COBIT 5（中文翻译版）

企业 IT 治理与管理框架

目录

插图索引

一. COBIT 5：一个治理和管理企业 IT 的业务框架

COBIT 5 出版物包含治理和管理企业 IT 的 COBIT 5 框架。本出版物是图表 1 所示的 COBIT 5 产品系列的一部分。

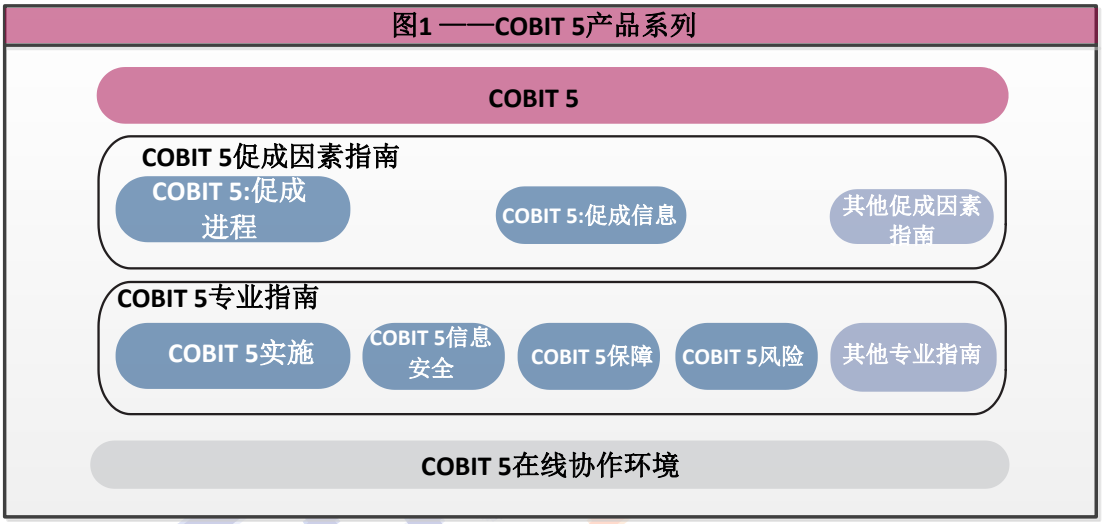

图 1.1　图表 1 COBIT 5 产品系列

COBIT5 框架基于 5 条基本原则，这些原则在其中有详细的描述，包括关于治理和管理企业 IT 的促成因素广泛的指导。

COBIT 5 产品系列包含以下产品：

- COBIT 5（框架）
- COBIT 5 促成因素指南，在指南中详细讨论了治理和管理促成因素。它们包括：

—COBIT 5：促成流程

—COBIT 5：促使信息（开发中）

—其它促成因素指南（查看 www.isaca.org/cobit）

- COBIT 5 专业指南，包括：

—COBIT 5 实施

—COBIT 5 信息安全（开发中）

—COBIT 5 保障（开发中）

—COBIT 5 风险（开发中）

—COBIT 5 其它专业指导（查看 www.isaca.org/cobit）

- 可用于支持 COBIT 5 使用的在线协作环境。

二. 概述

信息对所有企业来说都是关键资源，并且从信息诞生那一刻起一直到消失，技术扮演着重要的角色，信息技术已变得越来越先进并已在企业、社会环境、公共环境、商业环境中普及。

因此，今天企业及其管理人员比以往任何时候都更努力做到：

- 保持高质量的信息以支持业务决策；
- 从 IT 的投资获得商业价值，即通过高效、创新地应用 IT 实现战略目标和商业收益，；
- 通过可靠与有效的技术应用实现卓越运营；
- 将 IT 相关风险保持在可接受水平之内；
- 优化 IT 服务和技术的成本；
- 遵守不断增加的相关法律、法规、合同条款和政策。

在过去的十年中，“治理”一词已经转移到商业思想的最前沿，以回应充分表明良好治理的重要性，和天平的另一端——全球业务事故的先例。

成功的企业已经意识到董事会和高管需要像重视业务一样重视 IT，业务和 IT 部门的董事会成员和管理层必须合作并一起工作，以使 IT 包括在治理和管理方法之内。另外，越来越多的相关法律和规则得以通过和颁布实施来满足这个需求。

COBIT 5 提供一个综合的框架来帮助企业实现治理和管理企业 IT 的目标。简单地说，它通过保持实现效益与优化风险水平和资源使用平衡来帮助企业创造来

自 IT 的最佳价值，COBIT 5 能够使 IT 对整个企业包括所有端到端业务以及 IT 相关的功能区以一种整体的方式管理和控制，并考虑内外部利益相关者的有关 IT 的利益。COBIT 5 是通用的，对所有规模的企业，无论是商业化的、非盈利的或者公共部门均能应用。

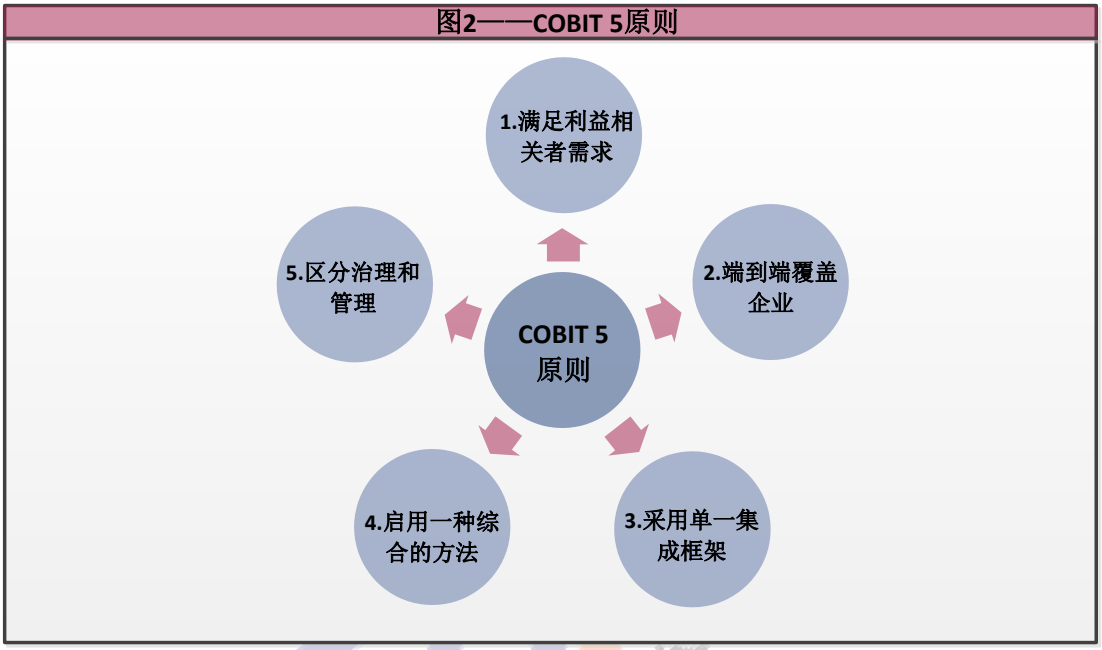

图 2.1　图表 2.COBIT 5 原则

COBIT 5 基于 5 条关键原则（如图 2 所示）治理和管理企业 IT

原则 1：满足利益相关者需求

企业存在的目的是为利益相关者创造价值，这些价值的创造通过保持效益实现与风险和资源使用优化之间的平衡来实现。COBIT 5 通过应用 IT 提供所有的必要的程序和促成因素来支持价值创造，因为不同企业有不同的目标，企业可以通过目标级联，自定义 COBIT 5 以适合其自身的情况，将高级别的企业目标转化成易管理、特定的、IT 相关的目标并将它们映射到具体的流程和实践。

原则 2：端到端覆盖企业

COBIT 5 将企业 IT 治理融合到企业治理中：

— 它包含企业内的所有职能部门与流程；COBIT 5 不仅关注“IT 部门”，而且把信息与相关技术当作资产，就像公司中每个人拥有的其他资产一样。

— 它考虑到了所有端到端的和企业范围的IT相关的治理和管理的促成因素，也就是说，它包括企业内部和外部的，与企业的信息和涉及的 IT 的治理与管理相关的每种东西和每个人。

原则 3：采用单一集成框架

— 有许多 IT 相关标准和最佳实践，每一个均提供一部分 IT 活动的指导，COBIT 5 与其它相关标准与框架保持高度一致，并因此能够成为企业 IT 治理和管理的总体框架。

原则 4：启用一种整体的方法

有效的企业 IT 治理和管理需要一种考虑多个相互影响的组件的整体的方法，，COBIT 5 定义一系列促成因素来支持企业 IT 综合的治理和管理系统的实施。促成因素宽泛的定义为任何能够实现企业目标的东西，COBIT 5 框架定义了 7 类促成因素：

— 原则、政策和框架

— 流程

— 组织结构

— 文化、伦理道德和行为

— 信息

— 服务、基础设施和应用

— 人、技能和竞争力

原则 5：区分管理和治理

COBIT 5 框架明确区分管理与治理，这两个概念包括不同种类的活动，需要不同的组织结构以及为不同的目的服务。COBIT 5 关于管理与治理的区别的观点是：

—治理

治理保证通过评估利益相关者的需求、条件和选择权，以决定所要实现的、平衡的、一致同意的企业目标，通过优先次序设定方向并决策，并监控绩效和对于共同方向和目标的符合性。

[illegible]

[illegible]

—管理

管理规划，构建，运营和监控与治理机构设定的方向保持一致的活动以实现企业目标。

在大多数企业中，管理是首席执行官（CEO）领导下的执行管理层的责任。

综上，这 5 条原则使企业能够建立一个有效的治理与管理框架，该框架为了利益相关者的利益，优化信息与技术投资和应用。

三. 第一章 COBIT 5 综述

COBIT 5 提供下一代关于企业 IT 治理与管理的 ISACA（美国信息系统审计和控制协会）的指导，它建立在 COBIT 超过 15 年的、许多企业及来自业务、IT、风险、证券、保险行业的用户的实践与应用的基础上。COBIT 5 发展的主要驱动因素包括以下的需要：

- 为更多利益相关者在决定他们期望从信息和相关技术得到什么方面提供发言权（在什么可接受的风险水平和多少成本下有多少收益）以及在确保期望收益有多少实际交付方面的优先权。一些利益相关者期望短期回报而另一些期望可持续性的回报，一些愿意承担较大的风险而另一些则不愿意，需要有效地处理这些有分歧的，有时甚至是冲突的期望。而且，这些利益相关者不仅希望更多地参与，他们也希望提高关于这将如何发生以及实际得到的结果的透明度。
- 关注企业成功对外部业务和 IT 团队，例如外包商、供应商、咨询人员、客户、云服务和其他服务提供者，以及一系列不同的内部的方法和交付预期价值的机制等，不断增加的依赖度。
- 处理显著增加的信息量，企业怎样选择相关的和可信的、能够促成卓有成效的业务决策的信息？信息同样需要有效的管理，而有效的信息模型可以帮助做到。
- 处理更加普及的 IT，这越来越成为业务的不可分割的一部分。通常，将 IT 从业务中分出来已经不能令人满意了。它需要成为业务项目、组织结

构、风险管理、政策、技术、流程等的不可分割的一部分。首席信息官（CIO）以及 IT 职能的角色在不断发展，越来越多业务部门的人拥有 IT 技能并且正在或者将会参与 IT 决策与 IT 运营。IT 与业务将需要更好地融合。

- 在创新和新兴技术领域提供进一步的指导，这关系到创造性、发明能力、研发新产品、使现有产品对顾客更具吸引力并且吸引新的顾客类型。创新也意味着以不断提升的效率、速度和质量水平将产品交付市场的流水线产品研发、制造和供应链流程。
- 包含所有端到端业务和 IT 职能责任以及所有促使企业 IT 有效治理和管理的所有方面，例如，组织结构、政策和文化及上述流程。
- 更好地控制不断增加的用户发起和用户控制的 IT 解决方案。
- 实现企业：
  - 通过有效和创新地应用企业 IT 创造价值
  - 业务使用者对 IT 业务与服务满意
  - 遵守相关法律、法规、合同协议和内部政策
  - 改善业务需求和 IT 目标之间的关系
- 连接到并匹配市场上的其他主要框架与标准，例如 ITIL®、TOGAF®、PMBOK®、PRINCE2®、COSO 和 ISO 标准。这将帮助利益相关者理解各种框架、最佳实践和标准如何相互关联以及它们如何一起得到应用。
- 融合所有主要的 ISACA 框架和指导，主要关注 COBIT、Val IT 和 Risk IT。但是，也要考虑信息安全业务模型（BMIS）、IT 保证框架（ITAF）、刊物《IT 治理董事会简报》和《推动治理资源(TGF)》，这样就使 COBIT 5 涵盖整个企业并且为融合其它的框架、标准和实践成为一个单个的框架提供了基础。

不同的产品和其它涵盖各种各样的利益相关者不同需求的指南将基于 COBIT 5 主体知识库建立，随着时间的推移会出现这种情况：使 COBIT 5 产品架构成为动态的文档。最新的 COBIT 5 产品架构可以在 ISACA 网站的 COBIT 页面找到 (www.isaca.org/cobit)。

3.1 本出版物的综述

COBIT 5 包含另外 7 个章节：

第二章阐述原则 1：**满足利益相关者需求。**它介绍了 COBIT 5 目标级联，企业的 IT 目标用于将利益相关者需求正规化和结构化，企业目标可以与 IT 相关目标联系，并且这些 IT 相关的目标可以通过优化应用和执行包括流程的各种促成因素实现，这一系列相互关联的目标称为 COBIT 5 目标级联。这一章提供利益相关者可能有的关于企业 IT 治理与管理典型的问题的例子。

第三章阐述原则 2：**涵盖企业端到端业务**。它解释了 COBIT 5 如何依靠涵盖企业所有部门与流程将企业 IT 治理融入到企业治理中去。

第四章阐述原则 3：**应用单一集成框架**，并简要描述了 COBIT 5 实现融合的架构。

第五章阐述原则 4：**启用一种整体的方法**。企业 IT 治理是系统的并且由一系列促成因素支撑。在这一章介绍了促成因素和一种普遍的看待促成因素的方法：通用促成因素模型。

第六章阐述原则 5：**区分治理与管理**，并讨论治理与管理的不同以及它们怎么相互关联。高级 COBIT 5 过程参考模型作为示例。

第七章包括**执行指南**的介绍。它主要描述合适的环境如何创造，需要的促成因素，典型的实施激发因素和难点以及生命周期的实施和不断改善。这一章基于名为《COBIT 5 实施》的刊物，这篇刊物详细说明如何实施基于可以发现的 COBIT 5 进行企业 IT 治理。

第八章阐述在 COBIT 评估方案方法(www.isaca.org/cobit-assessment-programme) 构想中 **COBIT 5 过程能力模型**，它与 COBIT 4.1 过程成熟性评估如何区别以及用户如何移植到新方法中。

附录包括参考信息、映射关系图和特定主题的更加详细的信息：

- ✧ 附录 A：列出 COBIT 5 开发中用到的参考文献
- ✧ 附录 B：**详细的企业目标与 IT 相关目标之间的映射关系**，描述企业目标通常如何由一个或多个 IT 相关目标支撑。

- ✧ 附录 C：**详细的 IT 相关目标与 IT 相关流程之间的映射关系**，描述 COBIT 流程如何支撑 IT 相关目标的实现。
- ✧ 附录 D：**利益相关者需求和企业目标**，描述利益相关者需求如何与 COBIT 5 企业目标联系。
- ✧ 附录 E：**与 COBIT 5 联系最密切的相关标准与框架的映射关系**
- ✧ 附录 F：**COBIT 5 信息模型与 COBIT4.1 信息标准比较**
- ✧ 附录 G：**COBIT 5 促成因素详细描述**，以第五章为基础并引入更多不同促成因素的详细信息，包括详细的描述特定元件的促成因素模型和一些例证说明。
- ✧ 附录 H：**术语表**

四. 第二章　原则一：满足利益相关者需求

4.1 引言

企业存在的目的是为利益相关者创造价值，因此，任何企业，无论是商业化的或非非商业化的，都将创造价值作为治理目标。创造价值意味着利用最优的资源成本实现效益，同时优化风险（见**图表 3**）。效益有多种形式，比如，商业企业的财务或者政府部门的公共服务。

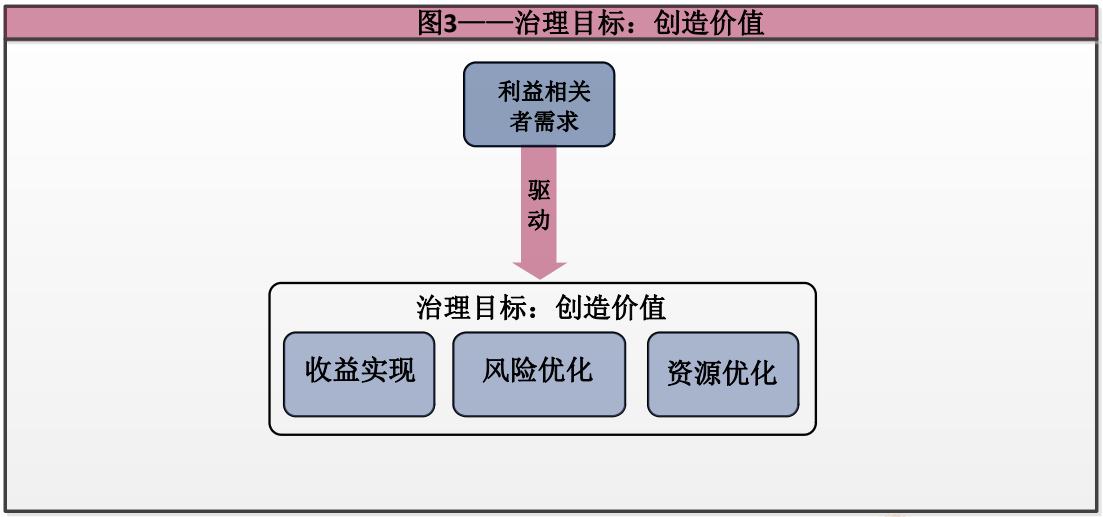

图 4.1　图表 3.治理目标：创造价值

企业拥有许多利益相关者，并且“价值创造”对他们来说意义并不相同，有时会相冲突。治理是在所有利益相关者的不同价值利益间协商与做决定。因此，在做效益、风险、资源评估决策时，治理系统应该考虑所有利益相关者。对于每个决策，以下问题可以也应该问及：为谁创造效益？谁承担风险？需要什么资源？

4.2 COBIT 5 目标级联

每个企业在不同的环境中运作，这个环境由外部因素（市场、产业、政治等）和内部因素（文化、组织、风险偏好等）决定，因此，企业需要一种定制的治理和管理系统。

必须将利益相关者的需求转化成企业可执行的战略。COBIT 5 目标级联是一种将利益相关者需求转化成特定的、可执行的、客户化的企业目标的机制，这一转化允许在企业的每一层级和每个领域设定特定目标，以支持总体目标和利益相关者要求，从而有效地支持企业需求和 IT 解决方案和服务之间的一致性。

COBIT 5 目标级联如**图表 4** 所示。

第一步，利益相关者驱动因素影响利益相关者的需求

利益相关者的需求受许多因素影响，例如，战略的变化、不断变化的业务和监管环境以及新技术。

第二步，利益相关者需求与企业目标的各级联系

利益相关者需求能够与一系列通用的企业目标联系，这些企业目标应用平衡记分卡（BSC）维度制定，并且它们代表了通常使用的、企业可能为自己定义的目标列表。尽管这个列表并不详尽，但是大多数的企业特定的目标可以容易的映射到一个或多个通用企业目标，附录 D 展示了利益相关者需求和企业目标的表格。

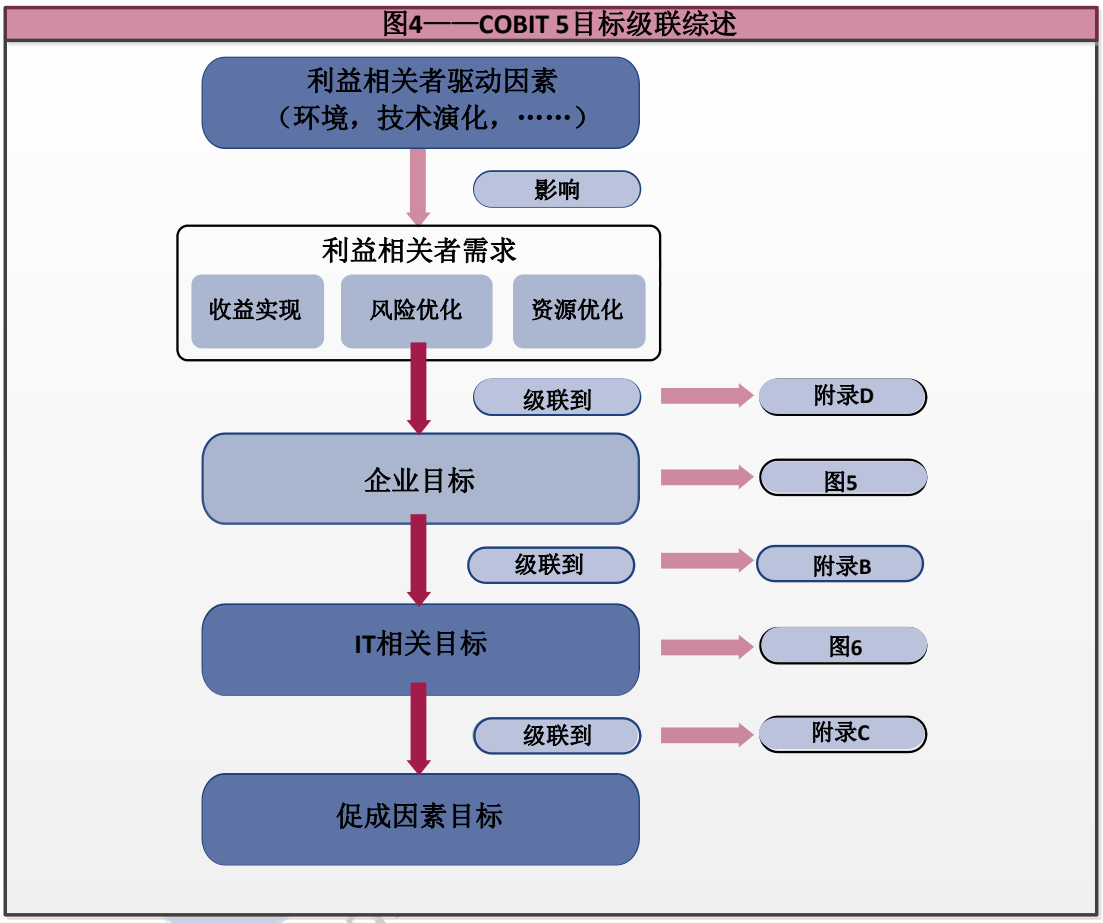

图 4.2　图表 4.COBIT 5 目标级联概述

COBIT 5 定义了 17 个通用的目标，如图表 5 所示，包括以下信息：

- 企业目标适合的 BSC 维度
- 企业目标
- 与三个主要治理目标——效益实现、风险优化、资源优化的关系（“P”代表主要关系，“S”代表次要关系，即稍弱一点的关系）

第三步，企业目标与 IT 相关目标的各级联系

企业目标的实现需要许多 IT 相关的结果，它们被 IT 相关目标和信息与相关技术的标准所呈现，IT 相关目标沿着 IT 平衡记分卡（IT BSC）的维度构建。COBIT 5 定义了 17 种 IT 相关的目标，列在**图表 6** 中。

IT 相关目标与企业相关目标的映射表包含在附录 B 中，它显示了每个企业目标如何由多个 IT 相关目标支持。

第四步，IT 相关目标与促成因素目标的各级联系

实现 IT 相关目标需要成功应用和使用一些促成因素，促成因素的概念在第五章中详细解释，促成因素包括流程、组织结构和信息，对于每个促成因素，定义一系列特定相关目标以支持 IT 相关目标。

流程是促成因素之一，附录 C 包含 IT 相关目标与 COBIT 5 相关流程的映射关系，而 COBIT 5 相关流程包含相关流程目标。

图 5——COBIT 5 企业目标

BSC 维度	**企业目标**	**与治理目标的关系**		
		收益实现	风险优化	资源优化
财务	1.业务投资的利益相关者的价值	P		S
	2.竞争产品和服务的组合	P	P	S
	3.管理业务的风险（资产维护）		P	S
	4.遵守外部法律和法规		P	
	5.财务透明	P	S	S
客户	6.面向客户的服务文化	P		S
	7.业务服务连续性和可用性		P	
	8.对业务环境变化的快速响应	P		S
	9.基于信息的战略决策	P	P	P
	10.服务交付成本的优化	P		P
内部因素	11.业务流程功能优化	P		P

	12. 业务流程成本优化	P		P
	13.管理业务的变化方案	P	P	S
	14.业务和员工生产力	P		P
	15.遵守内部政策		P	
学习和成长	16. 业务熟练和积极进取的人	S	P	P
	17.产品和业务创新文化	P		

图 4.3 图表 5.COBIT 5 企业目标

图 6——IT 相关的目标		
IT BSC 维度	**信息及其相关技术目标**	
财务	01	IT 调整和业务战略
	02	IT 遵守和支持企业遵守外部法律和法规的业务
	03	执行管理对 IT 相关决策的承诺
	04	管理与 IT 相关的业务风险
	05	从 IT 技术的投资和服务组合实现收益
	06	IT 成本，收益和风险的透明
客户	07	符合业务需求的 IT 服务的交付
	08	应用程序，信息和技术解决方案的充分利用
内部因素	09	IT 灵活性
	10	信息、处理基础设施和应用程序的安全性
	11	IT 资产、资源和能力的优化
	12	通过将应用程序和技术集成到业务流程中，启用和支持业务流程
	13	方案的执行提供的好处，按时间，按预算，并满足要求和质量标准
	14	用于决策的可靠和有用的信息的可用性
	15	IT 遵守内部政策

学习和成长	16	能干和积极进取的业务和 IT 人员
	17	业务创新的知识、专业知识和举措

图 4.4　图表 6.IT 相关目标

4.3 运用 COBIT 5 的目标级联

COBIT 5 目标级联的好处：

目标级联是重要的，因为它允许对实施、提升和保障基于企业目标和相关风险的企业 IT 治理的优先权进行定义，实际上，目标级联：

- 在各种责任级别下定义相关的有形的目标
- 基于企业目标过滤 COBIT 5 知识库来提取相关指南，以纳入特定的实施、提升或保障项目。
- 明确识别与沟通促成因素如何对实现企业目标很重要（有时是运作层面的）

仔细使用 COBIT 5 目标级联

目标级联（在企业目标和 IT 相关目标以及 IT 相关目标与 COBIT 5 包括流程在内的促成因素之间的映射表），不包含通用的真理，用户不能企图以一种完全机械的方式运用它，应该作为指导方针应用。这有各种各样的原因，包括：

- 每个企业在它的目标方面有不同的优先级，而且这些优先级可能随时间而变化；
- 映射表不能区分企业的规模和/或行业，总体上，它们代表不同等级的目标是怎样联系的一种共性；
- 映射中的指标使用重要性或相关性的两种等级，意味着关联等级是离散的，然而，实际中，映射中各种各样的关联的程度是接近连续的。

