COBIT® 2019

设计指南

信息和技术治理解决方案的设计

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 设计并编写了《*COBIT® 2019 设计指南：信息和技术治理解决方案的设计*》（下称“作品”），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 不保证使用本作品就一定能取得成功。本作品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。在确定任何具体信息、程序或测试的适宜性时，企业信息和技术治理 (EGIT)、鉴证、风险和安全专业人员应就具体的情况（特定的系统或信息技术环境）作出自己专业性的判断。

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 设计指南：信息和技术治理解决方案的设计
ISBN 978-1-60420-784-2

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
on 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

本页特意留白

图表列表

第 I 部分. 设计流程

第二章. 基本概念：治理系统及组件

第三章. 设计因素的影响

第四章. 设计量身定制的治理系统

第五章. 与《COBIT® 2019 实施指南》相关联

第 II 部分. 执行和示例

第七章. 示例

附录

本页特意留白

第 I 部分
设计流程

第一章
介绍和用途

1.1 治理系统

本书描述了企业如何设计量身定制的企业信息和技术 (I&T) 治理解决方案。高效和有效的 I&T 治理系统是创造价值的起点。这适用于各种类型和规模的企业。I&T 等复杂领域的治理需要多个组件，包括流程、组织结构、信息流和行为。所有这些要素必须系统地协调运作；因此，本书所描述的治理解决方案是企业应量身定制的“企业 I&T 治理系统”，简称为“治理系统”。

不存在放之四海而皆准的唯一企业 I&T 治理系统。每个企业有自身的特点和情况，在企业规模、行业领域、监管环境、威胁形势、IT 在组织中的角色以及与战略性技术相关的选择等关键方面，不同组织都会存在差异。所有这些方面（在 COBIT® 中统称为“设计因素”）都要求组织定制治理系统，以实现 I&T 使用的最大价值。

定制意味着企业应从 COBIT® 核心模型开始，并根据一系列设计因素的相关性和重要性对通用框架进行改变。这一流程称为“设计企业 I&T 治理系统”。

1.2 本书的结构

本书包含以下主要部分、章节和附录：

第 I 部分：设计流程

- 第 1 章介绍本书的结构和目标受众。
- 第 2 章回顾《*COBIT® 2019 框架：简介和方法*》中设计因素等诸多关键概念和定义。
- 第 3 章探讨设计因素对设计治理解决方案的影响。
- 第 4 章是本书的核心，介绍了基于潜在设计因素情况下，设计企业治理解决方案的工作流程。此工作流程分四个步骤，生成量身定制的治理解决方案。
- 第 5 章说明本书与《*COBIT® 2019 实施指南*》的关系以及应如何结合两者使用。

第 II 部分：执行和示例

- 第 6 章介绍《*COBIT® 2019 设计指南*》工具箱 — 一款有助于设计治理系统工作流程的 Excel® 工具。
- 第 7 章阐述如何使用工具来实施第 4 章所述的工作流程。
- 附录 A 至 K 提供了设计流程中使用到的各个对应关系表。

1.3 本书的目标受众

本书目标受众包括 I&T 治理方面的众多直接利益相关方：董事会成员、执行管理层或高级管理层，以及企业内业务、IT、审计、鉴证、合规、安全、隐私和风险管理等领域经验丰富的专业人员。

I&T 治理的间接利益相关方包括客户、用户和公民；尽管他们当中很少有人会参考本书，但却是企业实现良好治理的最重要受益方。由之前提到的直接利益相关方来把握他们的利益。

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。用户只有具备这种经验和了解，才能根据企业环境，对通用性质的核心 COBIT® 2019 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初步设计、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书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。

1.4 相关指南：《COBIT® 2019 实施指南》

*《COBIT® 2019 实施指南》*与本书相关。它描述了持续改进企业 I&T 治理的路线图。这里所描述的治理系统（初步）设计是该路线图初始阶段的一部分。

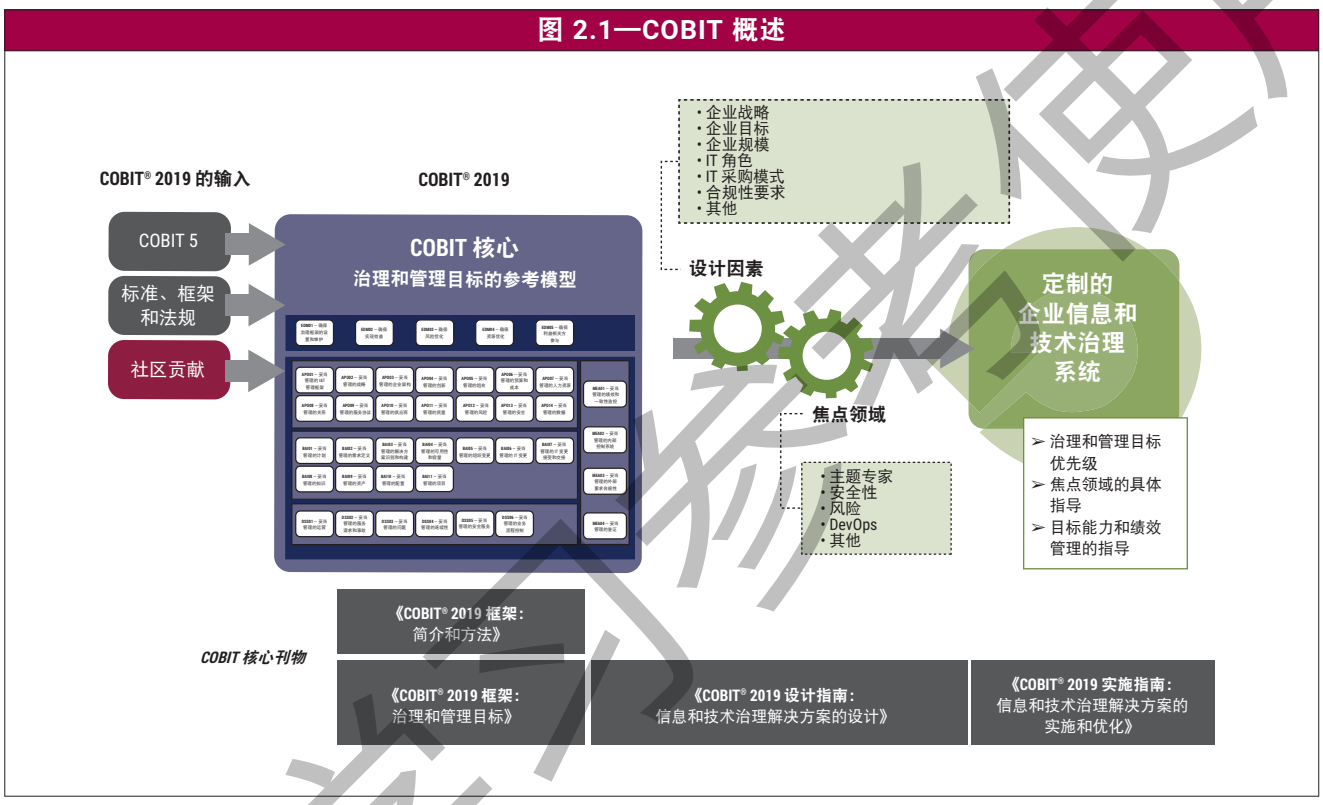
本指南第 5 章详细说明了这两本书之间的关系以及该如何结合使用。

第二章
基本概念：治理系统及组件

2.1 引言

图 2.1 高度概括了 COBIT® 2019，说明了系列丛书所涵盖的不同方面。

图 2.1—COBIT 概述



COBIT® 2019 基于 COBIT® 5 和其他权威资料。COBIT 遵循一系列相关标准和框架。*《COBIT® 2019 框架：简介和方法》*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 呼吁用户社区提供更新建议，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。

COBIT 产品系列是开放的。本指南发布时，以下图书已面市：

- ***《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 2.1 中标识为焦点领域的内容包含对特定主题的更详细指导。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。有关目前已发布和计划发布的图书最新信息和其他内容，请访问 *www.isaca.org/cobit*。

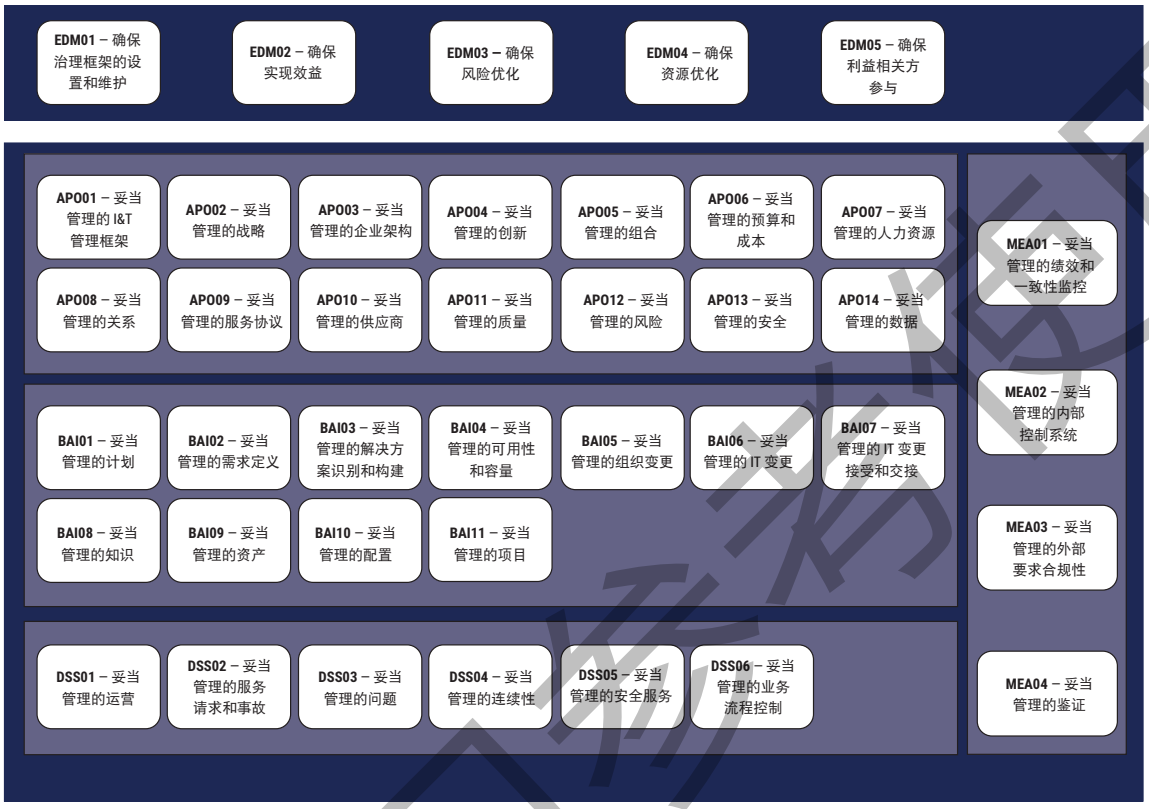
本节其余部分根据 COBIT 框架出版物中的定义，描述了 COBIT® 2019 的基本概念。设计因素、焦点领域和变体的概念将用于设计量身定制的企业 I&T 治理系统。基于 COBIT 的定制治理系统应采用 COBIT 的通用内容，并根据企业自身的环境和设计因素值，为治理和管理组件分配特定的优先级和目标能力级别。必要时还需实施特定的治理组件变体。

2.2 治理和管理目标

要通过信息和技术促进实现企业目标，应达到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 2.2** 中深蓝色背景所示）有关，而管理目标与管理流程（如**图 2.2** 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。

图 2.2—COBIT 核心模型



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。

2.3 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、信息项目、文化和行为、技能和能力以及服务、基础设施和应用程序。
- 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 2.2**）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。

2.4 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。[1] 焦点领域可能包含通用治理组件及变体的组合。

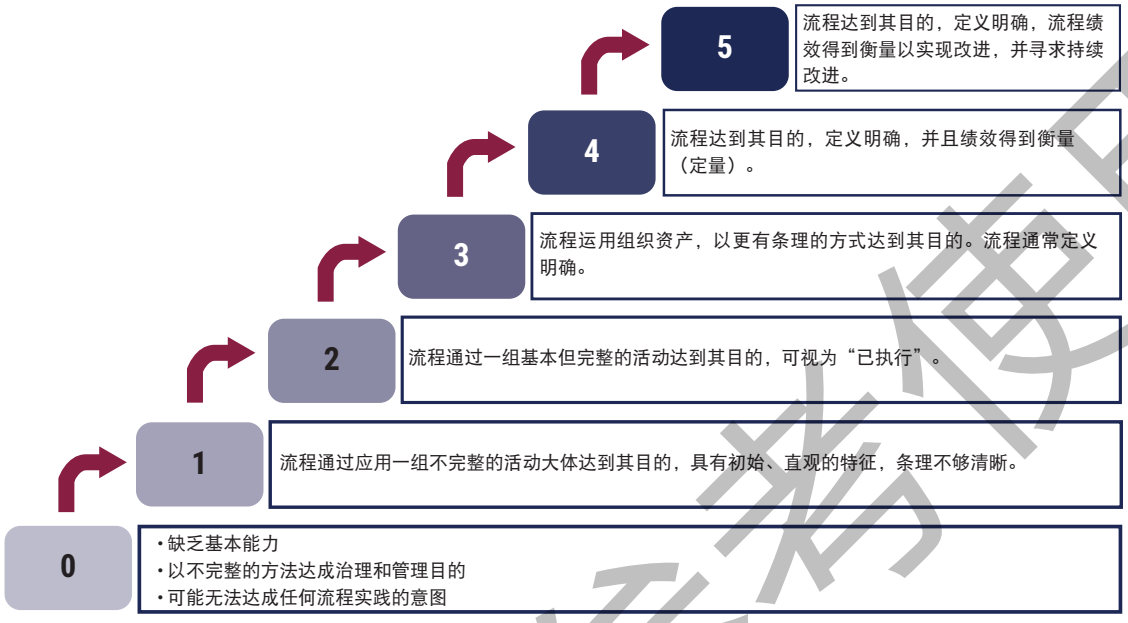
COBIT 作为开放式标准，其焦点领域的数量几乎没有限制。可根据需要添加新的焦点领域，或由主题专家和从业人员对开放式 COBIT 模型进行添加。

2.5 能力级别

COBIT® 2019 支持基于能力成熟度模型集成 (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 2.3** 描述了模型、递增的能力级别以及每个级别的一般特征。

[1] 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。

图 2.3—流程的能力级别



COBIT 核心模型为所有流程活动分配能力级别，从而对不同流程的能力级别有明确定义。本指南中有时会提到“较低”或“较高”的能力级别。通常，3 级或以上属于“较高”级别，3 级以下属于“较低”级别。

2.6 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。下面列出了设计因素，第 3 章阐述了它们对治理系统的潜在影响。

设计因素包括以下任意组合（**图 2.4**）：

图 2.4—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 2.5** 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 2.5—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）[2]
创新/差异化	企业专注于为客户提供不同的创新产品和服务[3]
成本领导	企业专注于短期的成本最小化[4]
客户服务/稳定性	企业专注于提供稳定、面向客户的服务[5]

2. **企业目标**支持企业战略 — 通过达成（一系列）企业目标来实现企业战略。这些目标已在 COBIT 框架中定义，按照平衡计分卡维度进行组织，并包含以下要素（**图 2.6**）：

图 2.6—企业目标设计因素

企业目标	BSC 维度	企业目标
EG01	财务	有竞争力的产品和服务的组合
EG02	财务	妥当管理的业务风险
EG03	财务	遵守外部法律和法规

[2] 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*。

[3] 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*，具体而言，有关愿景型和塑造型战略的内容。

[4] 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*。

[5] 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”。

图 2.6—企业目标设计因素（续）		
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

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 IT 相关风险，并指明了哪些风险领域超出风险偏好。

图 2.7 所列的风险类别应予以重视。[6]

图 2.7—风险概况设计因素（IT 风险类别）		
参考资料	**风险类别**	**风险场景示例**
1	IT 投资决策制定、投资组合定义和维护	A. 选定实施的计划与企业战略和优先级不一致 B. IT 相关投资未能支持企业的数字战略 C. 购置和实施的软件选择不当（就成本、性能、功能、兼容性、冗余等方面而言） D. 实施的基础设施选择不当（就成本、性能、功能、兼容性等方面而言） E. 不同投资举措之间出现重复或重要重叠 F. 新投资计划与企业架构之间长期不兼容 G. 与业务优先级不相符的资源配置错误、低效管理及资源竞争
2	计划和项目生命周期管理	A. 高级管理层未能终止（由于成本激增、过度延迟、范围偏离、业务优先级变更）失败的项目 B. I&T 项目预算超支 C. I&T 项目质量不佳 D. I&T 项目延迟交付 E. 第三方外包商未能按照合同协议交付项目（超出预算、质量问题、功能缺失、延迟交付等原因）
3	IT 成本和监督	A. 广泛依赖和使用用户创建、定义和维护的应用程序和临时解决方案 B. I&T 采购流程之外的 I&T 相关采购高价低效 C. 需求分析不足导致无效的服务水平协议 (SLA) D. I&T 相关投资缺乏资金
4	IT 专业知识、技能和行为	A. 由于新技术或新工作方法等因素导致IT 部门缺乏 IT 相关技能或技能不匹配 B. IT 员工不了解业务，影响了服务交付/项目质量 C. 无法招聘和留住 IT 员工 D. 由于招聘流程中未进行尽职调查而聘用了不合适的人员 E. 缺少 I&T 培训 F. I&T 服务过度依赖关键员工

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

图 2.7—风险概况设计因素（IT 风险类别）（续）		
参考资料	**风险类别**	**风险场景示例**
5	企业/IT 架构	A. 企业架构 (EA) 复杂且不灵活，阻碍了企业进一步的发展和扩张，导致错失商机 B. 未及时采用和利用新的基础设施或弃用过时的基础设施 C. 未及时采用和利用新软件（功能、优化等）或弃用过时的应用程序 D. 未文档化的 EA 导致效率低下和重复工作 E. 企业架构标准的例外情况数量过多
6	IT 运营基础设施事故	A. IT 设备意外损坏 B. IT 人员操作失误（在备份期间、系统升级期间、系统维护期间等） C. IT 人员或系统用户输入的信息不正确 D. 工作人员损坏（如破坏）数据中心 E. 存储敏感数据的设备被盗 F. 关键的基础设施组件被盗 G. 硬件组件配置错误 H. 硬件（如安全设备）遭到故意篡改 I. 滥用先前角色的权限访问 IT 基础设施 J. 丢失备份介质或未检查备份的有效性 K. 云提供商丢失数据 L. 云提供商的运营服务中断
7	未授权的行动	A. 软件遭篡改 B. 软件遭到故意修改或操纵，导致数据不正确 C. 软件遭到故意修改或操纵，导致欺诈行为 D. 软件遭到无意修改，导致结果不准确 E. 无意的配置和变更管理错误
8	软件采用/使用问题	A. 用户未采用新的应用程序软件 B. 用户使用新软件的效率不高
9	硬件事故	A. 安装新基础设施后系统不稳定，导致运营事故（如“自带设备”计划） B. 用户数量增加后系统无法处理交易量 C. 部署新的应用程序或举措后，系统无法处理负载 D. 电信、电力等公用事业故障 E. 过热和/或其他环境条件（如湿度）导致硬件故障 F. 内部员工损坏硬件组件导致数据损毁 G. 包含敏感数据的便携式介质（CD、USB 驱动器、便携式磁盘等）丢失/泄露 H. 发生硬件事故时解决时间延长或延迟支持
10	软件故障	A. 无法使用软件实现期望的成果（例如，未能建立所需的业务模型或执行组织变更） B. 实施的软件不成熟（早期采用者、软件存在缺陷等） C. 新软件上线运行后出现运行故障 D. 关键应用程序软件出现常规软件故障 E. 应用程序软件已过时（如过期、文档记录不合格、维护成本高、难以扩展、未集成到当前架构中） F. 新版本出现运行问题时无法恢复到先前的版本 G. 软件引起数据（库）损坏，导致数据无法访问

图 2.7—风险概况设计因素（IT 风险类别）（续）		
参考资料	风险类别	风险场景示例
11	逻辑攻击（黑客攻击、恶意软件等）	A. 未经授权的（内部）用户试图侵入系统 B. 拒绝服务 (DoS) 攻击导致服务中断 C. 网站遭篡改 D. 恶意软件攻击 E. 工业间谍 F. 黑客行动主义 G. 心怀不满的员工设置时间炸弹，导致数据丢失 H. 攻击者通过网络钓鱼攻击获取未授权的访问权限来盗取公司数据 I. 外国政府攻击关键系统
12	第三方/供应商事故	A. 外包商在大规模的长期外包安排中绩效欠佳（例如，没有对供应商进行财务能力、交付能力和供应商服务可持续性方面的尽职调查） B. 接受 IT 供应商提出的不合理业务条款 C. 供应商提供的支持和服务不足，与 SLA 不一致 D. 未遵守软件许可协议（使用和/或分发未经许可的软件） E. 过度依赖当前供应商，导致无法改用其他供应商 F. 企业在没有咨询 IT 部门或让其参与的情况下购买 IT 服务（尤其是云服务），导致无法整合 IT 服务与内部服务 G. SLA 不充分或未得到执行，导致无法获得商定的服务并且因违规而遭到处罚
13	违规	A. 未遵守国家或国际法规（如隐私、会计、制造、环境等方面的相关法规） B. 对可能影响业务的潜在监管变更缺乏意识 C. 法规带来的运营障碍 D. 不遵守内部程序
14	地缘政治问题	A. 其他工作场所因破坏性事故导致无法访问 B. 影响业务的政府干预和国家政策 C. 政府资助的团体或机构采取的针对性行动
15	劳工行动	A. 工会罢工导致无法进入设施和建筑 B. 罢工导致第三方提供商无法提供服务 C. 劳工行动（如运输或公用事业罢工）导致关键人员无法到位
16	自然灾害	A. 地震毁坏或破坏重要的 IT 基础设施 B. 海啸摧毁关键场所 C. 重大风暴和飓风或龙卷风破坏关键基础设施 D. 重大林火 E. 洪水 F. 地下水位上升导致关键位置无法使用 G. 温度上升导致关键位置的运营缺乏效益
17	基于技术的创新	A. 未能识别新的和重要的技术趋势 B. 未能认识到新技术的价值和潜力 C. 未能及时采用和利用新技术（功能、流程优化等） D. 未能提供技术来支持新业务模式
18	环境	A. 设备不环保（如功耗、包装）

图 2.7—风险概况设计因素（IT 风险类别）（续）		
参考资料	**风险类别**	**风险场景示例**
19	数据和信息管理	A. 信息保留/归档/处置的效率不高，导致未经授权人员发现敏感信息 B. 故意非法或恶意修改数据 C. 未经授权通过电子邮件或社交媒体披露敏感信息 D. 知识产权丢失和/或竞争情报泄漏

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[7] 包括（**图 2.8**）：

图 2.8—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，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，组织内的 IT 和业务实体受挫
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等
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，即用户部门在正常的 IT 投资决策机制控制范围和批准的预算之外的 I&T 支出
H	多个举措之间重复或重叠，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
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 IT 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、质量控制以及其他问题
R	业务部门在企业 IT 部门极少或者根本没有参与的情况下实施自己的信息解决方案 8[8]
S	忽视和/或违反安全和隐私法规
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 2.9** 所示。

图 2.9—威胁环境设计因素	
威胁环境	**说明**
正常	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。

[7] 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）第 3.3.1 节“典型痛点”。
[8] 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 2.10** 中列出的类别对企业所遵守的合规性要求进行分类。

图 2.10—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 2.11** 对企业 IT 角色进行分类。

图 2.11—IT 角色设计因素	
IT 角色[9]	**说明**
支持	IT 对业务流程和服务的运行、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 2.12** 对企业采用的采购模型进行分类。

图 2.12—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上述三种模式。

9. **IT 实施方法** — 可根据**图 2.13** 对企业采用的方法进行分类。

图 2.13—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”。

[9] 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 2.14** 对技术采用战略进行分类。

图 2.14—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 2.15** 所示。[10]

图 2.15—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

第 3 章阐述了设计因素对治理系统设计的影响。

2.6.1 为什么没有特定行业领域的设计因素?

每个行业在 I&T 使用的期望方面都有自己独特的要求。但是，通过结合上述表中列出的设计因素，可以捕捉到行业领域的重要特征。例如:

- 金融行业的特点如下：IT 受到严格监管且发挥战略性作用，IT 组织通常由大型企业组成，并且在高威胁环境中运营。
- 如医院等医疗服务提供者通常寻求将客户服务/稳定性和创新战略相结合，他们受到严格监管，面临很多特定风险领域（安全、安保、隐私、连续性等），在中度但不断加剧的威胁环境中运营，并且在战略上越来越依赖于 IT。
- 非营利性企业通常规模较小，受到的监管较少，他们注重成本，在技术采用方面并不是领先创新者。
- 公共机构通常是大型组织，采用客户服务和成本领导战略。他们面临中等至较高的风险概况，并且因其特殊性质而受到严格监管。从支持保守型机构到战略性的电子政府计划，IT 的作用不尽相同。采购模式越来越多地使用外包服务，而在技术采用方面，他们通常是主流追随者。

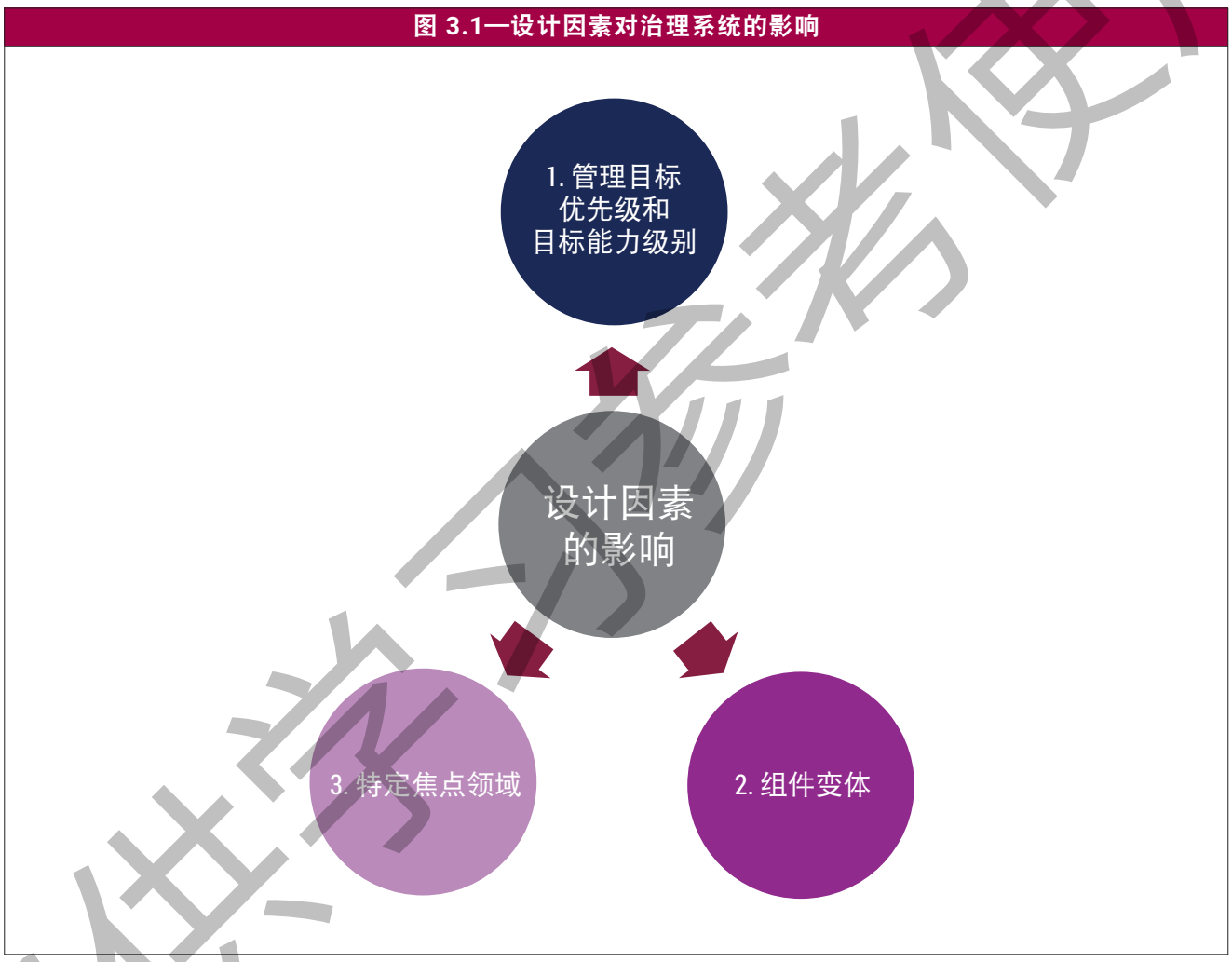
[10] 微型企业，即员工少于 50 人的企业，不在本书的讨论范围内。

第三章
设计因素的影响

3.1 设计因素的影响

设计因素对定制企业治理系统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 3.1** 所示。

图 3.1—设计因素对治理系统的影响



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相关组件构成。它们本质上是对等的，没有先后顺序。但是，设计因素可以影响这种对等关系，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的组合*”，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 专业人员对业务具有透彻的了解（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。设计因素可以要求特定的组件变体，也可以影响组件的重要性。

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，而使用简化版本作为替代。中小型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。[11]

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. 对特定焦点领域的指导需求 — 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 模型内容随具体环境而变化。

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[12] 的变体。

示例： 中小型企业的员工较少、IT 资源较少，汇报关系简单直接，与大型企业存在多方面的差异。因此，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。[13]

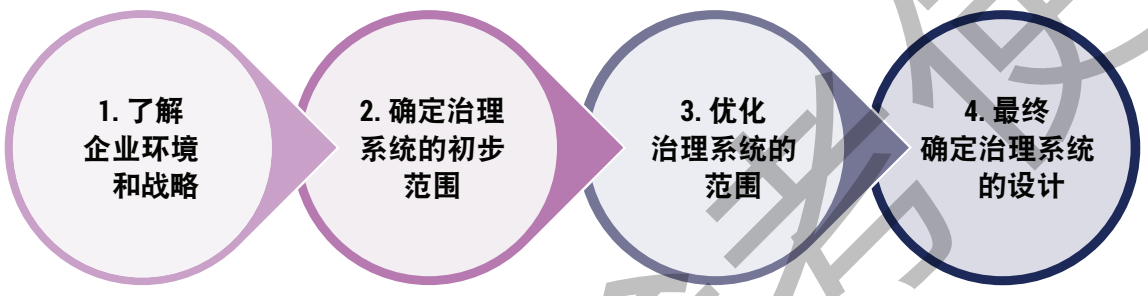
[11] *《COBIT® 2019 设计指南：信息和技术治理解决方案的设计》*出版时，中小型企业焦点领域的内容正在制定中，尚未发布。
[12] *《COBIT® 2019 设计指南：信息和技术治理解决方案的设计》*出版时，DevOps 焦点领域的内容正在制定中，尚未发布。
[13] *《COBIT® 2019 设计指南：信息和技术治理解决方案的设计》*出版时，中小型企业焦点领域的内容正在制定中，尚未发布。

