COBIT® 2019

实施指南

信息和技术治理解决方案的实施和优化

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

ISACA 设计编写了《*COBIT® 2019 实施指南：信息和技术治理解决方案的实施和优化*》（下称“本出版物”），主要供企业信息和技术治理 (EGIT)、鉴证、风险和安全专业人员作为学习资料使用。ISACA 不保证使用本出版物一定能够实现成功的结果。本出版物不应被视为包含所有适用的信息、程序和测试，不排除在其它信息、程序和测试的合理指导下获得同样结果的可能。在确定具体信息、程序或测试适用性时，企业信息和技术治理 (EGIT)、鉴证、风险及安全专业人员应就特定的系统或信息技术环境等具体的情况作出专业判断。

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 实施指南：信息和技术治理解决方案的实施和优化
ISBN 978-1-60420-786-6

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，并以本作品的问世为他的职业生涯画上圆满的句号。在 ISACA 的四十年间，John 参与了协会多方面的工作，并获得 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

Floris Ampe，CISA，CRISC，CGEIT，CIA，ISO27000，PRINCE2，TOGAF，PwC，比利时
Graciela Braga，CGEIT，审计师和顾问，阿根廷
James L. Golden，Golden Consulting Associates，美国
J. Winston Hayden，CISA，CRISC，CISM，CGEIT，南非
Abdul Rafeq，CISA，CGEIT，FCA，Wincer Infotech Limited 常务董事，印度
Jo Stewart-Rattray，CISA，CRISC，CISM，CGEIT，FACS CP，BRM Holdich，澳大利亚

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，CRISC，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。

本页特意留白

目录

图表列表

第一章. 引言

第二章. 企业 I&T 治理的定位

第三章. 迈向 EGIT 的第一步

第四章. 识别挑战和成功因素

第五章. 推行变革

第六章. 实施生命周期

附录 A. 决策矩阵示例

第一章
引言

1.1 企业信息和技术治理的改进

从数字转型来看，信息和技术 (I&T)[1] 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。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，创造了利益相关方的价值（即在优化风险的同时以最佳资源成本实现效益）。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) 受到日益广泛的关注。EGIT 是企业治理不可或缺的一部分。董事会执行 EGIT 并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 赋能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*，第 2 版，Springer International Publishing，瑞士，2015 年，*https://www.springer.com/us/book/9783319145464*

为推动国际化思维并为评估、指导和监控企业 I&T 的使用提供指引，ISACA® 在企业治理这一关键领域已耕耘多年。ISACA 开发了 COBIT® 框架来帮助企业实施健全的治理和管理。实际上，缺乏有效的治理框架几乎不可能实施良好的 EGIT。

有效的 EGIT 既能改善业务绩效，也能满足外部要求。但如何成功实施 EGIT 仍然困扰着许多企业。EGIT 非常复杂，涉及多个方面的工作。在组织内设计、实施和维护有效的 EGIT 是没有捷径可言的。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实施 EGIT 措施。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] 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。

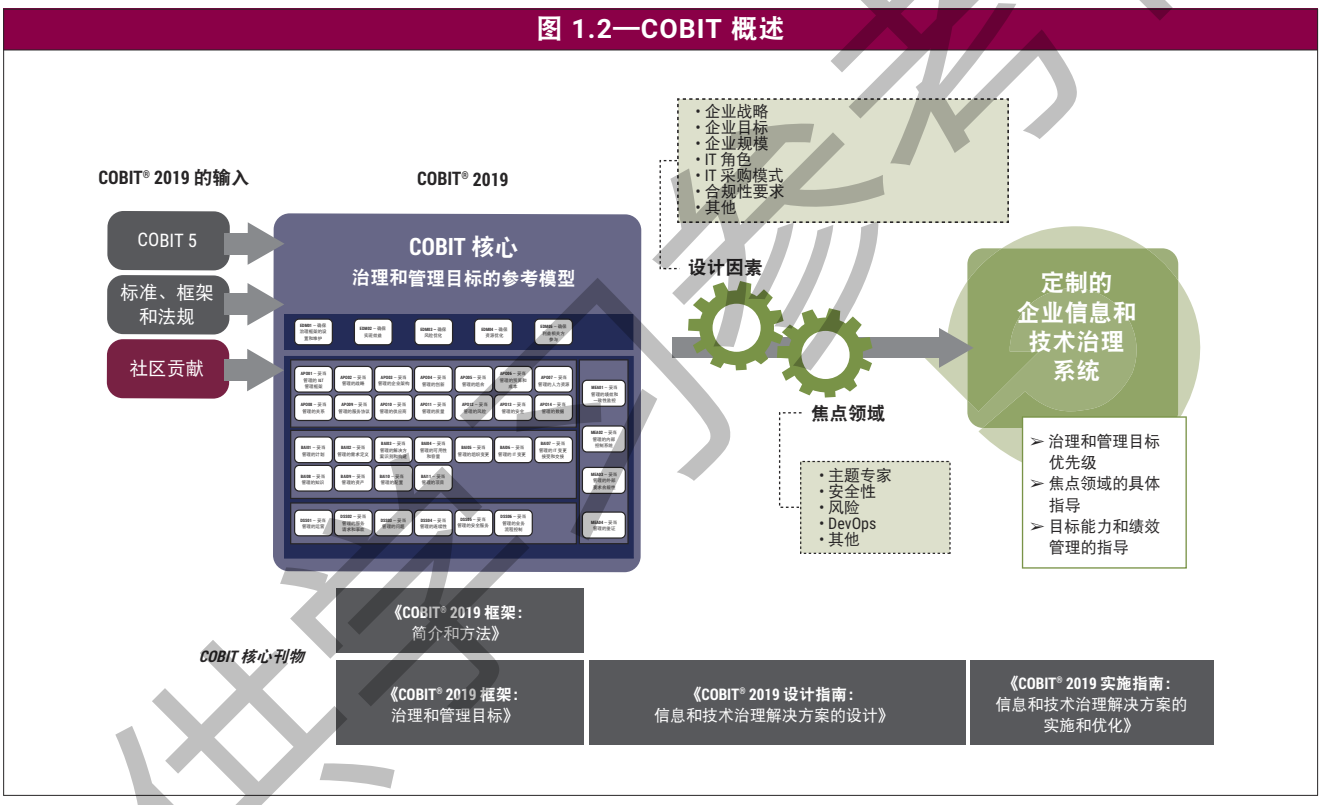
1.2 COBIT 概述

*《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® 2019 系列的第四本出版物（请参阅**图 1.2**）。部分其他出版物如下。

- ***《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。

本参考指南旨在通过运用针对企业具体需求而量身定制的持续改进生命周期方法，提供实施和优化 I&T 治理系统的良好实践。

图 1.2—COBIT 概述



1.3 本出版物的目标和范围

COBIT 原则上强调从整个企业角度来审视 I&T 治理（请参阅*《COBIT® 2019 框架：简介和方法》*）。信息和技术不局限于 IT 部门内，也渗透到企业的每个角落。要将业务与 I&T 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。

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，因而无法确保实现效益。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，采用计划和项目的方法不仅仅是为了有效地推动改进举措，也是为了同企业治理的其他方面一样，建立常规的业务实践和可持续的方法来治理和管理企业 I&T。因此，实施方法的基础是通过促进和推动变革，授权业务和 IT 利益相关方及角色来负责 IT 有关的治理和管理决策及活动。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时，实施计划将会关闭，并被纳入持续进行的业务活动中。

本出版物不是一个规范性方法或完整的解决方案，而是提供一个避免隐患、运用最新良好实践的指南，并协助取得成功的长期治理和管理结果。本出版物在很大程度上借鉴了*《COBIT® 2019 设计指南》*，该指南旨在帮助企业根据自身战略、风险和威胁问题以及 IT 角色等设计因素，确定实施具体计划或路线图。

确定当前起点也同样重要。目前大多数企业仍未意识到它们几乎都实施了 EGIT 结构或流程。因此，必须将重点放在优化完善企业已实施的结构和流程上，尤其是要利用好现有已取得成功的企业级方法而非另起炉灶。可直接采用或在必要时加以调整这些现有的方法以用于 I&T治理。此外，无需重新对运用 COBIT® 5 或其他标准和良好实践创建的之前的改进进行处理。相反，这些改进应该运用 COBIT® 2019 进行强化，并作为持续改进的一部分。

COBIT® 2019 可从 *www.isaca.org/cobit* 免费下载。此页面还包括可为实施提供支持的 ISACA 产品链接。

本出版物反映了对实施EGIT的深入理解和实践经验、在运用和使用以前版本的 COBIT 时汲取的经验教训，以及对 ISACA 指南的改进。但 I&T 绝不会停滞不前，因此本指南的用户应该留意为应对新兴主题而持续更新的ISACA 专业出版物及其他组织的标准和良好实践。即将出现的全新焦点领域内容将成为 COBIT 产品系列的一部分，并为这些新兴主题提供重要指引。[2]

1.4 本出版物的结构

本出版物的其余部分包含以下章节和附录：

- 第 2 章说明 EGIT 在企业中的定位。
- 第 3 章探讨改进 EGIT 的早期步骤。
- 第 4 章说明实施挑战和成功的因素。
- 第 5 章介绍 EGIT 的相关组织和行为变革。
- 第 6 章描述实施的生命周期，包括变革推行和计划管理。
- 附录提供了决策矩阵示例。

[2] 在*《COBIT® 2019 实施指南》*发布之时，焦点领域内容已计划好，但尚未发布。

1.5 本出版物的目标受众

本出版物的目标受众是企业内经验丰富的专业人士，包括业务部门、审计、安全、隐私、风险管理、IT 专业人员、外部专家以及其他已参与（或计划参与）EGIT 实施的人员。

要从本指南中获益，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定制具有通用性的核心 COBIT 指南，将其转变为有针对性的企业操作手册。

1.6 相关指南：《COBIT® 2019 设计指南》

*《COBIT® 2019 设计指南》*与本出版物有关。该指南阐述可能影响治理系统的设计因素，并包括为企业设计定制的治理系统的工作流程。*《COBIT® 2019 设计指南》*中介绍的工作流程与*《COBIT® 2019 实施指南》*有多个关联点；设计指南详细说明了本实施指南中定义的一组任务。

*《COBIT® 2019 设计指南》*的第 5 章探讨了两本出版物之间的联系，并阐明应如何将两者结合使用。

第二章
企业 I&T 治理的定位

2.1 了解背景

企业信息和技术治理 (EGIT) 不会凭空出现。开展实施所需不同条件和状况取决于内部和外部环境中的众多因素，例如：

- 社区道德和文化
- 适用的法律、法规和政策
- 国际标准
- 行业惯例
- 经济和竞争环境
- 技术进步和发展
- 威胁环境
- 企业的：
  - 存在原因、使命、愿景、目标和价值观
  - 治理政策与实践
  - 文化和管理风格
  - 角色与职责模型
  - 业务计划和战略意图
  - 运营模式和成熟度

因此，每个企业的 EGIT 实施都会有所不同，我们需要了解和考虑相应的背景，才能设计全新或改进的最佳 EGIT 环境。*《COBIT® 2019 设计指南》*中详细阐述了这一主题。

2.1.1 什么是 EGIT?

治理、企业治理和 EGIT 这些术语可能具有不同的含义，具体取决于组织背景（成熟度、行业和监管环境）、个体背景（工作角色、教育和经验）以及其他多种因素。本章所述内容为本指南的其余部分奠定了基础，但需要认识到，仍存在不同的观点。相较于专为 I&T 开发一种新方法，基于现有方法进行扩充和强化以纳入 I&T，才是更好的做法。

治理一词来自希腊语的动词 kubernáo，意思是“引导”。治理系统能使企业中的多个利益相关方在评估条件和选项、设定方向以及对照企业目标监控绩效方面拥有合理的发言权。董事会或类似机构应负责建立并维护适当的治理方法。

COBIT 对治理的定义如下：

> *治理旨在确保评估利益相关方的需求、条件和选择，以确定要实现的平衡且协商一致的企业目标；通过设定优先顺序和制定决策来确立方向；并根据商定的方向和目标监控绩效和合规性。*[3]

[3] 请参阅*《COBIT® 2019 框架：简介和方法》*第 1.3 节。

EGIT 不是孤立的规范，而是企业治理不可或缺的一部分。企业级治理需求的主要驱动因素是利益相关方价值的实现、企业风险的透明度和有效管理的需求。与 I&T 相关的重大机遇、成本和风险要求企业集中精力，全方位关注 EGIT。通过 EGIT，企业能够充分利用 I&T，从而实现效益最大化、有效利用机遇并获得竞争优势。

2.1.2 EGIT 为何如此重要?

全球企业，无论是上市公司还是私营企业，也无论其规模大小，都逐渐认识到，信息是一种关键资源，而技术是一种战略资产，两者对取得成功至关重要。

I&T 可成为一种强大的资源，帮助企业实现其最重要的目标。例如，I&T 能为合并、收购和剥离等大型交易节省成本。I&T 能够实现关键流程（如供应链）的自动化。I&T 能够成为新的业务战略或业务模式的基石，从而提高竞争力并实现数字产品交付（如在线出售和交付音乐）等创新举措。I&T 能够提高与客户的亲密度，例如，通过收集和挖掘不同系统中的数据并提供全方位的客户视角来实现此目的。I&T 是网络经济的基础，它能穿越地理位置和组织孤岛，提供全新和富有创意的价值创造方法。大多数企业都认识到信息和 I&T 的使用需要作为关键资产进行妥善管理。

虽然 I&T 具有推动业务转型的潜力，但往往同时代表了一笔非常重大的投资。在很多情况下，真实的 IT 成本并不透明，并且预算分散在各业务单位、职能部门和不同地理位置，未实现集中监督。最大的支出部分通常用于为实施后的维护和运营提供资金，而非用于创新或转型。在将资金用于战略举措时，往往无法实现预期成果。许多企业仍未展示 IT 赋能的投资所带来的具体、可衡量的业务价值，也未将 EGIT 视作解决这种状况的机制。

网络经济带来了一系列的 IT 相关风险，包括面向客户的业务系统遭到侵害、客户或专有数据发生泄露，或因 IT 架构不够灵活而错失商机。管理这些风险和其他 I&T 相关类型的风险是改善 EGIT 的另一驱动因素。

EGIT 能够应对当今许多行业和司法管辖区的企业所面临的复杂监管环境（通常与 IT 领域直接相关）。财务报告的相关要求和审查也促使企业重点关注 IT 相关的控制。一些国家和行业现已强制要求企业采用 COBIT 等良好实践。例如，土耳其银行监理署（BRSA）已发布规定，在土耳其境内运营的银行在开展 IT 相关管理流程时，应采用 COBIT 的良好实践，澳大利亚审慎监管局也有类似要求。南非的公司治理报告—《金氏报告》（第四版）—包含了实施 EGIT 的原则，并推荐采用 COBIT 等框架。I&T 治理框架能够以更有效和更高效的方式来促进合规。

相关研究早已证实 EGIT 的价值。某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“价值取向”的转变。[4]

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

研究表明，企业在设计或采用 EGIT 上采用了不恰当方法，那么在推动业务与 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转型取得预期的业务价值便没有多少胜算。[5]

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。

2.1.3 EGIT 应实现哪些价值?

从根本上说，EGIT 关注的是数字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，保持和增加现有 I&T[6] 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保持一致。IT 价值的衡量方式还应体现 IT 赋能的投资对企业价值创造流程的影响和促进作用。
- **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，风险管理侧重于保留价值。应将 I&T 相关风险的管理整合到企业风险管理方法中，以确保企业持续关注 IT。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。

在实施和演练 EGIT 的整个过程中，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。

2.2 利用 COBIT 并集成框架、标准和良好实践

COBIT 以企业视图为基础，与企业治理的良好实践保持一致。COBIT 以非技术的语言、通过表述一致的综合指南，提供了一个单一的总体框架。董事会应强制要求采用类似 COBIT 这样的 EGIT 框架，将其作为企业治理发展的重要组成部分。

[5] De Haes, S.；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-itin-organizations.aspx*。另请参阅 De Haes 和 van Grembergen 的前述著作，*Enterprise Governance of IT: Achieving Alignment and Value, Featuring COBIT 5*。

[6] 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。

在框架内工作并利用良好实践，有助于制定和优化相应的治理流程和其他治理系统组件。如果定制得当，EGIT 可作为企业常规业务实践的一部分有效运作，但前提是高级管理层需要以身作则，展现出支持 EGIT 的企业文化。

COBIT® 2019 不仅概述了通用的方法，还参考了其他详细标准。*《COBIT® 2019 框架：简介和方法》*第 10 章列出了与 COBIT® 2019 协调一致的标准；*《COBIT® 2019 框架：治理和管理目标》*的治理和管理目标、其相关实践及组件部分列出了这些标准，并在详细参考资料部分提供了详细阐述。

COBIT 作为 IT 审计程序的基础已被广泛接受，与 COBIT 保持一致还能实施更高效快捷的外部审计。

COBIT 框架载明了总体方法，企业在定制实施的过程中，可将标准和良好实践所提供的指南应用于具体流程、实践、政策和程序。具体而言，治理系统及其组件应与下述各项协调一致：

- 企业政策、战略、治理和业务计划以及审计方法
- 企业风险管理（ERM）框架
- 现有的企业治理组织、结构和流程

2.2.1 治理原则

COBIT® 2019 的开发基于两套原则：

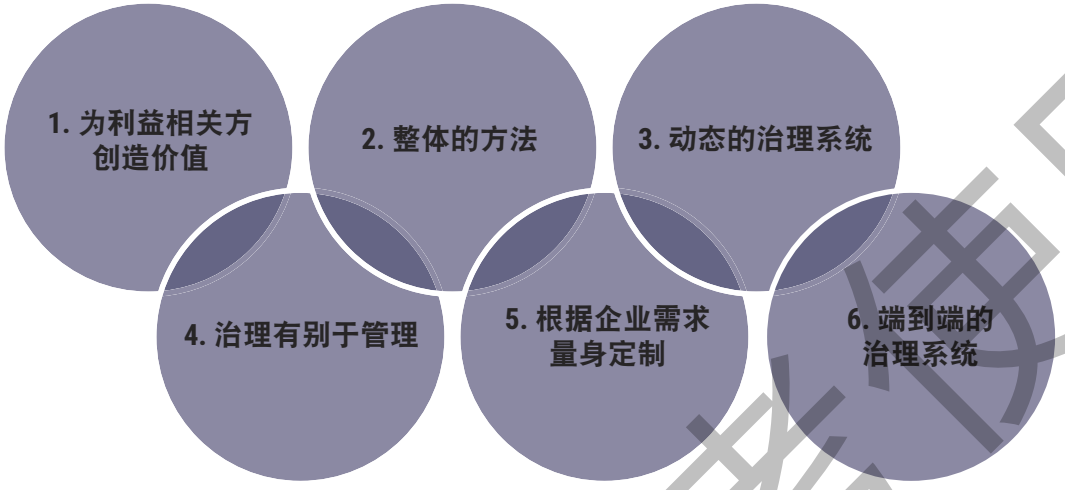
- 描述企业信息和技术**治理系统**核心要求的原则。
- 可用于构建企业治理系统的**治理框架**原则。

治理系统的六大原则（**图 2.1**）是：

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实施的所有技术和信息处理，无论其在企业的哪个位置实施。[7]

