内 容 简 介

本书是由工业和信息化部教育与考试中心组织编写的考试用书。本书根据《信息系统管理工程师考试大纲》（2024 年审定通过）编写，对信息系统管理工程师岗位所要求的主要知识以及应用技术做了阐述。

本书主要内容包括信息化发展、信息技术发展、信息系统架构、信息系统治理、信息技术服务管理、软件开发过程管理、系统集成实施管理、信息系统运维管理、云服务及其运营管理、项目管理、应用系统管理、网络系统管理、数据中心管理、桌面与外设管理、数据管理、信息安全管理、人员管理、知识管理、IT 管理标准化、职业素养与法律法规。

本书可作为信息系统管理工程师资格考试的教材，也可以作为信息化教育的培训和辅导用书，还可以作为高等院校信息管理专业的教学和参考用书。由于书中提供的一些技术、工具和方法具有较强的实践性，本书也能够作为在职人员的工具用书。

图书在版编目 (CIP) 数据

信息系统管理工程师教程 / 李超 , 岳素林主编 . —2 版 .
北京：清华大学出版社 , 2024. 9. —（全国计算机技术与软件专业技术资格（水平）考试用书）. — ISBN 978-7-302-67362-0

Ⅰ . C931.6

中国国家版本馆 CIP 数据核字第 202493VT42 号

责任编辑：杨如林　邓甄臻
封面设计：杨玉兰
版式设计：方加青
责任校对：徐俊伟
责任印制：

出版发行：清华大学出版社
网　　址：https://www.tup.com.cn，https://www.wqxuetang.com
地　　址：北京清华大学学研大厦 A 座　　**邮　　编：**100084
社 总 机：010-83470000　　**邮　　购：**010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 装 者：
经　　销：全国新华书店
开　　本：185mm×230mm　　**印　张：**41.25　　**字　数：**980 千字
版　　次：2006 年 1 月第 1 版　　2024 年 10 月第 2 版　　**印　次：**2024 年 10 月第 1 次印刷
定　　价：159.00 元

产品编号：107479-01

前　言

计算机技术与软件专业技术资格（水平）考试（以下简称软考）通过以考代评为我国信息技术及其应用创新领域培育了大量的专业技术人才，这些人才在新时代建设与发展过程中，发挥了重要作用，有力地支撑了各行业多领域的创新发展和转型升级，为各类组织的持续高质量发展作出了积极贡献。

信息系统的有序建设、稳定运行和安全可靠等，不仅是新时代组织转型升级的基础，也是其创新发展的关键，为其紧抓时代脉搏，乃至引领时代发展，提供了重要的环境支撑。随着信息技术与组织业务的深度融合，以及数据作为新生产要素的快速发展，信息系统的重要程度和对其的重视程度被提到了新的高度。同时，信息技术的高速发展，以及信息系统部署与运行模式的多元化等，给信息系统管理和持续发展带来了诸多挑战，科学高效的信息系统管理已经成为组织在新时代关键能力建设的重要组成部分。

信息系统管理不仅涉及众多知识领域，还关联多个管理域，需要进行多维度立体化建设。信息系统管理覆盖了信息技术、信息化、数字化转型等整体发展战略，IT 治理、项目管理、集成实施、IT 服务、IT 运维等信息系统全生命周期体系化管控，云服务、应用系统、数据中心、数据资源、网络、桌面与外设、信息安全等领域的运行管理，以及人员、知识、标准化等关键能力支撑等内容。信息系统管理工程师需要在充分掌握相关知识和技术的基础上，结合组织的不同发展阶段、不同发展环境等，在信息系统发展目标的牵引下，因地制宜、因势利导地持续改进管理措施、落实管理要求、实施技术操作等，从而确保组织的信息系统高可用和各项管理活动的高效等。