第四章
设计量身定制的治理系统

4.1 引言

图 4.1 提供了定制治理系统的建议设计流程。下面将详细讨论每个步骤。

图 4.1—治理系统设计工作流程



- 1.1 了解企业战略。
- 1.2 了解企业目标。
- 1.3 了解风险概况。
- 1.4 了解当前的 I&T 相关问题。

- 2.1 考虑企业战略。
- 2.2 考虑企业目标并运用 COBIT 目标级联。
- 2.3 考虑企业的风险概况。
- 2.4 考虑当前的 I&T 相关问题。

- 3.1 考虑威胁环境。
- 3.2 考虑合规性要求。
- 3.3 考虑 IT 角色。
- 3.4 考虑采购模式。
- 3.5 考虑 IT 实施方法。
- 3.6 考虑 IT 采用战略。
- 3.7 考虑企业规模。

- 4.1 解决固有的优先级冲突。
- 4.2 最终确定治理系统的设计。

如**图 4.1** 所示，在设计流程的不同阶段和步骤中，会提出如下建议，包括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相互冲突的指导意见，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。

注 1： 在开始治理系统的设计工作之前，应明确适用范围，这一点很重要。例如，设计治理系统面向的是某个业务部门、整个企业还是不同企业形成的网络等？[14]

注 2： 本书提出的工作流程包含四个步骤。每个步骤中的子步骤并不是强制性的。例如，企业可以决定设计一个治理系统，以（仅）解决特定的战略选择或（仅）解决某些 IT 风险领域，而无需完成工作流程的所有步骤。

[14] 了解这一范围完全符合递归的系统设计思维，即“任何活性企业 IT 治理系统都包含且包含在一个活性企业 IT 治理系统中”；请参阅 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。

4.2 第 1 步：了解企业环境和战略

在第 1 步中，企业检查自身的背景、战略和业务环境，以清楚地了解四个部分重叠、相互依赖且通常互补的领域。以下小节概述了第 1 步中的关键子步骤：

- 企业战略
- 企业目标和相应的一致性目标
- I&T 风险概况
- 当前的 I&T 相关问题

4.2.1 了解企业战略

企业必须确定哪种企业战略原型最适合自身。本书第 2.6 节第 1 项定义了企业战略原型（参见**图 2.5**）。

明确选择企业战略原型之后，最有效的机制是将企业战略转化为治理和管理目标重要性的相对评级。

最好的做法通常是确定一个主要原型并选择一个备用原型。当企业战略被定义为同等重要的战略原型组合时，COBIT 核心模型的治理和管理目标往往变得几乎同等重要，从而使优先级的确定变得非常困难。

4.2.2 了解企业目标

企业战略需要通过达成（一组）企业目标来实现。COBIT 定义了 13 个通用企业目标；每个企业都可以/根据所选择的企业战略确定企业目标的优先级。本书第 2.6 节第 2 项定义了一系列企业目标（参见**图 2.6**）。

为了将企业目标转化为治理和管理目标重要性的相对评级（参见第 4.3.3 节的目标级联），应明确选择企业目标。建议仅确定几个主要企业目标和若干个次要企业目标。当所有企业目标都有相同的优先级时，COBIT 核心模型的治理和管理目标也往往变得几乎同等重要，从而使优先级的确定变得非常困难。

4.2.3 了解风险概况

治理系统设计的另一个重要输入是了解企业的风险概况，即了解哪些风险场景可能会影响企业，以及如何评估其影响和发生的可能性。

为了解这些信息，应进行整体风险分析，包括：

- 确定相关风险场景（可基于第 2.6 节第 3 项定义的一系列风险场景类别；参见**图 2.7**）
- 评估场景的影响和发生的可能性，同时考虑风险缓解控制的当前状态
- 基于先前输入的总体风险评级

设计治理系统时，为了最有效地确定相应的风险概况，在评估 I&T 风险时应明确区分这些风险。

当所有 IT 风险都被评定为同等重要时，COBIT 核心模型的治理和管理目标往往变得几乎同等重要，从而使优先级确定变得困难。

4.2.4 了解当前的 I&T 相关问题

与 IT 风险密切相关的是企业当前面临的 I&T 相关问题，也称为痛点（可视为已发生的风险）。风险管理部门、审计部门、高级管理层或外部利益相关方可识别或报告 IT 问题。本书第 2.5 节第 4 项定义了一系列常见问题（参见**图 2.8**）。

应明确区分 I&T 问题的等级，以便为确定治理系统设计的优先级提供必要输入。

当所有 IT 问题都评为同等严重时，COBIT 核心模型的治理和管理目标往往变得几乎同等重要，从而使优先级确定变得非常困难。

4.2.5 总结

第 1 步结束时，企业将对企业战略、企业目标、IT 风险和当前的 I&T 问题形成清晰一致的看法。接下来（第 4.3 节），这些信息将被转化为优先治理/管理目标，用于为定制的企业治理系统划定初步范围。

4.3 第 2 步：确定治理系统的初步范围

为确定治理系统的初步范围，第 2 步综合了第 1 步所收集的信息。从企业战略、企业目标、风险概况和 I&T 相关问题推导出的数值被转化为一组优先治理组件，以形成初步定制的企业治理系统。

4.3.1 将设计因素转化为治理和管理优先级

第 2 步提供了一些相关的设计因素和关联的描述性值，所做的选择将推动确定治理和管理目标的优先级。针对这项评估有两种基本方法：定性方法和定量方法。

定性方法考虑与每个设计因素的值相关度最高的治理和管理目标。在初步设计并设计优化步骤（后者参见第 4.4 节）之后，对治理和管理目标优先级做出定性决策。

定量方法涉及为每个设计因素创建的数值对应关系表。这些对应关系表量化了与每个设计因素相关的描述性数值，用于表示它们与治理和管理目标的相关性。

- COBIT® 2019 中的对应关系表通常包含零 (0) 到四 (4) 之间的值。四表示治理或管理目标与特定设计因素的值的相关性最大；零表示没有相关性。
- 将设计因素的值转化为治理和管理目标的重要性需要进行矩阵计算，得出每个治理和管理目标的分数。
- 根据提出的实际方法，可进一步操作这些分数用于演示（例如，标准化到特定的固定度量指标）。
- 第 2 步和第 3 步结束时，需要整合其中一些计算结果。同样，不存在客观必需的固定整合方法，但通常情况下，最好使用（加权）求和来完成。

本书的第 7 章提供了定量方法的例子。所有例子都参考了本*《COBIT® 2019 设计指南》*配套的 Excel® 工具箱（可从 *www.isaca.org/COBIT/Pages/COBIT-2019-Design-Guide.aspx* 获取）。

4.3.2 思考企业战略（设计因素 1）

图 4.2 列出了对每个企业战略原型而言最重要的治理和管理目标、重要的治理组件以及相关的焦点领域指南。当企业战略被定义为混合战略时，重要的治理和管理目标将会反映各个要素的组合。

图 4.2—对应到企业战略设计因素的治理和管理目标优先级

设计因素的值	治理和管理目标优先级	组件	焦点领域的变体

成长/收购	重要的管理目标[15]包括：
	• APO02、APO03、APO05
	• BAI01、BAI05、BAI11
		重要的组件：
		• 组织结构
		  ■ 通过投资办公室来支持投资组合管理角色
		  ■ 企业架构师
		• 服务、基础设施和应用程序
		  ■ 促进自动化和成长，并实现规模经济效应
			COBIT 核心模型

创新/差异化	重要的管理目标包括： • APO02、APO04、APO05 • BAI08、BAI11	重要的组件： • 组织结构 ■ 首席数字官和/或首席创新官 • 文化和行为组件对创新的重要影响	COBIT 核心模型
成本领导	重要的治理和管理目标包括： • EDM04 • APO06、APO10	重要的组件： • 技能和能力 ■ 专注于 IT 成本和预算能力 • 文化和行为组件的重要影响 • 服务、基础设施和应用程序组件（例如，实现控制自动化、提高效率）	COBIT 核心模型
客户服务/稳定性	重要的治理和管理目标包括： • EDM02 • APO08、APO09、APO11 • BAI04 • DSS02、DSS03、DSS04	重要的组件： • 文化和行为组件（以客户为中心）的重要影响	COBIT 核心模型

4.3.3 思考企业目标并运用 COBIT 目标级联（设计因素 2）

企业战略需要通过达成（一组）企业目标来实现。COBIT® 2019 定义了 13 个通用企业目标（请参阅第 2.6 节第 2 项和**图 4.3**）；每个企业都应根据自身战略确定这些目标的优先级。

将企业目标转化为可执行的治理和管理目标：

1. 从通用企业目标开始，确定对组织而言最重要的目标。再从中选择三到五项优先级最高的企业目标；如果高优先级目标太多，会削弱目标级联结果的意义。
2. 在企业目标和一致性目标之间的对应关系表中找到优先的企业目标（附录 B）。使用对应关系表确定最重要的一致性目标。
3. 在一致性目标与治理和管理目标之间的对应关系表中找到优先的一致性目标（附录 C）。使用对应关系表确定最重要的治理和管理目标。

该子步骤基于优先的企业目标，确定了对企业而言重要性更高的治理和管理目标。

[15] “重要”对应了此设计因素与治理和管理目标的对应关系表中 3 分或更高的值。

注：这是使用通用对应关系表的纯机械性操作。企业必须谨慎地解释结果，或者根据自身经验和背景调整对应关系表。在本指南所描述的工作流程中，这项微调工作是在第 4 步*“最终确定治理系统的设计”*中完成的。

目标级联的应用示例包括在本*《COBIT® 2019 设计指南》*配套的工具箱中。[16]

4.3.4 思考企业的风险概况（设计因素 3）

在第 1 步（请参阅第 4.2.3 节“了解风险概况”）中，企业进行了整体风险分析，以识别超过企业风险偏好的风险类别。在这个步骤中，风险分析的结果被转化为治理和管理目标的优先级。风险管理中最常用的风险应对是风险缓释，它需要（以风险语言）实施一系列控制，或（以 COBIT 语言）实现治理和管理目标。附录 D 包含 COBIT® 2019 中 19 个 IT 风险类别与治理和管理目标之间的对应关系，阐明了每个治理和管理目标在多大程度上可被视为对每个风险场景的控制。

附录 D 中的对应关系表使用前面描述的相同技术和评分方法，将企业的风险概况与治理和管理目标及其优先级相关联。

示例：附录 D 说明了如果 IT 风险场景类别 1 (RISKCAT01)*“IT 投资决策制定、投资组合定义和维护”*令人担忧，则以下治理和管理目标将非常重要：

- EDM01、EDM02、EDM04、EDM05
- APO05

4.3.5 思考企业当前的 I&T 相关问题（设计因素 4）

在第 1 步（请参阅第 4.2.4 节“了解当前的 I&T 相关问题”）中，企业对其经历的 I&T 相关问题进行了整体诊断。在这个步骤中，诊断结果被转化为治理和管理目标的优先级。

附录 E 包含 I&T 问题与 COBIT® 2019 治理和管理目标之间的对应关系表。如附录 E 所示，每个 I&T 相关问题都与一个或多个可能影响 I&T 相关问题的治理或管理目标相关联。可使用前面描述的相同技术和评分机制。

示例：如果 I&T 相关问题“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”令人担忧，则以下治理和管理目标将非常重要：

- APO03
- BAI01、BAI02、BAI03、BAI05、BAI11

[16] 可通过 *www.isaca.org/COBIT/Pages/COBIT-2019-Design-Guide.aspx* 下载配套的工具箱。

4.3.6 总结

第 2 步结束时，所有元素都可用来定义定制治理系统的初步范围：

- **优先的治理和管理目标**表明了哪些治理和管理目标应成为重点。
- **关于特定治理组件的指导**也可能包含在初步设计中。

企业可以选择详细说明当前的初步设计，并解决各种输入之间的所有差异；也可以等到在工作流程第 4 步时，将不同的输入与第 3 步中确定的范围优化相结合。

4.4 第 3 步：优化治理系统的范围

第 3 步基于第 2.6 节定义的其余设计因素，确定对治理系统初步范围的优化。在本章中，并非所有设计因素都适用于每个企业。企业可忽略不适用的因素。

在这个步骤中，治理系统设计人员将：

1. 从 DF5 *“威胁环境”*到 DF11 *“企业规模”*，对每个设计因素 (DF) 进行浏览审查。
2. 确定每个设计因素是否适用。
3. 对于适用的设计因素，确定哪些潜在值或潜在值的组合最适用于企业。参考适用设计因素值的描述以及附录 F 至 K 中的对应关系表，确定哪些治理系统优化与这些值相关。

每次考量设计因素都会形成一份治理和管理目标的排序表，类似于第 2 步的结果。运用附录 F 至 K 中的对应关系表，可以使用前面描述的相同技术和度量指标。

4.4.1 思考威胁环境（设计因素 5）

在思考此设计因素时，应执行以下步骤：

- 根据**图 4.3** 中定义的条目，确定哪种值的组合最适合企业的当前状况。
- 思考列出的针对治理和管理目标、组件以及焦点领域的指南，并将相关信息包含在设计“画板”上，用于第 4 步的解决方案和结论。

图 4.3—对应到威胁环境设计因素的治理和管理目标优先级

设计因素的值	治理和管理目标优先级	组件	焦点领域的变体
高	重要的治理和管理目标包括： • EDM01、EDM03 • APO01、APO03、APO10、APO12、APO13、APO14 • BAI06、BAI10 • DSS02、DSS04、DSS05、DSS06 • MEA01、MEA03、MEA04	重要的组织结构包括： • 安全战略委员会 • 首席信息安全官 (CISO) 重要的文化和行为领域包括： • 安全意识 信息流包括： • 安全政策 • 安全战略	信息安全焦点领域[17]
正常	• *按照初步范围定义*	• *不适用*	COBIT 核心模型

[17] *《COBIT® 2019 设计指南：信息和技术治理解决方案的设计》*出版时，信息安全焦点领域的内容正在制定中，尚未发布。

4.4.2 思考合规性要求（设计因素 6）

在思考此设计因素时，应执行以下步骤：

- 根据**图 4.4** 中定义的条目，确定哪种值的组合最适合企业的当前状况。
- 思考列出的针对治理和管理目标、组件以及焦点领域的指南，并将相关信息包含在设计“画板”上，用于第 4 步的解决方案和结论。

图 4.4—对应到合规性要求设计因素的治理和管理目标优先级

设计因素的值	治理和管理目标优先级	组件	焦点领域的变体
高	重要的治理和管理目标包括： • EDM01、EDM03 • APO12 • MEA03、MEA04	合规职能的重要性： • 文档（信息项）以及政策和程序的高度相关性	COBIT 核心模型
正常	• *按照初步范围定义*	• *不适用*	COBIT 核心模型
低	• *按照初步范围定义*	• *不适用*	COBIT 核心模型

4.4.3 思考 IT 角色（设计因素 7）

在思考此设计因素时，应执行以下步骤：

- 根据**图 4.5** 中定义的条目，确定哪种值的组合最适合企业的当前状况。
- 思考列出的针对治理和管理目标、组件以及焦点领域的指南，并将相关信息包含在设计“画板”上，用于第 4 步的解决方案和结论。

图 4.5—对应到 IT 角色设计因素的治理和管理目标优先级

设计因素的值	治理和管理目标优先级	组件	焦点领域的变体
支持	• *按照初步范围定义*	• *不适用*	COBIT 核心模型
工厂	重要的治理和管理目标包括： • EDM03 • DSS01、DSS02、DSS03、DSS04	• *不适用*	信息安全焦点领域[18]
整顿	重要的治理和管理目标包括： • APO02、APO04 • BAI02、BAI03	• *不适用*	DevOps 焦点领域[19]

战略	重要的治理和管理目标包括：
	• EDM01、EDM02、EDM03
	• APO02、APO04、APO05、APO12、APO13
	• BAI02、BAI03
	• DSS01、DSS02、DSS03、DSS04、DSS05
		典型的双模式组件包括：
		• 组织结构
		  ■ 首席数字官
		• 技能和能力
		  ■ 可以在兼具探索与开发的灵活环境中工作的员工
		• 流程
		• 整合了探索与开发数字化转型机会的组合和创新流程
			数字化转型焦点领域[20]

[18] *《COBIT® 2019 设计指南：信息和技术治理解决方案的设计》*出版时，信息安全焦点领域的内容正在制定中，尚未发布。
[19] *《COBIT® 2019 设计指南：信息和技术治理解决方案的设计》*出版时，DevOps 焦点领域的内容正在制定中，尚未发布。
[20] *《COBIT® 2019 设计指南：信息和技术治理解决方案的设计》*出版时，正在考虑将数字化转型焦点领域的内容作为未来的潜在焦点领域。

4.4.4 思考 IT 采购模式（设计因素 8）

在思考此设计因素时，应执行以下步骤：

- 根据**图 4.6** 中定义的条目，确定哪种值的组合最适合企业的当前状况。
- 思考列出的针对治理和管理目标、组件以及焦点领域的指南，并将相关信息包含在设计“画板”上，用于第 4 步的解决方案和结论。

图 4.6—对应到 IT 采购模式设计因素的治理和管理目标优先级

设计因素的值	治理和管理目标优先级	组件	焦点领域的变体
外包	重要的管理目标包括： • APO09、APO10 • MEA01	• *不适用*	供应商管理焦点领域[21]
云	重要的管理目标包括： • APO09、APO10 • MEA01	• *不适用*	云焦点领域[22]
内包	• *按照初步范围定义*	• *不适用*	COBIT 核心模型
混合	*组合三种特定选项的指南*		

4.4.5 思考 IT 实施方法（设计因素 9）

在思考此设计因素时，应执行以下步骤：

- 根据**图 4.7** 中定义的条目，确定哪种组合最适合企业的当前状况。
- 思考列出的针对治理和管理目标、组件以及焦点领域的指南，并将相关信息包含在设计“画板”上，用于第 4 步的解决方案和结论。

图 4.7—对应到 IT 实施方法设计因素的治理和管理目标优先级

设计因素的值	治理和管理目标优先级	组件	焦点领域的变体
敏捷	重要的管理目标包括： • BAI02、BAI03、BAI06	• 敏捷焦点领域指南中确定的重要特定角色	敏捷焦点领域[23]
DevOps	重要的管理目标包括： • BAI03	• DevOps 焦点领域指南中确定的重要特定角色	DevOps 焦点领域[24]
传统	• *按照初步范围定义*	• *不适用*	COBIT 核心模型
混合	*组合三种特定选项的指南*		

[21] *《COBIT® 2019 设计指南：信息和技术治理解决方案的设计》*出版时，正在考虑将供应商管理焦点领域作为未来的潜在焦点领域。
[22] *《COBIT® 2019 设计指南：信息和技术治理解决方案的设计》*出版时，正在考虑将云焦点领域作为未来的潜在焦点领域。
[23] *《COBIT® 2019 设计指南：信息和技术治理解决方案的设计》*出版时，正在考虑将敏捷焦点领域作为未来的潜在焦点领域。
[24] *《COBIT® 2019 设计指南：信息和技术治理解决方案的设计》*出版时，DevOps 焦点领域的内容正在制定中，尚未发布。

4.4.6 思考技术采用战略（设计因素 10）

在思考此设计因素时，应执行以下步骤：

- 根据**图 4.8** 中定义的条目，确定哪种值的组合最适合企业的当前状况。
- 思考列出的针对治理和管理目标、组件以及焦点领域的指南，并将相关信息包含在设计“画板”上，用于第 4 步的解决方案和结论。

图 4.8—对应到技术采用战略设计因素的治理和管理目标优先级

设计因素的值	治理和管理目标优先级	组件	焦点领域的变体
先行者	重要的治理和管理目标包括： • EDM01、EDM02 • APO02、APO04、APO05、APO08 • BAI01、BAI02、BAI03、BAI05、BAI07、BAI11 • MEA01	• *不适用*	DevOps 焦点领域[24] 数字化转型焦点领域[25]
追随者	重要的治理和管理目标包括： • APO02、APO04 • BAI01	• *不适用*	COBIT 核心模型
滞后者	• *按照初步范围定义*	• *不适用*	COBIT 核心模型

4.4.7 思考企业规模（设计因素 11）

在思考此设计因素时，应执行以下步骤：

- 根据**图 4.9** 中定义的条目，确定哪种组合最适合企业的当前状况。
- 思考列出的针对治理和管理目标、组件以及焦点领域的指南，并将相关信息包含在设计“画板”上，用于第 4 步的解决方案和结论。

图 4.9—对应到企业规模设计因素的治理和管理目标优先级

设计因素的值	治理和管理目标优先级	组件	焦点领域的变体
大型	• *按照初步范围定义*	• *不适用*	COBIT 核心模型
中小型	• *按照初步范围定义*	• *中小型企业焦点领域的适用描述*	中小型企业焦点领域[26]

示例： 如果企业是中小型企业（SME，如拥有 250 名或更少的全职员工 [FTE]），应使用中小型企业焦点领域中包含的指南来设计其治理系统。

[24] *《COBIT® 2019 设计指南：信息和技术治理解决方案的设计》*出版时，DevOps 焦点领域的内容正在制定中，尚未发布。
[25] *《COBIT® 2019 设计指南：信息和技术治理解决方案的设计》*出版时，正在考虑将数字化转型焦点领域的内容作为未来的潜在焦点领域。
[26] *《COBIT® 2019 设计指南：信息和技术治理解决方案的设计》*出版时，中小型企业焦点领域的内容正在制定中，尚未发布。

4.4.8 总结

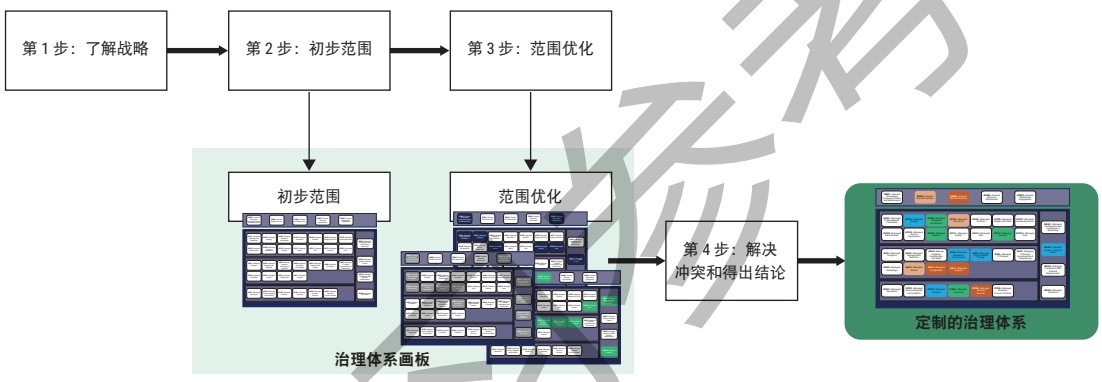
第 3 步结束时，企业确定初步治理系统的一系列潜在改进并放置在“画板”上，以便在接下来的第 4 步中进行整合。

以下改进层面的表达方式通常与第 2 步的结果类似：优先的治理和管理目标、治理系统的重要组件，以及特定焦点领域指南。

4.5 第 4 步：解决冲突并最终确定治理系统的设计方案

作为设计流程的最后一步，第 4 步整合了前面几个步骤的所有输入，以最终确定治理系统设计方案，如**图 4.10** 所示。得出的治理系统应对所有输入进行慎重考虑，并认识到这些输入之间有时可能存在冲突。

图 4.10—治理系统设计第 4 步 — 总结



4.5.1 解决固有的优先级冲突

第 4 步涉及协调冲突以最终确定设计。

4.5.1.1 目的

在做出结论之前，应考虑之前步骤的以下输出：

- 第 2 步中基于企业战略、企业目标、风险概况和 I&T 相关问题获得的治理系统初步设计。这种初步设计可能反映了一些存在分歧的优先管理目标。
- 第 3 步中通过分析其余设计因素和存在分歧的优先级而获得的范围改进。

4.5.1.2 解决战略

本指南所描述的工作流程可应用于不同的情况，需采取不同的战略来得出最终结论。简而言之，企业在以实施治理计划为目标应用设计因素后，需要分析数据和结果。

示例：如果企业***正在进行一项重要的举措***（例如，对企业应用程序、数字化转型计划等进行重大投资）或想要专注于***某个具体的主题或问题***（例如，解决一个重要的安全问题、采用 DevOps 方法、调整并遵守新的隐私法规等），企业不需要全部应用所提议的工作流程中的所有步骤，而是重点关注特定的感兴趣领域。

- 在进行重要的开发投资情况下，企业可以将企业战略（设计因素 1）视为创新/差异化战略，从而决定仅致力于该设计因素所强调的治理和管理目标。
- 如果出台新的隐私法规，企业可专注于与高合规性要求相对应的治理和管理目标（设计因素 6）。这些目标包括 EDM01*“确保治理框架的设置和维护”*、EDM03*“确保风险优化”*、APO12*“妥当管理的风险”*、MEA03*“妥当管理的外部要求合规性”*以及 MEA04*“妥当管理的鉴证”*。此外，企业还需关注 MEA03 中包含的合规性需求分析所提出的治理和管理目标。

示例：如果企业希望就其治理系统获得***广泛、全面和整体的认识***，建议企业应用本指南所描述的完整工作流程并慎重考虑所有设计因素。

在定义治理系统的设计时，企业应审查其治理和管理目标，并分析当前的绩效水平（即流程的能力级别）。之后，在制定实现目标治理系统的路线图时，企业应根据这些评估结果，优先考虑实施速效方案（即只需少量投入就能产生高效益的举措）。

4.5.1.3 解决方法

没有普遍适用的准则可以解决所有企业环境中存在的相互竞争或冲突的优先级。不过针对这个问题，有一些建议：

- 让所有关键利益相关方参与讨论治理系统设计，包括董事会、执行管理层、业务高管、IT 职能部门管理层以及风险和鉴证管理层。
- 考虑 COBIT 指南的通用性和对应关系表，它们无法兼顾到每个企业的所有具体情况。企业可以并且应该对偏离某些已确定优先级做好准备，只要它认可这类偏离存在的合理理由。
- 同样需要注意的是，企业的特定背景可能要求其偏离按照通用的预编程计算（如数学矩阵计算得出的结果）所产生的严格定量的治理和管理目标优先级。

4.5.2 最终确定治理系统的设计

4.5.2.1 最终确定设计

设计阶段结束时，必须形成一项企业 I&T 治理系统的设计。该设计将包括：

- 优先的治理和管理目标，并且：
  - 高优先级目标的数量保持在合理水平。
  - 已定义目标能力级别（对于非流程则为等效的绩效要求），其中针对最关键的目标定义更高的目标能力级别，针对不太重要的目标定义较低的目标能力级别。

- 各种流程的目标能力级别（或其他组件的等效绩效目标）。在定义这些目标时，不建议追求最高等级，因为：
  - 对于某些流程或其他组件，是不可能实现或定义五 (5) 级能力的。
  - 在运行治理系统时，以这种高能力级别要求所有目标的做法往往成本效益很低或不合理。
  - 很多组织发现，几乎不可能在合理时间内执行旨在实现这种高能力级别治理系统的路线图。
- 由于特定问题或情况，需要特别关注某个治理组件（例如，如果企业最担心的是隐私问题，则应额外关注隐私政策和程序）
- 与核心 COBIT 指南相辅相成的可用且必要适当的焦点领域指南

第 7 章提供了此类设计的案例。

4.5.2.2 维持治理系统

在设计工作流程的最后一步会形成一个设计良好的治理系统。但治理系统本质上是动态的，企业可能会改变战略或启动重要的投资计划，威胁环境和技术也在不断变化，这意味着企业应定期审查治理系统，必要时对系统进行完善。

治理系统具有动态性，为此，《*COBIT® 2019 实施指南*》概括了一个持续改进周期（另请参阅本书的第 5 章）。

第五章
与《COBIT® 2019 实施指南》相关联

5.1 《COBIT® 2019 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，并且认识到 I&T 已渗透到企业的每个角落，要将业务与 IT 相关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 职能领域责任。

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、明确适用范围并定义可实现的目标。只有这样才能让企业按计划跟上变革的步伐。因此，计划管理应作为实施生命周期不可或缺的一部分。

尽管推荐采用计划和项目的方式来有效推动改进举措，但总体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（像企业治理的其他方面一样）。因此，实施方法是基于赋能业务和 IT 利益相关方，通过促进和推行变革，让他们负责 I&T 相关的治理和管理决策以及活动。

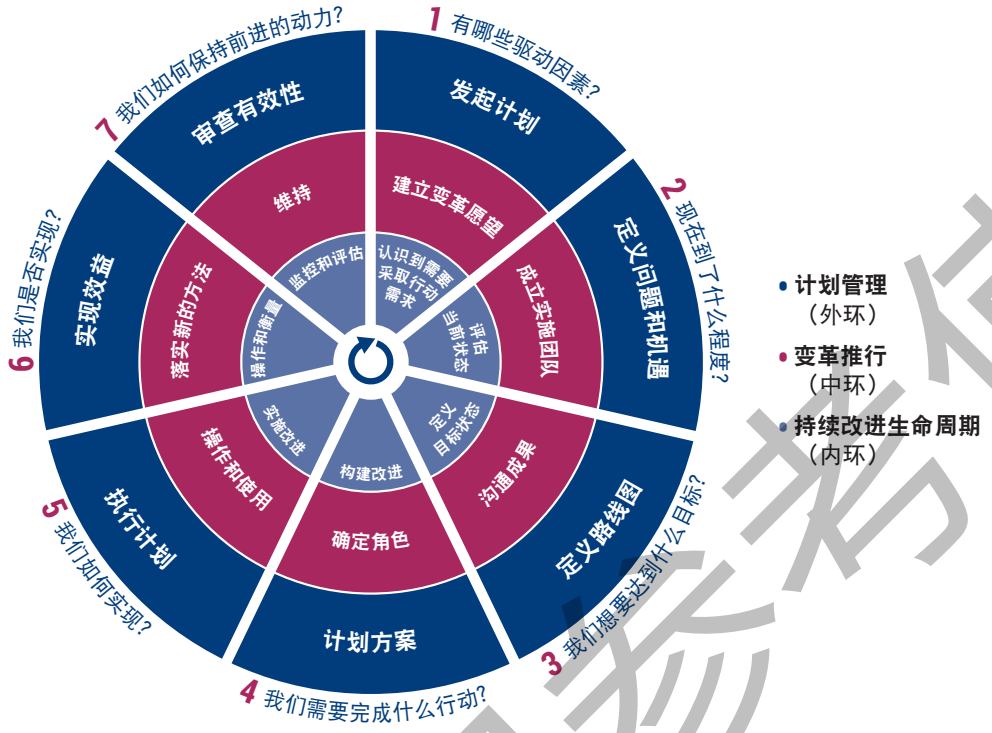
当侧重 IT 相关优先目标和治理改进的流程开始产生可衡量的效益，且计划成果已融入持续进行的业务活动中时，实施计划将会关闭。

有关这些主题的更多信息，请参阅《COBIT® 2019 实施指南》。

5.2 COBIT 实施方法

图 5.1 总结了 COBIT 实施方法。

图 5.1—COBIT 实施路线图



5.2.1 第 1 阶段 — 有哪些驱动因素?

