要驱动力。

(3) 资源管理。资源管理的主要功能是确保用户对组织的应用系统和基础设施都有良好的理解和应用，优化 IT 投资、IT 资源（人、应用系统、信息、基础设施）的分配，做好人员的培训、发展计划，以满足组织的业务需求。

(4) 价值交付。通过对 IT 项目全生命周期的管理，确保 IT 能够按照组织战略实现预期的业务价值。重点是对整个交付周期成本的控制和 IT 业务价值的实现，使 IT 项目能够在预算时间、成本范围内，按预定的质量要求完成。价值交付即是创造业务价值。

(5) 风险管理。风险管理是 IT 治理中非常重要的内容。风险管理是确保 IT 资产的安全和灾难的恢复、组织信息资源的安全以及人员的隐私安全。风险管理即是保护业务价值。

(6) 绩效管理。没有绩效管理 IT 治理中任何一个域都不可能有效地进行管理。绩效管理主要是追踪和监视 IT 战略、IT 项目的实施、信息资源的使用、IT 服务的提供以及业务流程的绩效。绩效管理所采用的工具，如平衡积分卡，可以将组织的战略目标转化成各个职能部门或团队具体的业务活动的目标，从而保证组织战略目标的实现。

4. IT 治理机制经验

建立 IT 治理机制的原则包括：①简单。机制应该明确地定义特定个人和团体所承担的责任和目标。②透明。有效的机制依赖于正式的程序。对于那些被治理决策所影响或是想要挑战治理决策的人来说，机制如何工作是需要非常清晰的。③适合。机制鼓励那些处于最佳位置的个人去制定特定的决策。

影响力高且具有挑战性的 IT 治理机制，如表 3-2 所示。

表 3-2 影响力高且具有挑战性的 IT 治理机制

机制	目标	期望行为	不期望行为
执行层和高级管理委员会	对业务包括 IT 的整体观念	整合 IT 的无缝管理	IT 被忽略
架构委员会	明确战略技术和标准是否被执行	业务驱动的 IT 决策制定	IT 限制和延迟
有 IT 人员参与的流程团队	有效地运用 IT 视角	端对端的流程管理	功能性技能的停滞和分散的 IT 基础设施
资金投资批准和预算	把 IT 看作另一种业务投资	对于不同投资类型的不同方法	分析瘫痪小项目，避开了正式批准
服务水平协议	对于 IT 服务的详细说明和衡量	专业的供应和需求	管理服务水平协议而不是业务需求
费用分摊机制	从业务中补偿 IT 成本	IT 的可靠应用	关于收费和歪曲的需求的争论
IT 业务价值的正式追踪	衡量 IT 投资，并通常运用平衡记分卡计算其对业务价值的贡献	使目标、利益和成本透明化	将 IT 同其他资产相分离，只关注资金流，而不关注价值

IT 治理可以从众多最佳实践中学习的经验主要包括：

- IT 指导委员会要吸纳有才干的业务经理，使之负责组织范围的 IT 治理决策，并在 IT 原则中加入严格的成本控制；
- 谨慎管理组织的 IT 架构和业务架构，以降低业务成本；
- 设计严格的架构例外处理流程，使昂贵的例外最小化，并可以从中不断学习；
- 建立集中化的 IT 团队，用以管理基础设施、架构和共享服务；
- 应用连接 IT 投资和业务需求的流程，既可以增加透明度，又可以权衡中心和各运营部门或团队的需求；
- 设计需要对 IT 投资进行集中协作和核准的 IT 投资流程；
- 设计简单的费用分摊和服务水平协议机制，以明确分配 IT 开支等。

3.1.3 IT 治理任务

组织的 IT 治理活动定义为统筹、指导、监督和改进。统筹现在和未来的 IT 战略和组织规划、管理和绩效的实施计划、策略；指导 IT 管理实施、绩效考评、风险控制和业务合规；监督 IT 与业务的一致性、符合性及 IT 应用的合规性；改进 IT 战略规划、组织策略、信息系统全生命周期管控和数据治理。组织开展 IT 治理活动的主要任务聚焦在如下五个方面。

(1) 全局统筹。统筹规划 IT 治理的目标范围、技术环境、发展趋势和人员责权利。组织需要适应当前信息环境和未来发展趋势，保证利益相关者理解和接受 IT 的战略、目标和发展方向。组织需要把 IT 治理作为组织治理的组成部分，建立 IT 治理机构，并明确组织负责人对 IT 治理工作负责。组织还需要关注 IT 发展的规划、实施、检查和改进全过程，重点包括①制订满足可持续发展的 IT 蓝图；②实施科学决策、集约管理的策略，实现横向的业务集成和纵向的业

务管控；通过内外部的监督，确保 IT 与业务的一致性和适用性；③建立适应内外部信息环境变化的持续改进和创新机制。

（2）价值导向。价值导向包括基于实现有效收益，确保预期收益清晰理解，明确实现收益的问责机制。组织需要建立 IT 投资的价值框架，确保在可承担成本和可接受风险水平的基础上，实现 IT 的战略目标。确保 IT 治理符合组织治理的价值导向，明确战略投资方向，以及由投资产生的 IT 服务、资产和其他资源。组织需要建立价值递送规则，确保利益相关者明确相应的权利和义务，包括：①认可信息技术、信息系统和数据在组织中的价值；②识别投资目录，并以相应的方式进行评估和管理；③对关键指标进行设定和监督，并对变化和偏差做出及时回应；④权衡实施成本与预期效益，并随组织内外部环境的变化及时调整。

（3）机制保障。机制保障是指组织应对自身 IT 发展进行有效管控，保证 IT 需求与实现的协调发展，并使 IT 安全和风险得到有效的识别、管理、防范和处置。组织需要建立适合组织特点的机制保障方法，满足疏漏互补、协同发展、监督改进和安全风险可控的原则，避免扭曲决策目标方向。组织需要明确管理责任，明晰上下左右权利关系，落实责任制和各项措施。组织可以根据相关法律法规、行业管理和上级监管机构发布的规范文件要求，制定本组织的信息技术治理制度并实施，重点聚焦在：①指导建立规范过程管理和痕迹管理，并向利益相关者公开质量设定举措；②评审 IT 管理体系的适宜性、充分性和有效性；③审计 IT 完整性、有效性和合规性；④监督由审计和管理评审，提出改进内容的实施。

（4）创新发展。创新发展是指利用 IT 创新开拓业务领域，提升管理水平，改进质量、绩效和降低成本，确保实现战略目标的灵活性和对环境变化的适应性。组织需要通过建立围绕知识资产的创新体系，支撑组织的技术进步、管理提升和业务模式变革。组织可以持续保持管理团队的创造技能，并指导培养各级成员的发问、观察、交际和实验能力。组织可以建立支持创新的人员、技术、制度、资金、风险、文化和市场需求的机制体系，包括：①创造基于业务团队与 IT 团队的深度沟通以及对内外部环境感知和学习的技术创新环境；②确保技术发展、管理创新、模式革新的协调联动；③对组织创新能力进行评估，并对关键创新要素进行分析和评价；④通过促进和创新有效抵御风险，并确保创新是组织文化的组成部分。

（5）文化助推。文化助推是指组织与利益相关者沟通 IT 治理的目标、策略和职责，营造积极向上、沟通包容的组织文化。组织需要引导组织人员适应 IT 建设所带来的变革、遵循道德和职业规范、端正态度和规范行为。组织可以要求各级管理层把符合信息技术战略发展的文化建设作为其职责的一部分。按照文化营造、实施和改进的生命周期，保障利益相关者的沟通和透明，包括：①建立与 IT 发展相适应的组织文化发展策略；②营造包括知识、技术、管理、情操在内的积极向上的文化氛围；③根据组织内部环境的变化，评估并改进组织文化的管理。

3.1.4 IT 治理方法与标准

考虑到 IT 治理对组织战略目标达成的重要性，国内外各类机构持续研究并沉淀 IT 治理相关的最佳实践方法、定义相关标准，这里面比较典型的是我国信息技术服务标准库（ITSS）中 IT 治理系列标准、信息和技术治理框架（COBIT）和 IT 治理国际标准（ISO/IEC 38500）等。

1. ITSS 中 IT 服务治理

我国 IT 治理标准化研究是围绕 IT 治理研究范畴, 为 IT 过程、IT 资源、信息与组织战略、组织目标的连接提供了一种机制。通过指导、实施、管理和评价等过程, 确保 IT 支持并拓展组织的战略和目标。在 IT 治理目标和边界确定的情况下, IT 治理围绕决策体系、责任归属、管理流程、内外评价四个方面, 通过相关框架体系的研究, 规范和引导组织的 IT 治理完成“做什么”“如何做”“怎么样”“如何评价”等问题, 如图 3-5 所示。

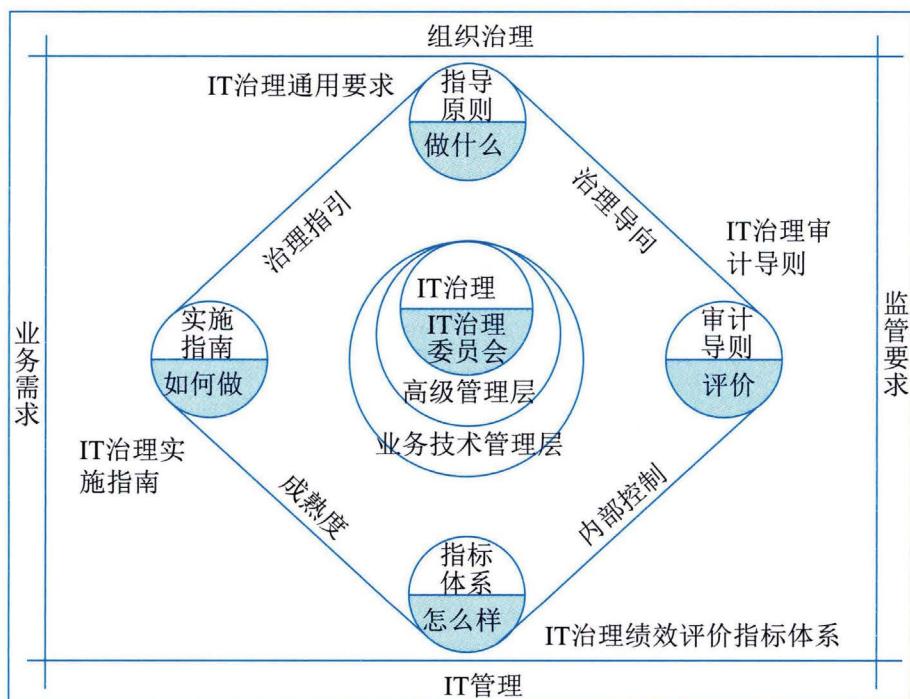


图 3-5 ITSS-IT 治理标准化的逻辑关系图

1) IT 治理通用要求

GB/T 34960.1《信息技术服务 治理 第 1 部分：通用要求》规定了 IT 治理的模型和框架、实施 IT 治理的原则, 以及开展 IT 顶层设计、管理体系和资源的治理要求。该标准可用于：①建立组织的 IT 治理体系, 并实施自我评价; ②开展信息技术审计; ③研发、选择和评价 IT 治理相关的软件或解决方案; ④第三方对组织的 IT 治理能力进行评价。各级各类信息化主管部门可根据法律法规、部门规章的要求, 使用该标准对所管辖各类组织的 IT 治理提出要求, 并进行评估、指导和监督。