随着“数字中国”等国家战略的深度推进，组织的信息系统无论是数量、可靠性需求、部署方法，还是迭代升级模式等都发生了巨大变化，局部、单项建设与管理等，被体系化建设、服务化管理和敏捷化升级所替代，相对单一的管理模式走向了多元融合模式，信息系统管理需要持续适应新的发展需求。2024 年为了适应新技术、新方法、新思想的需求以及信息系统管理领域的发展需要，工业和信息化部教育与考试中心广泛吸纳当前最新的研究成果，在原大纲的基础上，组织专家对《信息系统管理工程师考试大纲》进行了较大幅度的修改，更新了信息化发展、信息技术等信息系统基础的知识要求，增强了信息系统治理、系统架构、服务管理、运行维护、集成实施、项目管理等方面的知识要求，并结合新一代信息技术，针对各类信息系统管理对象，更新、丰富和完善了信息系统管理相关知识体系的要求，以及以体系化能力建设为目标，强化了人员、知识等方面的知识要求，更新、丰富和完善了信息系统管理相关标准与法律法规的要求。

依据新修订的《信息系统管理工程师考试大纲》（2024 年审定通过），工业和信息化部教育与考试中心组织专家对《信息系统管理工程师教程》（以下简称教程）进行了修订。针对信息化和信息技术等基础知识的论述尽量兼顾最新发展情况及成熟的技术基础。针对信息系统建设与

运行的全生命周期部分，采用从治理到管理、从总体到分项的模式进行论述，力求确保管控、管理、操作的层次化和立体化。针对管理对象部分，充分借鉴了我国信息技术服务标准化工作的成果，重点考虑执行的全面性，同时兼顾标识的一致性，强调对全生命周期管理的承接和一体化。将能力建设作为信息系统各项活动的关注重点，在各项管理中的人员管理和知识管理的基础上，增加了这些内容的体系化知识。

另外，为了便于参加软考的专业技术人员复习应考，修订教程为每章提供了相应的练习题。

第 1 章信息化发展由吴庆云、冯浩、张树玲编写；第 2 章信息技术发展由李超、冯浩、张树玲编写；第 3 章信息系统架构由李美翠、吴庆云、冯浩编写；第 4 章信息系统治理由尹宏、董雷、李瑞鑫编写；第 5 章信息技术服务管理由李世喆、刘成江、刘玲编写；第 6 章软件开发过程管理由方春燕、孙佩、曾寰嵩、黄锋编写；第 7 章系统集成实施管理由肖筱华、曹峥、李美翠编写；第 8 章信息系统运维管理由郭鑫伟、刘成江、岳素林编写；第 9 章云服务及其运营管理由陈宏峰、张一恒、李超编写；第 10 章项目管理由张伟、陈和兰、王东东编写；第 11 章应用系统管理由唐百惠、张伟娜、刘玲编写；第 12 章网络系统管理由王伟、申雅辉、岳素林编写；第 13 章数据中心管理由熊健淞、岳素林、陈睿编写；第 14 章桌面与外设管理由郭浩、于浩、张淑忠编写；第 15 章数据管理由马宁、方春燕、张树玲编写；第 16 章信息安全管理由孙佩、董涛、刘玲编写；第 17 章人员管理由岳素林、赵翔、薛丽编写；第 18 章知识管理由邓金花、黄国彬、沈顺厚编写；第 19 章 IT 管理标准化由郭创、毛慧丽、刘莹编写；第 20 章职业素养与法律法规由李修仪、李超编写。

另外，李超、岳素林依据考试大纲对全书做了内容统筹、章节结构设计和统稿，吴庆云、李美翠、方春燕等参加了本书的策划以及部分章节的审校，李京、申雅辉、陈睿、马婧、张艺淼、刘莹、李晴参与了本书部分章节的审校工作。清华大学出版社为本书的编写做了大量的组织管理工作，在此表示感谢。