实施方法的第 1 阶段识别当前变革驱动因素，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。变革驱动因素属于内部或外部事件、状况或关键问题，充当变革刺激因素。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。

5.2.2 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。

5.2.3 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子任务。

5.2.4 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识别和持续监控。

5.2.5 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。

5.2.6 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。

5.2.7 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，但它应该持续贯穿所有的阶段和迭代。

5.3 《COBIT 设计指南》与《COBIT 实施指南》的关系

*《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 5.2** 描述了两份指南之间的关联点，并且该表的目的是让*《COBIT® 2019 实施指南》*的用户能为*《COBIT® 2019 设计指南》*中的某些阶段和活动找到更为详细的指导。

图 5.2—《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。**	
1	确定当前的治理环境、业务和 IT 痛点、事件，以及触发行动需求的症状。	1.4	了解当前的 I&T 相关问题。
2	识别业务和治理驱动因素以及合规性要求，以改进企业 I&T 治理 (EGIT)；以及评估当前的利益相关方需求。	1.1 1.2 1.3	了解企业战略。 了解企业目标。 了解风险概况。
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。	1.1 1.2 1.3	了解企业战略。 了解企业目标。 了解风险概况。
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。	除了治理设计步骤之外，这些任务与《COBIT 实施指南》中的变革推行 (CE) 任务关系更为密切，并且已在该指南的相应部分适当涵盖。	
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了解并批准高层次方法，并接受不对重大问题采取任何措施可能带来的风险。		
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。**	
1	识别关键企业目标和 IT 相关支持目标。	2.1 2.2	思考企业战略。 思考企业目标并运用 COBIT 目标级联。
2	确定支持业务目标所需的 IT 能力（解决方案和服务）的重要性和类型。	2.2 3.3 3.4 3.5 3.6 3.7	思考企业目标并运用 COBIT 目标级联。 思考 IT 角色。 思考采购模式。 思考 IT 实施方法。 思考技术采用战略。 思考企业规模。
3	识别与当前和未来所需解决方案和服务有关的关键治理问题和缺陷、支持 IT 相关目标所需的企业架构，以及存在的制约或限制。	2.4	思考当前的 I&T 相关问题。
4	确定并选择对支持 IT 相关目标至关重要的流程，适当情况下还包括每个选定流程的关键管理实践。	2.1 2.2	思考企业战略。 思考企业目标并运用 COBIT 目标级联。
5	评估与关键 IT 流程有关的效益/价值实现风险、计划/项目交付风险和服务交付/IT 运营风险。	2.3	思考企业的风险概况。
6	确定并选择对规避风险至关重要的 IT 流程。	2.3	思考企业的风险概况。
7	了解管理层定义的风险接受水平。	1.3 2.3	了解风险概况。 思考企业的风险概况。

图 5.2—《COBIT 设计指南》与《COBIT 实施指南》的关联点（续）			
COBIT 实施指南		**COBIT 设计指南**	
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。**	
8	定义用于执行评估的方法。	流程的评估方法是《*COBIT® 2019 框架：简介和方法中描述的方法*》（基于 CMMI 能力级别）。	
9	记录对当前流程如何切实解决之前选定的管理实践的理解。	**2.1** **2.2** **2.3** **2.4** **3.1** **3.2** **3.3** **3.4** **3.5** **3.6** **3.7**	思考企业战略。 思考企业目标并运用 COBIT 目标级联。 思考企业的风险概况。 思考当前的 I&T 相关问题。 思考威胁环境。 思考合规性要求。 思考 IT 角色。 思考采购模式。 思考 IT 实施方法。 思考技术采用战略。 思考企业规模。
10	分析当前的能力级别。	**4.1** **4.2**	解决固有的优先级冲突。 最终确定治理系统的设计。
11	定义当前的流程能力评级。	**4.1** **4.2**	解决固有的优先级冲突。 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。**	
1	定义改进目标： ● 根据企业的绩效和一致性要求，确定每个流程短期和长期的初始理想目标能力级别。 ● 评估当前能力级别，确定改进的目标级别。 ● 评估竞争对手和同行的能力级别，确定改进目标级别的合理性。 ● 对目标级别（单独和整体）的合理性进行“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。	**4.1** **4.2**	解决固有的优先级冲突。 最终确定治理系统的设计。
2	分析差距： ● 了解当前能力（按属性）并加以运用，将其与目标能力级别进行比较。 ● 尽可能利用现有优势弥补差距，并根据 COBIT 管理实践和活动以及其他良好实践和标准（如 ITIL、国际标准化组织/国际电工委员会 (ISO/IEC) 27000、开放组架构框架 (TOGAF®) 以及项目管理知识体系 (PMBOK®)）的指导，弥补其他差距。 ● 寻找标示待解决根本原因的方式。	**4.1** **4.2**	解决固有的优先级冲突。 最终确定治理系统的设计。
3	识别潜在改进： ● 将差距整合到潜在改进中。 ● 确定未缓解的剩余风险并确保其被正式接受。		

本页特意留白

第 II 部分
执行和示例

第六章
治理系统设计工具包

6.1 引言

本章介绍《*COBIT 设计指南*》的配套工具包，一种基于 Excel® 电子表格的工具，能够简化第 4 章所述治理系统设计工作。

此工具包用于展示本书第 7 章所述的三个示例。此介绍应有助于读者了解此工具包的基础知识，并获悉如何为第 7 章中的示例生成结果。下载的工具包会显示本章描述的相关数值。若要使用该工具，需修改这些数值以适合企业环境。

注：有很多方法用于量化和确定治理和管理目标的优先级。虽然本书及其随附的工具包选择了一种方法，但这并不代表排除其他重要方法，这些方法也能提供可靠的结果。

6.2 工具包的基础知识

此工具包由 Excel 电子表格组成。该电子表格包含：

- 一个描述工具包基本信息和使用方法的介绍和说明选项卡。
- 一个整合治理系统设计工作所有结果的画板选项卡。
- 各设计因素 (DF) 对应的选项卡，其中：
  - 可输入数值并以图形方式展示
  - 将会计算治理和管理目标的优先级分数，并分别以表格格式和图形方式显示在两个图表中
- 两个以图形方式表示已完成步骤结果的摘要选项卡（一个在治理系统设计工作流程的第 2 步之后，另一个在第 3 步之后）
- 包含其他选项卡所用输入值的设计因素对应关系表（为增加电子表格的可读性，这些表已被隐藏）
  - 对应关系表（设计因素 2 *企业目标*除外）包含介于零 (0) 到四 (4) 之间的数值，这些数值表明各个设计因素、风险场景或 I&T 相关问题数值的相应治理/管理目标的相关性。
    - 数值 4 表示相关性最高，数值 0 表示无相关性。
    - 数值反映了专家组确定的平均值。这些数值不能也没有模拟所有给定的独特情况，因此应谨慎使用。但它们能提供良好且具有代表性的指标，可被视作方向性指导。
  - 设计因素 2 *企业目标*的对应关系表略有不同，因为它包含两个对应关系表。其中一个表为企业目标与一致性目标的对应关系，另一个表则是一致性目标与治理和管理目标的对应关系（参见附录 B 和 C）。

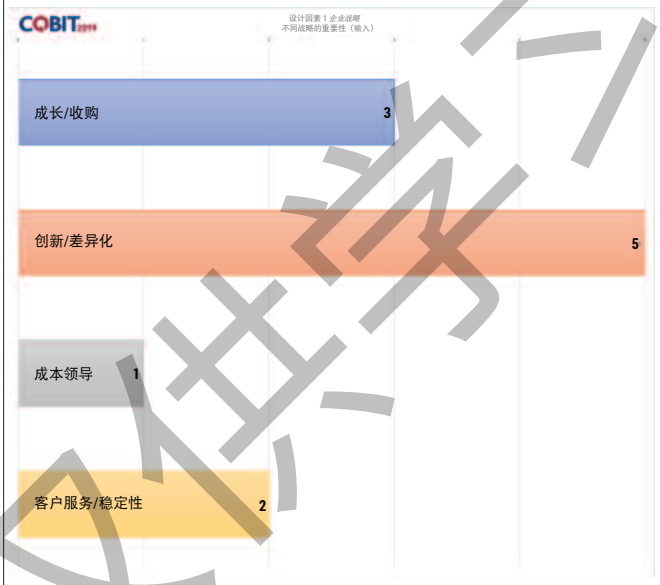
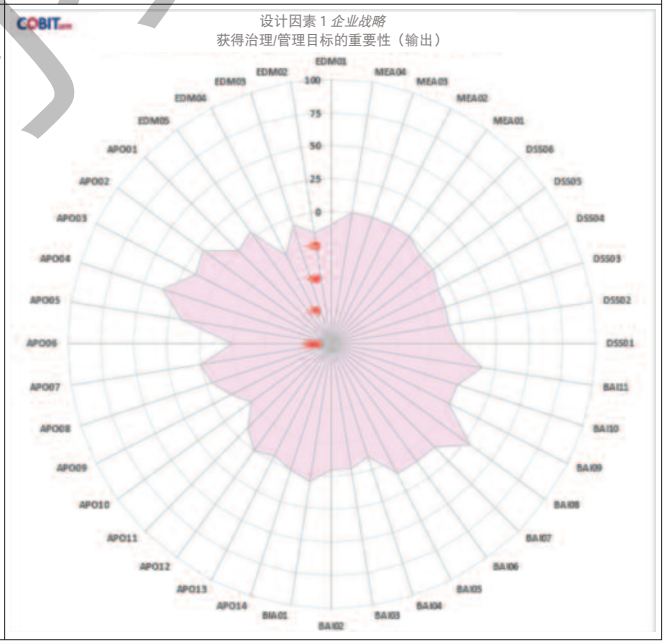
6.3 第 1 步和第 2 步：确定治理系统的初步范围

治理系统设计工作流程的这两个步骤会对企业战略、目标、风险概况和 I&T 相关问题进行评估。这两个步骤会评估前四个设计因素（定义见第 4 章），以确定它们对治理系统初始设计的影响：

1. 企业战略
2. 企业目标（通过目标级联）
3. IT 风险概况
4. I&T 相关问题

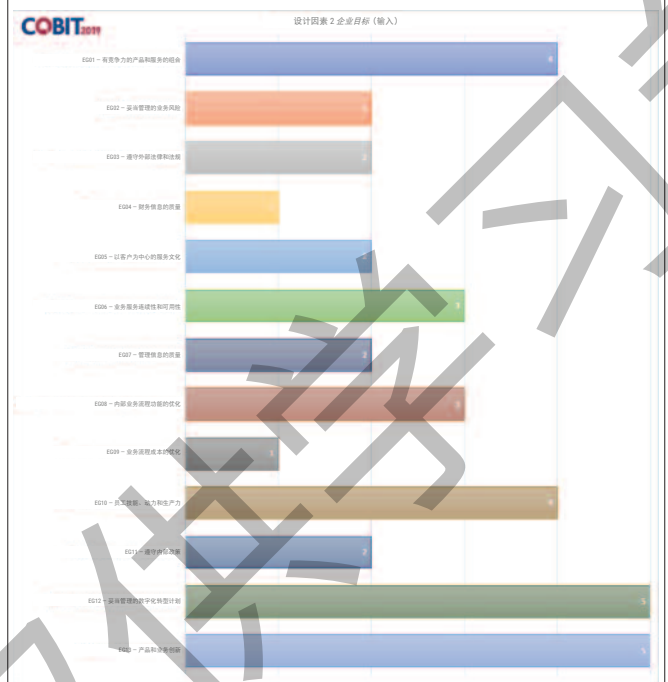
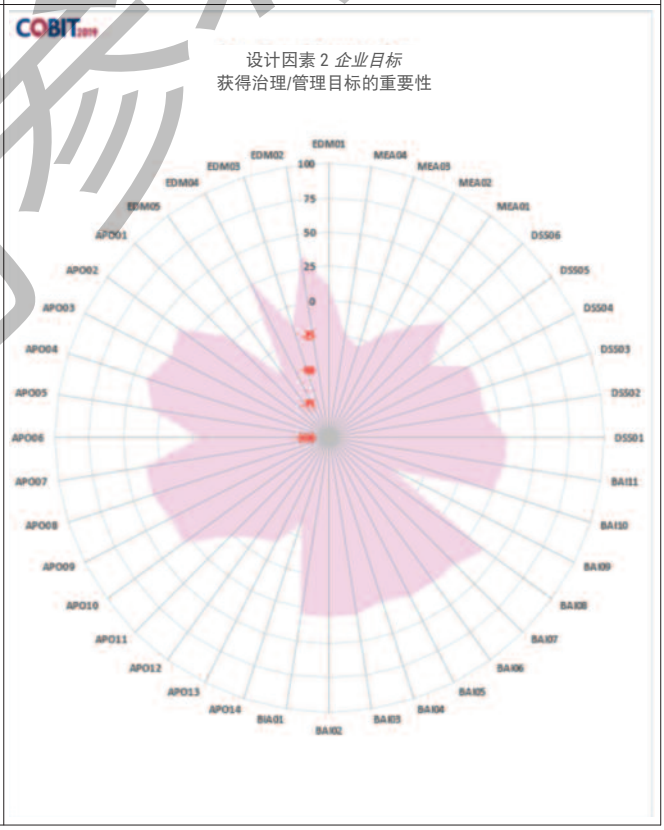
6.3.1 企业战略（设计因素 1）

输入	• 必须对企业战略设计因素四个可能的值（成长/收购、创新/差异化、成本领导、客户服务/稳定性）分别进行评级，评级范围介于 1（不重要）和 5（最重要）之间。 • 建议数值之间保持足够的离散度。
计算	• 工具包利用设计因素 1 *企业战略*的对应关系表对设计因素 1 的输入值执行矩阵计算，从而得出各治理/管理目标的分数。 • 工具包利用设计因素 1 的对应关系表对设计因素 1 的基准数值集执行第二次矩阵计算，从而得出各治理/管理目标的基准分数。 • 工具包随后计算各治理/管理目标的相对重要性，并作为两组值之间的相对差异，以百分比表示并四舍五入到 5。此数值既可以是正数，也可以是负数，表明与基准分数相比，治理/管理目标是更重要还是更不重要。
输出	• 此选项卡的输出部分包含为 40 项 COBIT® 2019 治理和管理目标分别计算得出的相对重要性。 • 这些结果在表格中表示为条形图和蜘蛛图。

输入图范例	输出图范例
	

6.3.2 企业目标和运用 COBIT 目标级联（设计因素 2）

输入	• 必须对 13 项企业目标分别进行评级，评级范围介于 1（不重要）和 5（最重要）之间。 • 利用通用企业目标确定对企业最为重要的目标。建议选择三到五项最为重要的企业目标；高优先级目标太多会弱化目标级联结果的意义。 • 建议数值之间保持足够的离散度。
计算	• 工具在 (1) 评级的企业目标及企业目标与 IT 一致性目标之间的对应关系表；和 (2) 第一次矩阵计算的结果及 IT 一致性目标与治理/管理之间的关系对应表之间执行双矩阵计算。 • 工具对设计因素 2 *企业目标*的基准数值集执行第二组矩阵计算，从而得出各治理/管理目标的基准分数。 • 工具随后计算各治理/管理目标的相对重要性，并作为两组值之间的相对差异，以百分比表示并四舍五入到 5。此数值既可以是正数，也可以是负数，表明与基准分数相比，治理/管理目标是更重要还是更不重要。
输出	• 此表格的输出部分包含为 40 项 COBIT® 2019 治理和管理目标分别计算得到的相对重要性。 • 这些结果在表格中表示为条形图和蜘蛛图。

输入图范例	输出图范例
	

6.3.3 企业风险概况（设计因素 3）

输入	• 风险概况设计因素所包含的 19 个风险类别必须分别按下述方式进行评级：
	  ■ 风险发生后的影响，此值应介于 1（不重要）和 5（重要）之间
	  ■ 风险发生的可能性，此值应介于 1（极不可能）和 5（极有可能）之间
	• 工具将根据影响和可能性的评分组合为每个风险类别确定风险等级（极高、高、中、低）。
	• 建议数值之间保持足够的离散度。

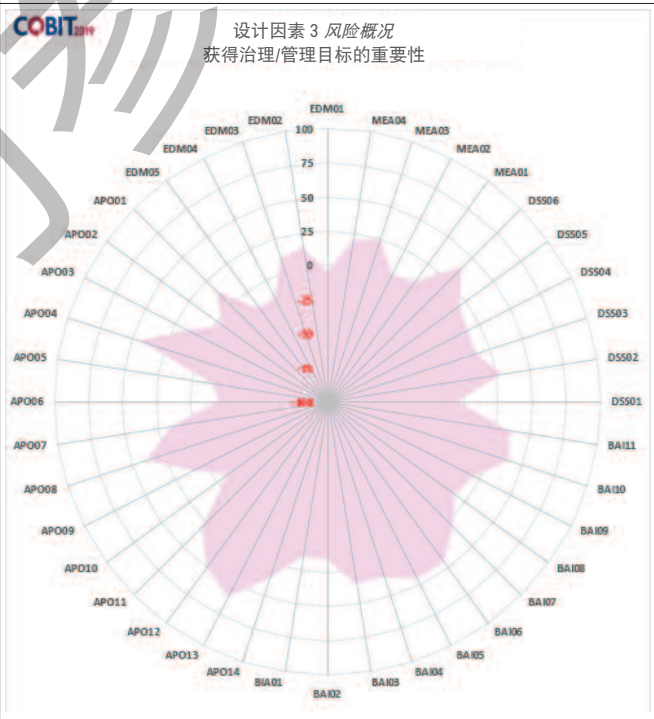
计算	• 工具利用设计因素 3 *风险概况*的对应关系表为风险评级执行矩阵计算，从而得出各治理/管理目标的分数。 • 工具利用设计因素 3 的对应关系表对设计因素 3 的基准风险评级集执行第二次矩阵计算，从而得出各治理/管理目标的基准分数。 • 工具随后计算各治理/管理目标的相对重要性，并作为两组值之间的相对差异，以百分比表示并四舍五入到 5。此数值既可以是正数，也可以是负数，表明与基准分数相比，治理/管理目标是更重要还是更不重要。
输出	• 此工具的输出部分包含为 40 项 COBIT® 2019 治理和管理目标分别计算得到的相对重要性。 • 这些结果在表格中表示为条形图和蜘蛛图。

输入表范例

风险情景类别	影响 (1-5)	可能性 (1-5)	风险评级	基准
IT 投资决策制定、投资组合定义和维护	2	2		
计划和项目生命周期管理	4	3		
IT 成本和监督	2	2		
IT 专业知识、技能和行为	4	4		
企业/IT 架构	2	2		
IT 运营基础设施事故	3	2		
未授权的行动	3	4		
软件采用/使用问题	4	3		
硬件事故	2	2		
软件故障	3	3		
逻辑攻击（黑客攻击、恶意软件等）	4	5		
第三方/供应商事故	2	2		
违规	3	3		
地缘政治问题	2	2		
劳工行动	1	3		
自然灾害	3	3		
基于技术的创新	5	3		
环境	2	3		
数据和信息管理	4	4		

	极高风险
	高风险
	中度风险
	低风险

输出图范例



6.3.4 企业的当前 I&T 相关问题（设计因素 4）

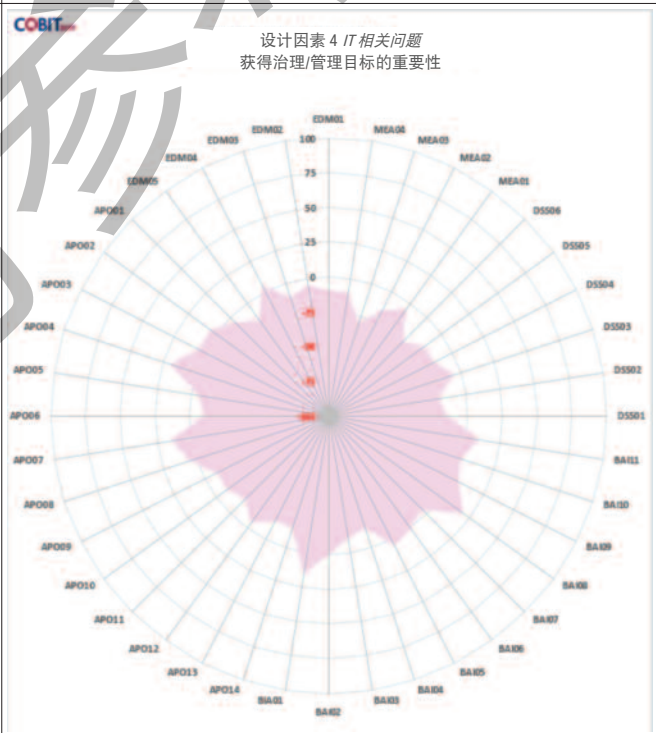
输入	• 必须对 I&T 相关问题设计因素的 20 个 I&T 相关问题分别进行评级，评级范围介于 1（无问题）和 3（严重问题）之间。将数字 1、2 或 3 键入工具；工具随后根据此评级对应的键将其自动转换为符号。 • 建议数值之间保持足够的离散度。
计算	• 工具利用设计因素 4 *I&T 相关问题*的对应关系表对设计因素 4 的输入值执行矩阵计算，从而得出各治理/管理目标的分数。 • 工具利用设计因素 4 的对应关系表对设计因素 4 的基准数值集执行第二次矩阵计算，从而得出各治理/管理目标的基准分数。 • 工具随后计算各治理/管理目标的相对重要性，并作为两组值之间的相对差异，以百分比表示并四舍五入到 5。此数值既可以是正数，也可以是负数，表明与基准分数相比，治理/管理目标是更重要还是更不重要。
输出	• 此选项卡的输出部分包含为 40 项 COBIT® 2019 治理和管理目标分别计算得到的相对重要性。 • 这些结果在表格中表示为条形图和蜘蛛图。

输入表范例

IT 相关问题	重要性 (1-3)	基准
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	1	2
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	1	2
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	2	2
IT 外包商的服务交付问题	2	2
不符合 IT 相关法规或合同要求	1	1
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	1	2
重大的隐性和反常的 IT 支出，即用户部门在正常的 IT 投资决策机制控制范围和批准的预算之外的 I&T 支出	2	2
多个举措之间的重复或重叠，或其他形式的资源浪费	3	2
IT 资源不足，员工技能欠缺或员工倦怠/不满	3	2
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	2	2
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	2	2
复杂的 IT 运营模式和/或缺乏明确的 IT 相关决策机制	2	1
过高的 IT 成本	1	1
当前 IT 架构和系统导致新举措或创新的实施受阻或失败	3	2
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	3	1
各种来源的数据经常出现数据质量和整合方面的问题	1	1
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、质量控制以及其他问题	1	2
业务部门在企业 IT 部门极少或者根本没有参与的情况下实施自己的信息解决方案（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）	2	2
忽视和/或违反隐私法规	1	1
无法利用新技术或使用 I&T 进行创新	3	1

1	无问题
2	问题
3	严重问题

输出图范例



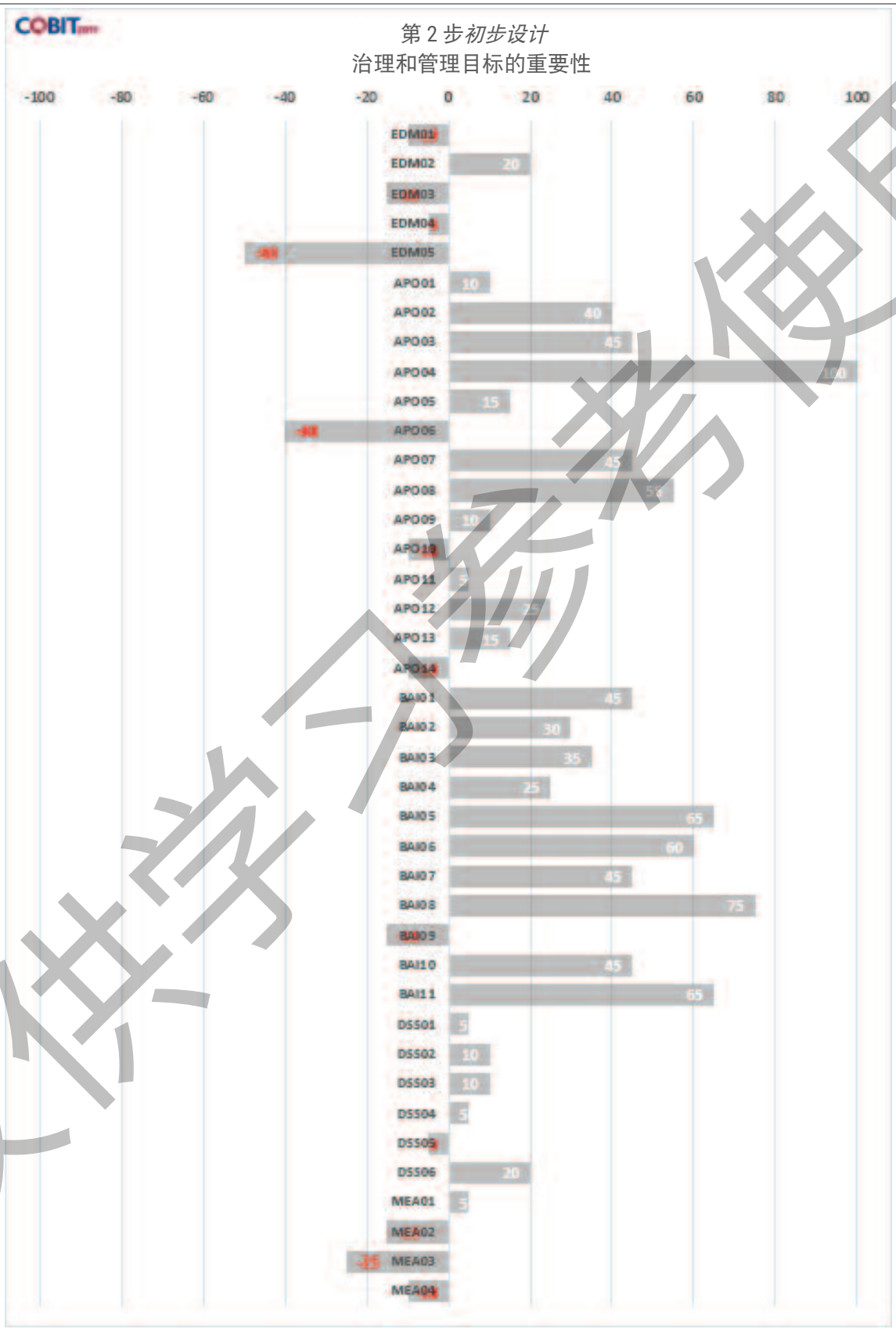
6.3.5 总结

输入	• 不适用

计算	• 工具对计算所得的与前四个设计因素有关的治理/管理目标的重要性分数进行加权求和。
	• 可在画板选项卡中输入权重，该值默认设置为 1。例如，如果企业战略比企业目标、风险或 I&T 相关问题更为重要，则可修改权重。
	• 然后将获得的结果按 100 分进行标准化（包含正、负值）并反映在第 2 步摘要选项卡上。
	  ■ 最高值（正值或负值）对应 100 分。
	  ■ 随后对照此值按比例指定所有其他值。
	• 由此得出的分数列表不仅能提供所有治理/管理目标之间相对重要性的可靠视图，而且还能表示绝对重要性。此输出不仅让企业能够排定治理/管理目标的相对优先级，而且还能定义适当的目标能力级别。

输出	• 第 2 步摘要选项卡包含为 40 项 COBIT® 2019 治理和管理目标分别计算得到的相对重要性。 • 这些结果将表示为表格格式（在画板选项卡上）和条形图格式（在第 2 步摘要选项卡上）

输出图范例



注：如果按照第 6 章提供的输入范例所示输入设计因素 1 到 4，则前述范例图将与各设计因素的范例图保持一致，因为它代表了实际结果。

6.4 第 3 步：优化治理系统的范围

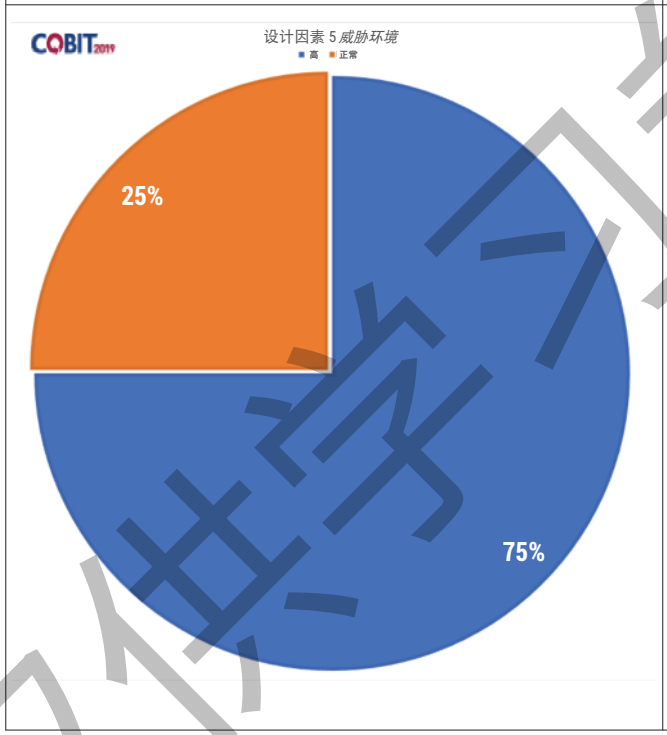
在此步骤中，需要基于剩余设计因素的评估进一步优化治理系统的初始范围：

1. 威胁环境
2. 合规性要求
3. IT 角色
4. IT 采购模式
5. IT 实施方法
6. 技术采用战略
7. 企业规模（请注意，该工具并未包含此设计因素；请参见第 6.4.7 节获取更多详情）

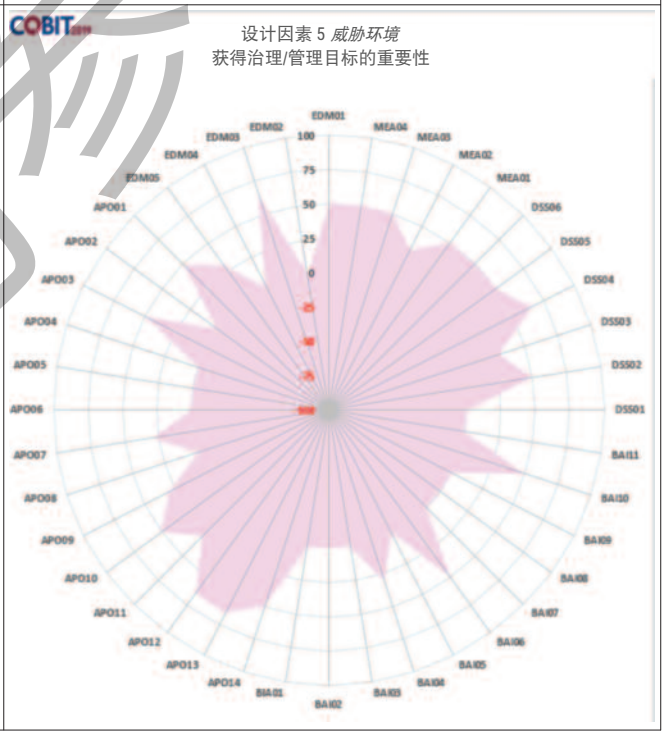
6.4.1 威胁环境（设计因素 5）

输入	• 必须对威胁环境设计因素的两个可能值（高和正常）分别进行评级，评级范围介于 0% 和 100% 之间。两个值的总和必须为 100%。 • 很多企业会将 100% 分配给其中一个类别。由于企业运营的一部分会面临较高威胁环境，而其他部分则面临常见的威胁环境，所以可使用此选项来分配百分比。
计算	• 工具利用设计因素 5 *威胁环境*的对应关系表对设计因素 5 的输入值执行矩阵计算，从而得出各治理/管理目标的分数。 • 工具利用设计因素 5 的对应关系表对设计因素 5 的基准数值集执行第二次矩阵计算，从而得出各治理/管理目标的基准分数。 • 工具随后计算各治理/管理目标的相对重要性，并作为两组值之间的相对差异，以百分比表示并四舍五入到 5。此数值既可以是正数，也可以是负数，表明与基准分数相比，治理/管理目标是更重要还是更不重要。
输出	• 此选项卡的输出包含为 40 项 COBIT® 2019 治理和管理目标分别计算得到的相对重要性。 • 这些结果在表格中表示为条形图和蜘蛛图。