实际应用 COBIT 5 目标级联

从之前的说明，显然，企业使用目标级联时迈出的第一步应该总是在考虑其自身特殊情况下自定义映射。换句话说，每个企业应该建立它们自己的目标级联，将它与 COBIT 比较并对其细化。

例如，企业可能希望：

- 为每个企业目标将其战略优先级转换成特定的“权重”或重要性
- 在考虑其特定的环境与行业等情况下，验证目标级联映射关系

例 1——目标级联
企业已经为自己定义了许多战略目标，其中提高顾客满意度是最重要的，从那里，企业想知道在与 IT 相关的所有东西中哪里需要改善。 企业认为使顾客满意是一个关键的优先级，等同于提高以下企业目标的优先级（来自图表 5）： ● 6.以客户为中心的服务文化； ● 7.业务服务的连续性与可用性； ● 8.对不断变化的市场环境的快速响应； 企业现在在目标级联中采取下一步措施：分析哪些 IT 相关目标对应到这些企业目标。在附录 B 中列出了一个建议的介于它们之间的映射关系。 从那里，以下 IT 相关目标建议作为最重要目标（所有关系为‘P’的） ➢ 01. IT 与业务战略的一致性； ➢ 04.受控的 IT 相关业务风险； ➢ 07.与业务要求一致的 IT 服务交付； ➢ 09.IT 敏捷性； ➢ 10.信息，流程基础设施与应用的安全性； ➢ 14.用于决策制定的、可靠有用的信息的可用性； ➢ 17.知识，专业技术和业务创新的积极性； 企业验证这个列表，并决定保留前 4 个目标作为优先考虑的目标。 在级联的下一步中，应用促成因素概念（见第 5 章），这些 IT 相关目标推动许多包括流程因素在内的促成因素目标。附录 C 中推荐了一种 IT 相关目标与 COBIT 5 流程的映射关系，这个表格允许识别最相关的支持 IT 相关目标的 IT 相关流程，但是，仅仅有流程是不够的。其它的促成因素，例如文化、行为和伦理道德、组织结构或者技能和专业知识是同等重要的，并且需要一系列清晰的目标。

当这些工作完成时，企业就拥有一套针对所有促成因素的、容许它到达阐明的战略目标的、一贯的目标和一套相关的衡量性能的标准。

例 2——利益相关者需求：可持续性

进行利益相关者需求分析之后，企业决定将可持续性作为战略优先。因为，可持续性不仅包括环境方面，而且包括所有有助于企业长期成功的所用东西。

基于利益相关者需求的分析结果，企业决定将重点放在以下 5 个目标，并增加了一些目标的进一步说明：

1. 业务投资的利益相关者价值，尤其对利益相关者团体；

4.遵守外部法律和法规，注重环境方面的法律和外包安排中劳动规章涉及的法律；

8.对不断变化的市场环境的快速响应；

16.熟练的和积极的员工，意识到企业的成功取决于它的员工；

17.产品和业务创新文化，注重长期创新；

基于以上优先顺序，目标级联可以如文章中所说的那样应用。

4.4 关于 IT 方面的治理与管理问题

考虑到对 IT 的高度依赖，在任何企业，利益相关者需求的满足将会引起许多关于企业 IT 治理和管理方面的问题（图 7）。

图 7——关于企业 IT 治理管理方面的问题

内部利益相关者	内部利益相关者的问题
● 董事会 ● 首席执行官（CEO）	● 我如何从使用 IT 中获得价值？终端用户对 IT 服务质量感到满意吗？

● 首席财务官（CFO） ● 首席信息官（CIO） ● 首席风险官（CRO） ● 业务主管 ● 业务流程负责人 ● 业务经理 ● 风险经理 ● 安全经理 ● 服务经理 ● 人力资源（HR）经理 ● 内部审计员 ● 保密人员 ● IT用户 ● IT经理 ● 等	● 我如何管理 IT 的性能？ ● 我如何最好地利用新技术发现新的战略机会？ ● 我如何建立和构造最佳 IT 部门？ ● 我对外部供应商的依赖度有多少？IT 外包协议管理得如何？我如何从外部供应商得到保障? ● 对信息的要求（控制）是什么？ ● 我处理所有 IT 相关的风险了吗？ ● 我是在高效有弹性地运营 IT 吗？ ● 我如何控制 IT 的成本？我如何以最切实有效的方式使用 IT 资源？最切实有效地采购选择是什么？ ● 我有足够的 IT 人员吗？我如何发展和保持他们的技能？我如何管理他们的绩效？ ● 我如何获得 IT 保障？ ● 我正在处理的信息得到很好的保护了吗？ ● 我如何通过更灵活的 IT 环境提供业务敏捷性？ ● IT 项目未能提供所承诺的结果吗？—如果是，为什么？IT 阻碍了业务战略的执行吗？ ● IT 对维持企业有多重要？如果 IT 不可用我怎么办？ ● 基于 IT 的至关重要的具体业务流程是什么？业务流程的要求是什么？ ● 运营预算的平均超支一直以来是多少？IT 项目超过预算的频率和额度多少？ ● IT 工作在多大程度上是救火而不是促使业务改善？ ● 是否有足够的满足企业战略目标的 IT 资源和基础设施可用？ ● 做出重大的 IT 决策需要多长时间？

	● 全部 IT 工作和投资是透明的吗？ ● IT 是在遵守法规和服务级别支持企业吗？我怎么知道我是否符合所有适用的法规？
外部利益相关者	**外部利益相关者的问题**
● 业务合作伙伴 ● 供应商 ● 利益相关者 ● 监管机构/政府 ● 外部用户 ● 客户 ● 标准化组织 ● 外聘审计师 ● 顾问 ● 等	● 我如何才能知道我的合伙伙伴的运营是安全可靠的？ ● 我如何才能知道企业是遵守适用的规则和条例的？ ● 我如何才能知道企业一直保持有效的内部控制制度？ ● 业务合作伙伴控制它们之间的信息链了吗？

图 4.5 图表 7.关于 IT 治理和管理的问题

如何找到这些问题的答案？

图 7 中所提到的所有问题都与企业目标相关，都可作为各级目标的输入，并且基于各级目标它们可被有效地解决。附录 D 包括图 7 中所提到的内部利益相关者的问题与企业目标之间的示范映射关系。

五. 第三章　原则二：端到端覆盖企业

COBIT 5 从整个企业范围内端到端的角度关注信息及相关技术的治理和管理。这意味着 COBIT 5：

- 将企业 IT 治理融入到企业治理当中。也就是说，COBIT 5 提出的企业 IT 治理系统无缝地集成在任何企业治理系统中。COBIT 5 与关于治理的最新观点一致。
- 覆盖了治理与管理企业信息与相关技术所需要的所有功能及流程，信息可能被处理的任何地方。鉴于此扩展的企业范围，COBIT 5 解决所有有关的内部与外部 IT 服务，同时处理内部与外部的业务流程。

在众多促成因素的基础上，COBIT 5 提供了对企业的 IT 治理与管理的整体性和系统性的观点（见原则 4），这些促成因素是企业范围的和端到端的，也就是说，包括与企业信息与相关 IT 的治理与管理有关的每件事和每个人，内部与外部，包括 IT 部门与非 IT 业务部门的活动与责任。

信息是 COBIT 的促成因素之一。COBIT 5 定义促成因素的模型允许每个利益相关者定义对信息与信息处理周期的扩展的、完整的要求。因此将业务与对充足的信息和 IT 功能的需求连接起来，同时支持业务与环境的重点。

5.1 治理方法

端到端的治理方法是图 8 的所描绘的 COBIT 5 的基础部分，图 8 也展示了一个治理系统的关键组成。

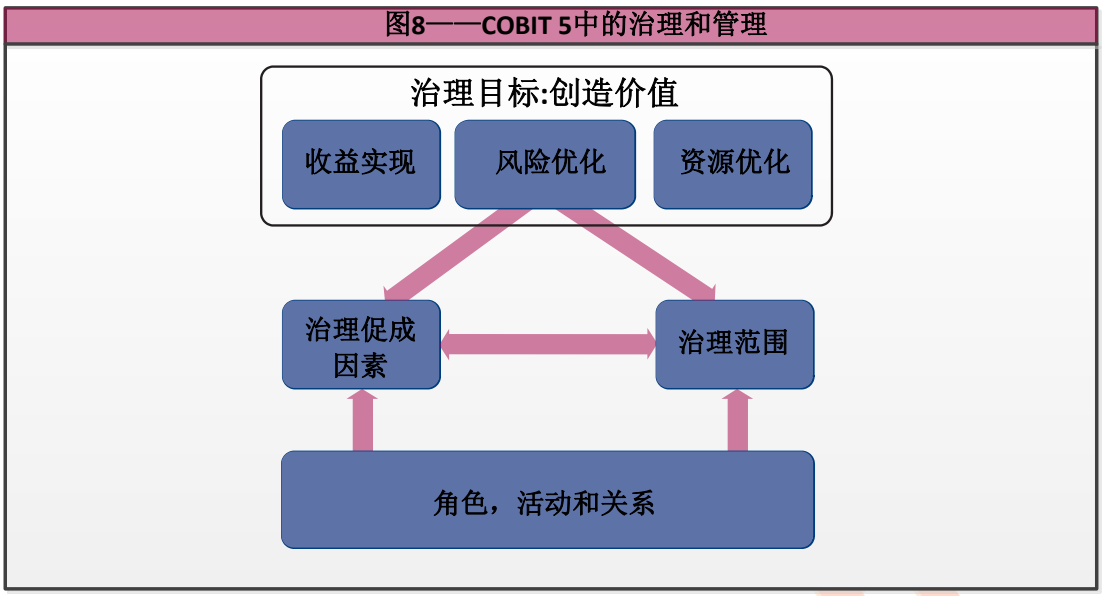

图 5.1　图表 8.COBIT 5 治理与管理

除治理目标外，治理方法的其他重要元素还包括促成因素、范围、角色、活动和关系。

治理促成因素

治理促成因素是治理的组织资源，如框架，原则，结构，流程，和实践，通过或对行动导向和实现目标。促成因素还包括企业的资源，例如，服务能力（IT 基础设施，应用软件等），人员和信息。资源或促成因素的缺乏，可能会影响企业创造价值的能力。

鉴于治理促成因素的重要性,COBIT 5 包括看待和处理促成因素的单一方式(见第 5 章）。

治理范围

治理可以应用到整个企业，机构，有形或无形的资产等等。也就是说，定义关于企业应用治理的不同视角是可能的，而定义治理系统的范围是必须的。COBIT 5 的范围是整个企业，但在本质上 COBIT 5 可以应对任何不同的视角。

角色，活动和关系

最后一个因素是治理的角色，活动和关系。在任何治理框架的范围内，它定义谁参与治理，他们是如何参与，他们做什么以及它们如何进行交互。 在 COBIT 5

中，明确区分治理和管理域的治理和管理活动，以及它们之间的和所涉及的角色的接口。图 9 详细描述了图 8 的下半部分，并列出不同的角色之间的相互作用。

有关治理的通用视图的更多信息，请参阅“推进治理”，网站 www.takinggovernanceforward.org。

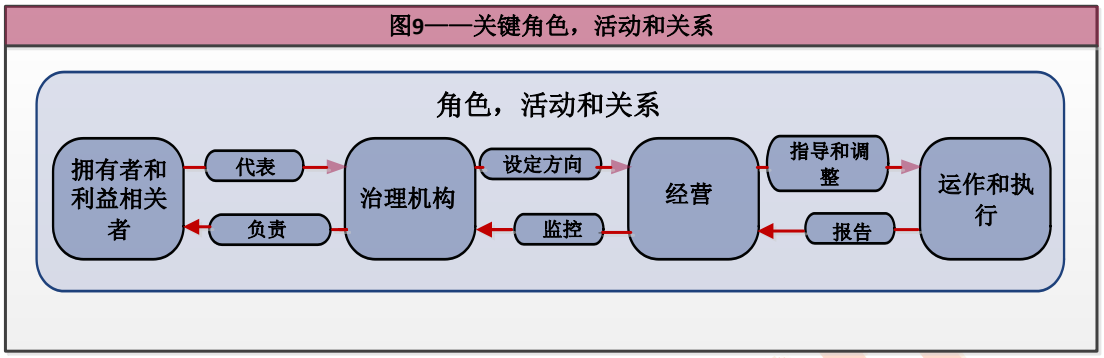

图 5.2　图表 9.关键的角色、活动与相互关系

六. 第四章　原则三：采用单一集成框架

COBIT 5 是一个单一的、集成的框架，因为:

- 它与其他最新的相关标准和框架相一致，从而允许企业把 COBIT 5 作为总体治理和管理框架的集成器。
- 它完全覆盖企业，提供有效地整合其他框架、 标准和所用的做法的基础。单一的总体框架以非技术性的，与技术无关的通用语言，用作一贯的综合指导资源。
- 它提供了一种简单的构建指导材料和生成一致的产品集的架构。
- 它集成了以前分散在不同的 ISACA 框架的所有知识。 ISACA 已研究企业治理的关键领域多年，并已开发了如 COBIT，Val IT，风险 IT，BMIS，出版物 IT 治理简报，以及 ITAF，它为企业提供指导和协助。COBIT 5 融合了所有这些知识。

6.1 COBIT 5 的框架集成器

图 10 提供了 COBIT 5 如何实现其一致和集成框架中的角色的图形化描述。

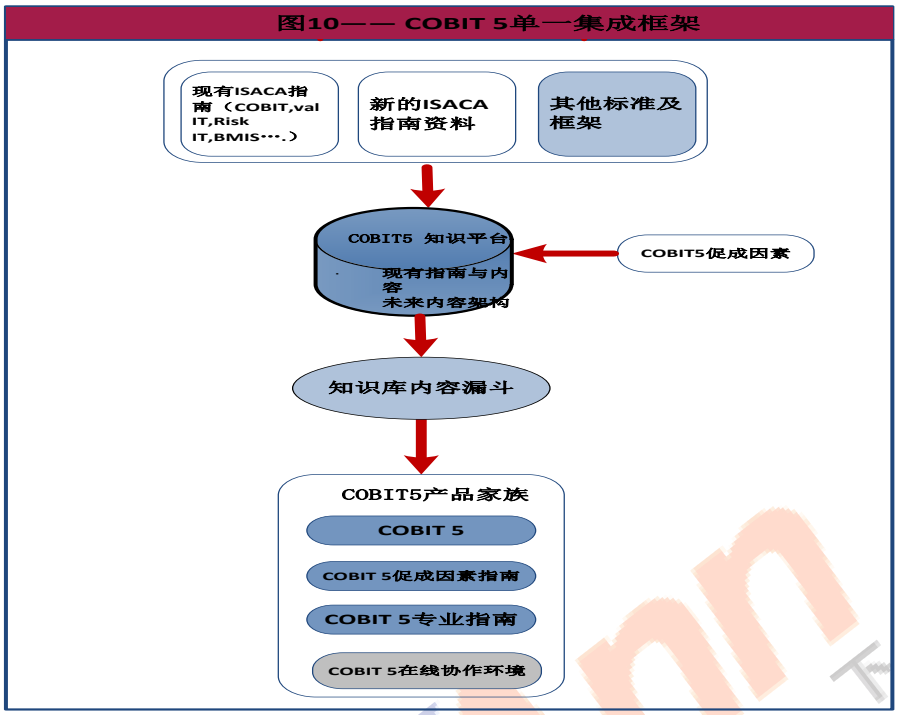

图 6.1　图表 10. COBIT 5 单一集成框架

COBIT 5 框架为利益相关者提供关于企业 IT 治理和管理的最完整的和最新的指南（见图 11），通过：

- 研究和应用一系列驱动新内容开发的资源，包括：

—把现存的 ISACA 指南（COBIT 4.1，Val IT 2.0，风险 IT，BMIS）整合到这个单一结构框架下

—在需要详细阐述和更新升级的地方进行内容补充

—与其他相关标准和结构相匹配，比如 ITIL、TOGAF 和 ISO 标准。在附录 A 中可以找到完整的参考文献列表

—定义一系列能提供所有指导资料结构的治理和管理的促成因素

- 普及 COBIT 5 的知识库，该知识库包括目前产生的所有指导和内容，也为将来提供附加内容的结构
- 提供一个完整的、综合的优良实践参照库

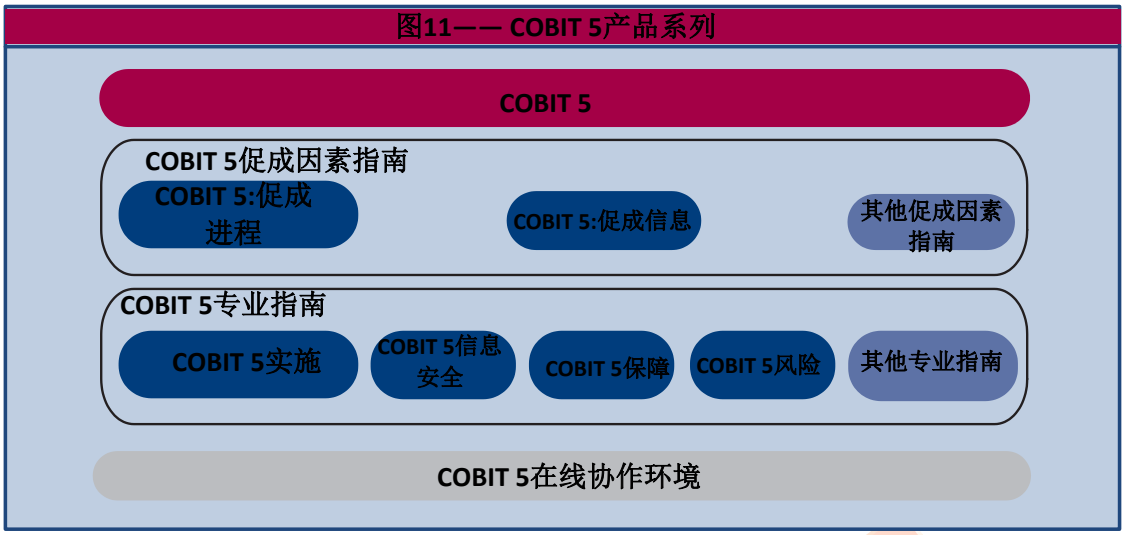

图 6.2　图表 11.COBIT 5 产品系列

七. 第五章　原则四：启用一种整体的方法

7.1 COBIT 5 促成因素

促成因素是单独或共同影响某物是否起作用的因素，在本例中是企业 IT 的治理和管理。促成因素由各级目标驱动，即 IT 相关的高级目标定义了不同促成因素应该达到的要求。

COBIT 5 框架描述了七类促成因素（**表 12**）：

- **原则，政策和框架**是把所期望的行为转变为日常管理的实践指导的工具。
- **流程**描述了一系列有组织的为达到特定目标和产生一系列的输出以支持实现整体 IT 相关目标的实践和活动。
- **组织结构**是在一个企业的关键的决策实体。
- **文化、伦理道德和行为，**个人和企业的文化、伦理道德和行为是在治理和管理活动中通常被低估的取得成功的因素。
- **信息**是在任何组织中是很普遍的，它包括企业产生和运用的所有信息。信

息是保证组织运行和有效治理所必需的，但是在操作层面上，信息通常是企业自身的主要产品。

- **服务、基础设施和应用程序**包括为企业提供信息技术服务和处理的基础设施和应用程序。
- **人才，技能和竞争力**与人有关，并且是做出正确决策和实施正确行动和成功完成所有活动所必需的。

图 7.1　图表 12.COBIT 5 企业促成因素

之前定义的一些促成因素同样是需要管理和治理的企业资源。这适用于：

- 信息，需要当做一种资源来处理。一些信息，比如管理报告和业务情报信息是企业治理和管理的重要促成因素。
- 服务，基础设施和应用程序
- 人才，技能和竞争力

7.2 通过相互关联的促成因素系统地治理和管理

图 12 也传达出这种应该被企业治理采纳的理念，包括 IT 治理，IT 治理是实现企业的主要目标。任何企业必须一直考虑一系列相互关联的促成因素。也就是说，每种促成因素：

- 要想完全有效，需要其他促成因素的输入，比如，流程需要信息，组织结构需要技能和行为。
- 为其他促成因素提供输出，比如，流程传递信息，技能和行为状况使流程生效。

所以当解决企业 IT 管理和治理中的问题时，只有当考虑这种系统性的治理与管理的本质时，好的决策才会被采纳。这意味着为了应对任何利益相关者的需要，必须分析所有相互关联的促成因素的相关性，如果需要做相应处理。这种思维模式必须由企业的顶层驱动，如下面的例子所示。

例 3——企业 IT 的治理和管理
假设提供给所有用户的 IT 服务需要服务能力（基础设施，应用程序），为实现些功能，需要有适当技能组合和行为的员工，也需要执行很多由适当的组织机构支持的服务交付程序，以展示服务成功地交付是如何需要所有的促成因素的。

例 4——企业 IT 的治理和管理
信息安全的需要要求建立大量的政策和工作规程并付诸实施。这些工作原则反过来需要实施很多安全相关的实践环节。然而，如果企业或者员工的文化或道德标准不适合，信息安全流程和程序将不会有效。

7.3 COBIT 5 促成因素的维度

所有的促成因素具有共同的维度组合，这一共同维度的组合（图 13）：

- 提供了一种通用的、单一的、结构化的方法来处理促成因素
- 允许一个实体来管理其复杂的相互作用
- 促成促成因素的成功结果

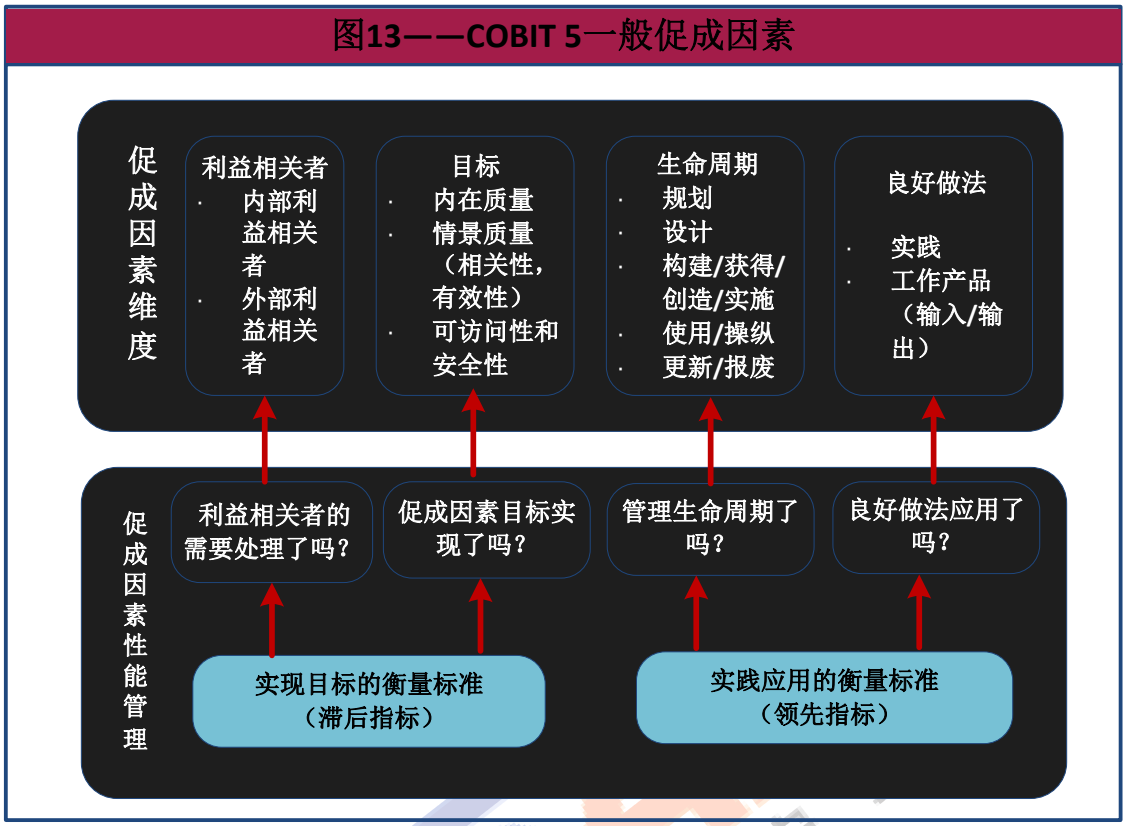

图 7.2　图表 13.COBIT 5 通用促成因素

促成因素维度

促成因素的 4 个通用维度是：

- **利益相关者**：每个促成因素都有利益相关者（发挥积极的作用和/或对促成因素感兴趣的各方）。例如，流程有执行流程中的活动和/或对流程结果感兴趣的不同各方；组织结构有利益相关者，每一个都有他/她各自的角色或兴趣，这是结构的一部分；利益相关者对企业可以是内部的或者外部的，他们都有自己的利益和需求，这些利益与需求有时可能是冲突的，利益相关者需求转换成企业目标，进而转化为企业的 IT 相关的目标。利益相关者列表在**图 7** 中显示。
- **目标**：每一个企业都有若干目标，并且促成因素通过实现目标提供价值，目标可以根据定义：

——促成因素期望输出结果

——促成因素自身的应用与运作

促成因素目标是 COBIT 5 目标级联中的最后一步，目标可以进一步分为不同的类别：

——**内在质量**：促成因素准确，客观地工作，并提供准确、客观、有信誉的结果的程度

——**环境质量**：促成因素及其结果，在考虑他们运营环境的情况下，适合目的的程度，举例来说，结果应该是相关的，完整的，最新的，适当的，一致的，易于理解和易于使用的。

——**访问和安全**：促成因素及其结果可访问和安全的程度。诸如：

- 当需要和如果需要时，促成因素是可得的。
- 输出是安全的，即访问仅限于那些有权并需要它的人。

- **生命周期**：每一个促成因素都有生命周期，从成立以来，经过运营/有用的生命，直到被处理掉。这适用于信息、结构、流程、政策等等。生命周期的阶段包括：

  —规划（包括概念的发展和概念的选择）

  —设计

  —建立/收购/创建/实施

  —应用/运作

  —评估/监控

  —更新/弃置

- **好的实践**：对每一个促成因素，可以定义好的实践。好的实践支持促成因素目标的实现，好的实践提供关于如何最佳实施促成因素和需要什么工作产品或输入输出的示例和建议。COBIT 5 提供一些由其自身提供的促成因素的好的实践的例子（例如流程）。对其它的促成因素，可以应用来自其它标准或框架等的指南。

促成因素性能管理

企业期望从应用促成因素中得到积极的结果，为了管理这些促成因素的性能，以下问题需要定期监控并从而随后解决（基于衡量指标）：

- 利益相关者额需求处理了吗？

- 促成因素目标实现了吗？
- 管理促成因素生命周期了吗？
- 好的实践应用了吗？

前两个问题对应促成因素的实际输出，用于衡量目标的实现程度的度量指标可称为“滞后指标”。

后两个问题对应促成因素自身的实际作用，这个指标可以称为“领先指标”。

7.4 实践中促成因素的例子

例 5 说明了促成因素，它们的相互联系和维度，以及如何应用它们以获得实际效益。

例 5：促成因素

组织已为 IT 相关的流程任命流程经理，负责在企业 IT 良好治理和管理的环境下，定义和运行有效和高效的 IT 相关的流程。

起初，流程经理将侧重于流程的促成因素，并考虑促成因素的范围：

- **利益相关者**：流程中的利益相关者包括所有流程参与者，即负责、有义务、咨询和被告知的各方为或在流程活动中。为此，RACI 表格如在 COBIT 5 中描述：促成流程可以得到应用。
- **目标**：对每一个流程，需要定义足够的目标和相关的衡量指标。例如，对于一个流程管理关系（COBIT 5：启用流程中的流程 APO08），可以发现一组流程的目标和指标如：