[7] 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*

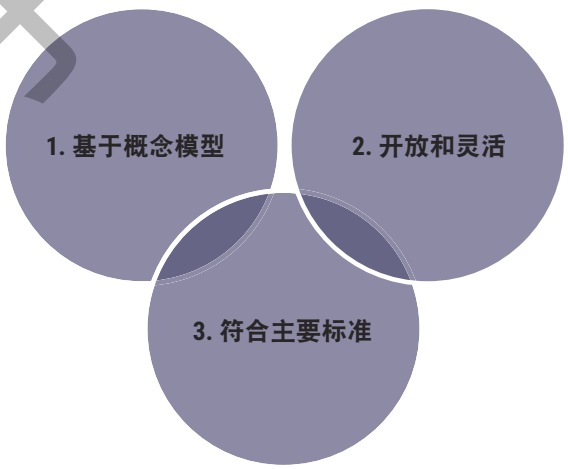
图 2.1—治理系统原则



治理框架的三大原则（**图 2.2**）是：

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 2.2—治理框架原则



2.2.2 治理系统及组件

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。与治理系统有关的基本概念包括：

- 组件可以是不同类型的。最通用的组件是流程，但治理系统的组件也包括组织结构、信息项、技能和能力、文化和行为、政策和程序、服务、基础设施和应用程序，这些也都需要纳入考虑范围。
- 所有类型的组件都可以通用，也可以基于通用组件进行定制。
- COBIT 核心模型（请参阅《*COBIT® 2019 框架：简介和方法*》，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。
- 可基于通用组件，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）进行定制。

2.2.3 治理和管理目标

COBIT 包括治理和管理目标以及基础流程，这些有助于指导如何创建和维护治理系统及其不同组件。就此而言，两个关键的治理和管理目标是：

- EDM01 *确保治理框架的建立和维护*（文化、道德和行为；原则、政策和框架；组织结构；以及流程）
- APO01 *妥当管理的 I&T 管理框架*（文化、道德和行为；原则、政策和框架；组织结构；以及流程）

COBIT 治理和管理目标可确保企业以可重复和可靠的方式组织其 I&T 相关活动。COBIT 核心模型包含五个领域、40 项治理和管理目标以及基础流程，这些共同构成了COBIT 指南的结构，《*COBIT® 2019 框架：治理和管理目标*》对此进行了详细说明。

第三章
迈向 EGIT 的第一步

3.1 创建适当的环境

实施 EGIT 改进时，确保存在适当的环境十分重要。这有助于确保举措受管理层监管并且得到适当指导和支持。很多重要的 I&T 举措经常因为管理层指导、支持和监督不够而失败。EGIT 实施亦无不同；如果它们得到正确的治理和管理，则成功的机会更大。

例如，关键利益相关方的支持和指导不足可能导致 EGIT 举措生成的新政策和程序缺乏正确的所有权或持久的效力。如果没有负责分配角色和责任、承诺连续运营和监控遵循情况的管理结构，改进就不可能变为正常的业务实践。

因此，为确保 EGIT 作为企业内总体治理方法不可分割的一个部分实施，应该营造并维护适当的环境。此外，还应该为实施举措（包括指导原则）提供适当的指导和监督。目的是提供足够的活动承诺、指导和控制，从而与企业目标保持一致，并得到董事会和执行管理层适当支持。

经验表明，EGIT 举措在某些情况下能够识别企业总体治理中存在的重大缺陷。企业治理环境不佳时成功实施 EGIT 格外困难，因此高管的积极支持和参与就变得更加重要了。董事会和高管不仅应该了解公司治理的概念和改善总体治理的需求，还应该意识到不解决缺陷会导致企业面临 EGIT 失败的风险。

不论是实施小规模还是主要举措，执行管理层都必须参与并推动创建合适的治理结构。最初的活动通常包括评估当前实践以及改进后的结构设计。在某些情况下，该举措可能导致重组业务部门和 IT 部门并改变他们之间的关系。

执行管理层应建立并维护治理框架。换言之，他们需要根据商定的治理设计原则、决策模型、权限级别以及做出明智决策所需的信息，来确定 EGIT 的结构、流程和实践。[8]

执行管理层还应明确分配指导 EGIT 改进计划的相关角色和职责。

要规范 EGIT 并为董事会及高管层提供一种机制来监督和指导 I&T 相关的活动，一种常见的方法是组建I&T 治理委员会。[9] 委员会代表董事会行使职权并对其负责。委员会负责确定企业内部 I&T 的使用方式，以及制定会对企业造成影响的关键 I&T 相关决策。该委员会还应拥有明确授权，并且最好由业务高管（理想情况下为董事会成员）担任主席。委员会的成员包括：代表主要业务部门的业务高管、首席信息官（CIO）、首席数字官（CDO）和/或首席技术官（CTO）以及其他 IT 高级经理（如需要）。内部审计、信息安全和风险职能部门应在其中担任顾问角色。

[8] 请参阅附录中的决策矩阵示例。
[9] I&T 治理委员会也可能被称为 IT 指导委员会、IT 委员会、IT 执行委员会或 IT 治理委员会。

高管需要根据事实、可靠信息、以及业务和 IT 经理、审计师、客户、用户和其他人提供的各种有理有据的意见制定决策。COBIT 框架能够为高管提供表述目标、目的和预期结果的通用语言，从而促进此类沟通。

图 3.1 和 **3.2** 描述了主要利益相关方的一般角色，并概述了实施适当环境以维持治理和确保取得成功的责任。下一节还会提供类似的图表来介绍实施生命周期的各个阶段。

图 3.1—在创建适当环境中的各种角色

如果您是……	那么您在创建适当环境中的角色是……
董事会和高管	• 为计划设定方向
	• 确保环境与企业范围的治理和风险管理协调一致 • 批准关键计划角色并定义相关职责 • 给予有形的支持和承诺 • 发起、传达和推动商定的举措
业务管理层	• 提供适当的利益相关方和推动者，以推动承诺并为计划提供支持 • 任命关键计划角色以及定义和分配相关职责
IT 管理层	• 确保业务部门和高管知悉并理解高层级的 I&T 相关问题和目标 • 任命关键计划角色以及定义和分配相关职责 • 与业务部门共同任命计划的执行人员
内部审计	• 就审计参与的相关角色和报告安排达成一致 • 确保审计在整个计划期间的适度参与
风险、合规及法律	• 确保在整个计划期间的适度参与

图 3.2—实施人员的职责

关键活动	实施人员的职责：董事会	I&T 治理委员会	CIO	业务高管	IT 经理	IT 流程所有者	IT 审计	风险与合规性	计划指导
为计划设定方向。	A	R	R	C	C	I	C	C	C
提供计划管理资源。	C	A	R	R	C	C	R	R	I
建立并维护方向，监督结构和流程。	C	A	C	I	I	I	I	I	R
建立并维护计划。	I	A	R	C	C	I	I	I	R
使方法与企业方法协调一致。	I	A	R	C	C	I	C	C	R

RACI 矩阵确定谁是执行人、责任人、咨询人以及知情人。

3.2 应用持续改进生命周期方法

持续改进生命周期方法能够使企业解决 EGIT 实施期间通常会遇到的复杂性和挑战。生命周期有三个相互关联的组件，如**图 3.3** 所示：

1. 核心的 EGIT 持续改进生命周期
2. 变革推行（阐述实施或改进的行为和文化方面）
3. 计划管理

图 3.3 将举措描述为持续生命周期，以强调这些活动并非孤立的、不连续的或一劳永逸。相反，它们会形成持续的实施和改进流程，并最终变为“常规业务”，那时计划即可结束。

图 3.3—应用持续改进生命周期方法

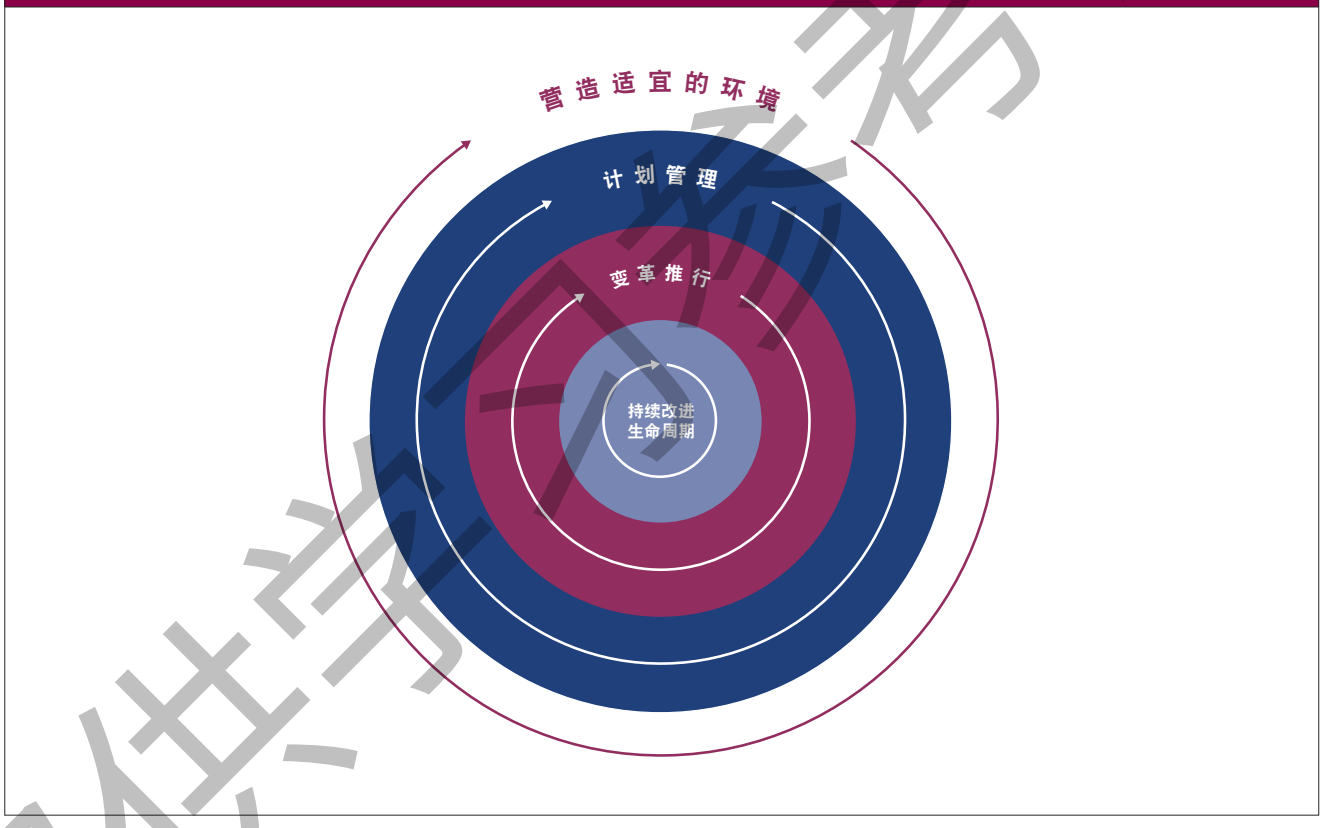
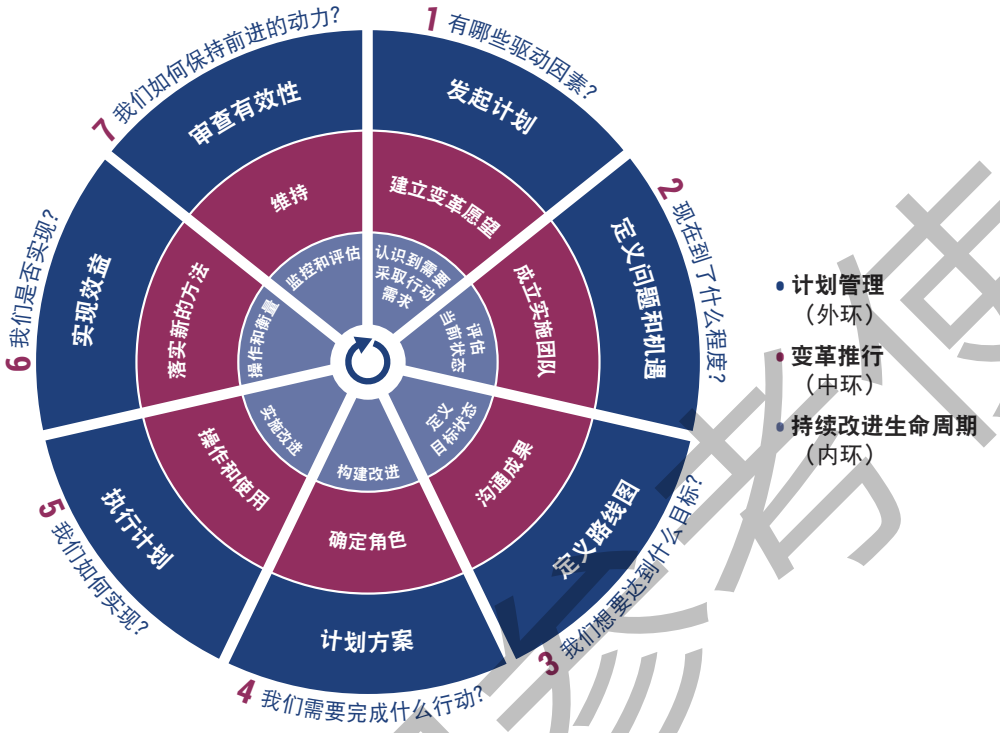


图 3.4 描述了实施路线图的七个阶段。高阶运行状况检查、评估和审计经常会触发对 EGIT 举措的考虑，其结果可成为第 1 阶段的信息依据。实施和改进计划通常需要持续重复进行。在最后一个阶段往往会出现新的目标和要求，并可能启动新的周期。

图 3.4—COBIT 实施路线图



3.2.1 第 1 阶段 — 有哪些驱动因素?

第 1 阶段确定当前变革驱动因素并在执行管理层级别形成变革愿望，然后表述在业务案例概述中。内外部事件、状况或关键问题都可能激发变革。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革驱动因素。

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。

3.2.2 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、一致性目标以及治理和管理目标的优先次序。*《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、一致性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。

3.2.3 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。

3.2.4 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革计划，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确定和持续监控。

3.2.5 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，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。

3.2.6 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。此外还强调了使用绩效指标和期望的效益来监控改进成果。

3.2.7 第 7 阶段 — 我们如何保持前进的动力?

第 7 阶段审查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。此外还确定进一步改进治理系统的优先机会。

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 *妥当管理的计划*”和“BAI11 *妥当管理的项目*”。虽然任何阶段都未明确提及报告，但它应该贯穿所有阶段和迭代。

每个阶段所花的时间大不相同，具体取决于企业环境、其成熟度和实施或改进举措的范围以及其他因素。但在理想情况下，采用逐步改进的方法，整个生命周期的每个迭代所花的总时间不应该超过六个月。否则，计划会面临失去利益相关方动力、关注度和支持的风险。这样做的目的是确定正常改进的节奏。大规模举措应该结构化为多个生命周期迭代。

随着时间的推移，构建可持续方法时，将会迭代执行该生命周期。生命周期阶段成为日常活动；持续改进自然而然地发生，并且变为正常的业务实践。

3.3 启动 — 识别行动需求：识别痛点和触发事件

许多因素可能表明需要新增或修订 EGIT 实践，仔细研究它们还会揭示错综复杂的根本问题。例如，如果业务部门抱有 I&T 成本高得无法接受的观点，这可能缘于治理或管理问题（例如管理 IT 投资时使用的标准不当）。但此痛点也可能是因为过去长期以来在 I&T 方面的投资不足所致，现在表现为成本激增、追加成本或成本居高不下。

使用痛点或触发事件来启动 EGIT 举措，可以将旨在实现改进的业务案例与利益相关方的具体问题相关联，这将有助于提高接受度。在企业内产生紧迫感，对于启动实施而言很有必要。此外，可以在企业最易于见效或获得认可的领域提供速效方案并展现带来的价值增长。反过来，速效方案将为引入进一步的变革提供平台，有助于让广大高级管理层投身其中，并支持范围更广的改进。

3.3.1 典型痛点

新增或修订 EGIT 实践通常可以解决或有助于解决以下现象，在*《COBIT® 2019 设计指南》*的“设计因素 4 *I&T 相关问题*”部分也列出了这些现象。（请注意，此列表并不详尽，并且每个组织都有自己的具体问题需要解决。）

- **由于被认为对业务价值的贡献较低，整个组织内的不同 IT 实体存在隔阂**—越来越多的企业已将 IT 实体分散或分离；每个实体为其利益相关方提供特定（并且通常是不连续的）服务。各群体之间可能存在依赖关系；如果不认真管理这些依赖关系，它们可能会影响 IT 效率和效益。
- **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 部门存在隔阂**—虽然很多企业不断增加在 I&T 方面的投资，但这些投资的价值以及 IT 的总体绩效常常受到质疑或未被完全理解。这种隔阂可能是存在 EGIT 问题的信号，表明 IT 与业务部门之间的沟通需要改善，或需要在 IT 角色和价值方面建立共识。它也可能是组合及项目拟定、提议和批准机制欠佳的结果。
- **重大 I&T 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**—重大事故（包括与 IT 有关的数据丢失、安全漏洞、项目失败和应用程序错误）往往只是冰山一角，如果引起公众或媒体注意，可能造成恶劣影响。进一步调查往往会发现更深层次的结构性错位，甚至是企业内完全没有 IT 风险意识文化。此时，通常需要更强大的 EGIT 实践来全面了解和管理 IT 相关风险。
- **IT 外包商的服务交付问题**—外部服务提供商的服务交付问题（例如始终未能达到商定的服务水平）可能缘于治理问题。例如，缺乏明确定义的第三方服务管理流程（包括控制和监控）或此类流程的按需定制不足，或缺乏履行业务和 IT 服务要求的相关责任和问责制。
- **无法满足 IT 相关法规或合同要求**—在很多企业中，低效或无效的治理机制会导致相关法律、法规和合同条款无法完整集成到组织系统内。另外，也有可能法律、法规和合同条款能够实现集成，但企业仍然缺乏管理它们的方法。（法规和合规要求正在全球范围内不断增加，并且通常会对 IT 赋能的活动造成直接影响。）

- **有关 IT 绩效欠佳的定期审计发现或其他评估报告，亦或报告的 IT 质量或服务问题**—评估欠佳可能表明服务水平落实不到位或运转不佳，或业务部门在 IT 决策方面的参与度不够。
- **重大的隐性和反常 IT 支出**—超出常规 IT 投资决策机制和批准预算的过度支出通常表明缺乏对 IT 支出和投资的充分透明和全面控制。IT 支出可能会隐含或被错分在业务部门预算中，造成 IT 成本的总体视角有失偏颇。
- **多个举措之间的重复或重叠，或其他形式的资源浪费**—当 I&T 举措未在单一全面的组合视角得到充分体现时，可能会导致项目重复和/或部署冗余资源。组合和绩效管理的相关流程和决策结构能力可能未落实到位。
- **IT 资源不足、员工技能欠缺和员工过劳/不满意**—这些属于严重的 IT 人力资源管理问题，需要有效监督和良好治理以确保人员管理和技能培养问题得到有效解决。它们还可能表示 IT 需求管理和内部服务交付存在不足（以及其他潜在问题）。
- **IT 赋能的变革或项目经常出现无法满足业务需求、延期交付或超出预算等痛点问题**—这些可能与业务和 IT 缺乏一致性、业务需求不明确、缺乏实现效益的流程、不理想的实施或项目/计划管理流程欠佳等因素有关。
- **多个复杂的 IT 鉴证措施**—这可能表示在 IT 相关鉴证审核的需求与执行方面，业务与 IT 之间的协同性不足。业务对 IT 缺乏信任，可能会导致业务开展自身审核。还可能表示 IT 鉴证审核缺乏业务问责制或是参与不足导致业务根本不知道何时发生审核。
- **董事会、执行管理层、高级管理层不愿参与 IT，或缺乏全身心投入 IT 的业务发起人**—这些痛点通常意味着对 IT 缺乏业务了解和洞察力，缺少适度的 IT 关注度或无效的管理结构。这也意味着通常由于业务和 IT 之间沟通欠佳、I&T 的业务发起人对业务和 IT 存在误解等因素而可能产生的董事会授权问题。
- **复杂的 IT 运营模式、不明确的 IT 相关决策机制**—分散或联合的 IT 组织通常具有不同的结构、实践和政策。由此产生的复杂性需要高度专注于 EGIT，以确保作出最佳 IT 决策，实现行之有效的运营。此痛点在全球化形势下变得越来越重要，因为每片地域或地区都有特定的、可能是独一无二的内部和外部环境因素需要解决。
- **过高的 IT 成本**—IT 往往被视为组织中应维持在尽可能低水平的成本上。当 IT 预算主要用于对业务没有多大价值的项目和持续运营，而不是带来新机会和创新时，往往会出现此问题。缺乏对所有 I&T 举措的整体组合视角可能会导致成本过高、组合和绩效管理的相关流程及决策结构能力未落实到位。
- **当前 IT 架构和系统导致创新的举措受阻或失败**—在许多组织中，传统的 IT 架构在实施新的创新解决方案上并不具备太多灵活性。数字化通常需要快速行动，敏捷地应对不断变化的环境。它需要更灵活的全新 IT 开发和运营方法，并对治理系统产生直接影响。
- **业务和技术知识之间的差距**—业务用户和 IT 专家经常难以交流。当业务用户对 I&T 缺乏足够的了解，或未能掌握 I&T 改进业务的方法；反过来说，当 IT 专家对业务环境中的挑战和机遇产生误解时，企业便无法实现成长和创新带来的成功。这种情况需要良好治理，确保人员管理和技能培养的问题得到有效解决。