输入图范例

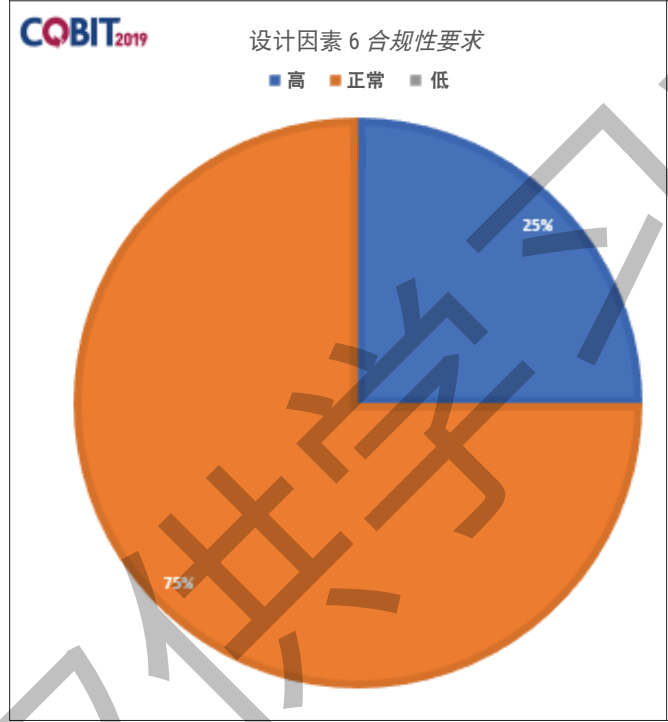
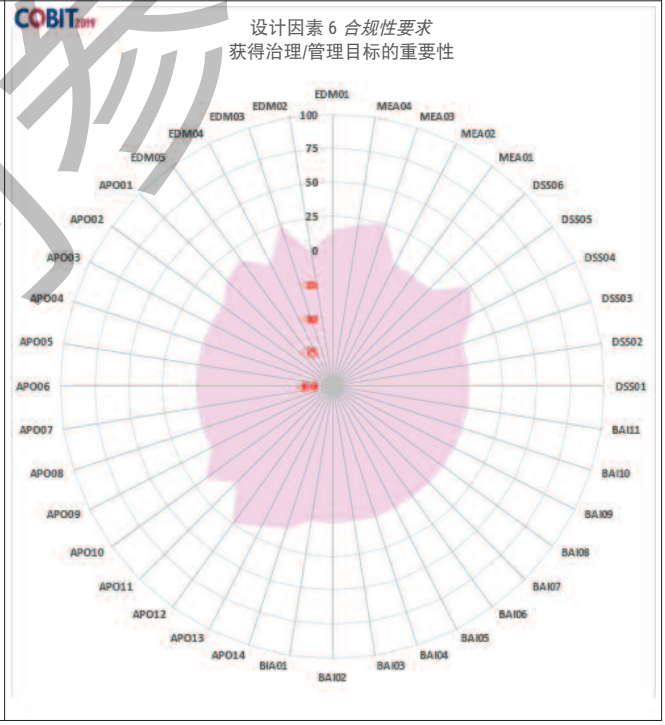


输出图范例



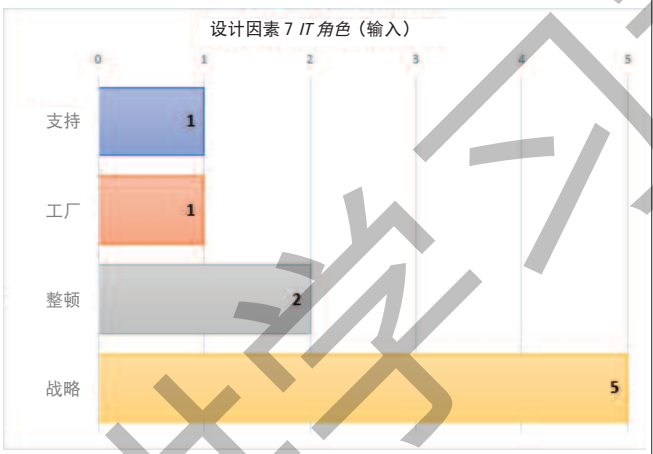
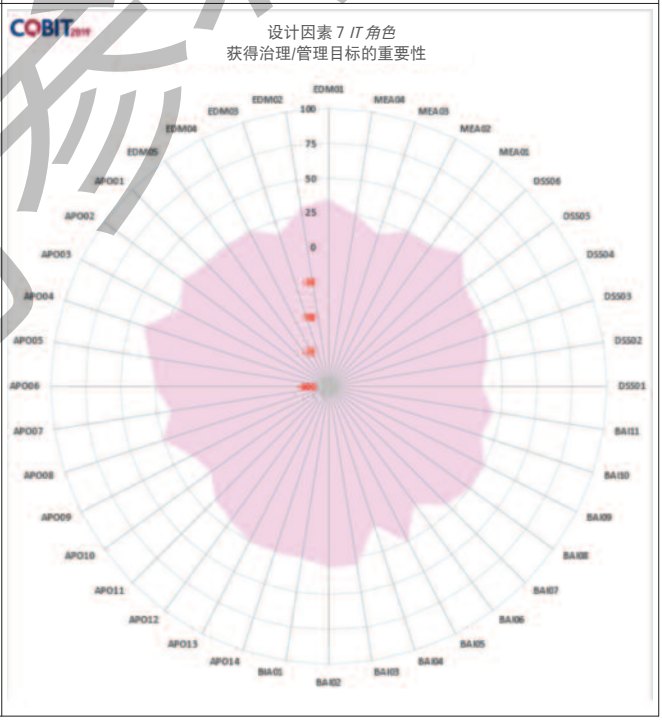
6.4.2 合规性要求（设计因素 6）

输入	• 必须对合规性要求设计因素的三个可能值分别进行评级，评级范围介于 0% 和 100% 之间。三个值的总和必须为 100%。 • 很多企业会将 100% 分配给其中一个类别。但如果企业的 IT 环境相当庞大，并且某些部分会受到严格的合规性监管，而其他部分则面临不太严格的监管，则可使用此选项来分配不同的百分比。
计算	• 工具利用设计因素 6 *合规性要求*的对应关系表对设计因素 6 的输入值执行矩阵计算，从而得出各治理/管理目标的分数。 • 工具利用设计因素 6 的对应关系表对设计因素 6 的基准数值集执行第二次矩阵计算，从而得出各治理/管理目标的基准分数。 • 工具随后计算各治理/管理目标的相对重要性，并作为两组值之间的相对差异，以百分比表示并四舍五入到 5。此数值既可以是正数，也可以是负数，表明与基准分数相比，治理/管理目标是更重要还是更不重要。
输出	• 此选项卡的输出包含为 40 项 COBIT® 2019 治理和管理目标分别计算得到的相对重要性。 • 这些结果在表格中表示为条形图和蜘蛛图。

输入图范例	输出图范例
	

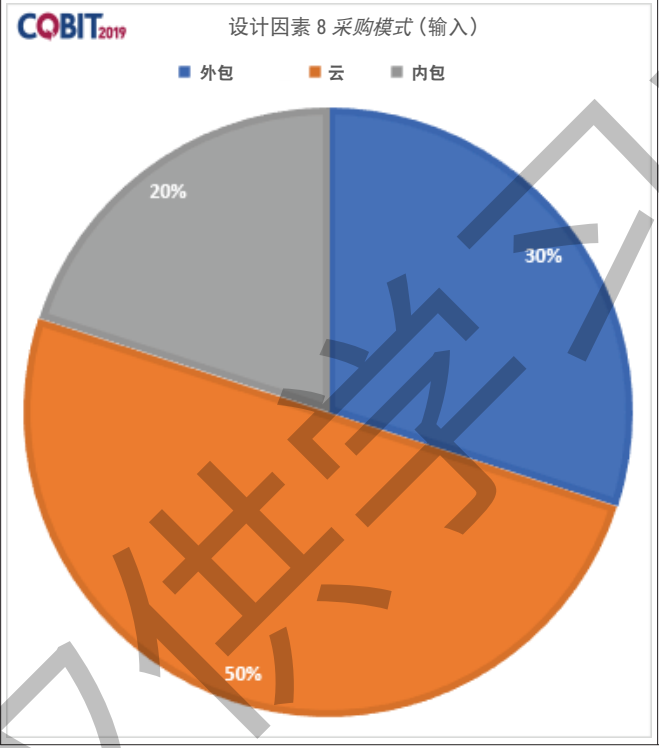
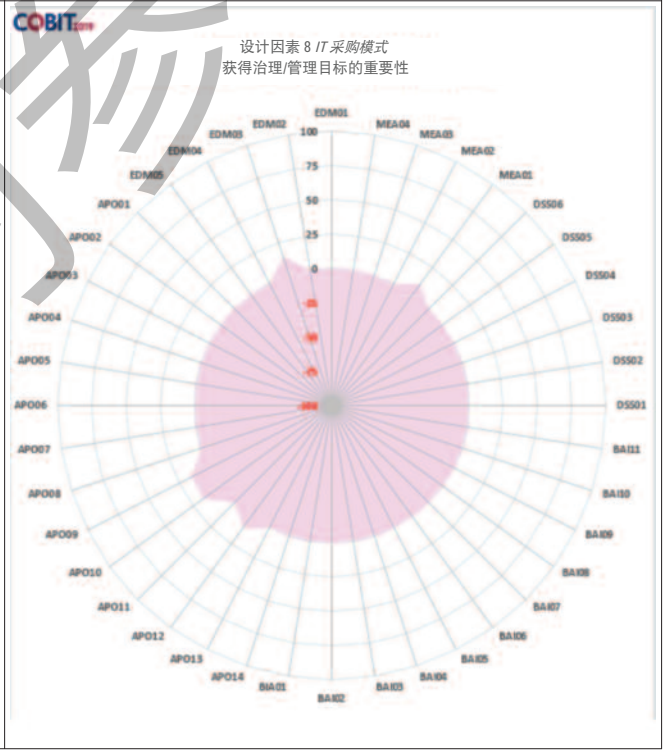
6.4.3 IT 角色（设计因素 7）

输入	• 必须对 IT 角色设计因素的四个可能值（支持、工厂、整顿和战略）分别进行评级，评级范围介于 1（不重要）和 5（最重要）之间。 • 建议数值之间保持足够的离散度。
计算	• 工具利用设计因素 7 *IT 角色*的对应关系表对设计因素 7 的输入值执行矩阵计算，从而得出各治理/管理目标的分数。 • 工具利用设计因素 7 的对应关系表对设计因素 7 的基准数值集执行第二次矩阵计算，从而得出各治理/管理目标的基准分数。 • 工具随后计算各治理/管理目标的相对重要性，并作为两组值之间的相对差异，以百分比表示并四舍五入到 5。此数值既可以是正数，也可以是负数，表明与基准分数相比，治理/管理目标是更重要还是更不重要。
输出	• 此选项卡的输出包含为 40 项 COBIT® 2019 治理和管理目标分别计算得到的相对重要性。 • 这些结果在表格中表示为条形图和蜘蛛图。

输入图范例	输出图范例
	

6.4.4 IT 采购模式（设计因素 8）

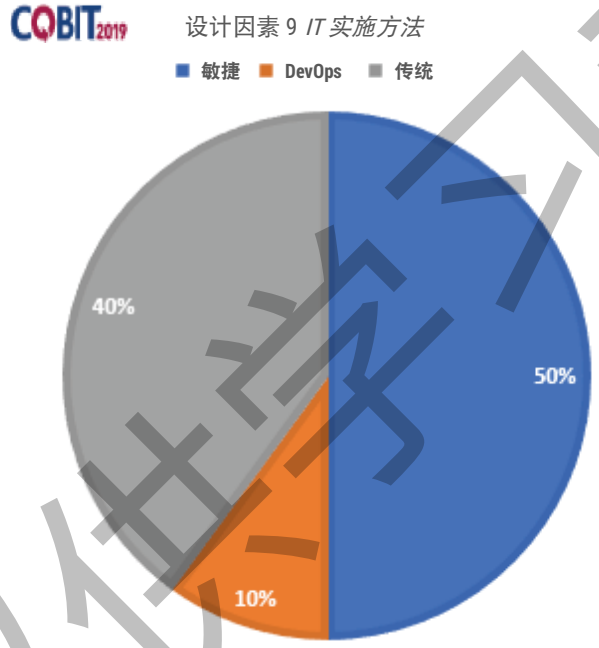
输入	• 必须对 IT 采购模式设计因素的三个可能值（外包、云和内包）分别进行评级，评级范围介于 0% 和 100% 之间。三个值的总和必须为 100%。 • 请注意，还有第四类 — 混合分类。工具中并未显示此分类，因为根据定义，将百分比分配给其他三个值中的多个值便会创建混合模型。
计算	• 工具利用设计因素 8 *IT 采购模式*的对应关系表对此设计因素的输入值执行矩阵计算，从而得出各治理/管理目标的分数。 • 工具利用设计因素 8 的对应关系表对设计因素 8 的基准数值集执行第二次矩阵计算，从而得出各治理/管理目标的基准分数。 • 工具随后计算各治理/管理目标的相对重要性，并作为两组值之间的相对差异，以百分比表示并四舍五入到 5。此数值既可以是正数，也可以是负数，表明与基准分数相比，治理/管理目标是更重要还是更不重要。
输出	• 此选项卡的输出部分包含为 40 项 COBIT® 2019 治理和管理目标分别计算得到的相对重要性。 • 这些结果在表格中表示为条形图和蜘蛛图。

输入图范例	输出图范例
	

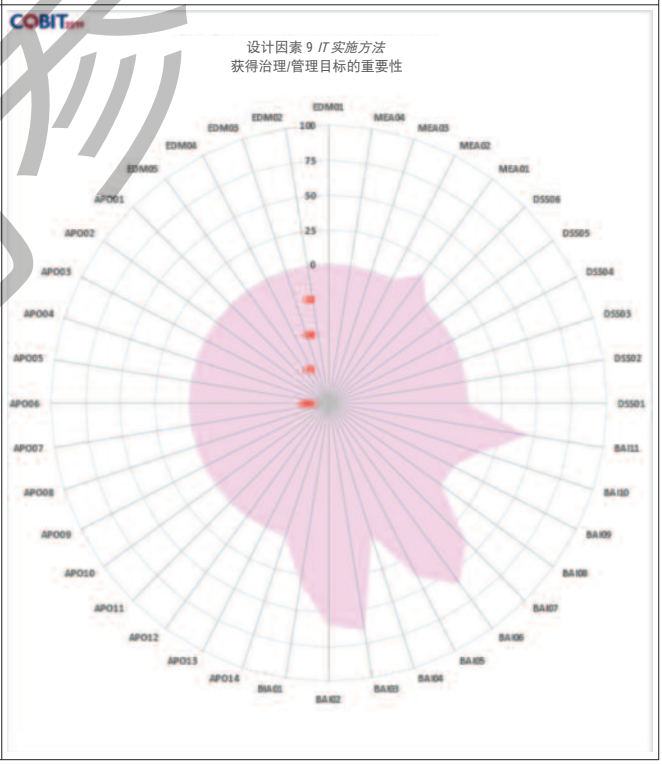
6.4.5 IT 实施方法（设计因素 9）

输入	• 必须对 IT 实施方法设计因素的三个可能值（敏捷、DevOps 和传统）分别进行评级，评级范围介于 0% 和 100% 之间。三个值的总和必须为 100%。 • 请注意，还有第四类 — 混合分类。工具中并未显示此分类，因为根据定义，将百分比分配给其他三个值中的多个值便会创建混合模型。
计算	• 工具利用设计因素 9 *IT 实施方法*的对应关系表对设计因素 9 的输入值执行矩阵计算，从而得出各治理/管理目标的分数。 • 工具利用设计因素 9 的对应关系表对设计因素 9 的基准数值集执行第二次矩阵计算，从而得出各治理/管理目标的基准分数。 • 工具随后计算各治理/管理目标的相对重要性，并作为两组值之间的相对差异，以百分比表示并四舍五入到 5。此数值既可以是正数，也可以是负数，表明与基准分数相比，治理/管理目标是更重要还是更不重要。
输出	• 此选项卡的输出部分包含为 40 项 COBIT® 2019 治理和管理目标分别计算得到的相对重要性。 • 这些结果在表格中表示为条形图和蜘蛛图。

输入图范例

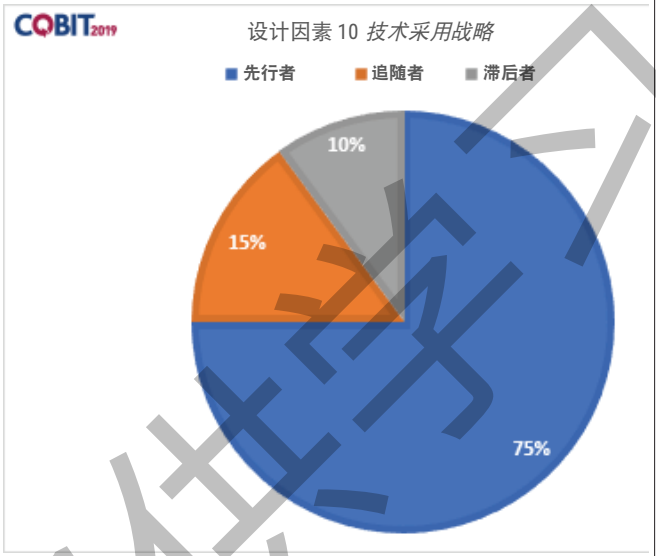
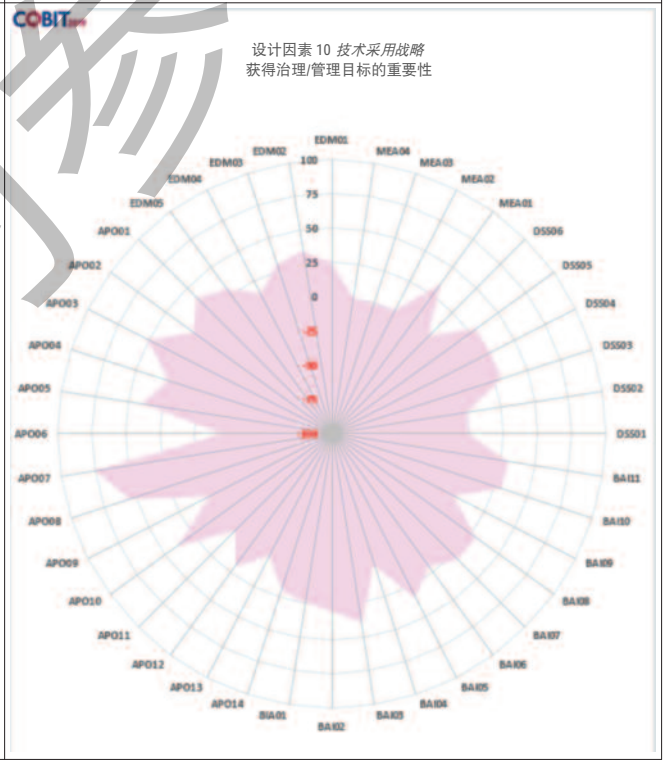


输出图范例



6.4.6 技术采用战略（设计因素 10）

输入	• 必须对技术采用战略设计因素的三个可能值（先行者、追随者、滞后者）分别进行评级，评级范围介于 0% 和 100% 之间。三个值的总和必须为 100%。 • 很多企业可能会将 100% 分配给其中一个类别。但如果企业的 IT 环境相当庞大，并且不同的领域会以不同的节奏采用技术，则可利用此选项来分配不同的百分比。
计算	• 工具利用设计因素 10 *技术采用战略*的对应关系表对设计因素 10 的输入值执行矩阵计算，从而得出各治理/管理目标的分数。 • 工具利用设计因素 10 的对应关系表对设计因素 10 的基准数值集执行第二次矩阵计算，从而得出各治理/管理目标的基准分数。 • 工具随后计算各治理/管理目标的相对重要性，并作为两组值之间的相对差异，以百分比表示并四舍五入到 5。此数值既可以是正数，也可以是负数，表明与基准分数相比，治理/管理目标是更重要还是更不重要。
输出	• 此选项卡的输出包含为 40 项 COBIT® 2019 治理和管理目标分别计算得到的相对重要性。 • 这些结果在表格中表示为条形图和蜘蛛图。

输入图范例	输出图范例
	

6.4.7 企业规模（设计因素 11）

企业规模设计因素仅表明是否应使用中小型企业焦点领域指南，而非核心 COBIT 指南。[27] 企业规模不会影响治理和管理目标的优先级和目标能力级别。

6.4.8 总结

输入	• 不适用

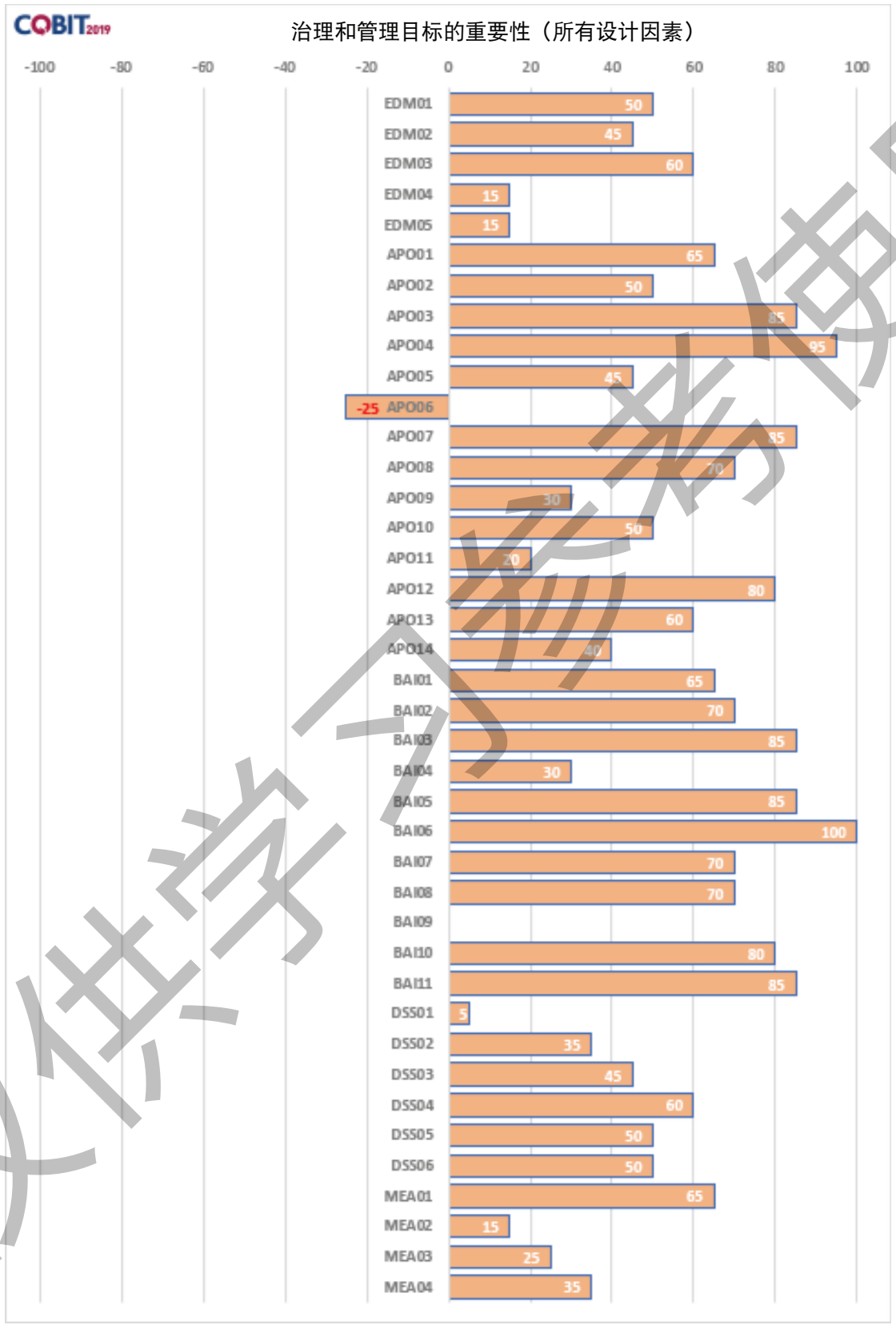
计算	• 工具对计算所得的与设计因素 5 到 10 有关的治理/管理目标的重要性分数进行加权求和，并将其与第 2 步*治理系统初始设计*的结果相结合。
	• 可在画板选项卡中输入权重，该值默认设置为 1。例如，如果合规性要求更为重要（因为企业在受到严格监管的行业中运营），则可修改权重。
	• 然后将获得的结果按 100 分进行标准化。
	  ■ 最高值（正值或负值）对应 100 分。
	  ■ 随后对照此值按比例指定所有其他值。
	• 由此得出的分数列表不仅能提供所有治理/管理目标之间相对重要性的可靠视图，而且还能表示绝对重要性。此输出不仅让企业能够排定治理/管理目标的相对优先级，而且还能定义适当的目标能力级别。

输出	• 第 3 步摘要选项卡包含为 40 项 COBIT® 2019 治理和管理目标分别计算得到的相对重要性。 • 这些结果将表示为表格格式（在画板选项卡上）和条形图格式（在第 3 步摘要选项卡上）

注：如果按照第 6 章所示的输入数据输入设计因素 5 到 10，则下述范例图将与各设计因素的范例图保持一致，因为它代表了实际结果。

[27] *《COBIT® 2019 设计指南：信息和技术治理解决方案的设计》*出版时，中小型企业焦点领域的内容正在制定中，尚未发布。

输出图范例



第七章
示例

7.1 引言

为了阐明治理系统的设计流程，本章将第 4 章所述工作流程应用于两个虚构示例和一个真实的案例研究。这些示例包括：

1. 制造企业（第 7.2 节）
2. 中型创新公司（第 7.3 节）
3. 知名政府机构（第 7.4 节）

7.2 示例 1：制造企业

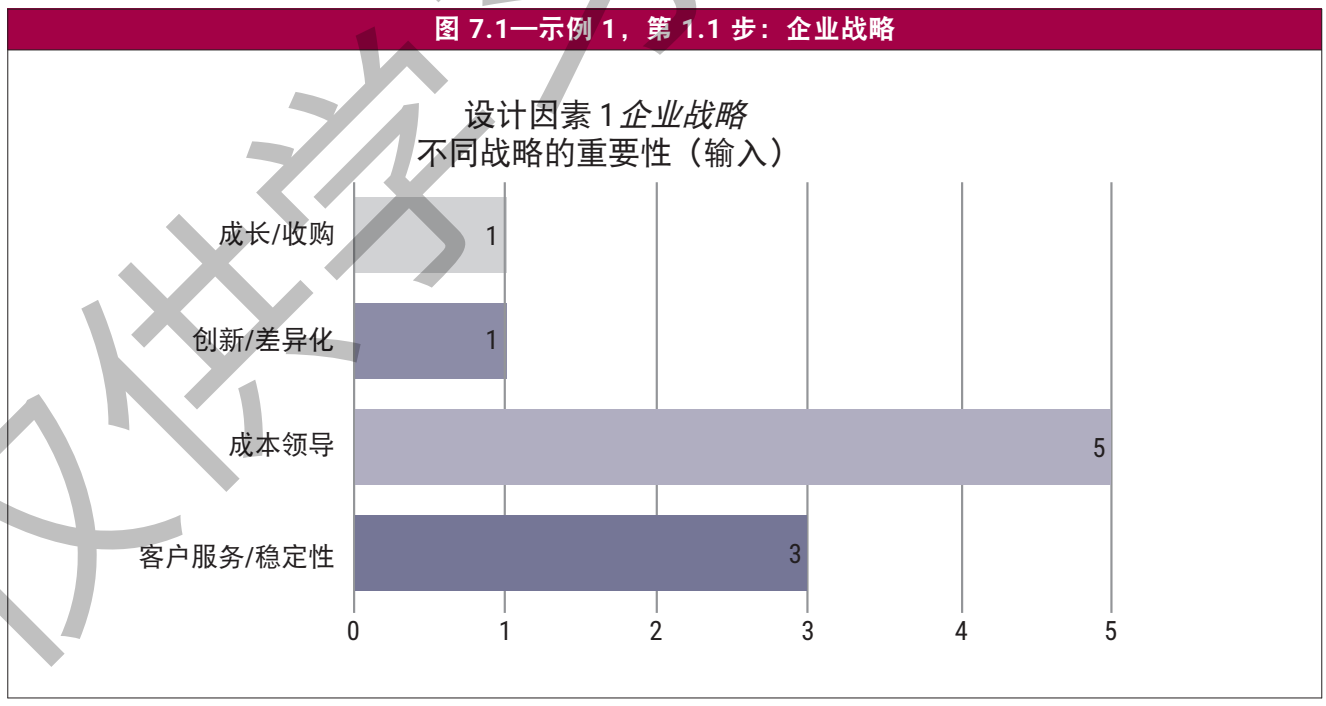
这是一家从事商品制造的大型企业，它强烈关注成本控制，希望成为所在行业中的成本控制领导者。该企业认为 I&T 仅是辅助提升运营效率与效果的支持部门。虽然 IT 仅仅是个支持部门，但该企业却极为依赖它。该企业采用传统方法进行开发和运营，对新技术的采用迟疑不决。该企业最近不仅遭受恶意软件攻击，还遇到了很多 IT 运营问题。该企业在内部部署和运营关键 IT 设备。