该标准定义的 IT 治理模型包含治理的内外部要求、治理主体、治理方法, 以及信息技术及其应用的管理体系, 如图 3-6 所示。

治理主体以组织章程、监管职责、利益相关方期望、业务压力和业务要求为驱动力, 建立评估、指导、监督的治理过程并明确任务。治理主体通过信息技术战略和方针, 指导管理者对信息技术及其应用的管理体系进行完善, 并对信息技术相关的方案和规划进行评估, 对信息技术应用的绩效和符合性进行监督。组织结合治理原则和模型, 在 IT 治理实施的过程中, 开展自我监督、自我评估和审计工作, 并持续改进。

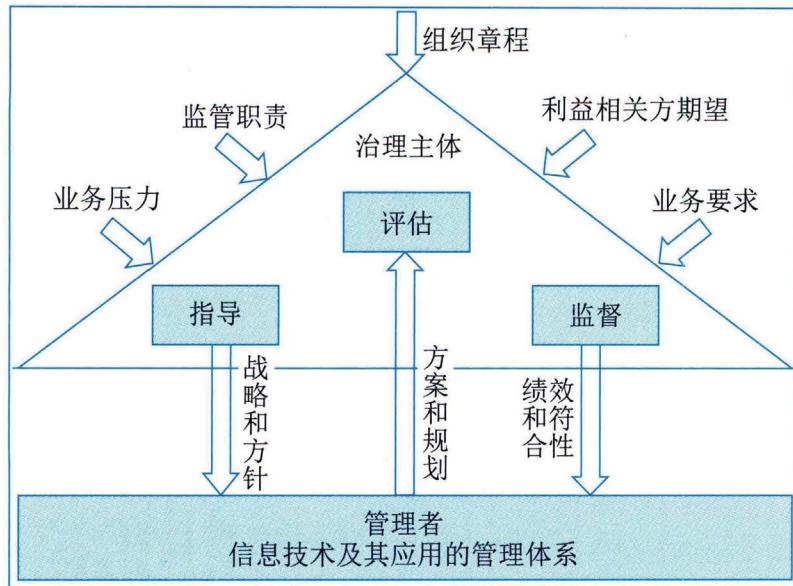


图 3-6 GB/T 34960.1 IT 治理模型

该标准定义的IT治理框架包含信息技术顶层设计、管理体系和资源三大治理域，每个治理域由如下若干治理要素组成，如图3-7所示。顶层设计治理域包含信息技术的战略，以及支撑战略的组织和架构；管理体系治理域包含信息技术相关的质量管理、项目管理、投资管理、服务管理、业务连续性管理、信息安全管理、风险管理、供方管理、资产管理和其他管理；资源治理域包含信息技术相关的基础设施、应用系统和数据。

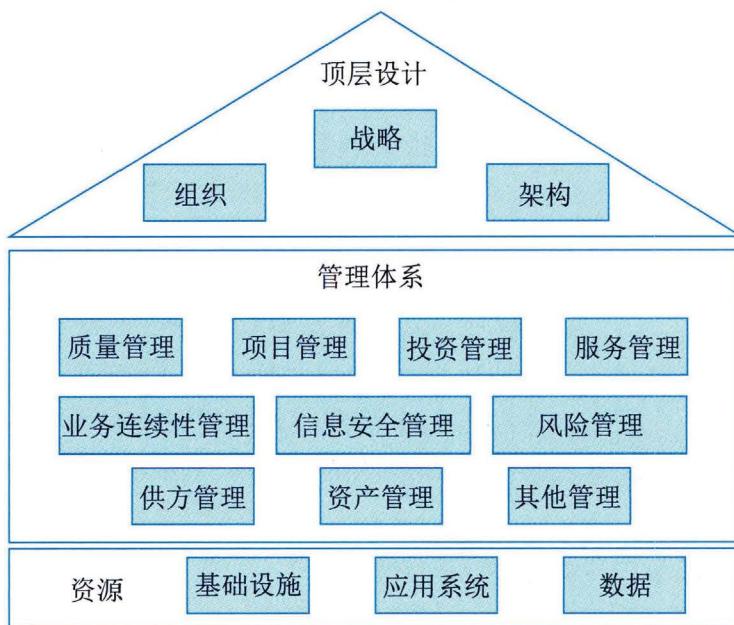


图 3-7 GB/T 34960.1 IT 治理框架

2) IT 治理实施指南

GB/T 34960.2《信息技术服务 治理 第2部分：实施指南》提出了IT治理通用要求的实施指南，分析了实施IT治理的环境因素，规定了IT治理的实施框架、实施环境和实施过程，并

明确顶层设计治理、管理体系治理和资源治理的实施要求。该标准适用于：①建立组织的 IT 治理实施框架，明确实施方法和过程；②组织内部开展 IT 治理的实施；③ IT 治理相关软件或解决方案实施落地的指导；④第三方开展 IT 治理评价的指导。

IT 治理实施框架包括治理的实施环境、实施过程和治理域，如图 3-8 所示。实施环境包括组织的内外部环境和促成因素。实施过程规定了 IT 治理实施的方法论，包括统筹和规划、构建和运行、监督和评估、改进和优化。治理域定义了 IT 治理对象，包括顶层设计、管理体系和资源。顶层设计包括战略、组织和架构；管理体系包括质量管理、项目管理、投资管理、服务管理、业务连续性管理、信息安全管理、风险管理、供方管理、资产管理和其他管理；资源包括基础设施、应用系统和数据。组织可以结合实施环境的分析，按照实施过程，以治理域为对象开展 IT 治理实施。

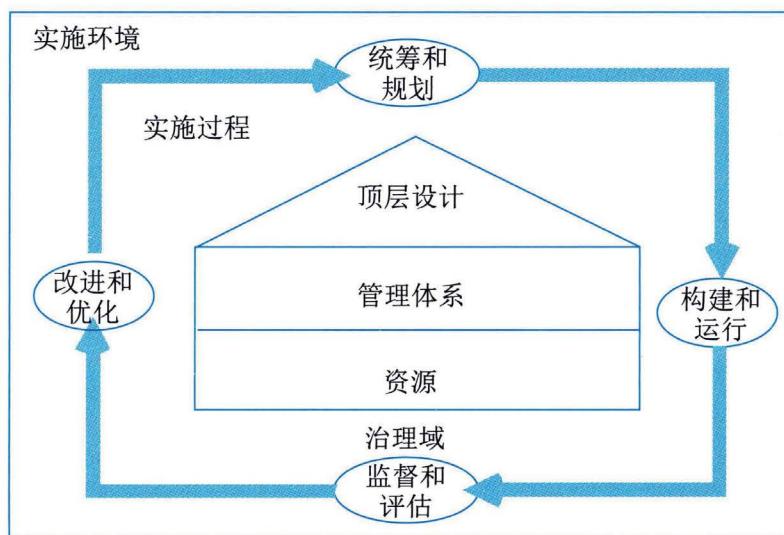


图 3-8 GB/T 34960.2 IT 治理实施框架

2. 信息和技术治理框架

COBIT 是面向整个组织的信息和技术治理及管理框架，由成立于 1969 年的美国信息系统审计与控制协会（ISACA）组织设计并编制的。COBIT 框架对治理和管理进行了明确区分，这两个学科涵盖不同的活动，需要不同的组织结构，并服务于不同目的：①治理确保对利益干系人的需求、条件和选择方案进行评估，以确定全面均衡、达成共识的组织目标；通过确定优先等级和制定决策来设定方向；根据议定的方向和目标监控绩效与合规性；②管理是指按治理设定的方向计划、构建、运行和监控活动，以实现组织目标。在大多数组织中，管理是首席执行官领导下的高级管理层的职责。ISACA 设计并编制了《框架：治理和管理目标》《设计指南：信息和技术治理解决方案的设计》，主要供组织信息和技术治理（EGIT）、鉴证、风险和安全专业人员作为学习资料使用。

1) 治理和管理目标

COBIT 框架介绍了 40 项核心治理和管理目标，以及其中包含的流程和其他相关组件。COBIT 核心模型如图 3-9 所示。COBIT 中治理目标被列入评估、指导和监控（EDM）领域，在

这个领域，治理机构将评估战略方案，指导高级管理层执行所选的战略方案并监督战略的实施。管理目标分为四个领域：①调整、规划和组织（APO）针对IT的整体组织、战略和支持活动；②内部构建、外部采购和实施（BAI）针对IT解决方案的定义、采购和实施以及它们到业务流程的整合；③交付、服务和支持（DSS）针对IT服务的运营交付和支持，包括安全；④监控、评价和评估（MEA）针对IT的性能监控及其与内部性能目标、内部控制目标和外部要求的一致程度。治理目标与治理流程有关，而管理目标与管理流程有关。治理流程通常由董事会和执行管理层负责，而管理流程则在高级和中级管理层的职责范围内。