由于编者水平所限，书中难免有不当之处，恳请读者不吝赐教并提出宝贵意见，相信读者的反馈将会为本书的再次修订提供良好的帮助。

编　者

2024 年 8 月

目　录

第 4 章　信息系统治理

4.1　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定总体规划，但制定 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的过程中，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行为。随着时代的发展，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 的依赖性越来越强，IT 治理对组织愈发重要，为确保 IT 治理有效，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，为进一步进行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 治理的因素包括：①良好的 IT 治理能够确保组织 IT 投资的有效性；② IT 属于知识高度密集型领域，其价值发挥的弹性较大；③ IT 已经融入组织管理、运行、生产和交付等领域，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；⑤ IT 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；⑥ IT 价值不仅仅取决于好的技术，也需要良好的价值管理，及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 IT 每项管理中，需要采用明确责权和清晰管理的方式确保 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：① IT 治理作为组织上层管理的有机组成部分，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，体现了治理层和高级管理层对信息相关活动的关注；② IT 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；③ IT 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；④ IT 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；⑤ IT 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，以实现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，成为战略计划的重要组成部分，它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 团队在整个组织中的作用，最终能够针对不同的业务发展要求，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 治理的主要目标包括：与业务目标保持一致、有效利用信息与数据资源、风险管理。

（1）与业务目标保持一致。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，为进一步进行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。

（2）有效利用信息与数据资源。目前，信息系统工程超期、IT 客户的需求没有得到满足、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，新出现的技术没有进行管理，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自上而下贯彻执行，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。其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。业务与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。

4.2　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的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 治理的核心关注 IT 定位和信息化建设与数字化转型的责权划分。IT 治理体系的构成如图 4-1 所示，具体包括 IT 定位（IT 应用的期望行为与业务目标一致）、IT 组织架构（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（决策、投资、风险、绩效和管理等）、IT 治理流程（统筹、评估、指导、监督）、IT 治理效果（内外评价）等。

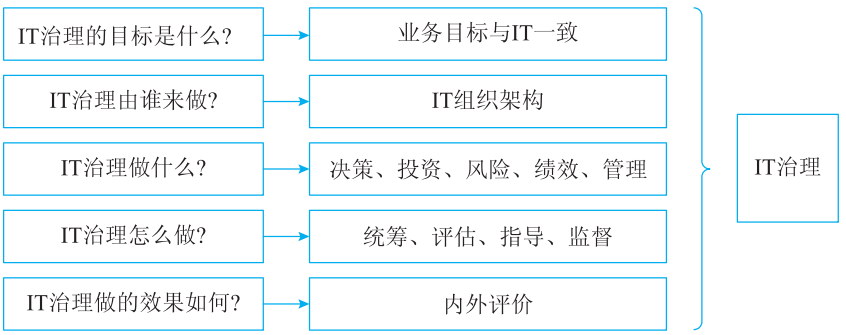

图 4-1　IT 治理体系的构成

1. IT 治理关键决策

有效的 IT 治理必须关注 5 项关键决策，如图 4-2 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的应用的构建，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。

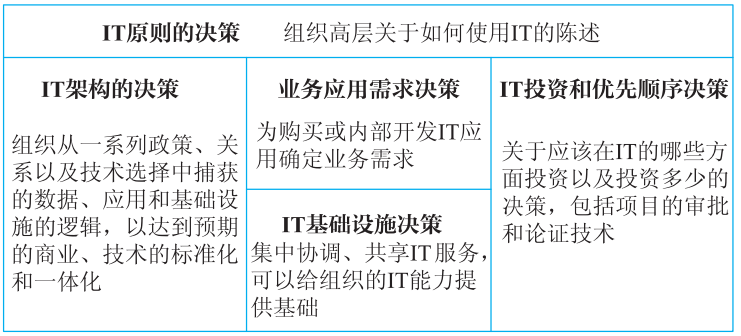

图 4-2 关键的 IT 治理决策

IT 决策过程中，需要关注各类关键问题，如表 4-1 所示。

表 4-1 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找到实施 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？组织级的投资与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，形成了一整套 IT 治理运行闭环，如图 4-3 所示。