7.2.1 第 1 步：了解企业环境和战略

治理设计工作的第一步是总结企业的内外部环境。

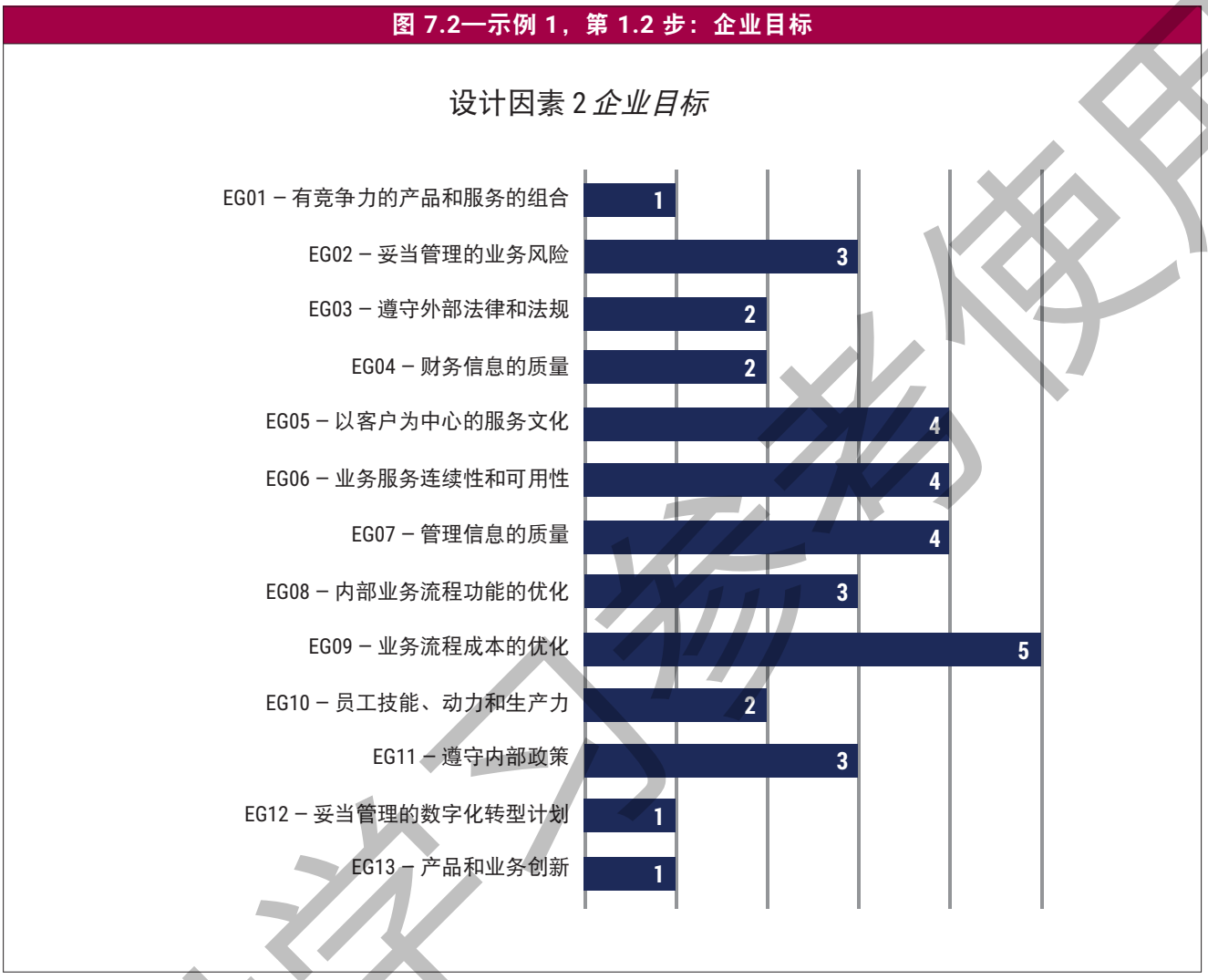
第 1.1 步：了解企业战略 — 将**成本领导**作为主要关注点，将**图 7.1** 所述的**客户服务/稳定性**作为次要关注点。

图 7.1—示例 1，第 1.1 步：企业战略



第 1.2 步：了解企业目标 — 该企业对下图所示的 13 个通用企业目标进行了评级（评级范围为 1 到 5 分）。**图 7.2** 表明，EG09 *业务流程成本的优化*是评级最高的企业目标。

图 7.2—示例 1，第 1.2 步：企业目标



第 1.3 步：了解风险概况 — 通过整体风险分析获得风险概况，下列是识别出的最高级别风险（在**图 7.3** 的风险评级列中以红色圆点标识）：IT 运营基础设施事件、未经授权的操作、软件采用/使用问题、硬件事件、软件故障和逻辑攻击。（此处为宽泛的分类，各类别风险情景的详细示例，请参阅第 2.6 节。）

图 7.3—示例 1，第 1.3 步：风险概况

设计因素 3 *风险概况*

风险情景类别	影响 (1-5)	可能性 (1-5)	风险评级
IT 投资决策制定、投资组合定义和维护	4	3	🟡
计划和项目生命周期管理	3	1	⚫
IT 成本和监督	2	2	🟢
IT 专业知识、技能和行为	3	3	🟡
企业/IT 架构	2	1	⚫
IT 运营基础设施事故	4	4	🔴
未授权的行动	5	4	🔴
软件采用/使用问题	4	4	🔴
硬件事故	4	4	🔴
软件故障	4	4	🔴
逻辑攻击（黑客攻击、恶意软件等）	5	3	🔴
第三方/供应商事故	2	4	🟢
违规	1	3	⚫
地缘政治问题	2	1	⚫
劳工行动	4	2	🟢
自然灾害	4	2	🟢
基于技术的创新	4	1	🟢
环境	2	2	🟢
数据和信息管理	4	3	🟡

🔴	极高风险
🟡	高风险
🟢	中度风险
⚫	低风险

第 1.4 步：了解 I&T 现存问题 — 对现状进行分析（评级范围为 1 到 3 分）可获得**图 7.4** 所述的 I&T 现存问题评估。以下问题为该企业所面临的重要问题：重大事故、外包商的服务交付问题、隐性 IT 成本和 IT 总成本。

图 7.4—示例 1，第 1.4 步：I&T 相关问题

值	重要性 (1-3)	*基准*
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	✔	*2*
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	!	*2*
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	X	*2*
IT 外包商的服务交付问题	X	*2*
不符合 IT 相关法规或合同要求	✔	*2*
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	✔	*2*
重大的隐性和反常的 IT 支出，即用户部门在正常的 IT 投资决策机制控制范围和批准的预算之外的 I&T 支出	X	*2*
多个举措之间的重复或重叠，或其他形式的资源浪费	✔	*2*
IT 资源不足，员工技能欠缺或员工倦怠/不满	!	*2*
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	✔	*2*
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	✔	*2*
复杂的 IT 运营模式和/或缺乏明确的 IT 相关决策机制	✔	*2*
过高的 IT 成本	X	*2*
当前 IT 架构和系统导致新举措或创新的实施受阻或失败	✔	*2*
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	✔	*2*
各种来源的数据经常出现数据质量和整合方面的问题	!	*2*
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、质量控制以及其他问题	✔	*2*
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	!	*2*
忽视和/或违反隐私法规	✔	*2*
无法利用新技术或使用 I&T 进行创新	✔	*2*

✔	无问题
!	问题
X	严重问题

7.2.2 第 2 步：确定治理系统的初步范围

利用第 1 步收集到的（部分或全部）信息，确定治理系统的初步范围。第 2 步将关于企业目标、企业战略和风险概况的信息转换为治理组件。

第 2.1 步：思考企业战略 — **图 7.5** 为第 1.1 步中确定的企业战略。**图 7.6** 表明了这些战略对治理和管理目标的相对影响。

图 7.5—示例 1，第 2.1 步：企业战略

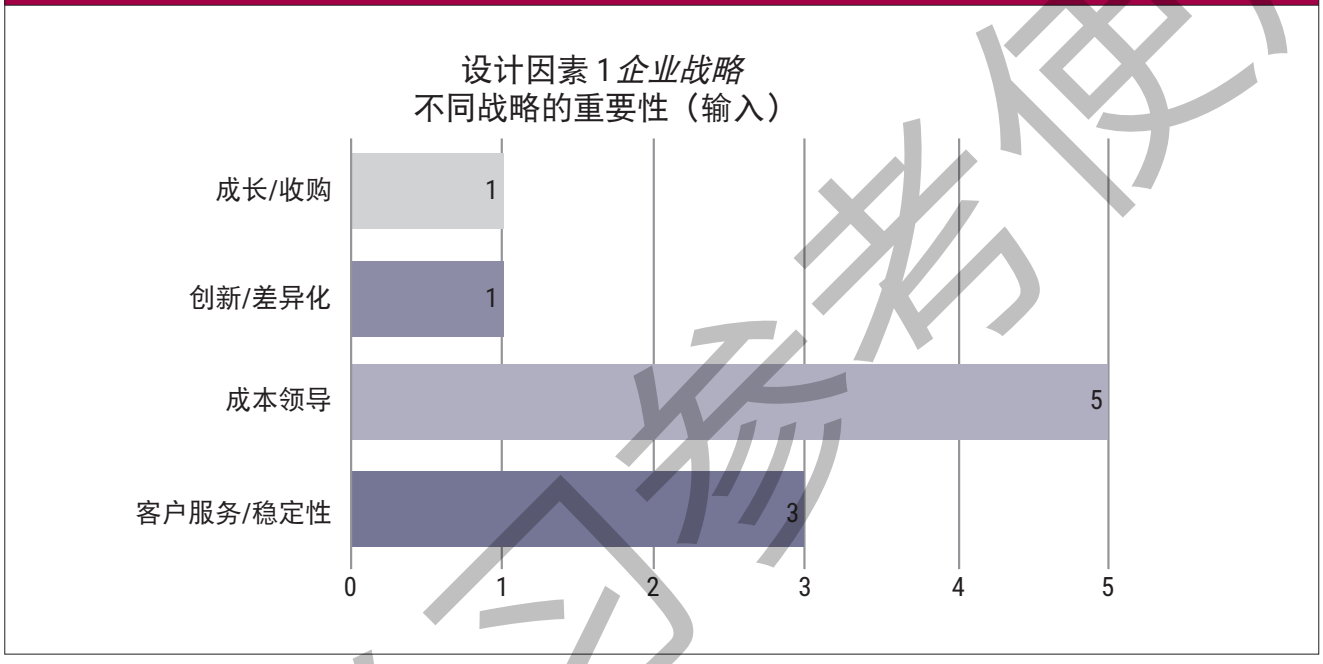
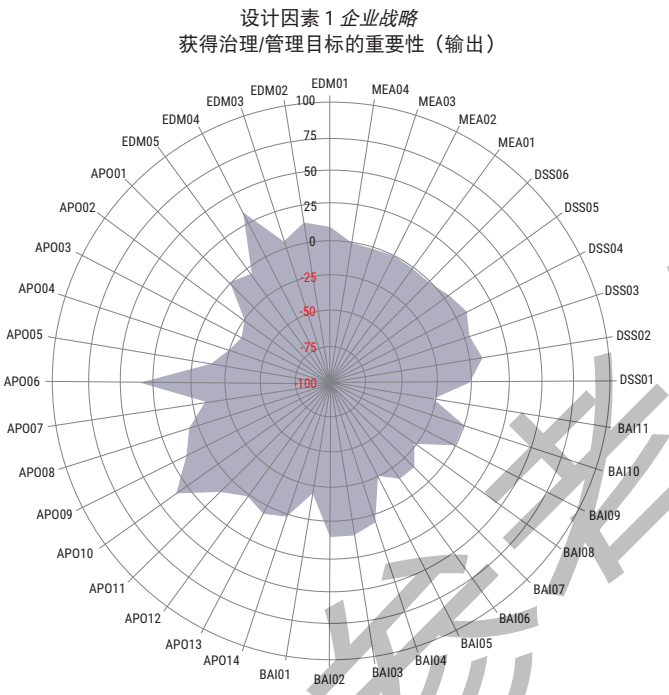


图 7.6—示例 1，第 2.1 步：针对设计因素 1 *企业战略*获得治理/管理目标的重要性



除了**图 7.6** 突出显示的治理和管理流程以外，还需注意下列组件：

- 专注于 IT 成本和预算能力
- 文化和行为组件的影响
- 服务、基础设施和应用程序组件的贡献（例如，实现控制自动化、提高效率）

第 2.2 步：思考企业目标并运用 COBIT 目标级联 — 此时需要按照第 1.2 步评级结果，运用 COBIT 目标级联来确定哪些治理和管理目标与需要优先实现的企业目标有关（**图 7.7**）。**图 7.8** 表明这些经过评级的企业目标对治理和管理目标的影响。

图 7.7—示例 1，第 2.2 步：企业目标

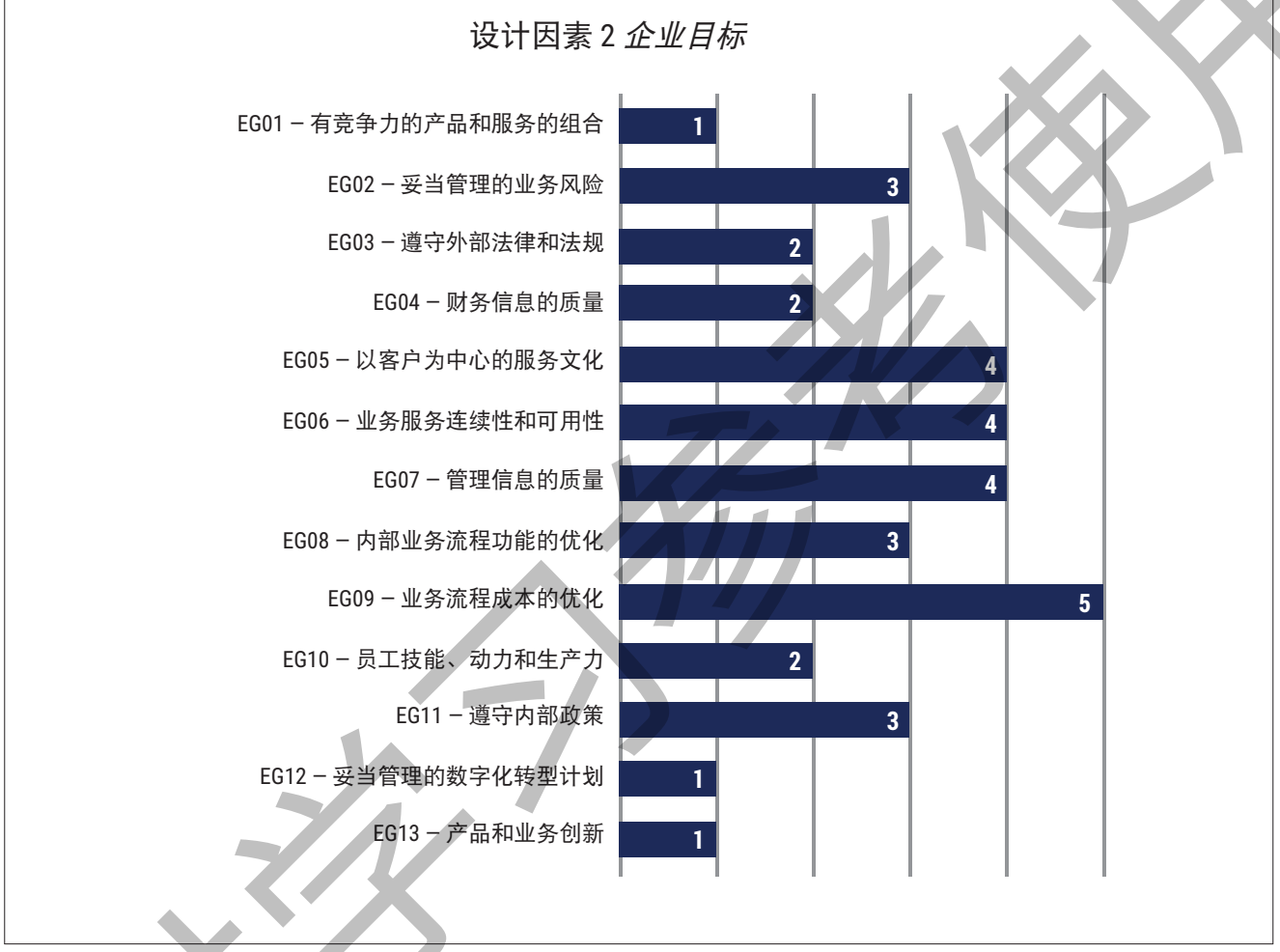
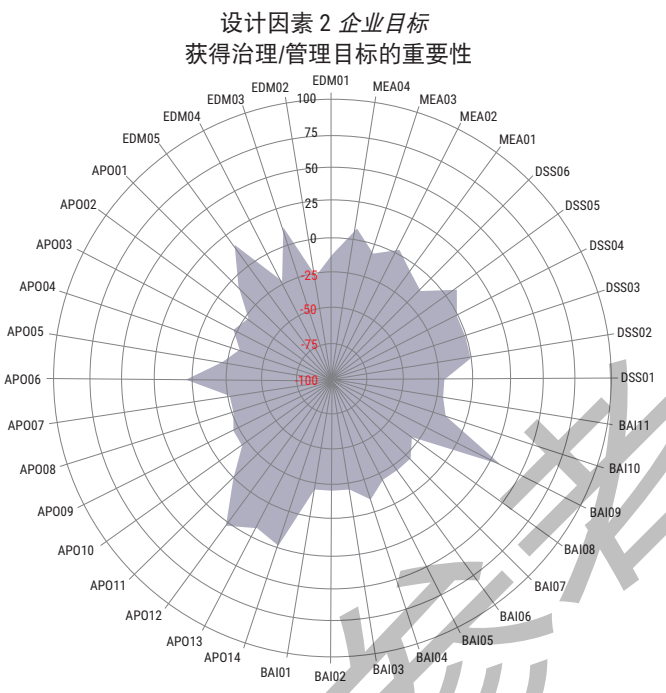


图 7.8—示例 1，第 2.2 步：针对设计因素 2 *企业目标*获得治理/管理目标的重要性



第 2.3 步：思考企业的风险概况 — 第 1.3 步已在总体层面识别和分析 IT 风险类别（**图 7.9**）。基于风险概况与 COBIT 治理和管理目标之间的对应关系（如第 4.2.3 节所述）以及附录 D 中的对应关系表，**图 7.10** 已按照风险分析的结果显示治理和管理目标的相对评级。

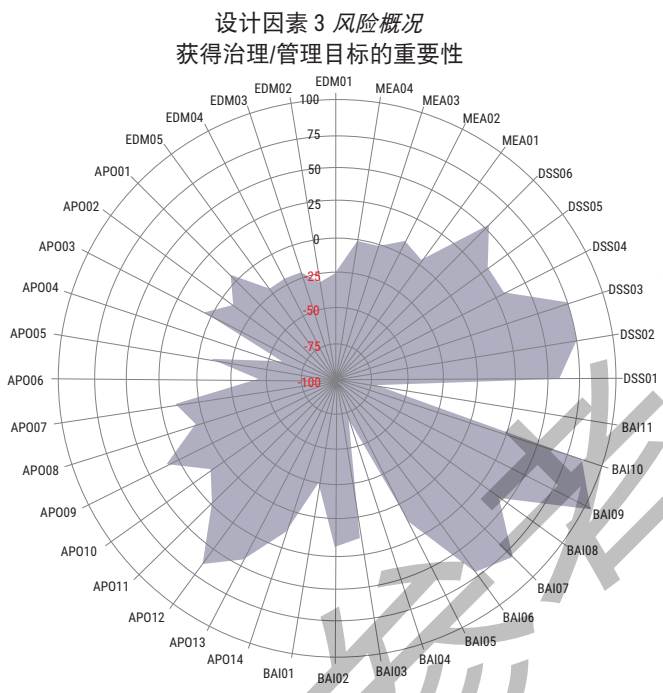
图 7.9—示例 1，第 2.3 步：风险概况

设计因素 3 *风险概况*

风险情景类别	影响 (1-5)	可能性 (1-5)	风险评级
IT 投资决策制定、投资组合定义和维护	4	3	高风险
计划和项目生命周期管理	3	1	低风险
IT 成本和监督	2	2	中度风险
IT 专业知识、技能和行为	3	3	高风险
企业/IT 架构	2	1	低风险
IT 运营基础设施事故	4	4	极高风险
未授权的行动	5	4	极高风险
软件采用/使用问题	4	4	极高风险
硬件事故	4	4	极高风险
软件故障	4	4	极高风险
逻辑攻击（黑客攻击、恶意软件等）	5	3	极高风险
第三方/供应商事故	2	4	中度风险
违规	1	3	低风险
地缘政治问题	2	1	低风险
劳工行动	4	2	中度风险
自然灾害	4	2	中度风险
基于技术的创新	4	1	中度风险
环境	2	2	中度风险
数据和信息管理	4	3	高风险

极高风险	
高风险	
中度风险	
低风险	

图 7.10—示例 1，第 2.3 步：针对设计因素 3 *风险概况*获得治理/管理目标的重要性



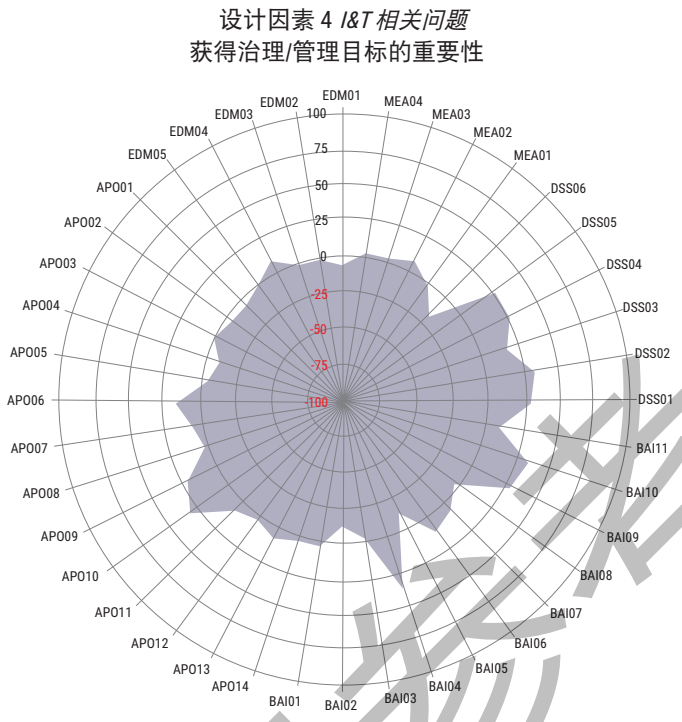
第 2.4 步：思考当前的 I&T 相关问题 — 此步骤利用对应关系表（**附录 E**）将第 1.4 步识别的问题与 COBIT 治理和管理目标相关联，此外，该对应关系表又将每个问题与可能影响该问题的一个或多个治理或管理目标进行关联。基于该对应关系（如第 4.2.4 节所述），**图 7.12** 已按照企业当前 I&T 相关问题的分析结果（**图 7.11**）显示治理和管理目标的相对评级。

图 7.11—示例 1，第 2.4 步：I&T 相关问题

值	重要性 (1-3)	*基准*
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	✔	2
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	!	2
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	X	2
IT 外包商的服务交付问题	X	2
不符合 IT 相关法规或合同要求	✔	2
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	✔	2
重大的隐性和反常的 IT 支出，即用户部门在正常的 IT 投资决策机制控制范围和批准的预算之外的 I&T 支出	X	2
多个举措之间的重复或重叠，或其他形式的资源浪费	✔	2
IT 资源不足，员工技能欠缺或员工倦怠/不满	!	2
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	✔	2
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	✔	2
复杂的 IT 运营模式和/或缺乏明确的 IT 相关决策机制	✔	2
过高的 IT 成本	X	2
当前 IT 架构和系统导致新举措或创新的实施受阻或失败	✔	2
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	✔	2
各种来源的数据经常出现数据质量和整合方面的问题	!	2
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、质量控制以及其他问题	✔	2
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	!	2
忽视和/或违反隐私法规	✔	2
无法利用新技术或使用 I&T 进行创新	✔	2

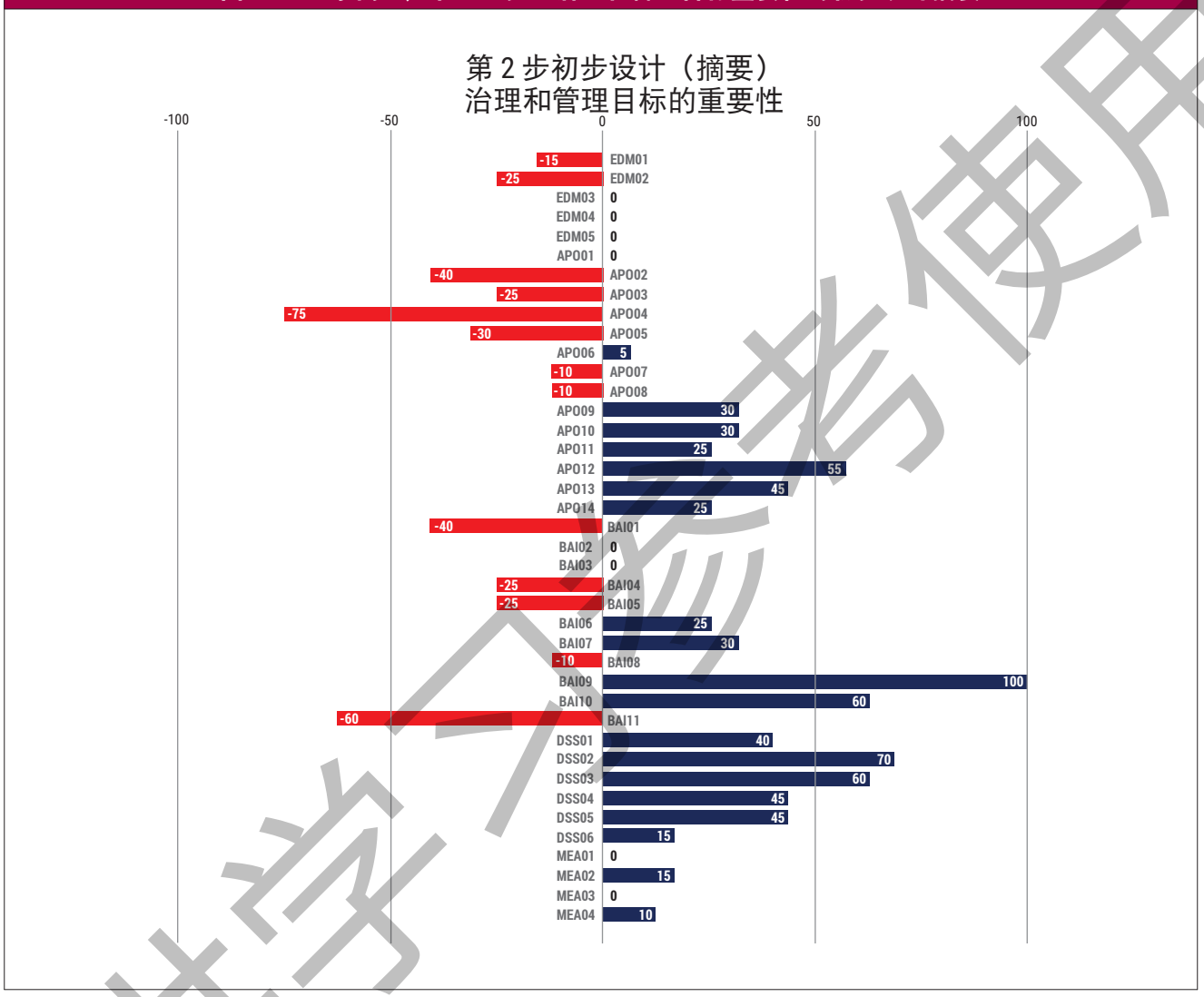
✔	无问题
!	问题
X	严重问题

图 7.12—示例 1，第 2.4 步：针对设计因素 4 *I&T 相关问题*获得治理/管理目标的重要性



第 2.5 步：治理系统的初步范围 — 可结合前四步所得到的治理和管理优先级，获得治理系统中下列治理和管理目标的初步优先级（**图 7.13**）。

图 7.13—示例 1，第 2.5 步：治理和管理目标重要性的初步设计摘要



下列五大管理目标可能对该企业的治理系统非常重要：

- BAI09 *妥当管理的资产*
- DSS02 *妥当管理的服务请求和事故*
- DSS03 *妥当管理的问题*
- BAI10 *妥当管理的配置*
- APO12 *妥当管理的风险*

下列管理目标（目前看来）最不重要：

- APO04 *妥当管理的创新*
- BAI11 *妥当管理的项目*
- APO02 *妥当管理的战略*
- BAI01 *妥当管理的计划*
- APO05 *妥当管理的组合*

下一步将确定此治理系统的初步范围仍需进行哪些优化。

7.2.3 第 3 步：优化治理系统的范围

第 3 步应根据对剩余设计因素的分析，识别范围所需优化。并非所有设计因素都适用于每家企业，可视情况删减。**图 7.14** 总结了本示例所述制造企业适用的第 5 至 11 号设计因素。如某个设计因素多于一个取值，则会在该图的数值列中显示。

图 7.14—示例 1 治理系统的定制版

参考编号	设计因素	值	治理和管理目标优先级	组件	焦点领域指南
DF5	**威胁环境**				
	高	90%[28]	重要的治理和管理目标包括： • EDM01、EDM03 • APO01、APO03、APO10、APO12、APO13、APO14 • BAI06、BAI10 • DSS02、DSS04、DSS05、DSS06 • MEA01、MEA03、MEA04	重要的组织结构包括： • 安全战略委员会 • CISO 重要的文化和行为领域包括： • 安全意识 信息流： • 安全政策 • 安全战略	信息安全焦点领域[29]
	正常	10%	• *按照初步范围定义*	• *不适用*	COBIT 核心模型
DF6	**合规性要求**				
	正常	75%	最重要但处于中等等级的管理目标包括： • EDM01、EDM03 • APO12 • MEA03	• *不适用*	COBIT 核心模型
	低	25%	• *按照初步范围定义*	• *不适用*	COBIT 核心模型
DF7	**IT 角色**				
	工厂	5（共 5 分）	重要的治理和管理目标包括： • EDM03 • DSS01、DSS02、DSS03、DSS04	• *不适用*	信息安全焦点领域[30]
	整顿	2（共 5 分）	重要的治理和管理目标包括： • APO02、APO04、 • BAI02、BAI03	• *不适用*	DevOps 焦点领域[31]

[28] 此数字表示 90% 的企业运营和 I&T 活动都在较高的威胁环境中完成。
[29] *《COBIT® 2019 设计指南：信息和技术治理解决方案的设计》*出版时，信息安全焦点领域的内容正在制定中，尚未发布。
[30] *《COBIT® 2019 设计指南：信息和技术治理解决方案的设计》*出版时，信息安全焦点领域的内容正在制定中，尚未发布。
[31] *《COBIT® 2019 设计指南：信息和技术治理解决方案的设计》*出版时，DevOps 焦点领域的内容正在制定中，尚未发布。

图 7.14—示例 1 治理系统的定制版（续）					
参考编号	**设计因素**	**值**	**治理和管理目标优先级**	**组件**	**焦点领域指南**
DF8	**IT 采购模式**				
	外包	20%	重要的管理目标包括： • APO09、APO10 • MEA01	• *不适用*	供应商管理焦点领域 [32]
	内包	80%	• *按照初步范围定义*	• *不适用*	COBIT 核心模型
DF9	**IT 实施方法**				
	传统		• *按照初步范围定义*	• *不适用*	COBIT 核心模型
DF10	**技术采用战略**				
	追随者	90%[33]	重要的治理和管理目标包括： • APO02、APO04 • BAI01	可以降速运转的流程	COBIT 核心模型
	滞后者	10%[34]	• *按照初步范围定义*	• *不适用*	COBIT 核心模型
DF11	**企业规模**				
	大型		• *按照初步范围定义*	• *不适用*	COBIT 核心模型

对于**图 7.14** 中的各设计因素而言，可将评估现状和与之对应的治理和管理目标以及**图 7.14** 中的其他指南相结合。下列示例是通过将输入值与这些值同治理和管理目标之间的对应关系进行矩阵计算而生成的。对应关系表位于本书的附录 F 至 K。生成包含优先治理和管理目标的蜘蛛图，展示其相较于基准级别的相对重要级别。相对重要级别以 -100 到 +100 的度量指标表示，其中零 (0) 表示对治理或管理目标的重要性毫无影响，+100 表示该目标会因当前设计因素而变得倍加重要。

[32] *《COBIT® 2019 设计指南：信息和技术治理解决方案的设计》*出版时，正在考虑将供应商管理焦点领域的内容作为未来的潜在焦点领域。
[33] 此数字表示在技术采用方面，该组织在 90% 的情况下被认为是追随者。
[34] 此数字表示 10% 的企业 I&T 活动被认为存在滞后情况。

第 3.1 步：思考威胁环境 — **图 7.15** 描述了企业对其运营所处威胁环境的认知。**图 7.16** 显示了所评估的威胁环境对治理和管理目标的影响。