图 3-9 COBIT 核心模型

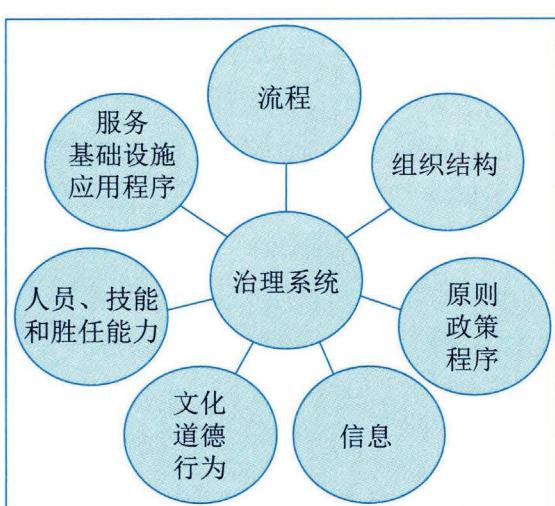


图 3-10 COBIT 治理系统组件

为满足治理和管理目标，每个组织都需要建立、定制和维护由多个组件构成的治理系统，如图3-10所示。治理系统的组件包括：①流程。流程描述了一组为实现某种目标而安排有序的实践和活动，并生成了一组支持实现整体IT相关目标的输出内容。②组织结构。组织结构是组织的主要决策实体。③原则、政策和程序。原则、政策和程序用于将理想行为转化为日常管理的实用指南。④信息。在任何组织中，信息无处不在，包括组织生成和使用的全部信息。COBIT侧重于有效运转组织治理系统所需的信息。⑤文化、道德和行为。个人和组织的文化、道德和行为作为治理和管理活动的成

功因素，其价值往往被低估。⑥人员、技能和胜任能力。人员、技能和胜任能力对做出正确决策、采取纠正行动和成功完成所有活动而言是必不可少的。⑦服务、基础设施和应用程序。服务、基础设施和应用程序包括为组织提供IT处理治理系统的基础设施、技术和应用程序。

2) 信息和技术治理解决方案的设计

COBIT设计指南描述了组织如何设计量身定制的组织IT治理解决方案。高效和有效的IT治理系统是创造价值的起点。COBIT定义的IT治理系统设计因素包括组织战略、组织目标、风险概况、IT相关问题、威胁环境、合规性要求、IT角色、IT采购模式、IT实施方法、技术采用战略、组织规模和未来因素，如图3-11所示。这些设计因素可能影响组织治理系统的设计，为成功使用IT奠定基础。

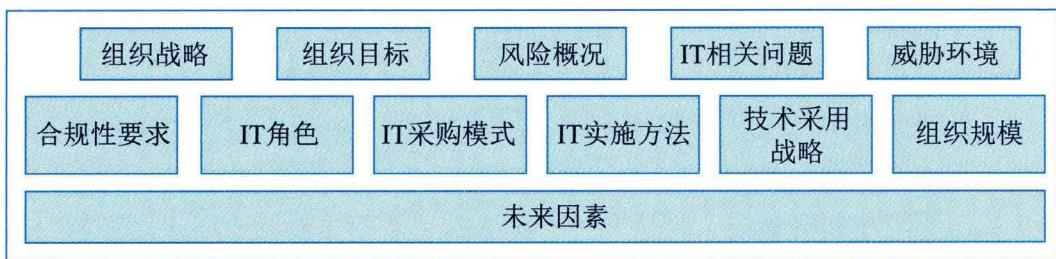


图3-11 COBIT治理体系设计因素

组织开展治理系统设计通过流程化的方式进行，如图3-12所示，COBIT给出了建议设计流程：①了解组织环境和战略；②确定治理系统的初步范围；③优化治理系统的范围；④最终确定治理系统的设计。



图3-12 COBIT治理系统设计工作流程

3. IT治理国际标准

2008年4月，ISO/IEC正式发布IT治理标准ISO/IEC 38500，它的出台不仅标志着IT治理从概念模糊的探讨阶段进入了一个正确认识的发展阶段，而且也标志着信息化正式进入IT治理时代。这一标准将促使国内外一直争论不休的IT治理理论得到统一，也促使我国在引导信息化科学方面发挥重要作用。2014年，ISO/IEC发布了第二版的ISO/IEC FDIS 38500，替换了2008第一版的ISO/IEC 38500，ISO/IEC FDIS 38500: 2014提供了IT良好治理的原则、定义和模式，

以帮助最高级别组织的人员理解和履行其在组织使用 IT 方面的法律、法规和道德义务。

该标准为组织的治理机构（可包括所有者、董事、合伙人、执行经理或类似机构）的成员提供了关于在其组织内有效、高效和可接受地使用信息技术（IT）的指导原则。该标准包括：①责任。组织内的个人和团体理解并接受他们在 IT 的供应和需求方面的责任。那些负有行动责任的人也有权执行这些行动。②战略。组织的业务战略考虑到 IT 的当前和未来的能力；使用 IT 的计划满足了组织业务战略的当前和持续的需求。③收购。IT 收购是出于正当的理由，在适当和持续的分析基础上，有明确和透明的决策。在短期和长期内，在利益、机会、成本和风险之间都存在着适当的平衡。④性能。IT 适合于支持组织，提供满足当前和未来业务需求所需的服务、服务水平和服务质量。⑤一致性。IT 的使用符合所有强制性法律和法规。政策和实践有明确的定义、实施和执行。⑥人的行为。IT 团队的政策、实践和决策表明了对人的行为的尊重，包括所有“在这个过程中的人”的当前和不断发展的需求。

该标准规定治理机构应通过评估、指导和监督三个主要任务来治理 IT。

(1) 评估。治理机构应审查和判断当前和未来的使用，包括计划、建议和供应安排（无论是内部、外部或两者兼有）。在评估 IT 的使用时，治理机构应考虑作用于组织的外部或内部压力，如技术变革、经济和社会趋势、监管义务、合法的利益相关者期望和政治影响。治理机构应根据情况的变化不断地进行评价。治理机构还应考虑到当前和未来的业务需要，即他们必须实现的当前和未来的组织目标，例如维持竞争优势，以及他们正在评估的计划和建议的具体目标。

(2) 指导。治理机构应负责战略和政策的编制和执行。战略应该为 IT 领域的投资设定方向以及 IT 应该实现的目标。政策应在使用 IT 时建立良好的行为。治理机构应通过要求管理者及时提供信息、遵守方向和遵守良好治理的六项原则来鼓励其组织中的良好治理文化。

(3) 监督。治理机构应通过适当的测量系统来监测 IT 的表现。他们应该保证自己业绩符合战略，特别是在业务目标方面。治理机构还应确保 IT 符合外部义务（法规、立法、普通法、合同）和内部工作惯例等。

3.2 IT 审计

随着大数据、云计算、人工智能、移动互联网、物联网等新一代信息技术快速普及和深入应用，以及商业新模式、制造新模式、运行新模式等的出现和迅速繁荣，在给组织带来快速发展的同时，也加大了组织的 IT 风险。为了有效控制 IT 风险，有必要对组织的信息系统治理及 IT 内控与管理等开展 IT 审计，充分发挥 IT 审计监督的作用，提高组织的信息系统治理水平，促进组织信息系统治理目标的实现。

3.2.1 IT 审计基础

IT 审计对组织 IT 目标的达成以及组织战略目的实现具备重要的作用，这与人们通常所说的传统审计的重要性概念不同。传统审计的重要性是指被审计单位会计报表中错报或漏报的严重程度，这一严重程度在特定环境下可能影响会计报表使用者的判断或决策。传统审计在量上表现为审计重要性水平，也就是被审计单位财务报表中可能存在的不影响报表使用者做出决策和

判断的错报及漏报最大限额。IT 审计重要性是指 IT 审计风险（固有风险、控制风险、检查风险）对组织影响的严重程度，如：财务损失、业务中断、失去客户信任、经济制裁等。

1. IT 审计定义

IT 审计经过多年的发展，国内外机构对 IT 审计从不同角度进行了描述，目前主流的 IT 审计定义如表 3-3 所示。

表 3-3 主流的 IT 审计定义

机构 / 标准名称	定义
国际信息系统审计协会 (Information Systems Audit and Control Association, ISACA)	IT 审计是一个获取并评价证据，以判断计算机系统是否能够保证资产的安全、数据的完整以及有效利用组织的资源并有效实现组织目标的过程
国际货币基金组织 (International Monetary Fund, IMF)	IT 审计是对计算机化的系统进行审计，不仅是对现有信息系统的控制，还包括对系统建立过程、计算机设备和网络管理等方面控制
最高审计机关国际组织 (International Organization of Supreme Audit Institutions, INTOSAI)	IT 审计是一个通过获取并评估证据，以判断 IT 系统是否保护组织的资产，有效地利用组织的资源，保障数据的安全性和一致性，以及有效地达到组织业务目标的过程
GB/T 34690.4《信息技术服务 治理 第 4 部分：审计导则》	IT 审计是根据 IT 审计标准的要求，对信息系统及相关的 IT 内部控制和流程进行检查、评价，并发表审计意见

2. IT 审计目的

IT 审计的目的是指通过开展 IT 审计工作，了解组织 IT 系统与 IT 活动的总体状况，对组织是否实现 IT 目标进行审查和评价，充分识别与评估相关 IT 风险，提出评价意见及改进建议，促进组织实现 IT 目标。

组织的 IT 目标主要包括：①组织的 IT 战略应与业务战略保持一致；②保护信息资产的安全及数据的完整、可靠、有效；③提高信息系统的安全性、可靠性及有效性；④合理保证信息系统及其运用符合有关法律、法规及标准等的要求。

3. IT 审计范围

一般来说，IT 审计范围需要根据审计目的和投入的审计成本来确定。在确定审计范围时，除了考虑前面提及的审计内容外，还需要明确审计的组织范围、物理位置以及信息系统相关逻辑边界。IT 审计范围的确定如表 3-4 所示。

表 3-4 IT 审计范围的确定

IT 审计范围	说明
总体范围	需要根据审计目的和投入的审计成本来确定
组织范围	明确审计涉及的组织机构、主要流程、活动及人员等
物理范围	具体的物理地点与边界
逻辑范围	涉及的信息系统和逻辑边界
其他相关内容

在实际的应用实践中，审计人员在实施IT审计项目前，应先对组织与信息系统相关的总体情况进行了解和风险评估，确定主要IT风险，如与环境控制相关的风险、与系统相关的风险、与数据相关的风险等，然后根据确定的风险来判断哪些控制、流程对组织的影响比较大，并结合审计项目预计的时间、配备的审计力量等来确定重点审计范围。

4. IT 审计人员

根据GB/T 34690.4《信息技术服务 治理 第4部分：审计导则》，对IT审计人员的要求包括职业道德、知识、技能、资格与经验、专业胜任能力及利用外部专家服务等方面，如表3-5所示。

