COBIT® 2019

框架

简介和方法

ISACA®

ISACA 简介

ISACA® (isaca.org) 是一家全球性协会，已成立近 50 年，致力于帮助个人和企业挖掘技术潜力，获得积极成果。现如今，科技推动世界发展，ISACA 为专业人士提供知识、认证、指导并打造社群网络，推动他们的职业发展及其所在组织的转型。ISACA 拥有五十万名从事信息与网络安全、治理、鉴证、风险与创新工作的专业人员，以及一家帮助企业提升绩效的子公司 CMMI® Institute，他们共同致力于推动技术创新。ISACA 成员遍布超过 188 个国家和地区，在美国和中国设有超过 217 个分会和办事处。

免责声明

版权

ISACA

1700 E. Golf Road, Suite 400
Schaumburg, IL 60173, USA
电话：+1.847.660.5505
传真：+1.847.253.1755
联系我们：https://support.isaca.org
网站：www.isaca.org

参加 ISACA 知识中心： https://engage.isaca.org/onlineforums

Twitter: http://twitter.com/ISACANews
LinkedIn: http://linkd.in/ISACAOfficial
Facebook: www.facebook.com/ISACAHQ
Instagram: www.instagram.com/isacanews/

COBIT® 2019 框架：简介和方法
ISBN 978-1-60420-779-8

谨此纪念：John Lainhart（1946-2018 年）

谨以此书献给 ISACA 董事会主席（任期 1984-1985 年）John Lainhart。John 帮助创建了 COBIT® 框架。他最近担任的职位是 COBIT® 2019 工作组主席，并以本作品的问世画上了圆满的句号。在 ISACA 工作的四十年间，John 参与了协会多方面的工作，并获得 ISACA 的 CISA、CRISC、CISM 和 CGEIT 认证。John 为我们留下了宝贵的专业遗产，他的工作成果给 ISACA 带来了深刻的影响。

本页特意留白

致谢

ISACA 向以下人员表示感谢：

COBIT 工作组（2017-2018 年）

John Lainhart，主席，CISA，CRISC，CISM，CGEIT，CIPP/G，CIPP/US，Grant Thornton，美国
Matt Conboy，Cigna，美国
Ron Saull，CGEIT，CSP，Great-West Lifeco & IGM Financial（退休），加拿大

开发团队

Steven De Haes 博士，安特卫普大学管理学院，比利时
Matthias Goorden，PwC，比利时
Stefanie Grijp，PwC，比利时
Bart Peeters，PwC，比利时
Geert Poels 博士，根特大学，比利时
Dirk Steuperaert，CISA，CRISC，CGEIT，IT In Balance，比利时

校审专家

Sarah Ahmad Abedin，CISA，CRISC，CGEIT，Grant Thornton LLP，美国
Floris Ampe，CISA，CRISC，CGEIT，CIA，ISO27000，PRINCE2，TOGAF，PwC，比利时
Elisabeth Antonssen，Nordea Bank，瑞典
Krzystof Baczkiewicz，CHAMP，CITAM，CSAM，Transpectit，波兰
Christopher M. Ballister，CRISC，CISM，CGEIT，Grant Thornton，美国
Gary Bannister，CGEIT，CGMA，FCMA，奥地利
Graciela Braga，CGEIT，审计师和顾问，阿根廷
Ricardo Bria，CISA，CRISC，CGEIT，COTO CICSA，阿根廷
Sushil Chatterji，CGEIT，Edutech Enterprises，新加坡
Peter T. Davis，CISA，CISM，CGEIT，COBIT 5 评估员，CISSP，CMA，CPA，PMI-RMP，PMP，Peter Davis+Associates，加拿大
James Doss，CISM，CGEIT，EMCCA，PMP，SSGB，TOGAF 9，ITvalueQuickStart.com，美国
Yalcin Gerek，CISA，CRISC，CGEIT，ITIL 专家，Prince2，ISO 20000LI，ISO27001LA，TAC AS.，土耳其
James L. Golden，Golden Consulting Associates，美国
J. Winston Hayden，CISA，CISM，CRISC，CGEIT，南非
Jimmy Heschl，CISA，CISM，CGEIT，Red Bull，奥地利
Jorge Hidalgo，CISA，CISM，CGEIT，智利
John Jasinski，CISA，CRISC，CISM，GEIT，COBIT 5 评估员，CSM，CSPO，IT4IT-F，ITIL 专家，Lean IT-F，MOF，SSBB，TOGAF-F，美国
Joanna Karczewska，CISA，波兰
Glenn Keaveny，CEH，CISSP，Grant Thornton，美国
Eddy Khoo S. K.，CGEIT，Kuala Lumpur，马来西亚
Joao Souza Neto，CRISC，CGEIT，Universidade Católica de Brasília，巴西
Tracey O'Brien，CISA，CISM，CGEIT，IBM Corp（退休），美国
Zachy Olorunojowon，CISA，CGEIT，PMP，卑诗省卫生部，维多利亚，加拿大卑诗省
Opeyemi Onifade，CISA，CISM，CGEIT，BRMP，CISSP，ISO 27001LA，M.IoD，Afenoid Enterprise Limited，尼日利亚

致谢（续）

校审专家（续）

Andre Pitkowski，CRISC，CGEIT，CRMA-IIA，OCTAVE，SM，APIT Consultoria de Informatica Ltd.，巴西
Abdul Rafeq，CISA，CGEIT，FCA，Wincer Infotech Limited 常务董事，印度
Dirk Reimers，Entco Deutschland GmbH，A Micro Focus Company
Steve Reznik，CISA，CRISC，ADP, LLC.，美国
Bruno Horta Soares，CISA，CRISC，CGEIT，PMP，GOVaaS (Governance Advisors, as-a-Service)，葡萄牙
Dr. Katalin Szenes 博士，CISA，CISM，CGEIT，CISSP，John von Neumann Faculty of Informatics，欧布达大学，匈牙利
Peter Tessin，CISA，CRISC，CISM，CGEIT，Discover，美国
Mark Thomas，CRISC，CGEIT，Escoute，美国
John Thorp，CMC，ISP，ITCP，The Thorp Network，加拿大
Greet Volders，CGEIT，COBIT 评估员，Voquals N.V.，比利时
Markus Walter，CISA，CISM，CISSP，ITIL，PMP，TOGAF，PwC，新加坡/瑞士
David M. Williams，CISA，CAMS，Westpac，新西兰
Greg Witte，CISM，G2 Inc.，美国

ISACA 董事会

Rob Clyde，CISM，Clyde Consulting LLC，美国，主席
Brennan Baybeck，CISA，CRISC，CISM，CISSP，Oracle Corporation，美国，副主席
Tracey Dedrick，Hudson City Bancorp 前首席风险官，美国
Leonard Ong，CISA，CRIS，CISM，CGEIT，COBIT 5 实施和评估员，CFE，CIPM，CIPT，CISSP，CITBCM，CPP，CSSLP，GCFA，GCIA，GCIH，GSNA，ISSMP-ISSAP，PMP，Merck & Co., Inc.，新加坡
R.V. Raghu，CISA，CRISC，Versatilist Consulting India Pvt. Ltd.，印度
Gabriela Reynaga，CISA，CRISC，COBIT 5 Foundation，GRCP，Holistics GRC，墨西哥
Gregory Touhill，CISM，CISSP，Cyxtera Federal Group，美国
Ted Wolff，CISA，Vanguard, Inc.，美国
Tichaona Zororo，CISA，CRISC，CISM，CGEIT，COBIT 5 评估员，CIA，CRMA，EGIT | Enterprise Governance of IT，南非
Theresa Grafenstine，CISA，CRISC，CGEIT，CGAP，CGMA，CIA，CISSP，CPA，Deloitte & Touche LLP，美国，2017-2018 年 ISACA 董事会主席
Chris K. Dimitriadis，博士，CISA，CRISC，CISM，INTRALOT，希腊，2015-2017 年 ISACA 董事会主席
Matt Loeb，CGEIT，CAE，FASAE，首席执行官，ISACA，美国
Robert E Stroud（1965-2018 年），CRISC，CGEIT，XebiaLabs, Inc.，美国，2014-2015 年 ISACA 董事会主席
Robert E Stroud 于 2018 年 9 月逝世，ISACA 谨此致以沉痛哀悼。

目录

图表列表

本页特意留白

第一章
引言

1.1 企业信息和技术治理

从数字化转型来看，信息和技术 (I&T) 对企业的支持、可持续发展和成长起着至关重要的作用。在此之前，治理委员会（董事会）和高级管理层可能一直委派、忽视或规避 I&T 相关决策。如今，在大多数行业和领域中，这种做法显得极不明智。利益相关方的价值创造（即在优化风险的同时以最佳资源成本实现效益）通常是由新业务模式的高度数字化、高效的流程和成功的创新等要素推动的。数字化企业的生存和发展越来越依赖于 I&T。

鉴于 I&T 在企业风险管理和价值创造中所起的核心作用，过去三十年来，企业信息和技术治理 (EGIT) 日益受到广泛的关注。EGIT 是企业治理不可或缺的一部分。它由董事会执行，董事会将负责监督组织中的流程、结构和关系机制的定义和实施，促使业务和 IT 人员各尽其责，支持业务/IT 的协调一致，以及从 I&T 促成的业务投资中创造业务价值（**图 1.1**）。

图 1.1—企业信息和技术治理的背景

Source: De Haes, Steven; W. Van Grembergen; *Enterprise Governance of Information Technology: Achieving Alignment and Value, Featuring COBIT 5*, Springer International Publishing, 瑞士, 第二版, 2015 年, *https://www.springer.com/us/book/9783319145464*

企业信息和技术治理非常复杂，涉及多个方面。在组织内设计、实施和维护有效的 EGIT 是没有灵丹妙药（或万能公式）可言的。因此，治理委员会和高级管理层通常需要因地制宜，根据具体情况和需求来定制 EGIT 措施和实施。他们还必须愿意承担更多的 I&T 责任，培育不同的思维方式和文化来实现 I&T 的价值。

1.2 信息和技术治理的优点

从根本上说，EGIT 关注的是数字化转型带来的价值以及随之而来的业务风险的缓解。更具体地说，成功采用 EGIT 预期可取得三项主要成果：

- **效益实现** — 包括通过 I&T 为企业创造价值，保持和增加从现有 I&T[1] 投资产生的价值，消除不能为企业创造足够价值的 IT 举措和资产。I&T 价值的基本原则是在预算范围内按时提供配套的服务和解决方案，从而产生预期的财务和非财务效益。I&T 创造的价值应与业务关注的价值恰好保持一致。IT 价值的衡量方式还应体现 IT 促成的投资对企业价值创造流程的影响和促进作用。

[1] 在本文中，IT 指的是主要负责技术的组织部门。I&T 则指企业生成、处理并用于实现目标的所有信息，以及在整个企业中支持这些行动的技术。

- **风险优化** — 包括应对与在企业中使用、拥有、运行、参与、影响和采用 I&T 相关的业务风险。I&T 相关的业务风险包括可能对业务产生影响的 I&T 相关事件。价值实现侧重于*创造*价值，风险管理侧重于*保护*价值。应将 I&T 相关风险的管理整合到企业风险管理方法中，以确保企业对 IT 的关注。此外，I&T 的衡量方式还应体现优化 I&T 相关的业务风险对价值保留的影响和贡献。
- **资源优化** — 确保有适当的能力来执行战略计划并提供充足、适当、有效的资源。资源优化可确保企业提供经济高效的综合 IT 基础设施，根据业务需求引入新技术，以及更新或替换过时的系统。除了硬件和软件之外，它还重视人员的重要性，因此，它很注重提供培训、提高保留率以及确保关键 IT 人员的能力。数据和信息是一项重要的资源，利用数据和信息来获取最佳价值是资源优化的另一个关键要素。

战略一致性和绩效衡量至关重要，应全面应用于所有活动，以确保 I&T 相关的目标与企业目标保持一致。

一家国际航空公司的一宗大型案例研究充分展现了 EGIT 的优势，包括：降低 IT 相关的连续性成本；提高 IT 支持的创新能力；增强数字投资与业务目标和战略之间的一致性；加深业务与 IT 之间的信任；以及朝着数字资产的“价值取向”的转变。[2]

研究表明，企业设计或采用 EGIT 的方法如果不得当，在推动业务与 I&T 战略及流程的一致性方面往往就会表现得不如人意。因此，这类企业达成预期的业务战略和通过数字化转型取得预期的业务价值便没有多少胜算。[3]

由此可见，要深入理解和实施治理，就不能满足于治理、风险与合规性 (GRC) 缩略词的常见（即狭义）解读。GRC 缩略词本身已经暗示，治理范畴内也存在合规性和相关的风险。

1.3 使用 COBIT 作为 I&T 治理框架

近年来，业界开发和推广了多种最佳实践框架，来协助完成 EGIT 的理解、设计和实施过程。COBIT® 2019 集该领域内超过 25 年的开发成果之大成，不仅融入了新的科学见解，还将这些见解付诸于实践。

COBIT® 立足 IT 审计领域，如今已发展为一种更广泛、更全面的 I&T 治理和管理框架，进而确立了其面向 IT 治理的行业公认框架的地位。

[2] De Haes, S.；W. van Grembergen；*Enterprise Governance of IT: Achieving Alignment and Value，Featuring COBIT 5*，Springer International Publishing，瑞士，第二版，2015 年，*https://www.springer.com/us/book/9783319145464*

[3] De Haes, Steven；A. Joshi; W. van Grembergen；“State and Impact of Governance of Enterprise IT in Organizations: Key Findings of an International Study”，*ISACA® 杂志*，第 4 卷，2015 年，*https://www.isaca.org/Journal/archives/2015/Volume-4/Pages/state-and-impact-of-governance-of-enterprise-it-in-organizations.aspx*。另请参阅 De Haes 和 van Grembergen 的*前述著作*。

1.3.1 COBIT 是什么？不是什么？

在介绍更新的 COBIT 框架之前，有必要解释一下 COBIT 是什么和不是什么：

COBIT 是面向整个企业的企业信息和技术治理及管理框架[4]。企业 I&T 是指企业为实现其目标而在任何领域实施的所有技术和信息处理。换句话说，企业 I&T 包括但不仅限于组织的 IT 部门。

COBIT 框架对治理和管理进行了明确区分。这两个学科涵盖不同的活动，需要不同的组织结构，并服务于不同目的。

- **治理**确保：
  - 对利益相关方的需求、条件和选择方案进行评估，以确定全面均衡、达成共识的企业目标。
  - 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。

在大多数企业中，全面治理是董事长领导下的董事会的职责。具体的治理职责可以赋予合适级别的专门组织结构，特别是在大型的复杂企业中。

- **管理层**按治理机构设定的方向计划、构建、运行和监控活动，以实现企业目标。

在大多数企业中，管理是首席执行官 (CEO) 领导下的高级管理层的职责。

COBIT 定义了构建和维持治理系统的组件：流程、组织结构、政策和程序、信息流、文化和行为、技能以及基础设施。[5]