（1）IT 战略目标。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。

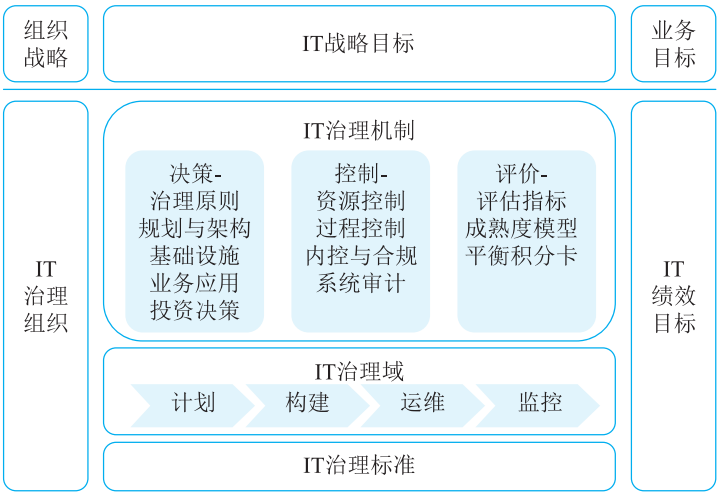

图 4-3　IT 治理体系框架

（2）IT 治理组织。界定组织中各相关主体在各自方面的治理范围、责权划分及其相互关系的准则，它的核心是治理组织（如 IT 治理委员会等）的设置和权限的划分，各治理组织职权的分配以及各机构间的相互协调，它的强弱直接影响治理的效率和效能，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 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“敏捷做决策”。其内容包括 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，它是组织实施 IT 治理的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；② IT 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 6 个方面，即组织职责、战略匹配、资源管理、价值交付、风险管理和绩效管理，如图 4-4 所示。

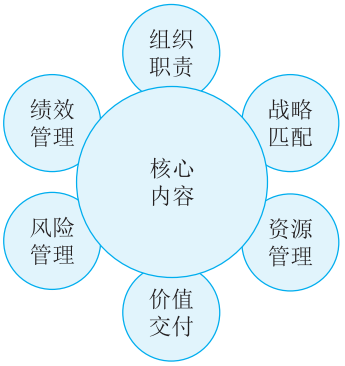

图 4-4　IT 治理核心内容

（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。价值交互就是创造业务价值。

（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。风险管理就是保护业务价值。

（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（如平衡计分卡）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 治理机制相关经验

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 4-2 所示。

IT 治理可以从众多最佳实践中学习的经验主要包括：

（1）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。

表 4-2　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
服务级别协议	对于 IT 服务的详细说明和衡量	专业的供应和需求	管理服务级别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，并通常运用平衡计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

（2）谨慎管理组织的 IT 架构和业务架构，以降低业务成本。

（3）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。

（4）建立集中化的 IT 团队，用以管理基础设施、架构和共享服务。

（5）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。

（6）设计需要对 IT 投资进行集中协作和核准的 IT 投资流程。

（7）设计简单的费用分摊和服务级别协议机制，以明确分配 IT 开支。

4.3　IT 治理任务

组织的 IT 治理活动定义为统筹、评估、指导和监督。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；评估信息技术应用与服务创新解决方案及措施等的有效性；指导 IT 管理实施、绩效考评、风险控制和业务创新；监督 IT 与业务的一致性、符合性及 IT 应用的合规性。组织开展 IT 治理活动的主要任务聚焦在如下 5 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。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 治理组织，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制定满足可持续发展的 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。这包括：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。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，明晰上下左右权力关系，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 的完整性、有效性和合规性；④监督由审计和管理评审提出的改进内容的实施。

（4）创新发展。创新发展指利用 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。

4.4 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，其中比较典型的是我国信息技术服务标准（Information Technology Service Standard，ITSS）库中的 IT 治理系列标准、信息和技术治理框架（COBIT）以及 IT 治理国际标准（ISO/IEC 38500）等。