表3-5 IT审计人员要求

分类	具体要求
职业道德	<ul style="list-style-type: none"> ● 在执业过程中保持独立、客观、公正 ● 在执业过程中保持正直、诚实和守信 ● 正确履行审计职责（其中包括遵守相应的职业审计标准） ● 对在实施IT审计业务中所获取的信息负有保密责任
知识、技能、资格与经验	<ul style="list-style-type: none"> ● 掌握与IT相关的专业知识和技能 ● 掌握审计、财务及管理等通用知识和技能 ● 拥有与IT审计工作相关的基本技能、专业技能和软技能 ● 拥有与所处管理或业务岗位相适应的IT审计职业资格及经验
专业胜任能力	<ul style="list-style-type: none"> ● 具备相应的IT审计专业胜任能力 ● 拥有与所处管理或业务岗位相适应的IT审计职业资格 ● 定期参加持续的职业教育和培训
利用外部专家服务	<ul style="list-style-type: none"> ● 对外部专家的专业资格及专业经验进行评价 ● 对外部专家的独立性、客观性进行评价 ● 对外部专家的专业胜任能力进行评价 ● 与外部专家签订书面协议 ● 对外部专家的服务结果进行评价和利用

5. IT 审计风险

IT审计风险主要包括固有风险、控制风险、检查风险和总体审计风险。固有风险、控制风险、检查风险的内容，如表3-6所示。

表3-6 固有风险、控制风险和检查风险的内容

类别	描述
固有风险	<ul style="list-style-type: none"> ● 含义：是指IT活动不存在相关控制的情况下，易于导致重大错误的风险 ● 分类：可从IT组织层面控制、一般控制及应用控制三个方面分析固有风险 ● 特点：固有风险是IT活动本身所具有的，审计人员只能评估，却无法控制或影响它；固有风险的衡量是主观的、复杂的，不同的IT活动其固有风险水平不同

(续表)

类别	描述
控制风险	<ul style="list-style-type: none"> ● 含义：是指与IT活动相关的内部控制体系不能及时预防或检查出存在的重大错误的风险 ● 分类：可从IT组织层面控制、一般控制及应用控制三个方面分析控制风险 ● 特点：与内部控制制度执行的有效性有关，与审计无关，属于内部控制的范畴，审计人员只能评估其风险水平而不能对其实施控制和影响。其风险水平的衡量由于需要兼顾传统内部控制的思想和计算机系统管理的知识，因而较为复杂且难以准确计量
检查风险	<ul style="list-style-type: none"> ● 含义：检查风险是指通过预定的审计程序未能发现重大、单个或与其他错误相结合的风险 ● 影响检查风险的因素：由于IT审计规范不完善、审计人员自身或者技术原因等造成影响审计测试正确性的各种因素

总体审计风险是指针对单个控制目标所产生的各类审计风险总和。良好的审计计划应尽可能评估和控制审计风险，减少或控制所检查领域的审计风险，比如采取合适的审计工具，在完成审计时把总体审计风险控制在足够低的水平之内，以达到预期保证水平。

审计风险也用于描述审计人员在执行审计任务时可接受的风险水平。审计人员可通过设定目标风险水平并调整审计工作量，以合适的审计成本满足最小化总体审计风险要求。

3.2.2 审计方法与技术

1. IT 审计依据与准则

IT 审计活动的开展需要结合相关法律法规、准则与标准。国际上发布的常用审计准则有：

- 信息系统审计准则（ISACA，国际信息系统审计协会发布）。
- 《内部控制—整体框架》报告，即通称的COSO（The Committee of Sponsoring Organizations of The National Commission of Fraudulent Financial Reporting，美国虚假财务报告委员会下属的发起人委员会）报告。
- 《萨班斯法案》（Sarbanes-Oxley Act, SOX）。SOX是美国政府出台的一部涉及会计职业监管、组织治理、证券市场监管等方面改革的重要法律。
- 信息及相关技术控制目标（Control Objectives for Information and related Technology, COBIT）是目前国际上通用的信息及相关技术控制规范。

我国的 IT 审计相关法律法规、准则与标准如表 3-7 所示。

表 3-7 IT 审计相关法律法规、准则与标准（举例）

类别	名称
法律法规	《中华人民共和国审计法》《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等
审计准则	《信息系统审计指南——计算机审计实务公告第 34 号》《第 2203 号内部审计具体准则——信息系统审计》等
IT 审计国际标准	GB/T 34960.4 《信息技术服务 治理 第 4 部分：审计导则》等
组织内部控制	《组织内部控制基本规范》《组织内部控制应用指引第 18 号——信息系统》等

(续表)

类别	名称
行业规范	《商业银行信息科技风险管理指引》《证券期货经营机构信息技术治理工作指引（试行）》《保险公司信息化工作指引（试行）》等

2. IT 审计常用方法

IT 审计方法就是为了完成 IT 审计任务所采取的手段。在 IT 审计工作中，要完成每一项审计工作，都应选择合适的审计方法。常用审计方法包括：访谈法、调查法、检查法、观察法、测试法和程序代码检查法等，如表 3-8 所示。

表 3-8 IT 审计常用方法表（举例）

分类	说明
访谈法	<ul style="list-style-type: none"> 含义：是指通过访谈人和受访人面对面地交谈来了解被审计对象的信息。依据不同研究问题的性质、目的或对象，访谈法具有不同的形式 分类：根据访谈进程的结构化程度，可将它分为结构型访谈和非结构型访谈
调查法	<ul style="list-style-type: none"> 含义：是指为了达到预期目的，在制订调研计划的基础上，通过书面或口头回答问题的方式收集研究对象的相关资料，并做出分析、综合，得到某一结论的研究方法 目的：可能是全面把握当前状况，也可能是为了揭示存在的问题，弄清前因后果，以便为进一步的研究或决策提供观点和论据
检查法	<ul style="list-style-type: none"> 含义：是指审计人员对被审计单位内部或外部生成的记录和文件（如纸质、电子或其他介质形式存在的资料）进行审查，或对资产进行实物审查 分类：从技术层面上可分为审阅法、核对法、复算法和分析法
观察法	<ul style="list-style-type: none"> 含义：是审计人员到被审计单位的经营场所及其他有关场所进行实地察看，来证实审计事项的一种方法 应用：观察程序具有方向性，即从书面记录观察到实物或过程，反之，从实物或过程观察到书面记录。观察法既可以用于对通过其他方法获得的审计证据进行补充，证实审计证据，也可以用于直接收集相关证据。观察法可以比较准确地获得审计项目如何运行的信息，适用于正在进行中的审计事项
测试法	<ul style="list-style-type: none"> 含义：通过测试来评估程序的质量是一项常用的审计技术，其基本原理是从计算机输入开始，跟踪某项业务直至计算机输出，以检验计算机应用程序、控制程序和系统可靠性。执行此类方法使用的是用于测试目的的业务数据，称之为测试数据 分类：主要包括黑盒法和白盒法。黑盒法测试是把程序看成黑盒子，完全不考虑其内部结构和处理过程，只检查程序的功能是否符合它的需求规格说明。白盒法是通过测试来检测产品内部动作是否按照规格说明书的规定正常进行，按照程序内部的结构测试程序，检验程序中的每条通路是否都能按预定要求正确工作，主要用于软件验证
程序代码检查法	<ul style="list-style-type: none"> 含义：是指对被审程序的指令逐条加以审查，以验证程序的合法性、完整性和程序逻辑的正确性 应用：审计人员可使用代码静态扫描工具进行程序代码的检查

3. IT 审计技术

常用的 IT 审计技术包括风险评估技术、审计抽样技术、计算机辅助审计技术及大数据审计技术。

1) 风险评估技术

IT 风险评估技术一般包括：

- 风险识别技术：用以识别可能影响一个或多个目标的不确定性，包括德尔菲法、头脑风暴法、检查表法、SWOT 技术及图解技术等。
- 风险分析技术：是对风险影响和后果进行评价和估量，包括定性分析和定量分析。
- 风险评价技术：是在风险分析的基础上，通过相应的指标体系和评价标准，对风险程度进行划分，以揭示影响成败的关键风险因素，包括单因素风险评价和总体风险评价。
- 风险应对技术：IT 技术体系中为特定风险制定的应对技术方案，包括云计算、冗余链路、冗余资源、系统弹性伸缩、两地三中心灾备、业务熔断限流等。

2) 审计抽样技术

审计抽样是指审计人员在实施审计程序时，从审计对象总体中选取一定数量的样本进行测试，并根据测试结果，推断审计对象总体特征的一种方法。审计抽样适用于时间及成本都不允许对既定总体中的所有交易或事件进行全面审计时。“总体”是指需要检查的全部事项，“样本”是用于测试总体的子集。审计抽样的方法如表 3-9 所示。

表 3-9 审计抽样方法分类表

类别	说明
统计抽样	<ul style="list-style-type: none"> ● 采用客观的方法来确定样本量和样本抽取标准。统计抽样采用概率学原理，涉及计算样本量、抽取样本 ● 评价样本结果并做出推断。利用统计抽样，审计人员可以量化描述样本与总体的接近程度（评价抽样精度）以及用百分比表示的样本能够代表总体的概念（可靠性或置信水平）。有效的统计抽样结果是量化的 ● 常用的统计抽样方法有：①属性抽样。固定样本量属性抽样或频率估计抽样——用于估计总体中某种特性（属性）的发生比率（百分率）的抽样方法，属性抽样回答“有多少？”的问题。可被测试的属性的一个例子是计算机访问申请表上的批准签字。②变量抽样。变量抽样也称为金额估计抽样或平均值估计抽样，是一种由样本估计总体的货币金额或其他度量单位（如重量）的抽样技术。变量抽样的一个例子是检查组织重要交易的余额表及对生成余额表的程序实施的应用系统审计
非统计抽样	常指判断抽样——采用审计人员判断来确定抽样方法、样本量（从总体中抽取的一定数量的事项以执行测试）及抽样标准（选择哪一些事项用于测试）。抽样结果是基于审计人员对抽样事项或交易的重要性及风险的主观判断

3) 计算机辅助审计技术

计算机辅助审计（Computer Assisted Audit Tools, CAAT），也称为利用计算机审计，是指审计人员在审计过程和审计管理活动中，以计算机为工具来执行和完成某些审计程序和任务的一种新兴审计技术。它并非电算化系统审计特有的一种方法，对手工系统的审计也可应用这些技术。

计算机辅助审计技术是审计人员在这种环境下收集信息的重要工具。由于系统有不同的硬件和软件环境、数据结构、记录格式或处理功能，如果没有软件工具来收集和分析记录内容，审计人员收集证据几乎是不可能的。CAAT 也使得审计人员可以独立地收集信息，CAAT

为针对既定的审计目标访问和分析数据提供了一种方法，并以系统记录的可靠性为重点报告审计发现。源信息可靠性是审计发现的保证基础。CAAT 包括多种工具和技术，如通用审计软件（GAS）、测试数据、实用工具软件、专家系统等。