—**目标**：业务战略、规划和要求得到很好地理解、记录和批准。

- **指标**：与企业业务要求/优先级相一致的方案的百分比

—**目标**：企业与 IT 部门之间良好的关系。

- **指标**：用户评价和 IT 人员的满意度调查

- **生命周期**：每个流程都有生命周期，即它需要被创建，执行和监测，并在需要时调整，最终，流程不复存在。在本例中，流程经理首先需要设计和定义过程，他们可以使用 COBIT 5：启用过程的一些元素来设计流程，即明确责

任和将流程分解为实践和活动，并定义过程的工作产品（输入和输出）的若。在稍后阶段，需要将流程设计得更强大和更有效率，并且为这一目的，流程经理可以提高流程的性能水平。由 ISO/IEC 15504 启发的 COBIT 5 过程能力模型和流程性能属性可以用于这个目的。

- **好的实践**：充足详细介绍了 COBIT 5：启用流程好的实践，如先前提到的，在那儿可以得到启示和获得示例流程，并全方位覆盖良好的企业 IT 治理和管理所需的活动。

除了流程促成因素的指导，流程经理可以决定看一些其他促成因素，诸如：

- RACI 表格，它描述角色与责任，其它促成因素深入这一维度诸如：

——在技能与竞争力促成因素中，可以定义每个角色需要的技能与竞争力，并且定义适当的目标（如技术和行为技能水平）与相关指标。

——RACI 表格也包括一些组织结构，在组织结构促成因素中，这些结构可以进一步阐述，其中可以提供更详细的结构描述，定义预期成果和相关指标（如决策），并且可以定义好的实践（如控制范围，结构的操作原则，授权级别）

- 原则和政策将使流程正式化并描述流程为什么存在，对谁可用以及流程怎么应用，这是原则和政策促成因素的重点领域。

在附录 G 中，更详细地描述了七类促成因素，为更好理解促成因素以及它们在组织企业 IT 治理和管理方面的强大程度，建议阅读本附录。

八. 第六章　原则五：区分治理与管理

8.1 治理与管理

COBIT 5 框架明确区分治理与管理，这两个概念包括不同类型的活动，需要不同的组织结构和服务于不同的目的。COBIT 5 认为治理与管理之间的主要区别是：

- **治理**

治理保证通过评估利益相关者的需求、条件和选择权，以决定所要实现的、平衡的、一致同意的企业目标，通过优先次序设定方向并决策，并监控绩效和对于共同方向和目标的符合性。

在大多数企业，治理是在董事会主席领导下的董事会负责的，

- **管理**

管理规划，构建，运营和监控与治理机构设定的方向保持一致的活动以实现企业目标。

在大多数企业中，管理是首席执行官（CEO）领导下的执行管理层的责任。

8.2 治理与管理的相互作用

从治理和管理的定义，可以明确知道，他们包含不同类型的活动，有不同的责任；然而，鉴于治理的角色（评估、指导和监督），在治理与管理之间需要一系列相互作用来形成一个切实有效的治理系统。这些相互作用，使用促成因素结构显示在**图 14** 中。

图 14——COBIT 5 治理和管理的相互作用

促成因素	治理—管理相互作用
流程	在说明性的 COBIT 5 的过程模型（COBIT 5：启用流程）中，治理和管理流程是有区别的，每种流程包括一系列具体的做法和活动。流程模型还包括 RACI 图表，描述企业内部不同的组织结构

	和角色的职责。
信息	流程模型描述从不同的流程实践到其他流程的输入和输出，包括治理和管理流程之间的信息交换。用于评估，指导和监督企业 IT 的信息在治理和管理之间交换，如流程模型的输入和输出所描述。
组织结构	每个企业都定义了若干组织结构，结构可以放在治理空间或管理空间中，这取决于其决策的组成和范围。由于治理是关于设定方向，在治理结构所做的决策（比如决定投资组合和风险偏好）和落实前面的决策和业务之间产生的互动。
原则，政策和框架	原则，政策和框架是企业内部治理决策的制度化的工具，出于这个原因，它们也是治理决策（设定方向）和管理（执行决策）之间的相互作用。
文化，伦理道德和行为	行为也是一个企业良好治理和管理的关键促成因素，它位于顶层，由示例引导，因此是治理和管理之间的重要的相互作用。
人，技能和竞争力	治理和管理活动需要不同的技能组合，但治理机构成员和管理层的一项基本技能是理解任务以及治理与管理之间的不同之处。
服务，基础设施和应用	服务是必需的，由应用程序和基础设施支持，从而为治理机构提供充足的信息，并支持治理活动的评估，方向设定和监控。

图 8.1　图 14　COBIT 5 治理和管理的相互作用

8.3 COBIT 5 流程参考模型

COBIT 5 不是规定性的，但它主张企业实施治理和管理流程以涵盖关键领域，如**图 15** 所示。

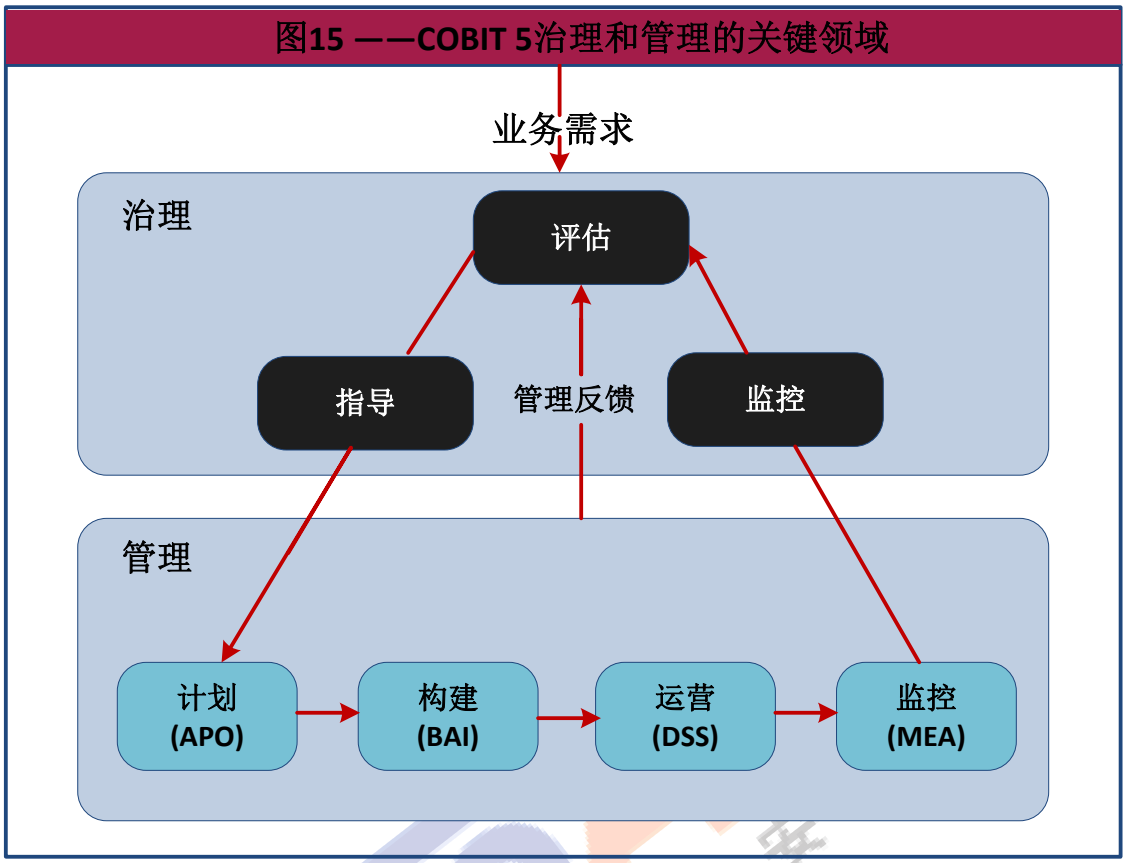

图 8.2　图表 15.COBIT 5 治理与管理的关键领域

企业组织它认为合适的流程，只要包含所有必要的治理和管理的目标，小的企业流程少，大的复杂的企业流程多，但均包含相同的目标。

COBIT 5 包括一个流程参考模型，详细地定义和描述若干治理和管理流程，它代表在企业 IT 相关活动中经常发现的所有流程，为 IT 运营和业务经理提供一个通用的易理解的参考模型。这个推荐的流程模型是一个完整的、综合的模型，但它并不是唯一可能的过程模型。考虑到其具体情况，每个企业都必须定义它自己的流程集，

结合企业在 IT 活动所涉及的所有部件的运作模式和共同的语言，是走向良好管理的最重要和最关键的步骤之一。它还提供了一个衡量、监控 IT 性能，提供 IT 保障，与服务供应商交流以及整合最好管理做法的框架。

COBIT 5 流程参考模型将企业 IT 治理和管理流程分为两个主要流程领域：

- **治理**：包括 5 个治理流程，在每个流程内，定义了评估、指导和监控（EDM）实践。

- **管理**：包含四个领域，根据责任区域的规划，构建，运行和监控（PBRM），并提供 IT 端到端的覆盖。这些领域是 COBIT4.1 域和流程结构的演变。这些领域的名称是根据主要领域的标识选择的，但包含了更多的动词描述他们：

—调整，规划和组织（APO）

—建立，获取和实施（BAI）

—交付，服务和支持（DSS）

—监控，评价和评估（MEA）

每个领域包含若干流程。如前所述，虽然大部分流程需要在流程内或所处理的特定议题内（例如质量、安全），“规划”，“实施”，“执行”和“监控”活动。根据在企业层面看待 IT 时，它们通常被置于最相关的活动领域。

COBIT 5 流程参考模型是 COBIT 4.1 流程参考模型的继承者，同时也融合了风险 IT、Val IT 流程模型。

图 16 显示了 37 种 COBIT 5 治理和管理流程的完整集合，根据前面介绍的流程模型，所有流程的详细情况包含在 COBIT 5：启用流程中。

图 8.3 图表 16.COBIT 5 流程参考模型

九. 第七章 实施指南

9.1 引言

只有当有效地采纳和调整 COBIT，以适应每个企业的独特环境时，才能从利用 COBIT 中实现最佳价值。每种实施方法也将需要解决包括管理文化和行为的变化在内的具体挑战。

ISACA 在基于生命周期持续改善的论文《COBIT 5 实施》中提供了实用的和广泛的实施指南，它不是一种指令性的方法，也不是一个完整的解决方案，而是避免经常遇到的陷阱，利用良好做法，并协助创造成功结果的指南。该指南还受到包含各种不断强化的资源的实施工具套件支持。它的内容包括：

- 自我评估。测量和诊断的工具
- 针对各种听众的介绍
- 相关文章和进一步解释

本章的目的是在一个较高层次介绍实施和持续改进的生命周期，突出强调来自 COBIT 5 实施的若干重要课题，诸如：

- 为 IT 治理和管理的实施和改进制作业务案例
- 认识典型的难点和触发事件
- 为实施创造适当的环境
- 利用 COBIT 来识别差距，并指导促成因素如政策、流程、原则、组织结构以及角色和责任的发展。

9.2 考虑企业环境

企业的 IT 治理和管理不会发生在真空中，每个企业的需要来设计自己的实施计划或路线图，设计需要根据企业特定的内部或外部环境，如企业的：

- 伦理道德和文化
- 实施的法律、法规和政策
- 使命、愿景和价值观
- 治理政策和实践
- 业务规划和战略意图
- 运营模式和成熟水平
- 管理方式
- 风险偏好
- 能力和可用资源
- 产业实践

同样重要的是充分利用和构建现有的企业治理的促成因素。

对每一个企业来说，企业 IT 治理与管理的最佳方法是不同的，并且需要理解并考虑环境因素，以在实施企业 IT 促成因素的治理与管理的过程中有效地采纳和调整 COBIT。COBIT 通常支持其它框架、好的实践和标准，并且这些也需要调整以满足特定的要求。

成功实施的关键成功因素包括：

- 高层管理者提供开始行动的指示与授权，以及看得见的持续的承诺与支持
- 支持治理与管理流程的所有各方理解业务和 IT 目标
- 确保对必要变革的有效的交流与促进
- 调整 COBIT 和其它辅助的好的实践和标准以适应特定企业环境
- 重视快速取胜和优先实现最易实施的最有效益的提升

9.3 创造合适的环境

利用 COBIT 的实施举措得到适当的治理和充分的管理是重要的，主要的 IT 相关的举措往往失败，因为各种利益相关者不适当的指导、支持和监督，利用 COBIT 的 IT 促成因素的治理或管理的实施也没有什么不同。来自关键利益相关者的支持和指导是重要的，以使改进得以采用和保持。在薄弱的企业环境（诸如不清晰的整体业务运营模式或缺乏企业级的治理促成因素）下，这种支持和参与甚至更重要。

采用 COBIT 的促成因素应该提供一个解决实际业务需求和问题的，而不是作为自己的终端的解决方案。基于当前难点和驱动因素的需求应该被管理人员作为需要处理的领域来识别与接受。基于 COBIT 的高层次的健康检查，诊断或能力评估是提升意识、促成一致意见、产生行动承诺的完美工具。必须从一开始就询问相关利益相关者的承诺和偏好。为实现这些，实施的目标和利益的需要在业务术语中明确表达，在业务案例概要明确总结。

一旦已取得承诺，需要为支持该方案提供足够的资源，定义和委任关键的项目角色与责任，需要注意持续保持来自所有受影响的利益相关者的承诺。

应当建立和保持适当的用于监督和指导的结构和流程，这些结构和流程也应该确保与整个企业的治理和风险管理方法持续一致。

关键利益相关者例如董事会和高管应该提供可见的支持和承诺，以设定的“顶层的基调”，并确保各级对方案的承诺。

9.4 识别难点与触发事件

有许多因素可能预示需要改善企业 IT 的治理和管理。

通过把难点和触发事件作为实施计划的启动点，企业 IT 改善的治理和管理的业务案例可以与实际的、正在经历的日常问题相联系，这将提高买入并且在企业范围内创造紧迫感，而这正是揭开实施序幕所需要的。另外，在企业中最容易看见或最易识别的领域中，可以识别快速取胜，并且可以显示价值增加。这为进一步转变提供了平台，并可以协助获得广泛的高级管理层的承诺和更加普遍的变化的支持。

一些典型的难点例子，新的或修订过的， IT 促成因素的治理或管理可以成为一个解决方案（或解决方案的一部分），如 COBIT 5 实施中确认的那样，是：

- 失败的方案、提高 IT 成本和低的业务价值感觉造成的业务挫折
- 与 IT 风险，如数据丢失或项目失败，相关的重大事故
- 外包服务交付问题，例如一致未能达到商定的服务水平
- 未能达到监管和合同要求
- IT 限制企业的创新能力与业务敏捷性
- 差的 IT 性能的日常审计结果或者已报告的 IT 服务质量问题
- 藏匿和欺诈 IT 花费
- 成倍或者方案重复或者资源浪费，例如过早终止项目
- 不充分的 IT 资源，技术不足的员工或员工倦怠/不满
- IT 促使的变化没有满足业务需求和交付推迟或者超过预算
- 董事会成员，高管以及高级经理不愿参与 IT 或者缺少信守诺言的令人满意的 IT 发起人
- 复杂的 IT 操作模型

除了这些难点之外，企业内部或外部环境中的其它因素可以暗示或触发对 IT 治理和管理的关注，第 3 章《COBIT 5 实施》出版物中的例子是：

- 兼并，收购或剥离
- 市场、经济与竞争地位的变化
- 业务操作模型与采购安排的变化
- 新的监管或合规性要求
- 重大的技术改变或模式改变
- 企业范围的治理重点或项目
- 新的 CEO、CFO、CIO 等
- 外部审计或咨询评估
- 新的业务战略或优先事项

9.5 启动变革

成功实施取决于以适当的方式实施适当的变化（适当的治理或管理促成因素）。在许多企业中，第一方面得到了很好的重视（IT 的核心治理与管理），但是对管理人力资源、行为和文化方面的变化以及激励利益相关者入股变化的重视不够。

不应该假定参与或者受新的或修订的促成因素影响的各种利益相关者将愿意接受和采纳变化，对变化的无知和/或抵制需要通过一个结构化的和主动的方法解决。同样，在整个方案的各个阶段，实施方案的最佳认识应通过一种“沟通什么，以何种方式沟通，由谁沟通”的沟通计划来实现。

通过获得利益相关者的承诺（投资为赢得民心，领导人的时间，并与员工沟通和回应），或者如仍需要，通过加强合规性（投资流程中的管理，监督和执行）可以实现持续改善。换句话说，需要克服人、行为和文化的障碍，以使有妥善采纳变化的共同利益，渗透采取改变的意愿，并确保采取变化的能力。

9.6 一种生命周期方法

实施生命周期提供了一种为企业使用 COBIT 解决在实施过程中通常遇到的复杂性和挑战的方法。生命周期的三个相互关联的组成部分是：

1.核心持续改善的生命周期：这不是一个一次性的项目

2.启用的变化：应对行为和文化方面

3.方案的管理

如前面所讨论的，需要创造适当的环境，以确保成功实施或改进计划。生命周期及它的七个阶段如**图 17** 所示。

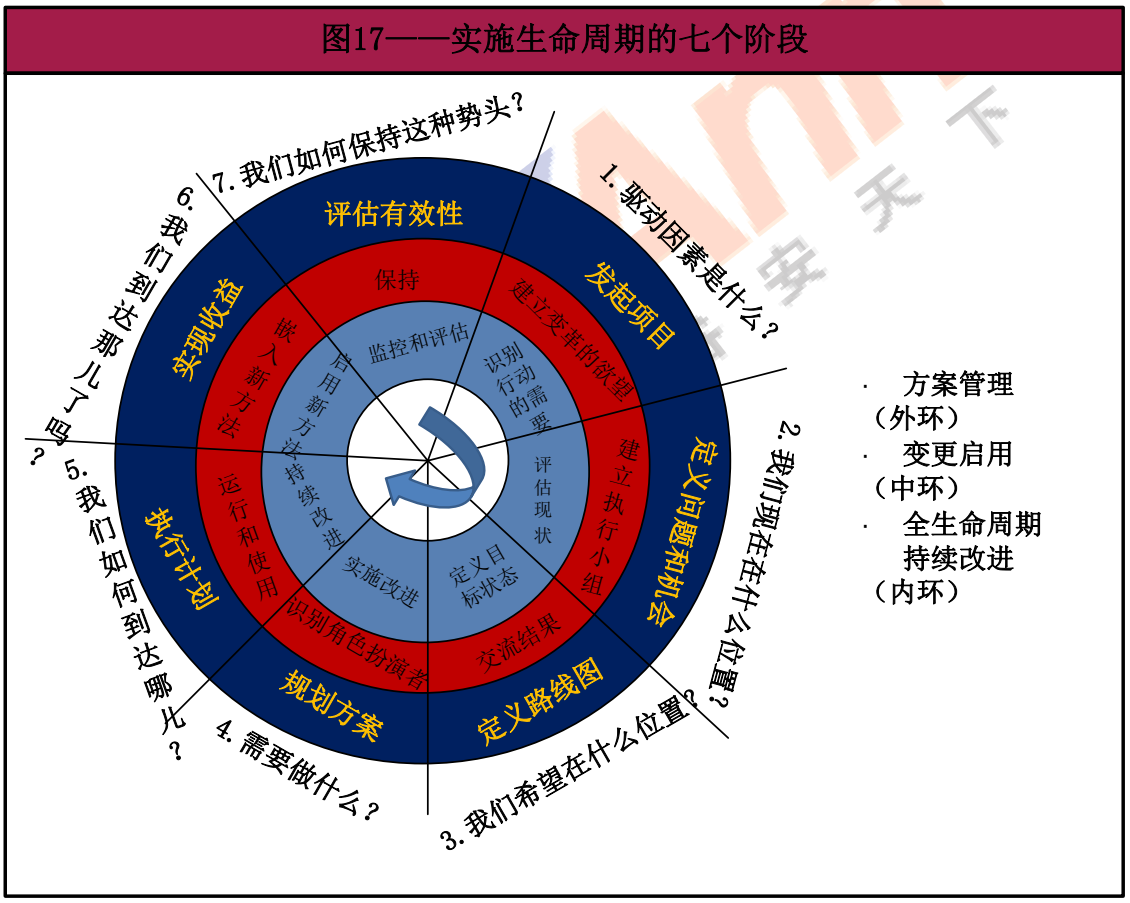

图 9.1　图表 17.实施生命周期的七个阶段

第一阶段开始认识到并同意实施或改进计划的必要性。它确定了目前的难点和触发点，并在执行管理层造成改变的欲望。

第二阶段的重点是通过使用 COBIT 框架中企业目标与 IT 相关的目标以及与相关的 IT 流程之间的映射关系，确定实施或改进计划的范围，并考虑风险情况也可以怎样突出所关注的关键工序。高层次的诊断也可对高优先级领域的范围确定和理解有用。接着，进行当前状态的评估，并通过程能力评估识别问题或不足之处。大型倡议的结构应作为生命周期的多重迭代，任何执行超过六个月的倡议，有失去动力，焦点和从利益相关者的买入的风险。

第三阶段，设置改进的目标，在 COBIT 框架的指导下，通过更详细的分析找出差距和潜在的解决方案。有些解决方案可能是迅速见效，但其他方案可能是更具挑战性的、更长期的活动。应优先考虑更容易实现和那些可能产生最大的效益的举措。

第四阶段，通过合理的业务案例支持的项目，规划确定切实可行的解决方案。还制定一个实施的改革计划。一个发展完善的业务案例有助于确保项目的效益确定和监控。

第五阶段，提出的解决方案在日常实践中实施。可以定义衡量标准和建立监控，使用 COBIT 的性能和指标，以保证维持和实现业务的一致性，性能可以被衡量。成功需要高层管理人员的参与和声明的承诺以及受影响的企业和 IT 利益相关者的所有权。

第六阶段侧重于新的或改进的促成因素的可持续运营和对预期效益实现的监测。

第七阶段，评估该方案的整体成功情况，确定企业 IT 治理或管理的进一步需求，持续改进的需求得以加强。

随着时间的推移，当为企业 IT 的治理和管理建立一种可持续的方法时，应遵循反复的生命周期。

9.7 入门：制作业务案例

为确保利用 COBIT 的实施方案的成功，企业内部应该广泛认识到和沟通采取行动的需要。这可以采取 “闹钟”（如前所述，正在经历具体的难点）的形式，

或要追求的改善机会的表达，重要的是将要实现的利益。需要灌输适当水平的紧迫感，并且关键利益相关者应该意识到不采取行动的风险和承担项目的收益。

倡议应有一个提案人，涉及所有主要利益相关者，并以业务案例为基础。最初，从战略的角度——自上而下——从清楚地了解预期的业务成果，发展到关键任务和里程碑，以及关键的角色和职责的详细描述，这可能是在一个较高的水平。业务案例是管理层可用的、指导业务价值创造的宝贵的工具。最起码，业务案例应包括以下内容：

- 确定业务利益目标，与业务战略及相关受益业主（业务中保证负责业务的人）的一致性。这可以基于难点和触发事件。
- 创造预想的价值需要的业务变化。这可基于健康检查和能力差距分析，并应明确说明什么在范围内，什么在范围之外。
- 企业 IT 的治理和管理变化（基于对所需项目的估计）需要的投资。
- 持续的 IT 和业务成本。
- 以改变后的方式运营的预期收益。
- 在过去的经济学中所固有的风险，包括任何限制或依赖性（基于挑战和成功因素）。
- 与倡议相关的角色，责任和义务。
- 在这个经济生命周期中，如何监控投资和价值创造，以及要使用的评价指标（基于目标和指标）

  业务案例不是一次性的静态文件，而是一个动态的业务工具，必须不断更新以反映未来的当前视图，以便可以保持方案的可行性。

量化实施和改善方案的效益是困难的，并且应该只关注现实的、可行的效益。在多家企业进行的研究可以提供对已经取得的收益的有用信息。

例 6：IT 治理的统计资料
ITGI 委托 PWC 做了一项关于 IT 治理的市场研究，有来自 21 个国家的 800 多名 IT 和业务受访者参与。38%的受访者列举降低 IT 成本作为 IT 治理实践的结果，28.1%认为提高企业竞争力，27.1%表示提高 IT 投资回报。此外，反映出一些无形的收益，如 IT 相关风险管理的改善（42.2%的受访者），业务与 IT 之

间的沟通和关系的改善（39.6%受访者），业务目标中 IT 交付的改善（37.3%受访者）。

ISACA 协会还承担了探索和验证 COBIT 的商业价值的研究，研究产生的数据集提供了许多分析机会，澄清了 IT 企业治理与业务绩效之间的关系。

另一项在全世界各地 250 家企业中开展的研究发现，具有优越的 IT 治理的企业比具有相同的目标的治理不善的企业高出至少 20%的利润率。它说明 IT 业务价值直接来源于有效的 IT 治理。

最后，在航空业的另一项研究得出的结论是企业 IT 治理的实施和持续保证恢复了业务和 IT 之间的信任，导致投资和战略目标的一致性增加。同时，研究报告了更多实实在在的利益，在本案例中，包括降低每个业务生产单元的 IT 连续性成本，并为创新腾出资金。在财务部门的其它跨案例研究证明拥有更好的 IT 治理方法的企业明显获得更高的业务/IT 一致性成熟度得分。

十. 第八章　COBIT 5 过程能力模型

10.1 引言

COBIT 4.1、风险 IT 和 Val IT 的用户对包含在那些框架中的流程成熟模型很熟悉，这些模型用来衡量目前的或者“现在”的企业的 IT 相关流程的成熟程度，以定义一个需要的“将来”的成熟状态，并且确定他们之间的差距以及如何改进这些流程达到希望的成熟水平。

COBIT 5 产品系列包括一个基于国际公认的 ISO/IEC15504 的软件工程——流程评估标准的流程性能系统，这个模型将实现相同的过程评估和过程改进支持的总体目标，即它将提供一种手段来衡量任何治理流程（基于 EDM 的）或管理（基于 PBRM 的）的流程性能，并将允许确定改进的区域。

然而，这个新模型与 COBIT 4.1 成熟模型在设计和使用方面是不同的，因此，以下问题需要讨论：

- COBIT 5 模型与 COBIT 4.1 模型的不同点
- COBIT 5 模型的好处
- COBIT 5 用户在实际应用中将遇到的不同点的总结
- 执行 COBIT 5 性能评估

COBIT 5 性能评估方法的详细信息包含在 ISACA 出版物《COBIT 流程评估模型（PAM）：使用 COBIT 4.1》中。

尽管这种方法将会提供关于流程状态的有价值信息，但是流程仅仅是治理和管理的七大促成因素之一，因此，流程评估不能提供企业治理状态的全景，因此，其它的促成因素也需要评估。