COBIT 阐明了企业应考虑的设计因素，以建立最合适的治理系统。

COBIT 在解决治理问题时采用的方法是，将相关的治理组件归类为可在所需的能力级别进行管理的治理和管理目标。

关于 COBIT 有一些误解需要澄清：

- COBIT 不是整个企业 IT 环境的完整说明。
- COBIT 不是用于组织业务流程的框架。
- COBIT 不是用于管理所有技术的 IT 技术框架。
- COBIT 不做出或规定任何 IT 相关的决策。它的目的不是确定最佳 IT 战略是什么、最佳架构是什么以及可能或应该投入多少 IT 成本，而是定义旨在描述应做出何种决策以及如何和由谁做出决策的所有组件。

[4] 在本出版物中，我们称其为“IT 治理框架”，实际隐含了这一完整描述。
[5] 在 COBIT® 5 中，这些组件被称为“动力”。

1.4 本出版物的结构

本书其余部分包含以下章节：

- 第 2 章讨论 COBIT 的目标受众。
- 第 3 章阐述 I&T 治理系统的原则，以及良好治理框架的原则。
- 第 4 章介绍 COBIT® 2019 的基本概念和术语，包括更新的核心 COBIT 模型及其 40 个治理和管理目标。
- 第 5 章详细说明 40 个治理和管理目标。
- 第 6 章介绍如何策划 COBIT® 2019 中的性能监控，尤其是如何引入受能力成熟度模型集成 (CMMI®) 启发的能力级别。
- 第 7 章包含《*COBIT® 2019 设计指南*》的工作流程简介和概述。
- 第 8 章包含《*COBIT® 2019 实施指南*》的简介和概述。
- 第 9 章包含一个详细示例，描述了如何在企业中采用和实施 COBIT。
- 第 10 章列出 COBIT® 2019 开发过程中使用的标准、框架和法规。

第二章
目标受众

2.1 治理利益相关方

COBIT 的目标受众是 EGIT 的利益相关方乃至企业治理的利益相关方。**图 2.1** 展示了这些利益相关方以及 COBIT 可能给他们带来的好处。

图 2.1—COBIT 利益相关方

利益相关方	COBIT 的好处
内部利益相关方	
董事会	提供有关如何使用 I&T 创造价值的见解，并说明相关的董事会职责
执行管理层	提供有关如何组织和监控整个企业中的 I&T 绩效的指导
业务经理	帮助了解如何获得企业所需的 I&T 解决方案以及如何充分利用新技术来获取新的战略机会
IT 经理	提供以下方面的指导意见：如何以最佳方式构建和组织 IT 部门、管理 IT 绩效、高效和有效地开展 IT 运营、控制 IT 成本，以及使 IT 战略与业务优先级保持一致等
鉴证提供商	帮助管理对外部服务提供商的依赖性、获得 IT 保证，并确保具备有效且高效的内部控制系统
风险管理	帮助确保识别和管理所有 IT 相关的风险
外部利益相关方	
监管机构	帮助确保企业遵守适用的规则和法规，并实施了适当的治理系统来管理和维持合规性
业务伙伴	帮助确保业务伙伴的运营安全、可靠且遵守适用的规则和法规
IT 供应商	帮助确保 IT 供应商的运营安全、可靠且遵守适用的规则和法规

要从 COBIT 框架中获益，需要一定的经验水平并对企业有深入的了解。只有具备这种经验和了解，用户才能根据企业环境，对通用性质的核心 COBIT 指南进行裁剪，将其转变为有针对性的企业指南。

目标受众包括从治理解决方案的设计、执行到鉴证的整个生命周期里的责任人员。实际上，鉴证提供商可以运用本出版物中制定的逻辑和工作流程来为企业创建有据可依的鉴证计划。

本页特意留白

第三章
COBIT 原则

3.1 引言

COBIT® 2019 的开发基于两套原则：

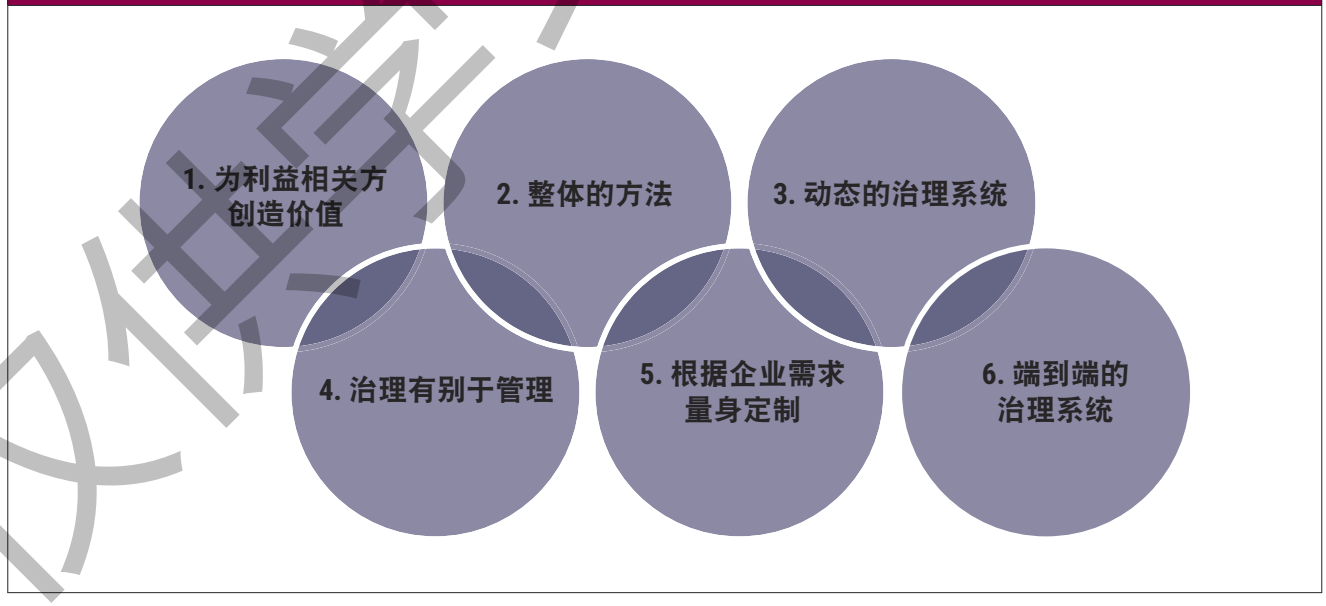
- 描述企业信息和技术**治理系统**核心要求的原则
- 可用于构建企业治理系统的**治理框架**的原则

3.2 治理系统的六大原则

治理系统的六大原则是（**图 3.1**）：

1. 每个企业都需要治理系统，以满足利益相关方的需求，并通过使用 I&T 来创造价值。价值反映了效益、风险与资源之间的平衡，企业需要可行的战略和治理系统来实现这一价值。
2. 企业 I&T 治理系统包括若干组件，这些组件可能是不同类型的，但能以整体协同的方式运作。
3. 治理系统应该是动态的。这意味着每次更改一个或多个设计因素（如战略或技术变更）时，必须考虑这些变化对 EGIT 系统的影响。EGIT 动态视图有助于构建可行的、面向未来的 EGIT 系统。
4. 治理系统应明确区分治理与管理的各自相关活动和结构。
5. 应根据企业需求量身定制治理系统，使用一系列设计因素作为参数来定制治理系统的组件并确定优先级。
6. 治理系统应全面覆盖整个企业，不仅关注 IT 职能，还关注企业为实现其目标而在任何领域实施的所有技术和信息处理。[6]

图 3.1—治理系统原则



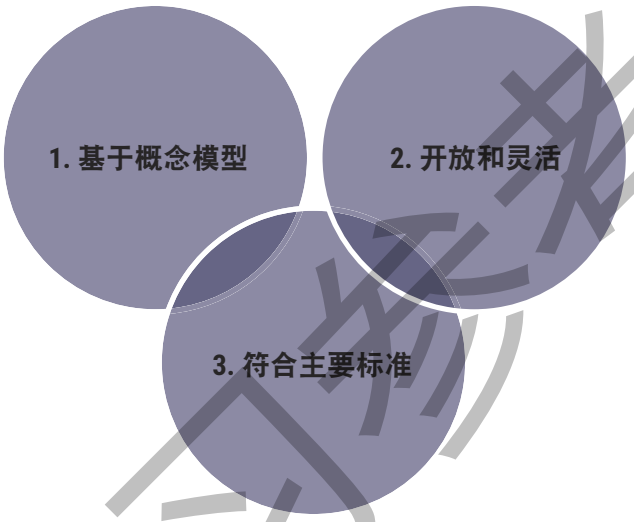
[6] Huygh, T.；S. De Haes；“Using the Viable System Model to Study IT Governance Dynamics: Evidence from a Single Case Study”，*第 51届夏威夷国际系统科学大会会议录*，2018 年，*https://scholarspace.manoa.hawaii.edu/bitstream/10125/50501/1/paper0614.pdf*

3.3 治理框架的三大原则

治理框架的三大原则是（**图 3.2**）：

1. 治理框架应基于概念模型，确定关键组件及这些组件之间的关系，从而最大限度保持一致性并实现自动化。
2. 治理框架应该是开放和灵活的。它允许添加新内容并能以最灵活的方式解决新问题，同时保持完整性和一致性。
3. 治理框架应遵守相关的主要标准、框架和法规。

图 3.2—治理框架原则



3.4 COBIT® 2019

COBIT® 2019 基于先前版本的 COBIT 进行了以下方面的改进：

- **灵活性和开放性** — 设计因素的定义和使用允许定制 COBIT，使其更符合用户特定的环境。COBIT 采用开放式架构，可以添加新的焦点领域（请参阅第 4.4 节）或修改现有的焦点领域，而不会直接影响 COBIT 核心模型的结构和内容。
- **现势性和相关性** — COBIT 模型支持引述和采用其他来源（如最新的 IT 标准和合规性法规）的概念。
- **规范性应用** — COBIT 等模型可以兼具描述性和规范性。COBIT 概念模型的结构和呈现令其实例化（即定制 COBIT 治理组件的应用）被视为定制 IT 治理系统的规范。
- **IT 绩效管理** — COBIT 绩效管理模型的结构已整合到概念模型中。为了更好地与 CMMI 保持一致，引入了成熟度和能力概念。

在 COBIT 指南中，术语“企业信息和技术治理”与“IT 治理”可以互换使用。

第四章
基本概念：治理系统及组件

4.1 COBIT 概述

COBIT® 2019 产品系列是采用可定制设计的开放式框架。目前提供以下出版物：[7]

- ***《COBIT® 2019 框架：简介和方法》***介绍了 COBIT® 2019 的关键概念。
- ***《COBIT® 2019 框架：治理和管理目标》***全面介绍了 40 个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。本指南还参考了其他标准和框架。
- ***《COBIT® 2019 设计指南：信息和技术治理解决方案的设计》***探讨了可能影响治理的设计因素，并包含了规划定制的企业治理系统的工作流程。
- ***《COBIT® 2019 实施指南：信息和技术治理解决方案的实施和优化》***是*《COBIT® 5 实施指南》*的演进版，并制定了一份持续治理改进的路线图。它可以和*《COBIT® 2019 设计指南》结合使用。*

图 4.1 高度概括了 COBIT® 2019，说明了该系列不同出版物所涵盖的不同方面。

图 4.1—COBIT 概述

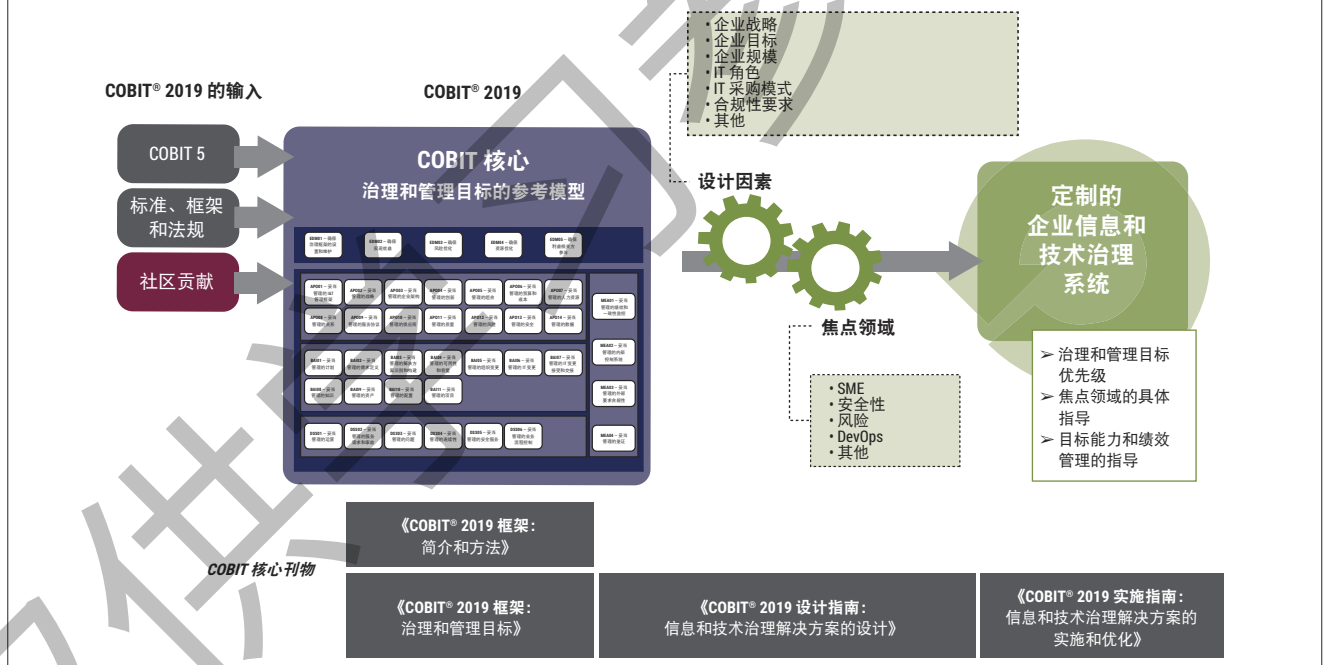


图 4.1 中标识为焦点领域的内容将包含有关特定主题的更详细的指导。[8]

[7] 本*《COBIT® 2019 框架：简介和方法》*发布时，COBIT® 2019 产品系列的其他书刊也已计划好，但尚未发布。

[8] 目前正在准备其中多个焦点领域的内容指南，其余焦点领域也已纳入计划。这些焦点领域的指南是开放式的，将会不断完善。有关目前已提供和规划中的出版物的最新信息和其他内容，请访问 *www.isaca.org/cobit*。

COBIT® 2019 基于 COBIT® 5 和其他权威资料来源。COBIT 遵循一系列相关标准和框架。第 10 章列出了这些标准。对相关标准以及 COBIT 与这些标准的一致性进行的分析，奠定了 COBIT 作为 I&T 治理框架“标志品牌”的地位。