4) 大数据审计技术

大数据审计是指遵循大数据理念，运用大数据技术方法和工具，利用数量巨大、来源分散、格式多样的数据，开展跨层级、跨系统、跨部门和跨业务等的深入挖掘与分析，提升审计发现问题、评价判断、宏观分析的能力。大数据审计技术包括大数据智能分析技术、大数据可视化分析技术及大数据多数据源综合分析技术等，如表 3-10 所示。

表 3-10 大数据审计技术（举例）

分类	说明
大数据智能分析技术	以各种高性能处理算法、智能搜索与挖掘算法等为主要研究内容，是目前大数据分析领域的研究主流。该技术从计算机的视角出发，强调计算机的计算能力和人工智能，如各类面向大数据的机器学习和数据挖掘方法等。常用技术包括 A/B Testing、关联规则分析、分类、聚类、遗传算法、神经网络、预测模型、模式识别、时间序列分析、回归分析、系统仿真等
大数据可视化分析技术	从人作为分析主体和需求主体的视角出发，强调基于人机交互的、符合人的认知规律的分析方法，目的是将人所具备的、机器并不擅长的认知能力融入数据分析过程中，如 R 语言、Python、D3.js、Leaflet 等
大数据多数据源综合分析技术	大多数大数据多数据源综合分析技术是对采集来的各行、各业、各类大数据，采用数据查询等常用方法或其他大数据技术方法进行相关数据的综合比对和关联分析，从而发现更多隐藏的审计线索的技术

4. IT 审计证据

审计证据是指由审计机构和审计人员获取，用于确定所审计实体或数据是否遵循既定标准或目标，形成审计结论的证明材料。审计证据是审计意见的支柱，是审计人员形成审计结论的基础。审计人员必须基于足够、相关和适当的审计证据，为其审计观点提供合理的结论。审计证据还可以被作为解除或追究被审计人经济责任的依据，并且审计证据还是控制审计工作质量的关键。

审计证据的特性是指审计证据内在性质和特征，具体体现为审计人员围绕这些性质和特征收集审计证据时应达到的基本要求。对审计证据的属性，在国际上有不同的描述。审计证据的特性如表 3-11 所示。

表 3-11 审计证据的特性

分类	说明
充分性	指要求审计人员根据所获证据足以对被审计对象提出一定程度保证的结论，是对审计证据数量的要求，主要与审计人员确定的样本量有关
客观性	指审计证据必须是客观存在的事实材料。客观的审计证据比需要判断或解释的证据可靠
相关性	指审计证据与审计事项之间必须有实质性联系
可靠性	指审计证据能够反映和证实客观经济活动特征的程度。审计证据的可靠性受到审计证据的类型、取证的渠道和方式等因素的影响
合法性	指审计证据必须符合法定种类，并依照法定程序取得

电子证据是信息环境下经常使用的一种证据类型。电子证据是指以电子的、数据的、磁性的或类似性能的相关技术形式存在并能够证明事件事实真实情况的一切材料。刑事诉讼法中指出电子证据无论是形式还是证据规则都与传统证据有很大区别，高要求的技术规范，贯穿于电子证据的收集、提取、保存到出示、审查、判断、认证的各个环节。因此，通过司法解释缓解司法实践中的矛盾仅仅是权宜之计，彻底解决电子证据法律定位问题还是要从立法上予以突破，即应通过修改诉讼法或出台证据法典来明确电子证据的法律地位，赋予电子证据独立的法律地位，以电子证据取代视听资料的证据地位。

为了使收集到的分散、个别、不系统审计证据变成充分、适当、具有证明力证据，审计人员必须按照一定的方法对审计证据进行分类整理与分析，使之条理化、系统化，然后对各种审计证据进行合理归纳，并在此基础上形成恰当的整体审计结论。审计证据评价应考虑的因素包括证据提供者的独立性、提供信息/证据的个人资质、证据的客观性、证据的时效性、与审计目标的相关性、审计证据的说服力及审计证据的充分性。此外，在审计过程中还必须考虑取得审计证据的经济性，必须考虑成本效益原则，合理把握审计证据的充分性。

5. IT 审计底稿

审计工作底稿是指审计人员对制订的审计计划、实施的审计程序、获取的相关审计证据，以及得出的审计结论做出的记录。审计工作底稿是审计证据的载体，是审计人员在审计过程中形成的审计工作记录和获取的资料。它形成于审计过程，也反映整个审计过程。审计底稿的作用表现在：

- 是形成审计结论、发表审计意见的直接依据；
- 是评价考核审计人员的主要依据；
- 是审计质量控制与监督的基础；
- 对未来审计业务具有参考备查作用。

审计工作底稿一般分为综合类工作底稿、业务类工作底稿和备查类工作底稿，具体如表 3-12 所示。

表 3-12 审计工作底稿分类

底稿类型	说明
综合类工作底稿	指审计人员在审计计划阶段和审计报告阶段，为规划、控制和总结整个审计工作并发表审计意见所形成的审计工作底稿，主要包括：审计业务约定书、审计计划、审计总结、审计报告、管理建议书、被审计单位管理当局声明书以及审计人员对整个审计工作进行组织管理的所有记录和资料
业务类工作底稿	指审计人员在审计实施阶段为执行具体审计程序所形成的审计工作底稿，包括：符合性测试中形成的内部控制问题调查表和流程图、实质性测试中形成的项目明细表等
备查类工作底稿	指审计人员在审计过程中形成对审计工作仅具有备查作用的审计工作底稿。备查类工作底稿应随被审计单位有关情况的变化而不断更新；应详细列明目录清单，并将更新的文件资料随时归档；应根据需要，将其中与具体审计项目有关的内容复印、摘录、综合后归入业务类审计工作底稿的具体审计项目之后。通常，备查类审计工作底稿是由被审计单位或第三者根据实际情况提供或代为编制，审计人员应认真审核，并对所取得的有关文件、资料标明其具体来源

审计工作底稿作为审计人员在整个审计过程中形成的审计工作记录资料，在编制上应满足内容和形式两方面的要求：

- 内容要求包括资料翔实、重点突出、繁简得当、结论明确；
- 形式要求包括要素齐全、格式规范、标识一致、记录清晰。

通常，根据审计机构的组织规模和业务范围，可以实行对审计工作底稿的三级复核制度。审计工作底稿三级复核制度是指以审计机构负责人、部门负责人和项目负责人（或项目经理）为复核人，依照规定的程序和要点对审计工作底稿进行逐级复核的制度。三级复核制度目前已成为较为普遍采用的形式，对于提高审计工作质量、加强质量控制起了重要的作用。

为了维护被审计单位及相关单位的利益，审计机构对审计工作底稿中涉及的商业秘密保密，建立健全审计工作底稿保密制度。但由于下列两种情况需要查阅审计工作底稿的，不属于泄密情形：

- 法院、检察院及国家其他部门依法查阅，并按规定办理了必要手续；
- 审计协会或其委派单位对审计机构执业情况进行检查。

审计工作底稿按照一定的标准归入审计档案后，应交由档案管理部门进行管理，并确保审计档案的安全、完整。

3.2.3 审计流程

审计流程是指审计人员在具体审计过程中采取的行动和步骤。科学、规范的审计流程不但是分配审计工作的具体依据，还是控制审计工作的有效工具，并同时具有的作用包括：①有效地指导审计工作；②有利于提高审计工作效率；③有利于保证审计项目质量；④有利于规范审计工作。

通常，审计流程的含义有广义和狭义两种之分。狭义的审计流程是指审计人员在取得审计证据、完成审计目标、得出审计结论过程中所采取的步骤和方法。广义的审计流程是指审计机构和审计人员对审计项目从开始到结束的整个过程采取的系统性工作步骤，一般分为审计准备、审计实施、审计终结及后续审计四个阶段，每个阶段又包含若干具体内容。

(1) 审计准备阶段。IT 审计准备阶段是指 IT 审计项目从计划开始，到发出审计通知书为止的期间。准备阶段是整个审计过程的起点和基础，准备阶段的工作是否充分、合理、细致，对提高审计工作效率，保证审计工作质量至关重要。准备阶段工作一般包括：①明确审计目的及任务；②组建审计项目组；③搜集相关信息；④编制审计计划等。

(2) 审计实施阶段。IT 审计实施阶段是审计人员将项目审计计划付诸实施的期间。此阶段的工作是审计全过程的中心环节，是整个审计流程的关键阶段，关系到整个审计工作的成败。实施阶段主要完成工作包括：①深入调查并调整审计计划；②了解并初步评估 IT 内部控制；③进行符合性测试；④进行实质性测试等。

(3) 审计终结阶段。IT 审计终结阶段是整理审计工作底稿、总结审计工作、编写审计报告、做出审计结论的期间。审计人员应运用专业判断，综合分析所收集到的相关证据，以经过核实的审计证据为依据，形成审计意见、出具审计报告。终结阶段的工作一般包括：①整理与复

核审计工作底稿；②整理审计证据；③评价相关 IT 控制目标的实现；④判断并报告审计发现；⑤沟通审计结果；⑥出具审计报告；⑦归档管理等。

(4) 后续审计阶段。后续审计是在审计报告发出后的一段时间内，审计人员为检查被审计单位对审计问题和建议是否已经采取了适当的纠正措施，并取得预期效果的跟踪审计。后续审计并不是一次新的审计，而是前一次审计的有机组成部分。实施后续审计，可不必遵守审计流程的每一过程和要求，但必须依法依规进行检查、调查，收集审计证据，写出后续审计报告。

3.2.4 审计内容

IT 审计业务和服务通常分为 IT 内部控制审计和 IT 专项审计。IT 内部控制审计主要包括组织层面 IT 控制审计、IT 一般控制审计及应用控制审计；IT 专项审计主要是指根据当前面临的特殊风险或者需求开展的 IT 审计，审计范围为 IT 综合审计的某一个或几个部分。有关 IT 内部控制审计与 IT 专项审计的具体内容如表 3-13 所示。