- **各种来源的数据经常出现数据质量和整合方面的问题**—企业逐渐认识到其信息中可能隐含的潜在价值。这些数据质量或整合的问题都会对企业的成功产生重大影响。EGIT 是建立正确流程、角色、责任和文化等且获取信息带来业务价值的关键。
- **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、质量控制等其他问题**—大量的最终用户计算可能会给 IT 与业务之间的沟通形成压力，并可能需授予业务应用程序的安装权限。这可能是组合和项目的拟定、提议和批准机制欠佳所致。EGIT 有助于建立 IT 的角色和价值方面的共识，以加强最终用户设备的安全和功能。
- **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**—此痛点可能关系到最终用户计算问题以及数据和信息的最佳使用方式；但这主要是因为业务部门试图在追求业务优势的正常过程中实施更强大的解决方案和服务。业务和 IT 之间缺乏沟通信任可能导致未经认可的独立开发，或以服务问题等形式加剧这种情况。
- **忽视或违反安全和隐私法规**—企业应该将减少新的安全和隐私威胁纳入议程，这不仅是出于合规性考虑，也是为了保护企业创造的价值。忽视或违反法规会严重损害企业，并且这种现象应通过适当的 EGIT 进行管理。
- **无法利用新技术或使用 I&T 进行创新**—业务认为 IT 应承担支持职能，而企业期望 IT 进行创新并提供竞争优势。这表示业务和 IT 之间可能缺乏真正的双向一致性、反映可能存在沟通问题或需要加强业务在 IT 决策方面的参与度。另外，业务可能太晚让 IT 参与到其战略规划或业务举措中。此问题通常在引入新产品或服务等经济状况下需要企业快速响应时最为明显。

3.3.2 内部和外部环境中的触发事件

除了第 3.3.1 节描述的痛点外，企业的内部和外部环境中的其他事件也会指示或触发对 EGIT 的关注并使其成为企业议程的重要内容。

- **合并、收购或剥离**—这些交易可能导致与 I&T 相关的重大战略和运营结果。尽责调查审查必须了解环境中的 IT 问题。整合或重组要求可能会规定适用于新环境的 EGIT 机制。
- **市场、经济或竞争地位的变化**—经济衰退可能导致企业修改 EGIT 机制以推动大规模的成本优化或绩效改进。
- **业务运营模型或采购安排的变化**—从分散或联合模式转变为集中的运营模式，这将要求变更 EGIT 实践以支持集中化的 IT 决策。在财务、人力资源 (HR) 或采购等领域实施共享服务中心也需要加强 EGIT。可以将碎片化的 IT 应用程序或基础设施领域与监管它们的 IT 决策结构或流程的相关变更进行整合。一些 IT 职能和业务流程的外包也同样会引起对 EGIT 的重新关注。企业决定接受更多风险以实现其目标等风险偏好变化也会影响 EGIT。
- **新的法规或合规要求**—遵守法律法规通常意味着对 EGIT 的影响。例如，公司治理报告要求及财务法规的加强通常会要求完善 EGIT，并关注由于广泛应用 IT 导致的信息隐私问题。

- **重大的技术变革或根本性的转变**—部分企业现已迁移到面向服务的架构 (SOA) 和云计算。此类举措不仅彻底改变了基础设施和应用程序功能的开发和交付方式，还涉及相关流程和其他组件的在治理和管理方面的变革。
- **企业治理的重点或项目**—如公司政策的广泛变革等大型项目可能会引发 EGIT 领域的相关举措。
- **新领导层**—任命新的 C 级代表（包括首席信息官 (CIO)、首席财务官 (CFO)、首席执行官 (CEO) 或董事会成员）经常会开展对当前 EGIT 机制和举措的评估，以处理发现的薄弱环节。
- **外部审计或顾问评估**—独立第三方针对相应实践进行的评估可能成为 EGIT 改进举措的起点。
- **新的业务战略或优先级**—追求新的业务战略通常意味着影响 EGIT。例如，贴近客户的业务战略（即了解客户及其需求并尽可能用最好的方式响应）需要既定的业务部门或国家具有 IT 决策权，而不是在公司或控股公司层级的总部进行决策。
- **显著提升从 I&T 获得价值的愿望**—对提高竞争优势、保持创新、优化资产或创造新的业务机会的需求都会唤起对 EGIT 的关注。

这些触发事件与*《COBIT® 2019 设计指南》*中详细介绍的设计因素存在直接关联。企业基于诸多设计因素构建和定制其治理系统。这些设计因素的变化会触发 EGIT 审查。例如，企业战略是一项重要的设计因素，并且与收购、市场变换或新业务战略等触发事件直接相关。另一项重要的设计因素是企业所遵循的合规要求，这与新的法规或合规等要求直接相关。

通过识别痛点以及内外部的触发事件，可以推动行动需求的认可、征询和沟通。这种沟通可以是“警钟”的形式（适用于正经历痛点的情况），也可以表述为改进机会以及可以实现的效益。当前的 EGIT 痛点或触发事件可提供起点。通常可通过全局运行状况检查、诊断或能力评估识别这些痛点。这些技术产生了在待解决问题上形成共识的额外益处。获得第三方对当前情况进行的独立、客观的高层次审查，对落实行动程度可能有一定的好处。

从一开始就努力争取董事会及执行管理层的承诺和支持至关重要。为此，需要用业务术语明确表达 EGIT 计划及其目标和效益。必须保持适度的紧迫感。董事会和执行管理层应意识到良好的 I&T 治理和管理为企业带来的价值以及不采取相应行动的风险。董事会和高级管理层的参与还有助于提前考虑 EGIT 计划、企业目标及战略、企业 IT 目标、企业治理和 ERM 举措（如果有）之间的一致性。识别并实现一些速效方案（能相对快地解决明显问题且获取效益，以帮助提升整体举措的可信度）是一种获得董事会承诺的较为有用机制。

一旦确定高层的方向，便应该确立所有层级对推行变革的总体认识。必须先从艰巨的业务角度理解更广泛的变革规模和范围，但也不能忽视人员和行为方面。需要识别参与变革或受其影响的所有利益相关方，并确定他们对此的态度。

3.3.3 利益相关方的参与

利益相关方需要团结合作才能实现改进 IT 绩效的总体目标。本指南所提供的方法有助于以协调一致的方式，就解决特定利益相关方关注的问题达成共识。最重要的利益相关方及其关注的问题包括：

- **董事会和执行管理层**—我们如何设定和定义企业的 I&T 使用方向，如何监控相关必要 EGIT 组件的建立，以提供业务价值并缓解 IT 相关风险？
- **高级业务管理层、IT 管理层**[10] **和流程所有者**—我们如何帮助企业定义一致性目标，以确保通过使用 I&T 获得业务价值并缓解 IT 相关风险？
- **业务管理层、IT 管理层和流程所有者**—我们如何对业务部门需要且董事会要求的信息、IT 解决方案和服务能力进行规划、构建、交付和监控？
- **风险、合规及法律专家**—我们如何确保企业遵守政策、法规、法律和合同，并确保风险得到识别、评估和缓解？
- **内部审计**—我们如何为价值实现和风险缓解提供独立鉴证？

实施的关键成功因素包括：

- 董事会提供指导，执行管理层提供授权和资源。
- 各方都了解企业和 I&T 相关目标。
- 必要的组织和流程变革能获得有效的沟通和实施。
- 定制框架及良好实践，以适应企业目标和设计。
- 刚开始需要重点关注速效方案并优先进行最容易实施且最有益的改进。这能够展现效益并为进一步改进建立信心。

3.4 识别利益相关方的角色和要求

3.4.1 内部利益相关方

图 3.5 概述了内部利益相关方及其在改进流程中担任的最重要的高阶职责和责任，以及他们对实施计划成果的兴趣。下列利益相关方代表了通用示例；还需要进行一些借鉴、扩展和定制。

[10] IT 管理层包括 IT 职能管理层级别的所有角色。

图 3.5—内部 EGIT 利益相关方概述		
内部利益相关方	**重要的高阶责任和职责**	**对实施计划成果的兴趣**
董事会和高级管理层	设定改进计划的总体方向、背景和目标，并确保与企业业务战略、治理和风险管理保持一致。为举措提供有形支持和承诺，包括确定发起和推动举措的角色。批准计划成果，并确保达到预期的效益和酌情采取纠正措施。确保为该举措提供所需的人财物等资源。确定高层的方向并以身作则。	董事会和执行管理层对从计划实施中获取最大业务效益感兴趣。他们希望确保所有相关必要问题和领域都得以解决、必要的活动均已开展并且成功交付预期成果。
业务管理和业务流程所有者	为核心实施团队提供适当的业务资源。与 IT 合作，确保改进计划的成果适用企业的业务环境、价值得以实现且风险得到缓解。为改进计划提供全面支持，并与 IT 合作解决所遇到的问题。确保业务部门充分参与实施和使用的过渡过程。	这些利益相关方希望该计划能够让 I&T 更加贴合总体业务环境及其特定领域的需求。
首席信息官 (CIO)	为计划提供指引，以及为核心实施团队提供适用的 IT 资源。与业务管理层和高管层共同为计划设立适当的目标、方向和方法。	CIO 希望所有 EGIT 实施目标都能实现。CIO 认为计划应该建立能持续改善与业务的关系并与业务保持一致的机制（包括就 I&T 绩效达成共识）；应该有助于更好地管理 IT 供需；以及改善 I&T 相关业务风险的管理。
IT 管理层和 IT 流程所有者（如运营负责人、首席架构师、IT 安全经理、隐私官、业务连续性管理专家）	为计划的适用工作流提供指引，并为实施团队提供资源。为各自领域流程方面的当前绩效评估和改进目标设定提供关键意见。对企业应纳入的相关良好实践提供意见和相关专家建议。确保业务案例和项目计划切实可行。	这些利益相关方对确保改进计划能够更好地治理 I&T 整体及其各自领域，以及以可能的最佳方式获得实现上述目标所需的业务投入感兴趣。
合规、风险管理和法律专家	根据需要参与整个计划，并就相关问题提供有关合规、风险管理和法律方面的意见。确保与整体 ERM 方法保持一致，并确认已考虑合规性和风险管理有关的问题，与此相关的目标及效益也已经实现。在实施期间提供所需指导。	利益相关方希望通过这些措施建立或改进机制，确保法律及合同合规性以及有效的 I&T 相关业务风险管理，并确保这些机制与企业范围内存在的其他方法相一致。
内部审计	根据需要参与整个计划，并就相关问题提供审计意见。就当前问题提供建议，并对控制实践和方法提出意见。审查业务案例和实施计划的可行性。实施期间根据需要提供建议和指导。 可独立验证评估结果。	利益相关方对控制实践和方法的相关实施计划成果以及所建立或改进的机制如何解决当前审计发现感兴趣。

图 3.5—内部 EGIT 利益相关方概述（续）		
内部利益相关方	**重要的高阶责任和职责**	**对实施计划成果的兴趣**
实施团队（业务和 IT 混合团队，由前述利益相关方类别的人员组成）	指导、设计、控制、推动和执行端到端的计划，涵盖了识别目标和需求到按照业务案例目标对计划进行最终评估，以及识别后续实施或改进周期的新触发因素和目标。确保从实施环境过渡到运营、使用和维护环境期间进行技能转移。	团队希望确保获得并最大程度地实现 EGIT 举措的所有预期成果。
用户	通过履行为他们分配的具体角色和职责来支持 EGIT。	这些利益相关方关心举措在他们日常活动（工作、角色和职责以及活动）中发挥的影响。
客户		客户是扩展价值链的一部分，他们对服务和产品等交付抱有期望。

3.4.2 外部利益相关方

除了**图 3.5** 中列出的内部利益相关方之外，还有一些外部利益相关方。虽然这些利益相关方对改进计划不负有任何直接责任或义务，但他们可能会提出企业需要满足的要求。**图 3.6** 提供了通用示例。

图 3.6—外部 EGIT 利益相关方概述	
外部利益相关方	**对实施计划成果的兴趣**
客户和社会	组织存在的目的是为客户提供服务。因此，企业 EGIT 目标的实现程度会对客户产生直接影响。如果企业面临影响客户的安全和隐私方面相关风险，如丢失客户银行数据，客户也会对 EGIT 实施计划的成果感兴趣。
IT 服务提供商	企业管理层应确保企业自身的整体 EGIT 与 IT 服务提供商提供的服务治理和管理保持一致并且能相互影响。
监管机构	监管机构对实施计划成果能否满足和/或通过合适的组织架构和机制满足所有适用法规和合规性要求感兴趣。
股东（如适用）	股东在做出投资决策时，可能会将企业的公司治理和 EGIT 治理状况及它们取得的成就记录作为部分依据。
外部审计师	经由审计证实的有效实施计划能使外部审计师更充分地依赖 I&T 相关控制。他们还对监管合规和财务报告感兴趣。
业务合作伙伴（如供应商等）	与企业一起使用自动电子交易的业务合作伙伴可能对实施计划在提高信息安全性、完整性和及时性方面的成果感兴趣。他们也许对计划结果可能包括的监管合规和国际标准认证感兴趣。

3.4.3 独立鉴证和审计师的角色

IT 经理和利益相关方需要了解鉴证专业人员的角色。鉴证专业人员可以是内部审计师、外部审计师、国际标准化组织/国际电工委员会 (ISO/IEC) 标准审计员或受托提供 IT 服务和流程评估的任何专业人员。确定 EGIT 实施计划期间将这些利益相关方及其关注点纳入考虑范围十分重要。董事会和执行管理层寻求关键 I&T 功能和服务方面的独立建议和意见的需求与日俱增。在证实企业遵守国家和国际法规方面的需求也普遍增多。

本页特意留白

第四章
识别挑战和成功因素

4.1 引言

EGIT 实施的相关经验表明，想要确保举措一举成功并维持持续改进，必须克服一些实际问题。本章介绍其中几项挑战和可能的根本原因以及确保取得成功应考虑的因素。

4.2 创建适当的环境

4.2.1 第 1 阶段 — 有哪些驱动因素?

图 4.1 列出了第 1 阶段的挑战和其根本原因以及成功因素。

图 4.1—第 1 阶段的挑战、根本原因和成功因素

第 1 阶段 — 有哪些驱动因素?	
挑战	• 缺乏高级管理层的认同、承诺和支持 • 难以证实价值和效益
根本原因	• 对改进治理于企业的重要性、紧迫性和价值缺乏了解（和证据） • 缺乏资源 • 对 EGIT 范围以及 I&T 治理和管理之间的差异理解欠佳 • 实施只是为了解决短期问题而不是为了积极实现范围更广的改进 • 担心成为“又一个可能失败的项目”；对 IT 管理缺乏信任 • 治理问题和效益沟通不当；未明确说明效益和时间计划 • 高管不愿发起计划或承担责任 • 对 IT 职能的可信度认识不足； CIO 不被重视 • 执行管理层认为 EGIT 仅仅是 IT 管理层的责任 • 不具备负责 EGIT 的合适团队（角色扮演者）或欠缺执行任务所需的足够技能 • 未使用公认的框架/缺乏相关培训和意识 • EGIT 在当前企业治理环境中的定位不正确 • 举措的推动者是鼓吹教科书方法的狂热“皈依者”
成功因素	• 将 EGIT 纳入董事会、审计委员会和风险委员会讨论的议程项目。 • 组建委员会或利用现有委员会（如 I&T 治理委员会）对行动进行授权和问责。 • 避免使 EGIT 成为旨在寻找问题的解决方案。必须拥有实际需求和潜在效益。 • 确定具有权限、了解情况并且值得信赖，能够全身心投入从而确保实施成功的领导者和发起人。 • 识别并传达能激发改变现状意愿的痛点。 • 使用适合受众的语言、方法和沟通方式。避免使用受众无法理解的行话和术语。 • （与业务）共同确定 IT 的预期价值并就其达成一致。 • 以（商定的）业务术语/指标说明效益。 • 获取外部审计师、顾问和咨询师（如有必要）的支持并提升技能。 • 制定指导原则，为变革工作确定基调和氛围。

图 4.1—第 1 阶段的挑战、根本原因和成功因素（续）	
第 1 阶段 – 有哪些驱动因素?	
	• 根据企业特有的变革工作确定要求，建立取得成功所需的信任和合作伙伴关系。 • 为目标受众定制业务案例，以展示 IT 投资计划的业务效益。 • 根据战略重点和目前存在的企业痛点，确定业务案例的优先级并使其与企业战略保持一致。 • 使业务案例与企业的总体治理目标保持一致。 • 获得 EGIT 问题和框架方面的教育和培训。
挑战	• 难以获得所需业务部门的参与 • 难以识别利益相关方和角色承担者
根本原因	• 业务高管没有将 EGIT 当作优先事项（EGIT 不是关键绩效指标 [KPI]） • IT 管理层更喜欢独立工作（在客户参与之前证实概念） • IT 与业务部门之间的隔阂阻碍了参与 • 未明确业务参与的角色和责任 • 关键业务人员和影响者未加入或参与 • 企业高管和流程所有者对 EGIT 的效益和价值理解有限
成功因素	• 鼓励高级管理层和 I&T 治理委员会确定授权范围，并在 EGIT 中担任业务角色和职责。 • 制定流程推动利益相关方参与。 • 明确阐述并推广业务效益。 • 阐述拒绝参与带来的风险。 • 识别关键服务或主要 IT 举措，将其用作业务参与 EGIT 改进的试点/模型。 • 找到支持者（认可改善 EGIT 具有价值的业务用户）。 • 在明确定义的政策和治理结构内，推动思想解放和授权。 • 确保那些负责和推动变革的人员能获得发起人的支持。 • 为业务参与创建论坛（如 I&T 治理委员会）并举办研讨会，公开讨论当前问题和改进机会。 • 让业务代表参与整体现状评估。
挑战	• IT 管理层缺乏业务视角
根本原因	• 公司治理绩效欠佳 • 具有运营技术背景的 IT 领导层在企业业务问题中的参与度不够 • IT 管理层在企业内被孤立，未参与高级管理层 • 业务关系流程较弱 • 绩效欠佳的传统认知将 IT 和 CIO 推向被动运营模式 • CIO 和 IT 管理层处于弱势，所以不愿暴露内部弱点
成功因素	• 以被认可 IT 员工的成功和绩效为基础来提高可信度。 • 使 IT 管理层成为企业执行委员会的永久成员（如可能），以确保 IT 管理层拥有适当的业务视角并尽早参与新举措。 • 实施有效的业务关系流程。 • 邀请业务部门参与并加入。考虑将业务人员放在 IT 部门（反之亦然），以获得经验并改善沟通。 • 必要时，重新制定 IT 管理层的角色，并与其他业务职能（如财务和人力资源）建立正式联系。 • 确保 CIO 拥有业务经验。考虑任命业务人员担任 CIO。 • 利用顾问建立更强大且以业务为导向的 EGIT 战略。 • 建立治理机制（如 IT 中的业务关系经理）以获得更多业务见解。

图 4.1—第 1 阶段的挑战、根本原因和成功因素（续）	
第 1 阶段 — 有哪些驱动因素?	
挑战	• 缺乏现行企业政策和方向 • 当前企业治理较弱
根本原因	• 承诺和领导层问题可能源于组织不够成熟 • 领导层独断专行，依赖个人命令而非企业政策 • 文化比控制环境更有利于促进思想解放和方法创新 • 企业风险管理薄弱
成功因素	• 基于合规性和企业绩效的实际问题，向董事会高管和非执行董事提出治理不佳所带来的风险。 • 向审计委员会或内部审计提出问题。 • 获得外部审计师的意见和指导。 • 考虑文化需要如何改变才能促进治理活动。 • 向 CEO 和董事会提出问题。 • 确保风险管理应用于整个企业。

4.2.2 第 2 阶段 — 现在到了什么程度？和第 3 阶段 — 我们想要达到什么目标?