未来，COBIT 将呼吁用户社区提供内容更新建议并持续采纳和管理这些建议，使 COBIT 与最新的行业见解和发展保持同步。

以下章节介绍 COBIT® 2019 中的关键概念和术语。

4.2 治理和管理目标

要让信息和技术促进企业目标的实现，应达成一系列的治理和管理目标。有关治理和管理目标的基本概念包括：

- 治理或管理目标**总会涉及一个流程**（具有相同或相似的名称）和一系列其他类型的相关组件，以帮助实现目标。
- 治理目标与治理流程（如**图 4.2** 中深蓝色背景所示）有关，而管理目标与管理流程（如**图 4.2** 中浅蓝色背景所示）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。

COBIT 中的治理和管理目标分为五个领域。这些领域的名称包含动词，传达了主要目的及目标涵盖的活动领域：

- 治理目标被列入**评估、指导和监控** (EDM) 领域。在这个领域，治理机构将评估战略方案、指导高级管理层执行所选的战略方案并监督战略的实施。
- 管理目标分为四个领域：
  - **调整、计划和组织** (APO) 针对 I&T 的整体组织、战略和支持活动。
  - **构建、购置和实施** (BAI) 针对 I&T 解决方案的定义、购置和实施以及它们到业务流程的整合。
  - **交付、服务和支持** (DSS) 针对 I&T 服务的运营交付和支持，包括安全。
  - **监控、评价和评估** (MEA) 针对 I&T 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。

图 4.2—COBIT 核心模型

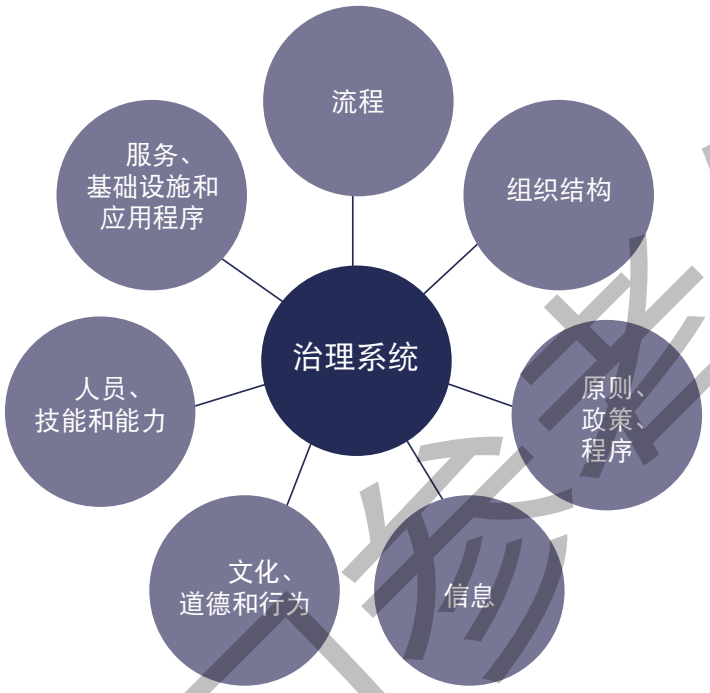
4.3 治理系统的组件

为满足治理和管理目标，每个企业都需要建立、定制和维护由多个组件构成的治理系统。

- 组件是单独或共同促进企业的 I&T 治理系统良好运营的因素。
- 这些组件彼此交互，形成了一个整体性的 I&T 治理系统。
- 组件可以是不同类型的。最熟悉的组件是流程。但是，治理系统的组件也包括组织结构、政策和程序、信息项、文化和行为、技能和能力以及服务、基础设施和应用程序（**图 4.3**）。
  - **流程**描述了一组为实现某种目标而安排有序的实务和活动，并生成了一组支持实现整体 IT 相关目标的输出内容。
  - **组织结构**是企业的主要决策实体。
  - **原则、政策和框架**将理想行为转化为实用的日常管理指导。
  - **信息**在任何组织中，信息无处不在，包括企业生成和使用的全部信息。COBIT 侧重于有效运转企业治理系统所需的信息。
  - **文化、道德和行为**（个人层面与企业层面）作为治理和管理活动的成功因素之一，其价值往往被低估。

- **人员、技能和能力**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。
- **服务、基础设施和应用程序**包括为企业提供 I&T 处理治理系统的基础设施、技术和应用程序。

图 4.3—COBIT 治理系统的组件



所有类型的组件都可能是通用的，也可能是通用组件的变体：

- COBIT 核心模型（请参阅**图 4.2**）描述了**通用**组件，原则上可以应用于任何情况。但是，它们本质上虽是通用的，在实际实施之前却通常需要定制。
- **变体**基于通用组件，但针对特定目的或焦点领域内的环境（如信息安全、DevOps 或特定法规）进行了定制。

4.4 焦点领域

焦点领域描述了一个特定的治理主题、领域或问题，可以通过一系列治理和管理目标及其组件来解决。焦点领域的例子包括：中小型企业、网络安全、数字化转型、云计算、隐私和 DevOps。[9] 焦点领域可能包含通用治理组件及变体的组合。

焦点领域的数量几乎没有限制，正因如此，COBIT 是开放式的。可根据需要添加新的焦点领域，或由主题专家和从业人员对开放式 COBIT 模型进行添加。

[9] DevOps 是组件变体和焦点领域的例证。为什么？DevOps 是市场中的最新主题，而且非常需要具体指导，因而成为一个焦点领域。DevOps 包括核心 COBIT 模型的若干通用治理和管理目标，以及与开发、运营和监控相关的流程及组织结构的一系列变体。

4.5 设计因素

设计因素可能影响企业治理系统的设计，为成功使用 I&T 奠定基础。

第 7.1 节阐述了设计因素对治理系统的潜在影响。有关如何使用设计因素来设计治理系统的更多信息和具体指导，请参阅《*COBIT® 2019设计指南*》。

设计因素包括以下任意组合（**图 4.4**）：

图 4.4—COBIT 设计因素

1. **企业战略** — 企业可以有不同的战略，这些战略可以用**图 4.5** 所示的一种或多种原型来表示。组织通常有一项主要战略，最多有一项次要战略。

图 4.5—企业战略设计因素

战略原型	说明
成长/收购	企业专注于成长（收入）。[10]
创新/差异化	企业专注于为客户提供不同的和/或创新的产品和服务。[11]
成本领导	企业专注于短期的成本最小化。[12]
客户服务/稳定性	企业专注于提供稳定的、面向客户的服务。[13]

[10] 与 Miles-Snow 战略类型学中的“探查者”(prospector) 相对应。请参阅 “Miles and Snow’s Typology of Defender, Prospector, Analyzer, and Reactor”，Elibrary，*https://ebrary.net/3737/management/miles_snows_typology_defender_prospector_analyzer_reactor*。

[11] 请参阅 Reeves, Martin；Claire Love，Philipp Tillmanns，“Your Strategy Needs a Strategy”，《*哈佛商业评论*》，2012 年 9 月，*https://hbr.org/2012/09/your-strategy-needs-a-strategy*，特别提及，有关愿景型和塑造型战略的内容。

[12] 与成本领导相对应；请参阅 University of Cambridge，“Porter’s Generic Competitive Strategies (ways of competing)”，Institute for Manufacturing (IfM) Management Technology Policy，*https://www.ifm.eng.cam.ac.uk/research/dstools/porters-generic-competitive-strategies/*。也与卓越运营相对应；请参阅 Treacy，Michael；Fred Wiersema，“Customer Intimacy and Other Value Disciplines”，《*哈佛商业评论*》，1993 年 1-2 月，*https://hbr.org/1993/01/customer-intimacy-and-other-value-disciplines*

[13] 与 Miles-Snow 战略类型学中的“防御者”(defender) 相对应。请参阅*前述著作* “Miles and Snow’s Typology of Defender, Prospector, Analyzer, and Reactor”。

2. **企业目标**支持企业战略 — 通过达成（一组）企业目标来实现企业战略。这些目标在 COBIT 框架中定义，按照平衡计分卡 (BSC) 维度进行组织，并包含**图 4.6** 所示的要素。

图 4.6—企业目标设计因素

参考资料	平衡计分卡 (BSC) 维度	企业目标
EG01	财务	有竞争力的产品和服务组合
EG02	财务	业务风险得到妥当管理
EG03	财务	遵守外部法律和法规
EG04	财务	财务信息的质量
EG05	客户	以客户为中心的服务文化
EG06	客户	业务服务连续性和可用性
EG07	客户	管理信息的质量
EG08	内部	内部业务流程功能的优化
EG09	内部	业务流程成本的优化
EG10	内部	员工技能、动力和生产力
EG11	内部	遵守内部政策
EG12	成长	妥当管理的数字化转型计划
EG13	成长	产品和业务创新

第 4.6 节包含有关 COBIT 目标级联的更多信息，其中详细说明了本设计因素。

3. 企业的**风险概况**和当前的 I&T 相关问题 — 风险概况标识了企业当前暴露的 I&T 相关风险，并指明了哪些风险领域超出风险偏好。风险类别[14] 如**图 4.7** 所列，应予以考虑。

图 4.7—风险概况设计因素（IT 风险类别）

参考资料	风险类别
1	IT 投资决策制定、投资组合定义和维护
2	计划和项目生命周期管理
3	IT 成本和监督
4	IT 专业知识、技能和行为
5	企业/IT 架构
6	IT 运营基础设施事故
7	未授权的行动
8	软件采用/使用问题
9	硬件事故
10	软件故障
11	逻辑攻击（黑客攻击、恶意软件等）
12	第三方/供应商事故
13	违规
14	地缘政治问题
15	劳工行动
16	自然灾害
17	基于技术的创新
18	环境
19	数据和信息管理

[14] 修订自 ISACA，*The Risk IT Practitioner Guide*，美国，2009 年

4. **I&T 相关问题** — 评估企业 I&T 风险的一个相关方法是考虑企业当前面临哪些 I&T 相关问题，换句话说，已存在哪些 I&T 相关风险。最常见的问题[15] 包括**图 4.8** 中列出的问题。

图 4.8—I&T 相关问题设计因素

参考资料	描述
A	由于被认为对业务价值的贡献较低，整个组织内的不同 IT 实体受挫
B	由于举措失败或被认为对业务价值的贡献较低，业务部门（即 IT 客户）和 IT 部门受挫
C	重大 IT 相关事故，例如与 IT 有关的数据丢失、安全漏洞、项目失败和应用程序错误
D	IT 外包商的服务交付问题
E	不符合 IT 相关法规或合同要求
F	关于 IT 绩效欠佳的定期审计结果或其他评估报告，或报告的 IT 服务或质量问题
G	重大的隐性和反常的 IT 支出，即用户部门的 IT 支出超出常规 IT 投资决策机制控制范围和批准的预算
H	多个举措之间的重复或重叠，或其他形式的资源浪费
I	IT 资源不足，员工技能欠缺或员工倦怠/不满意
J	IT 促成的变革或项目经常无法满足业务需求，并且延迟交付或超过预算
K	董事会成员、执行管理层或高级管理层不愿意参与 IT，或 IT 方面缺乏全身心投入的业务发起人
L	复杂的 IT 运营模式和/或缺乏明确的 IT 相关决策机制
M	过高的 IT 成本
N	当前 IT 架构和系统导致新举措或创新的实施受阻或失败
O	业务和技术知识之间的差距导致业务用户与信息和/或技术专家难以交流
P	各种来源的数据经常出现数据质量和整合方面的问题
Q	大量的最终用户计算导致对处于开发阶段和已投入运行的应用程序缺乏监督和质量控制（以及其他问题）
R	业务部门在企业 IT 部门极少甚至没有参与的情况下实施自己的信息解决方案[16]
S	忽视和/或违反隐私法规
T	无法利用新技术或使用 I&T 进行创新

5. **威胁环境** — 企业运营所处的威胁环境的分类如**图 4.9** 所示。

图 4.9—威胁环境设计因素

威胁环境	说明
Normal	企业运营环境被认为处于正常威胁水平。
高	由于地缘政治、行业领域或特定情况，企业在高威胁环境中运营。

[15] 另请参阅 ISACA《*COBIT 2019 实施指南：信息和技术治理解决方案的实施和优化*》（美国，2018 年）中的第 3.3.1 节“典型痛点”。
[16] 这个问题与最终用户计算有关，通常源于对 IT 解决方案和服务的不满。

6. **合规性要求** — 可根据**图 4.10** 中列出的类别对企业所遵守的合规性要求进行分类。

图 4.10—合规性要求设计因素	
监管环境	**说明**
低合规性要求	企业遵守最低限度的常规合规性要求，低于平均水平。
常规合规性要求	企业遵守不同行业通用的常规合规性要求。
高合规性要求	企业的合规性要求高于平均水平，通常与行业领域或地缘政治情况有关。

7. **IT 角色** — 可根据**图 4.11** 对企业 IT 角色进行分类。

图 4.11—IT 角色设计因素	
IT 角色[17]	**说明**
支持	IT 对业务流程和服务的运行和连续性及其创新都不是至关重要的。
工厂	如果出现 IT 故障，将会直接影响到业务流程和服务的运行和连续性。但 IT 并不被视为业务流程和服务的创新驱动力。
整顿	IT 被视为业务流程和服务的创新驱动力。但目前，业务流程和服务的运行和连续性对 IT 并没有重大依赖性。
战略	IT 对组织业务流程和服务的运行和创新至关重要。

8. **IT 采购模式** — 可根据**图 4.12** 对企业采用的采购模型进行分类。

图 4.12—IT 采购模式设计因素	
采购模式	**说明**
外包	企业委托第三方提供 IT 服务。
云	企业最大限度地利用云为其用户提供 IT 服务。
内包	企业有自己的 IT 员工和服务。
混合	采用混合模式，以不同程度结合采用三种模式。

9. **IT 实施方法** — 可根据**图 4.13** 对企业采用的方法进行分类。

图 4.13—IT 实施方法设计因素	
IT 实施方法	**说明**
敏捷	企业使用敏捷开发工作方法进行软件开发。
DevOps	企业使用 DevOps 工作方法进行软件构建、部署和运行。
传统	企业使用更经典的软件开发方法（瀑布式开发），并将软件开发与运行分离开来。
混合	企业将传统的和现代的 IT 实施相结合，通常被称为“双模式 IT”。

[17] 此表包含的角色摘自 McFarlan, F. Warren；James L. McKenney；Philip Pyburn；“The Information Archipelago—Plotting a Course”，*《哈佛商业评论》*，1993 年 1 月，*https://hbr.org/1983/01/the-information-archipelago-plotting-a-course*。

10. **技术采用战略** — 可根据**图 4.14** 对技术采用战略进行分类。

图 4.14—技术采用战略设计因素	
技术采用战略	**说明**
先行者	企业通常会尽早采用新技术，以抢占先发优势。
追随者	企业通常会先观望，直到新技术成为主流并得到验证才会采用。
滞后者	企业采用新技术的时间严重滞后。