1. ITSS 中的 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 4 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 4-5 所示。

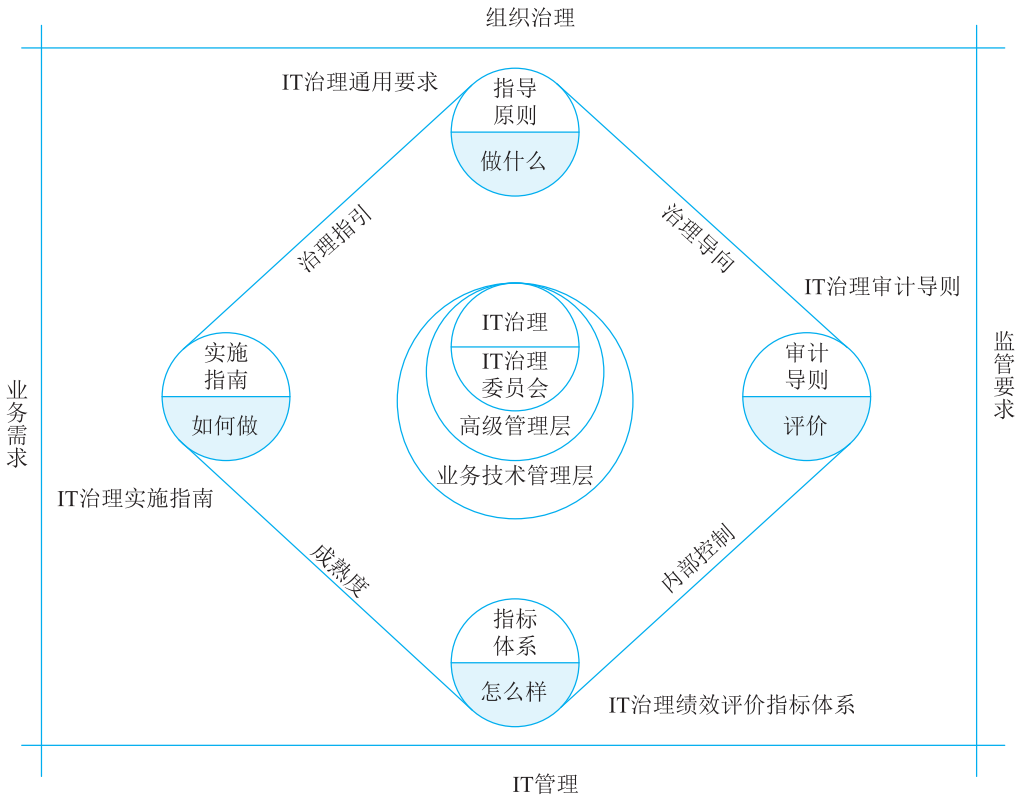

图 4-5　ITSS-IT 治理标准化的逻辑关系图

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 4-6 所示。

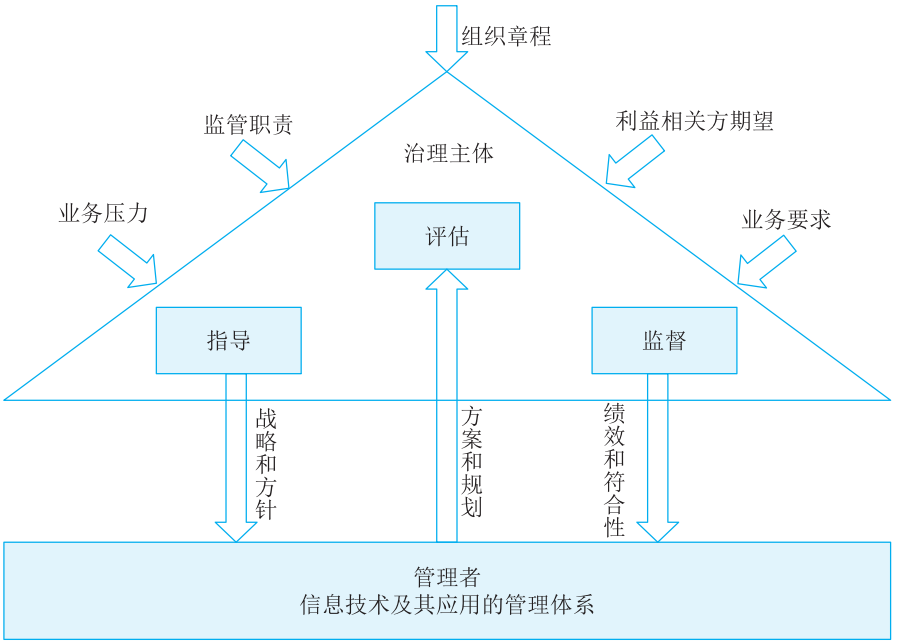

图 4-6　GB/T 34960.1 定义的 IT 治理模型

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。

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，每个治理域由若干治理要素组成，如图 4-7 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。