表 3-13 IT 审计业务分类表

大类名称	子类名称	审计内容
IT 内部控制审计	组织层面 IT 控制审计、IT 一般控制审计及应用控制审计	<ul style="list-style-type: none"> ● 组织层面 IT 控制审计主要指对 IT 战略、组织、架构、业务连续性、风险管理、外包管理、网络与信息安全及监督管理等进行审计 ● IT 一般控制审计主要是指针对与应用系统、数据库、操作系统、网络相关的策略和措施等进行审计 ● 应用控制审计是指针对业务流程层面运行的人工或自动化程序进行审计，主要包括输入控制、处理控制和输出控制的审计
IT 专项审计	信息系统生命周期审计	主要是对信息系统的规划、设计、开发、测试、运行和维护等进行审计
	信息系统开发过程审计	主要围绕信息系统规划、设计、建设、实施是否符合 IT 架构和战略进行评估和监督
	信息系统运行维护审计	主要针对 IT 运维能力、IT 运维流程策划、实施、监控改进等情况进行审计，内容包括基础设施的运行、系统的运行、维护、质量保证及 IT 服务管理等
	网络与信息安全审计	主要以网络与信息安全为核心，围绕安全相关的组织、人员、系统、设备和环境等，重点关注网络与信息安全相关流程、制度的执行情况，对相关法律法规的遵从性，包括适用的数据保护，个人隐私保护等合规要求
	信息系统项目审计	主要是通过对信息系统项目管理过程的评价，向管理层提供信息系统项目管理过程得到控制、监督并遵循最佳实践要求的合理保证
	数据审计	通过控制活动，负责定期分析、验证、讨论、改进数据安全管理相关的政策、标准和活动

针对信息系统项目的专项审计，其目标是通过对信息系统项目管理过程的评价，向管理层提供信息系统项目管理过程得到控制、监督并遵循最佳实践要求的合理保证。信息系统项目管理审计内容与方法举例如表 3-14 所示。

表 3-14 信息系统项目管理审计内容与方法举例

类别	审计内容	审计方法
组织管理	<ul style="list-style-type: none"> ● 组织是否设立项目管理机构或明确项目管理职能的归属 ● 组织是否制定了项目管理制度与流程 ● 组织级的项目管理制度与流程是否全面合理 ● 是否对信息系统项目团队的组成、人员的配备及能力等进行要求 	<ul style="list-style-type: none"> ● 访谈组织级项目管理相关人员，了解组织级信息系统相关组织机构、项目管理制度及流程等的制定情况 ● 检查组织级信息系统相关组织机构的架构、职责与权限设计的合理性
项目启动与计划	<ul style="list-style-type: none"> ● 项目启动会的组织是否规范 ● 项目管理目标是否清晰定义及跟踪 ● 是否建立与项目规模及重要程度相适应的项目管理团队并明确职责 ● 团队人员是否稳定 ● 是否存在职责不相容的情况 ● 项目人员配备及能力是否满足要求 ● 是否制订项目计划 ● 项目计划是否完备 	<ul style="list-style-type: none"> ● 访谈项目负责人，了解项目启动与计划的总体情况 ● 取得项目组织机构图、职责及人员配备，检查项目组织机构图、人员职责对应表的合理性；检查团队人员变更的情况 ● 取得项目资料（如项目合同、工作说明书、项目计划等），检查文档的编制是否符合要求，内容的全面性及合理性
项目实施与控制	<ul style="list-style-type: none"> ● 项目干系人是否参与到项目活动中，发挥作用 ● 是否建立了科学、高效的项目沟通机制 ● 项目的资源是否有效利用 ● 项目是否进行了必要的配置管理 ● 项目的采购是否规范 ● 是否建立了适合组织的风险管理方法 ● 项目是否建立了绩效评价体系 ● 各阶段产生的文档是否合理、真实 ● 项目是否采取措施，有效地制订了进度计划、控制进度的活动 ● 项目是否建立规划质量、实施质量保证、实施质量控制的控制手段 	<ul style="list-style-type: none"> ● 访谈项目相关人员，了解项目实施与控制的总体情况 ● 检查与观察项目现场物理环境的控制情况 ● 访谈项目相关人员，询问文档有关内容 ● 取得项目相关文档（如项目审查记录和发布通知、项目有效性审查评估记录、项目安全事件记录等），检查文档编制的规范性以及相关控制的合理性 ● 取得应用系统的测试资料，检查测试过程控制的规范性，以及测试报告编制的合理性等
项目收尾管理	<ul style="list-style-type: none"> ● 项目验收申请材料是否完整且规范 ● 是否建立项目验收流程 ● 项目验收评审流程是否规范 ● 是否在规定时间内完成项目验收 ● 项目质量是否达标 ● 第三方项目质量检测机构的流程是否规范，报告内容是否完整 	<ul style="list-style-type: none"> ● 访谈项目验收相关人员，了解项目收尾相关情况 ● 取得项目验收相关材料，检查材料编写的规范性、内容的合理性和全面性
工程方法审计	<ul style="list-style-type: none"> ● 是否真实地进行了可行性调研 ● 可行性阶段产生文档是否合理 ● 是否对系统实施的技术方案和方法进行过论证 ● 是否编制项目需求计划？内容是否全面、合理 	<ul style="list-style-type: none"> ● 访谈相关人员了解项目可行性研究情况 ● 取得项目投资报告及其审批文档，检查手续费的规范性、完整性 ● 检查信息来源的真实性及内容的合理性

(续表)

类别	审计内容	审计方法
工程方法审计	<ul style="list-style-type: none"> ● 是否编制概要设计文档？内容是否全面合理 ● 是否进行产品技术方案选型 ● 是否制定编码规范？内容是否全面合理 ● 是否每个开发人员都熟悉编码规范 ● 是否制订测试计划 ● 测试计划的内容是否全面、合理 ● 上线前是否对系统进行了确认测试，填写业务测试验收文档？是否得到客户的确认 ● 是否有系统运行的日志 	<ul style="list-style-type: none"> ● 取得项目技术方案及其论证文档，检查对系统实施的技术方案和方法论证内容的全面性、合理性 ● 访谈相关人员，了解项目需求计划制订情况 ● 取得项目需求计划及评审、批准的相关记录 ● 检查项目需求计划的内容是否全面合理

3.3 本章练习

1. 选择题

(1) “计算机硬件故障或软件不足，易造成信息的损坏和丢失，导致数据处理过程中发生偶发错误”，描述的风险类型是_____。

- A. 固有风险 B. 控制风险 C. 检查风险 D. 审计风险

参考答案：A

(2) _____指审计人员在审计实施阶段为执行具体审计程序所形成的审计工作底稿。

- A. 综合类工作底稿 B. 业务类工作底稿
C. 备查类工作底稿 D. 技术类工作底稿

参考答案：B

(3) 关于 IT 审计范围的描述，不正确的是：_____。

- A. 总体范围需要根据审计目的和投入的审计成本来确定
B. 组织范围需明确审计涉及的组织机构、主要的流程、活动及人员等
C. 逻辑范围需明确涉及的信息系统
D. 物理范围需明确具体的物理地点与边界

参考答案：C

(4) 组织外包其软件开发，_____是该组织 IT 管理的责任。

- A. 作为开发人员参加系统设计 B. 支付服务提供商
C. 与服务提供商谈判合同 D. 控制服务提供商遵守服务合同

参考答案：D

(5) _____不属于 IT 治理的三大主要目标。

- A. 与业务目标一致 B. 质量控制
C. 有效利用信息与数据资源 D. 风险管理

参考答案：B

(6)《信息技术服务治理 第1部分：通用要求》标准不适用于_____。

- A. 建立组织的IT治理体系并实施自我评价
- B. 组织的IT治理能力进行自我评价
- C. 研发、选择和评价IT治理相关的软件或解决方案
- D. 开展信息技术审计

参考答案：B

(7) COBIT[®] 2019核心模型中的治理和管理目标分为五个领域，_____领域是由董事会和执行管理层负责。

- A. 评估、指导和监控(EDM)
- B. 调整、规划和组织(APO)
- C. 内部构建、外部采购和实施(BAI)
- D. 交付、服务和支持(DSS)

参考答案：A

2. 思考题

(1) IT治理的管理层次可分为三层：最高管理层、执行管理层、业务与服务执行层，请简要描述这3个层次的主要职责分别是什么？

参考答案：略

(2) IT治理的核心内容包括哪6个方面，请简述？

参考答案：略

(3) 请指出IT审计的常用方法，并根据你的理解举例说明信息系统项目管理可能使用的方法及具体运用。

参考答案：略

第4章 信息系统管理

在信息技术和数据资源要素的推动下，社会各领域已经并正在加速进入数字化的全新发展时期，基于智能、网络和大数据的新经济业态正在形成，从“数字融合”向“数字原生”的发展是这个时期的主要特征，表现为信息技术和工业制造深度融合、人和机器的融合、信息资源和材料资源的融合等，进而基于这种深度融合所构造的数字化新世界，将引发社会各个领域为完全适应数字世界而产生各种数字原生发展模式，这些模式将不断诞生、发展、凋亡和重塑，从而极大地改变了人们的生活方式和行为模式。这个进程是一场比过往的工业化和信息化更加广泛的社会变革。支撑这场变革的重要基础，是不断与社会发展各方面深度融合的信息系统，只有对信息系统实施有效管理，才能承担变革赋予的重任。

4.1 管理方法

信息系统管理是一项需要组织各层级充分参与的业务运行工作。大多数组织都拥有专门用于信息系统管理的职能部门，这些部门配备了相关技术领域的高技能专业人员。同时，组织的管理者也需要了解并参与相关的决策。

4.1.1 管理基础

对信息的高效管理与利用，是在新时代发展环境中取得成功的关键技能。现代化组织做出的所有决策在某种程度上都与信息系统的管理和使用密切相关。对管理者来说，了解其组织能力和信息的开发利用，与懂得如何获取金融资源和平衡预算一样至关重要。随着智能手机、笔记本电脑和平板电脑等个人设备的广泛使用，通过互联网访问组织内外部的应用程序以执行日常工作和业务动作的频度越来越高，凸显了“技术底座构成了几乎所有业务模式的支柱”这一事实。当这种技术底座具备全球可达的特性时，对管理者的技能又增加了全球化能力的要求。基于信息系统技术底座，协作工具和数字化引擎的可用性产生了变化，即信息系统与业务流程日益集成，逐渐变成业务流程演变的革命性因素。迫切需要组织管理者参与技术决策，以确保信息系统对业务的正向支撑，并避免技术的负面影响。

1. 层次结构

信息系统是对信息进行采集、处理、存储、管理和检索，形成组织中的信息流动和处理，必要时能向有关人员提供有用信息的系统。它是由人、技术、流程和数据资源组成的人机系统，目的是及时、正确地收集、加工、存储、传递和提供信息，以实现组织中各项活动的管理、调节和控制。信息系统是为组织用来生产和管理信息（数据）的技术（“什么”）、人员（“谁”）和过程（“如何”）的组合。信息系统包括四个要素：人员、技术、流程和数据，如图 4-1 所示。