11. **企业规模** — 针对企业治理系统的设计确定了两类规模，如**图 4.15** 所示。[18]

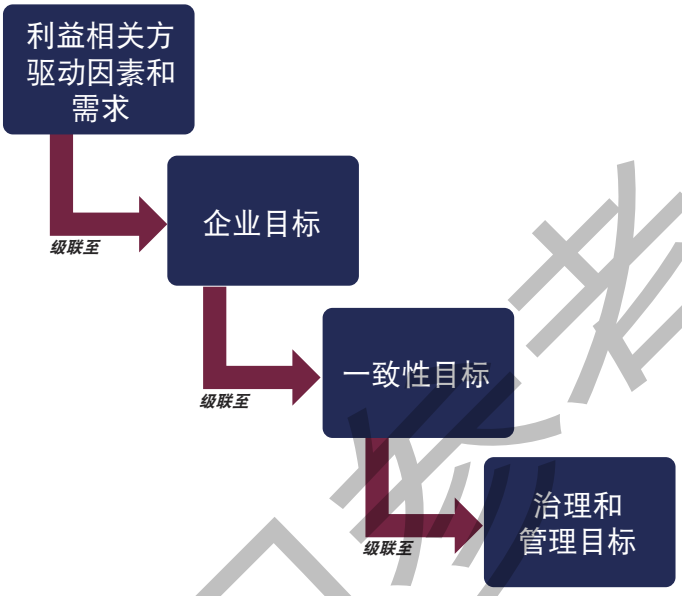
图 4.15—企业规模设计因素	
企业规模	**说明**
大型企业（默认）	拥有超过 250 名全职员工 (FTE) 的企业
中小型企业	拥有 50-250 名全职员工的企业

[18] 微型企业，即员工少于 50 人的企业，不在本书的讨论范围内。

4.6 目标级联

利益相关方需求必须要转化为企业的可执行战略。目标级联（**图 4.16**）支持企业目标，是治理系统的关键设计因素之一。它支持基于企业目标的优先级来确定管理目标的优先级。

图 4.16—COBIT 目标级联



目标级联进一步支持将企业目标转化为优先的一致性目标。COBIT® 2019 全面更新了目标级联：

- 整合、精简、更新和澄清了企业目标。
- 一致性目标强调所有 IT 工作与业务目标的一致性。[19] 此术语的更新是为了避免一个常见误解：这些目标仅代表企业 IT 部门的内部目标。与企业目标一样，一致性目标也进行了必要的整合、精简、更新和澄清。

[19] 在 COBIT 5 中，一致性目标被称为“IT 相关目标”。

4.6.1 企业目标

利益相关方需求级联至企业目标。**图 4.17** 展示了 13 项企业目标及一些配套的指标示例。

图 4.17—目标级联：企业目标和指标

参考资料	BSC 维度	企业目标	指标示例
EG01	财务	有竞争力的产品和服务组合	• 达到或超过收益和/或市场份额目标的产品和服务的百分比
			• 达到或超过客户满意度目标的产品和服务的百分比 • 带来竞争优势的产品和服务的百分比 • 新产品和服务的上市时间
EG02	财务	业务风险得到妥当管理	• 风险评估涵盖的关键业务目标和服务的百分比 • 风险评估未发现的重大事故数量与总事故数量的比率 • 合适的风险概况更新频率
EG03	财务	遵守外部法律和法规	• 不合规的成本，包括结算和罚款 • 引起负面舆论或负面影响的不合规问题的数量 • 监督或监管机构指出的不合规问题的数量 • 与业务伙伴合同协议有关的不合规问题的数量
EG04	财务	财务信息的质量	• 有关企业财务信息的透明度、了解度和准确性的关键利益相关方满意度调查 • 财务相关法规要求的不合规成本
EG05	客户	以客户为中心的服务文化	• 客户服务中断的次数 • 业务利益相关方确信客户服务交付达到议定水平的百分比 • 客户投诉的数量 • 客户满意度调查结果的趋势
EG06	客户	业务服务连续性和可用性	• 导致重大事故的客户服务或业务流程中断的次数 • 事故的业务成本 • 因计划外服务中断而损失的业务处理小时数 • 与承诺的服务可用性目标有关的投诉百分比
EG07	客户	管理信息的质量	• 董事会和执行管理层对决策信息的满意度 • 基于不准确信息的错误业务决策所导致的事故数量 • 为有效业务决策提供支持性信息所花的时间 • 管理信息的及时性
EG08	内部	内部业务流程功能的优化	• 董事会和执行管理层对业务流程能力的满意度 • 客户对服务交付能力的满意度 • 供应商对供应链能力的满意度
EG09	内部	业务流程成本的优化	• 成本与达到的服务水平的比率 • 董事会和执行管理层对业务流程成本的满意度
EG10	内部	员工技能、动力和生产力	• 相较于基准的员工生产力 • 利益相关方对员工专业知识和技能的满意度 • 相对角色所需能力而言技能不足的员工的百分比 • 满意员工的百分比
EG11	内部	遵守内部政策	• 与违反政策有关的事故数量 • 了解政策的利益相关方的百分比 • 得到有效标准和工作实践支持的政策的百分比

图 4.17—目标级联：企业目标和指标（续）			
参考资料	BSC 维度	企业目标	指标示例
EG12	成长	妥当管理的数字化转型计划	• 按时在预算内交付的计划的百分比 • 对计划交付满意的利益相关方的百分比 • 中止的业务转型计划的百分比 • 定期报告状态更新的业务转型计划的百分比
EG13	成长	产品和业务创新	• 对业务创新机会的认识和理解水平 • 利益相关方对产品以及创新专长和想法的满意度 • 源自创新想法的已批准产品和服务举措的数量

4.6.2 一致性目标

企业目标级联至一致性目标。**图 4.18** 包含一组一致性目标和指标示例。

图 4.18—目标级联：一致性目标和指标			
参考资料	IT BSC 维度	一致性目标	指标
AG01	财务	I&T 合规且支持业务部门遵守外部法律和法规	• IT 不合规的成本，包括费用结算和罚款，以及声誉损失造成的影响 • 向董事会报告或者引起舆论或难堪的 IT 相关不合规问题的数量 • 与 IT 服务提供商的合同协议有关的不合规问题的数量
AG02	财务	妥善管理的 I&T 相关风险	• 合适的风险概况更新频率 • 涵盖 I&T 相关风险的企业风险评估的百分比 • 风险评估中未识别的 I&T 相关重大事故的数量
AG03	财务	通过 I&T 促成的投资和服务组合所实现的效益	• 达到或超过业务案例宣称效益的 I&T 促成的投资的百分比 • 实现预期效益（如服务水平协议所述）的 I&T 服务的百分比
AG04	财务	技术相关财务信息的质量	• 有关 IT 财务信息的透明度、了解度和准确性水平的关键利益相关方满意度 • 已定义运营成本和预期效益并获得批准的 I&T 服务的百分比
AG05	客户	提供符合业务要求的 I&T 服务	• 确信 IT 服务交付达到议定服务水平的业务利益相关方的百分比 • 因 IT 服务事故造成业务中断的次数 • 对 IT 服务交付质量满意的用户的百分比
AG06	客户	将业务需求转化为可运作的解决方案的敏捷性	• 业务高管对 IT 响应新需求的满意度水平 • 新的 I&T 相关服务和应用程序的平均上市时间 • 将战略 I&T 目标转化为议定的已批准举措所需的平均时间 • 受最新基础设施和应用支持的关键业务流程的数量
AG07	内部	信息、处理基础设施和应用程序的安全，以及隐私	• 导致财务损失、业务中断或公众形象受损的保密性事故的数量 • 导致财务损失、业务中断或公众形象受损的可用性事故的数量 • 导致财务损失、业务中断或公众形象受损的完整性事故的数量
AG08	内部	通过集成应用程序和技术来推行和支持业务流程	• 执行业务服务或流程的时间 • 因技术集成问题而延迟或产生额外成本的 I&T 促成的业务计划的数量 • 因技术集成问题而延迟或返工的业务流程变更的数量 • 独立运行和未集成的应用程序或关键基础设施的数量

图 4.18—目标级联：一致性目标和指标（续）			
参考资料	**IT BSC 维度**	**一致性目标**	**指标**
AG09	内部	在预算内按时交付计划且满足需求和质量标准	• 在预算内按时交付的计划/项目的数量 • 因质量缺陷需要重大返工的计划的数量 • 对计划/项目质量满意的利益相关方的百分比
AG10	内部	I&T 管理信息的质量	• 考虑到可用资源，用户对 I&T 相关管理信息的质量、及时性和可用性的满意度水平 • 主要因 I&T 相关信息错误或不可用导致的错误业务决策的比率和程度 • 满足质量标准的信息的百分比
AG11	内部	I&T 遵守内部政策	• 与违反 IT 相关政策有关的事故的数量 • 内部政策的例外情况的数量 • 政策审查和更新的频率
AG12	学习和发展	既了解技术又熟知业务、能力出众且积极上进的员工	• 精通 I&T 的业务人员（即具备必要的 I&T 知识且了解 I&T，能够引导、指导、创立和发现在其专业领域运用 I&T 的机会）的百分比 • 精通业务的 IT 人员（即具备必要的相关业务领域知识和理解，能够引导、指导、创立和发现在业务领域运用 I&T 的机会）的百分比 • 拥有技术管理经验的业务人员的数量或百分比
AG13	学习和发展	业务创新的知识、专业技能和举措	• 业务高管对 I&T 创新可能性的认识和理解水平 • 源自 I&T 创新想法的已批准举措的数量 • 获得认可/奖励的创新推动者的数量

本页特意留白

第五章
COBIT 治理和管理目标

5.1 目的

第 4.2 节图 **4.2** 展示了 COBIT 核心模型，包括 40 项治理和管理目标。**图 5.1** 列出了所有治理和管理目标及相应的目的说明。目的说明是对各项治理和管理目标的进一步解释。

图 5.1—COBIT 核心模型：治理和管理目标及目的

参考资料	名称	目的
EDM01	确保治理框架的设置和维护	提供与企业治理方法相结合的一致方法。I&T 相关决策必须与企业的战略和目标保持一致，并实现期望的价值。为此，应确保 I&T 相关流程得到有效和透明的监督，符合法律、合同和监管要求，以及满足董事会成员的治理要求。
EDM02	确保实现效益	保证从 I&T 促成的举措、服务及资产中获得最佳价值；以经济高效的方式提供解决方案和服务；可靠准确地维护成本和效益信息，从而有效和高效地支持业务需求。
EDM03	确保风险优化	确保 I&T 相关企业风险不超过企业的风险偏好和风险容忍度，识别和管控 I&T 风险对企业价值的影响，以及最大程度地降低不合规的可能性。
EDM04	确保资源优化	确保以最优的方式满足企业的资源需求，优化 I&T 成本，提高效益实现的可能性，并为未来的改变做好准备。
EDM05	确保利益相关方参与	确保利益相关方支持 I&T 战略和路线图；与利益相关方保持及时有效的沟通；以及建立报告基础以提高绩效。识别待改进的领域，并确认 I&T 相关目标和战略与企业战略保持一致。
APO01	妥当管理的 I&T 管理框架	实施一致的管理方法来满足企业治理要求，且涵盖以下治理组件，例如：如管理流程、组织结构、角色和职责、可靠且可重复的活动、信息项、政策和程序、技能和能力、文化和行为以及服务、基础设施和应用程序。
APO02	妥当管理的战略	支持组织的数字化转型战略，并通过递增路线图实现期望的价值。采用 I&T 整体性方法，确保每项举措都与总体战略明确相关。推动组织实现所有方面的变革，从渠道和流程到数据、文化、技能、运营模式和激励机制。
APO03	妥当管理的企业架构	表示不同的构建区块，它们构成企业及其相互关系以及指导设计与发展演变的原则，促进标准、快速及有效地交付运营和战略目标。
APO04	妥当管理的创新	利用 I&T 发展和新兴技术来获取竞争优势、推动业务创新、提高客户体验以及改善运营效率和效果。
APO05	妥当管理的组合	优化总体计划组合的绩效，以应对个别计划、产品和服务的绩效以及不断变化的企业优先级和需求。
APO06	妥当管理的预算和成本	促进 IT 与企业利益相关方之间的合作伙伴关系，有效和高效地使用 I&T 相关资源，在解决方案和服务的成本与业务价值方面保持透明并采取问责制。使企业能够就 I&T 解决方案和服务的使用做出明智的决策。
APO07	妥当管理的人力资源	优化人力资源能力，以实现企业目标。
APO08	妥当管理的关系	掌握正确的知识、技能和行为，来创造更好的成果，增强信心和相互信任，以及有效地利用资源，以促进与业务利益相关方建立富有成效的关系。
APO09	妥当管理的服务协议	确保 I&T 产品、服务和服务水平满足当前和未来的企业需求。
APO10	妥当管理的供应商	优化可用的 I&T 能力，以支持 I&T 战略和路线图，最大程度地降低与不履约或不合规供应商相关的风险，并确保有竞争力的定价。

图 5.1—COBIT 核心模型：治理和管理目标及目的（续）		
参考资料	名称	目的
APO11	妥当管理的质量	确保以一致的方式交付技术解决方案和服务，以满足企业的质量要求和利益相关方的需求。
APO12	妥当管理的风险	将 I&T 相关企业风险管理整合到总体企业风险管理 (ERM) 中，并平衡 I&T 相关企业风险管理的成本和效益。
APO13	妥当管理的安全	确保将信息安全事故的发生和影响保持在企业的风险偏好水平内。
APO14	妥当管理的数据	确保有效利用关键数据资产，以实现企业目标和目的。
BAI01	妥当管理的计划	实现期望的业务价值，降低因意外的延迟、成本和价值流失带来的风险。为此，应改进与业务部门和最终用户的沟通并提高他们的参与度，确保计划交付成果和计划内后续项目的价值和质量，并最大程度地提高对投资组合的贡献。
BAI02	妥当管理的需求定义	创建最优解决方案，在满足企业需求的同时最大程度降低风险。
BAI03	妥当管理的解决方案识别和构建	确保以敏捷和可扩展的方式交付数字产品和服务。建立及时、成本高效并且能够支持企业战略和运营目标的解决方案（技术、业务流程和工作流程）。
BAI04	妥当管理的可用性和容量	通过预测未来的性能和容量要求来维护服务可用性、有效的资源管理并优化系统性能。
BAI05	妥当管理的组织变更	为业务变更做好准备和承诺，减少失败的风险。
BAI06	妥当管理的 IT 变更	快速、可靠地交付业务变更。缓解对变更后环境的稳定性或完整性产生负面影响的风险。
BAI07	妥当管理的 IT 变更接受和交接	根据协定的期望和成果，安全地实施解决方案。
BAI08	妥当管理的知识	为所有员工提供能支持企业 I&T 治理和管理以及做出明智决策所需的知识和管理信息。
BAI09	妥当管理的资产	核算所有 I&T 资产并优化这些资产提供的价值。
BAI10	妥当管理的配置	提供关于服务资产的充分信息，以有效地管理服务。评估变更影响并处理服务事故。
BAI11	妥当管理的项目	通过改进与业务部门和最终用户的沟通并提高他们的参与度来实现定义的项目成果，并降低因意外的延迟、成本和价值流失带来的风险。确保项目交付成果的价值和质量，并最大程度地提高它们对定义的计划和投资组合的贡献。
DSS01	妥当管理的运营	按计划提供可运行的 I&T 产品和服务成果。
DSS02	妥当管理的服务请求和事故	通过快速解决用户查询和事件来实现生产力的提升和最大程度减少中断。评估变更影响并处理服务事故。处理用户请求并在事故后恢复服务。
DSS03	妥当管理的问题	通过减少运营问题来提高可用性和服务水平，降低成本，提高客户的便利度和满意度，以及通过确定根本原因协助解决问题。
DSS04	妥当管理的连续性	在发生重大中断事件（如威胁、机会、要求）时快速调整，维持业务运营，并将资源和信息的可用性保持在企业可接受的水平之上。
DSS05	妥当管理的安全服务	最大程度降低运营信息安全漏洞和事故造成的业务影响。
DSS06	妥当管理的业务流程控制	维护企业内部业务流程或外包运营所处理的信息资产的完整性和安全性。
MEA01	妥当管理的绩效和一致性监控	提供透明的绩效和一致性，并推动目标的实现。
MEA02	妥当管理的内部控制系统	在内部控制系统的充分性方面实现关键利益相关方透明度，从而建立运营信任、对实现企业目标的信心并充分了解剩余风险。
MEA03	妥当管理的外部要求合规性	确保企业符合所有适用的外部要求。
MEA04	妥当管理的鉴证	促使组织设计和制定高效和有效的鉴证举措，并使用基于公认的鉴证方法的路线图来指导鉴证审查的规划、范围界定、执行和后续跟进。