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 4-8 所示。实施环境包括

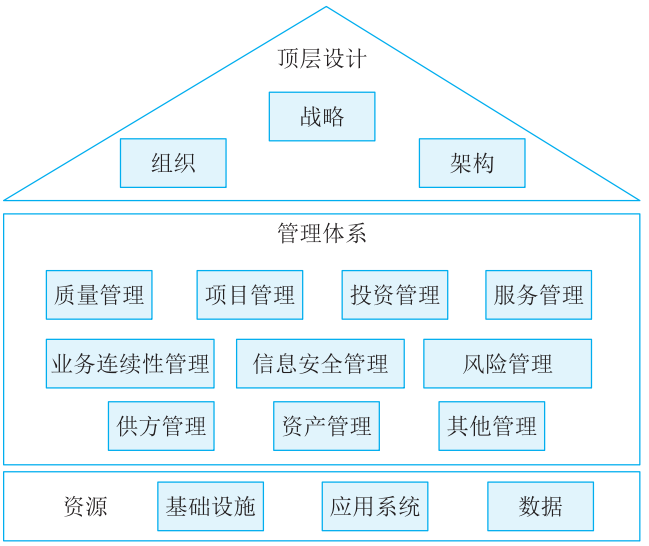

图 4-7　GB/T 34960.1 定义的 IT 治理框架

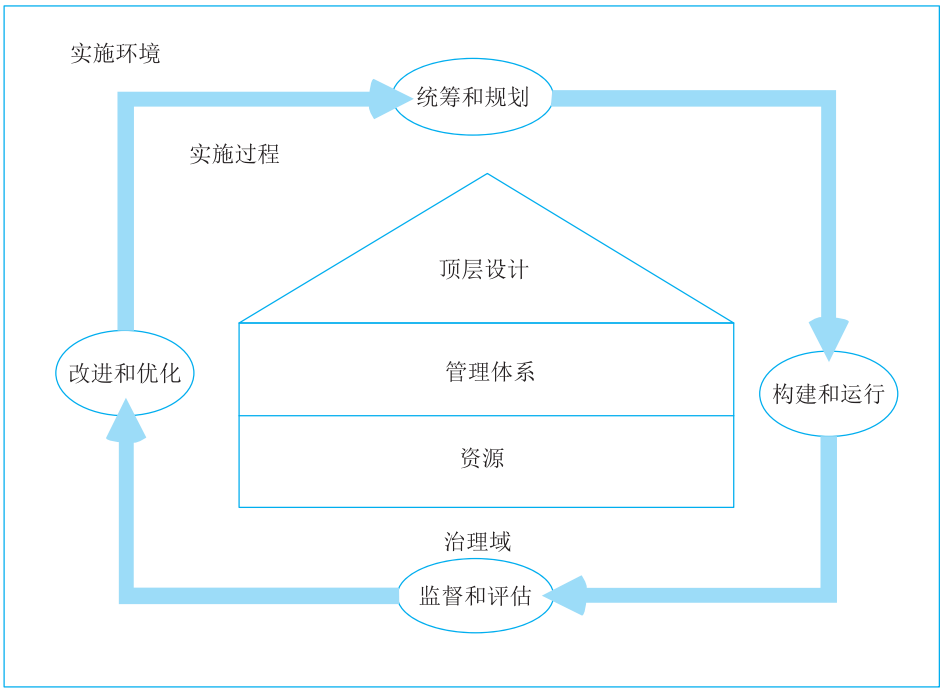

图 4-8　GB/T 34960.2 定义的 IT 治理实施框架

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。

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 年的国际信息系统审计协会（ISACA）组织设计并编制。COBIT 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，并服务于不同的目的。具体区别为：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 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 4-9 所示。在 COBIT 中治理目标被列入评估、指导和监控（EDM）领域，在这个领域，治理组织将评估战略方案、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 4 个领域：①调整、规划和组织（APO）领域针对 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）领域针对 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）领域针对 IT 服务的运营交付和支持，包括安全；④监控、评价和评估（MEA）领域针对 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。

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 4-10 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 治理系统的基础设施、技术和应用程序。