10.2 COBIT 4.1 成熟度模型与 COBIT 5 过程能力模型的不同点

COBIT 4.1 成熟度模型方法的元素如**图 18** 所示：

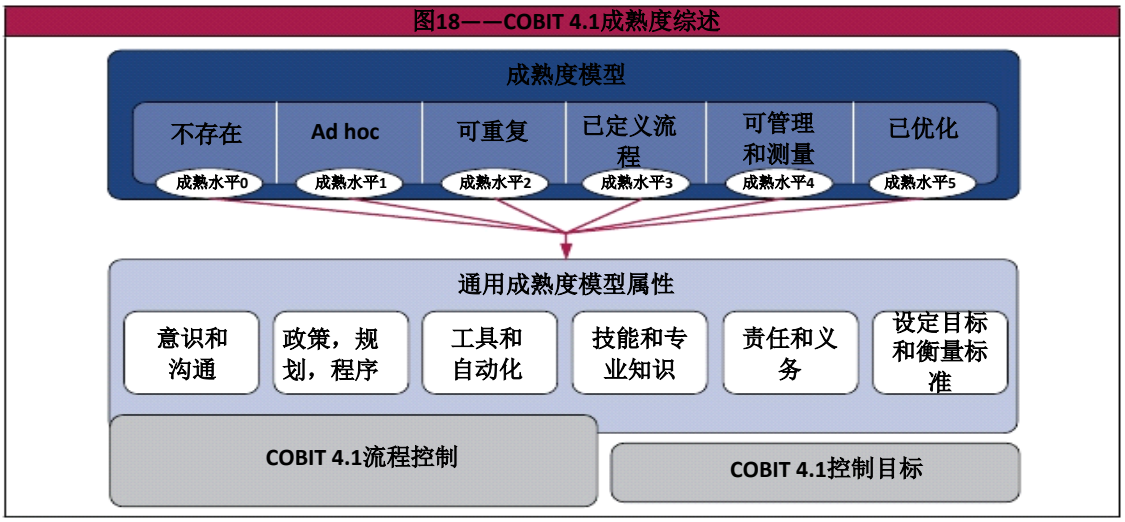

图 10.1　图表 18.COBIT 4.1 成熟度模型概要

使用 COBIT 4.1 成熟度模型实现流程改进目的（过程成熟度评估，确定目标成熟度水平并确定差距）需要使用以下 COBIT 4.1 元素。

- 首先，需要做一个流程控制目标是否满足的评估。
- 其次，包含在每个流程的管理指导方针中的成熟模型可以用来获取流程的成熟度轮廓。
- 另外，通用的 COBIT 4.1 成熟度模型提供 6 个截然不同的属性，它们可以在每个流程应用，并且帮助获取关于流程成熟水平的更详细的认识。
- 流程控制是一般控制目标，做流程评估时，它们也需要审查，流程控制与通用的成熟度模型属性部分重叠。

COBIT 5 流程性能方法可以总结如**图 19** 所示

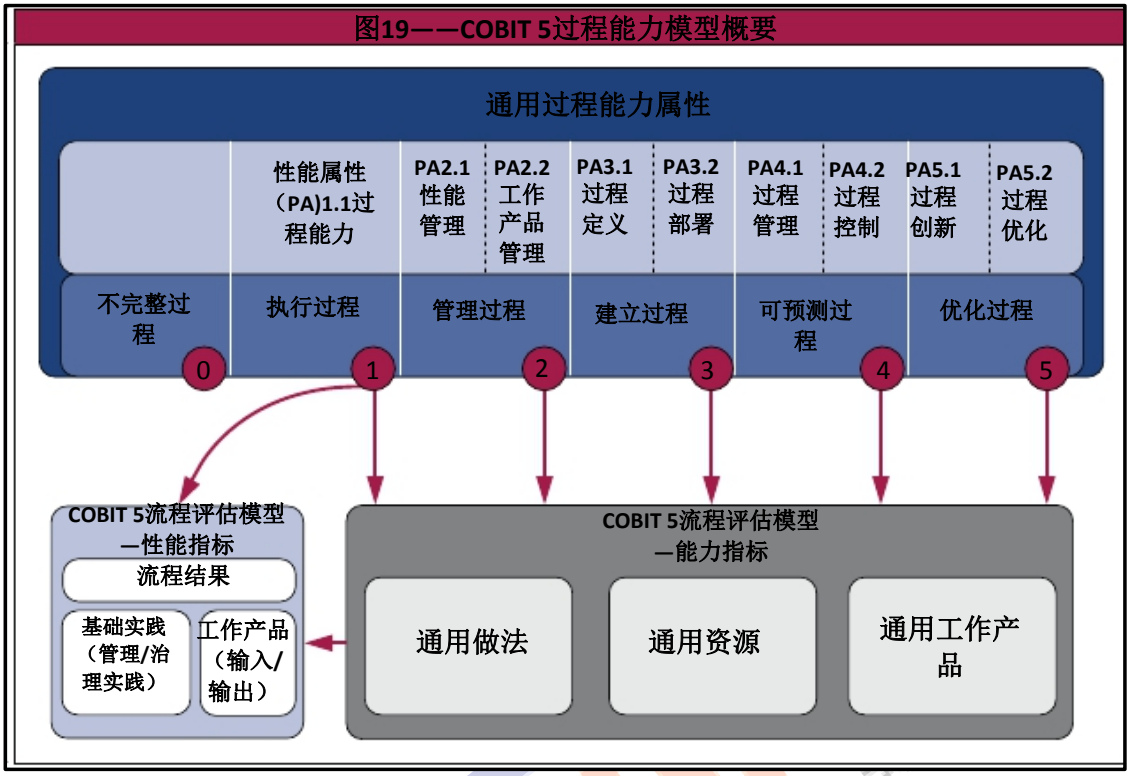

图 10.2　图表 19.COBIT 5 过程能力模型概要

有流程可以实现的 6 种性能等级，包括一个“不完整流程”的称号，如果其中的实践没有达到流程的预期目标。

- **0 不完整流程**—流程没有实施或没能实现流程目标。在这个级别，几乎　没有或者没有任何流程目标的系统实现的证据。
- **1 执行过程**（1 个属性）—实施过程实现流程目标。
- **2 管理过程**（2 个属性）—上面所描述的执行过程现在以管理的方式实施（规划、监控和调整），其工作产品得到适当的建立、控制和维护。
- **3 建立的流程**（2 个属性）—上面所描述的管理过程现在使用已定义的、能够实现流程输出的流程进行实施。
- **4 可预测的流程**（2 个属性）—上面所描述的建立的过程现在在定义的限制内运行以实现它的流程输出。
- **5 优化的流程**（2 个属性）—上面所描述的可预测的过程不断改善以满足有关的当前和预期的业务目标。

只有已经完全达到下面的级别，每一个性能等级才可以实现。例如，流程性能等级 3（建立的流程）需要在很大程度上实现流程定义和流程部署属性，在充分实现流程性能 2（管理过程）的属性之上。

流程性能等级 1 与更高性能等级之间有重要的区别，流程性能等级 1 的实现需要在很大程度上实现流程性能属性，这实际上意味着流程正在顺利进行和企业获得所需的结果，然后较高的能力水平为其添加不同的属性。在此评估计划中，实现性能等级 1，甚至等级是 5，对于一个企业已经是重要成果。请注意，每个独立的企业应当选择（基于成本——效益和可行性的原因）它的目标或希望的水平，这很少是最高等级之一。

基于 ISO/IEC 15504 的流程性能评估和目前 COBIT 4.1 成熟度模型（和类似的 Val IT 和风险 IT 基于域的成熟度模型）的最重要区别可以总结如下：

- 在流程方面，ISO/IEC 15504 定义的性能水平的命名与意义与目前 COBIT 4.1 成熟水平相当不同。
- 在 ISO/IEC 15504 中，性能水平被一组 9 种流程属性定义，这些属性覆盖一些目前 COBIT 4.1 成熟度属性和/或流程控制覆盖的领域，但只到特定程度并以不同的方式。

一种与 ISO/IEC 15504:2 兼容的过程参考模型的要求描述了任何将评估的过程，即任何 COBIT 5 的治理和/或管理流程：

- 根据其目的与结果描述流程
- 流程描述不应包括任何高于 1 级的衡量框架的任何方面，这意味着任何超出 1 级的流程属性的特征不能出现在一个流程的描述中。一个流程是否被衡量与监控或者它是否得到正式描述等，不能成为一个流程的描述或任何管理做法/活动的一部分。这意味着流程描述如《COBIT 5：促成流程》所包括的一样，只包含实现实际流程的目的和目标的必要的步骤。
- 如之前描述的一样，适用于所有企业流程的通用属性现在定义为评估模型的 2 到 5 级。这些流程在出版物《COBIT 第三版》中产生重复控制目标并在 COBIT 4.1 中归为流程控制（PC）目标。

10.3 实际应用的不同

从之前的描述可知，很显然，有一些与流程模型变化联系的实际应用方面的不同，用户需要了解这些变化并能够将它们考虑到实际的行动计划中。

需要考虑的主要变化包括：

- 尽管由于数量规模和用于形容它们的词的明显的相似之处而尝试对比 COBIT 4.1 和 COBIT 5 评估结果，但因为在范围、关注点和意图方面的差异，比较是困难的，如**图 20** 所示。
- 一般来说，COBIT 5 过程能力模型的的得分要小一些，如**图 20** 所示。在 COBIT 4.1 成熟度模型中，一个流程可以达到等级 1 或等级 2 而不需要完全实现整个流程目标。在 COBIT 5 流程性能等级中，这将导致一个较低的得分为 0 或 1。

COBIT 4.1 和 COBIT 5 能力规模大约可被视为'地图'，如**图 20** 所示。

- COBIT 5 中详细的流程内容在每个流程中不再有特定的成熟度模型，因为在 ISO /IEC 15504 的过程能力评估方法并不需要这甚至不允许此方法。相反，该方法定义“过程参考模型”所要求的信息（该过程模型可用于评估）：

—流程的描述，有目的的陈述

—基本的做法，在 COBIT 5 术语中，这是相当于过程治理或管理的做法的等同物

—工作产品，在 COBIT 5 术语中，输入和输出的等同物

- COBIT 4.1 成熟度模型产生一个企业的成熟度轮廓，这个轮廓的主要目的是确定在哪个维度或为哪个属性有需要改进的具体弱点。当有改善焦点而不是为报道目的而获得一个成熟度的数字的需求时，企业使用这种方法。在 COBIT 5 中，流程评估模型为各性能属性和如何应用的指导提供了一个测量尺度，所以每个流程的评估可以针对这九个功能属性。
- COBIT 4.1 成熟度属性和 COBIT 5 流程性能属性并不是完全相同的，它们在一定程度上重叠或相互映射，如**图 21** 所示。一直应用 COBIT 4.1 成熟度模型属性方法的企业可以重用它们现有的评估数据，并对它们在基于**图**

21 的 COBIT 5 属性评估进行重新分类。

图 20——成熟水平（COBIT 4.1）和流程能力水平（COBIT 5）对照表		
COBIT4.1 成熟度模型级别	**基于 ISO/IEC 15504 的流程能力**	**背景**
5 已优化——基于与其他企业的不断完善和成熟度建模，过程已细化到一个良好的实践水平。IT 以集成的方式用以使工作流程自动化，并提供工具以提高质量和效益，使企业快速适应变化	**5 级：优化流程**——4 级可预测的过程不断完善，以满足相关的当前和预计的业务目标。	**企业角度——企业知识**
4 管理和可衡量——管理监控和衡量与步骤的遵守情况，并在流程不能有效地工作时采取行动。流程在不断改善，并提供良好的实践。自动化和工具以有限或零散的方式使用。	**4 级：可预测的流程**——3 级建立的过程现在在以实现其过程的结果的范围内运行。	
3 已定义的流程——流程已经标准化和记录，并通过培训沟通。按照要求，这些应遵循流程，然而，这是不可能的，将检测出偏差。流程本身并不复杂，但却是现行做法的正规化。	**3 级：建立过程**——2 级管理过程使用所定义的，能够实现其过程的结果的过程现在实现了。	

	2 级：管理过程——2 级执行过程现在以管理方式实施（计划，监控和调整），其工作产品得到适当的建立，控制和维护。	**示例角度——个人知识**
2 可重复但直观——流程已经发展到是由承担着相同任务的不同的人遵守相似的程序的阶段。没有正规的培训或标准程序的交流，其责任留给个人。高度依赖个人的知识，因此，可能出现错误。	**1 级：执行过程**——已实施的过程实现其过程目标。 **备注：如果流程结果没有达到的话。有些归为成熟度模型 1 的过程将列为 155040 是可能的，**	
1 最初/Ad hoc——有证据表明企业已认识到问题存在并需要加以解决，然而，并没有标准化的流程，而是有 ad hoc 方法，往往被应用于个人或逐案的基础上。整体的管理方式杂乱无章。		
0 不存在——完全缺乏可识别的过程。企业甚至还没有认识到有要解决的问题。	**0 级：不完整的过程**——过程没有实施或者未能达到其目的	

图 10.3　图表 20.成熟水平（COBIT4.1）和过程能力水平（COBIT 5）对照表

图21—成熟度属性（COBIT4.1）和流程属性（COBIT 5）对照表									
COBIT 4.1成熟度属性	COBIT 5过程能力属性								
	过程性能	性能管理	工作产品管理	过程定义	过程部署	过程管理	过程控制	过程创新	过程优化
认识和沟通									
政策，规划和程序									
工具和自动化									
技能和专业知识									
责任和义务									
目标设定和衡量标准									

图表 21.成熟度属性（COBIT4.1）和流程属性（COBIT 5）对照表

10.4 这些变化的好处：

与 COBIT 4.1 成熟度模型相比，COBIT 5 的过程能力模型的优点包括：对正在处理的过程的关注的改善，以保证它正在实现其目的并产生预期的需要的结果。

- 通过减少重复的东西以减少内容，因为 COBIT 4.1 成熟度模型评估需要使用许多特定的元件，包括通用的成熟度模型，过程成熟度模型，控制目标和流程的控制以支持流程的评估。
- 改善了过程能力评估活动及评价的可靠性及可重复性，同时减少利益相关者在评估结果上的争论与分歧。
- 提高了过程能力评估结果的可用性，因为这个新模型为实现内部和潜在的外部目的，为将要执行的更正规的更严格的评估建立了一个基础。
- 与普遍接受的过程评估标准一致，也因此强烈支持市场上的过程评估方法。

10.5 在 COBIT 5 中执行过程能力评估

ISO / IEC 15504 标准规定，过程能力评估可以用于各种用途，也适用于不同严谨的程度。可以是内部的目的，着重于与企业领域和/或内部收益的流程改进之间的比较，或者也可以是外部目的，着重于正式的评估，报告和认证。

COBIT 5 的基于 ISO / IEC 15504 的评估方法，一直促进下列目标的实现，自 2000 年以来这已成为一种重点 COBIT 的方法：

- 使得治理机构和管理层能够为过程能力设定基准；
- 使得高水平的“现在”和“将来”健康性检查能支持与过程改善有关的，治理主体与管理层投资决策的制定。
- 提供差距分析和和改善计划信息以支持合理的改善项目的确定。
- 向治理主体和管理层提供评估等级以衡量和监控当前的能力。

这一节介绍了为什么可以用 COBIT 5 过程能力模型执行一个高水平的评估以实现这些目标。

评估能力 1 级和更高级之间有区别。事实上，如前所述，过程能力级别 1 描述了过程是否达到预期目的，因此是一个要达到的非常重要的级别，也是使能力要达到更高的水平的基础。

评估过程是否实现其目标，或者换句话说，达到 1 级能力，可以通过：

1、审查过程的结果，因为他们为每个流程中所描述的详细过程描述，并使用 ISO / IEC 15504 评定量表，为实现不同程度的目标分配一个等级。这个量表包括以下的评定等级：

- N（未实现）——在评估过程中，有很少或没有证据显示定义的属性的实现程度。（0％至 15％的实现率）
- P（部分实现）——在评估过程中，有一些证据显示定义的属性的一种方法或部分完成。在考察属性的完成情况的某些方面可能是不可预知的。（15％至 50％的实现率）
- L（基本上实现）——对定义在评估过程中的属性，有系统化方法的证据和显著的成就。在评估过程中可能存在的一些有关此属性的弱点。 （50 至 85％的实现率）
- F（完全实现）——对定义在评估过程中的属性有一个完整和系统的方法和证据，并充分实现。在评估过程中不存在有关该属性明显的弱点。（85 至 100％的实现率）

2、此外，流程（治理或管理）实践可以使用相同的评定量表评估，表示在何种程度上的基本实践得到应用。

3、要进一步完善评估，也可以考虑工作产品以确定一个具体的评估属性已经实现到何种程度。

虽然确定目标的能力级别取决于每个企业，许多企业将有希望将他们所有的流程达到一级水平。（否则，拥有这些流程还有什么意义？）如果没有达到这个水平，没有达到这个水平的原因会立即从以上解释的方法中得出，可以确定改进计划：

1. 如果一直没有实现所需的流程的结果，那么该流程不符合目标，需要加以改进。
2. 流程实践的评估将揭示哪些做法是缺乏的或是失败的，并使这些实践实施和/或改善发生，并允许实现所有流程的成果。

对于较高的过程能力等级，从 ISO/IEC 15504:2 标准看，使用通用的做法。它们为每一个能力等级提供通用描述。

十一. 附录 B　企业目标—IT 相关目标之间的详细映射关系

在第 2 章解释了 COBIT 目标级联。

图 22 中的映射表的目的是演示如何支持企业目标（或转换成）IT 相关的目标。出于这个原因，表格中包含以下信息：

- 在列中，所有的 17 个通用的企业目标在 COBIT 5 定义，按 BSC 的维度进行分组。
- 在行中，所有的 17 个与 IT 相关的目标，也按 BSC 的维度进行分组。
- 每个企业的目标是如何支持 IT 相关的目标的映射。此映射使用以下尺度表示：

“P”代表主要关系，当有重要的关系时，即与 IT 相关的目标是实现企业目标的主要支持。

“S”代表次要关系，当仍然有一个强大的、但不太重要的关系是，即与 IT 有关的目标是实现企业目标的辅助支持。

例 7：映射表格

映射表表明人们通常会期望：

- 企业目标 7，业务服务连续性和可用性：
  - ✓ 主要取决于 IT 相关目标的实现
    - ➢ 04 受控的 IT 相关业务保险
    - ➢ 10 信息、流程基础设施和应用的安全性
    - ➢ 14 用于决策的可靠有用的信息的可得性
  - ✓ 也依赖于 IT 相关目标的实现，也依赖程度低一个等级
    - ➢ 01 IT 和业务战略的一致性
    - ➢ 07 IT 服务交付与业务要求的一致性
    - ➢ 08 应用、信息和技术解决方法的充分应用
- 沿相反的方向使用表格，以实现 IT 相关目标 09.IT 敏捷性将有助于多个企业目标的实现：
  - ✓ 主要的，企业目标：
    - ➢ 2.竞争产品和服务组合
    - ➢ 8.对不断变化的业务环境的快速响应
    - ➢ 11.优化的业务流程功能
    - ➢ 17.产品和业务创新文化
  - ✓ 低一个等级，企业目标：
    - ➢ 1. 业务投资的利益相关者价值
    - ➢ 3.受控的业务风险（资产维护）
    - ➢ 6.面向客户的服务文化
    - ➢ 13.受控的业务变化方案
    - ➢ 14.业务和员工的工作效率
    - ➢ 16.技能和积极进取的人

该表的创建基于以下输入：

- 安特卫普大学管理学院 IT 调整和治理研究所的研究
- 在 COBIT 5 的发展和审查过程中获得的额外的评论和专家的意见

应用图 **22** 中的表格时，请考虑第二章做的关于如何应用 **COBIT 5** 目标级联的评价。

图 22——COBIT 5 企业目标与 IT 相关目标之间的映射关系

			企业目标																
			业务投资的利益相关者	竞争性产品和服务的投	受控的业务风险（保护	遵守外部法律法规	财务透明	以客户为中心的服务文	业务服务连续性和可用	对业务环境变化的灵活	基于信息的战略决策	服务交付成本的优化	业务流程职能的优化	业务流程成本的优化	受控的业务变化方案	运营效率和员工生产力	遵守内部政策	技术熟练和积极的员工	产品和业务创新文化
			1.	2.	3.	4.	_	6.	7.	8	9.	10.	11.	12.	13.	14.	15.	16.	17.
IT 相关目标			**财务**					**客户**					**内部因素**					**学习和成长**	
财务	01	IT 和业务战略的一致性	**P**	**P**	**S**			**P**	**S**	**P**	**P**	**S**	**P**	**S**	**P**			**S**	**S**
	02	IT 业务合规性和对遵守外部法律和法规的业务的支			**S**	**P**											**P**		
	03	执行管理者对 IT 相关的决	**P**	**S**	**S**					**S**	**S**		**S**		**P**			**S**	**S**
	04	受控的 IT 相关业务的风险			**P**	**S**			**P**	**S**		**P**			**S**		**S**	**S**	
	05	从 IT 驱动的投资和服务组	**P**	**P**				**S**		**S**		**S**	**S**	**P**		**S**			**S**
	06	IT 成本，收益和风险的透	**S**		**S**		**P**				**S**	**P**		**P**					
客户	07	与业务需求一致的 IT 服务	**P**	**P**	**S**	**S**		**P**	**S**	**P**	**S**		**P**	**S**	**S**			**S**	**S**
	08	应用程序，信息和技术解	**S**	**S**	**S**			**S**	**S**		**S**	**S**	**P**	**S**		**P**		**S**	**S**
内 部	09	IT 敏捷性	**S**	**P**	**S**			**S**		**P**			**P**		**S**	**S**		**S**	**P**
	10	信息，流程基础设施和应			**P**	**P**			**P**								**P**		

因素	11	IT 资产，资源和能力的优	**P**	**S**						**S**		**P**	**S**	**P**	**S**	**S**			**S**
	12	通过集成到业务流程中的	**S**	**P**	**S**			**S**		**S**		**S**	**P**	**S**	**S**	**S**			**S**
		应用和技术启用和支持业																	
	13	按时，按照预算交付产生	**P**	**S**	**S**			**S**				**S**		**S**	**P**				
		收益的方案，并满足要求																	
	14	对决策可靠有用信息的可	**S**	**S**	**S**	**S**			**P**		**P**		**S**						
	15	遵守内部政策的 IT			**S**	**S**											**P**		
学习和成长	16	能干和积极进取的业务和	**S**	**S**	**P**			**S**		**S**						**P**		**P**	**S**
	17	知识，专业知识和业务创	**S**	**P**				**S**		**P**	**S**		**S**		**S**			**S**	**P**

图 11.1 图表 22.COBIT 5 企业目标与 IT 相关目标的映射关系

十二. 附录 C　IT 相关目标—IT 相关流程之间详细的映射关系

这个附录包括 IT 相关目标和 IT 相关流程之间的映射关系表和 IT 相关流程是如何支持它们的，作为第二章解释的目标级联的一部分。

图表 23 包括：

- 在纵列中，在第二章中，定义了所有 17 个通用的 IT 相关目标，按 IT BSC 维度分组。
- 在行中，所有的 37 个 COBIT 5 流程，依据范围分组。
- 每一个 IT 相关目标如何被 COBIT 5 IT 相关流程支持的映射关系，这一映射关系用以下尺度表示：

“P”代表主要关系，当有一个重要关系时，即 COBIT 5 流程是实现 IT 相关目标的主要支持。

“S”代表次要关系，当有一个仍然很强，但不太重要的关系时，即 COBIT 5 流程是实现 IT 相关目标的次要支持。

例 8：APO13 管理安全

流程 AP013 管理安全将有助于：

- 主要的，实现 IT 相关目标：
  - —02 IT 遵守并支持业务遵守外部的相关法律与法规
  - —04 受控的 IT 相关业务风险
  - —06 IT 成本、效益和风险的透明度
  - —10 信息，流程基础架构与应用的安全性
  - —14 用于决策制定的可靠与有用的信息的可用性
- 弱一个等级，对 IT 相关目标的实现：
  - —07IT 服务交付与业务要求的一致性
  - —08 应用程序、信息和技术解决方案的充分运用

这个表格的创建基于以下输入：

- 安特卫普大学管理学院 IT 调整和治理研究所的研究
- 在 COBIT 5 的发展和审查过程中获得的额外的评论和专家的意见

应用图 23 中的表格时，请考虑第二章做的关于如何应用 COBIT 5 目标级联的评价。

图 23——COBIT 5 IT 相关目标与流程之间的映射关系

			IT 相关目标																
			IT 和业务战略的一致性	IT 业务合规性和对遵守	执行管理者对 IT 相关的	受控的 IT 相关业务的风	从 IT 驱动的投资和服务	IT 成本，收益和风险的	与业务需求一致的 IT 服	应用程序，信息和技术	IT 敏捷性	信息，流程基础设施和	IT 资产，资源和能力的	通过集成到业务流程中	按时，按照预算交付产	对决策可靠有用信息的	IT 遵守内部政策	能干和积极进取的业务	知识，专业知识和业务
			01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17
COBIT 5 流程			**财务**					**客户**					**内部因素**					**学习和成长**	
评价,指导和监控	EDM01	确保治理框架的设	**P**	**S**	**P**	**S**	**S**	**S**	**P**		**S**	**S**	**S**	**S**	**S**	**S**	**S**	**S**	**S**
	EDM02	确保收益实现	P		**S**		**P**	**P**	**P**	**S**			**S**	**S**	**S**	**S**		**S**	**P**
	EDM03	确保风险优化	**S**	**S**	**S**	**P**		**P**	**S**	**S**		**P**	**S**		**S**	**S**	**P**	**S**	**S**
	EDM04	确保资源优化	S		**S**	**S**	**S**	**S**	**S**	**S**	**P**		**P**		**S**			**P**	**S**
	EDM05	确保利益相关者透	**S**	**S**	**P**			**P**	**P**						**S**	**S**	**S**		**S**
调整,规划	AP001	管理 IT 管理框架	**P**	**P**	**S**	**S**			**S**		**P**	**S**	**P**	**S**	**S**	**S**	**P**	**P**	**P**
	AP002	管理战略	**P**		**S**	**S**	**S**		**P**	**S**	**S**		**S**	**S**	**S**	**S**	**S**	**S**	**P**
	AP003	管理企业架构	**P**		**S**	**S**	**S**	**S**	**S**	**S**	**P**	**S**	**P**	**S**			**S**		**S**

和 组	AP004	管理创新	S		S	P			P	P		P	S		S				P
织	AP005	管理投资组合	P		S	S	P	S	S	S	S		S		P	S			S
	AP006	管理预算和开支	S		S	S	P	P	S	S			S		S				
	AP007	管理人力资源	P	S	S	S			S		S	S	P		P		S	P	P
	AP008	管理关系	P		S	S	S	S	P	S			S	P	S		S	S	P
	AP009	管理服务协议	S			S	S	S	P	S	S	S	S		S	P	S		
	AP010	管理供应商		S		P	S	S	P	S	P	S	S		S	S	S		S
	AP011	管理质量	S	S		S	P		P	S	S		S		P	S	S	S	S
	AP012	管理风险		P		P		P	S	S	S	P			P	S	S	S	S
	AP013	管理安全性		P		P		P	S	S		P				P			

图 23——COBIT 5 IT 相关目标与流程之间的映射关系(续)

	IT 相关目标																
	IT和业务战略的一致性	IT业务合规性和对遵守	执行管理者对IT相关的	受控的IT相关业务的风	从IT驱动的投资和服务	IT成本，收益和风险的	与业务需求一致的IT服	应用程序，信息和技术	IT敏捷性	信息，流程基础设施和	IT资产，资源和能力的	通过集成到业务流程中	按时，按照预算交付产	对决策可靠有用信息的	IT遵守内部政策	能干和积极进取的业务	知识，专业知识和业务
	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17