图 7.15—示例 1，第 3.1 步：威胁环境

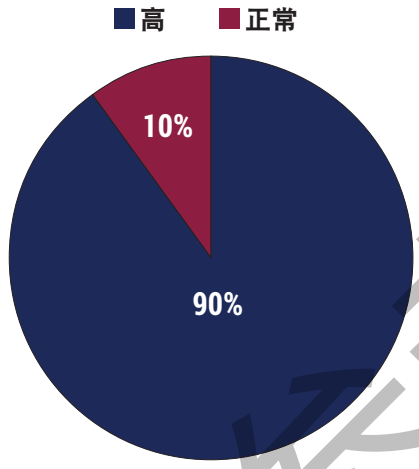
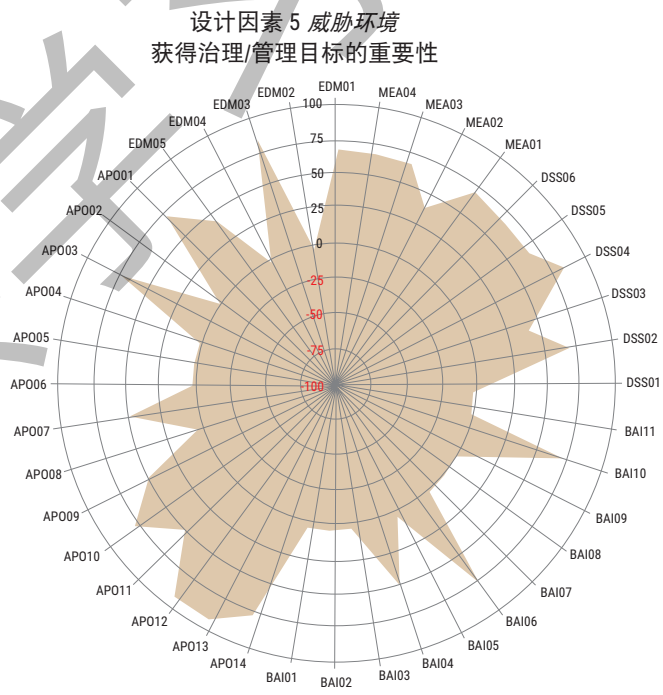


图 7.16—示例 1，第 3.1 步：针对设计因素 5 *威胁环境*获得治理/管理目标的重要性



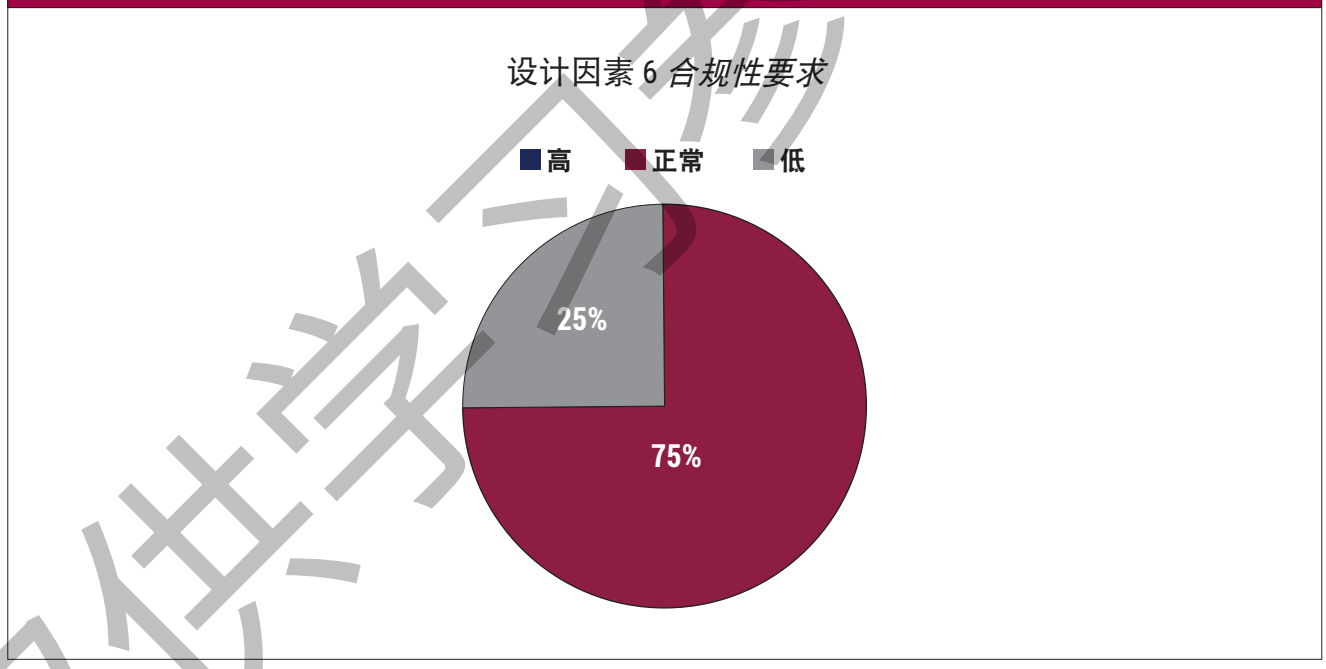
根据**图 7.14** 中的高威胁环境相关条目，这种威胁环境分类使得大量的治理和管理目标变得更加重要。应从信息安全焦点领域指南中抽取治理和管理目标的相关指南，[35] 因为该指南包含比 COBIT 核心模型更为详细且具体的信息安全指南。

此外，企业必须考虑下列各项是否存在及其表现（并将其纳入治理系统设计中）：

- 重要的组织结构，包括：
  - 安全战略委员会
  - CISO
- 重要的文化和行为领域，包括：
  - 安全意识
- 信息流：
  - 安全政策
  - 安全战略

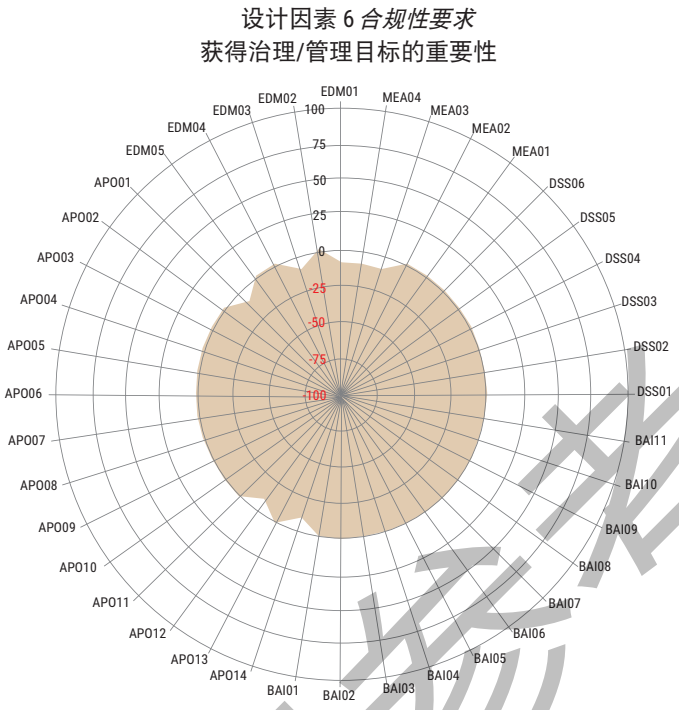
第 3.2 步：思考合规性要求 — **图 7.17** 描述了该企业的合规性要求，这些要求的预估级别为正常偏低。**图 7.18** 显示了所评估的合规性要求对治理和管理目标的影响，不出意料，这些要求的影响很小。

图 7.17—示例 1，第 3.2 步：合规性要求



[35] *《COBIT® 2019 设计指南：信息和技术治理解决方案的设计》*出版时，信息安全焦点领域的内容正在制定中，尚未发布。

图 7.18—示例 1，第 3.2 步：针对设计因素 6 *合规性要求*获得治理/管理目标的重要性



第 3.3 步：思考 IT 角色 — **图 7.19** 显示了以工厂为首要、以整顿为次要选择的IT角色，表明该企业运营非常依赖 IT 服务。**图 7.20** 显示了所评估的 IT 角色对治理和管理目标的影响。

图 7.19—示例 1，第 3.3 步：IT 角色

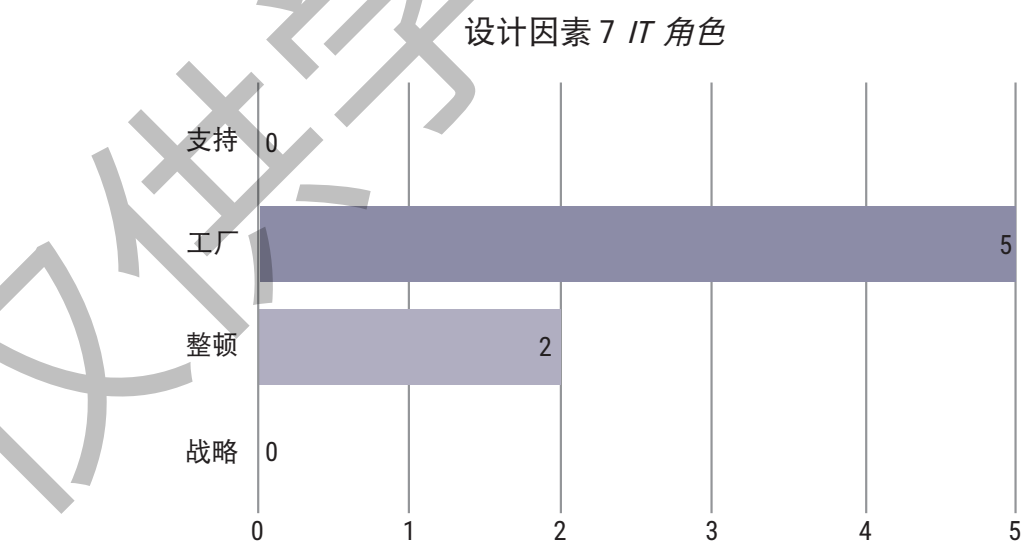
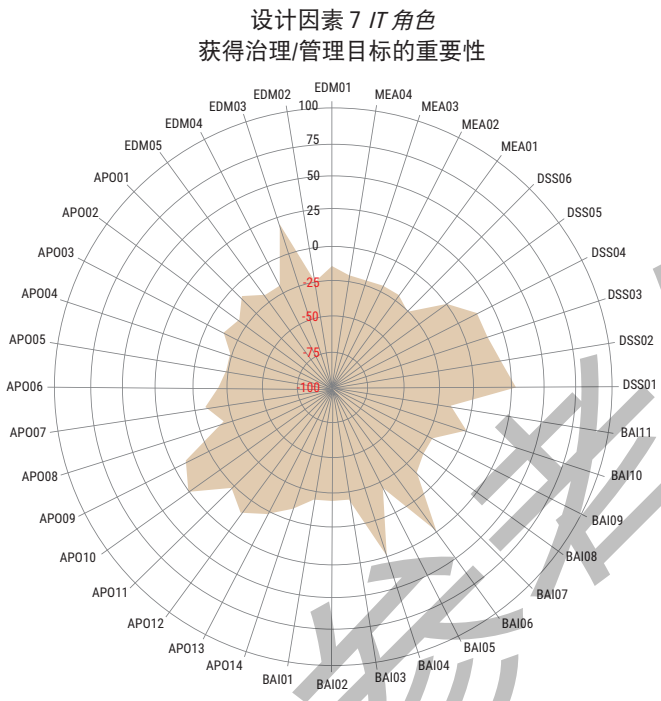


图 7.20—示例 1，第 3.3 步：针对设计因素 7 *IT 角色*获得治理/管理目标的重要性



除了优先级别的治理和管理目标以外，还应从信息安全和 DevOps 焦点领域抽取指南（如果适用且需要）。

第 3.4 步：思考采购模式 — **图 7.21** 描述了该企业所选择的采购模式（主要是内包）。**图 7.22** 显示采购模式对治理和管理目标的影响。此设计因素的影响十分有限。

图 7.21—示例 1，第 3.4 步：IT 采购模式

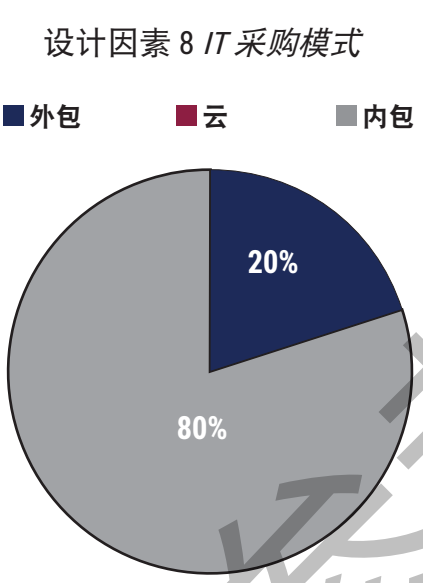
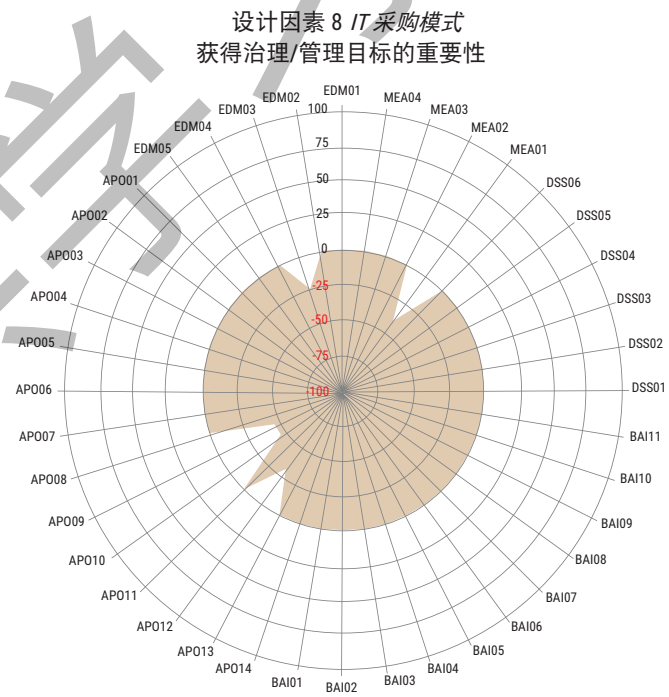


图 7.22—示例 1，第 3.4 步：针对设计因素 8 *IT 采购模式*获得治理/管理目标的重要性



第 3.5 步：思考 IT 实施方法 — 该企业使用传统的 IT 开发和运营方法（**图 7.23**），不对治理和管理目标产生任何影响（**图 7.24**）。

图 7.23—示例 1，第 3.5 步：IT 实施方法

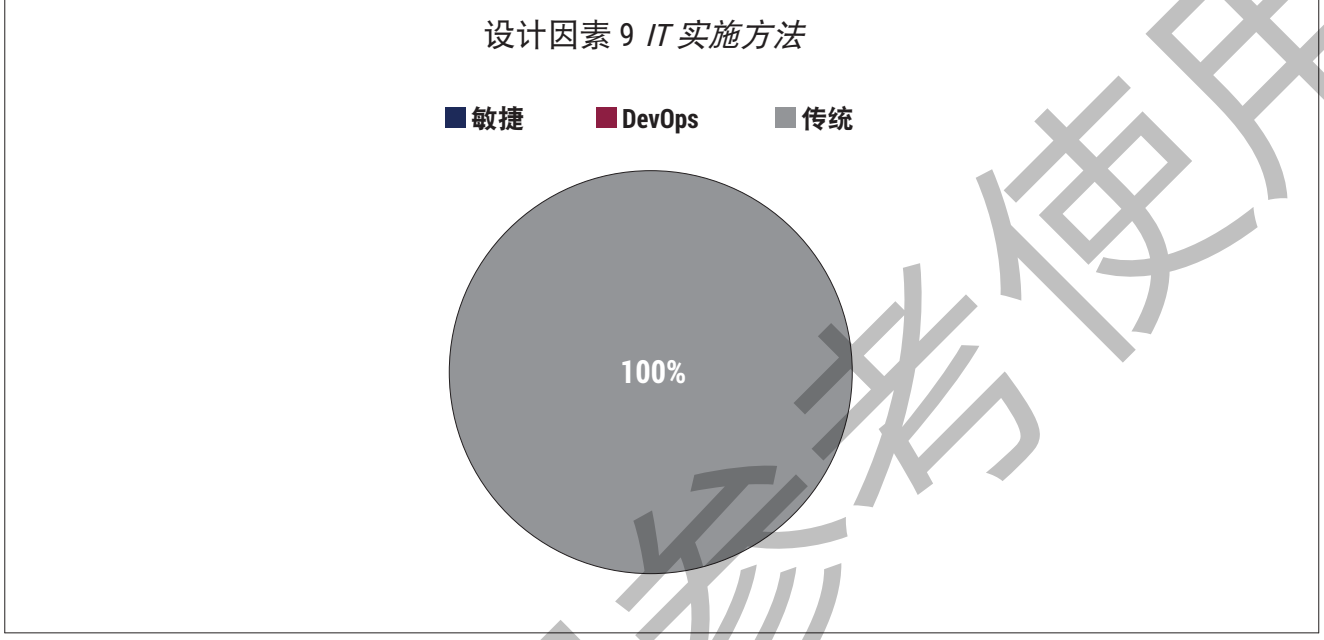
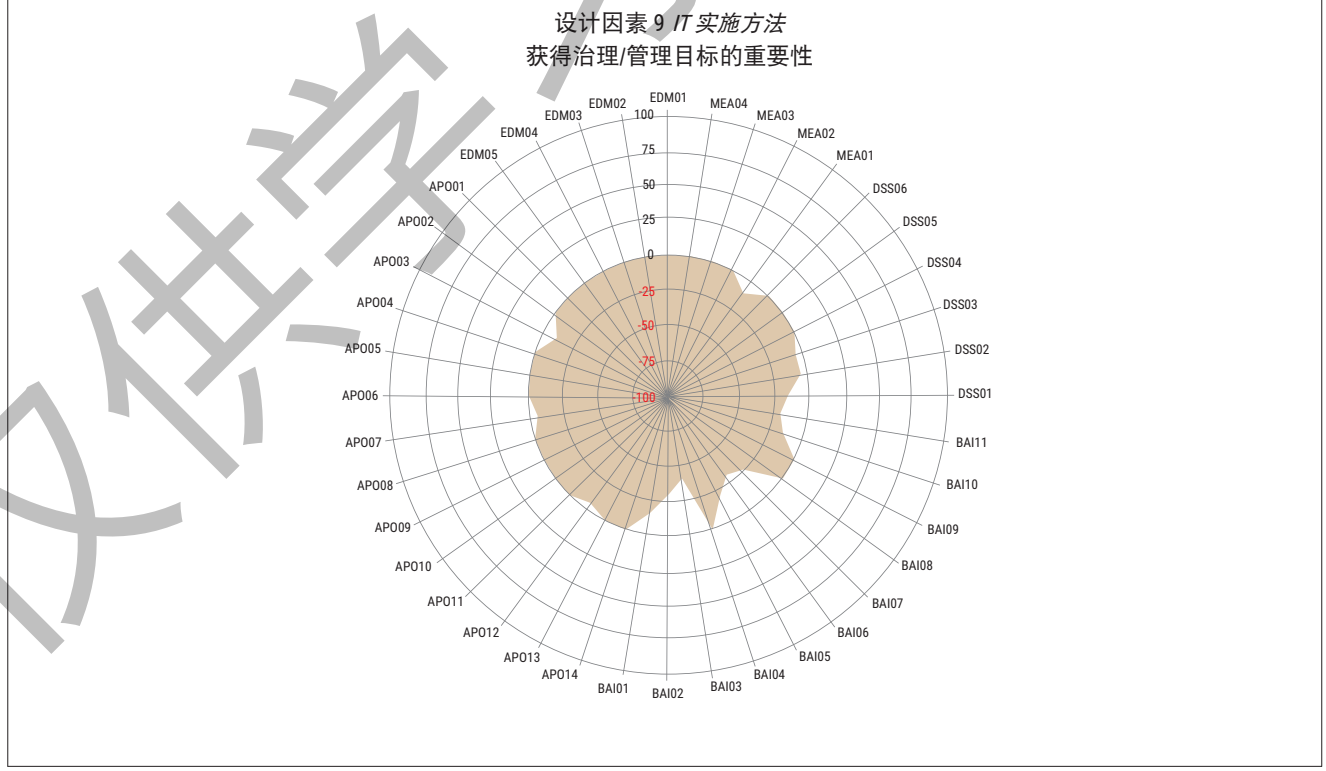


图 7.24—示例 1，第 3.5 步：针对设计因素 9 *IT 实施方法*获得治理/管理目标的重要性



第 3.6 步：思考技术采用战略 — **图 7.25** 表明该企业在新技术应用方面最多只能充当追随者。**图 7.26** 表明这对治理和管理目标的优先级影响十分有限。

图 7.25—示例 1，第 3.6 步：技术采用战略

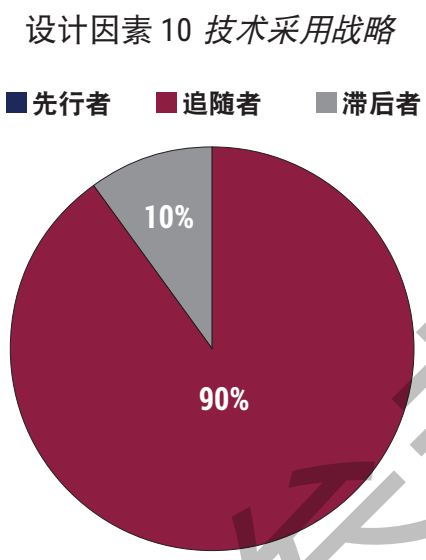
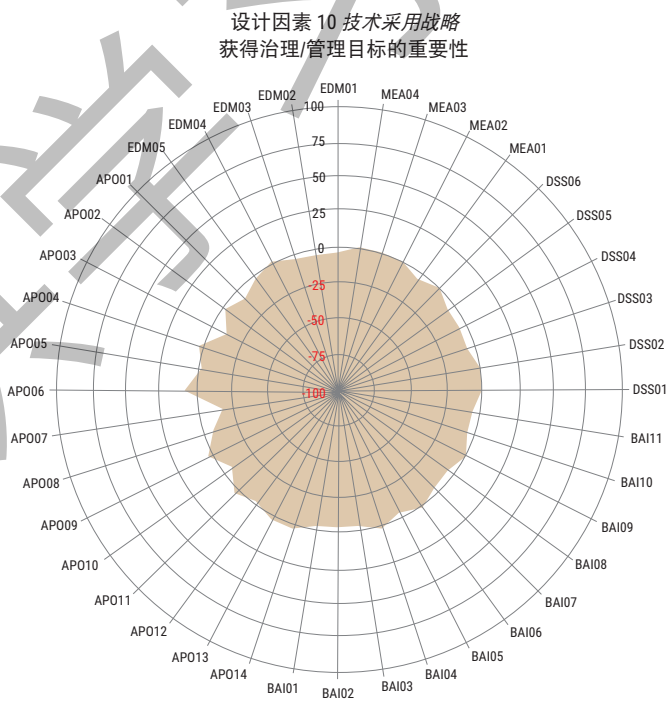


图 7.26—示例 1，第 3.6 步：针对设计因素 10 *技术采用战略*获得治理/管理目标的重要性



第 3.7 步：思考企业规模 — 该企业被归类为大型企业。根据**图 7.14**，这表明应将 COBIT 核心模型用作定义治理系统的基础。

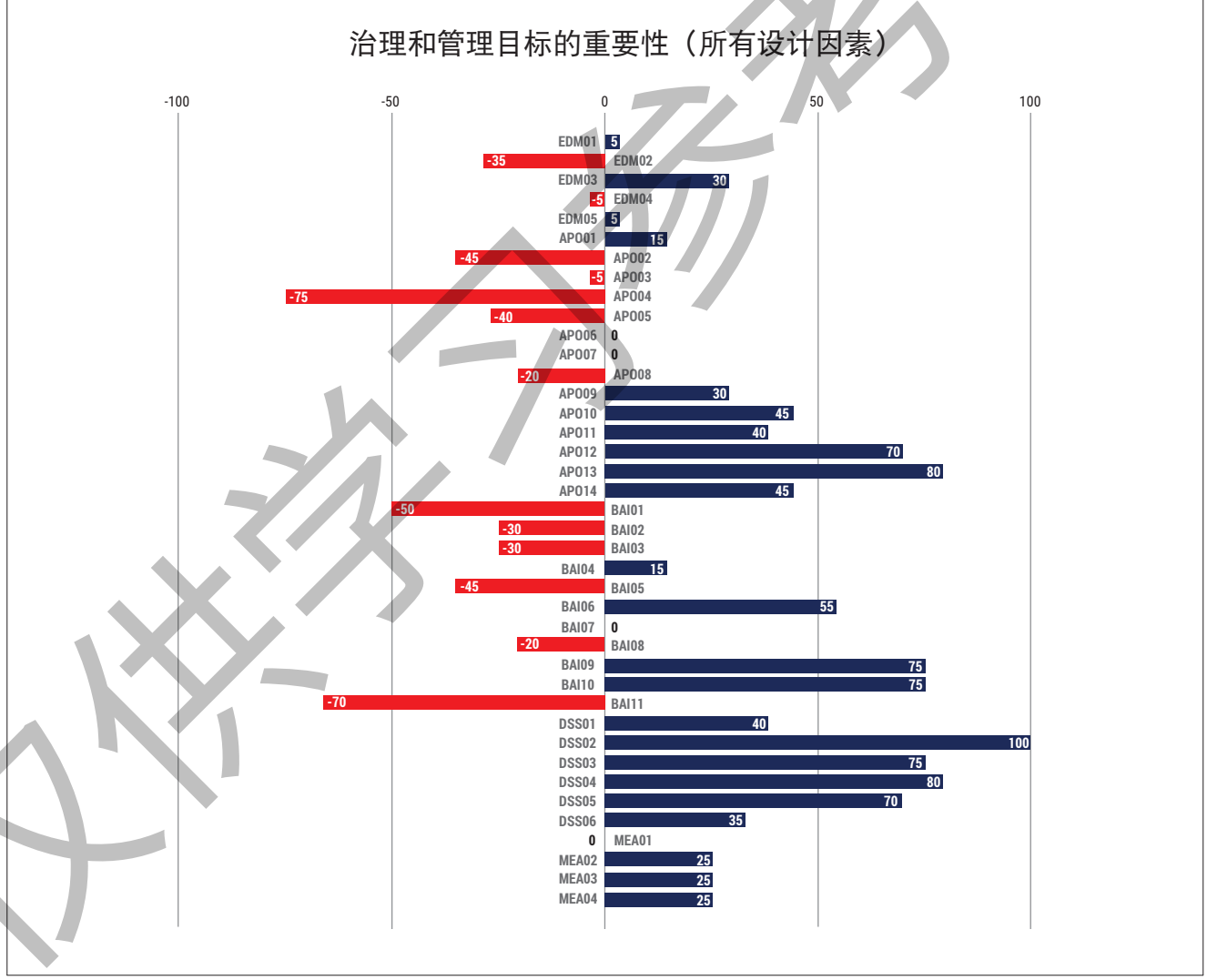
7.2.4 第 4 步：确定治理解决方案的最终设计

设计过程的最后一步需要讨论前述步骤的所有输入，解决冲突，并达成一致。由此产生的治理系统体现了对所有输入的慎重考虑，并考虑了对输入可能存在的冲突做出合理选择。

7.2.4.1 治理和管理目标

此时可将第 3.1 至 3.7 步获得的治理和管理优先级添加到第 2.1 至 2.4 步所产生的初步治理系统设计中。综合得出治理系统中下列治理和管理目标优先级调整结果（**图 7.27**）。

图 7.27—示例 1，第 4 步：治理和管理目标的重要性（所有设计因素）



下列管理目标可能对该企业的治理系统非常重要：

- DSS02 *妥当管理的服务请求和事故* (100)
- APO13 *妥当管理的安全* (80)
- DSS04 *妥当管理的连续性* (80)
- DSS03 *妥当管理的问题* (75)
- BAI09 *妥当管理的资产* (75)
- BAI10 *妥当管理的配置* (75)

与第 2.5 步中的初步范围定义所识别的列表相比，最重要的目标略有变化。部分治理/管理目标更换了位置，删除了其中一个目标 (APO12) 并新增了两个目标（DSS04 和 APO13）。

下列管理目标似乎最不重要：

- APO04 *妥当管理的创新*
- BAI11 *妥当管理的项目*
- BAI01 *妥当管理的计划*
- APO02 *妥当管理的战略*
- BAI05 *妥当管理的组织变更*

相较于最重要的目标，最不重要的目标列表与第 2.5 步中初步范围定义所识别的列表之间的差异更小。这一方面证明了基于基础设计因素得出的初始范围非常准确，另一方面也证明了考虑其他设计因素会导致额外调整。

在讨论期间，该企业认为，某些治理/管理目标自动生成的重要性值不够准确，所以进行了下列调整：

- APO06 *妥当管理的预算和成本：*+75
- EDM04 *确保资源优化：*+75
- DSS02 *妥当管理的服务请求和事故：*-25

综上所述，该企业认为其第一阶段的治理系统设计将由**图 7.28** 所示的治理和管理目标（和基础流程）组成。

图 7.28—示例 1：治理和管理目标以及目标流程能力级别

参考资料	治理/管理目标	目标流程能力级别
EDM03	确保风险优化	2
EDM04	确保资源优化	3
APO06	妥当管理的预算和成本	4
APO09	妥当管理的服务水平协议	2
APO10	妥当管理的供应商	2
APO11	妥当管理的质量	2
APO12	妥当管理的风险	3
APO13	妥当管理的安全	4
APO14	妥当管理的数据	2
BAI06	妥当管理的 IT 变更	3
BAI09	妥当管理的资产	4
BAI10	妥当管理的配置	4

图 7.28—示例 1：治理和管理目标以及目标流程能力级别（续）		
参考资料	治理/管理目标	目标流程能力级别
DSS01	妥当管理的运营	2
DSS02	妥当管理的服务请求和事故	4
DSS03	妥当管理的问题	4
DSS04	妥当管理的连续性	4
DSS05	妥当管理的安全服务	3
DSS06	妥当管理的业务流程控制	2
MEA02	妥当管理的内部控制系统	2
MEA03	妥当管理的外部要求合规性	2
MEA04	妥当管理的鉴证	2

图 7.28 显示了参考资料、治理或管理目标的标题，以及流程应实施的目标能力级别。鉴于很多流程都极为重要，所以目标能力级别被设定为更高的值（3 或 4）。该企业所运用的逻辑是：

- 如果任何治理/管理目标的得分为 75 或更高，则表明其重要性相比基准情况至少高 75%，所以需要能力级别 4。
- 得分为 50 或更高的任何治理/管理目标需要能力级别 3。
- 得分为 25 或更高的任何治理/管理目标需要能力级别 2。

将剩余流程的能力级别设定为 1 也属合理。

7.2.4.2 其他组件

该企业需要特别注意，应强化实施下列角色和结构：

- 安全战略委员会
- CISO

该企业还需确保整个企业具备足够的安全意识，并实施重要的信息项和信息流（安全政策和安全战略）。

7.2.4.3 具体焦点领域指南

该企业会将下列指南作为 COBIT 核心模型的补充指南：

- 信息安全焦点领域[36]指南，考虑到高威胁环境以及风险分析结果和当前的 I&T 相关问题
- DevOps 和供应商管理焦点领域[37]指南（如适用）

[36] *《COBIT® 2019 设计指南：信息和技术治理解决方案的设计》*出版时，信息安全焦点领域的内容正在制定中，尚未发布。
[37] *《COBIT® 2019 设计指南：信息和技术治理解决方案的设计》*出版时，DevOps 焦点领域的内容正在制定中，尚未发布，并且正在考虑将供应商管理焦点领域作为未来的潜在焦点领域。