图 4.2 列出了第 2 阶段和第 3 阶段的挑战、根本原因和成功因素。

图 4.2—第 2 阶段和第 3 阶段的挑战、根本原因和成功因素	
第 2 阶段 — 现在到了什么程度? 第 3 阶段 — 我们想要达到什么目标?	
挑战	• 无法获得和维持对改进目标的支持 • IT 与业务之间缺乏沟通
根本原因	• 没有明确的或具有说服力的理由来采取行动 • 预期的收益不能证明投资（成本）的合理性 • 聚焦于变革导致生产力或效率的损失 • 对发起和承诺实现改进目标缺少明确的问责 • 未从战略、战术和运营层面就业务参与制定适当的结构 • 沟通方式不当（不够简单、不够简洁、未用业务语言表达、不适合政治和文化方面）或未调整风格以适应不同受众 • 未妥善建立或阐明改进业务案例 • 对变革推行和所需相关层面的支持关注不够
成功因素	• 就 EGIT 改进的价值达成一致。 • 建立适当的结构（如 IT 指导委员会和审计委员会）以促进沟通，就目标达成一致，并为交流战略状态、澄清误解和分享信息制定会议日程。 • 实施有效的业务关系流程。 • 制定并执行变革推行战略和沟通计划，阐述提高成熟度级别的必要性。 • 使用正确的语言和通用术语，并根据受众群体调整风格。利用视觉效果吸引受众的兴趣。 • 为实现改进目标，将最初的 EGIT 业务案例细化成详细业务案例，并明确阐述风险。将关注点放在业务的附加价值（以业务术语表述）和成本上。 • 开展 COBIT 和本实施方法方面的教育和培训。
挑战	• 改进成本超过感知的效益
根本原因	• 倾向于仅关注控制和绩效改进，而不关注效率改进和创新 • 改进计划的阶段划分不当，不能将改进效益和成本明确关联 • 优先选择复杂、昂贵的解决方案，而不是成本更低且更简单的解决方案 • 由于大量 IT 预算和员工被投入到维护现有的基础设施，导致能用于处理 EGIT 的直接资金或时间很有限

图 4.2—第 2 阶段和第 3 阶段的挑战、根本原因和成功因素（续）	
第 2 阶段 — 现在到了什么程度? 第 3 阶段 — 我们想要达到什么目标?	
成功因素	• 识别基础设施、流程和 HR 中可通过改善治理来提高效率和直接节省成本的方面（如标准化、提高成熟度和减少事故）。 • 按照实施的效益和难易度确定优先顺序，尤其是速效方案。
挑战	• IT 与企业之间缺乏信任和良好关系
根本原因	• 由于对项目和服务交付的 IT 跟踪记录欠佳而导致的后遗症 • IT 缺乏对业务问题的了解，反之亦然 • 未正确传达和妥善管理范围和期望 • 未明确业务中的治理角色、职责和问责机制，导致推卸关键决策的责任 • 缺乏阐述改进需求的支持信息和指标 • 不愿被证明之前的错误，一味抗拒变革
成功因素	• 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，帮助建立和保持信心。 • 确保 CIO 在建立信任和关系方面拥有公信力和领导力。 • 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（业务方面）。 • 专注于变革推行的规划。

4.2.3 第 4 阶段 — 我们需要完成什么行动?

图 4.3 列出了第 4 阶段的挑战、其根本原因和成功因素。

图 4.3—第 4 阶段的挑战、根本原因和成功因素	
第 4 阶段 — 我们需要完成什么行动?	
挑战	• 不了解环境
根本原因	• 未充分考虑组织和文化所需的改变以及利益相关方的看法 • 未充分考虑 IT 和整个企业内部的现有治理优势和实践
成功因素	• 开展利益相关方评估，并侧重于制定变革推行计划。 • 以 IT 和整个企业内部的现有优势和良好实践为基础并加以利用。避免仅为 IT 另起炉灶。 • 了解不同群体及其目标和心态。
挑战	• 不同的复杂程度（技术、组织、运营模式）
根本原因	• 对 EGIT 实践不够了解 • 试图一次实施过多内容 • 在缺少实践经验时，优先实施关键和困难的改进 • 存在复杂或多种公司运营模式
成功因素	• 开展 COBIT 和本实施方法方面的教育和培训。 • 拆分成较小项目，并且一次执行一个步骤。优先考虑速效方案。 • 收集不同群体的改进需求。找出这些需求之间的关联并确定优先级，然后将其对应到变革推行计划中。 • 依据业务优先级进行分阶段实施。

图 4.3—第 4 阶段的挑战、根本原因和成功因素（*续*）	
第 4 阶段 – 我们需要完成什么行动?	
挑战	• 难以理解 COBIT 及相关框架、程序和实践
根本原因	• 技能和知识储备不足 • 生搬硬套良好实践，未进行相应调整 • 只关注程序，而不关注角色、责任和所需技能等其他动力
成功因素	• 开展 COBIT、其他相关标准和良好实践、本实施方法等方面的教育和培训。 • 获得具有资格且经验丰富的外部指导和支持（如需要）。 • 调整和定制适合企业环境的良好实践。 • 设计流程时，考虑所需技能、角色和职责、流程所有权、目的和目标以及其他治理组件。
挑战	• 抗拒变革
根本原因	• 当现状受到威胁时，抗拒是很自然的行为反应，但这也可能表示潜在顾虑，例如： ■ 对需要什么及其用处存在误解 ■ 觉得工作量和成本会增加 ■ 不愿意承认缺陷 ■ 由于在企业强制推行通用治理框架导致的非自主发明综合症 ■ 难以推翻根深蒂固的思想、对角色或权力基础产生威胁、不了解“对我有什么好处”
成功因素	• 关注特定痛点和驱动因素的意识沟通。 • 通过为业务和 IT 经理以及利益相关方提供培训来提高认知。 • 使用具备业务和 IT 技能且经验丰富的变革推动者。 • 定期跟踪里程碑，确保相关各方的实施效益得到实现。 • 寻求快速且相对容易的成果以吸引关注，促进对所提供价值的广泛认可。 • 将 COBIT 等通用框架与企业环境关联起来。 • 专注于变革推行计划，例如： ■ 开发 ■ 培训 ■ 指导 ■ 辅导 ■ 转移技能 • 组织沟通会议/演示活动，并主动向支持者宣传效益。
挑战	• 未采用改进
根本原因	• 外部专家在没有获得充足信息的情况下，孤立地设计解决方案或实施解决方案 • 内部 EGIT 团队独自运作并担任实际流程所有者的非正式代理，从而导致误解并抗拒变革 • 关键利益相关方的支持和指导不足，导致 EGIT 项目生成缺少有效所有权的新政策和程序
成功因素	• 让流程所有者和其他利益相关方参与设计过程。 • 适当情况下，利用试点和演示进行教育并获得认同和支持。 • 从速效方案开始，体现效益并以此为基础。 • 寻找那些能理解抗拒行为并希望改善的支持者，而不是迫使抗拒者屈服。 • 鼓励管理架构优化，包括分配相应角色和责任、承诺持续运营、监控合规性。 • 将从外部专家获取的知识转移给流程所有者。 • 委派责任并为流程所有者授权。
挑战	• 难以整合内部治理方法与外包合作伙伴的治理模型
根本原因	• 害怕暴露不当实践 • 未向外包提供商明确或与其分享 EGIT 要求 • 角色和责任分工不明确 • 方法和期望之间存在差异 • 外包合同中的条款约束

图 4.3—第 4 阶段的挑战、根本原因和成功因素（续）	
第 4 阶段 — 我们需要完成什么行动?	
成功因素	• 让供应商/第三方参与实施和运营活动（如适用）。 • 将条件和审计权纳入合同中。 • 想办法实现框架和方法的集成。 • 提前与第三方确定角色、责任和治理结构，而不是事后考虑。 • 将服务提供商流程、人员和技术的证据（经由审计和文件审查）与所需的 EGIT 实践和级别相匹配。

4.2.4 第 5 阶段 — 我们如何实现?

图 4.4 列出了第 5 阶段的挑战、其根本原因和成功因素。

图 4.4—第 5 阶段的挑战、根本原因和成功因素	
第 5 阶段 — 我们如何实现?	
挑战	• 未能兑现实施承诺
根本原因	• 对目标过于乐观，低估了所需的努力 • IT 处于救火模式，并且侧重于运营问题 • 缺乏专门的资源或能力 • 优先级分配错误 • 范围与要求不一致或实施者有所误解 • 未妥善应用项目管理原则（如业务案例） • 对业务环境（如运营模式）的认识不足
成功因素	• 管理期望。 • 遵循指导原则。 • 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。 • 确保实施范围符合相关要求，并且所有利益相关方对交付范围达成共识。 • 侧重于支持业务价值的实施。 • 确保为之分配专用资源。 • 应用项目管理和治理原则。 • 利用现有机制和工作方式。 • 确保对业务环境有正确的认识。
挑战	• 同时进行太多的工作；处理的问题过于复杂、困难或数量过多
根本原因	• 对范围和相关工作缺乏了解（以及人员方面缺乏共同语言） • 不了解适应变化的能力（其他举措过多） • 缺乏正式的项目规划和管理；未打好基础，提高工作的成熟度 • 实施压力过大 • 未利用速效方案 • 另起炉灶，未以当前情况为基础 • 对组织格局缺乏认识 • 缺少技能
成功因素	• 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。

图 4.4—第 5 阶段的挑战、根本原因和成功因素（续）	
第 5 阶段 — 我们如何实现?	
挑战	• IT 或业务处于救火模式
根本原因	• 缺乏资源或技能 • 缺乏内部流程，内部效率低下 • 缺乏强大的 IT 领导层 • 变通方案过多
成功因素	• 运用良好的管理技能。 • 获得最高管理层的承诺和支持，使所有人员专注于 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和管理。 • 适当使用外部资源。 • 获得外部协助。
挑战	• 缺乏必要的技能和能力，例如对治理、管理、流程和软技能缺乏了解
根本原因	• 对 COBIT 和 IT 管理良好实践的理解程度不够 • 通常业务和管理技能未被纳入培训 • IT 人员对业务领域不感兴趣 • 业务人员对 IT 不感兴趣
成功因素	• 专注于变革推行的规划： ■ 开发 ■ 培训 ■ 指导 ■ 辅导 ■ 反馈到招聘流程 ■ 跨技能

4.2.5 第 6 阶段 — 我们是否实现？和第 7 阶段 — 我们如何保持前进的动力?

图 4.5 列出了第 6 阶段和第 7 阶段的挑战、根本原因和成功因素。

图 4.5—第 6 阶段和第 7 阶段的挑战、根本原因和成功因素	
第 6 阶段 — 我们是否实现? 第 7 阶段 — 我们如何保持前进的动力?	
挑战	• 未采用或应用改进
根本原因	• 解决方案过于复杂或不切实际 • 解决方案由顾问或专家团队独立开发 • 生搬硬套良好实践，未根据企业运营情况进行调整 • 解决方案不归流程所有者/团队所有 • 组织缺乏明确的角色和责任 • 管理层没有为变革提供授权和支持 • 抗拒变革 • 对如何应用已开发的新流程或工具缺乏了解 • 技能和经验不符合角色要求

图 4.5—第 6 阶段和第 7 阶段的挑战、根本原因和成功因素（续）	
第 6 阶段 – 我们是否实现? 第 7 阶段 – 我们如何保持前进的动力?	
成功因素	• 专注于速效方案和可管理的项目。 • 实施小的改进来测试方法并确保其有效。 • 让流程所有者和其他利益相关方参与制定改进措施。 • 确保角色和职责非常清晰并且已被接受。修改角色和工作描述（如必要）。 • 自上而下（从管理层到整个企业）推动改进。 • 必要时进行适当的培训。 • 在尝试实施自动化执行之前制定流程。 • 必要时进行重组，以实现更好的流程所有权。 • 使角色（特别是对取得成功而言至关重要的角色）与个人能力和特征相匹配。 • 提供有效的教育和培训。
挑战	• 难以展现或证明效益
根本原因	• 目标和指标未建立或未发挥有效作用 • 实施后未进行效益跟踪 • 不关注获得的效益和价值 • 对成功的沟通欠佳
成功因素	• 制定清晰、可衡量、切合实际的目标（期望通过改进实现的成果）。 • 制定切实可行的绩效指标（以监控改进是否有利于实现目标）。 • 制作计分卡来显示衡量绩效的方式。 • 以业务影响的角度沟通正在实现的结果和效益。 • 实施速效方案并在短期内提供解决方案。
挑战	• 失去兴趣和动力，变革疲劳
根本原因	• 未将持续改进作为文化的一部分 • 管理层未推动可持续的结果 • 资源侧重于救火和服务交付，而非改进 • 员工动力不足，无法看到变革所带来的个人收益
成功因素	• 确保管理层定期沟通并强化稳定可靠的服务、解决方案和良好治理的需求。向所有利益相关方传达已经取得的成功改进。 • 重新审视利益相关方并获得其支持以推动发展势头。 • 抓住机会在工作中实施改进。在资源稀缺的情况下，可将之作为日常工作的一部分。 • 侧重于可管理的常规改进任务。 • 获得外部援助，但仍需保持参与。 • 确保个人奖励系统与流程以及组织绩效改进目标和指标保持一致。

第五章
推行变革

5.1 推行变革的需求

成功实施或改进取决于以正确的方式实施适当变革。许多企业都将重点放在实施良好实践方面，但对另一方面，即以正式的方式实施变革（强调人员、行为和文化方面的变革管理，以及激励利益相关方支持变革），投入还不够。包括利益相关方管理在内的变革推行是 EGIT 实施的最大挑战之一。

对于新的或修改后的治理安排所牵涉或影响的各种利益相关方，不应该假设他们必然会即刻接受和适应变革。如果出现无视、抗拒变革或变革疲劳的情况，需要通过结构化的积极方法来应对。[11] 应通过一个沟通计划来让人们充分了解项目，该计划明确沟通的内容、沟通方式、沟通人员和沟通对象。

COBIT 将推行变革定义为，确保所有利益相关方做好准备并投身于涉及从当前状态进入未来理想状态的变革的全面系统化流程。

所有关键利益相关方都应该参与。在较高级别，变革推行通常必须：

- 评估变革对企业、人员和其他利益相关方的影响
- 建立人员/行为方面的未来状态（愿景）以及描述它的相关衡量指标
- 建立变革响应计划来积极管理变革影响并最大限度地提高整个过程中的参与度。这些计划可能包括培训、沟通、组织设计（工作内容、组织结构）、流程再设计以及更新绩效管理系统。
- 持续监测变革朝未来理想状态推进的状况

虽然每项 EGIT 实施各有不同，但变革推行的共同目标是让来自业务和 IT 的企业利益相关方以身作则，引领并鼓励各级员工按照理想的新方式开展工作。理想行为的示例包括：

- 遵循议定流程
- 参与变革批准或顾问委员会等既定 EGIT 结构
- 实施既定指导原则、政策、标准、流程或实践，例如新的投资或安全方面的政策

这最好能通过赢得利益相关方投身其中（尽心尽责、领导力以及沟通和回应员工）以及宣传变革效益来实现。如有必要，可能需要强制遵循。换句话说，必须克服人员、行为和文化障碍，才能构建共同利益，以正确采纳、愿意采纳并确保有能力采纳新的工作方式。在企业内运用变革推行技能十分有用，如有必要，可以借助外部顾问来推进行为变革。

[11] 美国退伍军人事务部 (VA) 表示，在审查一项重大 IT 转型举措时，“VA 在实现这项转型期间面临的主要挑战是获得所有 VA 人员（包括领导层、中层管理人员和现场员工）的接受和支持”。See Walters, J.；“Transforming Information Technology at the Department of Veterans Affairs”，IBM 政府事务中心，美国，2009 年，*http://www.isaca.org/Knowledge-Center/cobit/Documents/WaltersVAReport-June09.pdf*。VA 表示，如果只解决技术转型问题，这些努力无法取得成功；它认识到，获得接受、开展组织变革和改变业务方式所需的人为因素对取得成功至关重要。

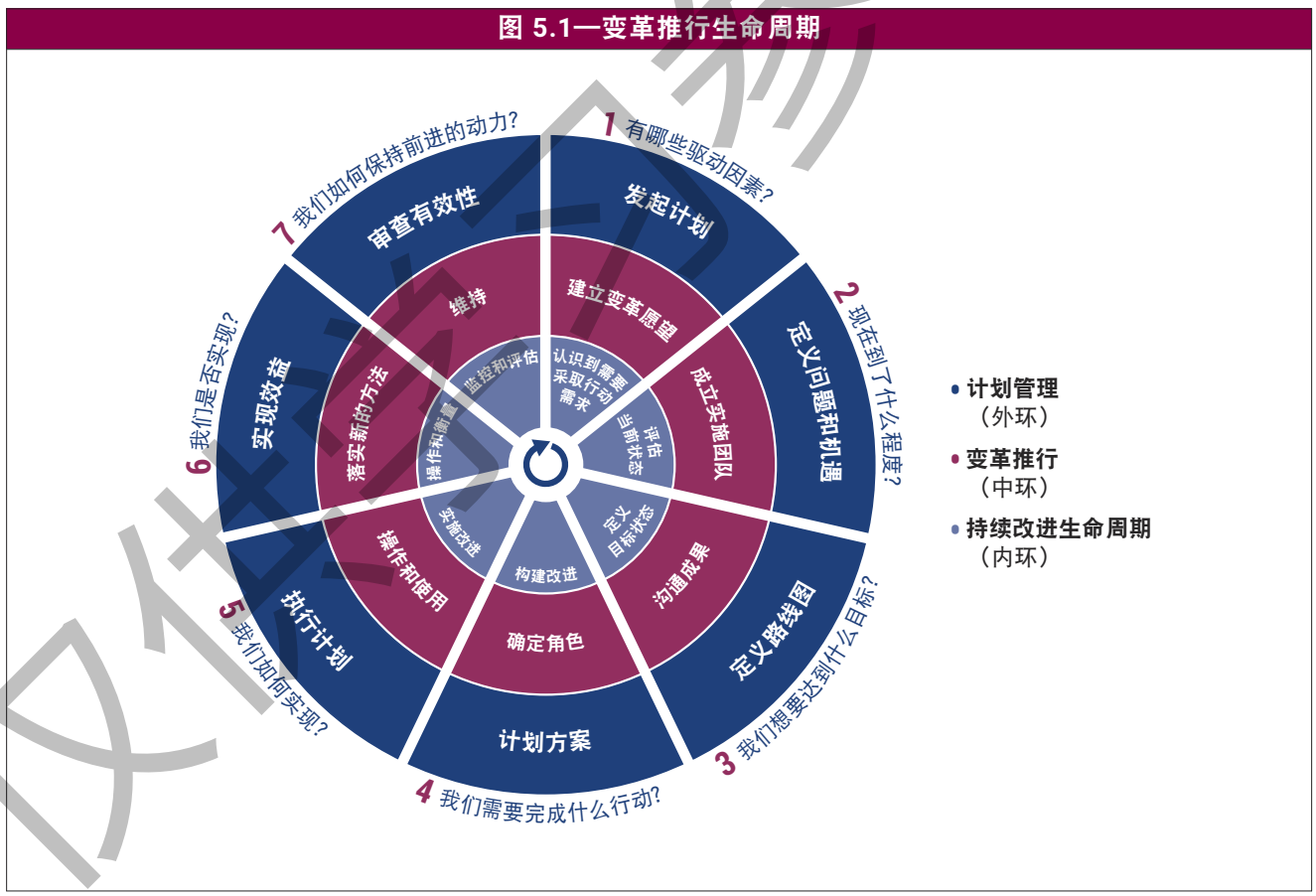
5.1.1 EGIT 实施的变革推行

多年以来，推行变革的方法层出不穷，它们提供了可以在实施生命周期使用的有价值的输入信息。其中一种得到最广泛认可的变革推行方法是由 John Kotter 开发的：[12]