COBIT 5 流程			财务					客户					内部因素					学习和成长	
构建，获得和实施	BAI01	管理方案和项目	P		S	P	P	S	S	S			S		P			S	S
	BAI02	管理需求定义	P	S	S	S	S		P	S	S	S	S	P	S	S			S
	BAI03	管理解决方案识别	S			S	S		P	S			S	S	S	S			S
	BAI04	管理可用性和能力				S	S		P	S	S		P		S	P			S
	BAI05	管理组织变革启用	S		S		S		S	P	S		S	S	P				P
	BAI06	管理变革			S	P	S		P	S	S	P	S	S	S	S	S		S
	BAI07	管理变更的验收和				S	S		S	P	S			P	S	S	S		S
	BAI08	管理知识	S				S		S	S	P	S	S			S		S	P
	BAI09	管理资产		S		S		P	S		S	S	P			S	S		
	BAI10	管理配置		P		S		S		S	S	S	P			P	S		
交付，服务和支持	DSS01	管理运营		S		P	S		P	S	S	S	P			S	S	S	S
	DSS02	管理服务请求和事故				P			P	S		S				S	S		S
	DSS03	管理问题		S		P	S		P	S	S		P	S		P	S		S
	DSS04	管理连续性	S	S		P	S		P	S	S	S	S	S		P	S	S	S
	DSS05	管理安全服务	S	P		P			S	S			S	S		S	S		
	DSS06	管理业务流程控制		S		P			P	S		S	S	S		S	S	S	S
监控，评价	MEA01	监控，评价和评估性	S	S	S	P	S	S	P	S	S	S	P		S	S	P	S	S
	MEA02	监控，评价和评估内		P		P		S	S	S		S				S	P		S

和 评估	MEA03	**监控，评价和评估与外部要求的一致性**		**P**		**P**	**S**		**S**			**S**					**S**		**S**

图 12.1　图表 23. IT 相关目标与流程的映射关系

十三. 附录 D　利益相关者需求和企业目标

第四章说明了目标级联的单独步骤，从利益相关者需求开始一直向下到促成因素目标。

第二章包括一个典型的关于 IT 治理与管理问题的表格。从利益相关者的观点来看，知道这些问题如何联系到到企业目标是有趣的。因此，**图 24** 被包括进来，它显示了内部利益相关者需求如何与企业目标相联系的一个列表。

这个表格可以用来帮助基于特定利益相关者需求设置和优先考虑特定的企业目标或 IT 相关的目标，当使用这些图表与其他目标等级表时，可以应用同样的预防措施，即每个企业情况不同，这些表格不能以机械的方式使用，而是作为一个推荐的通用的关系的集合应用。在**图 24** 中，如果某个目标需要考虑某项需求，则填充利益相关者需求与企业目标交叉点（这里用字母“ P ”代表填充）。

图 24——COBIT 5 企业目标与治理和管理问题之间的映射关系

利益相关者需求	业务投资的利益相关者价值	竞争性产品和服务的投资组合	受控的业务风险（保护资产）	遵守外部法律法规	财务透明	以客户为中心的服务文化	业务服务连续性和可用性	对业务环境变化的灵活响应	基于信息的战略决策	服务交付成本的优化	业务流程职能的优化	业务流程成本的优化	受控的业务变化方案	运营效率和员工生产力	遵守内部政策	技术熟练且积极的员工	产品和业务创新文化
	1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14	15.	16.	17.
我如何从使用 IT 中获得价值？终端用户对 IT 服务质量满意吗？	P	P				P	P						P			P	P
我如何管理 IT 性能？		P			P				P	P	P	P		P			
我如何利用新技术发现战略机遇？	P	P						P					P			P	P
我如何建立和构造最佳 IT 部门？								P		P	P	P		P	P	P	
我对外部供应商的依赖度有多少？IT 外包协议管理得如何？我			P	P						P							

如何从外部供应商得到保障?																	
对信息的要求（控制）是什么?				**P**				**P**							**P**		
我处理所有 IT 相关的风险了吗?			**P**			**P**		**P**							**P**		
我是在高效有弹性地运营 IT 吗?					**P**	**P**											
我如何控制 IT 的成本？我如何以最切实有效的方式使用 IT 资源？最切实有效地采购选择是什么?										**P**		**P**		**P**			
我有足够的 IT 人员吗？我如何发展和保持他们的技能？我如何管理他们的绩效?										**P**		**P**		**P**			
我如何获得 IT 保障?				**P**											**P**		

图 13.1　图表 24. COBIT 5 企业目标与治理管理问题的映射关系

十四. 附录 E　COBIT 5 与最相关的相关框架和标准的映射关系

14.1 引言

这个附录将 COBIT 5 与管理范围内最相关的应用的标准和框架进行对比。对 ISO/IEC 38500 是通过基于 ISO/IEC 38500 的原则的对比进行的。对其它的对比，使用了一种带格式的表格，其中 COBIT 5 流程与所涉及的标准或框架的等同内容进行映射。

14.2 COBIT 5 和 ISO/IEC 38500

以下总结了 COBIT　5 如何支持采用标准的原则和实施方法。标准，ISO / IEC 38500:2008——企业信息技术治理，基于六个关键原则。这里解释了每个原则的实际运用，连同 COBIT 5 指南如何促成好的实践。

ISO/IEC 38500 原则

原则 1——责任

这在实践中意味着：

业务（客户）和 IT（供应商）应该在一个合作模式中合作，利用有效的基于积极和信任关系的沟通，表明清晰的相关责任与义务。对于规模较大的企业，IT 执行委员会（也称为 IT 战略委员会）代表董事会行事，由董事会成员主持，是一种非常有效的评估、指导和监督在企业中使用 IT 以及向董事会就关键的 IT 问题提出建议的机制。小型和中型企业拥有更简单的命令结构和较短的通信路径，它们的董事在监督 IT 活动时，需要采取更直接的办法。在所有情况下，适当的治理组织结构、角色和责任，必须由治理机构授权，提供重要的决定和任务的明确的所有权和问责制，这应该包括与关键的第三方 IT 服务提供商的关系。

ISACA 指南如何促使好的实践：

1. COBIT 5 框架定义了若干治理企业 IT 的促成因素。“流程 ”促成因素

和“组织结构”促成因素，结合 RACI 表是在这种环境中特别相关的。它们极力主张责任的分配，并为董事会成员和所有关键相关的流程和活动的管理者提供示范角色和活动。

2. 《COBIT 5 实施》解释了当实施或加强 IT 治理安排时，利益相关者和其他有关各方的责任。
3. COBIT 5 有两个层面的监测，第一个层次是与治理环境有关，流程 EDM05 确保利益相关者透明用建立目标及相关指标的通用方法，解释了董事在监测和评估 IT 治理和 IT 性能方面的作用。

原则 2：战略

这在实践中意味着：

IT 战略规划是一个复杂和关键的任务，要求企业的业务部门和 IT 战略计划之间的密切协调，优先安排最有可能实现预期效益的计划，并有效地分配资源也是至关重要的。高层次的目标需要被转化成可实现的战术计划，确保最小的失败和意外，我们的目标是提供支持战略目标的价值，同时考虑到相关的与董事局风险偏好有关的风险。尽管以自上而下的方式的级联计划是重要的，但计划还必须是具有灵活性和适应性，以满足瞬息万变的业务需求和 IT 机遇。

此外，存在或缺乏 IT 能力可以启用或阻碍企业的战略，因此，IT 战略规划应包括透明的和适当的 IT 能力规划。这应包括评估当前的 IT 基础设施和人力资源的能力，以支持未来的业务需求和使竞争优势和/或优化成本的未来的技术发展的考虑。IT 资源包括与许多外部产品供应商和服务供应商的关系，其中一些人可能在支持业务方面发挥了关键作用。因此，治理的战略采购是一个非常重要的战略规划活动，需要行政级别的指导和监督。

ISACA 指南如何促成好的实践

1. COBIT 5 提供了具体的关于管理 IT 投资和（特别是，在这个过程中 EDM02 确保在治理领域的收益交付）战略目标应如何通过适当的业务案例支持的指导。
2. COBIT 5 APO 领域解释了为有效地规划所需的流程和内部和外部的 IT 资源的组织，包括战略规划、技术和架构的规划、组织规划、创新规划、

投资组合管理、投资管理、风险管理、客户关系管理和质量管理。也解释了业务和 IT 目标的一致性，用通用的例子说明他们如何基于业界研究它们如何支持所有 IT 相关的流程的战略目标。

3. 确定和调整企业目标与 IT 相关的目标的工作，提出了企业目标、IT 相关的目标和促成因素的级联关系的更好的理解，其中包括 IT 流程。它提出了一个实力雄厚的 17 个通用企业的目标和 17 个通用的 IT 相关的目标的列表，在不同部门之间验证和优先，连同两者之间的连接信息，它提供了建立一个业务目标与 IT 目标之间的通用级联关系的良好的基础。

原则 3：收购

这在实践中意味着：

IT 解决方案的存在，以支持业务流程，因此必须注意不考虑在隔离或只是一个“技术”项目或服务的 IT 的解决方案。另一方面，不适当技术架构选择，未能保持当前和适当的技术基础设施，或缺乏熟练的人力资源，可能导致项目失败，无法维持业务或价值减少的业务。IT 资源的收购应被视为更广泛的 IT 业务变化的一部分。所收购的技术也必须支持和运作现有的和计划中的业务流程和 IT 基础设施。实施也并不只是一个技术问题，而是一个组织的变化、修订后的业务流程、培训、变化促成因素。因此，IT 项目应进行更广泛的企业级的包括其他项目的一部分的变化方案，满足全方位的需要，以帮助确保取得圆满成功的活动。

ISACA 指南如何促成好的实践

1. COBIT 5 EDM 领域提供了经历他们的整个生命周期（收购，实施，运行和退役）的治理和管理 IT 业务的投资的指导，APO05 管理集合流程针对如何运用有效的组合和这样的投资计划管理，以帮助确保实现利益和成本进行优化。
2. COBIT 5 APO 领域提供收购计划的指导，包括投资规划，风险管理，计划和项目规划，质量规划。
3. COBIT 5 BAI 领域提供收购和实施 IT 解决方案所需的过程，包括定义的要求、确定可行的解决方案、准备、文档和培训，使用户和业务运行新系统的指导。此外，提供指导，以帮助确保该解决方案进行测试和变化的管

理业务和 IT 环境的适当控制。

4. COBIT 5MEA 领域和 EDM05 流程包括指导董事如何可以监测和评估收购过程以及内部控制，以帮助确保收购得到妥善管理和执行。

原则 4：绩效

这在实践中意味着：

有效的绩效衡量取决于正在解决的两个关键方面：绩效目标明确的定义和建立有效的指标来监控目标的实现。还需要一个性能测量过程，以帮助确保性能一致和可靠的监测。达到设定的目标是从上往下，并与高层次的、经批准的管理目标相一致，有效的治理指标建立从下往上，使在各级层被管理阶层监控目标的实现的方式相一致。两个关键的治理的成功因素是利益相关者的目标的批准和接受问责的董事和经理的目标的实现。它是一个复杂和技术方面的问题，因此，重要的依靠言语方式表达目标、指标和绩效报告来对利益相关者实现透明度，因此可以采取适当的行动。

ISACA 指南如何促成好的实践：

1. COBIT 5 框架提供全方位的 IT 相关的流程和其它促成因素目标和指标的通用例子，并说明它们如何与业务目标，使企业能够适应他们自己的特定用途。
2. COBIT 5 提供关于设置 IT 目标与业务目标相一致的指导管理，并介绍如何监视这些目标、应用目标和衡量。流程性能可以使用 ISO/ IEC 15504 履约能力评估模型评估。
3. 两个关键的 COBIT 5 过程提供特定的指导：
   - APO02 管理战略重视设定目标。
   - APO09 管理服务协议注重定义适当的服务和服务目标并记录在他们的服务水平协议。
4. 在流程 MEA01 监测、评价和评估性能和一致性，COBIT 5 对这项活动的执行管理职责提供了指导。
5. 计划 COBIT 5 保证指南将解释如何保证专业人士可以为董事提供独立的对 IT 性能的保证。

原则 5：合规性

这在实践中意味着：

在今天的全球市场，通过互联网和先进的技术支持，企业需要遵守的法律法规和监管要求越来越多。由于近年来的公司丑闻和财务失败，在更严厉的法律和法规的存在和影响的会议室有明显增强的意识。利益相关者需要加强保证企业遵守法律、法规和符合他们的管理环境的良好的企业管治常规。此外，因为 IT 促使企业之间的无缝业务流程，也是不断增长的帮助确保合同包括 IT 相关的重要领域，如隐私，保密，知识产权和安全要求的需求。

董事需要确保遵从外部需求作为战略规划的一部分，而不是作为一种昂贵的事后处理。他们还需要设置高层话语权和为建立他们管理政策和程序，确保实现企业目标，风险最小且符合实现。高层管理人员，必须取得性能和一致性之间的适当平衡，确保绩效目标不危及遵守，反之，一致性制度是恰当的，并不过分限制业务运作。

ISACA 指南如何促成好的实践：

1. COBIT 5 治理和管理实践提供了一个在企业中建立一个适当的控制环境的基础。过程能力评估使管理 IT 过程能力评估和衡量。
2. COBIT 5 流程 APO02 管理策略有助于确保 IT 计划和整体管理目标之间有对应关系，包括治理要求相一致。
3. COBIT 5 流程 MEA02 监测、评价和评估内部控制制度，评估控制是否足以满足董事要求。
4. COBIT 5 流程 MEA03 监测、评价和评估遵守外部的要求有助于确保外部要求遵守的确定，董事设定遵守的方向，并且作为一个整体符合企业要求的一部分符合本身进行监测、评估和报告。
5. COBIT 5 计划保证指南解释了审计员如何提供来自内部指令或外部的法律、法规或合同规定的内部政策，确认可以提供独立保证遵守和坚持，已经由负责采取任何纠正措施，以解决任何遵守差距及时的流程的所有者。

原则 6：人的行为

这在实践中意味着：

实施任何 IT 功能的变化，包括 IT 治理本身，通常需要显着的文化和行为的改变，企业内部以及与客户和业务伙伴。这可能会造成员工之间的恐惧和误解，因此需要认真管理人员如果要保持积极从事执行。董事必须明确沟通目标，并积极支持建议修改。加强人员培训和技能是关键方面的变化，尤其是考虑到技术的快速移动的性质。人们都受到它的影响，在企业中的各级，作为利益相关者，管理者和使用者，或作为专家提供 IT 相关的服务和解决方案业务。以外的企业，它会影响客户和业务伙伴，并越来越多地使国家内部以及跨越国界的自助服务和自动化的公司间交易。的 IT 支持的业务流程，同时带来了新的利益和机会，他们也进行类型的风险增加。个人隐私和欺诈等问题日益关注，以及这些风险和其他类型的需要进行管理，如果人们相信他们使用的 IT 系统。信息系统也极大地影响工作实践，通过手工程序自动化。

ISACA 指南如何促成好的实践：

以下 COBIT 5 促成因素（包括流程）提供指导与人类行为有关的要求：

1. COBIT 5 的促成因素包括人才、技能和能力以及文化、道德和行为。对于每一个促成因素模型通过实例说明提出了关于如何处理促成因素。
2. COBIT 5 流程 APO07 管理人力资源解释了个人与企业目标对应如何表现，应保持什么 IT 专业技能，以及如何定义的角色和责任。
3. COBIT 5 过程 BAI02 管理需求定义有助于确保应用程序的设计，以满足人类的操作和使用要求。
4. COBIT 5 流程 BAI05 管理组织变革的启用和 BAI08 管理知识帮助确保用户能够有效地使用系统。

此外，ISACA 协会为专业人员提供进行有关 IT 治理的关键角色四个认证，知识主体 COBIT 5 的内容大体覆盖：

- 企业 IT 管理认证（CHEIT）
- 系统审计员信息认证（CISA）
- 系统安全经理信息认证（CISM）
- 风险信息系统控制认证（CRISC）

证书的持有人在执行这种角色的能力和经验都已经证明这些。

ISO/IEC 38500 评估、直接和监控

ISACA 指南如何促成好的实践：

COBIT 5 流程模型控制模型有 5 个流程，并且每个流程定义了 EDM 实践，这是在 COBIT 5 治理相关的活动定义的主要位置。

14.3 与其它标准对比

COBIT 5 考虑一些其他的标准和框架，这些标准在附录 A 中列出。

COBIT 5：启用过程包含了每个 COBIT 流程和包含附加指南的相关标准与框架最相关部分之间高水平示意图。

在这一部分，一个包括每个框架与标准简要描述，说明 COBIT 5 涉及了那个领域。

ITIL V3 2011 和 ISO/IEC 20000

以下 COBIT 5 领域被 ITIL V3 2011 和 ISO/IEC 20000 包括：

- DSS 领域流程子集
- BAI 领域流程子集
- APO 领域一些流程

ISO/IEC 27000 系列

以下 COBIT 5 领域被 ISO/IEC 27000 覆盖：

- EDM、APO 和 DSS 中安全和风险相关流程
- 其它领域流程各种安全相关活动
- MEA 领域监控和评估活动

ISO/IEC 310000 系列

以下 COBIT 5 领域被 ISO/IEC 31000 覆盖：

- 在 EDM 和 APO 领域风险相关管理流程

TOGAF

通过 TOGAF，以下 COBIT 5 地区和领域涵盖：

- 在 EDM（经济学）域的建筑板 TOGAF 的组件资源相关的流程，治理架构和架构成熟度模型映射到资源优化配置。

- 在 APO 域的企业架构过程。在 TOGAF 的核心是架构开发方法（AMD），映射到了 COBIT 发展的架构愿景的做法（AMD 的阶段 A），定义的参考架构（AMD 阶段 B，C 和 D），选择的机会和解决方案（AMD 阶段 E），并定义架构的实施（AMD 阶段 F，G）的。TOGAF 的组件映射到了 COBIT 5
  - ✓ ADM 需求管理
  - ✓ 架构的原则
  - ✓ 利益相关者管理
  - ✓ 业务转型准备评估
  - ✓ 风险管理
  - ✓ 基于能力的规划
  - ✓ 架构合规
  - ✓ 架构合同

资源成熟度模型集成（CMMI）（发展）

CMMI 所涵盖的下列 COBIT 5 的地区和领域：

- 应用建设和收购相关的流程，BAI 域
- 从 APO 域的一些组织和质量相关的流程

PRINCE2

通过 PRINCE2，以下 COBIT 5 的地区和领域的：

- 在 APO 域组合相关的流程
- 在 BAI 域的方案和项目管理流程

图 25 描述了 5 COBIT 的和其他的标准和框架之间的相对覆盖。

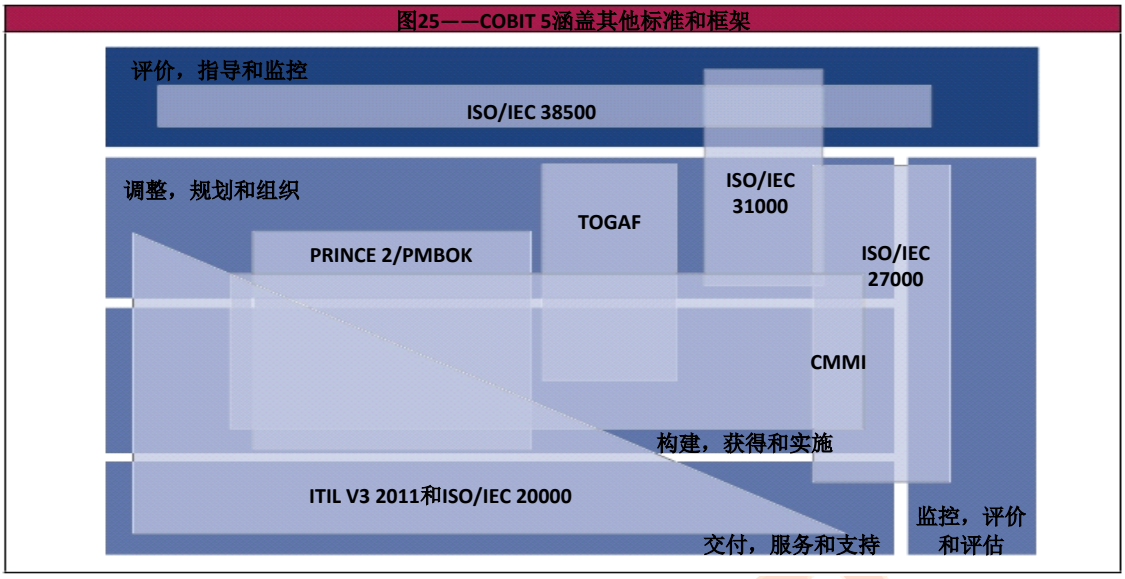

图 14.1　图表 25.COBIT 5 其它标准与框架覆盖范围

十五. 附录 F　COBIT 5 信息模型与 COBIT 4.1 信息标准的对比

COBIT4.1 的 7 个信息标准——有效性、效率、完整性、可靠性、可用性、保密性、合规性如何与 COBIT 5 的信息促成因素的信息质量的类别和维度联系？如附录 G 中**图 32** 所示。

以下表格包括含两列：

- 第一列罗列了 COBIT 4.1 七个信息标准的每一个。
- 第二列罗列 COBIT 5 的替换物，即相应的促成因素目标。

图 26—COBIT 5 与 COBIT4.1 信息标准的等同物

COBIT4.1 信息标准	COBIT 5 的等同物
有效性	如果信息满足了为完成特定任务而使用信息得信息消费者的需求，那么它是有效的。如果信息消费者可以使用信息执行任务，那么该信息是有效的。这对应于以下信息质量目标：适量，相关性，可理解性，解释性，客观性
效率	虽然有效性把信息视为一种产品，效率更多地与获取和使用信息的有关，所以它与“信息作为一种服务”的观点相一致。如果满足信息消费的需求的信息可以用一种简单的方法获得和使用，那么信息的使用是高效的。这对应于以下信息质量目标：可信度，可访问性，易于操作，美誉度。
完整性	如果信息具有完整性，那么它是没有错误的、完整的。它对应信息的以下质量

	目标：完整性，准确性。
可靠性	可靠性常常被看作是准确性的代名词，然而，也可以说，如果它是真实可信的，那么信息是可靠的。相对于完整性，可靠性更主观，与认知更相关，而不只是事实。它对应于以下信息质量目标：可信度，美誉度，客观性。
可用性	可用性是信息的质量目标之一，位于可访问性和安全性标题下。
保密性	保密性对应“限制访问”的信息质量目标。
合规性	根据需求，合规性在信息必须符合规范这个意义上被任何信息质量目标所涵盖。 遵守规范更多的是使用信息过程中的一个目标或要求，而不是信息的内在品质。

图 15.1　图表 26.COBIT 5 与 COBIT4.1 信息标准的等同物

此表显示所有来自 COBIT4.1 的信息标准都被 COBIT 5 所涵盖，但 COBIT 5 的信息模型允许定义另一套标准，因此增加了 COBIT 4.1 标准的价值。

十六. 附录 G　COBIT 5 促成因素的详细描述

16.1 引言

本节包含了更详细的 COBIT 5 框架的七大类促成因素的讨论，它们最初在第 5 章介绍，在**图 27** 中重复。

图 16.1　图表 27.COBIT 5 通用促成因素

促成因素维度

四个通用的促成因素维度：

- **利益相关者**：每个促成因素都有利益相关者，即在促成因素中发挥了积极的作用的和/或对其感兴趣的各方。例如，流程有不同的执行流程活动和/或对流程输出有兴趣的不同各方，组织结构有利益相关者，每个有他/她

自己的角色和利益，是结构的一部分。利益相关者可以是企业内部或外部的，都具有自己的，有时是相互冲突的利益和需求。利益相关者的需求转化为企业的目标，进而转化为企业的 IT 相关的目标。如**图 7** 所示的利益相关者的列表。

- **目标**：每个促成因素有若干目标，促成因素通过实现这些目标提供价值。目标可以根据以下方面定义：
  - ✓ 促成因素的期待结果
  - ✓ 促成因素自身应用与运营

促成因素目标是 COBIT 5 个目标级联中的最后一步。目标可以进一步分割在不同的类别，例如：

——**内在质量**：促成因素准确、客观地工作，并提供准确、客观、有信誉的结果的程度。

——**环境质量**：鉴于其运作的环境，促成因素及其输出适合目标的程度。举例来说，结果应该是相关的，完整的，最新的，适当的，一致的，易于理解和易于使用的。

——**访问和安全**：促成因素及其结果可访问和安全的程度

- ➢ 如果需要或当需要时，促成因素是可用的
- ➢ 输出是安全的，即访问只限于那些被授权和需要它的人。

- **生命周期**：每一个促成因素都有生命周期，从成立以来，经过业务/使用寿命直到被处置掉，这适用于信息、结构、流程、政策等。生命周期的阶段包括：
  - ✓ 计划（包括概念发展和概念选择）
  - ✓ 设计
  - ✓ 建立/收购/创建/实施
  - ✓ 使用/操作
  - ✓ 评估/监控
  - ✓ 更新/弃置
- **好的实践**：对于每一个促成因素，可以定义好的实践。良好做法支持促成

因素目标的实现。良好做法就如何更好地贯彻落实促成因素，需要什么样的工作产品或投入和产出提供示例或建议。COBIT 5 框架提供 COBIT 5 促成因素的良好做法（例如，流程）的例子。对于其他的促成因素，可用于来自其他标准、框架等的指导。

促成因素性能管理

企业期望从应用促成因素中得到积极的结果，为了管理这些促成因素的性能，以下问题需要定期监控并从而随后解决（基于衡量指标）：

- 利益相关者额需求处理了吗？
- 促成因素目标实现了吗？
- 管理促成因素生命周期了吗？
- 好的实践应用了吗？

前两个问题对应促成因素的实际输出，用于衡量目标的实现程度的度量指标可称为“滞后指标”。

后两个问题对应促成因素自身的实际作用，这个指标可以称为“领先指标”。

对于每个促成因素有一个单独的部分，从与图 27 类似的图开始，但包括一些现有的促成因素的特定元素，指示红色和**粗体**。

接下来，四个组成部分中的每一个都要详细讨论，讨论的具体组成部分与其他促成因素的关系。

已包括一些例子以说明促成因素的意义和使用。

本节的目的是增加对 COBIT 5 框架的了解，以及促成因素概念如何用于实施和改善企业 IT 的治理和管理。

16.2 COBIT 5 的促成因素：原则、政策和框架

原则和政策是指落实到位的用于传达治理机构和管理层的指导和指示的交流机制。原则、政策和框架促成因素与通用促成因素比较的具体情况在**图 28 中**显示。

原则、政策和框架模型显示：

- **利益相关者**：原则和政策的利益相关者可以是企业内部和外部的。他们包括董事会和高级管理层、合规人员、风险管理、内部和外部审计、服务供

应商和客户、和监管机构。利害关系是双重的：一些利益相关者定义和制定政策，另一些人必须与政策保持一致，遵守政策。

- **目标和评价指标**：方针、政策和框架是传达企业规则，以支持治理目标和企业价值观的工具，由董事会和高级管理层定义。原则需要：
  - ✓ 数量限制
  - ✓ 用简单的语言表达，尽可能清楚地表达企业的核心价值观

政策提供如何将原则付诸实践以及他们影响决策如何与原则一致的更详细的指导。良好的政策是：

- ✓ 有效的——实现既定的目的
- ✓ 高效的——他们保证以最高效的方式实施原则。
- ✓ 非侵入式的——它们对那些必须遵守他们的人来说看上去符合逻辑，也就是说，他们不造成不必要的阻力。