7.3 示例 2：中型创新企业

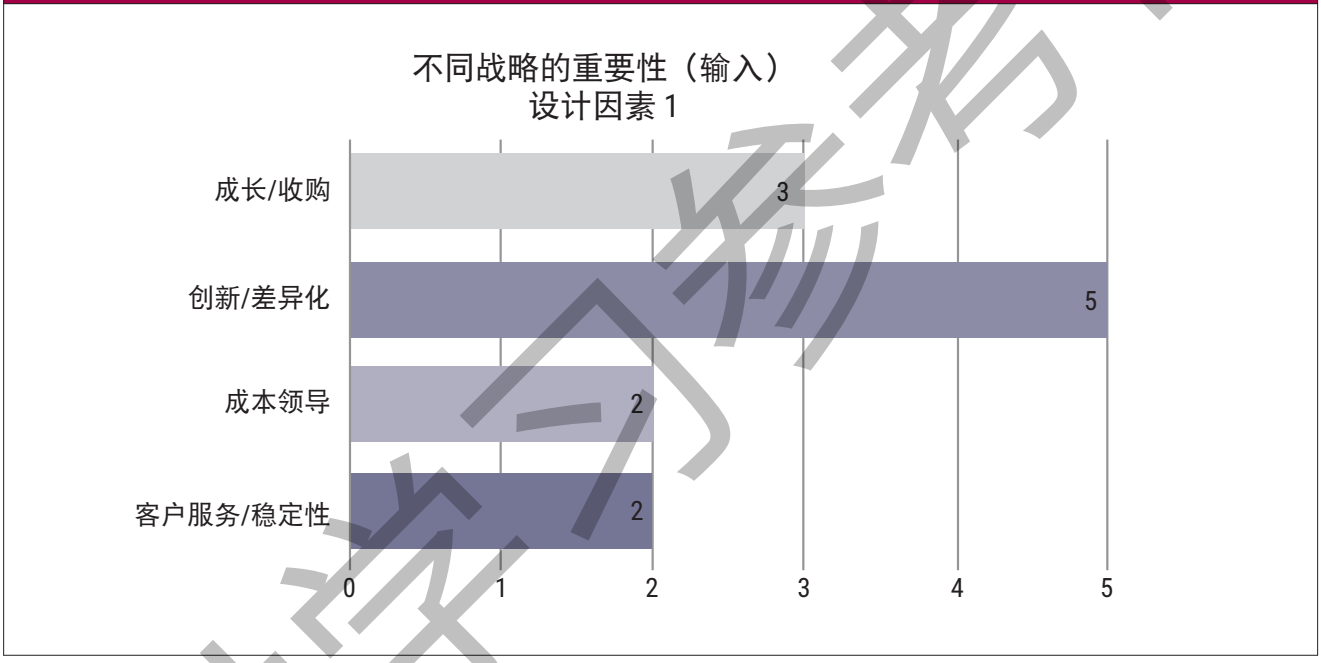
此示例涉及一家为汽车行业开发电器的中型创新企业。该企业规模相对较小，但却因快速创新声名远扬。该企业在产品开发和电器制造方面极度依赖 IT。该企业既是软件用户也是软件开发者。它非常希望能受益于各种新技术，并且尽可能对 DevOps 方法进行投入。它已制定将与基础设施相关的所有 IT 服务全部外包并转向云端的战略。

7.3.1 第 1 步：了解企业环境和战略

治理设计工作的第一步是总结该企业的内外部环境。

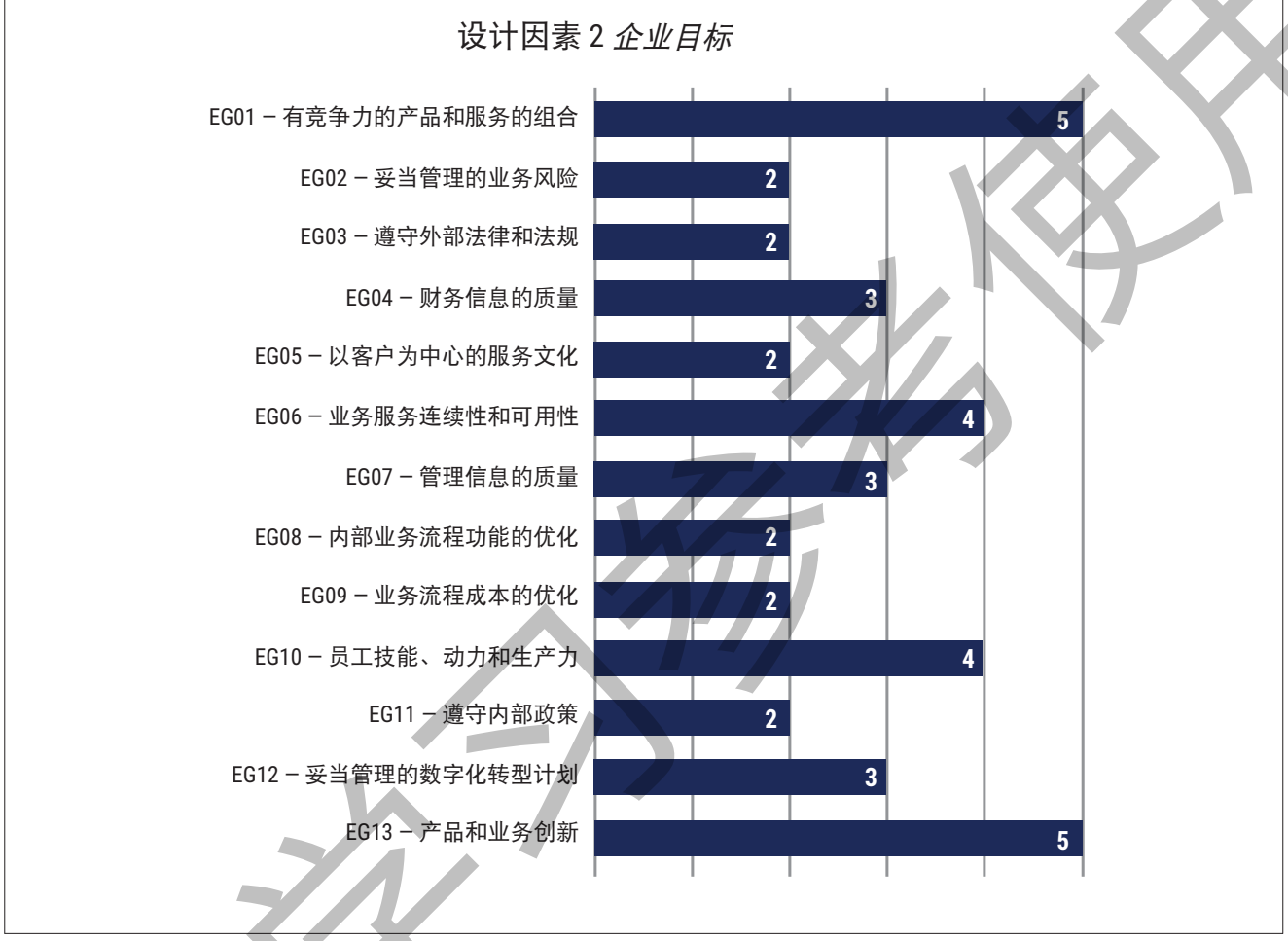
第 1.1 步：了解企业战略 — 如**图 7.29** 所述，将**创新和差异化**作为主要关注点，将**成长/收购**作为次要关注点。

图 7.29—示例 2，第 1.1 步：企业战略



第 1.2 步：了解企业目标 — 该企业对**图 7.30** 所示的 13 个通用企业目标进行了评级（评级范围为 1 到 5 分）。该图显示 EG01 *有竞争力的产品和服务的组合*以及 EG13 *产品和业务创新*是评级最高的企业目标。

图 7.30—示例 2，第 1.2 步：企业目标



第 1.3 步：了解风险概况 — 利用整体风险分析获得的风险概况，识别最高风险类别（在**图 7.31** 的风险评级列中以红色圆点标识）：IT 投资决策、投资组合定义和维护，IT 专业知识、技能和行为，基于技术的创新。（此处为宽泛的分类。各类别风险情景的详细示例，请参阅第 2.6 节。）

图 7.31—示例 2，第 1.3 步：风险概况

设计因素 3 *风险概况*

风险情景类别	影响 (1-5)	可能性 (1-5)	风险评级
IT 投资决策制定、投资组合定义和维护	5	3	🔴
计划和项目生命周期管理	4	2	🟢
IT 成本和监督	5	1	🟢
IT 专业知识、技能和行为	4	4	🔴
企业/IT 架构	4	2	🟢
IT 运营基础设施事故	4	2	🟢
未授权的行动	4	3	🟡
软件采用/使用问题	3	2	🟢
硬件事故	4	2	🟢
软件故障	3	2	🟢
逻辑攻击（黑客攻击、恶意软件等）	3	4	🟡
第三方/供应商事故	4	2	🟢
违规	2	3	🟢
地缘政治问题	2	2	🟢
劳工行动	2	1	⚫
自然灾害	2	1	⚫
基于技术的创新	5	3	🔴
环境	3	1	⚫
数据和信息管理	4	3	🟡

🔴	极高风险
🟡	高风险
🟢	中度风险
⚫	低风险

第 1.4 步：了解当前的 I&T 相关问题 — 对现状进行分析（重要性评级范围为 1 到 3 分）可获得**图 7.32** 所述的当前 I&T 相关问题的评估。下述各项被视为该企业面临的重要问题：IT 资源不足、IT 架构和数据质量问题。

图 7.32—示例 2，第 1.4 步：I&T 相关问题

值	重要性 (1-3)	*基准*
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	✔	*2*
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	✔	*2*
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	!	*2*
IT 外包商的服务交付问题	!	*2*
不符合 IT 相关法规或合同要求	✔	*2*
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	✔	*2*
重大的隐性和反常的 IT 支出，即用户部门在正常的 IT 投资决策机制控制范围和批准的预算之外的 I&T 支出	!	*2*
多个举措之间的重复或重叠，或其他形式的资源浪费	✔	*2*
IT 资源不足，员工技能欠缺或员工倦怠/不满	X	*2*
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	!	*2*
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	!	*2*
复杂的 IT 运营模式和/或缺乏明确的 IT 相关决策机制	✔	*2*
过高的 IT 成本	!	*2*
当前 IT 架构和系统导致新举措或创新的实施受阻或失败	X	*2*
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	!	*2*
各种来源的数据经常出现数据质量和整合方面的问题	X	*2*
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、质量控制以及其他问题	✔	*2*
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	✔	*2*
忽视和/或违反隐私法规	✔	*2*
无法利用新技术或使用 I&T 进行创新	!	*2*

✔	无问题
!	问题
X	严重问题

7.3.2 第 2 步：确定治理系统的初步范围

利用第 1 步收集到的（部分或全部）信息，确定治理系统的初步范围。第 2 步会将这些关于企业战略、企业目标、风险概况和 I&T 相关问题的信息转换为相关的治理组件。

第 2.1 步：思考企业战略 — **图 7.33** 为第 1.1 步中确定的企业战略。**图 7.34** 表明了这些战略对治理和管理目标的相对影响。

图 7.33—示例 2，第 2.1 步：企业战略

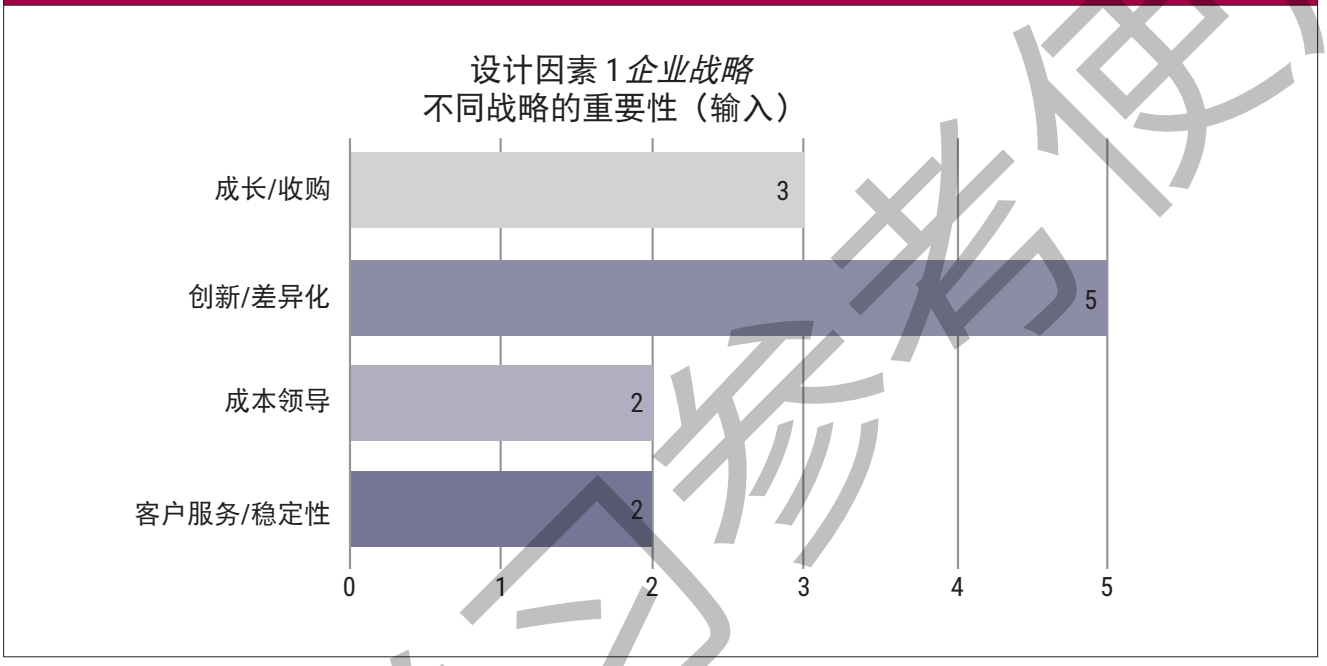
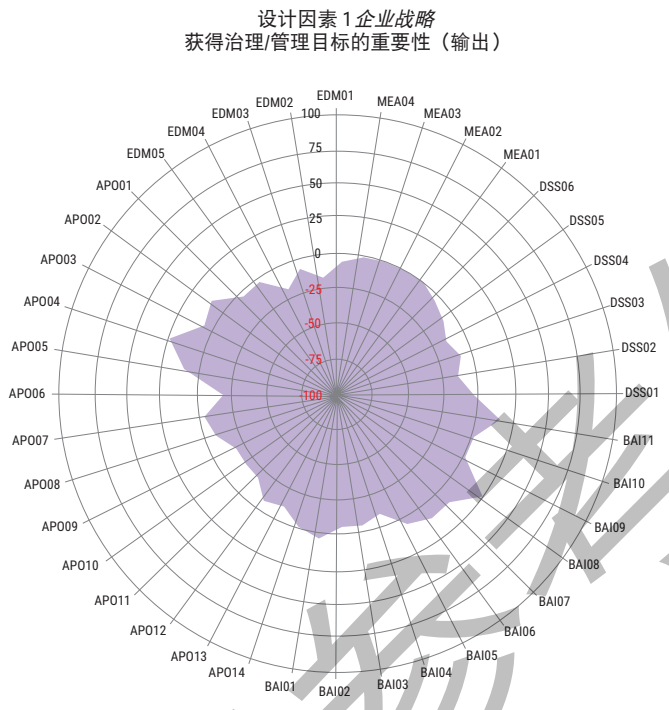


图 7.34—示例 2，第 2.1 步：针对设计因素 1 *企业战略*获得治理/管理目标的重要性



除了**图 7.34** 突出显示的治理和管理流程以外，还需要注意下列组件：

- 为负责监督所有投资的投资组合管理角色提供支持
- 企业架构师和首席数字官的角色
- 旨在促进自动化和发展以及实现规模经济的服务、基础设施和应用程序组件
- 文化和行为组件对创新的影响

第 2.2 步：思考企业目标并运用 COBIT 目标级联 — 此时可按照第 1.2 步指定的评级，运用 COBIT 目标级联来确定哪些治理和管理目标与实现优先的企业目标有关（**图 7.35**）。**图 7.36** 表明了这些已评级的企业目标对治理和管理目标的相对影响。

图 7.35—示例 2，第 2.2 步：企业目标

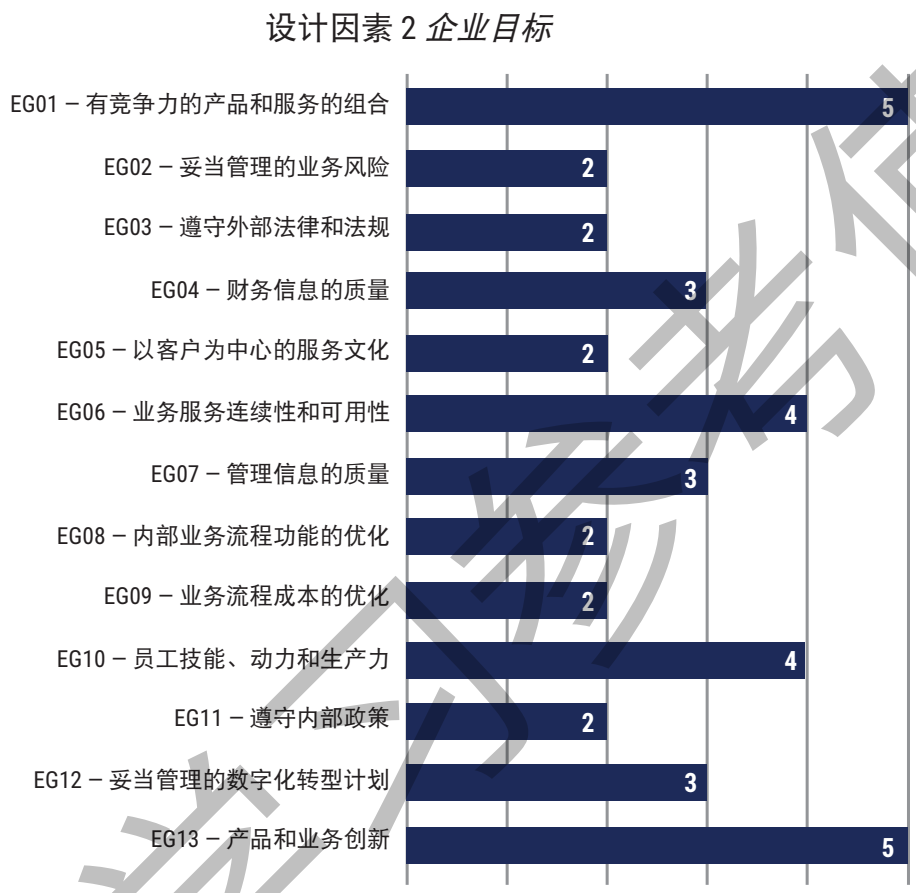
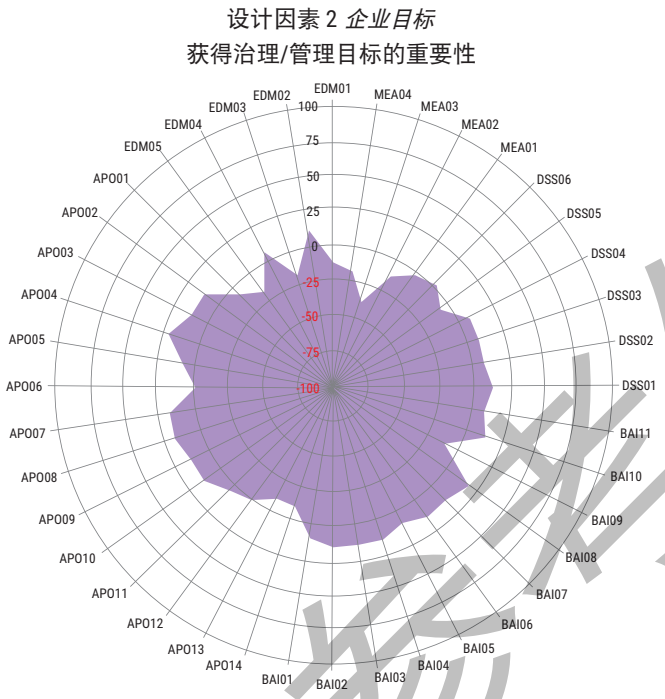


图 7.36—示例 2，第 2.2 步：针对设计因素 2 *企业目标*获得治理/管理目标的重要性



第 2.3 步：思考企业的风险概况 — 第 1.3 步已在总体层面识别和分析 IT 风险类别（**图 7.37**）。基于风险概况与 COBIT 治理和管理目标之间的对应关系（如第 4.2.3 节所述）以及附录 D 中的对应关系表，**图 7.38** 已按照风险分析的结果显示治理和管理目标的相对评级。

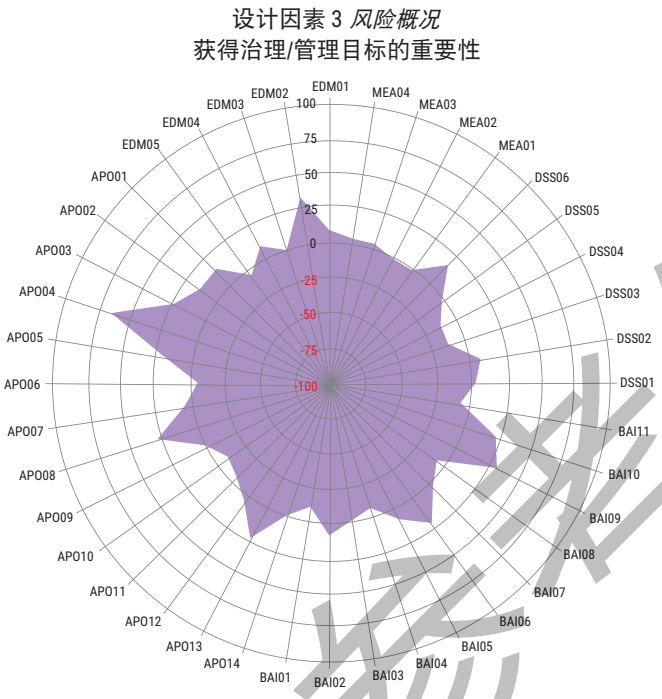
图 7.37—示例 2，第 2.3 步：风险概况

设计因素 3 *风险概况*

风险情景类别	影响 (1-5)	可能性 (1-5)	风险评级
IT 投资决策制定、投资组合定义和维护	5	3	●
计划和项目生命周期管理	4	2	●
IT 成本和监督	5	1	●
IT 专业知识、技能和行为	4	4	●
企业/IT 架构	4	2	●
IT 运营基础设施事故	4	2	●
未授权的行动	4	3	●
软件采用/使用问题	3	2	●
硬件事故	4	2	●
软件故障	3	2	●
逻辑攻击（黑客攻击、恶意软件等）	3	4	●
第三方/供应商事故	4	2	●
违规	2	3	●
地缘政治问题	2	2	●
劳工行动	2	1	●
自然灾害	2	1	●
基于技术的创新	5	3	●
环境	3	1	●
数据和信息管理	4	3	●

●	极高风险
●	高风险
●	中度风险
●	低风险

图 7.38—示例 2，第 2.3 步：针对设计因素 3 *风险概况*获得治理/管理目标的重要性



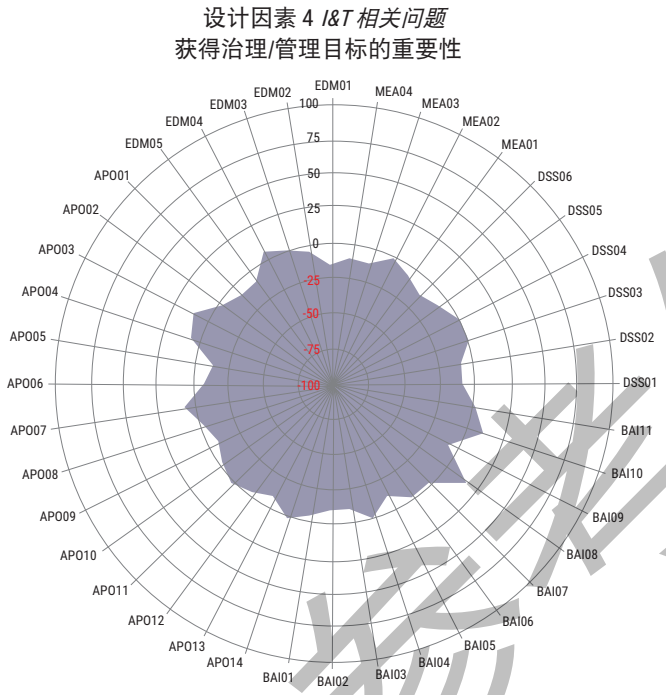
第 2.4 步：思考当前的 I&T 相关问题 — 此步骤利用对应关系表（**附录 E**）将第 1.4 步所识别的问题与 COBIT 治理和管理目标相关联，而该对应关系表又将每个问题与可能影响该问题的一个或多个治理或管理目标进行关联。基于该对应关系（如第 4.2.4 节所述），**图 7.40** 已按照当前 I&T 相关问题的分析结果（**图 7.39**）显示治理和管理目标的相对评级。

图 7.39—示例 2，第 2.4 步：I&T 相关问题

值	重要性 (1-3)	*基准*
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	✔	*2*
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	✔	*2*
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	!	*2*
IT 外包商的服务交付问题	!	*2*
不符合 IT 相关法规或合同要求	✔	*2*
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	✔	*2*
重大的隐性和反常的 IT 支出，即用户部门在正常的 IT 投资决策机制控制范围和批准的预算之外的 I&T 支出	!	*2*
多个举措之间的重复或重叠，或其他形式的资源浪费	✔	*2*
IT 资源不足，员工技能欠缺或员工倦怠/不满	X	*2*
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	!	*2*
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	!	*2*
复杂的 IT 运营模式和/或缺乏明确的 IT 相关决策机制	✔	*2*
过高的 IT 成本	!	*2*
当前 IT 架构和系统导致新举措或创新的实施受阻或失败	X	*2*
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	!	*2*
各种来源的数据经常出现数据质量和整合方面的问题	X	*2*
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、质量控制以及其他问题	✔	*2*
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	✔	*2*
忽视和/或违反隐私法规	✔	*2*
无法利用新技术或使用 I&T 进行创新	!	*2*

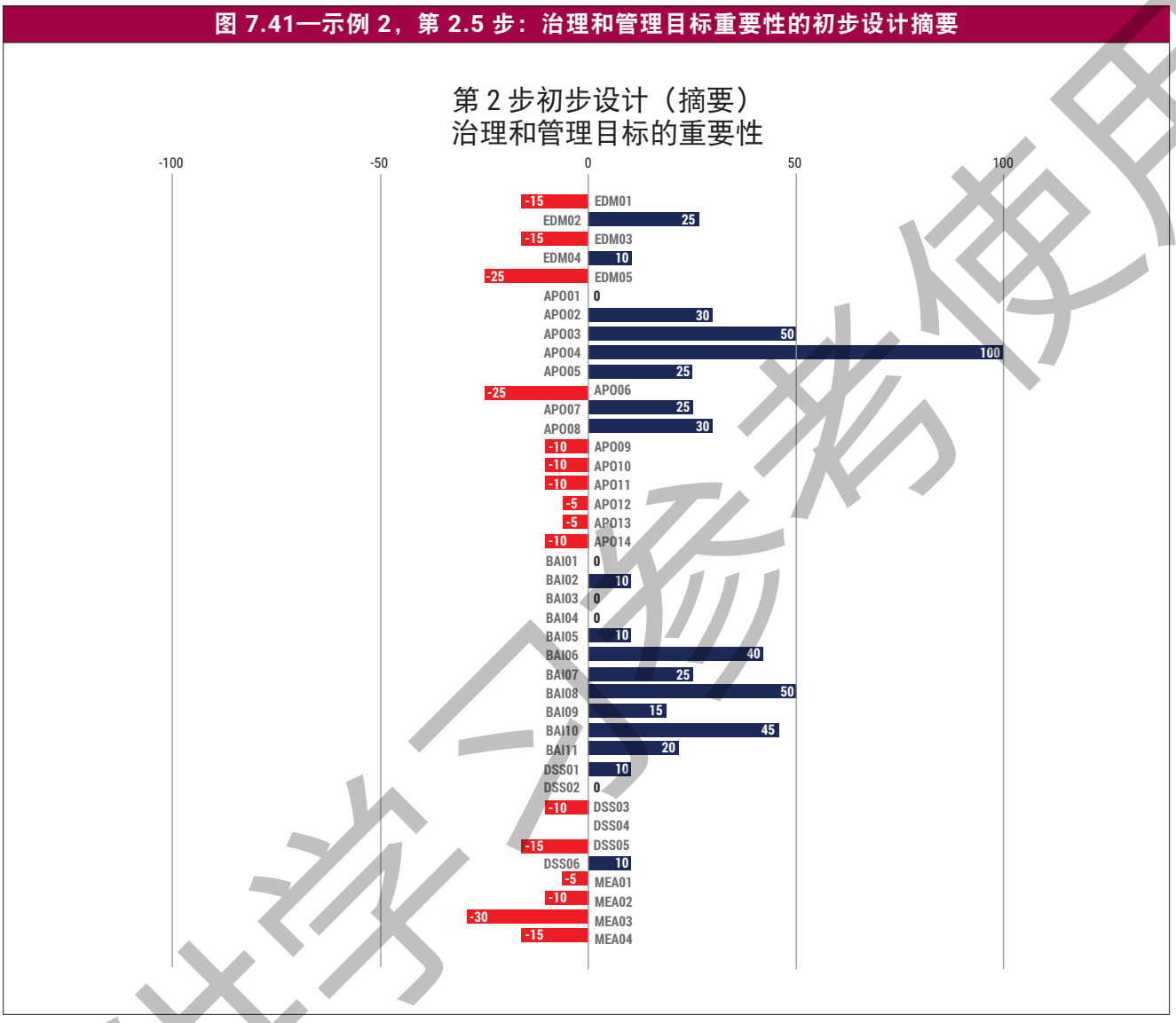
✔	无问题
!	问题
X	严重问题

图 7.40—示例 2，第 2.4 步：针对设计因素 4 *I&T 相关问题*获得治理/管理目标的重要性



第 2.5 步：治理系统的初步范围 — 此时可结合前述步骤所得到的治理和管理优先级，获得治理系统中的治理和管理目标的初步优先级（**图 7.41**）。

图 7.41—示例 2，第 2.5 步：治理和管理目标重要性的初步设计摘要



下列五大管理目标可能对该企业的治理系统非常重要：

- APO04 *妥当管理的创新*
- BAI08 *妥当管理的知识*
- APO03 *妥当管理的企业架构*
- BAI10 *妥当管理的配置*
- BAI06 *妥当管理的 IT 变更*

下列管理目标（目前看来）最不重要：

- MEA03 *妥当管理的外部要求合规性*
- EDM05 *确保利益相关方参与*
- APO06 *妥当管理的预算和成本*
- EDM01 *确保治理框架的设置和维护*
- EDM03 *确保风险优化*
- DSS05 *妥当管理的安全服务*