第六章
COBIT 中的绩效管理

6.1 定义

绩效管理是治理和管理系统中不可或缺的一部分。“绩效管理”是所有活动和方法的总称。它说明了企业治理和管理系统及所有组件的运作情况，以及如何改进它们以达到所需的水平。它包括概念和方法，如能力级别和成熟度级别。COBIT 使用术语“COBIT 绩效管理”(CPM) 来描述这些活动，这个概念是 COBIT 框架不可或缺的一部分。

6.2 COBIT 绩效管理原则

COBIT® 2019 基于以下原则：

1. CPM 应易于理解和使用。
2. CPM 应符合且支持 COBIT 概念模型。它应促进所有类型的治理系统组件的绩效管理；如用户要求，它还能管理流程以及其他类型组件（如组织结构或信息）的绩效。
3. CPM 应提供可靠、可重复且相关的结果。
4. CPM 必须足够灵活，才能支持具有不同优先级和需求的不同组织的要求。
5. CPM 应支持不同类型的评估，包括自我评估、正式评估和审计。

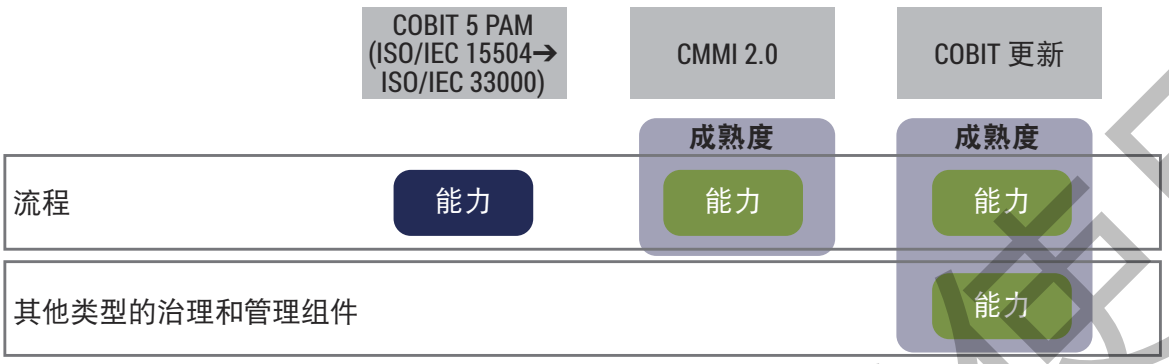
6.3 COBIT 绩效管理概述

CPM 模型（**图 6.1**）大体符合以下 CMMI® Development V2.0 [20] 概念并进行了扩展：

- 流程活动与能力级别相关。这包含在*《COBIT® 2019 框架：治理和管理目标》*指南中。
- 未来的指南可能会定义其他治理和管理组件类型（如组织结构、信息）的能力级别。
- 成熟度级别与焦点领域（即一系列治理和管理目标及支持组件）相关，达到所有必需的能力级别便可达到相应的成熟度级别。

[20] CMMI® Development V2.0，CMMI Institute，美国，2018 年，*https://cmmiinstitute.com/model-viewer/dashboard*

图 6.1—能力级别



如果企业希望继续使用基于国际标准化组织 (ISO)/国际电工技术委员会 (IEC) 15504（即现在的 ISO/IEC 33000，其中能力级别有不同的含义）的 COBIT 5 流程能力模型，*《COBIT® 2019 框架：治理和管理目标》*中提供了他们所需的全部信息。单独的流程评估模型 (PAM) 出版物不是必要的，COBIT® 2019 中也不会附带这类出版物。

在 COBIT® 2019 中，流程实践本身取代了具体的流程成果或流程目标。这使得 ISO/IEC33000 评估面临以下情况：

1. 流程成果现在与流程实践一一对应（即流程成果是成功完成流程实践的结果）。注：流程实践被设计为可以产生成果的实务。示例：“APO01.01 *设计企业 I&T 的管理系统*”的流程成果是 APO01.01：*已设计企业 I&T 管理系统*。
2. 基本实践相当于每个治理和管理目标的 COBIT® 2019 流程实践。
3. 工作成果相当于组件 C 下每个治理/管理目标的信息流和项目。

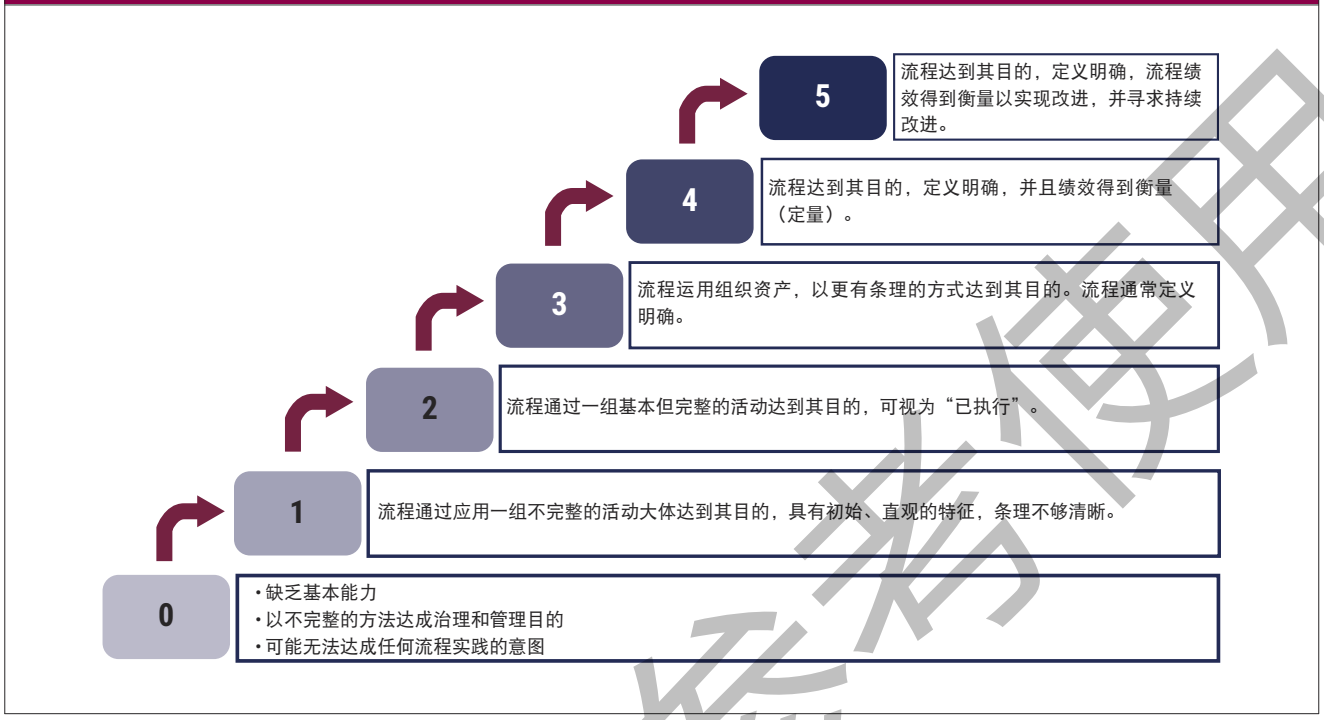
因此，基本实践成果和工作成果的映射是通过 COBIT® 2019 中的定义来完成的。

6.4 管理流程绩效

6.4.1 流程能力级别

COBIT® 2019 支持基于 CMMI 的流程能力方案。每个治理和管理目标内的流程可在 0 到 5 之间的不同能力级别下运行。能力级别用于衡量流程的实施和执行情况。**图 6.2** 描述了模型、递增的能力级别以及每个级别的一般特征。

图 6.2—流程的能力级别



COBIT 核心模型为所有流程活动分配了能力级别，从而明确定义了流程以及达到不同能力级别所需的活动。请参阅《*COBIT® 2019 框架：治理和管理目标*》，了解更多详细信息。

6.4.2 流程活动评级

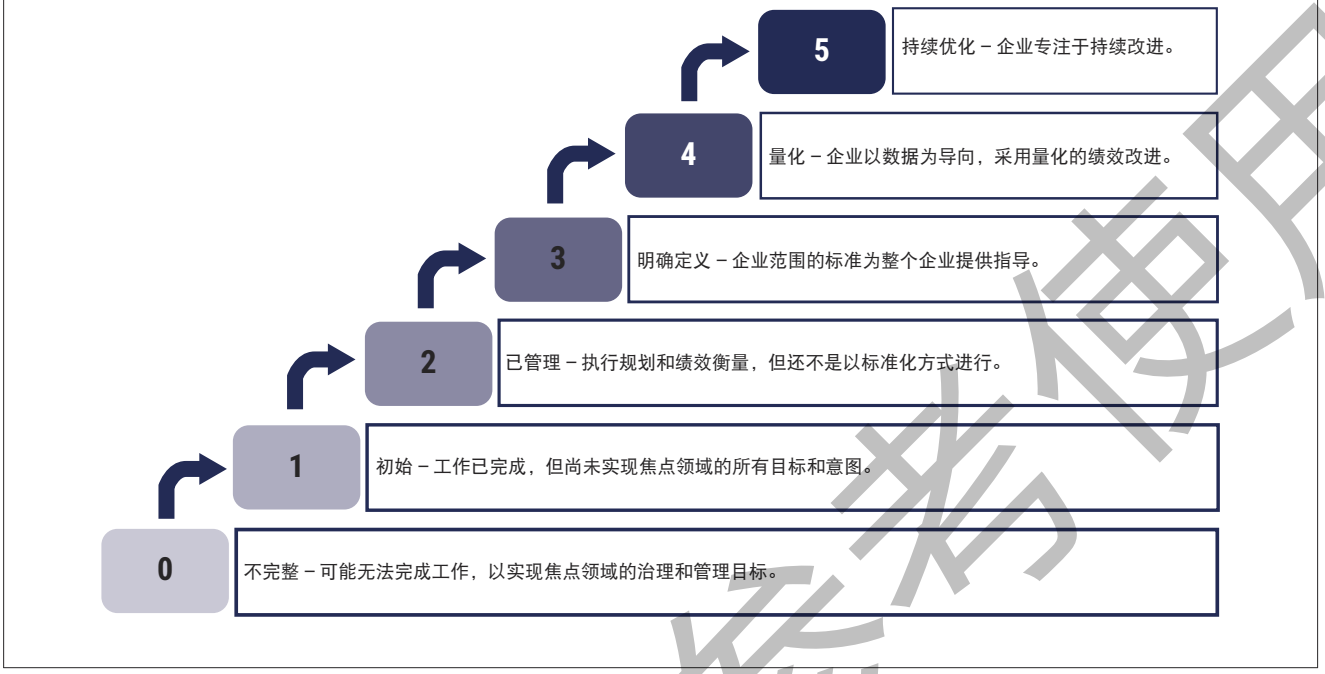
能力级别的实现程度可能有所不同，可以用一组评级来表示。可用评级的范围取决于执行绩效评估的背景：

- 有些独立认证的正式方法会采用二元的通过/未通过的评级方式。
- 不太正式的方法（通常用于绩效改进背景）在使用较大范围的评级时效果更好，例如：
  - *完全* — 达到能力级别的程度超过 85%。（仍带有主观性，但可以通过审查或评估动力组件来证实，例如流程活动、流程目标或组织结构的良好实践。）
  - *大致* — 达到能力级别的程度在 50% 到 85% 之间。
  - *部分* — 达到能力级别的程度在 15% 到 50% 之间。
  - *未达到* — 达到能力级别的程度低于 15%。

6.4.3 焦点领域的成熟度级别

有时如果没有适用于单个流程能力评级的颗粒度，则需要一个更高的级别来表示绩效。成熟度级别可实现此目的。COBIT® 2019 将成熟度级别定义为焦点领域层级的绩效衡量指标，如**图 6.3** 所示。

图 6.3—焦点领域的成熟度级别



成熟度级别与焦点领域（即一系列治理和管理目标及支持组件）相关。如果焦点领域所包含的全部流程都达到特定的能力级别，则该焦点领域达到了相应的成熟度级别。

6.5 管理其他治理系统组件的绩效

6.5.1 组织结构的绩效管理

虽然目前还没有公认或正式的方法用于评估组织结构，但可以根据以下标准进行非完全正式的评估。每个标准还可以定义多个关联到不同能力级别的子标准。这些标准是：

- 成功执行了组织结构（或角色）负有责任或职责（在执行人、责任人、咨询人和知情人 [RACI] 矩阵中分别对应责任人 [A] 和执行人 [R]）的流程实践
- 成功运用了一些组织结构方面的良好实践，例如：
  - 运作原则
    - 正式建立了组织结构。
    - 组织结构具有明确、有记录且易于理解的要求。
    - 记录了运作原则。
    - 根据运作原则定期召开会议。
    - 可提供有意义的会议报告/记录。
  - 组成
    - 正式建立了组织结构。