访问政策：是否有一个在用的机制，为所有利益相关者提供方便的访问的政策呢？换言之，利益相关者是否知道在哪里找到这些政策？

图28—— COBIT 5促成因素：准则、政策和框架

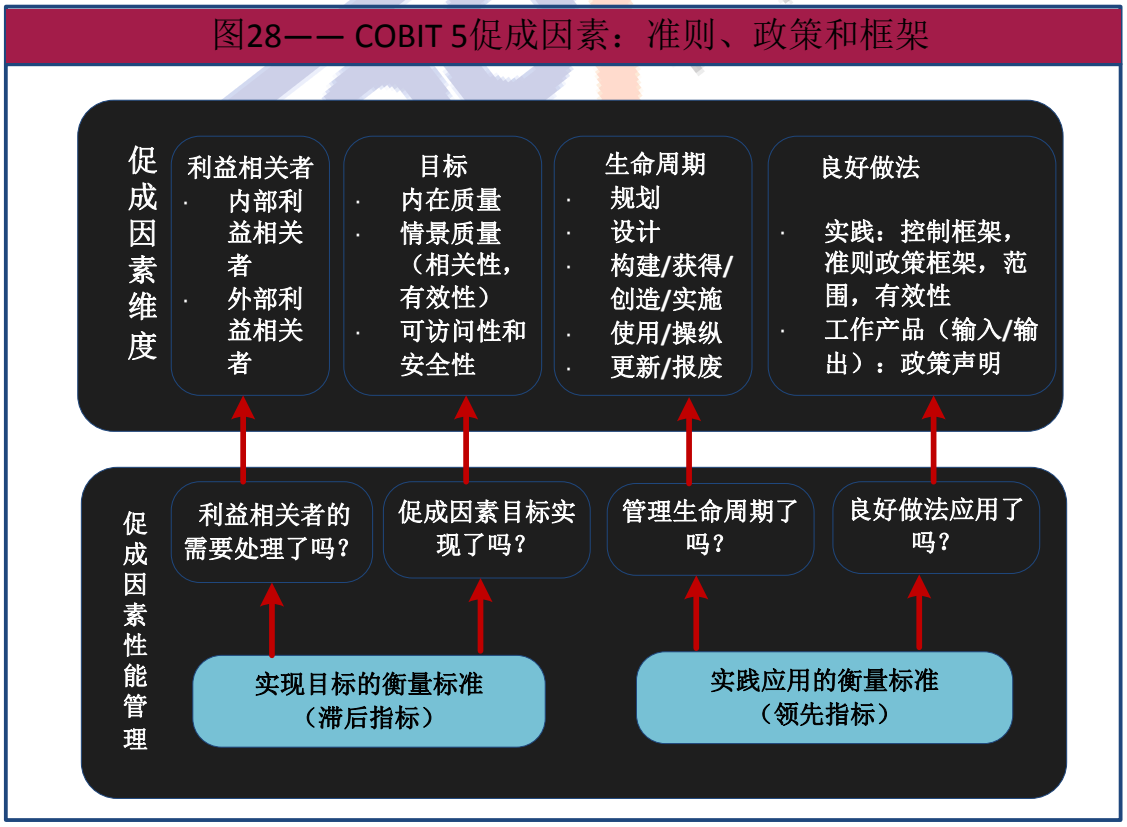

图 16.2　图表 28.COBIT 5 促成因素：原则、政策和框架

治理和管理框架应该为管理层提供结构、指导、工具等，允许企业合适的 IT 治理和管理。该框架应是：

- ✓ 综合的，涵盖所有必需的领域
- ✓ 开放的和灵活的，允许适应企业的具体情况
- ✓ 当前的，即反映了企业的当前方向和当前治理目标
- ✓ 对所有利益相关者可用和可访问

- **生命周期**——该政策有一个生命周期来支持实施完成既定的目标。架构是关键，因为它们为统一指导提供了框架。例如，一个政策框架提供了可以建立和维持的一致政策的框架，同时它在个人保险之间也提供了一种简单的指向性标识。

根据企业运作的外部环境，它们为了加强内部的控制，会随着法规要求的程度不同而不同，结果造就了一个很牢固的政策框架。货币政策是政策框架要考虑的一个方面——如果当政策评估或更新时，是否有完善的机制来确保人们能够知道这些更新，这些最新版本是否很容易被接受，那些废弃的框架是否被归档或废弃？

- **好的实践：**
  - ✓ 优良的实践要求，政策作为全部管理和管理框架的一部分，提供了一种所有政策都能适应的框架并且使这种联系基于以下原则。
  - ✓ 作为政策框架的一部分，下面的条目需要指出：
    - ➢ 作用域和有效性
    - ➢ 不遵循政策的结果
    - ➢ 例外处理的途径
    - ➢ 政策的承诺方式需要检查和判断
  - ✓ 一般公认的，在实际情况中管理和管理框架能够提供有价值的引导
  - ✓ 政策应该和企业的风险偏好相契合。政策是企业内部控制系统的关键一环，其目的是管理和限制风险。作为风险管理活动的一部分，要确定企业的风险偏好，并且应该反映在政策中。一个不愿意承担风险的

企业比激进的企业应该有更加严密的政策。

- ✓ 应该定期更新政策

- **与其他促成因素的关系**——与其它促成因素的联系包括：
  - ✓ 原则、政策和框架应该反映企业的文化与道德价值，并且应该鼓励他们所期待的行为。因此，在政策和文化、道德价值以及行为之间有很强的联系。
  - ✓ 流程控制实践和活动对于执行政策是最重要的。
  - ✓ 组织机构能够在它们的控制范围内确定和实施政策，并且他们的活动也由确定。
  - ✓ 政策同时也是信息，所以所有与信息适应的实践也与政策相适应。

例 9　社会媒体

一个企业从员工到利益相关者正考虑如何处理快速发展的社会媒体和压力。直到现在，因为安全因素，这个公司还坚持远离这类服务。

关于社会媒体，有来自各个方面的压力。员工希望得到与在家相同级别的酬劳，而公司本身为了市场和提升知名度也想应用和开发社会媒体的效益。

在企业网络和系统中，这个决定被用来确定政策，包括公司提供给员工的笔记本电脑。新政策在“接收可用的政策”这一策略下，可以和既有的政策框架契合，而较之前的政策更宽松。结果，为了解释施行新政策的理由，通信得到了发展。同时，对其他促成因素也产生了影响：

员工需要学习如何应用新媒体以避免为公司造成困境。他们需要根据公司正在发展和实施的得体行为而学习得体的行为。

许多关于安全性的程序需要改变。数据对度媒体是开放的，所以安全设置和配置必须改变，并且一些补偿措施也需要重新定义。

注意：如在本促成因素中所描述的，COBIT 5 是一个框架示例。

16.3 COBIT 5 的促成因素：流程

流程促成因素与通用促成因素比较的具体情况如图 29 所示。

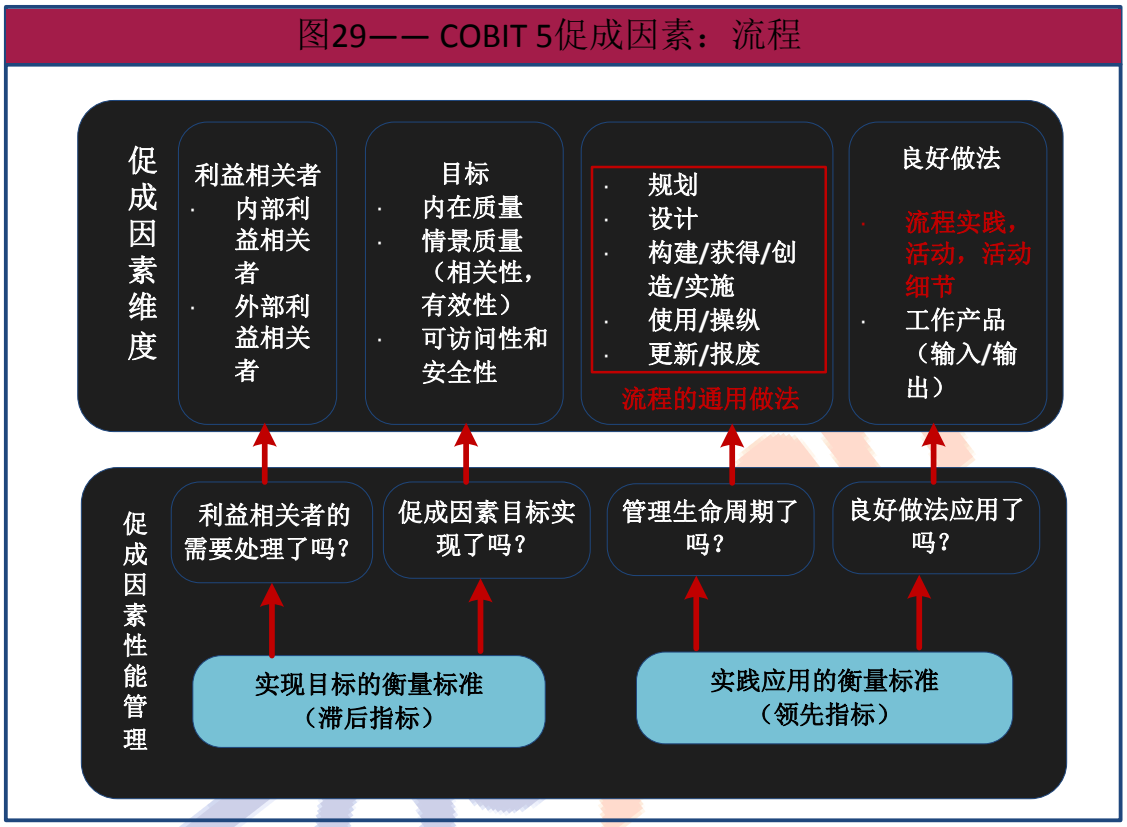

图 16.3　图表 29 COBIT 5 的促成因素：流程

流程被定义为**“受到企业的政策和程序影响的实践的集合，从多个来源（包括其他流程）获得输入，操纵输入并产生输出（例如：产品，服务）”**。

流程模型显示：

- **利益相关者**——利益相关者的流程有内部和外部之分，都有自己的角色；利益相关者和他们的责任通过各级 RACI 图表记录。外部利益相关者包括客户，业务伙伴，利益相关者和监管机构。内部利益相关者包括董事会，管理层，工作人员和志愿者。
- **目标**——目标流程的目标被定义为‘描述的过程中所需的结果的声明’。结果可能是一个假象，显著的能力的提升状态或其他流程。他们的目标级联，即一部分，流程目标的支持与 IT 相关的目标，这反过来又支持企业的目标。

流程目标可归纳为：

—**内在目标**——内在目标的流程是否有内在的质量？这是准确和具有良好的做法呢？这符合内部和外部的规则吗？

—**环境目标**——环境的目标是流程定制和适应企业的具体情况吗？和流程有关的是可以理解的，容易申请吗？

—**可访问性和安全性目标**——有需要时，辅助功能和安全目标的流程仍然是保密的，众所周知接触那些需要的。

在每个目标级联的水平，因此也为流程，指标定义来衡量这些目标的实现程度。指标可以被定义为“一个可以量化的实体，实现目标流程的测量。指标应该是智能具体，可衡量的，可操作的，相关并及时”。

有效和高效管理的促成因素，需要定义指标来衡量取得预期成果的程度。此外，性能管理的促成因素的第二个方面介绍了做法被应用的程度。在这里还要定义相关指标，以帮助促成因素管理。

- **生命周期**：每个流程都有一个生命周期。它被定义、创建、操作、监控、调整/更新或退休。如基于 ISO / IEC 15504 的 COBIT 的过程评估模型中定义的通用过程的做法可以协助定义、运行、监控和优化流程。
- **好的实践**：COBIT 5 过程包含一个流程参考模型，在这模型中更详细地描述了流程内部好的实践：实践、活动和详细的活动。

实践：

对于每个 COBIT 5 过程中，治理/管理实践为有效和实际的治理和管理企业 IT 提供了一套完整的高层次要求。它们分别是：

— 行动带来好处，优化的风险程度和优化资源的使用报表

— 符合有关普遍接受的标准和良好做法

— 通用的，因此需要为每个企业适应

— 在这个过程中覆盖业务和 IT 的角色球员（年底）

对于这些治理和管理实践，企业治理机构和管理需要做出选择：

— 选择那些适用的，并决定对那些将实施

— 添加和/或适应需要的做法

— 定义和添加在业务流程整合的非 IT 相关的做法

— 选择如何实现它们（频率，大跨度，自动化等）

— 接受不执行可能导致的风险。

活动：在 COBIT 中，操作流程采取的主要行为：

它们被定义为“成功企业的 IT 治理和管理，实现管理实践的指导。COBIT 5 活动提供如何、为何及如何实施每个治理或管理的实践来提高 IT 性能和/或解决 IT 解决方案和服务交付风险。使用这种材料是：

— 管理、服务提供商、最终用户和 IT 专业人员需要规划、建设、运行、监控企业 IT。

— 保证可能被要求提供他们的关于当前或建议实现必要的改进意见的专业人士。

一般的和特定的提供包括所有对必须且足够实现关键治理实践/运营实践的步骤的方法的一组完整的活动框架。它们在 GP/ MP 水平之下提供高层次的指导，来评估实际性能评估和考虑潜在的改进。活动：

— 描述了一套面向行动的必要和足够的实施步骤，以实现一个 GP/ MP

— 考虑过程的输入和输出

— 基于普遍接受的标准和良好做法

— 支持建立明确的角色和责任

— 非指令性的、需要进行调整和发展成适当的企业特定的程序

详细的活动：这些活动可能不在一个足够执行和进一步指导的详细水平上，可能需要：

— 从特定的相关标准和良好做法，如 ITIL、ISO / IEC27000 系列和 PRINCE2 上获取

— 在 COBIT 5 产品系列本身开发了额外发展及更详细或更具体的活动

输入输出：考虑到支持流程操作的需要，COBIT 5 输入和输出是流程工作产品/加工品。它们促使关键决策、提供流程活动的记录和审计跟踪，促使后续事件的发生。它们定义在关键的治理/管理实践层面，可能包括一些只能在流程中使用的并且往往是其他流程必要的输入工作产品。

外部良好做法可以存在于任何形式或详细程度，大多参照其他标准和框架。用户可以在任何时候参考这些外部良好做法，知道 COBIT 与相关标准一致，并且映射信息可用。

促成因素性能管理

企业希望从促成因素的使用得到积极的成果。为管理促成因素的性能，下列问题将定期基于测量（一个通用基础）监控和回答：

- 利益相关者需求满足了吗？
- 促成因素目标实现了吗？
- 管理促成因素生命周期了吗？
- 好的实践应用了吗？

在流程促成因素的情况下，前两项处理过程中的实际输出。可用于测量到目标的实现程度的度量称为“滞后指标”。在 COBIT 5：启用流程，一些每个流程的目标的度量得到定义。

后两项处理促成因素本身的实际运作，为这个指标可以被称为“领先指标”。

流程性能水平：一级 COBIT 5 包括一个 ISO/ IEC 15504 为基础的过程能力评估计划。COBIT 58 章讨论了这个问题，单独的 ISACA COBIT 5 的出版物提供进一步的指导。总之，流程能力水平衡量目标实现和好的做法的应用。

与其它促成因素的关系：流程和其他类别的促成因素之间的联系存在以下几个关系：

- 流程需要信息（作为输入的一种类型）并能产生信息（作为一种工作产品）
- 流程需要组织结构和运营的角色，如通过 RACI 表等 IT 指导委员会、企业风险委员会、董事会、审计、CIO、CEO 所表达。
- 流程产生也需要服务性能（技术设施、应用等）
- 流程会和将依赖流程
- 流程产生、需要、政策和程序来确保联系实施和执行
- 文化和行为的方面决定流程执行良好程度

实际应用流程促成因素的例子

例如 10 说明这一流程的促成因素，它的相互作用和促成因素范围。这个例子基于前文所述例 7。

COBIT 5 流程参考模型

管理和管理流程

COBIT 的指导原则之一是治理和管理之间的区别。本着这一原则，每家企业将期望实施治理流程和管理流程，为客户提供全面的治理和管理企业 IT 的流程。

当考虑在企业范围内的治理和管理的流程时，不同类型流程之间的区别在于流程的目标：

- **治理流程**：治理流程处理与利益相关者的治理目标（价值交付，风险优化和资源优化）包括实践和活动、旨在评估战略选择、提供方向和监测结果（EDM 与 ISO / IEC38500 标准的概念一致）。
- **管理流程**：与管理定义相一致，流程管理中的做法和活动覆盖涵盖企业 IT PBRM 责任区和提供覆盖 IT 的端到端业务。

例 10 流程促成因素互联

组织已为与 IT 相关的流程任命流程经理，负责在良好企业 IT 治理和管理的背景下，定义和运行有效和高效的 IT 相关的流程。

起初，流程经理将侧重于过程的促成因素，考虑促成因素维度：

- **利益相关者**：过程利益相关者包括所有流程的参与者，即所有负责的，有义务的，被咨询或通知（RACI）的各方，或活动过程。对于这一点，如 COBIT 5 中描述的 RACI 图表：启用可使用的流程。
- **目标**：对于每一个过程，需要定义适当的目标和相关指标。例如，对于管理过程 APO08 的关系（COBIT 5：启用流程），可以发现一组流程的目标和指标如下：

— **目标**：充分理解，记录和批准地业务战略，计划和要求。

  - **衡量标准**：与企业的业务需求/优先级一致的方案的百分比

—**目标**：企业和 IT 部门之间存在的良好关系。

  - **衡量标准**：用户的评价和 IT 人员满意度调查

- **生命周期**：每个流程都有生命周期，也就是说，它要创建、执行和监测，

并在需要时调整。最终，流程不复存在。在这种情况下，流程经理首先需要设计和定义过程。他们可以使用 COBIT 5 的多种元素：使流程设计流程，即明确责任和把流程分解成实践和活动，并定义（输入和输出）过程的工作产品。在以后的阶段，这个过程需要做得更强大和更有效率的，出于这一目的，过程管理者可以提高过程的能力水平。为该目的可以使用由 ISO/IEC 15504 启发的 COBIT 5 流程能力模型和流程能力属性如下：——过程能力 2 级需要实现两个属性：绩效管理和工作产品管理。第一个属性需要若干与规划阶段有关的活动：

- 所定义过程的性能目标。
- 计划过程表现。
- 定义执行过程中的责任。
- 确定资源。
- 等等。

相同的能力水平规定为监测流程的生命周期阶段的活动：

- 监测过程中的表现。
- 调整工艺性能以满足计划。
- 等等

—同样的方法可以用来获得指导，这些不同生命周期阶段来自处于过程能力增长阶段的不同性能属性。

- **良好做法**：COBIT 5 以充足的细节描述 COBIT 5 中流程的好的做法：启用流程，根据前点中提到的，启示性的和示范性的过程可以发现，并覆盖良好的企业 IT 治理和管理的全方位所需的活动。

除了流程的促成因素指导之外，流程经理可以决定看一些其他促成因素诸如：

- RACI 图表描述角色和职责。其他促成因素允许追溯到这一维度如：

— 在技能和能力的促成因素中，每个角色所需的技能和能力可以定义，也可以定义适当的目标（例如，技术和行为技能水平）和相关指标。

— RACI 图表还包含一些组织结构。这些结构可以在组织结构的促成因素

中进一步阐述，组织结构的促成因素可以提供结构的更详细的说明，预期成果和相关的指标，可以定义（例如，决策），可以定义好的做法（例如，控制范围，结构的管理原则，权限级别）。

- 原则和政策将流程正式化，规定过程存在的原因，它对谁适用，并如何使用过程。这是原则和政策促成因素重点关注的领域。

虽然两种类型的流程的结果不同，针对不同的受众

从过程本身的背景来看，所有的流程需要“规划”，“建设或实施”，“执行”和“监测”。

COBIT 5 流程参考模型

COBIT 5 不是指令性的，但是从以前的文本，，它明确主张企业实施治理和管理流程以便涵盖关键领域，如**图 30** 所示。

从理论上讲，只要覆盖基本的治理和管理目标，一个企业可以按照它认为合适的方法组织其流程。规模较小的企业可能有更少的流程;更大和更复杂的企业可能有多个流程，所有都包含相同的目的。

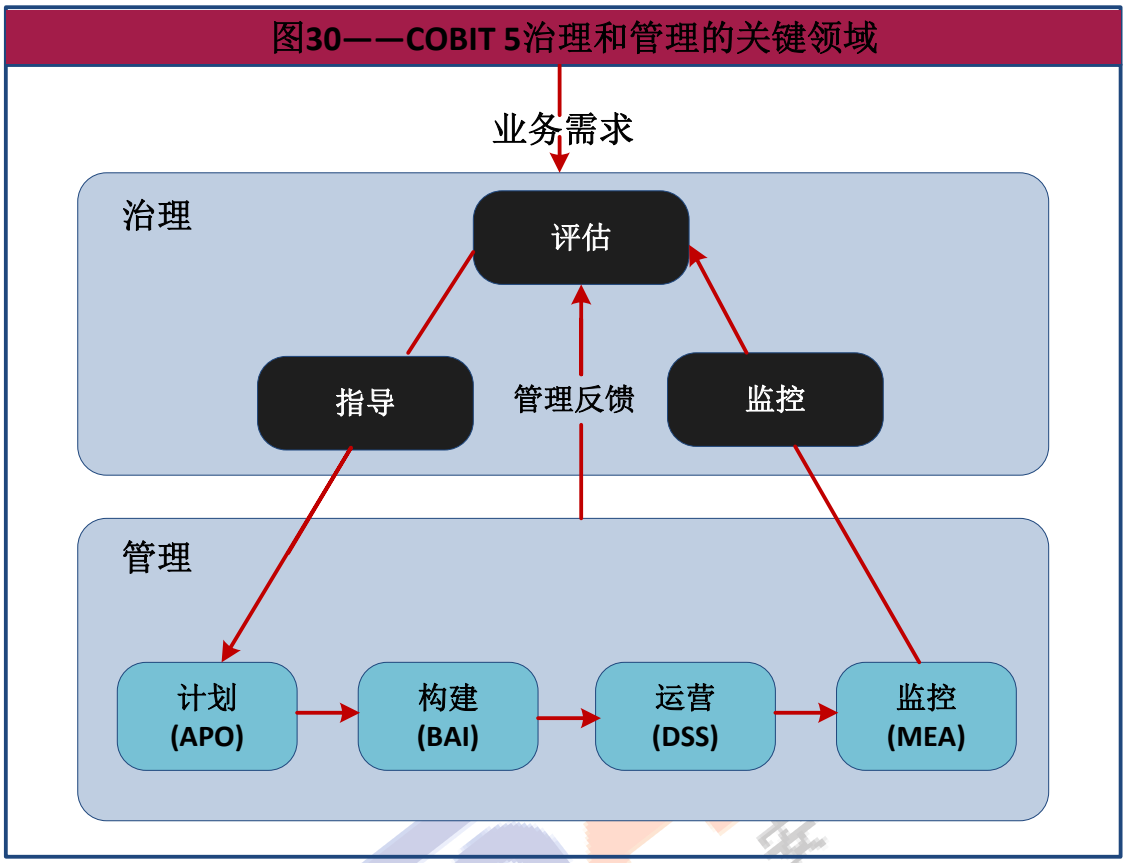

图 16.4　图表 30.COBIT 5 治理和管理的关键领域

尽管有以前的文本，COBIT 5 包括一个流程参考模型，定义和详细描述一些治理和管理流程。它提供了一个流程参考模型，代表企业中所有有关 IT 活动通常发现的过程，提供一个共同的 IT 运营官和业务经理都可理解的参考模型。所提出的过程模型是一个完整的，全面的模型，但并不是唯一可能的过程模型。考虑到具体情况，每个企业都必须定义其自身的流程组。

结合企业在 IT 活动所涉及的所有部件的运作模式和共同的语言，是走向良好治理的最重要和最关键的步骤之一。它还提供了一个框架，用于测量和监控 IT 性能，与服务提供商沟通并整合最佳管理做法。

COBIT 5 的过程参考模型将企业的 IT 治理和管理流程细分为两个主要活动领域—治理和管理——划分为过程域：

- **治理**——该领域包含五个治理过程，在每个过程中定义 EDM 实践。
- **管理**——这四个领域与 PBRM（COBIT 4.1 域的演变）的责任区域一致，他们提供 IT 月底到年底全覆盖。正如 COBIT 4.1 和以前的版本，每个域包含一些流

程数。虽然如前所述，大部分的流程需要在过程内或在解决的具体问题（例如，质量，安全）范围内“规划”，“实施”，“执行”和“监控”活动。当涉及到企业层面 IT 时，根据一般最相关的活动区域把它们放到域中。

在 COBIT 5 中，过程也包括全部业务范围和涉及到企业的 IT 治理和管理的活动，从而使过程模型成为真正的企业级模型。

COBIT 5 的过程参考模型继承了 COBIT 4.1 流程模型，同时集成风险 IT 和 Val IT 流程模型。**图 31** 显示了一套完整的 37 种 COBIT 5 中的治理和管理流程。根据前面所述的过程模型，所有流程的详细信息包括在 COBIT 5：启用流程中。