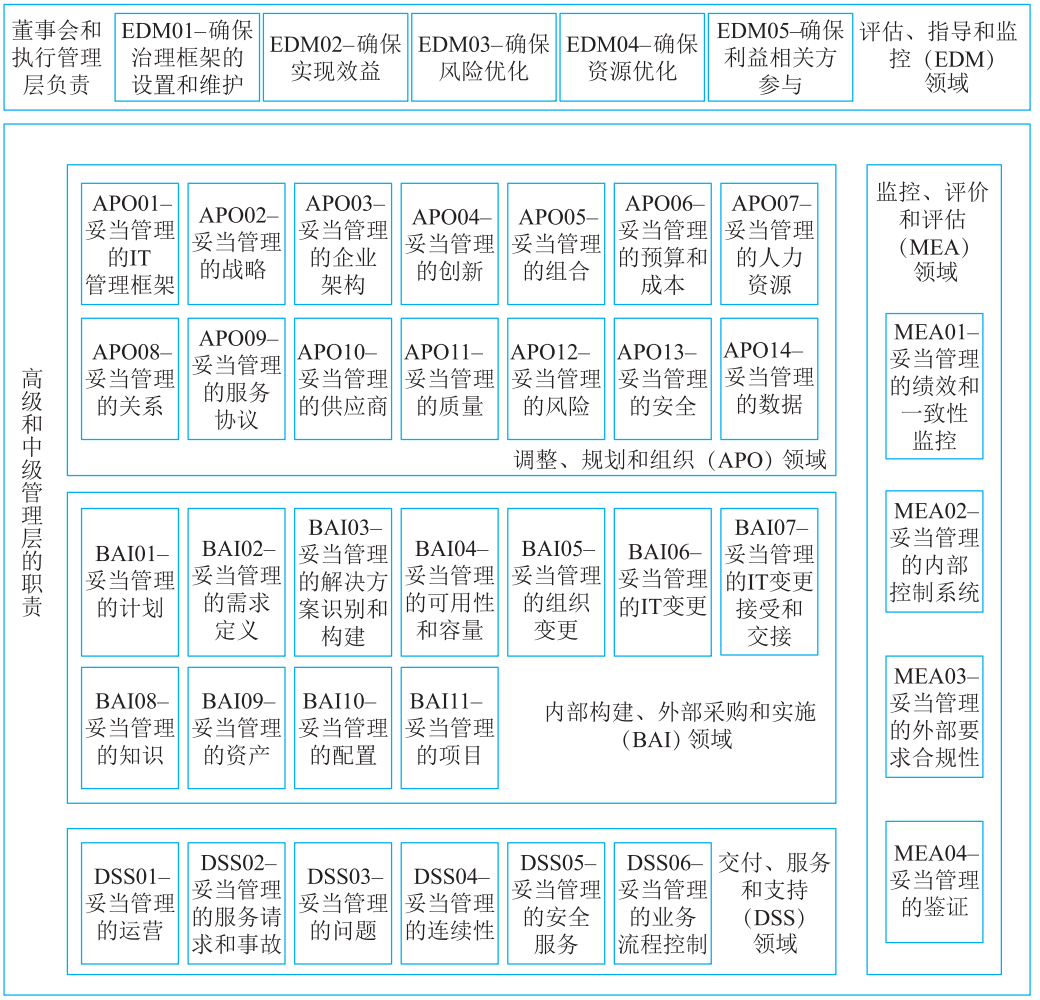

图 4-9　COBIT 核心模型

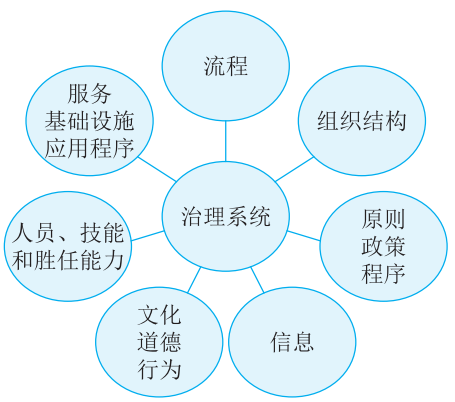

图 4-10　COBIT 治理系统组件

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 4-11 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。

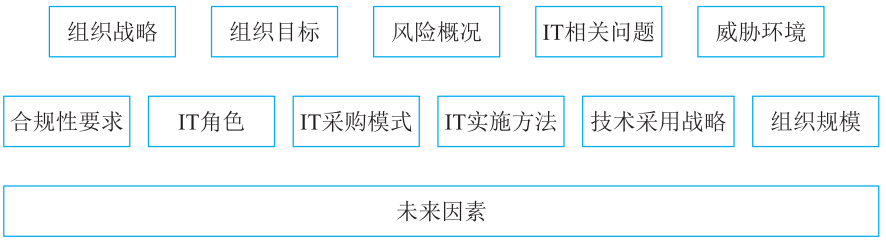

图 4-11　COBIT 定义的 IT 治理系统设计因素