1. 建立紧迫感。
2. 形成强大的指导同盟。
3. 制定表述简洁的清晰愿景。
4. 沟通愿景。
5. 鼓励他人采取行动来实现愿景。
6. 计划并创造短期效益。
7. 巩固改进方面并推行更多变革。
8. 制度化新方法。

Kotter 方法已被选作范例，并针对 EGIT 实施或改进的具体要求作适当改编（如本出版物所述）。**图 5.1** 中的变革生命周期阐述了优化后的 Kotter 准则。

图 5.1—变革推行生命周期



[12] Kotter, J.；*Leading Change*，Harvard Business School Press，美国，1996 年，*https://www.kotterinc.com/book/leading-change/*

以下小节简要讨论了应用于典型 EGIT 实施的变革推行生命周期的各个阶段，从较高层次全面概述了变革推行生命周期。

5.2 在变革生命周期中的各个阶段创造适当的环境

应对整个企业环境进行分析，以确定最合适的变革推行方法。这包括管理风格、文化、正式和非正式关系以及态度等方面。了解正在进行或计划中的其他 I&T 或企业举措，确保相关的依存关系和影响已纳入考虑范围，这一点也很重要。

从一开始就应确保能够获得和利用必要的变革推行技能、能力和经验。例如，这可能需要获取 HR 职能部门的资源或外部援助。

作为此阶段的成果之一，可以设计一种合理的平衡，即，为实现可持续效益而需进行的指导性与包容性变革支持活动间的平衡。

5.2.1 第 1 阶段 — 建立变革愿望

此阶段旨在了解所设想的变革广度和深度、受影响的各利益相关方、对各利益相关方群体的影响性质、各利益相关方群体所需的参与，以及当前采用变革的准备情况和能力。

目前的痛点和触发事件能够为建立变革愿望奠定良好基础。“警钟”是计划的初步沟通内容，与企业可能遇到的实际问题有关。此外，可将初期效益与企业中容易看到变革效果的领域联系起来，为进一步的变革和获取更广泛的承诺和支持创造平台。

虽然沟通是贯穿整个实施或改进计划的共同主线，但初步沟通是最为重要的沟通之一，并且还应展示高级管理层的承诺。因此，理想情况下，应由执行委员会或 CEO 进行初步沟通。

5.2.2 第 2 阶段 — 组建有效的实施团队

组建有效的核心实施团队时需要考虑的方面：业务人员和 IT 人员适合参与的领域，团队成员的知识和专长、经验、可信度及威信。获得外部相关方（如顾问和变革推动者）提供的独立且客观的观点也非常有益，比如助力实施过程或解决企业内可能存在的技能差距。因此，还需考虑的一个方面是内部和外部资源的适当组合。

团队应致力于以下工作：

- 制定清晰的愿景和预期目标
- 始终确保所有团队成员的全力参与
- 确保团队流程、问责机制和沟通的清晰度和透明度
- 保持坦诚、相互支持，并全力促进彼此的成功
- 双向问责制和集体责任

- 持续衡量自身绩效及其作为团队的行为方式
- 远离舒适区，不断寻求改进方法，从而发现新机会和拥抱变革

识别不同业务的潜在变革推动者非常重要，核心团队可以与之合作，共同支持愿景和逐层向下的变革。

5.2.3 第 3 阶段 — 沟通预期愿景

在此阶段，结合整体项目计划来制定变革推行整体计划。沟通战略是变革推行计划的一个关键环节，该战略需要确定核心受众群体及其行为特征、信息需求、沟通渠道和原则。

以变革所影响群体的语言来沟通实施或改进计划的预期愿景。沟通内容应包括变革的根本原因、效益、不进行变革的影响（目的），以及愿景（蓝图）、实现愿景的路线图（计划）和各利益相关方（组成）的必要参与。[13] 高级管理层应提供关键信息（如预期愿景）。沟通时应关注行为/文化和逻辑方面，并要注意沟通一定是双向的。应获取意见、建议和其他反馈，并采取适当行动。

5.2.4 第 4 阶段 — 为角色授权并确定速效方案

完成改进设计和构建后，应制定变革响应计划，明确所有参与者的权力。这些计划的范围可能包括：

- 组织架构优化，如工作内容或团队结构
- 运营优化，如工艺流程或物流
- 人员管理优化，如所需培训或绩效管理和绩效考核系统的优化

从变革推行的角度来看，实现速效方案非常重要。这些可能与第 3 章讨论的痛点和触发事件有关。快速见效的方案能为计划实施建立动力和可信度，还有助于消除可能存在的任何怀疑态度。

在设计和构建改进方案时必须采用参与式方法。让变革影响人员参与设计（如借由研讨会和审查会议）有助于获得更多支持。

5.2.5 第 5 阶段 — 启动运营和使用

关键实施生命周期的各项举措得以执行，也使变革响应计划得到了实施。速赢方案取得成效并奠定基础后，应考虑推进行为习惯和文化方面的大规模变革（比如如何处理担心职责丢失、新的目标要求和未知任务等问题）。

平衡集体与个人之间的关系非常重要，这不仅可以获得更多支持和参与，而且确保所有利益相关方获得变革的整体视图。

[13] 如需了解四 P（目的、蓝图、计划和组成），请参阅 Bridges, W.；*Managing Transitions: Making the Most of Change*，Addison-Wesley，美国，1999 年。

在实施解决方案期间，指导和辅导对于确保适用用户环境至关重要。应重新审视启动举措时设立的变革要求和目标，以确保这些变革要求和目标得到适当满足。

应定义成功的衡量指标，包括业务定量指标和用于跟踪人们对变革看法的定性指标。

5.2.6 第 6 阶段 — 落实新方法

实施成功后，应使新的工作方式成为企业文化的一部分，并内置于企业准则和价值观中（“我们在这里的做事方式”）。实施相应的政策、标准和程序是实现此目标的方法之一。还应对变革的实施效果进行跟踪、对变革响应计划的有效性进行评估，并视情况采取纠正措施。必要时可能强制执行合规性。

应保持沟通机制，以持续强化意识。

5.2.7 第 7 阶段 — 维持

变革需要借由意识强化、持续的沟通活动和高级管理层承诺来维持。

此阶段需要在更广泛的企业范围内实施纠正行动计划、获取经验教训和分享知识。

本页特意留白

第六章
实施生命周期

6.1 引言

EGIT 的持续改进是通过第 3 章概述的实施生命周期的七个阶段来实现的。每个阶段的辅助文档如下：

- 一份图表，总结了每组角色在该阶段承担的职责。所定义的角色是通用的，不一定对应到具体职能部门。
- 一份表格，包含以下信息：
  - 阶段目标
  - 阶段描述
  - 持续改进 (CI) 任务
  - 变革推行 (CE) 任务
  - 计划管理 (PM) 任务
  - 可能需要的输入的示例
  - 建议使用的 ISACA 或其他框架
  - 需生成的输出
- 一份图表，描述了从持续改进 (CI)、变革推行 (CE) 和计划管理 (PM) 任务中选择的关键活动的执行人、责任人、咨询人和知情人 (RACI)，以及相关参考材料。RACI 矩阵包含了最重要的活动，这些活动要么为下一阶段提供交付成果或输出，要么具有与之关联的里程碑，或者对整个举措的成功非常关键。篇幅所限，本指南并未涵盖所有活动。

本指南不是规范性文件，而是一个通用的阶段和任务计划，应根据具体实施情况进行调整。

本指南引用了《*COBIT® 2019 设计指南*》中第 1-3 阶段 CI 任务的一些步骤。《*COBIT® 2019 设计指南*》中包含了对本章所述 CI 任务的更详细指导。在治理改进计划的初始阶段应结合使用这两本指南。

6.2 第 1 阶段 — 有哪些驱动因素?

图 6.1—第 1 阶段 — *有哪些驱动因素?*

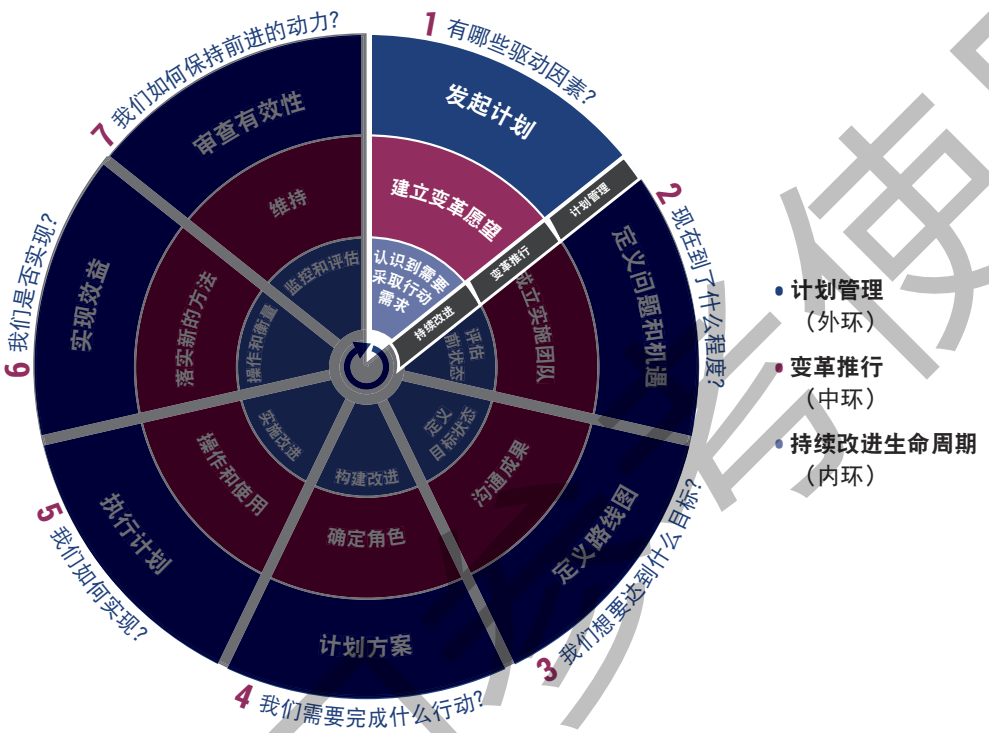


图 6.2—第 1 阶段的角色

如果您是.....	您在本阶段的角色是.....
董事会和执行管理层	提供有关 EGIT 的利益相关方需求（包括客户需求）、业务战略、优先级、目标和指导原则的指引。批准高层次方法。
业务管理层	与 IT 部门一起确保利益相关方需求和业务目标得到充分明确的阐述，以便将其转化为 I&T 业务目标。提供输入来帮助了解风险和优先级。
IT 管理层	收集利益相关方的要求和目标，并就方法和范围达成共识。提供有关 IT 事务的专家建议和指导。
内部审计	提供建议并审查活动和行动建议，确保做出客观均衡的决策。就当前问题提出意见。提供有关控制和风险管理实践和方法的建议。
风险、合规及法律	提供有关风险、合规及法律事务的建议和指导。确保管理层建议的方法符合风险、合规及法律要求。

图 6.3—第 1 阶段的目标、描述、任务、输入、资源和输出	
第 1 阶段描述 — 驱动因素是什么?	
阶段目标	了解计划的背景、目标以及当前的治理方法。定义初步计划概念的业务案例。获得所有关键利益相关方的支持和承诺。
阶段描述	这一阶段阐述了在组织环境中开展行动的有说服力的理由。在此情况下定义计划的背景、目标和当前的治理文化，制定初步计划概念的业务案例，并获得所有关键利益相关方的支持和承诺。
持续改进 (CI) 任务	部分 CI 任务相当于《*COBIT® 2019 设计指南*》中定义的活动。本指南就前三项任务提供了详细指导，特别是设计指南的步骤 1.1“了解企业战略”；步骤 1.2“了解企业目标”；步骤 1.3“了解风险概况”；以及步骤 1.4“了解当前的 I&T 相关问题”。 识别行动需求: **1.** 确定当前的治理环境、业务和 IT 的痛点、事件，以及产生行动需求的原因。 **2.** 确定改进 EGIT 的业务和治理驱动因素以及合规性要求，并评估当前的利益相关方需求。 **3.** 确定依赖于 IT 的业务优先级和业务战略，包括当前任何重大项目。 **4.** 与企业政策、战略、指导原则以及任何持续开展的治理举措保持一致。 **5.** 提高执行管理层对 IT 对企业的重要性和 EGIT 价值的认识。 **6.** 制定 EGIT 政策、目标、指导原则和高层次改进目标。 **7.** 确保执行管理层和董事会理解并批准高层次方法，并接受对重大问题不采取任何措施可能带来的风险。
变革推行 (CE) 任务	建立变革愿望: **1.** 确保与企业级的变革推行方法或计划（如有）整合。 **2.** 分析需要推行变革的一般组织环境，包括组织结构、管理风格、文化、工作方式、正式和非正式关系，以及态度。 **3.** 识别其他正在开展或计划中的企业举措，并确定变革的依存关系或影响。 **4.** 了解变革的广度和深度。 **5.** 确定参与举措的来自企业不同部门（例如业务、IT、审计、风险管理）和不同层级（例如高级管理层、中级管理层）的利益相关方并考虑他们的需求。 **6.** 确定每个利益相关方团体或个人支持和参与的程度、他们的影响力以及变革举措对他们的影响。 **7.** 逐一确认每个利益相关方团体或个人实施变革的就绪情况和能力。 **8.** 以痛点和触发事件为起点建立“警钟”。通过 I&T 治理委员会或类似治理结构沟通信息，以便所有利益相关方了解计划及其驱动因素和目标。 **9.** 通过强调合规要求与出错的数量等方式，消除在安全方面可能存在的忽视情况。 **10.** 根据变革的优先级和影响，保持适度的紧迫感。
计划管理 (PM) 任务	启动计划: **1.** 提供高层次的战略方向，并与 I&T 治理委员会或同等组织（如有）一起制定高层次的计划目标。 **2.** 定义并分配计划中的高层次角色和职责，从执行主管开始，包括计划经理和所有重要的利益相关方。 **3.** 制定业务案例大纲，说明用于推动治理改进的绩效监控和报告的成功因素。 **4.** 获得高级管理层的支持。

图 6.3—第 1 阶段的目标、描述、任务、输入、资源和输出（续）

第 1 阶段描述 – 驱动因素是什么？	
输入	• 企业政策、战略、治理和业务计划，以及审计报告 • 可能存在依存关系或受到影响的其他重大企业举措 • I&T 治理委员会绩效报告的客户服务部门统计数据、IT 客户调查，或其他指出当前 IT 痛点的输入 • 任何有用且相关的行业概况、案例研究和成功案例（请参阅 *www.isaca.org/cobitcasestudies*） • 具体的客户要求、营销和服务战略、市场定位、企业愿景和使命宣言
ISACA 材料和其他框架	• *《COBIT® 2019 设计指南》*（设计因素） • *《COBIT® 2019 框架：治理和管理目标》*（尤其是 EDM01、APO01、MEA01）和 *《COBIT® 2019 框架：简介和方法》*第 9 章“开始实施 COBIT：制作案例”，*www.isaca.org/cobit* • 本出版物附录中的决策矩阵示例 • 当前在 *www.isaca.org* 列出的支持 ISACA 的产品
输出	• 业务案例大纲 • 高层次角色和职责 • 已确定的利益相关方图，包括所需的支持和参与、影响力和受到的影响，以及对人员变更管理所需工作的共识 • 计划的“警钟”（所有利益相关方） • 计划的启动沟通（关键利益相关方）

图 6.4—第 1 阶段 RACI 矩阵

关键活动	董事会	I&T 治理委员会	CIO	业务高管	IT 经理	IT 流程所有者	IT 审计	风险与合规性	计划指导
	实施人员的职责								
确定会触发采取行动的问题 (CI1)。	C/I	A	R	R	C	C	C	C	R
确定影响 IT 的业务优先级和业务战略 (CI3)。	C	A	R	R	C	C	C	C	R
获得管理层的行动批准和高级管理层的支持 (CI7)。	C	A/R	R	C	I	I	I	I	R
保持适度的变革紧迫感 (CE10)。	I	A	R	R	C	C	C	C	R
制定具有说服力的业务案例大纲 (PM3)。	I	A	R	C	C	C	C	C	R

RACI 矩阵确定谁是执行人、责任人、咨询人以及知情人。

6.3 第 2 阶段 — 现在到了什么程度?