  - 控制范围
    - 组织结构具有明确、有记录且易于理解的要求。
    - 记录了运作原则。
    - 根据运作原则定期召开会议。
    - 可提供有意义的会议报告/记录。
  - 权力级别和决策权
    - 定义和记录了组织结构的决策权。
    - 尊重并遵守组织结构的决策权（也属于文化/行为问题）。
  - 授权
    - 以有意义的方式实施授权。
  - 上报程序
    - 定义并运用了上报程序。
- 成功运用了一些组织结构方面的管理实践（对组织结构而言是非功能性实践）：
  - 识别了组织结构的绩效目标。
  - 规划并监控了组织结构的绩效。
  - 调整了组织结构绩效以满足计划要求。
  - 识别、提供、分配并使用了组织结构必需的资源和信息。
  - 管理了组织结构与其他利益相关方之间的接口，以确保有效的沟通及明确的责任分配。
  - 通过定期评估，对组织结构实施必要的持续改进，包括其组成、要求或任何其他参数。

对流程来说，达到较低的能力级别只需满足一部分标准，要达到更高的能力级别则需要满足所有标准。之前已经提到，目前还没有公认的组织结构评估方案，但这并不妨碍企业自行定义组织结构能力评估方案。

6.5.2 信息项的绩效管理

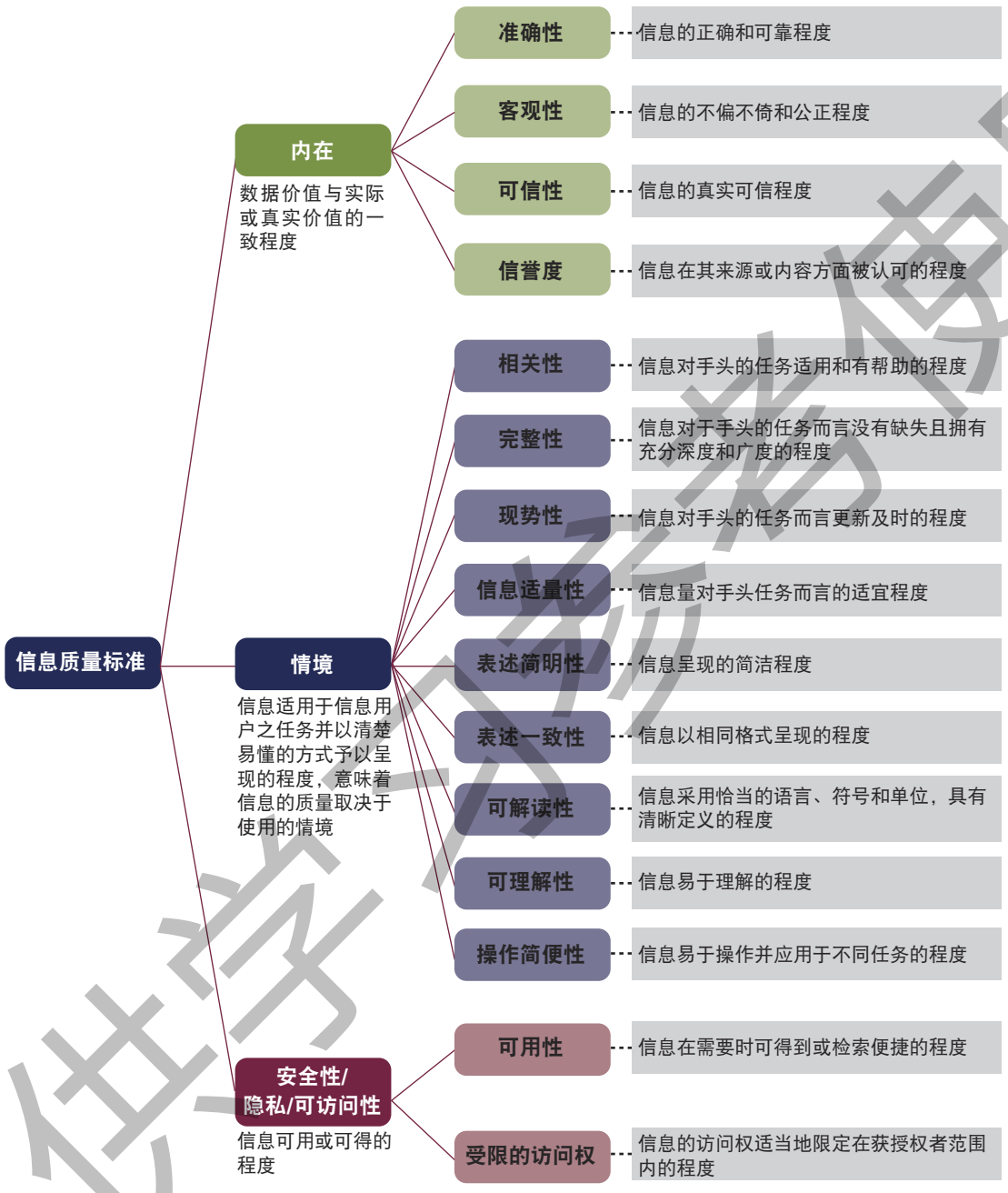
I&T 治理系统的信息项组件大体相当于《*COBIT® 2019 框架：治理和管理目标*》中所述的流程工作成果。

目前还没有公认或正式的方法用于评估信息项，但可以根据在《*COBIT® 5：启用信息*》首次提出的信息参考模型来进行非完全正式的评估。[21]

此模型定义了三项主要的信息质量标准以及 15 项子标准，如**图 6.4** 所示。

[21] 请参阅 ISACA，《*COBIT® 5：启用信息*》第 3.1.2 节“目标”，美国，2013 年，*http://www.isaca.org/COBIT/Pages/COBIT-5-Enabling-Information-product-page.aspx*

图 6.4—信息参考模型：信息的质量标准



信息项可通过衡量其达到相关质量标准（如**图 6.4** 所示）的程度进行评估。

6.5.3 文化和行为的绩效管理

对于文化和行为治理组件，可针对良好的 IT 治理和管理定义一组可取的和/或不可取的行为，并为每个行为分配不同的能力级别。

*《COBIT® 2019 框架：治理和管理目标》*针对大多数目标提供了文化和行为组件方面的定义，可据此评估达到这些条件或行为的程度。

后续将会进一步开发该焦点领域的内容，以包含一组更详细的可取的行为。如需了解最新状态和可用的焦点领域指南，欢迎用户咨询 *isaca.org/cobit*。

本页特意留白

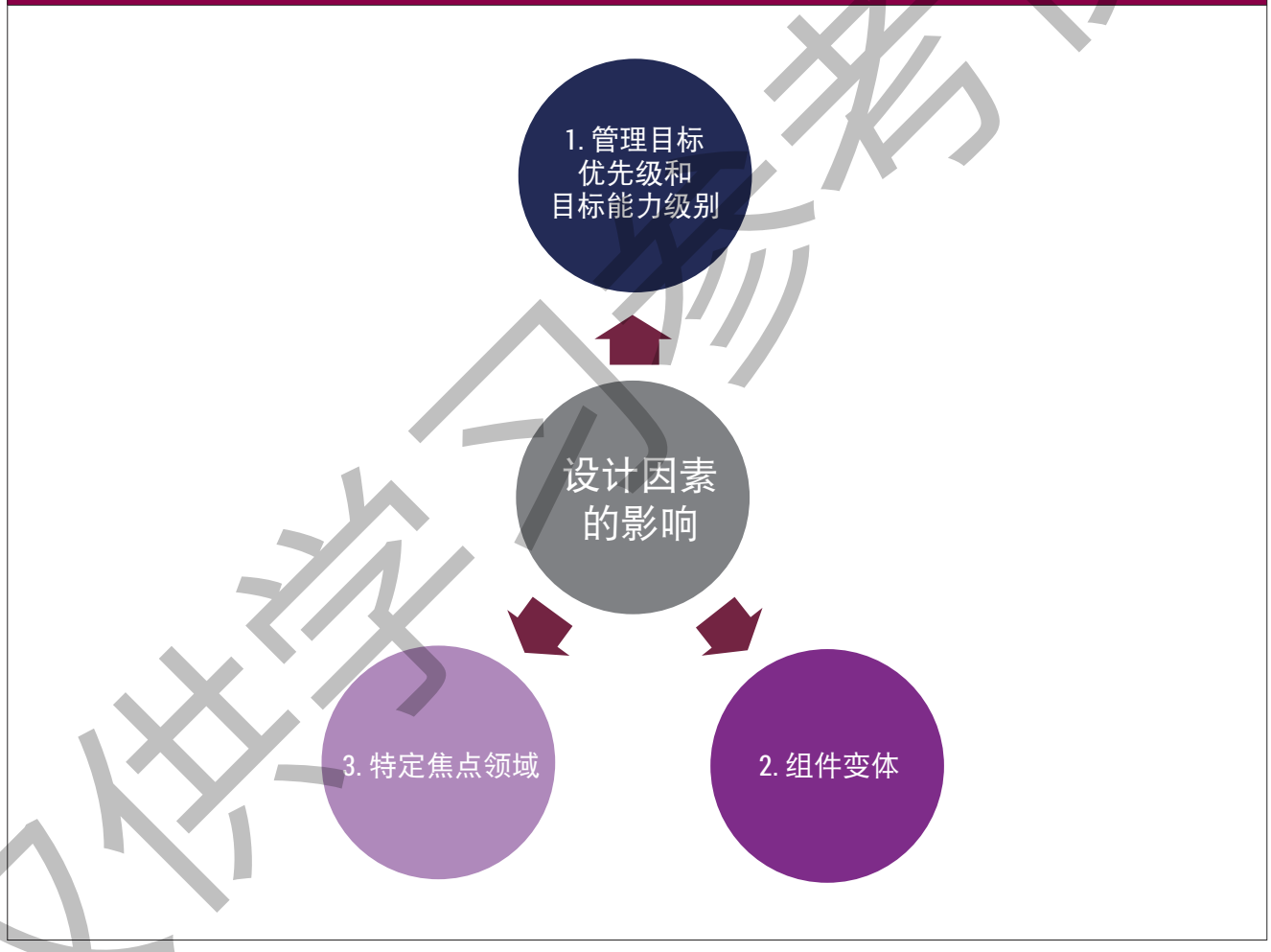
第七章
设计量身定制的治理系统

7.1 设计因素的影响

本节概述了设计因素对企业 I&T 治理系统的潜在影响。它还从更高层面上描述了为企业设计量身定制的治理系统的工作流程。有关这些主题的更多信息，请参阅《*COBIT® 2019 设计指南*》。

设计因素对企业治理系统的定制产生的影响体现在多个方面。本书将这些影响划分为三种不同的类型，如**图 7.1** 所示。

图 7.1—设计因素对治理和管理系统的影响



1. **管理目标优先级/选择** — COBIT 核心模型包含 40 个治理和管理目标，每个目标由相应的流程和一些相关组件构成。它们本质上是均等的，没有先后顺序。但是，设计因素可以影响这种均等关系，使某些治理和管理目标比其他目标更重要，甚至使某些治理和管理目标变得可忽略不计。在实践中，治理和管理目标的重要性越高，意味着为其设定的目标能力级别越高。

示例： 如果一家企业从企业目标列表中确定了相关度最高的企业目标并应用目标级联，将会产生一系列优先的管理目标。例如，如果企业高度重视“*EG01 有竞争力的产品和服务组合*”，则管理目标“*APO05 妥当管理的组合*”将成为该企业治理系统的重要组成部分。

示例： 对风险极度敏感的企业会更加重视可促进治理及管理风险和安全的管理目标。治理和管理目标“EDM03 *确保风险优化*”、“APO12 *妥当管理的风险*”、“APO13 *妥当管理的安全*”和“DSS05 *妥当管理的安全服务*”将成为该企业治理系统的重要组成部分，企业将为它们定义更高的目标能力级别。

示例： 在高威胁环境中运营的企业需要高能力的安全相关流程：“APO13 *妥当管理的安全*”和“DSS05 *妥当管理的安全服务*”。

示例： 如果 IT 角色对业务成功具有战略性和关键性的作用，则企业需要组织结构中 IT 相关角色的高度参与、IT 专业人员对业务透彻的了解（反之亦然），及对“APO02 *妥当管理的战略*”和“APO08 *妥当管理的关系*”等战略流程的关注。

2. **组件变体** — 实现治理和管理目标需要多个组件。一些设计因素可能影响一个或多个组件的重要性，或者要求特定的变体。

示例： 中小型企业可能不需要 COBIT 核心模型中列出的全套角色和组织结构，但可能使用简化版本作为替代。中小企业焦点领域中定义了这些简化的治理和管理目标及其包含的组件。[22]

示例： 在受到严格监管的环境中运营的企业会更加重视*有记录的工作成果、政策和程序*，以及某些角色，例如合规官职能。

示例： 使用 DevOps 进行解决方案开发和运营的企业需要侧重于有关“BAI03 *妥当管理的解决方案识别和构建*”和“DSS01 *妥当管理的运营*”的特定活动、组织结构和文化等。

3. **对特定焦点领域的需求** — 一些设计因素（如威胁环境、特定风险、目标开发方法和基础设施设置）将会推动核心 COBIT 模型内容到具体环境转变的需求。

示例： 采用 DevOps 方法的企业需要在治理系统中包含 COBIT 的 DevOps 焦点领域指南中所述的若干通用 COBIT 流程[23] 的变体。

示例： 中小型企业的员工人数较少，IT 资源较少，汇报关系更简单和直接，与大型企业存在多方面的差异。因此，与大型企业相比，他们的 I&T 治理系统不能太繁杂。COBIT 的 SME 焦点领域指南中对此进行了详细说明。[24]

[22] 本《*COBIT® 2019 框架：简介和方法*》出版时，中小企业焦点领域的内容正在制定中，尚未发布。
[23] 本《*COBIT® 2019 框架：简介和方法*》出版时，DevOps 焦点领域的内容正在制定中，尚未发布。
[24] 本《*COBIT® 2019 框架：简介和方法*》出版时，中小企业焦点领域的内容正在制定中，尚未发布。

7.2 设计流程的阶段和步骤

图 7.2 提供了建议的定制治理系统设计流程。

图 7.2—治理系统设计工作流程

如**图 7.2** 所示，在设计流程的不同阶段和步骤中，会提出实现治理和管理目标或实施相关治理系统组件的优先级建议，针对目标能力级别的建议，以及采用特定治理系统组件变体的建议。

其中一些步骤或子步骤可能会产生彼此冲突的指导，考虑到存在大量设计因素，以及设计因素指导意见和所用映射表的通用性质，这也是不可避免的。

建议在设计流程的最后阶段，将在不同步骤中获得的所有指导意见排列在设计“画板”上，尽可能地解决“画板”上所有要素之间的冲突，并得出最终结论。这一过程没有万能秘方。最终设计将是基于设计“画板”上所有要素的具体决策。通过遵循这些步骤，企业将获得针对其需求定制的治理系统。