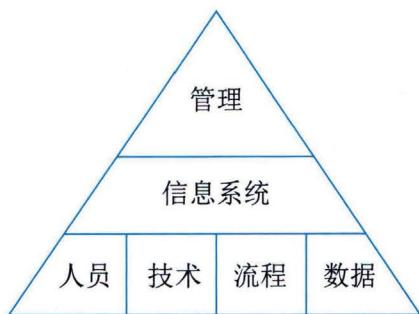


图 4-1 信息系统层次架构

在信息系统层次架构中，信息系统之上是管理，它监督系统的设计和结构，并监控其整体性能。同时，组织管理层制定信息系统层应满足的业务需求和业务战略。信息系统层次架构提供了一个蓝图，可以将业务和系统策略转换为组件或基础架构，并以恰当的人员、技术、流程和数据组合加以实现。

2. 系统管理

信息系统的管理需要提高各组织管理人员对信息系统相关问题的认识。信息技术及其系统在本质上都具有矛盾性，一方面具备前瞻性，不可或缺，因为它们为充满潜力的创新（大数据、人工智能和万物互联等）铺平了道路。另一方面则是主要漏洞（网络安全、数字化和隐私丧失等）的载体，且目前难以衡量其范围和后果。这就是为什么信息系统的管理越来越重要且必要的原因。除了纯粹的运行问题之外，还可以清楚地看到信息系统的管理与道德问题，以及其与世界的复杂性的关联程度越来越密切。基于信息系统构建和执行业务部门的流程，越来越多地限制了价值链中利益干系人之间的关系，那么关于信息系统的决策就会越来越对战略产生影响。一旦信息系统的影响不再局限于工作效率和劳动强度，将不断地为个人空间提供连续性的能力，信息系统的决策也会对每个人产生影响。

信息系统管理覆盖四大领域：

- 规划和组织：针对信息系统的整体组织、战略和支持活动。
- 设计和实施：针对信息系统解决方案的定义、采购和实施，以及他们与业务流程的整合。
- 运维和服务：针对信息系统服务的运行交付和支持，包括安全。
- 优化和持续改进：针对信息系统的性能监控及其于内部性能目标、内部控制目标和外部要求的一致性管理。

4.1.2 规划和组织

信息系统的规划和组织需要根据组织的发展目标和其他相关因素规划信息系统的战略、组成、建设、运行和运营等。目标是通过实施具备一致性的管理方法，满足业务对信息系统的管理需求。规划和组织的相关内容涵盖信息系统管理所需的所有组件，如：管理流程与组织结构的执行，角色和职责的部署管理，可靠且可重复的活动规范，信息化项目的执行，技能和能力的建设优化，以及服务、基础设施和应用程序的运行管理等。

1. 规划模型

战略是实现目标、意图和目的的一组协调行动。战略往往始于使命，而使命是对组织的宗旨给出的一个清晰并令人信服的陈述。信息系统战略三角突出了业务战略、信息系统和组织机制之间的必要一致性，如图 4-2 所示。它用于描述信息系统与业务系统必要的协同关系，以及理解信息系统与组织机制间的相互影响。当业务战略、组织机制与信息系统运转良好时，这种多方战略决策的一致性往往很难被组织认知。但是，当发生重大生产事故和灾难时，在规划一

项业务时，需要正确调整业务战略、信息系统和组织机制之间的协同实践。

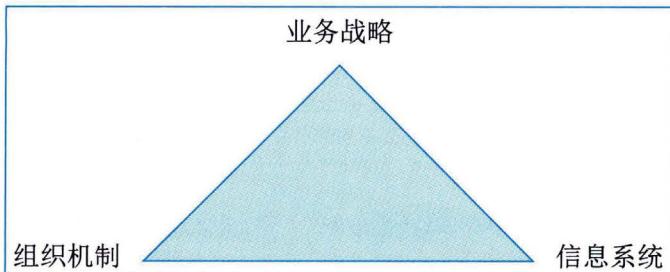


图 4-2 信息系统战略三角

成功的组织有一个压倒一切的业务战略，可以推动组织机制和信息系统的有机融合。有关组织机制的结构、招聘实践和其他组成部分的决策，以及有关应用程序、硬件和其他信息系统组件的决策，都是由组织的业务目标、总体战略与战术驱动的。成功的组织会仔细平衡信息系统战略三角，对自己的组织和信息系统战略进行细致规划，以补充其业务战略。

信息系统战略本身可以影响并受到组织业务和组织机制战略变化的影响。为了保持成功运行所需的平衡，信息系统战略的改变必然伴随着组织机制战略的变化，并且必须适应整体业务战略。如果组织在规划其业务战略时利用信息系统来获得战略优势，那么信息系统的领导地位必须通过不断创新来维持。业务、信息和组织机制战略需要不断进行动态调整。

信息系统战略总是涉及业务和组织机制战略造成的影响。信息系统规划时应努力避免有害的意外后果，这意味着在设计信息系统部署时要记住所需考虑的业务和组织策略。例如，信息系统部署并期望员工使用平板电脑提升生产率，但没有对职位描述、流程设计、薪酬计划和业务策略等进行一系列变更，将无法产生预期的生产力改进。信息系统的这类调整只有通过专门设计战略三角的所有三个组成部分才能取得成功。

2. 组织模型

观察历史上曾经发生的重大系统失效灾难，常常发现信息系统战略三角在灾难发生时会出现协同方面的问题。例如：组织机制战略（例如，关于系统运行监测、测试和相应的人事策略、安全策略和实践）不支持信息系统战略（例如，在危机情况下实施监测，管理和中止自动化生产过程的分布式系统网络的运行机制）。而这意味着上述两种策略在规划时都没有充分支持组织的业务战略。而实现三种战略的协同，达成三种战略的一致性代表实现了三角之间的平衡，在一致性基础上，可以向同步与融合方向发展。通过同步，技术不仅可以支撑实现当前的业务战略，还可以预测和塑造未来的业务战略。而融合更进一步，业务战略和信息战略交织在一起，管理团队成员甚至可以互换运作。

1) 业务战略

业务战略阐明了组织寻求的业务目标以及期望如何达成的路径。业务战略是组织传达宣示其目的的方法。管理层根据经济与社会情况、产品与服务对象需求和组织能力构建业务战略计划。经济与社会情况为该类业务构建了竞争环境。产品与服务对象需求是个人及组织想要和需要的可用产品和服务。组织能力包括知识、技能和经验，这些知识、技能和经验为组织提供了

一种可以在经济与社会中增加价值的能力。

描述业务战略的经典框架是迈克尔·波特（Michael E. Porter, 1947—）提出的竞争力优势模型，如图 4-3 所示。



图 4-3 获得竞争力优势的三种战略

当组织的目标是成为市场上成本最低的生产者时，总成本领先战略就会产生。采用该战略的组织通过最大限度地降低成本，从而获得高于平均水平的绩效。所提供的产品或服务必须在质量上与业内其他人提供的产品或服务相当，以便客户对象感知其相对高性价比。通常，一个行业中只存在一个成本引领者。

采用差异性战略时，组织通过差异化，以一种在市场上显得独特的方式，定义其产品或服务。组织确定哪些定性维度对其客户对象最重要，然后找到在其中一个或多个维度增加产品和服务价值的方法。为了使此策略起作用，差异化因素向客户对象收取的价格必须相对于竞争对手收取的价格，是公平的。

采用专业化战略时，专业化允许组织将其范围限制在更狭窄的细分市场，并为该组客户对象量身定制其产品。该策略有两种变体：①专注成本，在其细分市场内寻求成本优势；②专注差异化，寻求细分市场内的产品或服务的差异化。这种策略使组织能够实现区域竞争优势，即使它没有在整个经济与社会中实现竞争优势，也可以通过专注于某些细分市场的方式获得局部的竞争优势。

2) 组织机制战略

组织机制战略包括组织的设计以及为定义、设置、协调和控制其工作流程而做出的选择。组织机制战略本质上需要回答“组织将如何构建以实现其目标并实施其业务战略”这一问题，并围绕这一问题形成有效的规划。理解组织设计的经典框架是哈罗德·莱维特（Harold J. Leavitt,

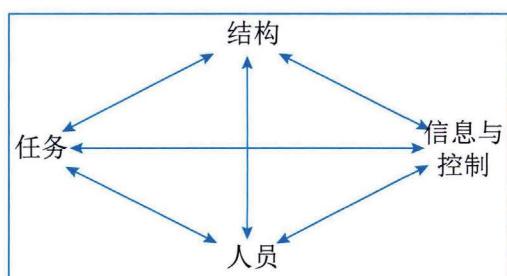


图 4-4 莱维特钻石模型

1922—2007）提出的钻石模型，如图 4-4 所示。钻石模型将组织计划的关键组成部分标识为其信息与控制、人员、结构和任务，所有组件都是相互关联的。这个简单的框架对于设计新组织和诊断组织问题非常有用。例如，试图改变员工但未能改变其信息与控制方式的组织无法有效运行，因为所有这些组件都会相互影响。

新时代的组织，其组织机制战略的成功执行包括组织、控制和文化的变量的最佳组合。组织变量包括决策权、业务流程、正式报告关系和非正式沟通网络。控制变量包括数据的可得性、规划的性质和质量、业绩计量和评价制度的有效性以及做好工作的激励措施。文化变量构成组织的价值观。这些组织、控制和文化的变量是决策者用来影响组织变革的管理杠杆。

组织管理人员应具备一套框架，用于评估组织设计的各个方面。使用这些框架，管理人员可以审查当前的组织，并评估哪些组件可能缺失以及未来有哪些可用的选项。基于此框架，管理人员应回答如下问题：

- 组织内有哪些重要的结构和报告关系；
- 谁拥有关键决策的决策权；
- 什么是重要的以人为本的网络（社交和信息网络），我们如何利用它们来更好地完成工作；
- 组织内人员的特征、经验和技能水平是什么；
- 关键业务流程是什么；
- 有哪些控制系统（管理和测量系统）到位；
- 组织的文化、价值观和信仰是什么。

3) 信息系统战略

信息系统战略是组织用来提供信息服务的计划。信息系统支撑组织实施其业务战略。业务战略是关于竞争（服务对象想要什么，竞争做什么），定位（组织想以什么方式竞争）和能力（公司能做什么）的功能。信息系统帮助确定组织的能力。现在使用一个基本的矩阵框架来理解组织必须做出的与信息系统相关的决策，如表 4-1 所示。