图 6.5—第 2 阶段 — *现在到了什么程度?*

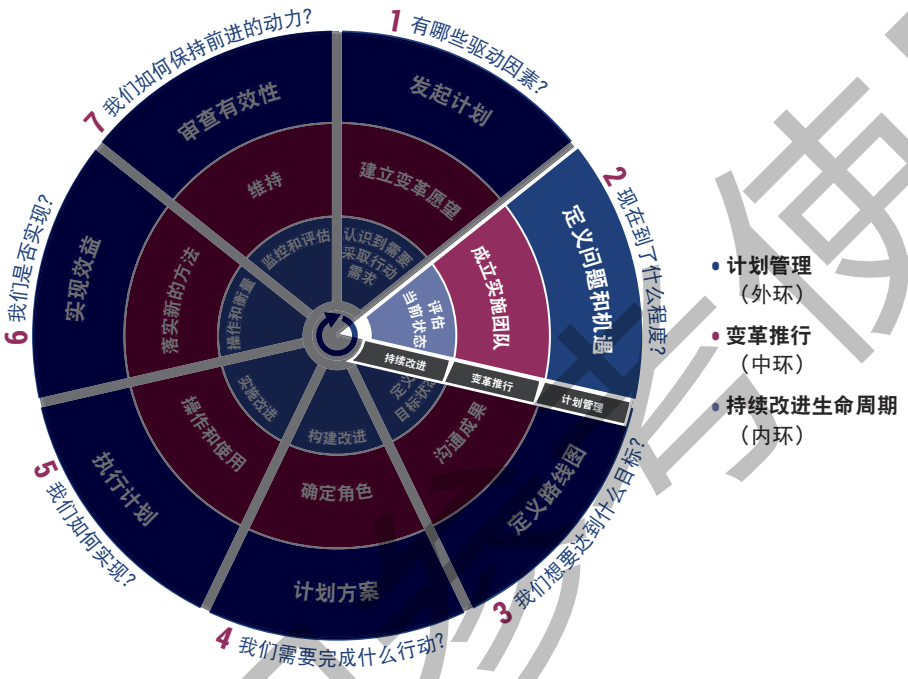


图 6.6—第 2 阶段的角色	
如果您是.....	**您在本阶段的角色是.....**
董事会和执行管理层	验证并解读评估的结果/结论。
业务管理层	通过提供客户观点来协助 IT 部门确定当前评估的合理性。
IT 管理层	确保对 IT 活动进行开放和公正的评估。指导对当前实践的评估。达成共识。
内部审计	为现状评估提供建议、意见和协助。必要时独立验证评估结果。
风险、合规及法律	审查评估，确保已充分考虑风险、合规及法律问题。

图 6.7—第 2 阶段的目标、描述、任务、输入、资源和输出	
第 2 阶段描述 — 现在到了什么程度?	
阶段目标	确保计划团队知道并理解企业目标以及业务和 IT 职能部门应如何实现 I&T 价值来支持企业目标，包括当前的重大项目。确定将在改进计划中处理的关键流程或其他动力。为选定的流程确定适当的管理实践。了解企业目前和将来对风险和 IT 风险状况的态度，并确定对计划有什么影响。确定选定流程当前的能力。了解企业的变革容量和能力。

图 6.7—第 2 阶段的目标、描述、任务、输入、资源和输出 *（续）*	
第 2 阶段描述 – 现在到了什么程度?	
阶段描述	这一阶段确定企业目标和一致性目标，并阐述 I&T 如何通过解决方案和服务来促进企业目标的实现。 重点是识别并分析 I&T 如何通过以敏捷的方式推动业务转型、提高当前业务流程的效率、提高企业效率以及满足治理相关要求（如管理风险、确保安全性，以及遵守法律和监管要求）来为企业创造价值。 根据企业风险概况、风险历史和偏好，以及实际效益/价值实现风险来定义企业目标和一致性目标的效益/价值实现风险以及计划/项目交付和服务交付/IT 运营风险。*《COBIT® 2019 设计指南》*包含一般风险场景与 COBIT 治理和管理目标的对应关系表，可用于支持此分析。 了解业务和治理驱动因素并进行风险评估，确保专注于对实现一致性目标至关重要的治理和管理目标。根据流程描述、政策、标准、程序和技术规范建立支持各项治理和管理目标的不同治理组件的绩效水平，以确定它们能否支持业务和 I&T 要求。 企业中存在的特定 IT 相关问题也有助于选择应重点关注的治理和管理目标。 *《COBIT® 2019 设计指南》*包含常见的 IT 相关问题（如第 3 章所述）与 COBIT 治理和管理目标的对应关系示例。
持续改进 (CI) 任务	评估当前状态: 了解 I&T 应如何支持当前的企业目标。（*《COBIT® 2019 设计指南》*详细探讨了企业战略和 COBIT 目标级联。） 部分 CI 任务相当于*《COBIT® 2019 设计指南》*中定义的活动。请参阅该指南，获取关于下述大多数 CI 任务的更多详细指导。 **确定关键的企业目标和支持的一致性目标** — 更多详细指导，请参阅*《COBIT® 2019 设计指南》*第 4 节步骤 2.1“考虑企业战略”和步骤 2.2“考虑企业目标并运用 COBIT 目标级联”。 **1. 确定支持业务目标所需的 I&T 贡献（解决方案和服务）的重要性和性质** — 更多详细指导，请参阅*《COBIT® 2019 设计指南》*第 4 节步骤 2.2“考虑企业目标并运用 COBIT 目标级联”、步骤 3.1“考虑企业规模”、步骤 3.4“考虑 IT 角色”、步骤 3.5“考虑采购模式”、步骤 3.6“考虑 IT 实施方法”以及步骤 3.7“考虑 IT 采用战略”。 **2. 确定与当前和未来所需的解决方案和服务有关的关键治理问题和弱点，以及支持 IT 相关目标所需的企业架构** — 更多详细指导，请参阅*《COBIT® 2019 设计指南》*第 4 节步骤 2.4“考虑当前的 I&T 相关问题”。 **3. 确定并选择对支持 IT 相关目标至关重要的治理和管理目标，适当情况下还包括每个选定流程的关键管理实践** — 更多详细指导，请参阅*《COBIT® 2019 设计指南》*第 4 节步骤 2.1“考虑企业战略”和步骤 2.2“考虑企业目标并运用 COBIT 目标级联”。 **4. 评估与关键治理和管理目标有关的效益/价值实现风险以及计划/项目交付和服务交付/IT 运营风险** — 更多详细指导，请参阅*《COBIT® 2019 设计指南》*第 4 节步骤 2.3“考虑企业的风险概况”。 **5. 确定并选择对规避风险至关重要的治理和管理目标** — 更多详细指导，请参阅*《COBIT® 2019 设计指南》*第 4 节步骤 2.3“考虑企业的风险概况”。 **6. 了解管理层定义的风险接受立场** — 更多详细指导，请参阅*《COBIT® 2019 设计指南》*第 4 节步骤 1.3“了解风险概况”和步骤 2.3“考虑企业的风险概况”。

图 6.7—第 2 阶段的目标、描述、任务、输入、资源和输出（续）	
第 2 阶段描述 – 现在到了什么程度?	
	评估实际绩效（请参阅《*COBIT® 2019 框架：简介和方法*》第 6 章“COBIT 中的绩效管理”）： 1. 定义用于执行评估的方法。请参阅《*COBIT® 2019 框架：简介和方法*》第 6 章“COBIT 中的绩效管理”。 2. 记录对当前治理组件如何切实解决之前选定的管理实践的理解。请参阅《*COBIT® 2019 设计指南*》步骤 2 和 3。 3. 分析当前的能力水平。请参阅《*COBIT® 2019 设计指南*》第 4 节步骤 4 以及《*COBIT® 2019 框架：简介和方法*》第 6 章“COBIT 中的绩效管理”。 4. 定义当前的流程能力评级和其他组件的绩效水平。请参阅《*COBIT® 2019 设计指南*》第 4 节步骤 4 以及《*COBIT® 2019 框架：简介和方法*》第 6 章“COBIT 中的绩效管理”。
变革推行 (CE) 任务	成立强有力的实施团队： 1. 组建一支核心团队，由具备适当的知识、专业技术、履历、经验、信誉和权威的业务和 IT 人员组成，以推动举措的实施。确定最理想的人选（获得利益相关方信赖的高效领导者）来领导这支团队。考虑让外部相关方（如顾问）加入团队，以提供独立客观的观点或弥补可能存在的任何技能差距。 2. 识别并管理这支团队中可能存在的既得利益的情况，从而建立所需的信任环境。 3. 营造适宜的环境来优化团队合作，包括确保提供必要的时间和参与度。 4. 举办研讨会，在团队内达成共识（共同愿景），并对变革举措进行授权。 5. 利用级联支持的原则（在所有层级拥有支持愿景的支持者，沟通速效方案，向下级联变革，以及与可能存在的任何阻拦者和质疑者合作）确定核心团队可以与之合作的变革推动者。这有助于确保在生命周期的每个阶段都获得广泛的利益相关方支持。 6. 记录在现状评估期间确定的有助于推动积极沟通的优势，以及从变革推行的角度来看可加以利用的潜在速效方案。
计划管理 (PM) 任务	定义问题和机遇： 1. 审查和评估业务案例大纲、计划可行性和潜在的投资回报 (ROI)。 2. 分配角色、职责和流程所有权。确保获得受影响的利益相关方对制定和执行计划的承诺和支持。 3. 识别挑战和成功因素。
输入	• 业务案例大纲 • 高层次角色和职责 • 已确定的利益相关方图，包括所需的支持和参与、影响力和受到的影响，以及实施或支持变革的就绪情况和能力 • 计划的“警钟”（所有利益相关方） • 计划的启动沟通（关键利益相关方） • 业务和 IT 计划及战略 • IT 流程描述、政策、标准、程序、技术规范 • 了解业务和 IT 贡献 • 审计报告、风险管理政策、IT 绩效报告/仪表盘/计分卡 • 业务连续性计划 (BCP)、影响分析、监管要求、企业架构、服务水平协议 (SLA) 和运营水平协议 (OLA) • 投资计划和项目组合、计划及项目规划、项目管理方法、项目报告

图 6.7—第 2 阶段的目标、描述、任务、输入、资源和输出（续）	
第 2 阶段描述 – 现在到了什么程度?	
输出	• 商定的一致性目标和对 I&T 的影响 • 对一致性目标不一致，无法交付服务或项目，造成的风险和影响达成共识 • 选定的治理和管理目标 • 选定的治理和管理目标的当前绩效水平，包括流程能力级别 • 风险接受立场和风险概况 • 效益/价值实现风险以及计划/项目交付和服务交付/IT 运营风险的评估 • 奠定基础优势 • 企业不同部门和不同层级的变革推动者 • 核心团队及分配的角色和职责 • 已评估的业务案例大纲 • 对问题和挑战（包括流程能力级别）达成共识
ISACA 资源	• *《COBIT® 2019 框架：简介和方法》*（治理和管理目标、目标级联、企业目标与一致性目标级联），*www.isaca.org/cobit* • *《COBIT® 2019 框架：治理和管理目标》*（APO01、APO02、APO05、APO12、BAI01、BAI11、MEA01、MEA02、MEA03、MEA04，用于流程选择和流程能力评估，以及实施和计划规划） • 本出版物第 5 章“推行变革” • 当前在 *www.isaca.org* 列出的支持 ISACA 的产品

图 6.8—第 2 阶段 RACI 矩阵

关键活动	实施人员的职责：董事会	I&T 治理委员会	CIO	业务高管	IT 经理	IT 流程所有者	IT 审计	风险与合规性	计划指导
确定支持业务目标的关键 IT 目标 (CI1)。	I	C	R	C	R	C	C	C	A
确定对支持 IT 和业务目标至关重要的流程 (CI4)。		I	R	C	R	C	C	C	A
评估与目标实现相关的风险 (CI5)。		I	R	C	R	R	C	R	A
确定对规避重大风险至关重要的流程 (CI6)。		I	R	R	R	C	C	R	A
评估关键流程的当前绩效（CI1 至 CI11）。		I	R	C	R	R	C	C	A
组建由业务和 IT 人员组成的核心团队 (CE1)。		I	R	R	C	C	C	C	A
审查和评估业务案例 (PM1)。	I	A	R	R	C	C	C	C	R

RACI 矩阵确定谁是执行人、责任人、咨询人以及知情人。

6.4 第 3 阶段 — 我们想要达到什么目标?

图 6.9—第 3 阶段 — *我们想要达到什么目标?*

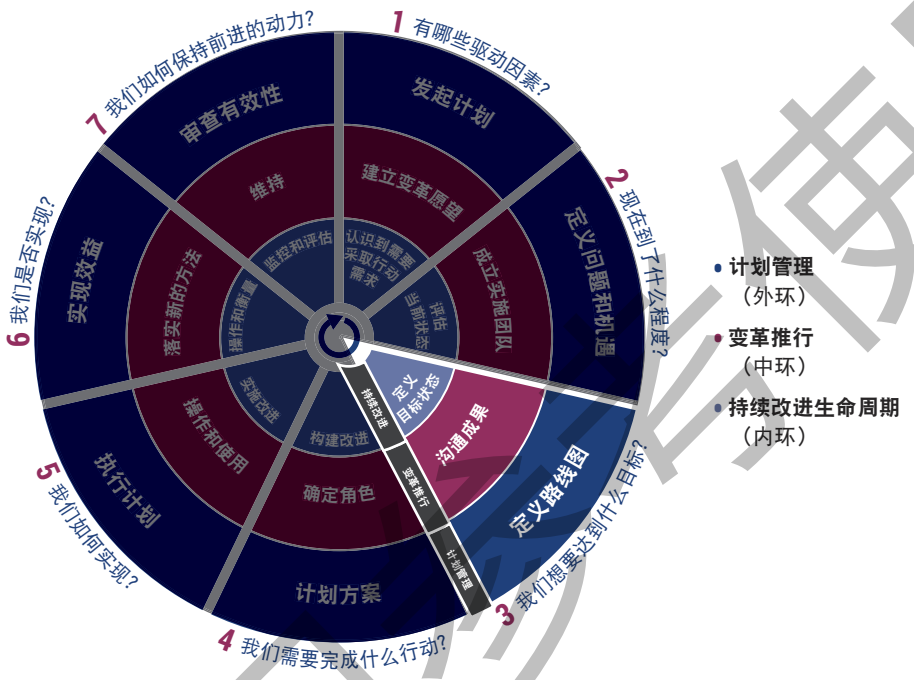


图 6.10—第 3 阶段的角色

如果您是.....	您在本阶段的角色是.....
董事会和执行管理层	设定 I&T 未来能力需求的优先级、时间范围和期望。
业务管理层	协助 IT 部门设定能力目标。确保设想的解决方案与企业目标保持一致。
IT 管理层	运用专业判断来制定优先的改进计划和举措。就所需的能力目标达成共识。确保设想的解决方案与一致性目标保持一致。
内部审计	提供建议并协助设定目标状态和差距优先级。必要时独立验证评估结果。
风险、合规及法律	审查计划，确保风险、合规及法律问题得到恰当的解决。

图 6.11—第 3 阶段的目标、描述、任务、输入、资源和输出	
第 3 阶段描述 – 我们想要达到什么目标?	
阶段目标	确定每个选定的治理和管理目标中的流程目标能力。确定选定流程的现状与理想状态之间的差距，并将这些差距转化为改进机会。使用此信息制定详细的业务案例和高层次的计划方案。
阶段描述	根据已评估的当前流程能力级别、之前执行的企业目标与一致性目标分析的结果以及已确定的流程重要性，为各个流程确定合适的目标能力级别。选择级别时应考虑可用的内部和外部基准。确保所选级别与业务相称，这一点很重要。 确定当前流程能力并设定目标能力之后，应评估现状与未来理想状态之间的差距并识别改进机会。确定差距之后，应确定根本原因、常见问题、剩余风险、现有优势以及弥合上述差距的良好实践。 这一阶段可能会识别出一些相对容易实现的改进措施，例如加强培训、分享良好实践以及标准化程序。但是，差距分析可能要求组织在业务和 IT 管理技术方面拥有丰富的经验，才能制定出切实可行的解决方案。此外，还要求组织在行为和组织变革方面具备一定的经验。 组织可能需要了解流程技术、高级业务和专业技术，以及业务和系统管理软件应用程序和服务。为确保有效执行这个阶段，团队应与业务和 IT 流程所有者以及其他利益相关方开展合作，充分运用内部的专业知识。必要时应寻求外部建议。另外，组织应识别弥合差距之后仍不能缓解的风险，并且应获得管理层的正式接受。
持续改进 (CI) 任务	下述 CI 任务 1 和 2 可基于《*COBIT® 2019 设计指南*》所述的治理系统设计方法的结果开展，尤其是治理系统设计工作流程的步骤 4（包括步骤 4.1“解决固有的优先级冲突”和步骤 4.2“最终确定治理系统的设计”）。此步骤概述了如何对治理系统组件的目标能力和绩效水平作出明智且有据可依的决策，相当于以下 CI 任务。 1. 定义改进目标： ● 根据企业的绩效和一致性要求，确定每个流程的初始能力级别以及理想的短期和长期目标能力级别。 ● 在可能的范围内进行内部基准检测，确定可采用的更好实践。 ● 在可能的范围内进行外部基准检测（与竞争对手和同行），帮助确定所选目标级别的适当性。 ● 对目标级别（单独和整体）的合理性执行“完整性”检查，确定可实现的级别和理想级别，以及在所选时间范围内可产生最大积极影响的级别。 2. 差距分析： ● 了解当前能力（按属性）并将其与目标能力级别进行比较。 ● 尽可能利用现有优势来弥补差距。关于如何弥补其他差距，请参阅 COBIT 管理实践和活动以及有关的良好实践和标准，例如 ITIL®、ISO/IEC 27000、开放组架构框架 (TOGAF®) 以及项目管理知识体系 (PMBOK®)。 ● 寻找存在深层次原因的情况。 3. 识别潜在改进： ● 将差距整合到潜在改进中。 ● 识别未缓释的剩余风险并确保其被正式接受。

图 6.11—第 3 阶段的目标、描述、任务、输入、资源和输出（续）	
第 3 阶段描述 – 我们想要达到什么目标?	
变革推行 (CE) 任务	描述并沟通预期成果： 1. 描述高层次的变革推行计划和目标，其中包括以下任务和组件。 2. 制定沟通战略来提高认识和赢取支持。该战略应包括核心受众群体、每个群体的行为概况和信息需求、核心信息，以及最佳沟通渠道和沟通原则。 3. 确保参与意愿（变革蓝图）。 4. 阐明变革的理由和益处，以支持愿景。描述不进行变革的影响（变革的目的）。 5. 在沟通中关联举措的目标，并展示变革将如何兑现益处。 6. 描述实现愿景的高层次路线图（变革计划）以及所需的各利益相关方的参与（变革中的角色）。 7. 通过高级管理层传达关键信息，在高层确定工作基调。 8. 除正式沟通外，通过变革推动者进行非正式沟通。 9. 在行动中沟通。指导团队应起到示范作用。 10. 调动人员情绪，必要时鼓励他们改变行为。 11. 获取初始沟通反馈（反应和建议）并相应地调整沟通战略。
计划管理 (PM) 任务	定义路线图： 1. 设定更高层面的计划方向、范围、效益和目标。 2. 确保目标与业务和 IT 战略保持一致。 3. 考虑风险并相应地调整范围。 4. 考虑变革推行的影响。 5. 获得必要的预算并定义计划的责任及问责制。 6. 创建和评估详细的业务案例、预算、时间线和高层次的计划方案。
输入	• 商定的企业目标和对一致性目标的影响 • 选定流程的当前能力级别 • 一致性目标的定义 • 选定的流程和目标 • 风险接受立场和风险概况 • 已评估的效益/价值实现风险，以及计划/项目交付和服务交付/IT 运营风险评估 • 奠定基础优势 • 企业不同部门和不同层级的变革推动者 • 核心团队及分配的角色和职责 • 已评估的业务案例大纲 • 挑战和成功因素 • 内部和外部能力基准 • 来自 COBIT 和其他参考文献的良好实践 • 利益相关方分析
输出	• 选定流程的目标能力级别 • 改进机会的描述 • 风险响应文档，包括未得到缓解的风险 • 变革推行计划和目标 • 变革愿景的沟通战略和沟通，包括四个“P”（蓝图、目的、计划、组成） • 详细的业务案例 • 高层次的计划方案 • 用于跟踪计划和运行情况的关键指标
ISACA 资源	• *《COBIT® 2019 框架：简介和方法》*（企业目标），*www.isaca.org/cobit* • *《COBIT® 2019 框架：治理和管理目标》*（针对目标状态定义和差距分析的管理实践和活动，APO01、APO02） • 当前在 *www.isaca.org* 列出的支持 ISACA 的产品

图 6.12—第 3 阶段 RACI 矩阵

关键活动	董事会	I&T 治理委员会	CIO	业务高管	IT 经理	IT 流程所有者	IT 审计	风险与合规性	计划指导
	实施人员的职责								
商定改进目标 (CI1)。	I	A	R	C	R	R	C	C	R
分析差距 (CI2)。		I	R	C	R	R	C	C	A
识别潜在改进 (CI3)。		I	R	C	R	R	C	C	A
沟通变革愿景 (CE3)。		A	R	R	C	I	I	I	R
设定计划方向并准备详细的业务案例（PM1、PM6）	I	A	R	C	C	C	I	I	R

RACI 矩阵确定谁是执行人、责任人、咨询人以及知情人。

6.5 第 4 阶段 — 我们需要完成什么行动?