本页特意留白

第八章
实施企业 IT 治理

8.1 COBIT 实施指南的目的

《*COBIT® 2019 实施指南*》强调从整个企业的角度来审视 I&T 治理。本指南认识到 I&T 已渗透到企业的每个角落，要将业务与 IT 相关的活动分开既不现实也不是一种良好实践。因此，企业 I&T 治理和管理应作为企业治理不可或缺的一部分来实施，全面覆盖端到端的业务和 IT 职能领域的责任。

有些治理系统的实施之所以会失败，一个常见的原因是没有按照计划发起并继以妥善的管理，无法确保实现效益。治理计划须由执行管理层发起、确定适当的范围并定义可实现的目标。这样，企业才能按计划跟上变化的步伐。因此，计划管理应作为实施生命周期不可或缺的一部分。

也有人认为，尽管推荐采用计划和项目的方式来有效推动改进举措，像企业治理的其他方面一样，其目标也是为治理与管理企业 I&T 建立起常规的业务实践和可持续的方法。因此，实施的方法是基于赋能业务和 IT 利益相关方及相关角色，通过促进和推行变革，让他们负责 IT 相关的治理和管理决策以及活动。当侧重 IT 相关优先目标和治理改进的流程开始产生可衡量的效益，且计划已被嵌入持续进行的业务活动中时，实施计划将会关闭。

有关这些主题的更多信息，请参阅《*COBIT® 2019 实施指南*》。

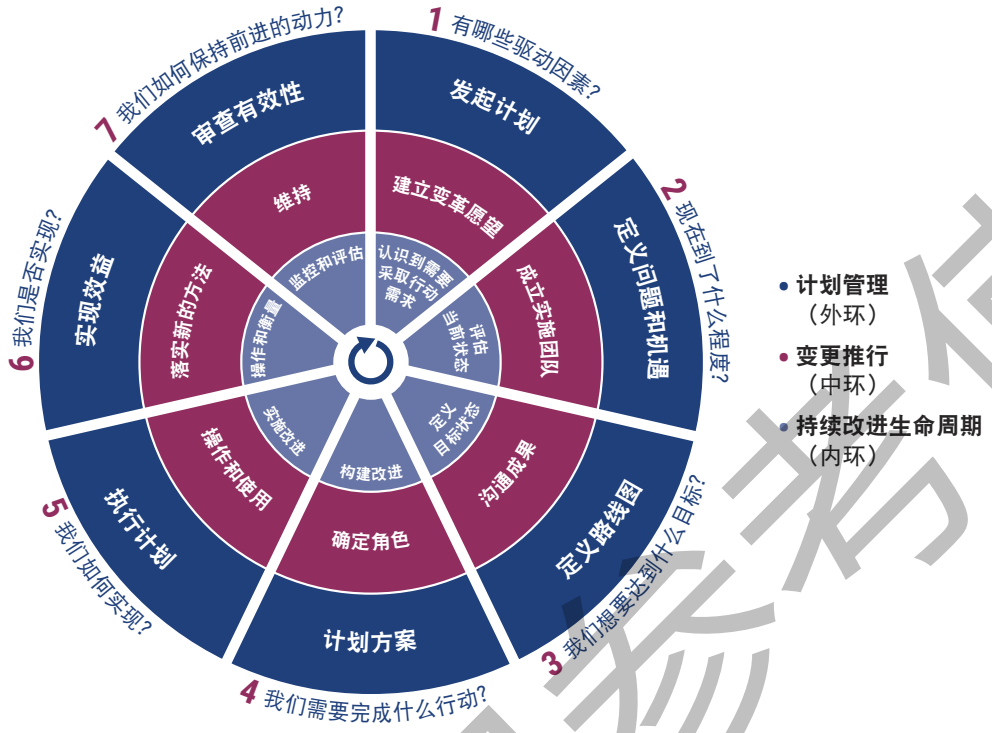
8.2 COBIT 实施方法

COBIT 实施方法包含 7 个阶段：

- 有哪些驱动因素?
- 现在到了什么程度?
- 我们想要达到什么目标?
- 我们需要完成什么行动?
- 我们如何实现?
- 我们是否实现?
- 我们如何保持前进的动力?

图 8.1 总结了 COBIT 实施方法。

图 8.1—COBIT 实施路线图



8.2.1 第 1 阶段 — 有哪些驱动因素?

实施方法的第 1 阶段识别当前变更驱动因素，促使执行管理层产生变革愿望，然后通过业务案例概述来表达。变更驱动因素属于内部或外部事件、状况或关键问题，充当变更刺激因素。事件、趋势（行业、市场或技术）、绩效下降、软件实施甚至企业目标都可以充当变更驱动因素。

与计划实施本身有关的风险将在业务案例中说明并在整个生命周期中进行管理。准备、维护和监控业务案例是评判、支持以及确保任何举措（包括治理系统的改进）成功的重要课题。它们确保企业持续关注计划的效益及其实现。

8.2.2 第 2 阶段 — 现在到了什么程度?

第 2 阶段确保 I&T 相关目标与企业战略和风险保持一致，并确定最重要的企业目标、一致性目标和流程的优先次序。*《COBIT® 2019 设计指南》*提供了几项设计因素来协助企业做出选择。

根据选定的企业目标、IT 相关目标和其他设计因素，企业必须确定关键的治理和管理目标以及具备足够能力的支持流程，以确保成功获得所需的结果。管理层需要了解其当前能力以及可能存在的不足。这可以通过对选定流程的现状进行流程能力评估来实现。

8.2.3 第 3 阶段 — 我们想要达到什么目标?

第 3 阶段是设定改进目标，然后进行差距分析来确定潜在解决方案。

有些解决方案将快速带来效益，而有些则是更具挑战性的长期任务。应该优先执行可以轻松实现并可能带来最大效益的项目。长期任务应该分解成容易管理的片段。

8.2.4 第 4 阶段 — 我们需要完成什么行动?

第 4 阶段描述了如何通过定义有合理业务案例支持的项目和实施变更计划，来规划切实可行的解决方案。完善的业务案例有助于确保项目效益得以识别和持续监控。

8.2.5 第 5 阶段 — 我们如何实现?

第 5 阶段通过日常实践来实施提议的解决方案，并建立衡量和监控系统来确保业务一致性得以实现，且绩效得到衡量。

成功离不开员工的参与、意识和沟通；离不开最高管理层的理解和承诺；离不开受影响的业务和 IT 流程所有者的主人翁精神。

8.2.6 第 6 阶段 — 我们是否实现?

第 6 阶段侧重于将改进后的治理和管理实践持续转变为正常业务运营。此阶段还侧重于使用绩效指标和期望的效益来监控改进成果。

8.2.7 第 7 阶段 — 我们如何保持前进的动力?

第 7 阶段回顾举措的总体成功程度，确定进一步的治理或管理要求并强化持续改进的需要。此阶段还确定进一步改进治理系统的各机会的优先级。

计划和项目管理基于最佳实践并在七个阶段的每个阶段设置了检查点，从而确保计划进展不会偏离轨道，业务案例和风险得到持续更新，并根据情况调整下一阶段的计划。假定遵守企业的标准方法。

有关计划和项目管理的进一步指导，还可参阅 COBIT 管理目标“BAI01 *妥善管理的计划*”和“BAI11 *妥善管理的项目*”。虽然任何阶段都未明确提及报告，但它应该持续贯穿所有的阶段和迭代。

8.3 《COBIT® 2019 设计指南》与《COBIT® 2019 实施指南》之间的关系

《COBIT® 2019 设计指南》中阐述的工作流程与《COBIT® 2019 实施指南》存在以下关联点。《COBIT® 2019 设计指南》详细说明了《COBIT® 2019 实施指南》中定义的一组任务。**图 8.2** 高度概括了这些关联点。更多详细信息，请参阅《COBIT® 2019 设计指南》。

图 8.2—COBIT 设计指南与 COBIT 实施指南的关联点

COBIT 实施指南		COBIT 设计指南
第 1 阶段 – 有哪些驱动因素？（持续改进 [CI] 任务）	→	**第 1 步** – 了解企业环境和战略。
第 2 阶段 – 现在到了什么程度？（CI 任务）	→	**第 2 步** – 确定治理系统的初步范围。 **第 3 步** – 完善治理系统的范围。 **第 4 步** – 最终确定治理系统的设计。
第 3 阶段 – 我们想要达到什么目标？（CI 任务）	→	**第 4 步** – 最终确定治理系统的设计。

第九章
开始实施 COBIT：制作案例

9.1 业务案例

准备业务案例以分析和证明启动大型项目和/或财务投资的合理性，是一种常见的业务实践。以下示例作为非规定性的一般指导，鼓励企业准备业务案例，以证明投资 EGIT 实施计划的合理性。每个企业都有各自改进 EGIT 的理由以及准备业务案例的方法，包括注重量化效益的详细方法和更概要性的定性方法。企业应遵循现有的内部业务案例和投资论证方法（如有）。本书之所以提供这个例子和指导意见，旨在帮助企业聚焦于进行业务案例分析时要考虑的事项。

在示范的情景中，Acme Corporation 是一家大型跨国企业，既有建制完善的传统业务，又有采用最新技术的基于互联网的新业务。很多业务部门是通过并购获取的，位于政治、文化和经济环境都各不相同的多个国家/地区。中央集团的执行管理层受到最新企业治理指南（包括 COBIT）的影响，这些指南已经集中使用了一段时间。他们想确保迅速扩张和采用先进 IT 的做法能够实现预期的价值，此外还希望管理新的重大风险。因此，他们要求在整个企业内统一推行 EGIT 方法。该方法需要审计和风险职能部门的参与，并要求业务部门管理层针对所有实体的控制充分性进行内部年度报告。

虽然这个例子来源于真实情景，但并非反映某个具体的真实存在的企业。

9.2 执行摘要

这个业务案例概述了向 Acme Corporation 提议的基于 COBIT 的 EGIT 计划的范围。

Acme Corporation 需要一个适当的业务案例，确保获得董事会和各业务部门对该举措的支持，以及确定潜在的效益。Acme Corporation 将监控业务案例，以确保实现预期的效益。

对 Acme Corporation 的各个业务实体来说，计划范围是全包括的。必须认识到的是，由于计划资源有限，初步实施 EGIT 计划时，将对所有实体实施某种形式的优先排定。

关注 EGIT 计划成果的利益相关方有很多，包括 Acme Corporation 董事会和各个实体的当地管理层，以及股东和政府机构等外部利益相关方。

在全球范围内实施 EGIT 计划时必须考虑某些巨大的挑战和风险。最具挑战性的一个方面是很多互联网业务的企业家精神特性以及 Acme Corporation 内部的分散或联合业务模型。

要完成 EGIT 计划，需要关注 Acme 流程和 COBIT 中定义的与各个业务部门有关的其他治理系统组件的能力。EGIT 计划的成员将通过引导型专题研讨会的方式，确定各个实体应重点达成的相关和优先治理及管理目标。首先确定的是各个部门的战略和企业目标，以及适用于特定业务部门的 IT 相关的业务风险场景。

EGIT 计划的目标是确保企业拥有合适的治理系统（包括治理架构），以及提高相关 IT 流程的能力级别和充分性，并预期在提高 IT 流程能力的过程中，促进效率和质量的提升，同时相应地降低相关风险。这样一来，各个业务部门都可以实现实际业务效益。

各个业务部门建立能力级别评估流程之后，预计可按常规业务实践继续进行自我评估。

EGIT 计划的交付分为两个不同阶段。第一个阶段是开发阶段，团队将开发和测试可在整个 Acme Corporation 中使用的方法和工具集。第 1 阶段结束时会向集团管理层陈述结果，以获得最终批准。获得最终批准（即业务案例获得批准）之后，将以商定的方式在整个企业中推行 EGIT 计划（即第 2 阶段 — 实施）。

必须注意的是，实施各个业务部门所确定的补救措施不是 EGIT 计划的责任。EGIT 计划只负责统一报告各个部门所提供的进展情况。

EGIT 计划需要应对的最后一个挑战是未来继续以可持续的方式报告结果。这方面需要花费时间，并且需要进行大量的讨论和开发。讨论和开发的结果应有助于改进公司现有的报告机制和计分卡。

针对 EGIT 计划的开发阶段，已制定初步预算。该预算在单独的计划文件中详述。对于项目的第 2 阶段，也会完成详细预算并提交集团管理层审批。

9.3 背景

EGIT 是企业整体治理不可或缺的一部分，侧重于 IT 绩效和管理企业对 IT 的依赖性所造成的风险。

IT 已融入 Acme Corporation 的业务运营当中。对很多业务来说，互联网处于运营的核心位置。因此，EGIT 遵循集团的管理结构，即分散式结构。各个附属机构/业务部门的管理层负责确保实施与 EGIT 相关的适当流程。

各个主要附属公司的管理层每年都需要向董事会领导下的相应风险委员会提交正式书面报告，详细陈述财年期间 EGIT 政策的实施进度。如有重大的例外情况，管理层将在相应风险委员会按计划召开的会议中报告。

董事会将在风险和审计委员会的协助下，确保在企业年度汇总报告的 EGIT 声明中评估、监控、报告和披露了集团的 EGIT 绩效。EGIT 声明将基于从风险、合规性和内部审计团队以及各个主要附属公司的管理层获取的报告，为内部和外部利益相关方提供集团 EGIT 绩效质量的相关和可靠信息。

内部审计服务将向管理层和审计委员会保证 EGIT 的充分性和有效性。

作为风险管理流程的一部分，呈交给相关风险委员会的风险登记表将会报告和讨论 IT 相关业务风险。

9.4 业务挑战

由于 IT 已经普及且技术变化速度极快，需要可靠的框架才能适当地控制整个 IT 环境，避免出现为企业带来不可接受风险的控制缺口。

这样做的目的不是阻碍不同运营部门的 IT 操作，相反，是为了以商业上合理的方式改进部门的风险概况，提高服务质量和效率，同时明确遵循 Acme Corporation 集团的 EGIT 章程以及其他法律、法规和/或合同要求。

可能遇到的痛点包括：[25]

- 很多业务部门的企业性质使 IT 鉴证工作变得复杂
- 现有的基于互联网服务的业务模型使 IT 运营模式变得复杂

[25] 列举的示例摘自第 4.5 节（设计因素），*《COBIT® 2019 实施指南》*中也有相关讨论。

- 地理位置分散的实体涉及多种文化和语言
- 集团采用了分散/联合且大体自治的业务控制模式
- IT 员工技术性高但有时不稳定，因此必须实施合理的 IT 管理水平
- IT 正在平衡企业对创新能力和业务敏捷性的期望与管理风险和实施充分控制的需求
- 各个业务部门的风险和容忍度设定
- 关注法规（隐私）和合同（支付卡行业 [PCI]）合规性的需求日益增长
- 关于 IT 控制欠佳、IT 服务质量相关的问题等的定期审计发现
- 在竞争激烈的市场中成功、及时地提供新的创新服务

9.4.1 差距分析和目标

目前还没有覆盖整个集团的方法或框架能够实施 EGIT 或运用 IT 良好实践和标准。各个当地业务部门采用 EGIT 良好实践的程度参差不齐。因此，对 IT 流程能力级别的关注通常很少。根据经验，这些能力级别通常较低。