表 4-1 信息系统战略矩阵

	有什么	谁使用	在哪里
硬件	信息系统的物理组件清单	系统用户和管理者	组件的物理位置（云端、数据中心等）
软件	程序、应用和工具的清单	系统用户和管理者	软件驻留的硬件，以及硬件的物理位置
网络	硬件和软件组件如何联接的图表	系统用户和管理者；提供服务的组织	节点、线路和其他传输介质所在地
数据	系统中存储的信息位	数据所有者；数据管理者	信息所在地

矩阵框架的目的是为管理者提供一个信息系统组件与策略间关系的观察视图，整体信息系统的四个基础结构组件与其他资源相关事项之间的关系构成了信息系统战略的关键点。基础结构包括：①硬件，如桌面单元和服务器；②软件，如用于开展业务，管理计算机本身以及在系统之间进行通信的程序；③网络，它是硬件组件之间交换信息的物理手段，例如通过专用数字网络实现信息交换；④数据，数据包括存储在系统中的位和字节。在当前的系统中，数据不一定与使用它们的程序一起存储；因此，了解系统中有哪些数据以及它们的存储位置非常重要。

4.1.3 设计和实施

开展信息系统设计和实施，首先需要将业务需求转换为信息系统架构，信息系统架构为将组织业务战略转换为信息系统的计划提供了蓝图。信息系统是支持组织中信息流动和处理的所有基础，包括硬件、软件、数据和网络组件，并以最适合计划的方式进行选择和组装，因此其最能体现组织总体业务战略。

1. 设计方法

大量的可选信息技术，加上技术快速进步，使得组织完成信息系统的建设似乎成为“不可完成的任务”。这就需要组织首先将业务战略转化为信息系统架构，然后将该架构转化为信息系统设计，如图 4-5 所示。

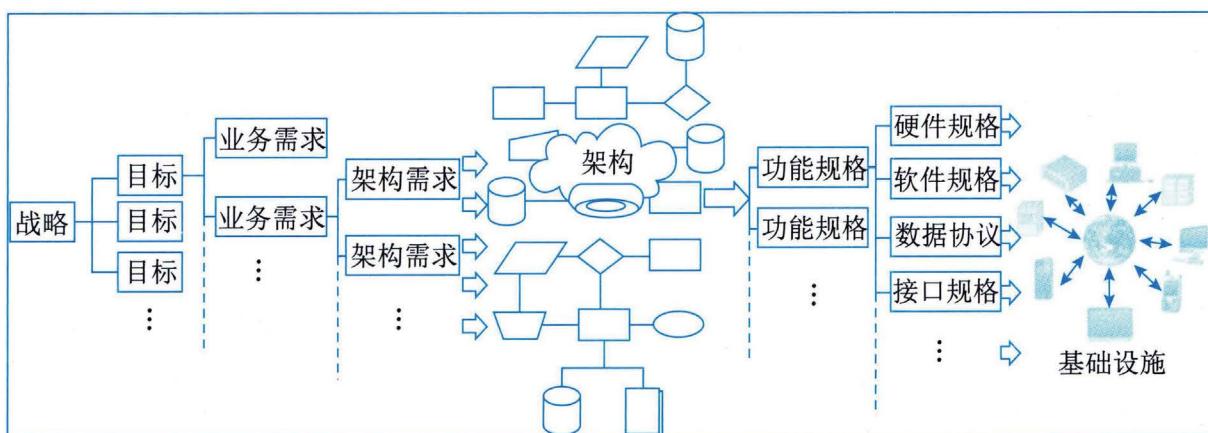


图 4-5 从战略到信息系统设计转换示意图

1) 从战略到系统架构

组织必须从业务战略开始，使用该战略制定更具体的目标。然后从每个目标派生出详细的业务需求。组织需要与架构设计人员合作，将这些业务需求转换为构成信息系统架构的系统要求、标准和流程的更详细视图。这个更详细的视图，即信息系统架构要求，包括考虑数据和流程需求以及安全目标等事项。组织还可以向架构设计人员清楚地了解信息系统必须完成的工作以及确保其顺利开发、实施和使用所需的治理安排。治理安排指定组织中哪个人保留对信息系统的控制权和责任。

2) 从系统架构到系统设计

将信息系统架构转换为系统设计时，需要继承信息系统架构并添加更多细节，包括实际的硬件、数据、网络和软件。进而扩展到数据的位置和访问过程、防火墙的位置、链路规范、互联设计等。信息系统架构被转换为功能规格。功能规格可以分为硬件规格、软件规格、存储规格、接口规格、网络规格等。然后决定如何实现这些规范，并在信息系统基础架构中使用什么硬件、软件、存储、接口、网络等。

信息系统指的不仅仅是组件，这些组件必须根据设计蓝图进行组装，硬件、软件、数据和网络必须以一致的模式组合在一起，才能拥有可行的信息系统。信息系统具有多个级别：①全

局级别可能侧重于整个组织，并构成整个组织的信息环境；②组织间级别信息系统则为跨组织边界的服务对象、供应商或其他利益干系人的沟通交流奠定基础；③应用级信息系统是在考虑特定业务应用时，通常重点考虑的数据库和程序组件，以及它们运行的设备和操作环境。

3) 转换框架

转换框架将业务战略转化为信息系统架构进而转变为信息系统设计，转换框架提出了三类问题：内容、人员和位置，需要为每个信息系统组件回答这些问题。“内容”相关问题是常被问到的，需要回答组件是什么，并确定特定类型的技术等。“人员”相关问题旨在了解相关组件涉及哪些个人、团体和部门。例如，在大多数情况下，单个用户并非系统的所有者；在另外情况下，系统也可能由组织租赁，而不是拥有，这样系统的所有者就成为了组织的外部一方。第三类问题涉及“何处”，随着网络的激增，许多信息系统的建设可能跨越多个位置使用组件，了解信息系统意味着需要了解所有内容各自的位置，如表 4-2 所示。

表 4-2 信息系统架构与基础设施分析框架举例

组件	有什么		谁使用		在哪里	
	系统架构	系统设计	系统架构	系统设计	系统架构	系统设计
硬件	用户将使用什么类型的个人设备	笔记本电脑配备什么尺寸的硬盘驱动器	谁最了解组织中的服务器	谁将运营服务器	架构需要集中式还是分布式服务器	将在 C 地数据中心放置哪些特定的计算机
软件	业务战略是否需要 ERP 软件支持	应该选择 A 品牌还是 B 品牌应用	谁会受到系统向 B 品牌迁移的影响	谁需要 B 品牌的系统培训	组织的地理状况是否需要部署多个数据库基础设施	可以使用一个 D 品牌云数据库实例作为系统数据库吗
网络	需要多大带宽来实现战略	E 单位交换机能否满足需要	哪些人需要连接到网络	无线网络是谁提供的	是否允许每一个用户的手机成为无线接入热点	是否会租赁线缆或使用卫星来支持通信
数据	销售管理系统需要哪些数据	使用什么格式存储数据	哪些人需要访问敏感数据	授权用户如何识别他们自己	备份数据是现场存储还是异地存储	数据是存放于云端系统还是存放于自己的数据中心

2. 架构模式

传统上，信息系统体系架构有三种常见模式（见表 4-3）：①集中式架构。集中式架构下所有内容采用集中建设、支持和管理的模式，其主体系统通常部署于数据中心，以消除管理物理分离的基础设施带来的困难。②分布式架构。硬件、软件、网络和数据的部署方式是在多台小型计算机、服务器和设备之间分配处理能力和应用功能，这些设施严重依赖于网络将它们连接在一起。③面向服务的系统架构（Service-Oriented Architecture, SOA）。SOA 架构中使用的软件通常被引向软件即服务（Software-as-a-Service, SaaS）的相关架构，同时，这些应用程序在通过互联网交付时也被称为 Web 服务。

表 4-3 常见信息系统架构模式

系统架构	描述	别称术语	什么时候使用
集中式架构	大型中央计算机系统处理系统的所有功能。通常，计算机位于数据中心，并由 IT 部门直接管理。存储的数据和应用程序都运行于中央计算机上。网络连接允许用户从远程位置访问大型机	主机架构	当需要系统易于管理时：所有功能都在同一个地方；当业务本身高度集中的时候
分布式架构	运行业务所需的计算能力分散在许多设备中，包括不同位置的服务器、PC 和笔记本电脑、智能手机和平板电脑。设备（有时也被称为客户端）具有足够的处理能力来执行所需的许多服务，并根据数据和专用服务的需要连接中央服务器	基于服务器的架构	当担心可伸缩性时，模块化在这里会有所帮助；当业务主要是非集中化的时候
面向服务的架构	在被称为编排的过程中，将较大的软件程序分解为相互连接的服务。基于此，它们共同构成了一个应用来运行整个业务流程。通常，这些服务可从互联网上的一系列供应商处获得，而应用程序则是这些服务链接在一起形成的组合	基于 Web 的架构	当希望系统成为敏捷架构：可重用性和组件化利于创造新应用；当业务对新应用和快速设计迭代要求较高时

组织在考虑集中式与分布式架构决策时，必须注意权衡与取舍。例如，分布式架构比集中式架构更加模块化，允许相对容易地添加其他服务器，并能为特定用户添加具有特定功能的客户端，从而提供更大的灵活性和多中心化的组织治理机制，这有可能令架构决策与组织治理目标更协调。相比之下，集中式体系架构在某些方面更易于管理，因为所有功能都集中在主机或小型机中，而不是分布在所有设备和服务器中。集中式架构往往更适合具有高度集中式治理的组织。而 SOA 则越来越受欢迎，因为该设计允许几乎完全从现有的软件服务组件构建大型功能单元。它对于快速构建应用程序非常有用，因为它为管理人员提供了模块化和组件化设计，是一种更易于变更的构建应用程序的方法。

4.1.4 运维和服务

信息系统的运维和服务应从信息系统运行的视角进行整合性的统筹规划，包括对信息系统、应用程序和基础设施的日常控制进行综合管理，以有效支持组织目标达成和流程实现。信息系统的运维和服务由各类管理活动组成，主要包括：运行管理和控制、IT 服务管理、运行与监控、终端侧管理、程序库管理、安全管理、介质控制和数据管理等。

1. 运行管理和控制

IT 团队发生的所有活动都应受到管理和控制。这意味着操作人员执行的所有操作和活动，都应是由管理层批准的控件、过程和项目的一部分。过程和项目应具有足够的记录保存，以便管理层能够了解这些活动的状态。管理层最终负责信息系统运行团队发生的所有活动。管理信息系统运行的管理控制主要活动包括：

- 过程开发：操作人员执行的重复性活动应以过程的形式记录下来，需要开发、审查和批准描述每个过程及其每个步骤的相关文档，并将其提供给运营人员。