图 6.13—第 4 阶段 — *我们需要完成什么行动?*

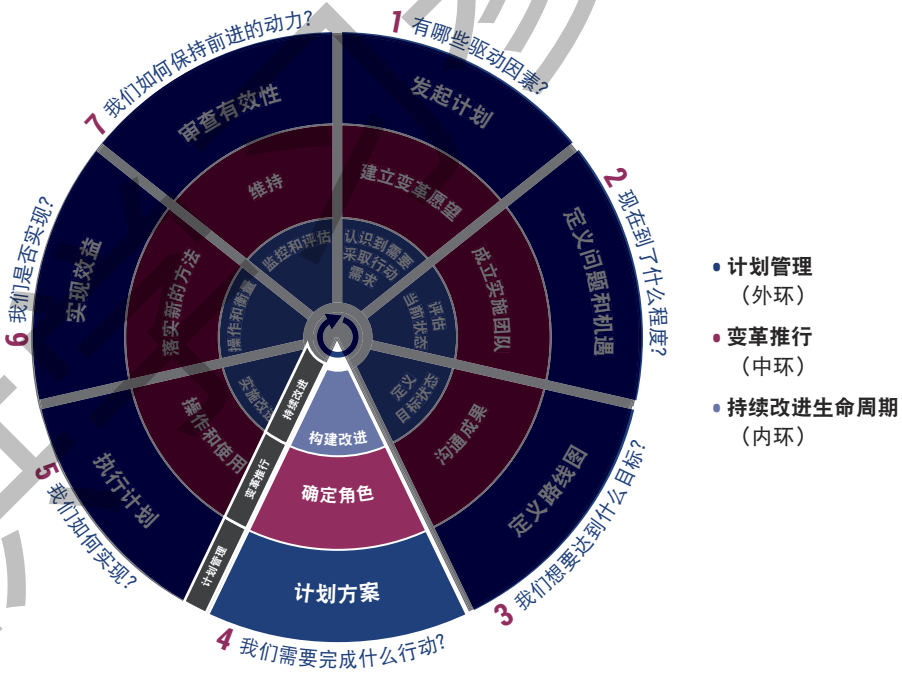


图 6.14—第 4 阶段角色	
如果您是……	**您在本阶段的角色是……**
董事会和执行管理层	考虑并审查建议书，支持合理的行动，提供预算，以及合理设定优先级。
业务管理层	与 IT 部门一起确保建议的改进措施与商定的企业和 IT 相关目标保持一致，并确保业务部门支持任何需要其提供输入或采取行动的活动。确保分配和提供所需的业务资源。与 IT 部门就衡量改进计划成果的指标达成共识。
IT 管理层	确保计划方案的可行性和合理性。确保计划可实现，并且有资源来执行计划。综合考虑计划和 I&T 赋能的企业投资组合的优先级，为投资决策提供依据。
内部审计	提供独立鉴证，确保有效地识别问题，客观和准确地展示业务案例，以及计划是可实现的。在适当的情况下提供专家建议和指导。
风险、合规及法律	确保已识别的任何风险、合规及法律问题得到解决，并且建议书符合任何相关政策或法规的要求。

图 6.15—第 4 阶段的目标、描述、任务、输入、资源和输出	
第 4 阶段描述 – 我们需要完成什么行动?	
阶段目标	将改进机会转化为合理的促进项目。优先考虑并重点关注高影响力的项目。将改进项目整合到总体计划方案中。执行速效方案。
阶段描述	确定所有潜在的改进举措之后，应确定优先顺序并转化为正式且合理的项目。优先选择效益高且易于实施的项目，并将其转化为正式且合理的项目。为每个项目制定一份项目计划，包括项目对计划目标的贡献。确认目标是否仍符合最初的价值和风险驱动因素，这一点非常重要。这些项目将包含在该计划经过更新的业务案例中。应在登记表中记录任何未经批准的项目建议书的详细信息，以供将来参考。发起人可以重新评估，适当情况下也可在日后重新提交新的建议。 根据机会网格、项目定义、资源计划和 I&T 预算，将已识别且确定优先级的改进转化为一系列有文档记录的可支持整体改进计划的项目。确定执行计划对企业的影响，并制定变革计划来描述计划中的活动，这些活动将确保以可持续的方式在企业中落实项目带来的改进。这个阶段的一个重要元素是指标的定义，即计划的成功指标，用于衡量流程改进是否可以实现预期的业务效益。应以甘特图的形式记录完整的改进计划时间表。 新项目可能会识别出需要改变或优化组织结构或其他动力，以维持有效的治理。必要时应包括改进环境的行动（如第 5 章所述）。

图 6.15—第 4 阶段的目标、描述、任务、输入、资源和输出 （续）	
第 4 阶段描述 – 我们需要完成什么行动?	
持续改进 (CI) 任务	设计和构建改进： **1.** 考虑每项改进的潜在效益和实施难度（成本、工作量和可持续性）。 **2.** 在机会网格上绘制改进图，以确定优先行动（基于效益和实施难度）。 **3.** 关注效益高/易于实施的替代方案。 **4.** 针对规模较小的改进措施，考虑采用效益高/实施难度低的替代方案。将它们分解为更小的改进措施，并再次审视效益和实施难度。 **5.** 确定改进的优先级并加以选择。 **6.** 分析选定的改进，详细程度与高层次的项目定义相称。考虑方法、交付成果、所需资源、预计成本、预计时间范围、依存关系和项目风险。通过可用的良好实践和标准进一步完善详细的改进要求。与负责流程领域的经理和团队讨论。 **7.** 思考可行性，并回溯到最初的价值与风险驱动因素。对纳入待审批商业案例的项目清单达成共识。 **8.** 将未批准的项目和举措记录在登记表中，以供将来参考。
变革推行 (CE) 任务	为角色授权并确定速效方案： **1.** 通过研讨会或审查流程等机制获得受影响用户的支持。请他们负责质量验收。 **2.** 设计变革响应计划，以主动管理变革影响并最大限度地提高整个实施过程中的参与度。这可能包括组织变革，例如工作内容或组织结构；人员管理变革，如培训；绩效管理系统；或激励/薪酬和奖励系统。 **3.** 确定能够证明改进计划概念的速效方案。这些方案应是有形且明确的，能够创造动力，并可帮助加强流程管控。 **4.** 以第 2 阶段确定的任何现有优势为基础，尽可能实现速效方案。 **5.** 确定现有企业流程中可加以利用的优势。例如，项目管理的优势可能存在于其他业务领域，例如产品开发。避免另起炉灶，尽可能与当前的企业级方法保持一致。
计划管理 (PM) 任务	制定计划方案： **1.** 按优先顺序将潜在项目整合到总体计划中，并考虑这些项目对预期成果、资源要求和依存关系的贡献。 **2.** 使用组合管理技术确保计划与战略目标保持一致，并且拥有一系列均衡的 I&T 举措。 **3.** 确定改进计划对 IT 和业务组织的影响，并指出如何保持改进动力。 **4.** 制定变革计划，记录任何必须纳入计划并作为其组成部分来实施的迁移、转换、测试、培训、流程或其他活动。 **5.** 根据原始计划成功因素，确定用于衡量改进计划成果的指标并达成一致意见。 **6.** 指导实现计划和项目目标所需的业务、IT 和审计资源的分配和优先顺序。 **7.** 定义能够实现所需的计划成果的项目组合。 **8.** 确定所需的交付成果，考虑实现目标所需的全部活动。 **9.** 必要时，为计划中的特定项目成立项目指导委员会。 **10.** 通过制定项目计划和报告程序，监控项目进度。

图 6.15—第 4 阶段的目标、描述、任务、输入、资源和输出（续）

第 4 阶段描述 – 我们需要完成什么行动?	
输入	• 选定流程的目标成熟度级别 • 改进机会的描述 • 风险应对文档 • 变革推行计划和目标 • 变革愿景的沟通战略和沟通，包括四个 "P"（蓝图、目的、计划、组成） • 详细的业务案例 • 机会工作表、良好实践和标准、外部评估、技术评估 • 机会网格、项目定义、项目组合管理计划、资源计划、I&T 预算 • 在较早阶段识别的优势
输出	• 改进项目的定义 • 制定的变革响应计划 • 已识别的速效方案 • 未批准的项目记录 • 根据分配的资源、优先级和交付成果对各个计划进行排序的计划方案 • 通过技能和投资等承诺的资源实现的项目计划和报告程序 • 成功指标
ISACA 资源	• *《COBIT® 2019 框架：简介和方法》*（治理和管理目标、治理系统的组件），*www.isaca.org/cobit* • *《COBIT® 2019 框架：治理和管理目标》*（APO5、APO12、BAI01、BAI11、目标和指标） • 当前在 *www.isaca.org* 列出的支持 ISACA 的产品

图 6.16—第 4 阶段 RACI 矩阵

关键活动	董事会	I&T 治理委员会	CIO	业务高管	IT 经理	IT 流程所有者	IT 审计	风险与合规性	计划指导
	实施人员的职责								
确定改进的优先级并加以选择 (CI5)。		A	R	C	C	R	C	C	R
定义项目并证明合理性（CI6 和 CI7）。		I	R	C	R	R	C	C	A
设计变革响应计划 (CE2)。		I	R	R	C	C	C	C	A
确定速效方案并利用现有优势 (CE3)。		I	C	C/I	R	R	C/I	C/I	A
制定包含已分配资源和项目计划的计划方案（PM1 至 PM10）。		A	C	C	R	C	I	I	R

RACI 矩阵确定谁是执行人、责任人、咨询人以及知情人。

6.6 第 5 阶段 — 我们如何实现?

图 6.17—第 5 阶段 — *我们如何实现?*

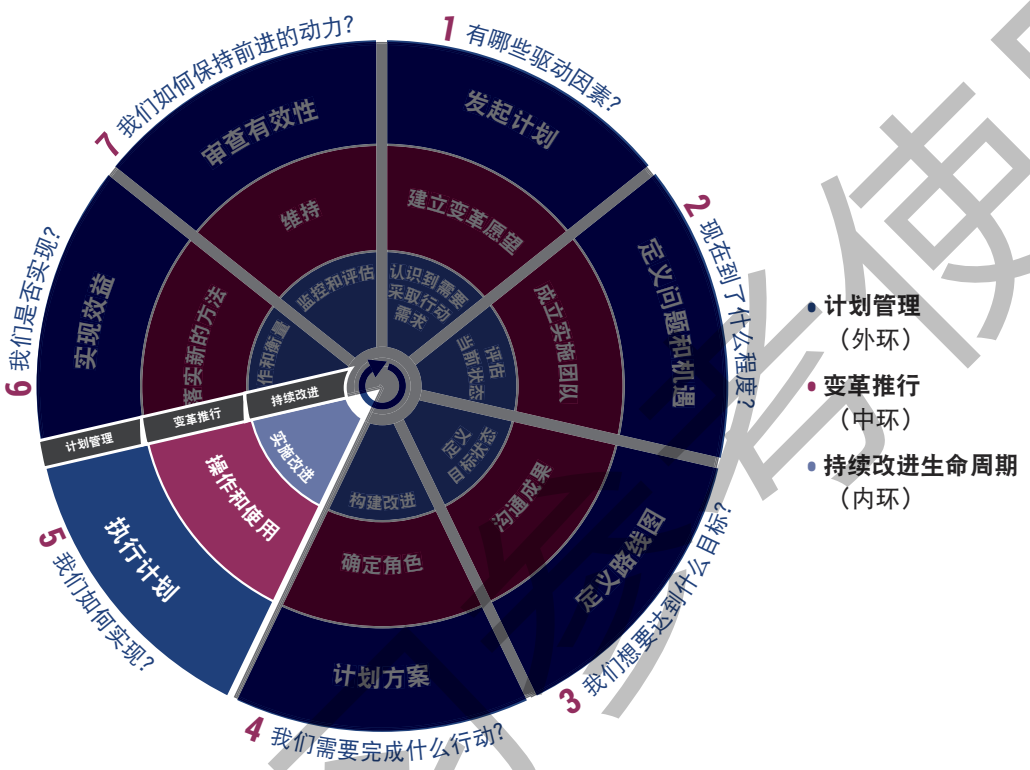


图 6.18—第 5 阶段的角色

如果您是.....	您在本阶段的角色是.....
董事会和执行管理层	监控实施，必要时提供支持和指导。
业务管理层	负责业务部门参与的实施内容，尤其是在业务流程受影响且 IT 流程需要用户/客户参与的情况下。
IT 管理层	确保实施过程涵盖所需的全部活动（例如政策和流程变更、技术解决方案、组织变革、新的角色和职责或其他动力）；确保实施内容是切实可行的，并且可能被采用和使用。确保流程所有者参与其中、支持新方法并负责最终建立的流程。解决问题并管理实施过程中遇到的风险。
内部审计	在实施过程中提供审查和意见，避免事后才发现缺失的动力，尤其是关键控制。提供关于控制实施方面的指导。必要时提供项目/实施风险审查服务，监控可能危及实施的风险并向计划和项目团队提供独立的反馈。
风险、合规及法律	在实施过程中提供风险、合规及法律方面的指导。

图 6.19—第 5 阶段的目标、描述、任务、输入、资源和输出	
第 5 阶段描述 — 我们如何实现?	
阶段目标	运用企业计划，项目管理能力、标准和实践来实施详细的改进项目。监控、衡量和报告项目进度。
阶段描述	到此阶段，获得批准的改进项目（包括所需的变革活动）已做好实施准备，可以购置或开发计划所定义的解决方案并在企业中实施。这样一来，项目成为常规开发生命周期的一部分，并且应采用既定的计划和项目管理方法进行治理。解决方案的推行应与既定的项目定义和变革计划保持一致，以支持改进的可持续性。 在所有生命周期阶段中，这一阶段包含的工作量通常最大且耗时最久。另外，务必确保此阶段是可管理的，并且可以在合理的时间范围内实现效益，从而避免规模过大和总耗时过长。对前几次迭代而言尤其如此，这对所有参与的人员来说也是一次学习经历。 必须监控每个项目的绩效，确保实现目标。定期向利益相关方报告，确保其了解项目进展并且没有偏离轨道。
持续改进 (CI) 任务	实施改进： **1.** 开发涵盖所需全部活动的解决方案，必要时可以购置。这些活动可能包括文化、道德和行为；组织结构；原则和政策；流程；服务能力；技能和能力；以及信息。 **2.** 采用并调整可用的指南来执行良好实践，以适应企业的政策和流程。 **3.** 测试解决方案在实际工作环境中的实用性和适用性。 **4.** 推行解决方案，并考虑现有的流程和迁移要求。
变革推行 (CE) 任务	启用操作和使用： **1.** 借助速效方案带来的动力和信心，引入更广泛和更具挑战性的变革工作。 **2.** 宣传速效方案取得的成功，并表彰和奖励参与的人员。 **3.** 实施变革响应计划。 **4.** 确保更多的角色群体拥有所需的技能、资源和知识，并获得他们对变革的支持和承诺。 **5.** 平衡团体和个人干预，确保关键利益相关方对变革形成全面的认识。 **6.** 制定在文化和行为习惯方面更深入的改进计划（处理对缺失责任/独立性/决策权以及接受新期望和未知任务的担忧）。 **7.** 沟通采用的角色和职责。 **8.** 定义衡量成功的指标，包括业务视角和感知视角的衡量指标。 **9.** 提供辅导和指导，确保获得理解和支持。 **10.** 结束工作循环并确保所有变革要求已得到解决。 **11.** 监控变革推行的有效性，必要时采取纠正措施。
计划管理 (PM) 任务	执行计划： **1.** 确保计划的执行是基于对计划内各个项目的最新整合（业务和 IT）规划。 **2.** 指导和监控计划中所有项目的贡献，确保实现预期成果。 **3.** 定期向利益相关方报告，确保其了解项目进展并且没有偏离轨道。 **4.** 记录和监控重大的计划风险和问题，并商定补救措施。 **5.** 批准每个主要计划阶段的启动并与所有利益相关方沟通。 **6.** 批准针对计划和项目计划的所有重大变更。

图 6.19—第 5 阶段的目标、描述、任务、输入、资源和输出（续）

第 5 阶段描述 – 我们如何实现?	
输入	• 改进项目的定义 • 制定的变革响应计划 • 已识别的速效方案 • 未批准的项目记录 • 包含分配的资源、优先级和交付成果的计划方案 • 项目计划和报告程序 • 成功指标 • 项目定义、项目甘特图、变革响应计划、变革战略 • 整合的计划和项目规划
输出	• 已实施的改进 • 已实施的变革响应计划 • 已实现的速效方案和有形的成功变革 • 成功的沟通 • 常规业务环境中已定义和沟通过的角色和职责 • 项目变更日志和问题/风险日志 • 已定义的业务和感知方面的成功衡量指标 • 通过持续监控实现过程所获取的效益
ISACA 资源	• *《COBIT® 2019 框架：治理和管理目标》*（所有目标作为良好实践的输入，BAI01、BAI11），*www.isaca.org/cobit* • 当前在 *www.isaca.org* 列出的支持 ISACA 的产品

图 6.20—第 5 阶段 RACI 矩阵

关键活动	实施人员的职责								
	董事会	I&T 治理委员会	CIO	业务高管	IT 经理	IT 流程所有者	IT 审计	风险与合规性	计划指导
开发解决方案，必要时可以购置 (CI1)。		A	C	C	R	R	C	C	R
采纳并调整良好实践 (CI2)。		I	R	C	R	R	C	C	A
测试并推行解决方案（CI3 和 CI4）。		I	R	C	R	R	C	C	A
利用速效方案（CE1 和 CE2）。		I	C	C/I	R	R	C/I	C/I	A
实施变革响应计划 (CE3)。	I	I	R	C	R	R	I	I	A
指导和监控计划中的项目 (PM2)。	I	A	C	C	R	C	I	I	R

RACI 矩阵确定谁是执行人、责任人、咨询人以及知情人。

6.7 第 6 阶段 — 我们是否实现?