组织开展治理系统设计通过流程化的方式进行，如图 4-12 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优化治理系统范围；④最终确定治理系统的设计。

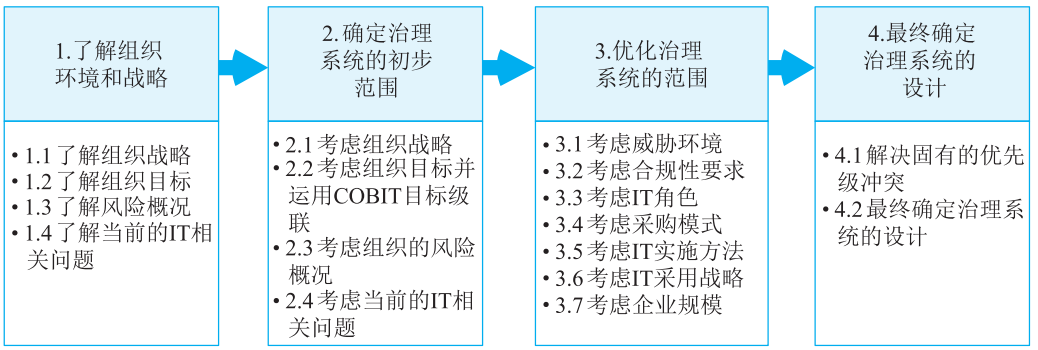

图 4-12　COBIT 治理系统设计工作流程

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 年第一版的 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内使用 IT 方面的法律、法规和道德义务。