因此，EGIT 计划的目标是以优先的方式提高各个业务部门中相应的 IT 相关流程和控制的能力级别和充分性。

预期成果是识别和阐述重大风险，管理层能够应对风险并报告其状态。随着各个业务部门能力级别的提高，质量和效率应该也能得到相应地改善，同时降低 IT 相关的业务风险。

最终，有效的 EGIT 能够提高业务价值。[26]

9.4.2 考虑的替代方案

IT 框架有很多，目的都是对 IT 的某个方面实施控制。COBIT 框架被众多组织视为世界领先的 EGIT 和控制框架。Acme Corporation 的部分下属公司已经实施了这个框架。

Acme 选择 COBIT 作为实施 EGIT 的首选框架，因此，所有附属公司都应采用这个框架。

没有必要实施完整的 COBIT；只需要实施与特定附属公司或业务部门相关的领域；需要考虑的因素如下：

1. 各个实体在业务生命周期中的发展阶段
2. 各个实体的业务目标
3. IT 对业务部门的重要性
4. 各个实体所面临的 IT 相关业务风险
5. 法律与合同要求
6. 其他相关理由

如果特定附属公司或业务部门已经实施或计划未来实施其他框架，为方便报告、审计和理清内部控制，此类实施应与 COBIT 相对应。

[26] 有实证研究可支持这一断言，请参阅 De Haes、Joshi 和 van Grembergen 的*前述著作*。

9.5 提议的解决方案

EGIT 计划的规划分为两个不同阶段。

9.5.1 第 1 阶段：前期规划

EGIT 计划的第 1 阶段是开发阶段。在这一阶段应采取以下步骤：

1. 最终确定利益相关方和项目参与者在核心团队的构成。
2. 核心团队完成 COBIT 基础培训。
3. 与核心团队开展研讨会，确定适用于集团的方法。
4. 在 Acme Corporation 内部创建在线社区，作为分享知识的仓库。
5. 识别所有利益相关方及其需求。
6. 如果需要，阐明和调整现有的委员会结构、角色和职责、决策规则以及汇报安排。
7. 制定和维护针对 EGIT 计划的业务案例，作为成功实施计划的基础。
8. 制定在整个计划期间沟通指导原则、政策和预期效益的沟通计划。
9. 开发在计划的生命周期内和之后使用的评估和报告工具。
10. 在一个当地实体测试方法。这项活动是为了方便后勤工作以及推动方法和工具的优化。
11. 在一个国外实体试行优化过的方法。目的是了解和量化在更有挑战性的业务环境下运行 EGIT 计划评估阶段的难点。
12. 向 Acme Corporation 执行管理层陈述最终的业务案例和方法，包括推行计划，以获得他们的批准。

9.5.2 第 2 阶段：计划实施

EGIT 计划旨在通过以下步骤，基于简化的迭代式生命周期，启动一项长期的持续改进计划：

1. 从 Acme Corporation 集团和业务部门的角度出发确定 EGIT 改进的驱动因素。
2. 确定 EGIT 现状。
3. 确定 EGIT 的理想状态（短期和长期）。
4. 确定在业务部门级别为实现当地业务目标应实施的事项，从而与集团期望保持一致。
5. 在当地业务部门实施识别和商定的改进项目。
6. 实现和监控效益。
7. 通过保持前进的动力维持新的工作方式。

9.5.3 计划范围

EGIT 计划将涵盖：

1. 所有集团实体。由于计划资源有限，应对这些实体进行优先排序。
2. 确定优先级的方法。需要与 Acme Corporation 管理层达成共识，也可以基于以下因素来决定：
   a. 投资规模
   b. 收益/对集团的贡献
   c. 集团角度的风险概况
   d. 综合上述标准
3. 当前财年期间将要涉及的实体名单。应与 Acme Corporation 管理层协商并最终确定此名单。

9.5.4 计划方法和调整

为实现其目标，EGIT 计划采用的方法是与所有实体开展引导型的互动式研讨会。

这种方法从业务目标和目标负责人（通常是 CEO 和 CFO）开始，应确保计划成果与预期的业务成果和优先级保持高度一致。

确定业务目标后，将焦点转移到通常由首席技术官 (CTO) 或首席信息官 (CIO) 控制的 IT 运营。在 IT 运营层面，考虑 IT 相关业务风险和目标的更多详细信息。

之后，业务目标、IT 目标以及 IT 相关业务风险将整合到一个工具中（基于 COBIT 指南），该工具可提供 COBIT 流程中的一系列焦点领域，以供业务部门考虑。通过这种方式，业务部门将能够确定补救措施的优先顺序，以解决 IT 风险领域。

9.5.5 计划交付成果

如前所述，EGIT 计划的总体目标是将 EGIT 良好实践融入各个集团实体的持续运营中。

EGIT 计划将产生具体成果，以支持 Acme Corporation 衡量预期成果的交付情况。这些成果包括：

1. EGIT 计划将通过内网平台协调内部知识分享，并利用现有的供应商关系为各个业务部门带来利益。
2. 将通过 EGIT 计划评估工具，针对业务部门的每次协调创建详细报告。报告将包含：
   a. 基于 COBIT 的当前优先业务目标和相关的 IT 目标
   b. 业务部门通过标准化形式识别的 IT 相关风险；基于 COBIT 流程和实务以及其他建议组件商定的需要业务部门关注的焦点领域
3. 将创建总进度报告，阐述 EGIT 计划预期覆盖的 Acme Corporation 业务部门。
4. 集团汇总报告将涵盖：
   a. 业务部门参与其商定的实施项目的进度（基于对商定的性能指标的监控）
   b. 所有 Acme Corporation 实体的综合 IT 风险概况
   c. 风险委员会的具体要求

5. 将生成关于计划预算与实际支出的财务报告。
6. 将参照业务部门定义的价值目标和指标建立效益监控和报告。

9.5.6 计划风险

以下是在计划中考虑的可能影响 Acme Corporation EGIT 计划的成功启动和持续开展的潜在风险类型。风险将通过关注变更推行来缓解，并通过计划审查和风险登记进行持续监控和化解。这些风险类型是：

1. 集团和当地业务部门的管理层对计划的承诺和支持
2. 向各个当地实体证明通过采用计划实现的实际价值和效益。当地实体应该是为了流程所创造的价值而实施流程，而不仅是因为政策要求。
3. 当地管理层积极参与计划的实施
4. 确定各个实体中应参与计划的关键利益相关方
5. IT 管理层的业务洞察
6. 与集团内现有的任何治理或合规性举措的成功整合
7. 由合适的委员会架构来监督计划。例如，可将整个 EGIT 计划的进展列入 IT 执行委员会的议程项目。此外还需在当地建立对等的架构。可以在地理位置层面复制这种架构，适当时还可以在地方控股公司层面复制这种架构。

9.5.7 利益相关方

以下是已确定的 EGIT 计划成果的利益相关方：

1. 风险委员会
2. IT 执行委员会
3. 治理团队
4. 合规人员
5. 地区管理层
6. 当地实体的执行管理层（包括 IT 管理层）
7. 内部审计服务

与集团管理层协商后，将整理和发布包含利益相关方具体人员的最终架构。

确定的利益相关方应向 EGIT 计划提供：

1. 关于 EGIT 计划总体方向的指导意见，包括对重大的治理相关主题（根据 COBIT 指南在集团 RACI 表中定义）的决策。此外还包括设定优先级、商定资金筹措以及批准价值目标。
2. 验收交付成果并监督 EGIT 计划的预期效益

9.5.8 成本效益分析

计划应确定预期效益并进行监控，以确保投资可以带来实际业务价值。地方管理层应激励和维护计划运行。将合理的 EGIT 应产生的效益设为每个业务部门的具体目标，并在实施过程中进行监控和衡量，以确保实现效益。这些效益包括：

1. 通过 IT 最大限度地实现业务机会，同时将 IT 相关业务风险降至可接受的水平，从而确保以负责任的方式对所有业务举措中的机会进行风险权衡
2. 通过关键投资和这些投资的优化回报来支持业务目标，使 IT 举措和目标与业务战略保持一致
3. 遵守法律、法规和合同要求以及内部政策和程序
4. 采用一致的方法来衡量和监控进度、效率和有效性
5. 提高服务交付的质量
6. 在更短的时间内以更少的资源持续完成更多工作，从而降低 IT 运营成本和/或提高 IT 生产力

主要成本包括集团计划管理所需的时间、外部咨询资源和初始培训课程。已预估第 1 阶段的这些主要成本。单独的业务部门管理层和流程所有者的评估研讨会费用（出勤、场地、引导员和其他相关费用）将由当地承担并提供估算。将在第 2 阶段估算每个业务部门的具体项目改进举措，并根据具体情况和总体情况进行斟酌，这将支持集团最大限度地提高效率和标准化。

9.5.9 挑战和成功因素

图 9.1 总结了计划实施期间可能影响 EGIT 计划的挑战以及为确保成功实施而应解决的关键成功因素。

图 9.1—Acme Corporation 的挑战和计划行动

挑战	关键成功因素 – 计划的行动
无法获得和维持对改进目标的支持	• 通过集团内的委员会架构（待商定和组建）加以缓解。
IT 与业务之间的沟通隔阂	• 让所有利益相关方参与。
改进成本超过感受到的效益	• 专注于效益识别。
IT 与企业之间缺乏信任和良好关系	• 促进公开、透明的绩效沟通，并与企业绩效管理联系起来。 • 专注于业务接口和服务理念。 • 发布积极成果和经验教训，帮助建立和维护信誉。 • 确保 CIO 在建立信任和关系方面维持公信力和领导力。 • 规范企业中的治理角色和职责，从而明确决策责任。 • 确定和沟通关于实质问题的证据、需要规避的风险，以及待实现的与改进提议有关的效益（用业务语言）。 • 专注于变革推行的规划。
负责 EGIT 计划的人员对 Acme 的环境缺乏了解	• 采用一致的评估方法。
不同的复杂程度（技术、组织、运营模式）	• 考虑各个实体的具体情况。从经验教训和知识分享中获益。
了解 EGIT 框架、程序和实践	• 培训和指导。
抗拒变革	• 确保生命周期的实施还包括变更推行活动。
采纳改进方案	• 启用实体层级的当地授权。
EGIT 与外包合作伙伴的治理模型整合中的困难	• 让供应商/第三方参与 EGIT 活动。 • 将条件和审计权纳入合同中。
未能实现 EGIT 实施承诺	• 管理期望。 • 保持简单、切实可行的期望。 • 将总体项目分解为多个可实现的小项目，积累经验和效益。
同时进行太多的工作；IT 处理的问题过于复杂和/或困难	• 运用计划和项目管理原则。 • 使用里程碑。 • 优先考虑符合 80/20 法则（20% 的投入带来 80% 的效益）的任务，并注意按正确顺序进行。利用速效方案。 • 建立信任/信心。具备足够的技能和经验，使工作简单可行。 • 重复运用基本实践。
IT 处于“救火”模式和/或缺乏有效的优先考虑，无法专注于 EGIT	• 运用良好的领导技能。 • 获得最高管理层的承诺和支持，使相关人员专注于 EGIT。 • 解决运营环境中的根本原因（外部干预、管理层优先处理 IT）。 • 实施更严格的业务请求纪律/管理。 • 获得外部协助。

缺乏必要的 IT 技能和能力，例如对业务、流程和软技能缺乏了解	• 专注于变更推行的规划：
	  ■ 开发
	  ■ 培训
	  ■ 指导
	  ■ 辅导
	  ■ 反馈到招聘流程
	  ■ 交叉培训

未采纳或应用的改进	• 根据商定的原则对当地实体采取因地制宜的方法。该方法必须切实可行。
难以展示或证明的效益	• 确定绩效指标。
失去兴趣和动力	• 建立集团层面的承诺，包括沟通。

第十章
COBIT 和其他标准

10.1 指导原则

COBIT® 2019 开发过程所遵循的指导原则之一是维护 COBIT 作为总括性框架的定位。这意味着 COBIT 继续与多种相关标准、框架和/或法规保持一致。

在此背景下，一致性表示 COBIT 与相关标准中的任何指导都不冲突。同时，需要指出的是，COBIT 不会复制这些相关标准的内容。相反，它通常提供等效的陈述或相关指南的参考。

10.2 参考标准清单

COBIT® 2019 开发过程中使用的标准和指南包括：

- CIS® 互联网安全中心®，*The CIS Critical Security Controls for Effective Cyber Defense*，第 6.1 版，2016 年 8 月
- 云标准和良好实践：
  - Amazon Web Services (AWS®)
  - *Security Considerations for Cloud Computing*，ISACA
  - *Controls and Assurance in the Cloud: Using COBIT® 5*，ISACA
- CMMI® 网络安全平台，2018 年
- CMMI® 数据管理成熟度 (DMM)℠ 模型，2014 年
- CMMI® Development V2.0，CMMI Institute，美国，2018 年
- 发起组织委员会 (COSO) 企业风险管理 (ERM) 框架，2017 年 6 月
- 欧洲标准化委员会 (CEN)，*e-Competence Framework (e-CF) - A common European Framework for ICT Professionals in all industry sectors - Part 1: Framework*，EN 16234-1:2016
- HITRUST® 通用安全框架，第 9 版，2017 年 9 月
- 信息安全论坛 (ISF)，*The Standard of Good Practice for Information Security 2016*
- 国际标准化组织/国际电工技术委员会 (ISO/IEC) 标准
  - ISO/IEC 20000-1:2011(E)
  - ISO/IEC 27001:2013/Cor.2:2015(E)
  - ISO/IEC 27002:2013/Cor.2:2015(E)
  - ISO/IEC 27004:2016(E)
  - ISO/IEC 27005:2011(E)
  - ISO/IEC 38500:2015(E)
  - ISO/IEC 38502:2017(E)
- 信息技术基础架构库 (ITIL®) 第 3 版，2011 年
- 内部审计师学会® (IIA®)，“Core Principles for the Professional Practice of Internal Auditing”

- *King IV Report on Corporate Governance*™，2016 年
- 美国国家标准与技术研究所 (NIST) 标准：
  - *Framework for Improving Critical Infrastructure Cybersecurity*，第 1.1 版，2018 年 4 月
  - 特别出版物 800-37，修订版 2（草稿），2018 年 5 月
  - 特别出版物 800-53，修订版 5（草稿），2017 年 8 月
- “Options for Transforming the IT Function Using Bimodal IT”，*MIS Quarterly Executive*（白皮书）
- *A Guide to the Project Management Book of Knowledge: PMBOK® Guide，第 6 版*，2017 年
- PROSCI® 3-Phase Change Management Process
- Scaled Agile Framework for Lean Enterprises (SAFe®)
- Skills Framework for the Information Age (SFIA®)，第 6 版，2015 年
- The Open Group IT4IT™ Reference Architecture，第 2.0 版
- The Open Group Standard TOGAF®，第 9.2 版，2018 年
- The TBM Taxonomy，TBM 委员会