图 6.21—第 6 阶段 — *我们是否实现?*

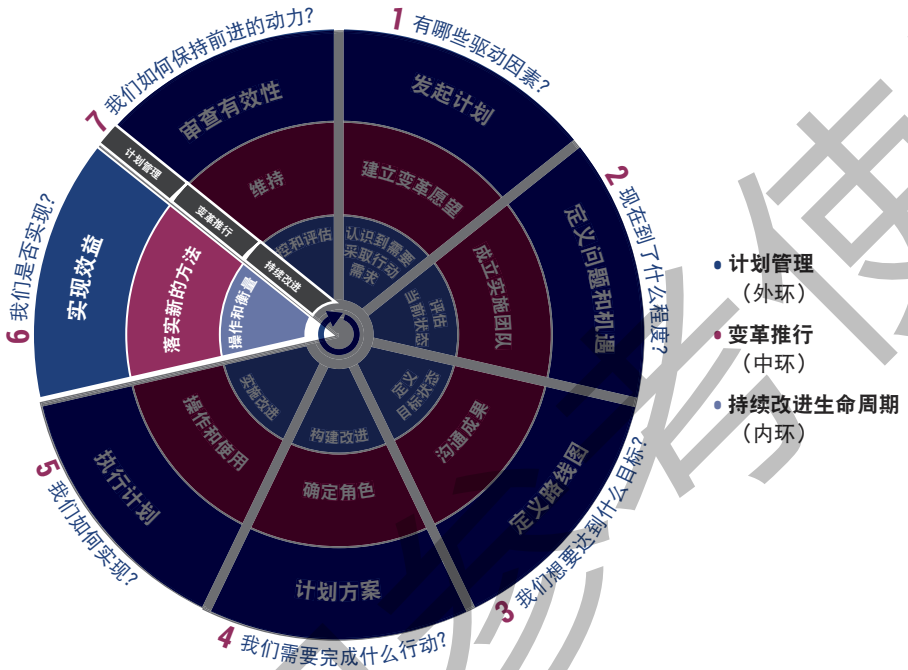


图 6.22—第 6 阶段的角色

如果您是.....	您在本阶段的角色是.....
董事会和执行管理层	评估实现原始目标的绩效并确认是否实现了期望的结果。考虑是否需要重新确定未来活动的方向并采取更正行动。必要时协助解决重大问题。
业务管理层	提供反馈并考虑业务对举措的贡献度。运用积极的成果来改善当前的业务相关活动。利用经验教训来调整和改进业务部门实施未来举措的方法。
IT 管理层	提供反馈并思考 IT 对举措的贡献度。运用积极的成果来改善当前的 IT 相关活动。在项目过程中采用计划管理和项目管理技术，根据项目的关键性对其进行监控。做好充分准备，在早期迹象表明项目已偏离轨道且可能无法达成关键的里程碑时更改计划或取消一个或多个项目，或采取其他纠正措施。利用经验教训来调整和改进 IT 部门实施未来举措的方法。
内部审计	对举措的总体效率和有效性进行独立的评估。提供反馈并思考审计对举措的贡献的有效性。运用积极的成果来改善当前的审计相关活动。利用经验教训来调整和改进审计部门实施未来举措的方法。
风险、合规及法律	评估举措是否提高了企业识别和管理风险以及法律、法规和合同要求的能力。提供反馈和任何必要的改进建议。

图 6.23—第 6 阶段的目标、描述、任务、输入、资源和输出	
第 6 阶段描述 – 我们如何实现?	
阶段目标	将整体治理改进计划的项目绩效和效益实现指标整合到绩效衡量系统中，以进行定期和持续的监控。
阶段描述	必须采用适当的技术（如 IT 平衡计分卡 [BSC] 和效益登记表），通过对照一致性目标和流程目标，监控计划中所描述的改进，确认是否实现了变革成果。这可以确保举措不会偏离轨道且符合最初的企业目标和一致性目标，并继续实现预期的业务效益。务必针对每个指标设定目标，定期与实际情况进行比较，并通过绩效报告进行沟通。 为确保成功，务必向所有利益相关方报告绩效衡量的积极和消极结果，以建立信心并及时采取任何纠正措施。在项目过程中，应采用计划管理和项目管理技术对项目进行监控。做好充分准备，在早期迹象表明项目已偏离轨道且可能无法达成关键的里程碑时更改计划或取消项目。
持续改进 (CI) 任务	操作和衡量： 1. 为各项指标设定商定时间段内的目标。目标应有助于监控 I&T 绩效和改进措施，以及确定成功或失败。 2. 在可能的情况下，获得这些指标的当前实际衡量值。 3. 收集实际衡量值并定期（例如每个月）与目标进行比较。调查任何重大差异。 4. 如果差异表明需要进行纠正，制定和商定建议的纠正措施。 5. 必要时基于经验调整长期目标。 6. 向所有相关的利益相关方沟通绩效监控的正面和负面结果，并提出纠正措施建议。
变革推行 (CE) 任务	落实新的方法： 1. 确保新的工作方式成为企业文化的一部分。它们应植根于企业的常态和价值观中。这对取得切实成果非常重要。 2. 在从项目模式到业务的过渡期间，通过修订工作说明、工作绩效标准、相关的激励和奖励系统、KPI 以及通过变革响应计划实施的运营程序来塑造行为。 3. 监控分配的角色和职责是否得到落实。 4. 跟踪变革并评估变革响应计划的有效性，将结果与最初的变革目的和目标联系起来。这包括定量业务指标和定性感知指标，如感知调查、反馈会议和培训评估表。 5. 利用局部的卓越成果寻求更多灵感。 6. 维护沟通战略，以培养持续的意识并强调取得的成功。 7. 确保所有角色之间保持开放的沟通以解决问题。 8. 将无法解决的问题上报至发起人。 9. 必要时通过管理权力来强制执行变革。 10. 记录变革推行期间的经验教训，以用于未来的实施举措。
计划管理 (PM) 任务	实现效益： 1. 根据业务案例目标监控计划的总体绩效。 2. 监控投资绩效（成本与预算的比较、效益的实现）。 3. 记录（正面和负面的）经验教训，以用于后续改进举措。

图 6.23—第 6 阶段的目标、描述、任务、输入、资源和输出（续）

第 6 阶段描述 – 我们如何实现？	
输入	• 已实施的改进 • 已实施的变革响应计划 • 已实现的速效方案和所取得成功的沟通 • 常规业务环境中已定义和沟通过的角色和职责 • 项目变更日志和问题/风险日志 • 已定义的业务和感知方面的成功衡量指标 • 需求分析中确定的一致性目标和 IT 流程目标 • 现有的衡量指标或计分卡 • 业务案例的效益 • 变革响应计划和沟通战略
输出	• 已更新的项目和计划计分卡 • 变革有效性的衡量指标（业务和感知方面） • 说明计分卡结果的报告 • 在运营中巩固的改进 • 添加到持续 IT 绩效衡量方法的关键指标
ISACA 资源	• *《COBIT® 2019 框架：治理和管理目标》*（作为良好实践输入，EDM05、APO05、BAI01、BAI11、MEA01），*www.isaca.org/cobit* • 当前在 *www.isaca.org* 列出的支持 ISACA 的产品

图 6.24—第 6 阶段 RACI 矩阵

关键活动	实施人员的职责：董事会	I&T 治理委员会	CIO	业务高管	IT 经理	IT 流程所有者	IT 审计	风险与合规性	计划指导
执行解决方案并获得绩效反馈（CI1 至 CI3）。		I	A	R	R	R	I	I	I
根据成功指标监控绩效（CI4 至 CI5）。		I	A	C	R	R	C	C	I
沟通积极和消极结果 (CI6)。	I	I	A	C	R	C	I	I	I
监控角色和职责的落实 (CE3)。		A	R	C	C	C	C	C	I
监控计划结果（目标和效益的实现情况）（PM1 和 PM2）。	I	A	C	C	C	C	C	C	R

RACI 矩阵确定谁是执行人、责任人、咨询人以及知情人。

6.8 第 7 阶段 — 我们如何保持前进的动力?

图 6.25—第 7 阶段 — *我们如何保持前进的动力?*

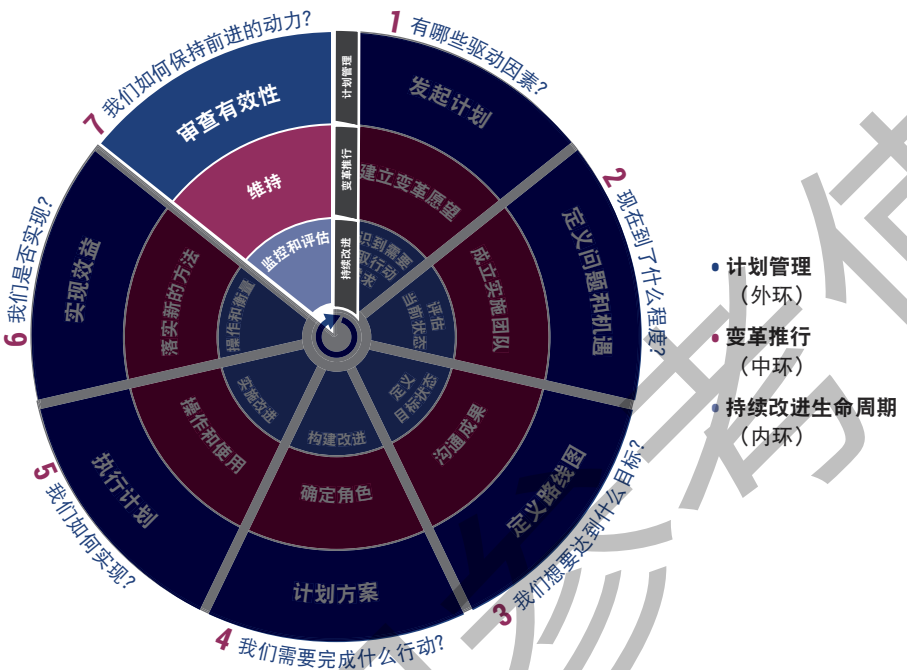


图 6.26—第 7 阶段的角色	
如果您是.....	**您在本阶段的角色是.....**
董事会和执行管理层	为企业持续使用和改进 EGIT 方法提供方向、设定目标以及分配角色和职责。继续在高层确定工作基调，发展组织结构，以及在业务和 IT 高管间推行良好的 I&T 治理和问责制文化。确保 IT 部门尽可能及时地了解并适当参与新的业务目标和要求。
业务管理层	继续与 IT 部门保持积极合作，提供支持并承诺会改进 EGIT 并将其转变为常规事项。验证新的 EGIT 目标是否与当前的企业目标保持一致。
IT 管理层	推动并提供强有力的领导，以保持改进计划的动力。参与治理活动并将其作为常规业务实践的一部分。制定政策、标准和流程，确保将治理转变为常规业务活动。
内部审计	提供客观且具有建设性的意见，鼓励自我评估，并向管理层保证治理得到有效运行，从而建立对 I&T 的信心。采用 IT 和业务部门基于 COBIT® 2019 框架而共同适用的标准，提供以综合治理为基础的持续性审计服务。
风险、合规及法律	与 IT 和业务部门合作，预测法律和监管要求。作为 EGIT 的一项常规活动，识别和应对 I&T 相关风险。

图 6.27—第 7 阶段的目标、描述、任务、输入、资源和输出	
第 7 阶段描述 – 我们如何保持前进的动力?	
阶段目标	评估从计划中获得的结果和经验。记录并分享所有经验教训。改进组织结构、流程、角色和职责，以改变企业行为，使 EGIT 成为一项常规业务活动并得到持续优化。确保新的必要行动可以进一步推动生命周期的迭代。 持续监控绩效并确保定期报告结果。获得承诺并落实所有职责和责任。
阶段描述	在此阶段，团队可以确定能否按预期实现计划。为此，可以将结果与最初的成功标准进行比较，或通过访查、研讨会和满意度调查收集实施团队和利益相关方的反馈。经验教训中可能包含对团队成员和项目利益相关方有价值的信息，以便应用于持续进行的举措和改进项目。它涉及持续监控、定期和透明的报告，以及责任确认。 确定进一步的改进并作为下一次生命周期迭代的输入。在此阶段，企业应借助治理实施项目的成果和经验教训，取得并巩固所有 IT 和业务利益相关方的承诺，以持续改进 I&T 治理。 应制定和优化政策、组织结构、角色和职责以及治理流程，使 EGIT 有效运行并成为常规业务实践的一部分，并且最高管理层所展示的文化支持这一点。
持续改进 (CI) 任务	监控和评估： **1.** 根据获得的经验、当前的 I&T 业务目标或其他触发事件确定新的治理目标和要求。 **2.** 收集反馈并开展利益相关方满意度调查。 **3.** 根据最初制定的项目成功衡量标准来衡量和报告实际结果。落实持续监控和报告。 **4.** 与项目团队成员和项目利益相关方一起执行引导式项目审查流程，以记录和传递经验教训。 **5.** 寻找其他影响大且成本低的机会，进一步改进 EGIT。 **6.** 总结经验教训。 **7.** 沟通和记录利益相关方的进一步改进需求，作为下一次生命周期迭代的输入。
变革推行 (CE) 任务	维持： **1.** 提供意识强化和持续沟通活动，并展现最高管理层的持续承诺。 **2.** 确保与目标和要求保持一致。 **3.** 持续监控变革本身的有效性、变革推行活动以及利益相关方的支持。 **4.** 必要时实施纠正行动计划。 **5.** 提供绩效反馈，奖励取得成就的人，以及宣传成功案例。 **6.** 吸取经验教训。 **7.** 在更广的企业范围分享从举措中获取的知识。
计划管理 (PM) 任务	审查计划有效性： **1.** 计划结束时，确保开展计划审查并批准结论。 **2.** 审查计划有效性。
输入	• 已更新的项目和计划计分卡 • 变革有效性的衡量指标（业务和感知方面） • 说明计分卡结果的报告 • 实施后审查报告 • 绩效报告 • 业务和 IT 战略 • 新的触发因素，例如新的监管要求

图 6.27—第 7 阶段的目标、描述、任务、输入、资源和输出 （续）	
第 7 阶段描述 – 我们如何保持前进的动力?	
输出	• 关于在一段时间的规范化后开展进一步的 EGIT 活动的建议 • 利益相关方满意度调查 • 记录的成功案例和经验教训 • 持续沟通计划 • 绩效奖励方案
ISACA 资源	• *《COBIT® 2019 框架：治理和管理目标》*（EDM01、APO01、BAI08、MEA01），*www.isaca.org/cobit* • 当前在 *www.isaca.org* 列出的支持 ISACA 的产品

图 6.28—第 7 阶段 RACI 矩阵

关键活动	实施人员的职责								
	董事会	I&T 治理委员会	CIO	业务高管	IT 经理	IT 流程所有者	IT 审计	风险与合规性	计划指导
确定新的治理目标 (CI1)。	C	A	R	R	C	C	C	C	I
总结经验教训 (CI2)。		I	A	C	R	R	C	C	I
维持和巩固变革 (CE1)。		A	R	R	R	R	C	C	I
确保与目标和要求保持一致 (CE2)。	I	A	R	C	R	R	R	I	R
通过正式的有效性审查关闭计划 (PM1)。	I	A	C	C	C	C	C	C	R

RACI 矩阵确定谁是执行人、责任人、咨询人以及知情人。

附录 A
决策矩阵示例

本附录提供了一个示例，展示了如何确定需要明确决策角色和职责的关键主题领域。它是指导性的，企业可以根据具体的组织和要求进行修改和调整。[14]

图 A.1—决策矩阵示例

决策主题	范围	执行人、责任人、被咨询人和知情人 (RACI)							
		执行委员会	I&T 治理委员会	企业风险委员会	组合经理	指导（计划/项目）委员会	IT 管理层[15]	业务流程所有者	员工
治理	• 与企业治理整合 • 制定原则、结构和目标	A/R	R	C			C	R	I
企业战略	• 定义企业目的和目标 • 确定 I&T 在何处以及如何帮助实现和支持企业目标	A/R	R	C			C	R	I
I&T 政策	• 向利益相关方提供准确、易于理解且经过批准的政策、程序、准则和其他文件 • 制定并推行 I&T 政策 • 确保政策根据指导原则产生有益成果 • 强制执行 I&T 政策	I	A	C			R	C	C
I&T 战略	• 结合 IT 和业务管理，将业务要求转化为服务产品，并制定战略，以透明和有效的方式交付这些服务 • 与业务部门和高级管理层合作，使 I&T 战略规划与当前和未来的业务需求保持一致 • 了解当前的 I&T 能力 • 为业务目标提供能够量化业务需求的优先级方案	I	A	C	I		R	C	C
I&T 方向	• 根据已定义的 I&T 架构和信息技术标准，提供合适的业务应用程序和服务平台 • 制定信息和技术供应计划	I	C	C			A/R	C	C

[14] 以下示例基于 IT Winners 开发的 EGIT 矩阵。此处使用已获得他们的许可。
[15] IT 管理层包括 IT 职能管理层级别的所有角色。

图 A.1—决策矩阵示例（续）									
		执行人、责任人、被咨询人和知情人 (RACI)							
决策主题	范围	执行委员会	I&T 治理委员会	企业风险委员会	组合经理	指导（计划/项目）委员会	IT 管理层[15]	业务流程所有者	员工
I&T 方法和框架	• 建立透明、灵活且响应快速的 IT 组织结构，并定义和实施 I&T 流程，将所有者、角色和职责整合到业务和决策流程中 • 定义切实可行的 I&T 流程框架 • 建立适当的组织主体和结构 • 定义角色和职责	I	C	C	I	I	A/R	I	I
企业架构	• 定义和实施能够识别并利用技术机会的架构和标准 • 建立一个论坛来指导架构并验证合规性 • 建立与成本、风险和需求相应的架构计划 • 定义信息结构，包括建立一个包含数据分类方案的企业数据模型 • 确保信息架构和数据模型的准确性 • 分配数据所有权 • 使用已商定的分类方案对信息进行分类	A	C	C	I	I	R	R	C
I&T 赋能的投资和组合的优先级确定	• 制定有效和高效的 I&T 赋能的投资和组合决策 • 预测并分配预算 • 制定正式的投资标准 • 根据预测衡量和评估业务价值	I	A		C	C	R		
I&T 赋能的投资和计划的优先级确定	• 根据 I&T 战略和投资决策设定和跟踪 I&T 预算 • 根据预测衡量和评估业务价值 • 定义应用于 I&T 赋能的业务项目的计划和项目管理方法，并使利益相关方能够参与并监控项目风险和进度 • 定义并实施计划和项目框架及方法 • 发布项目管理准则 • 为项目组合中详述的每个项目进行项目规划	I	A		R	C	C/I	C/I	C/I
管理、监控和评估 SLA	• 确定服务要求，就服务水平达成共识并监控服务水平的达成情况 • 根据要求和交付能力规范化内部和外部协议 • 报告服务水平的达成情况（报告和会议） • 确定并沟通新的和修订的战略规划服务要求 • 达到计划的数据处理、保护敏感输出以及监控和维护基础设施等方面的运营服务水平	I	A	R			R	R	I

[15] IT 管理层包括 IT 职能管理层级别的所有角色。

图 A.1—决策矩阵示例（续）

决策主题	范围	执行人、责任人、被咨询人和知情人 (RACI)							
		执行委员会	I&T 治理委员会	企业风险委员会	组合经理	指导（计划/项目）委员会	IT 管理层[15]	业务流程所有者	员工
IT 应用程序管理	• 确定技术上可行且具成本效益的解决方案 • 定义业务和技术要求 • 开展开发标准中定义的可行性研究 • 批准（或拒绝）要求及其可行性研究结果 • 确保拥有及时且具成本效益的开发或采购流程 • 将业务要求转化为设计规范 • 选择适当的开发和维护标准（瀑布、敏捷、DevOps 等）并在修改时遵守标准 • 分离开发、测试和运营活动	I	I	C			A/R	C	C
IT 基础设施管理	• 按商定的服务水平和已定义的规范来运作 IT 环境 • 维护 IT 基础设施	I	I	C			A/R	C	C
I&T 安全	• 定义 I&T 安全政策、计划和程序并监控、检测、报告和解决安全漏洞和事故 • 根据业务要求和影响了解安全要求，包括隐私和网络安全、漏洞和威胁 • 以标准化的方式管理用户身份和授权 • 定期测试安全性	I	A	R			R	R	C/I
采购和合同	• 获取并维护用于响应交付策略的 I&T 资源，建立集成和标准化的 IT 基础设施，并降低 IT 采购风险 • 获取专业的法律和合同建议 • 制定采购程序和标准 • 按已定义的程序采购所需的硬件、软件和服务	I	I	C			A/R	C	C
I&T 合规性	• 确定所有适用的法律、法规和合同；确定相应的 I&T 合规性水平；优化 IT 流程以降低不合规风险 • 确定 I&T 相关的法律、法规和合同要求 • 评估合规性要求的影响 • 监控和报告这些要求的遵守情况	C/I	A	C			A/R	C	C/I

[15] IT 管理层包括 IT 职能管理层级别的所有角色。

本页特意留白