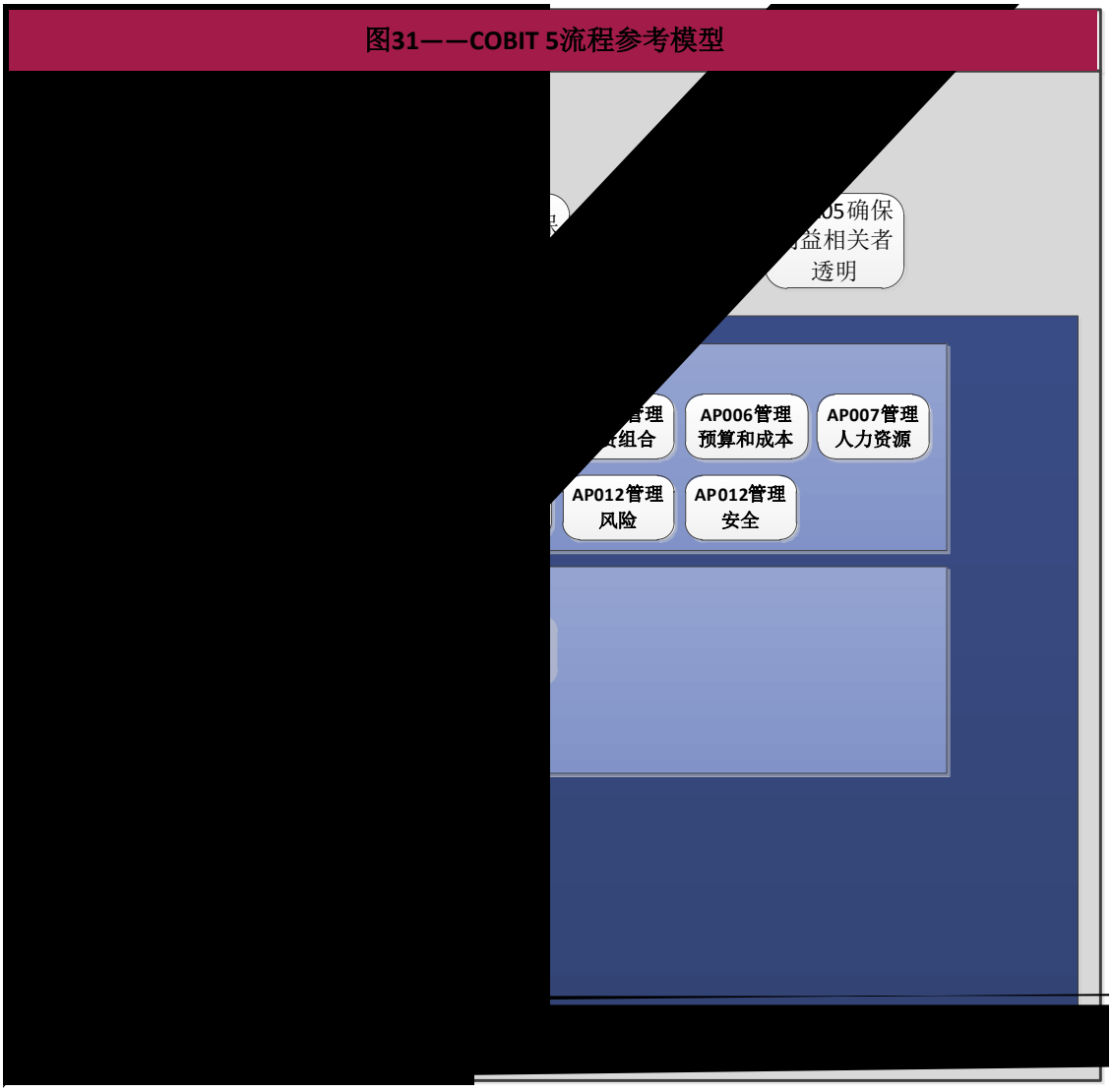

图 16.5　图表 31.COBIT 5 流程参考模型

16.4 COBIT 5 的促成因素：组织结构

组织结构促成因素与通用促成因素比较的具体情况如图 32 所示。

组织结构模型显示：

- **利益相关者**——组织结构的利益相关者可以是企业内部和外部的，他们包括结构的个别成员，其他结构，组织机构，客户，供应商和监管机构。他们的角色有所不同，包括决策，影响和建议。每个利益相关者的利害关系也各不相同，比如，他们在结构所作的决定中有什么利益？
- **目标**——组织结构促成因素本身的目标将包括有适当的任务期限，明确的管理方针和其他良好做法的应用。组织结构促成因素的成果应包括若干良好的活动和决策。
- **生命周期**——组织结构有生命周期。它被创建，存在和调整，最终可以解散。在其成立以来，必须定义任务—其存在的原因和目的。
- **好的做法**——组织结构的一些良好做法可按如下区分：

— 管理原则——关于结构将如何运作的实际安排，如会议的频率，文件和管理规则；

— 组成—结构拥有成员，他们是内部或外部利益相关者。

— 控制跨度——组织结构决策权利的边界— 权力/决策权等级——结构被授权采取的决定

— 权力委派——结构可以委托给（一个子集）向它报告的其他结构决策权。

— 升级程序——结构的升级路径说明在制定决策时，万一出现问题的情况下需要采取的行动。

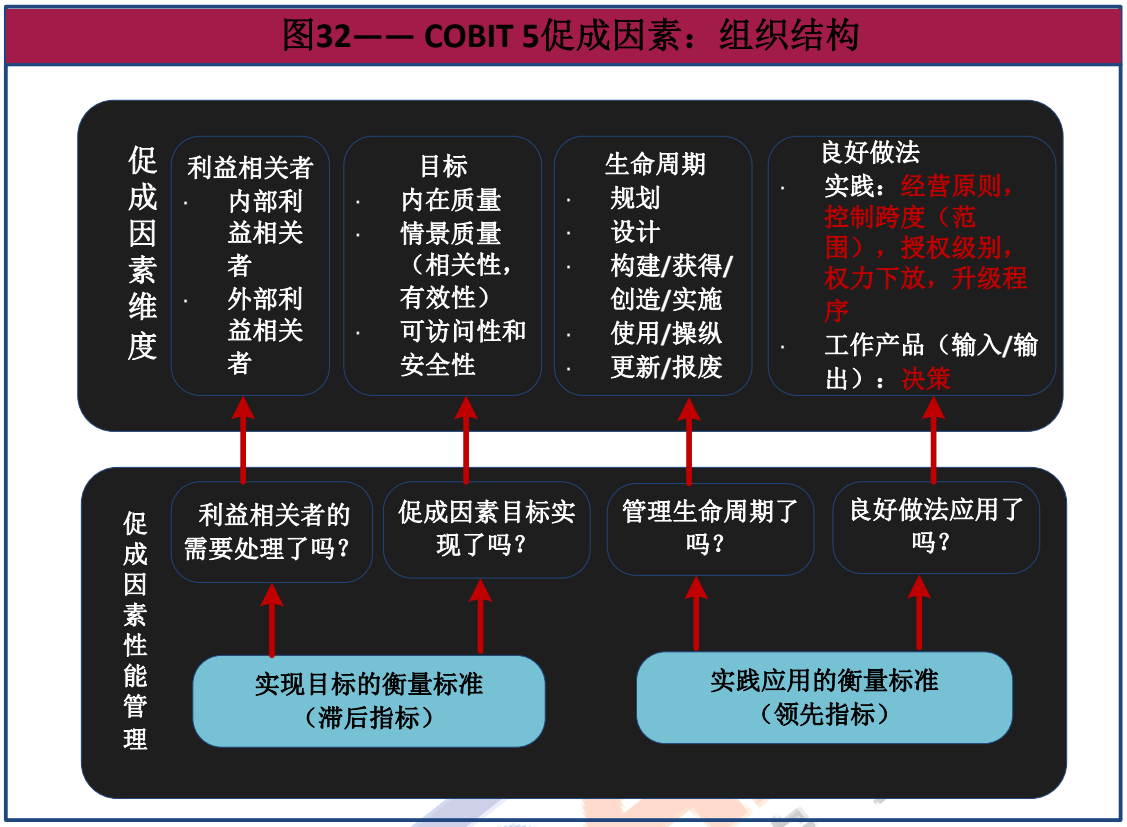

图 16.6　图表 32.COBIT 5 促成因素：组织结构

- **与其他促成因素的关系**——与其他促成因素的关系包括：
  - RACI 图表将企业中的组织结构和/或个别的角色与过程中的活动联系起来。他们了描述每个流程实践中的每个角色的参与程度：有责任，有义务，被咨询或通知。
  - 文化、道德和行为决定组织结构及其决策的效率和有效性
  - 组织结构的任务和工作原理由制定的政策框架指导
  - 输入和输出——在能够做出明智的决定前，结构需要输入（通常是信息），它也产生输出，比如，决策，其他信息，或者要求额外输入。

COBIT 5 中示范性的组织结构

诸如 COBIT 5 的过程模型的讨论中所提到的，已经建立了一个示范性的 COBIT 5 的过程参考模型，并在 COBIT 5 中详细描述：启用流程。该模型包括使用的许多角色和结构的 RACI 图表。**图 33** 描述了这些预定义的角色和结构。

注意：

- 他们不必与企业已实现的实际功能对应，但尽管如此，他们在描述结构目的或对于大多数企业来说仍然有效的角色的意义上仍提供价值。
- 这个表格的目的不是为每个企业规定通用的组织图表，而应被视作一个实例。

图 33 COBIT 5 的角色和组织结构	
角色/结构	**定义/描述**
董事会	企业的最高层管理人员和/或负责企业治理和整体控制企业资源的非执行经理的团体
CEO（首席执行官）	负责企业总体管理的最高级别的官员
CFO(首席财务官)	企业的负责财务管理的各个方面，包括金融风险和控制，可靠和准确的账户， 的最高级官员
COO(首席运营官)	企业的负责企业运营的最高级官员，
CRO(首席风险官)	对整个企业的风险管理的所有方面负责的企业的最高级官员。可设立 IT 风险官职位监督与 IT 相关的风险。
CIO(首席信息官)	企业的负责协调 IT 和业务战略及负责规划，资源和管理 IT 服务和解决方案的交付，以支持企业目标的最高级官员
CISO(首席信息安全官)	企业的负责所有形式的企业信息安全的最高级官员
高级商务师	负责特定业务单位或子公司的运作的高级管理人员
业务流程所有者 战略（IT 主管）委员会	负责过程在实现其目标的性能，推动过程改善，审批过程变化的人员 一组由董事会委任，以确保董事会参与，并随时了解 IT 相关的重大事项和决定的高级管理人员。该委员会负责管理 IT 技术的投资组合，IT 服务和 IT 资产，确保价值交付和风险管理。该委员会的主席通常是董事会成员，而不是 CIO。

（项目和方案）督导委员会	一组的利益相关者和专家，他们负责指导方案和项目，包括管理和监测计划，资源分配，收益和价值交付，方案和项目风险的管理。
架构委员会	一组的利益相关者和专家，他们负责指导企业架构相关的事项和决定，并设置架构的政策和标准
企业风险委员会	一组对支持企业风险管理（ERM）的活动和决策所需的企业级协作和共识负责的企业管理人员。可以建立 IT 风险理事会以更详细地考虑 IT 风险，并为企业风险管理委员会提出建议。
人事经理	企业负责规划和该企业内的所有人力资源方面的政策的最高级官员
合规	负责指导企业遵守法律，法规和合同的功能
审计	企业内负责提供内部审计的职能
架构经理	负责企业架构过程的资深人士
研发经理	负责 IT 相关解决方案的开发流程的资深人士
IT 运营经理	负责 IT 运营环境和基础设施的资深人士
IT 行政管理经理	负责 IT 相关的记录，并负责支持与 IT 相关的行政实物的资深人士
方案和项目管理办公室（PMO）	负责支持方案和项目经理，并收集，评估和报告其方案和组成项目的行为的信息的功能
价值管理办公室（VMO）	充当管理投资和服务组合总部，该组合包括评估和建议投资机会和业务案例，推荐价值治理/管理方法和控制，以及报告从投资和服务保持和创造价值的进展情况的功能
服务经理	管理，为针对特定客户（用户）或客户群的新的和现有的产品和服务的开发，实施，评价和日常管理的人员
信息安全经	管理，设计，监督和/或评估企业信息安全的人员

理	
业务连续性管理	管理，设计，监督和/或评估企业的业务持续性，以确保企业的关键职能经历破坏性事件后继续管理
保密主任	负责监测隐私法律的风险和业务影响，并负责指导和协调确保满足隐私指令的政策和活动实施的人员，也被称为数据保护官。

图 16.7　图表 33.COBIT 5 角色和组织结构

16.5 COBIT 5 的促成因素：文化、伦理道德和行为

文化、伦理道德和行为是指企业内部的个人和集体行为的集合。

文化、伦理道德和行为促成因素与通用促成因素比较的具体情况如图 34 所示。

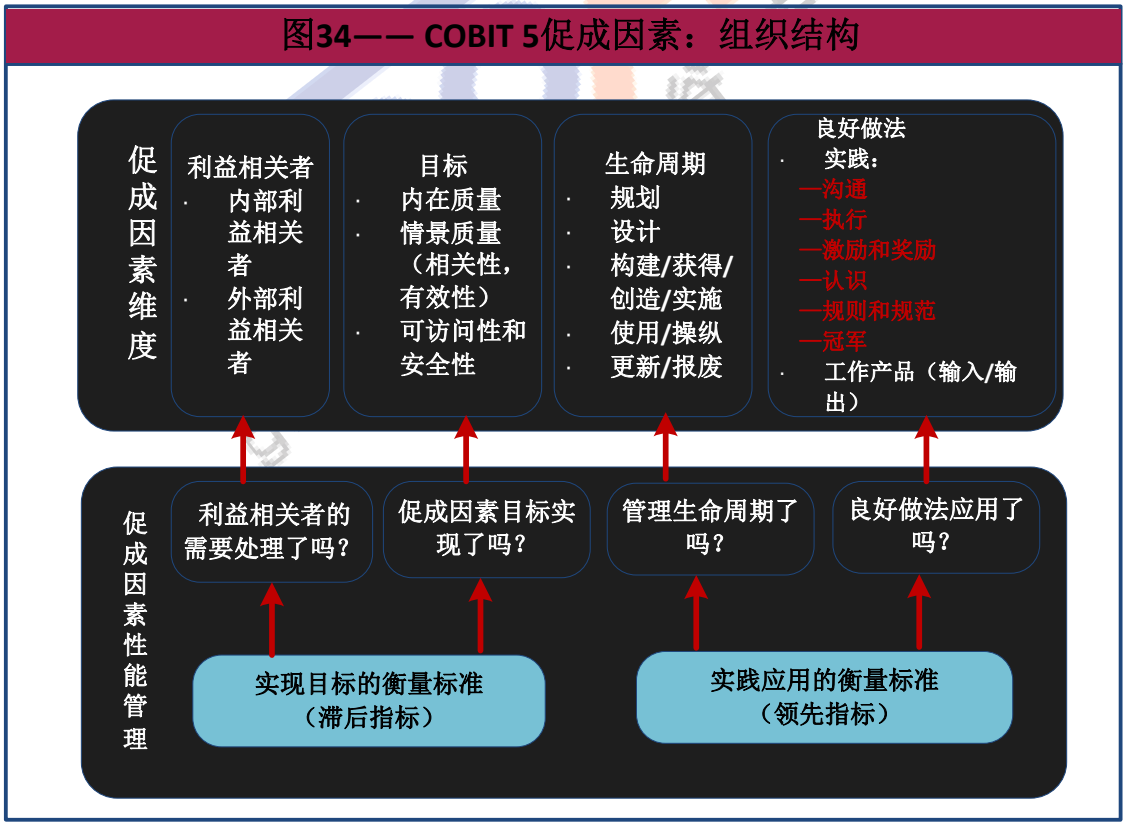

图 16.8　图表 34.COBIT 5 促成因素：文化、伦理道德和行为

文化、伦理道德和行为的模型如下：

- **利益相关者**——文化，伦理道德和行为的利益相关者可以是企业内部和外部的。内部利益相关者包括整个企业，外部利益相关者包括监管机构，例如，外部审计师或监督机构。奖金是双重的：一些利益相关者，例如，法律人员，风险经理，人力资源经理，薪酬委员会和人员，处理定义、执行和实施所需的行为，而其他必须遵守所定义的规则和规范。
- **目标**——文化，道德和行为的促成因素的目标涉及到：— 组织伦理，由该企业要生存下去的价值观确定— 个人伦理，由企业中的每一个人的个人价值观决定，并在在很大程度上取决于外部因素，如宗教，种族，社会经济背景，地理环境和个人经历— 个人的行为，共同决定一个企业的文化。许多影响因素，如上面提到的外部因素，而且企业内的人际关系，个人的目标和抱负，驱动行为。可能在这方面的相关某些类型的行为包括：

  —走向冒险的行为——企业认为可以吸收多少风险和它愿意承担何种风险？

  —走向遵守政策的行为——在何种程度上人们拥护和/或遵守政策？

  —走向负面结果的行为——企业如何应对的负面结果？比如，损失事件或错过机会。它会从它们中学到教训，并尝试调整吗？或者它会不深究根本原因就定罪吗？
- **生命周期**——一个组织的文化，伦理立场和个人行为等，都有其生命周期。从现有的文化开始，企业可以找出所需的更改，并努力实施。可以使用好的做法中描述的几个工具
- **好的做法**——在整个企业中创造，鼓励和维护所需行为的好的做法包括：— 整个企业所期望的行为和基础的企业价值观的交流— 所需的行为意识，通过高级管理人员和其他冠军的示范行为得以加强

  —鼓励所需行为的诱因和加强所需行为的威慑。个人行为和人力资源的奖励计划之间有明显的联系

  — 规则和规范，提供了更多期望的组织行为上的指导。这与企业实施的原则和政策之间关系明显。

- **与其他促成因素的关系**——与其他促成因素的关系包括：

— 过程可以设计得达到完美的水平，但如果这一流程的利益相关者不愿意按计划执行过程中的活动，即他们不遵守计划，将无法实现过程的结果。

— 同样，组织结构可以根据教科书设计和建造，但如果他们决定不落实，如因不同的个人安排，缺乏激励机制等，他们将不会产生像样的企业 IT 治理和管理。

— 原则和政策是企业价值观和所期望的行为的非常重要的沟通机制。

例 11 质量改进

企业在新的应用中多次面临着严重的质量问题。尽管完善的软件项目开发方法已经到位，软件问题往往会导致日常业务运作上的问题。

一项调查显示，根据开发团队成员和管理层的项目在预算范围内交付的及时性进行评估和奖励。他们的衡量不与质量标准或业务利益标准矛盾。因此，他们在开发过程中努力专注于交货时间和成本削减，如，测试时间。调查还显示，遵从既定的方法和程序几乎是不存在的，因为它会从开发预算中（有利于质量）花费更多的时间。此外，组织结构是这样的，以便于当开发成果移交给运营团队时，官方对开发的干预停止。从那时起，开发是通过建立事件管理和问题管理流程间接参与的。

这带给我们的教训是，必须对解决方案的开发管理层和团队采用更好的激励机制以鼓励高质量的工作。

例 12 IT 相关的风险

有关 IT 相关的风险方面的文化的不足或问题的一些症状包括：

- 真正的风险偏好与过渡到政策之间的偏差。对风险管理的实际价值可以合理的激进和冒险一些，而制定的政策反映更为保守的态度，因此在价值观和来实现价值的手段之间存在不匹配，这样必然导致冲突。例如，管理层激励组合和加强失调政策之间可能出现冲突。
- 存在一种“责备文化”，这种类型的文化无论如何应该避免，相关和有效的沟通是最有效的抑制剂。在责备文化中，当项目不能按时交货或不符合期望时，业务单位往往职责 IT。这样做，他们没有意识到业务部门的参与，预先

影响了项目的成功。在极端情况下，业务单位可能注定因不能满足期望而受责备，因为该单位从未明确沟通过。 “指责游戏”只会削弱跨单位之间的有效沟通，进一步助长拖延。如果要促进整个企业的协作，执行领导必须查明并迅速控制责备文化。

16.6 COBIT 5 的促成因素：信息

引言—信息周期

信息的促成因素涉及到与企业相关的所有信息，而不仅仅是自动化信息。信息的形式可以是结构化的或非结构化的，带格式的或不带格式的。

可把信息视为企业“信息周期”的一个阶段，在信息循环（图 35）中，业务流程生成并处理数据，同时把它们转化成信息和知识，最终为企业创造价值。信息促成因素的范围主要涉及信息在信息周期中的阶段，但在 COBIT 5 中也涵盖了数据和知识等方面。

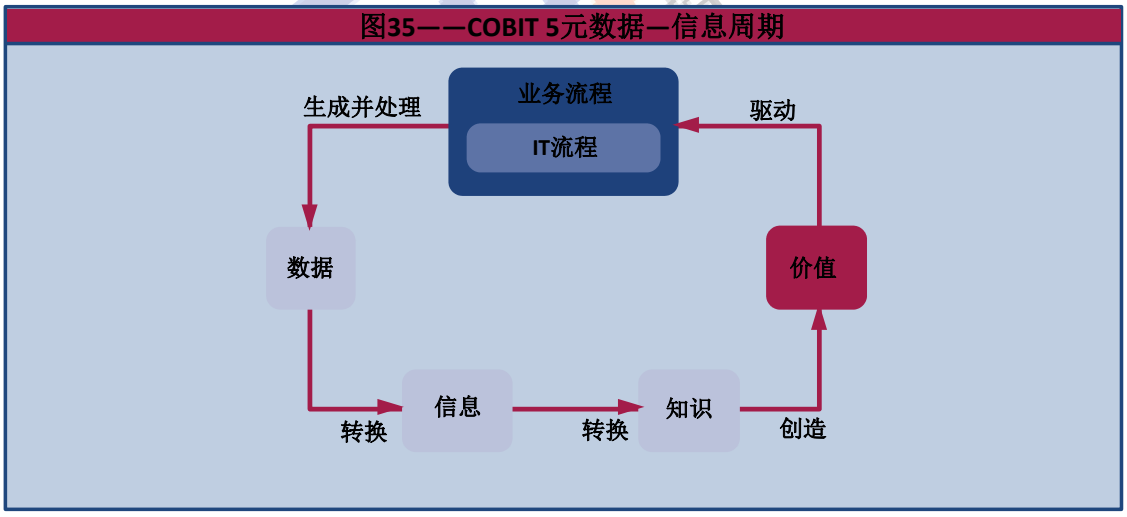

图 16.9 图表 35.COBIT 5 元数据——信息循环

COBIT 5 信息的促成因素

信息促成因素与通用促成因素比较的具体情况如图 36 所示。

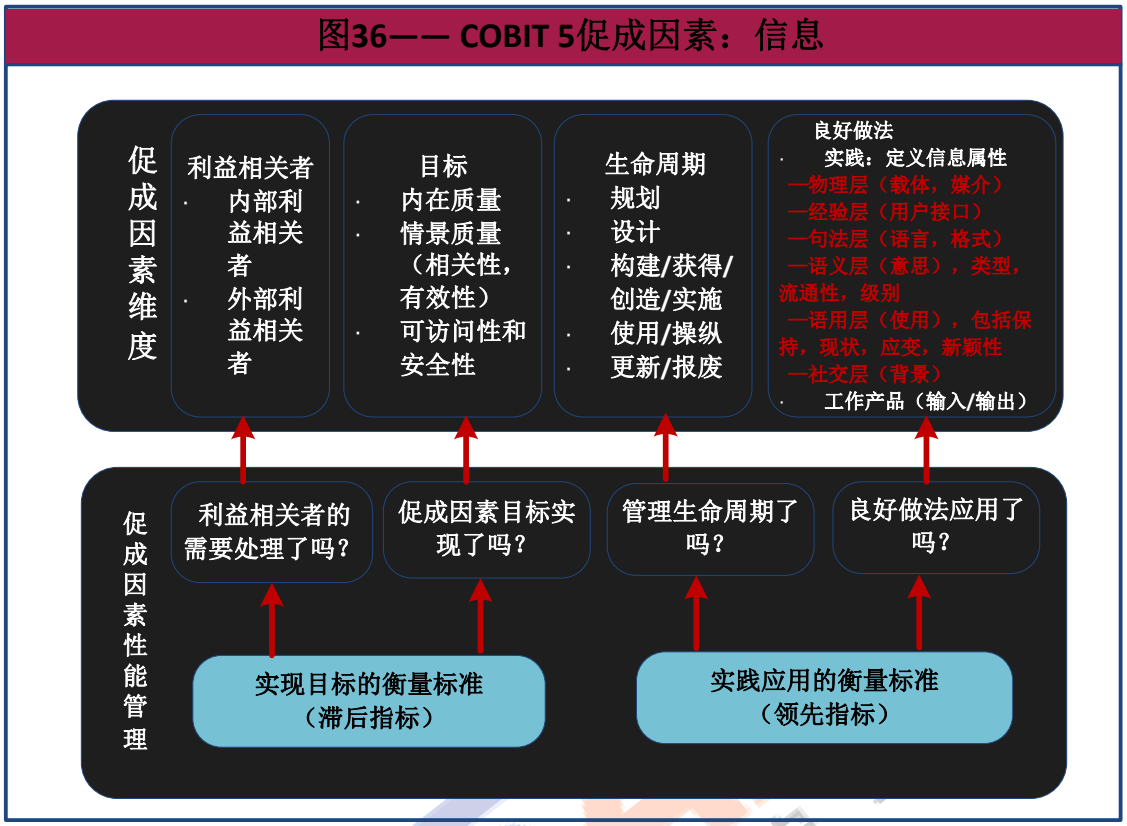

图 16.10　图表 36.COBIT 5 促成因素：信息

信息模型（IM）显示:

- **利益相关者——**可以是企业内部或企业外部的，通用模型也表明，除了确定利益相关者外，他们的利害关系也需要确定，比如，他们为什么关心或对信息感兴趣。

关于存在哪些信息利益相关者，可能有不同的信息处理的角色，从具体的建议，如提出具体的数据或信息角色，诸如架构师，所有者，管事，受托人，供应者，受益人，建模师，质量经理，安全经理，到更一般的建议，例如区分信息生产者，信息保管者，信息消费者：

—信息生产者，负责产生信息

—信息保管者，负责存储和维护信息

—信息消费者，负责使用信息

这些类别是指与信息资源相关的特定活动，这些活动是基于信息所处的生命周期阶段，因此，可以使用 IM 的信息生命周期维度为 IM 找到合适间隔尺寸水平的一类角色。这意味着信息利益相关者角色可根据信息生命周期阶段来定义，比如，信息规划者，信息获取者，信息用户。同时，这也意味着信息利益相关者不是一个独立的维度，不同生命周期阶段有不同的利益相关者。

虽然相关的角色取决于信息生命周期阶段，但利害关系与信息的目标有关。

- **目标—**信息的目标按质量分为三个子维度。

固有质量—数据值与实际值或真值的一致程度，包括

—准确性——信息准确和可靠的程度。

—客观性——信息不偏不倚，不带偏见和公正的程度

—可信性——信息可被当作真实可信的程度

—美誉度——信息在来源或内容方面被高度评价的程度

语境和代表性的质量—信息对信息用户的任务的可用程度以及信息以清晰易于理解的方式呈现的程度，要认识到信息的质量取决于使用的背景，它包括：

—相关度—信息对当前任务的有用或帮助程度；

—完整性—信息对当前任务的完好程度并有足够的深度和广度；

—流通性—信息对当前任务来说足够的新

—适量的信息—信息的数量的当前任务来说是使得的

—准确表达—信息简洁表达的程度

一致的表达—信息以相同的格式表达

—解释性—信息用是适当的语言，符合和单位，并清晰定义的程度

—易懂性—信息容易理解的程度

—易于处理—信息易于处理和用于不同任务的程度

安全性/可获得性质量—信息可提供和获取的程度，包括：

—可得性/及时性—当需要时信息可提供或容易快速获取的程度

—限制访问—对授权方获取信息的适当限制

附录 F 提供了 COBIT 5 信息质量标准与 COBIT 4.1 信息标准对比的详细情况。例如，完整性（如 COBIT 4.1 中定义）包含于信息目标的完整性和准确性中。

- **生命周期**—需要考虑信息的全生命周期，而且在生命周期的不同阶段可能需要不同的获取信息的途径，COBIT 5 信息促成因素区分以下阶段：

—规划—准备创造和使用信息源的阶段，这一阶段的活动可能是指目标的确定，信息架构的规划，标准和定义的制定，比如数据定义，数据采集程序

—设计

—构建/获取—获取信息源的阶段，这一阶段的活动可能是指数据记录的产生，数据的购买和外部文件的下载。

—使用/操作，包括：

- 存储—信息电子化或硬拷贝保存的阶段（或者甚至仅仅是人的记忆），这一阶段的活动可能是指信息以电子形式或硬拷贝存储。
- 共享—信息通过分布式方法变得可用，这一阶段的活动可能是指把信息放在可被获取和使用的位置，比如通过电子邮件发送文件。对于电子化存储的信息，这一生命周期阶段可能很大程度上与存储阶段重叠，比如，通过访问数据库，文件/文件服务器共享信息。
- 使用—信息用于完成目标的阶段，这一阶段的活动可能是指各种信息的使用（比如，制定管理决策，运行自动化程序），也可能包括信息检索，信息格式转换等，

按照推进治理的观点，信息是企业治理的促成因素，因此，信息使用（如 IM 所定义）可被看作企业治理的利益相关者需要信息，同时扮演自己的角色，完成自己的活动并参与互动。

这些角色，活动和关系可从图 8 获得，利益相关者之间的互动需要信息流，其目的是：责任、授权、监控、设置方向、一致、执行和控制。

监控—确保信息源继续正常工作的阶段，例如，仍有价值，这一阶段的活动可能是指保持信息更新以及其他信息管理活动，比如，强化，清洁，合并，删除数据仓库中的重复信息，

丢弃—当信息不再有用时，信息源的舍弃阶段，这一阶段的活动可能是指信息的存档和销毁。

- **最佳实践**—信息的概念在不同的学科（诸如，经济学，通信理论，信息科学，

知识管理和信息系统）中的理解不同。因此，并没有关于信息什么的普遍认同的定义，然而信息的本质却可以通过定义和描述它的属性澄清。

提出下面的计划以构建信息的不同属性：它由定义和描述信息属性的六个级别或层次组成。这六个层面提出了连续的属性，从物理世界的信息，其属性涉及到信息技术和信息获取、存储、处理、分发和展示，到社交世界的信息使用、理解和行动。

可以对层和信息属性作如下描述：

- **物理世界层**—可通过经验观察到所发生的所有现象的世界。

—信息载体/媒介—识别信息的物理载体的属性，例如，纸，电子信号，声波

- **经验层**—

法律，文化。

—语境—识别信息有意义，被使用，具有价值等的语境的属性，比如，文化语境，主题域上下文。

关于信息的进一步考虑—在信息及相关技术领域投资要基于包括成本收益分析的业务案例。成本和收益不仅指有形的、可衡量的因素，而且要将诸如竞争优势，顾客满意度，技术不确定性在内的无形因素考虑在内。只有当信息源被使用，企业才会产生收益，所以，信息的价值只决定于它被使用，而且信息并没有固有的价值。只有将信息付诸行动才会产生价值。

IM 是一种新的模型，就组件而言是十分丰富的。在新的出版物中将会有它新的发展。为使它对 COBIT 用户来说更可观，也为使它在 COBIT 5 的整体框架下的相关性更加明确，提供可能有用的例 13，例 14 和例 15。

例 13 用于信息规范的信息模型

当开发一项新的应用时，IM 可以用来协助应用的规范和相关的信息或数据模型。

IM 的信息属性可用来应用的规范和使用信息的业务流程。

例如，需要指定新系统的设计和规范：

- **物理层**—信息将存储在哪儿？
- **经验层**—如何才能访问信息？
- **句法层**—信息将如何结构化和编码？
- **语义层**—是什么类型的信息？信息级别是什么？
- **语用层**—保留要求是什么？为使这些信息有用和可用还需要什么其他信息？

结合信息生命周期来看利益相关者维度，就可定义谁在信息生命周期的那个阶段需要何种访问权限。

当对应用进行测试时，测试人员可以看信息的质量标准，制定一个全面的测试用例集。

例14 用于确定所需保护的信息模型

企业内部的安全组可受益于 IM 的属性维度，事实上，负责信息保护，他们需要看：

- **物理层**—信息是如何进行物理存储的？存储在哪儿？
- **经验层**—访问信息的渠道是什么？
- **语义层**—信息的类型是什么？信息是当前的还是与过去或将来有关？
- **语用层**—保留要求是什么？信息是历史的还是当前的？

使用这些属性可以使得用户可确定保护级别和需要的保护机制。

看一下 IM 的另一个维度，安全专业人员也可以考虑信息生命周期的阶段，因为在生命周期全过程中信息都需要保护。事实上，安全开始于信息规划阶段，意味着存储、共享和处置信息的不同保护机制。

例 15　用于确定数据易于使用的信息模型

当回顾一项业务流程（或应用）时，IM 可用来协助全面回顾流程所处理和交付的信息以及底层的信息系统。质量标准可用于评估信息可得的程度，即信息是否完整，及时提供，确凿无误，相关和适当数量可用。也可以考虑可访问性标准，即当需要时，信息是否可被访问并被足够地保护。

审评甚至可以扩展到包括表达形式标准，比如，理解，解释，使用和操纵信息的方便程度。

采用 IM 的信息质量标准的审评可为企业通过一个关于一项业务流程范围内的当前信息质量的全面完整的视图。

16.7 COBIT 5 的促成因素：服务，基础设施和应用

服务能力是指在 IT 相关的服务交付过程中所利用的资源，如应用程序和基础设施。

服务能力促成因素与通用促成因素比较的具体情况如图 37 所示。

服务，基础设施和应用的模型显示:

- **利益相关者**—服务能力的利益相关者可以是内部或外部的。可以由内部或外部

各方提供服务—内部 IT 部门，运营经理，外包服务提供商，服务的用户也可以是内部的（企业用户）和企业外部的（合作伙伴，顾客，供应商）。需要确定每个利益相关者的利害关系，或者将重点放在提供足够的服务，或者从供应商接收所要求的服务。

- **目标**—服务水平能力目标将在服务（应用，基础设施，技术）和服务水平方面表示，同时考虑哪种服务和服务水平对企业来说最经济。同样，目标将涉及到的服务，以及它们是如何提供的以及它们的结果，例如，对成功地支持业务流程的贡献。
- **生命周期**—服务能力有生命周期，未来或计划中的服务能力通常是以目标架构描述，它包括构建模块，诸如未来应用和目标基础设施模型，还介绍了这些模块之间的联系和关系。

目前使用或管理的通过当前 IT 服务的服务能力按基准架构描述。根据目标架构的时间框架，也可以定义一个过渡架构，表明在目标和基准架构之间的处于增长状态的企业。

图37—— COBIT 5促成因素：服务，基础设施和应用程序

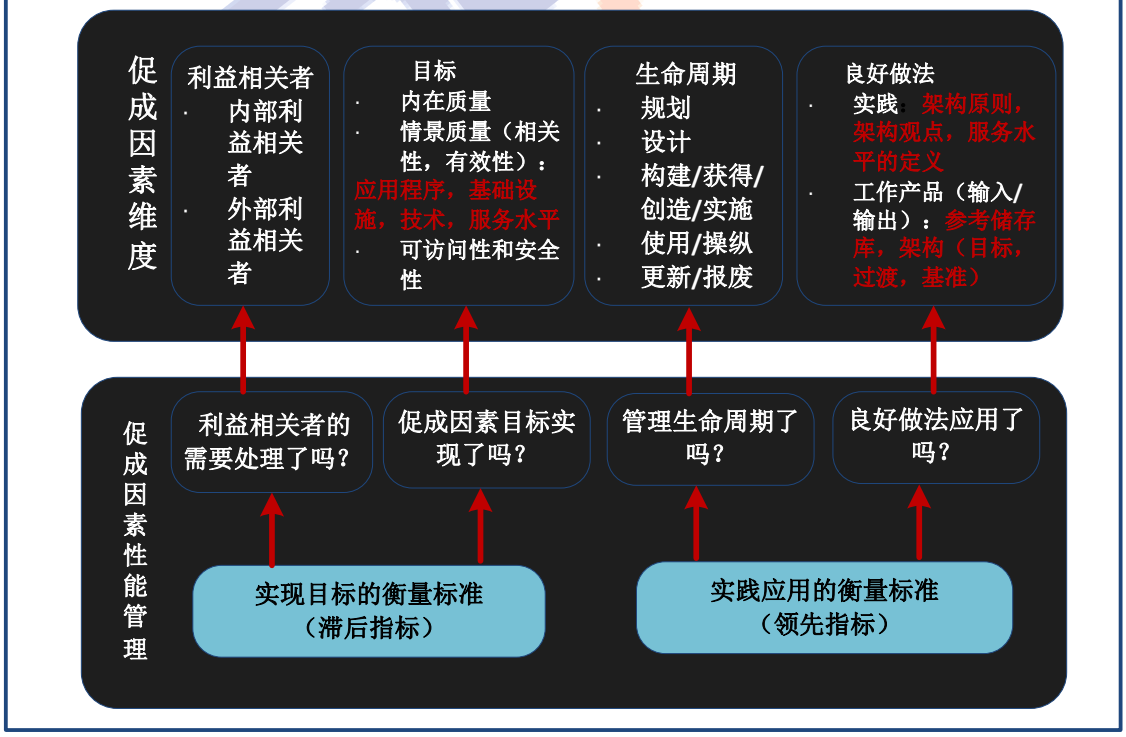

图 16.11　图表 37.COBIT 5 促成因素：服务、基础设施和应用

- **好的做法**——服务能力的良好做法包括：

——架构原则的定义，架构原则是企业内部管理 IT 相关资源实施和使用的总的指导方针，可能的架构原则的例子有：

- **重用**—当设计和实施方案作为目标或过渡架构的一部分时，应使用架构的通用组件。
- **购买和构建**—除非有批准内部构建的利用，应购买解决方案。
- **简洁性**—企业架构在满足企业要求的同时应设计和维护地尽可能简单。
- **灵活性**——企业架构应具有有效和高效地满足不断变化的业务需求的灵活性。
- **开放性**—企业架构应采用开放工业标准。

——企业对以满足不同利益相关者的需求的最合适的架构观点的定义。

这些都是用来描述基准，目标或过渡架构的模式，目录和矩阵，例如，应用程序框架结构可以通过应用程序界面图描述，应用程序界面图中显示其中在使用（或计划）的应用程序和接口描述。

——有一个架构库，它可以用来存储不同类型建筑的产出，包括建筑的原则和标准，架构参考模型，和其他架构的交付以及定义服务的模块，如：

- 应用程序，提供的业务功能；
- 技术基础设施，包括硬件，系统软件和网络基础设施；
- 物理基础设施；

——需要定义服务水平，并由服务提供商实现。

外部也有架构框架和服务能力的良好做法，这些原则，范本或标准可以用来快速跟踪架构成果的创造，示例有：

——TOGAF 提供一种技术参考模型和集成信息基础设施参考模型。

——ITIL 就如何设计和运营服务提供全面的指导。

- **与其他促成因素的关系**——与其他促成因素的关系包括：

——信息是服务功能的一种，服务功能通过提供内部和外部服务的过程放大。

——当需要建立面向服务的文化时，文化和行为方面也是相关的。

——在 COBIT 5 中，管理实践和活动的输入和输出可以包括需要作为输入或输出交付的服务能力。

16.8 COBIT 5 的促成因素：人，技能和竞争力

人，技能和竞争力促成因素与通用促成因素比较的具体情况如**图** 38 所示。

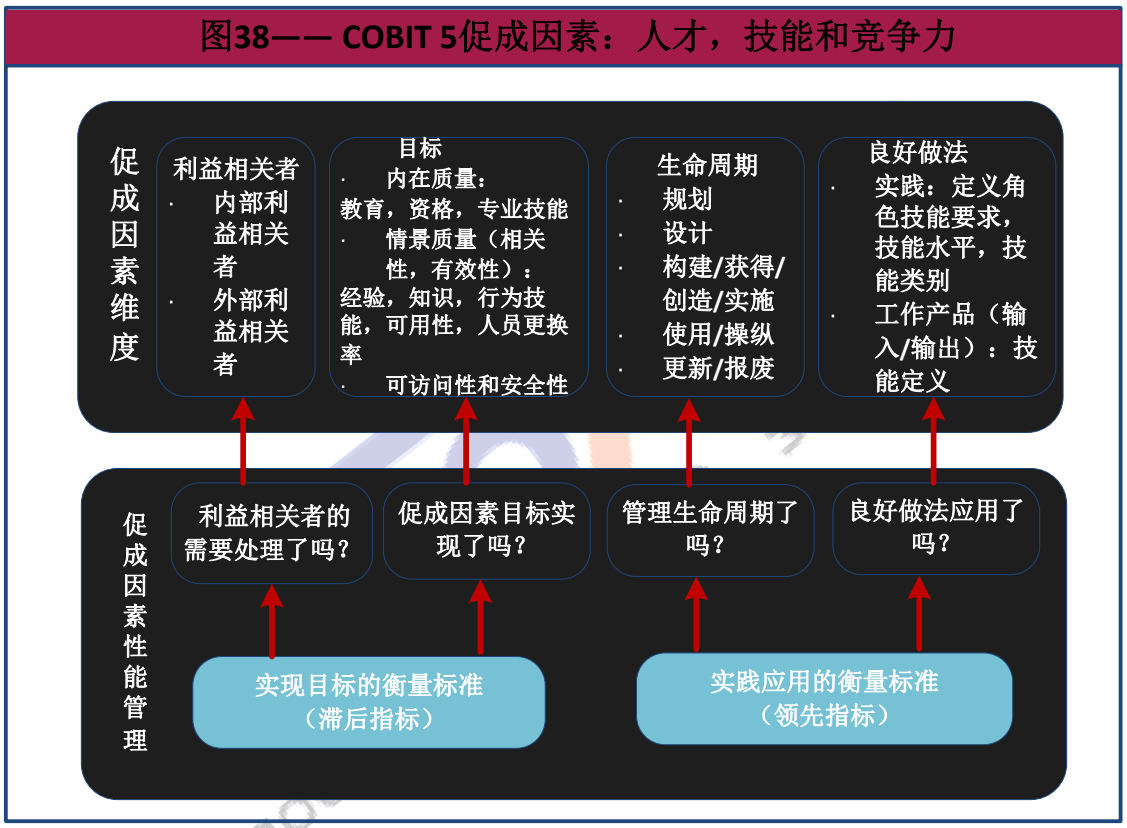

图 16.12　图表 38.COBIT 5 促成因素：人才、技能和竞争力

人才，技能和竞争力模型显示：

- **利益相关者**—技能和能力的利益相关者可以是企业内部和外部的，不同的利益相关者承担不同的角色——业务经理，项目经理，合作伙伴，竞争对手，招聘员，培训者，开发人员，IT 技术专家等，每个角色需要不同的技能集。
- **目标**——技能和能力的目标与教育和学历水平，技术能力，经验水平，需要提供和成功执行过程活动的行为的知识和技能，组织角色等有关，人的目标包括

正确的工作人员的可用性和周转率水平。

- **生命周期：**

——技能和能力有生命周期，企业必须知道其当前的技术基础是什么，并计划它应该是什么，这受企业战略和目标的影响，在组织架构内部的多种角色中需要发展的（如通过培训）、获得的（如通过招聘）调配的技能，技能也可能需要丢弃，如，如果活动是自动的或外包的。

——每隔一段时间，如以每年为基础，企业需要评估技能基础，以便了解所发生的演变，并反馈到今后一个时期的规划过程。

——这种评估也可以反馈到人力资源的奖励和认可过程。

- **好的做法：**

——良好的技能和能力的做法包括确定各利益相关者所扮演的每个角色的目标技能要求的需要，这可以是通过在不同的技能类别不同的技能水平来描述，对每个技能类别的每个适当的技能水平，一种技能的定义应该可用。技能类别与开展的 IT 有关的活动相对应，比如，信息管理，业务分析。

——其他好的做法：

- 有一些源于外部的好的做法，比如，信息时代的技能框架（SFIA），它提供了全面的技能定义。
- 潜在的技能类别示例，映射到 COBIT 5 个过程域，如**图 39** 所示。

图 39——COBIT 5 技能类别

流程领域	**技能类别的范例**
评估，指导和监控（EDM）	● 企业 IT 的治理
调整，规划和组织（APO）	● IT 政策制定 ● IT 战略 ● 企业架构 ● 创新 ● 财务管理 ● 投资组合管理
构建，获得和实施（BAI）	● 业务分析

	● 项目管理 ● 效用评估 ● 需求定义和管理 ● 程序设计 ● 系统人体工程学 ● 软件停用 ● 能力管理
交付，服务和支持（DSS）	● 可用性管理 ● 问题管理 ● 服务台和事件管理 ● 安全管理 ● IT 运营 ● 数据库管理
监控，评价和评估（MEA）	● 合规性审查 ● 性能监控 ● 控制审计

图 16.13 图表 39.COBIT 5 技能类别

- **与其他促成因素的关系**——与其他促成因素的关系包括：

——执行过程中的活动，并在组织结构作决定所需要的技能和能力，相反，一些流程旨在支持生命周期的技能和能力。

——也有通过行为技巧链接到文化，伦理道德和行为，行为技巧推动个人行为并受个人伦理和组织伦理的影响。

——技能的定义也是信息，这需要考虑信息的最佳做法的促成因素。

十七. 附录 H 术语表

术语	定义
负责方	最终对一个主题、过程或范围负责的个人、团体或机构
治理问责制	治理确保通过评估利益相关者的需求，条件和选择，实现企业目标，同时通过优先次序和决策制定，对计划和监视性能，遵守和进展情况来设置方向。在大多数企业中，治理是董事会在主席的领导下的责任
活动	在 COBIT 中，操作过程中采取的主要行动。IT 企业实现成功治理和企业管理的管理实践的指南。活动包括： ● 描述一系列为实现治理或管理实践所必须的足够的面向行动的实施步骤 ● 考虑过程的输入和输出 ● 基于普遍认可的标准和优良做法 ● 建立清晰的角色和责任支持 ● 是非指令性的，能被企业接受并发展成适合企业的特定程序
一致性	IT 企业治理和管理的促成因素支持企业的目标和战略的状态
应用架构	进行处理信息和支持企业的目标必要的管理对象的能力逻辑分组的说明
架构委员会	一组的利益相关者和专家，他们负责指导企业架构的相关事宜和决策，并负责设置架构的政策和标准
认证	验证用户身份的行为和用户访问电脑信息的资格。 请注意使用范围：保证：设计验证以防止欺诈登录活动，它也可以指一堆数据的正确性验证。
基准架构	现有的进入了一个架构审查和重新设计周期之前的基本

	业务系统的组成部分的基本设计的描述
收益实现	治理的目标之一，为企业带来新的效益，现有形式的收益的维护和扩展，并消除没有创造足够的价值的举措和资产
业务连续性	防止，减轻和恢复中断。术语“业务恢复规划”，“灾难恢复规划”和“应急计划”，也可能被用来在这种情况下，他们集中在恢复方面的连续性，因此也应考虑“恢复力”方面
业务目标	把企业的使命从意向声明转换成性能指标和结果
业务流程控制	为业务流程将实现其目标提供合理保证所设计的政策，程序，做法和组织结构，
退款	在公司内部单位的支出的再分配 请注意适用范围：退款是重要的，因为如果没有这样的政策，关于产品或服务的真实盈利能力可能给出误导性的意见，一些重点支出将被忽略或根据任意公式计算。
COBIT	1. COBIT 5：前身为信息及相关技术控制目标(COBIT)，现在只用在其第五次修订后的首字母缩写。一个完整的，国际公认的治理和管理企业信息和技术（IT）的框架，支持在他们的定义和实现业务目标和相关的 IT 目标的企业高层和管理层。COBIT 描述了五个原则和七种促成因素，支持企业对良好的 IT 相关的治理和管理实践的发展，实施和持续改进和监测。 请注意适用范围：COBIT 的早期版本专注于 IT 流程相关的控制目标，IT 流程和 IT 治理的管理和控制方面。COBIT 框架的采纳和使用来自越来越多的配套产品序列的支持。（更多信息请参阅 www.isaca.org/ cobit）。 2. COBIT 4.1 和更早版本：前身为信息及相关技术控制目标(COBIT)，一个完整的，国际公认的 IT 流程框架，

	通过提供全面的 IT 治理，管理，控制和保证模型，支持业务和 IT 管理人员在他们的定义和实现业务目标和相关的 IT 目标。COBIT 描述了 IT 流程和相关的控制目标，管理方针（活动，责任，职责和性能指标）和成熟度模型。COBIT 支持企业管理层对良好的 IT 相关的实践的发展，实施和持续改进和监测。 请注意适用范围：COBIT 框架的采纳和使用由管理层（IT 治理董事会简报，第二版），IT 治理实施者(*COBIT* 快速入门，第二版)和 IT 保证和审计专业人士 (使用 COBIT 的 IT 保证指南）的指导做支持。指导也为一定的立法和监管要求及相关信息安全支持其适用性。COBIT 映射到其他的框架和标准，以说明 IT 管理生命周期的完整覆盖，并支持其在使用多个 IT 相关的框架和标准的企业使用。
职业道德规范	旨在通过确定组织的价值观和在某些情况下所应用的规则影响个人和员工的组织行为的文件。采用来帮助那些企业中被要求作出决定的人理解“准确”和“错误”之间的区别，并将这种理解运用到他们的决策中。
胜任力	成功地执行特定任务，行动或职能的能力
被咨询的一方（RACI）	是指在活动（双向交流）中被征求意见那些人。 在 RACI 表中，回答这个问题：谁提供输入？ 关键角色提供输入。注意也是由负责任的角色从其他单位或外部合作伙伴获得的信息，然而，要考虑来自列出的角色的输入，而且如果需要，采取适当的行动以便升级，包括流程拥有者和/或督导委员会 的信息
背景	可能会影响或确定企业，实体，过程或个人行为的整体的内部和外部因素集

	请注意适用范围：背景包括： ● 技术背景——影响组织从数据中提取价值的能力的技术因素 ● 数据背景——数据的正确性，可用性，现时性和质量 ● 技能和知识——普遍经验，分析，技术和业务技能 ● 组织和文化背景——政治因素，组织更偏好于数据还是直觉 ● 战略背景——企业的战略目标
控制	管理风险的手段，包括政策，程序，原则，惯例或组织结构，它可以是行政，技术，管理或法律的性质，也可用作保障或对策的代名词。
文化	行为，信念，假设，态度和处事方式的模式
驱动力	发起和影响企业或个人如何采取行动或改变的外部和内部因素
企业追求的目标	见企业目标
企业治理	一组以提供战略方向为目标由董事会和高级管理层行使的职责和实践，以确保目标可以实现，确定这种风险可适当的控制并核实企业的资源被负责任地使用。它也意味着一种侧重于企业的整体的治理角度，所有其他人必须调整的治理的最高级别。
全经济生命周期	材料业务收益预计将上升而材料支出（包括投资，运营和退休费用）预计将招致投资项目
良好的做法	已成功地用于多个企业，并已被证明产生可靠的结果的行之有效的活动或过程
治理	用于设置方向，并监督企业的总体目标和明确的目标相一致的合规性和性能的框架，原则和政策，结构，程序和做法，信息，技术，文化，道德，行为。治理定义了问责制，责任和决策（在其他元素中）。

治理/管理实践	对于每个 COBIT 过程，治理和管理实践为企业有效和实用地 IT 治理和管理提供了一套完整的高层次需要。它们是来自治理主体和管理层的行动的证明
治理促成因素	协助实现有效治理的东西（有形的或无形的）
治理框架	框架是一个基本的概念结构，用于解决或应对复杂问题，治理的促成因素，一组定义如何可以接近或理解某事的概念，假设和做法，所涉及的实体之间的关系，参与的角色和边界（治理系统包括和不包括 什么）。
企业 IT 的治理	一种确保信息和相关技术支持企业战略和企业目标的实现的治理观点。它还包括功能的 IT 治理，即确保有效地提供 IT 的能力，。
信息	像其他重要业务资产一样，对企业的业务是必不可少的一种资产。它可以以多种形式存在：打印或写在纸上，以电子形式储存，通过邮寄或电子化传输，在电影中展示，或在谈话中谈及
知情方（RACI）	指那些保持知道最新活动进展情况的人（单向沟通） 在 RACI 表中，回答这个问题：谁在接收信息？被告知任务的成绩和/或交付物的角色。当然，“负责”的角色应始终得到适当的信息以监督任务，他们感兴趣的领域的负责任的角色也是一样。
输入和输出	认为有必要支持过程运行的工作产品/手工艺品。他们使关键决策成为可能，提供流程活动的记录和审计跟踪，使跟进后续事件成为可能。他们在关键的管理实践层面定义，可能包括一些只有在过程中使用的产品，并经常成为其他流程的必要输入。 说明性的 COBIT 5 的输入和输出不应该被视为一个详尽的清单，因为根据特定的企业环境和过程框架可以定义额外的信息流。

投资组合	正在考虑和/或正在进行的投资集合
IT 应用	IT 承担或协助构成部分业务流程的电子功能
IT 目标	描述企业 IT 所期望的结果以支持企业目标的声明。结果可以是人工产物，状态的显著变化或能力的显著提高
IT 服务	每天为客户提供 IT 基础设施和应用，并支持其使用。例子包括服务台，设备供应和运输以及安全授权
管理	即是指明智地利用资源，人，流程，实践等手段，实现确定的目标，是治理机构达到结果或目标的手段或工具。管理对治理机构设置的方向范围内的执行负责。管理与规划，建设，组织和控制业务活动有关，配合治理机构设置的方向，并汇报这些活动
模型	一种描述给定的组件以及这些组件如何相互关联的方式，以描述对象，系统或概念的主要工作原理
度量	使测量流程目标的实现情况成为可能的可以量化的实体。度量框架应该是智能的，具体的，可测量的，可操作的，相关和及时的。完备度量指南定义所使用的单位，测量频率，理想的目标值（如适用的话），也定义了进行测量的程序和解释评估的程序。
目标	期望结果的说明
组织结构	治理和管理的促成因素。包括企业及其结构，层次结构和依赖关系。 例如：指导委员会
输出	见输入和输出
拥有者	持有或拥有企业，实体或资产的权利和责任的个人或团体，例如，流程所有者，系统所有者
政策	由管理层正式表述的总体意图和方向
原则	治理和管理的促成因素。包括企业持有的价值观和基本假设，指导和限制企业的决策，企业内部和外部的沟通，

	管理工作—照顾另一个拥有的资产—的信念 例如：伦理宪章，社会责任宪章
流程	一般来说，一个企业的政策和程序，需要从多个来源（包括其他流程）获得输入，管理输入和产生输出（例如，产品，服务），流程就是受其影响的实践的集合 请注意适用范围：流程的存在有明确的业务原因，负责任的业主，流程执行中明确的角色和责任和衡量绩效的手段
流程（能力）属性	ISO/IEC 15504：应用于任何流程的流程能力的可衡量的特征
流程能力	ISO/IEC 15504：满足目前或预计的业务目标的流程能力的特征
流程目标	描述流程所期望的结果。结果可以是人工产物，状态的显著变化或其他流程能力的显著提高
方案和项目管理办公室（PMO）	负责支持方案和项目经理，并收集，评估和报告其方案和组成项目处理的信息的功能
质量	与其目的相符（达到预期值）
RACI 表	说明在组织框架内谁有责任，有义务，被咨询和通知
资源	任何可以帮助组织实现其目标企业的资产
资源最优化	治理的目标之一。涉及到有效，高效和负责任的使用所有资源——人力，财力，设备，设施等
负责方（RACI）	指必须确保活动顺利完成的人 在 RACI 图表中，回答这个问题：到底是谁完成的任务？执行列出的活动并实现预期成果，持主要业务股份的角色
风险	一件事及其结果可能的组合（ISO/IEC 73）
风险管理	治理的目标之一。包括识别风险，评估风险的影响和可能性，制订策略，如避免风险，减少风险的负面影响和/

	或转移风险，以将其控制在企业的风险承受能力范围内
服务目录	为客户提供的所有 IT 服务的结构化信息
服务	见 IT 服务
技能	为实现预定的结果学到的能力
利益相关者	任何在企业中有责任，有期望或有其他一些利益的人，如利益相关者，用户，政府，供应商，客户和公众
内部控制系统	所设计的为实现企业目标和阻止、检测或纠正意外的事件而提供合理保证的政策，标准，计划和程序以及组织结构
价值创造	一个企业的主要治理目标，当实现三个基本目标（利益的实现，风险优化和资源优化）都平衡时得以实现