下一步将确定此治理系统的初步范围需要进行哪些优化。

7.3.3 第 3 步：优化治理系统的范围

第 3 步根据待分析的一组剩余设计因素来识别初步范围所需的优化。并非所有设计因素都适用于每家企业，所以有时可以忽略其中的某些因素。**图 7.42** 概述了设计因素 5 至 11，这些设计因素适用于本示例所述中型创新企业。如不止一个值适用于某个设计因素，则会在该图的数值列中显示该值。

图 7.42—适用于示例 2 的治理系统范围优化表

参考编号	设计因素	值	治理和管理目标优先级	组件	焦点领域指南
DF5	**威胁环境**				
	高	50%	重要的治理和管理目标包括： • EDM01、EDM03 • APO01、APO03、APO10、APO12、APO13、APO14 • BAI06、BAI10 • DSS02、DSS04、DSS05、DSS06 • MEA01、MEA03、MEA04	重要的组织结构包括： • 安全战略委员会 • CISO 重要的文化和行为领域包括： • 安全意识 信息流： • 安全政策 • 安全战略	信息安全焦点领域[38]
	正常	50%	• *按照初步范围定义*	• *不适用*	COBIT 核心模型
DF6	**合规性要求**				
	正常	100%	重要的管理目标包括： • EDM01、EDM03 • APO12 • MEA03、MEA04	• *不适用*	COBIT 核心模型
DF7	**IT 角色**				

	战略	5（共 5 分）	战略和工厂模式相结合（双模式方法）；请参阅**图 4.5** 了解与工厂和整顿 IT 有关的治理和管理目标	典型的双模式组件，包括：
				• 组织结构
				  ■ 首席数字官
				• 技能和能力
				  ■ 可以在兼具探索与开发的灵活环境中工作的员工
				• 流程
				  ■ 整合了探索与开发数字化转型机会的组合和创新流程
					数字化转型焦点领域[39]

[38] *《COBIT® 2019 设计指南：信息和技术治理解决方案的设计》*出版时，信息安全焦点领域的内容正在制定中，尚未发布。
[39] *《COBIT® 2019 设计指南：信息和技术治理解决方案的设计》*出版时，正在考虑将数字化转型焦点领域的内容作为未来的潜在焦点领域。

图 7.42—适用于示例 2 的治理系统范围优化表（续）					
参考编号	**设计因素**	**值**	**治理和管理目标优先级**	**组件**	**焦点领域指南**
DF8	**IT 采购模式**				
	云	100%	重要的管理目标包括： • APO09、APO10 • MEA01	• *不适用*	云焦点领域[40]
DF9	**IT 实施方法**				
	DevOps 敏捷 传统	70% 15% 15%	重要的治理和管理目标包括： • BAI02、BAI03、BAI06	DevOps 焦点领域指南所识别的重要且具体的角色	DevOps 焦点领域[41]
DF10	**技术采用战略**				
	先行者	100%	重要的治理和管理目标包括：	能以较快步伐运行的流程	DevOps 焦点领域[41]
			• EDM01、EDM02 • APO02、APO04、APO05、APO08 • BAI01、BAI02、BAI03、BAI05、BAI07、BAI11 • MEA01		数字化转型焦点领域
DF11	**企业规模**				
	中型		• *按照初步范围定义*	• *不适用*	SME 焦点领域

对于**图 7.42** 中的各设计因素而言，可将所评估的当前状况和与之对应的治理和管理目标以及**图 7.42** 中的其他指南相结合。下列示例是通过将输入值与这些值同治理和管理目标之间的对应关系进行矩阵计算而生成的。对应关系表位于本书的附录 F 至 K。生成包含优先治理和管理目标的蜘蛛图，展示其相较于基准级别的相对重要级别。相对重要级别以 -100 到 +100 的度量指标表示，其中零 (0) 表示对治理或管理目标的重要性毫无影响，+100 表示该目标会因当前设计因素而变得加倍重要。

[40] *《COBIT® 2019 设计指南：信息和技术治理解决方案的设计》*出版时，正在考虑将云焦点领域的内容作为未来的潜在焦点领域。
[41] *《COBIT® 2019 设计指南：信息和技术治理解决方案的设计》*出版时，DevOps 焦点领域的内容正在制定中，尚未发布。

第 3.1 步：思考当前 IT 威胁环境 — **图 7.43** 描述了该企业认为其运营所处的威胁环境。**图 7.44** 显示了所评估的威胁环境对治理和管理目标的影响。

图 7.43—示例 2，第 3.1 步：威胁环境

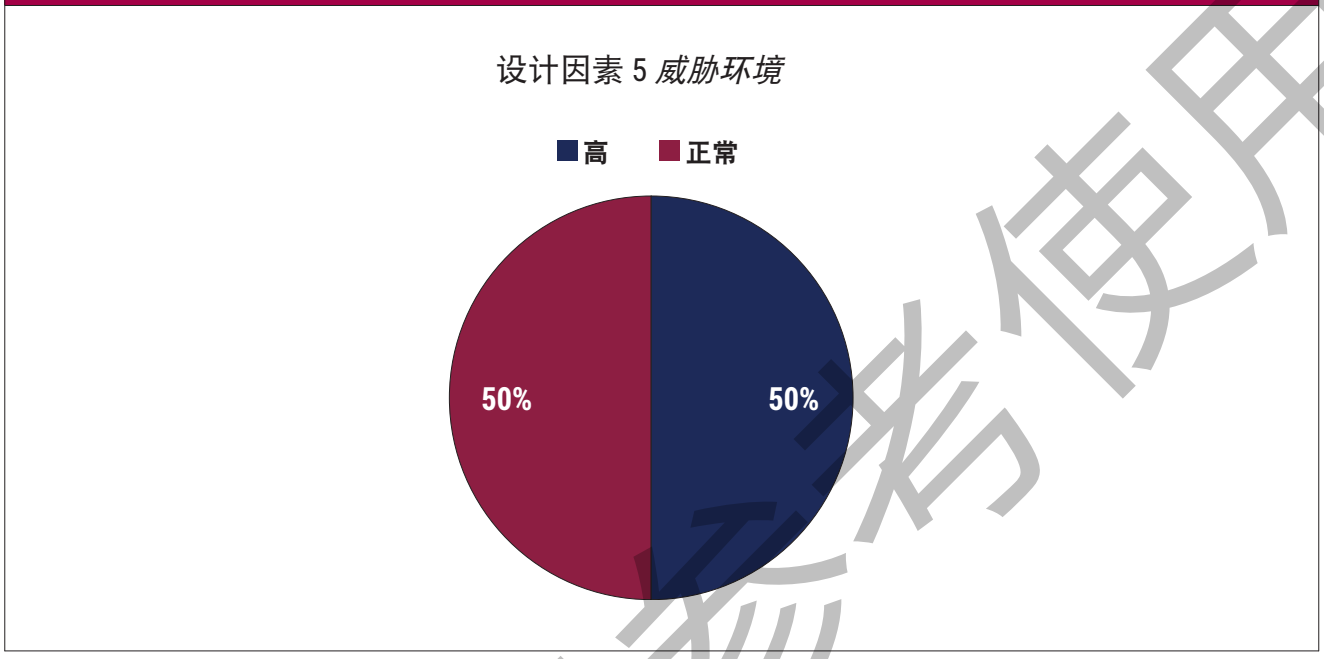
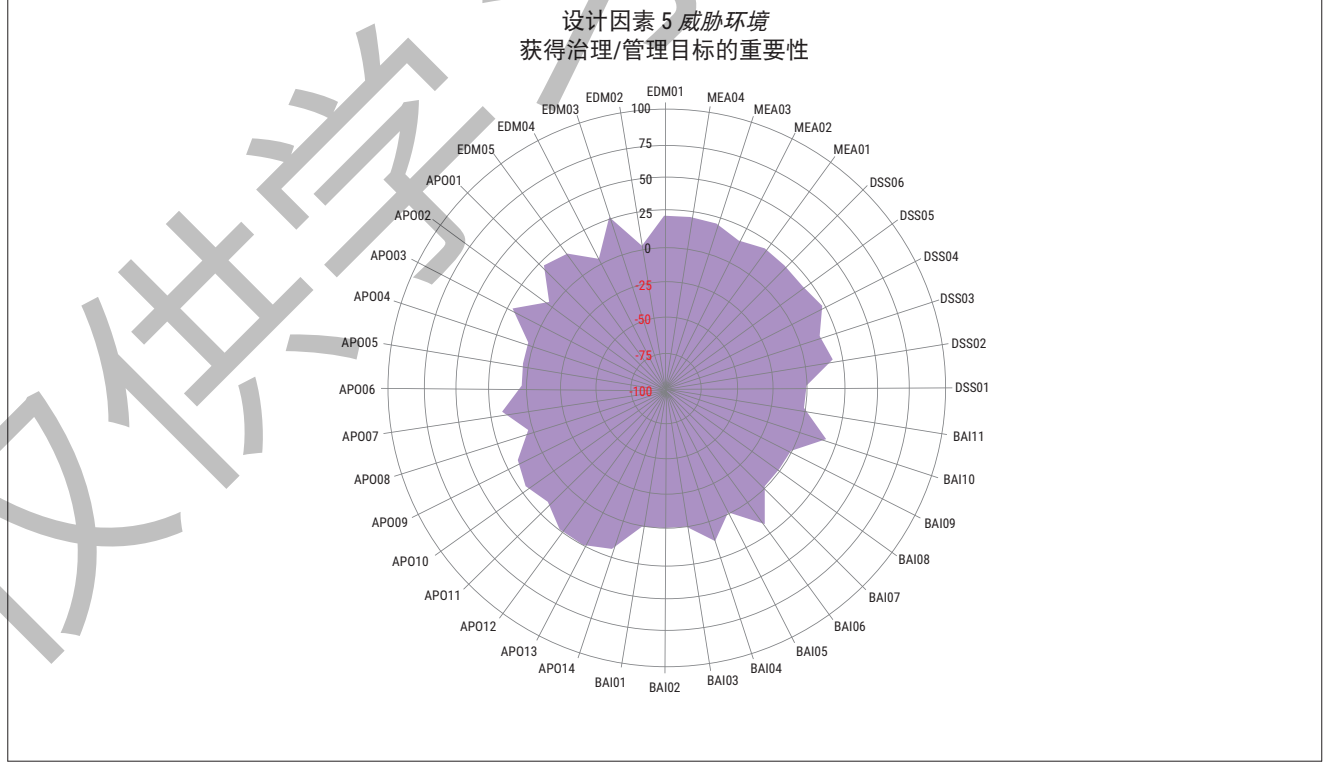


图 7.44—示例 2，第 3.1 步：针对设计因素 5 威胁环境获得治理/管理目标的重要性



根据**图 7.42** 中的高威胁环境相关条目，这种威胁环境分类提高了大量治理和管理目标的重要性。这些和治理以及管理目标相关的指南应从信息安全焦点领域指南中提取，因为该指南包含比 COBIT 核心模型更为详细且具体的网络安全指南。[42]

此外，该企业必须考虑将下列各项纳入其治理系统设计：

- 重要的组织结构，包括：
  - 安全战略委员会
  - CISO
- 重要的文化和行为领域，包括：
  - 安全意识
- 信息流：
  - 安全政策
  - 安全战略

[42] *《COBIT® 2019 设计指南：信息和技术治理解决方案的设计》*出版时，信息安全焦点领域的内容正在制定中，尚未发布。

第 3.2 步：思考合规性要求 — **图 7.45** 描述了该企业的合规性要求，这些要求的预估级别为正常。**图 7.46** 显示了所评估的合规性要求对治理和管理目标的影响。这不会造成任何影响，因为正常属于基准情况，所以这是意料之中的结果。

图 7.45—示例 2，第 3.2 步：合规性要求

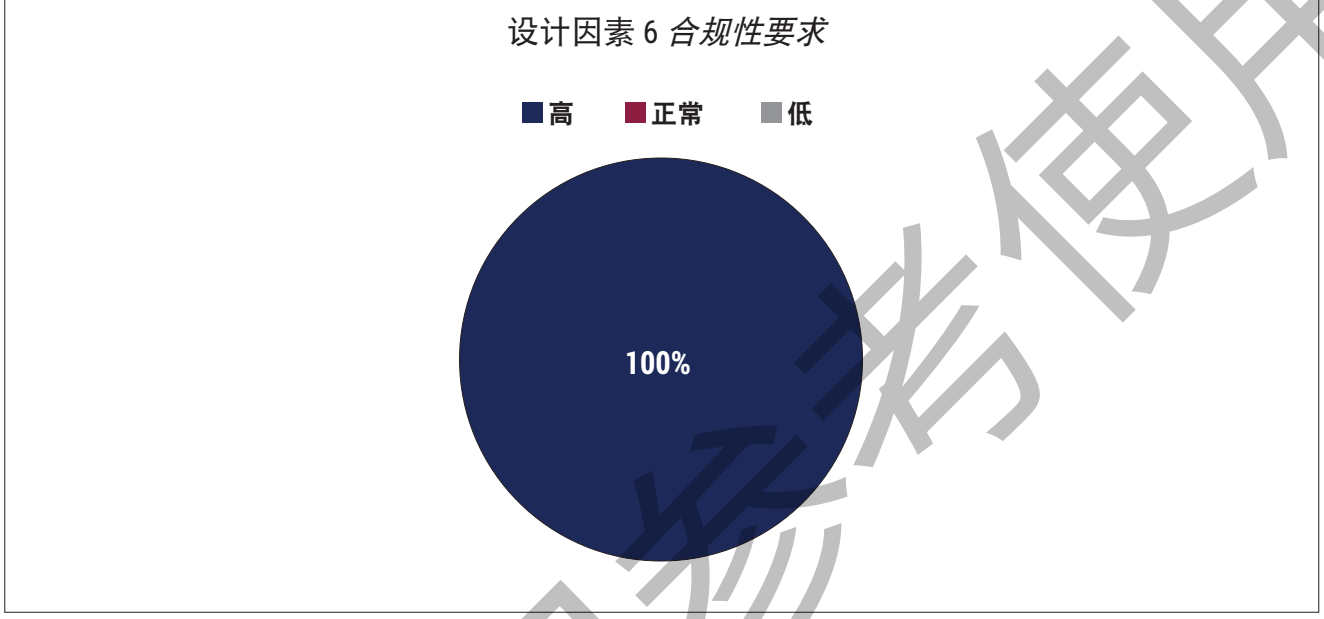
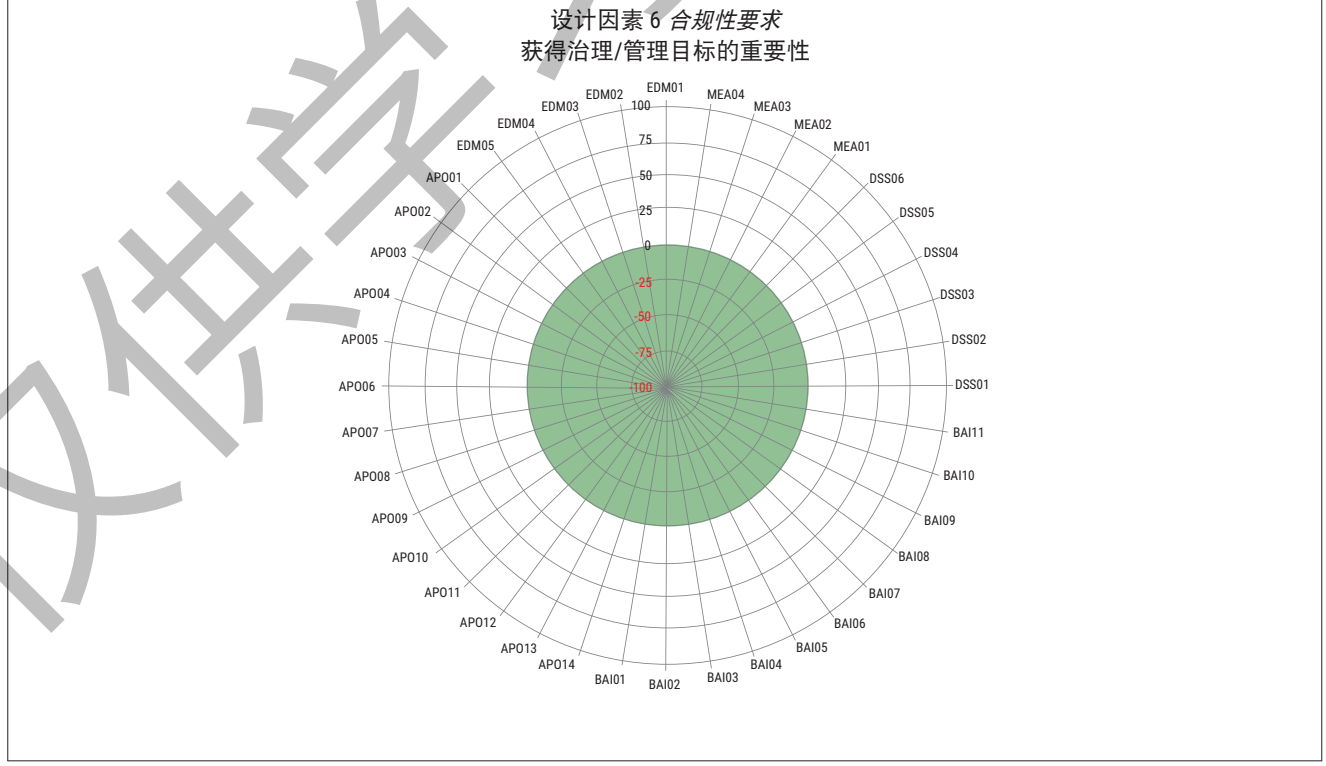


图 7.46—示例 2，第 3.2 步：针对设计因素 6 *合规性要求*获得治理/管理目标的重要性



第 3.3 步：思考 IT 角色 — **图 7.47** 显示了作为“战略”的 IT 角色。**图 7.48** 显示了所评估的 IT 角色对治理和管理目标的影响。

图 7.47—示例 2，第 3.3 步：IT 角色

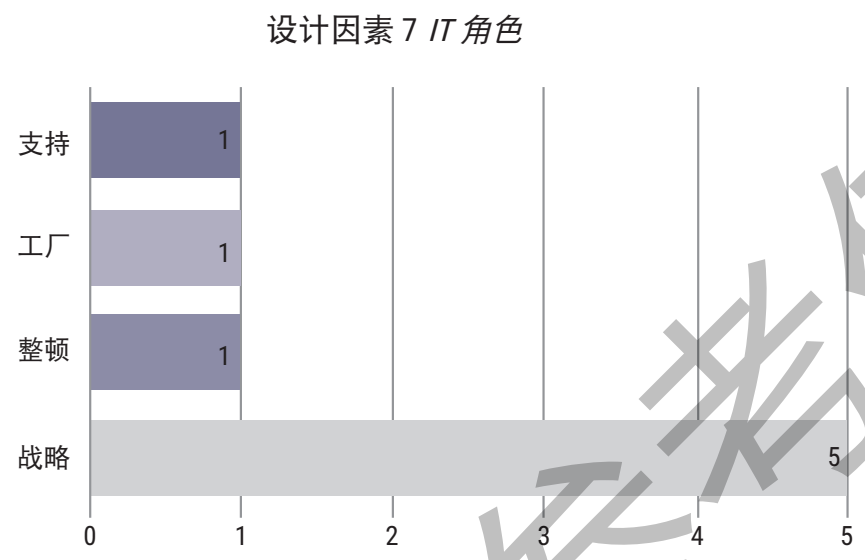
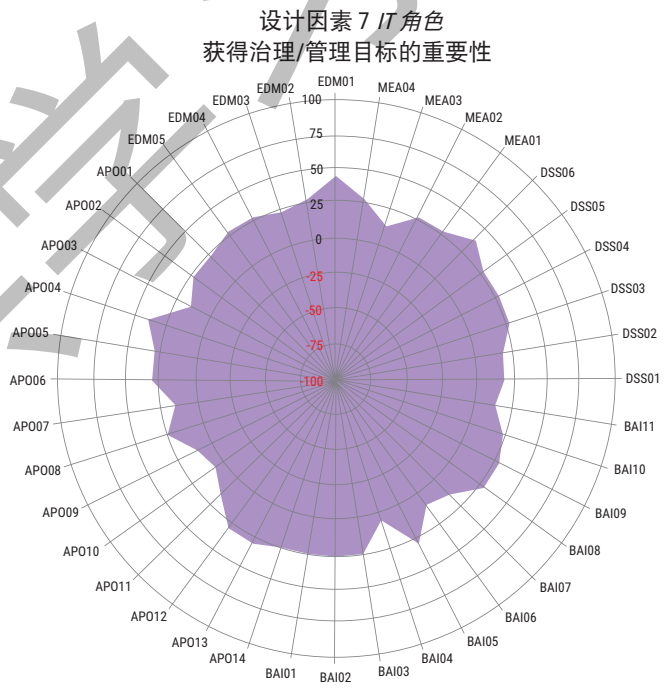


图 7.48—示例 2，第 3.3 步：针对设计因素 7 *IT 角色*获得治理/管理目标的重要性



该企业还必须思考下列典型的双模式组件，并将其纳入治理系统设计中：

- 组织结构：首席数字官
- 技能和能力：可以在兼具探索和开发的灵活环境中工作的员工
- 流程：投资组合和创新过程，这个过程整合了对数字化转型机会的探索和开发

除了优先的治理和管理目标以外，还应从数字化转型焦点领域提取指南（如可用）。

第 3.4 步：思考 IT 采购模式 — **图 7.49** 描述了该企业所选择的全云端采购模式。**图 7.50** 显示了所评估的采购模式对治理和管理目标的影响。该图显示，此影响仅集中在三个管理目标上。此外，该企业将不得不借鉴云焦点领域指南（如可用）。

图 7.49—示例 2，第 3.4 步：IT 采购模式

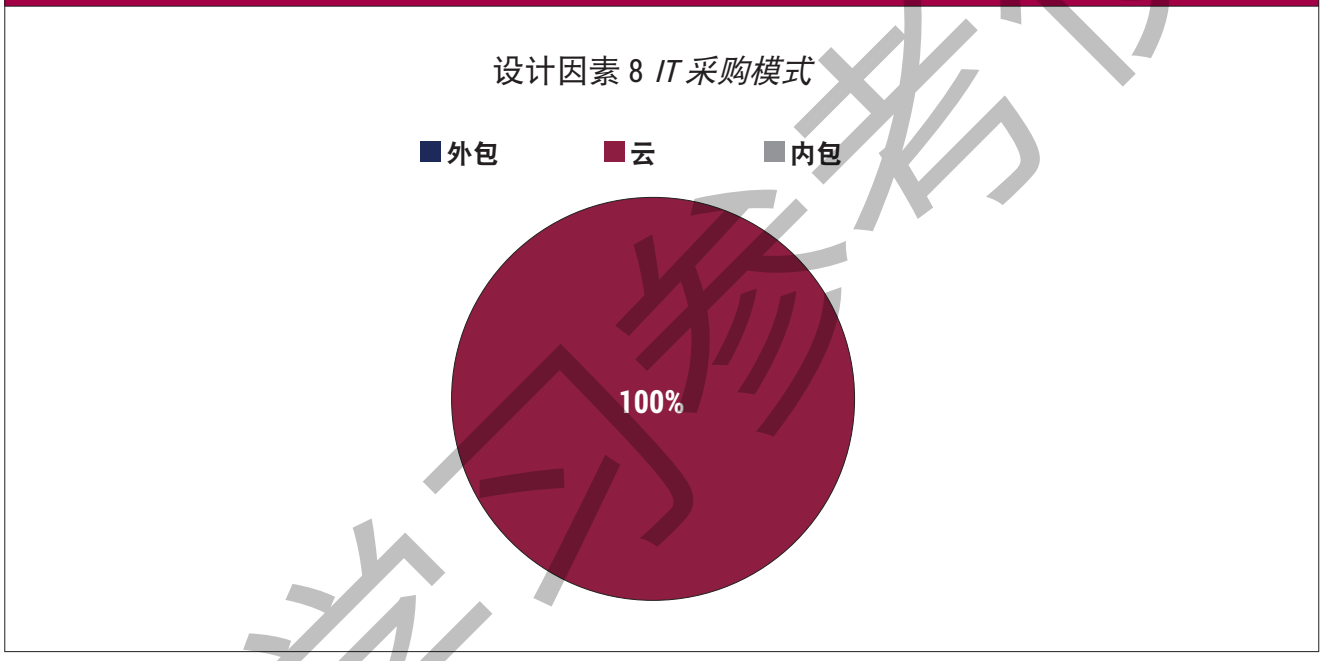
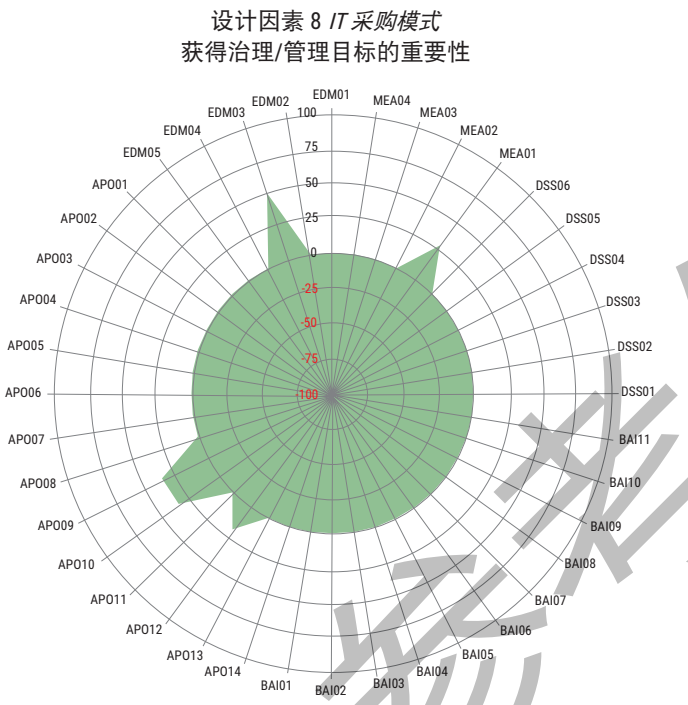


图 7.50—示例 2，第 3.4 步：针对设计因素 8 *IT 采购模式*获得治理/管理目标的重要性



第 3.5 步：思考 IT 实施方法 — 该企业主要使用 DevOps IT 实施方法（参见**图 7.51**）。**图 7.52** 显示了这对治理和管理目标的影响。相关指南应从**图 7.42** 所示的 DevOps 管理焦点领域提取。

图 7.51—示例 2，第 3.5 步：IT 实施方法

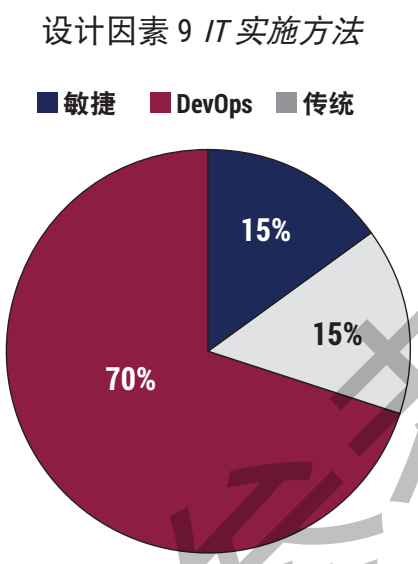
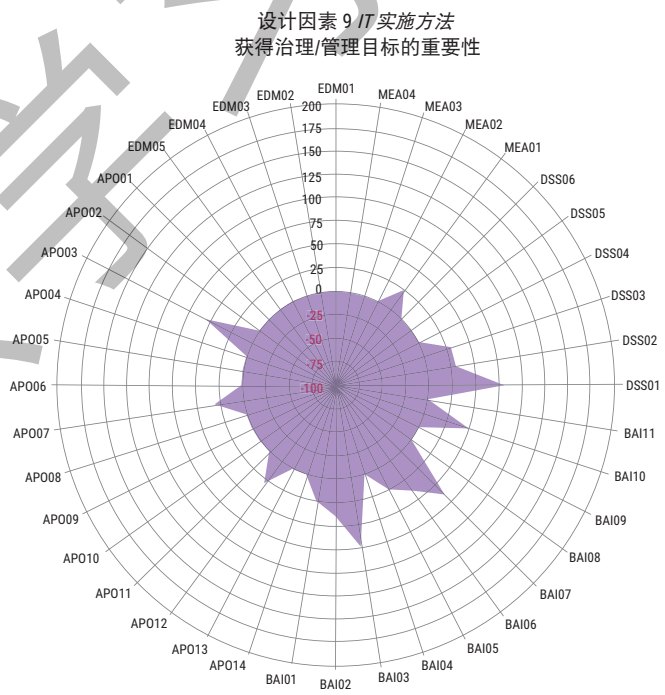


图 7.52—示例 2，第 3.5 步：针对设计因素 9 *IT 实施方法*获得治理/管理目标的重要性



第 3.6 步：思考技术采用战略 — **图 7.53** 表明该企业在采用新技术方面是先行者。**图 7.54** 显示了这对治理和管理目标优先级的影响。

图 7.53—示例 2，第 3.6 步：技术采用战略

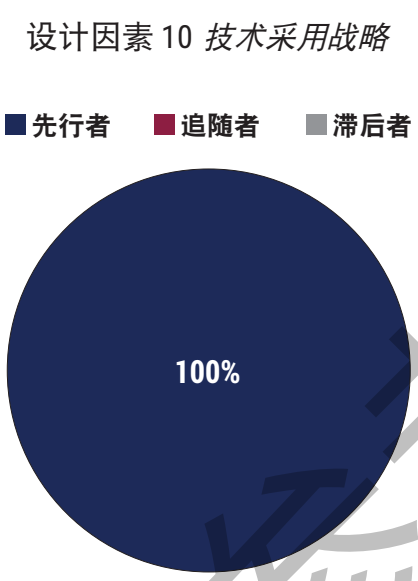
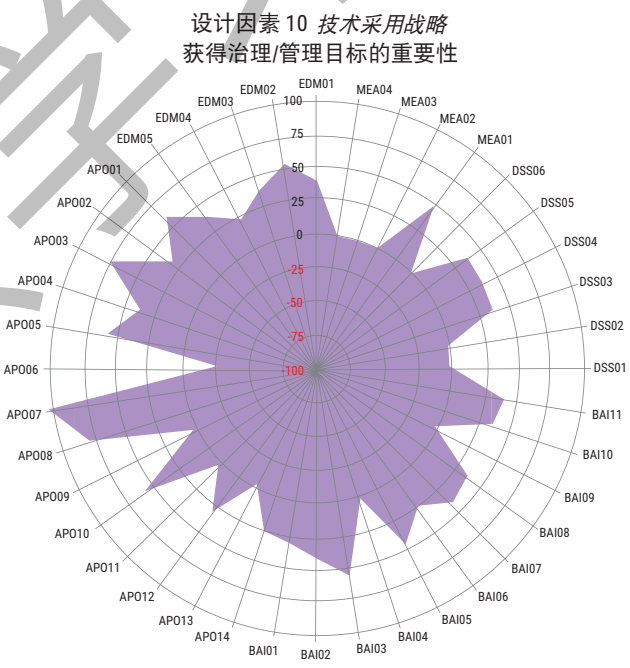


图 7.54—示例 2，第 3.6 步：针对设计因素 10 *技术采用战略*获得治理/管理目标的重要性



除了优先的治理和管理目标以外，还应从数字化转型和 DevOps 焦点领域提取指南（如可用）。

第 3.7 步：思考企业规模 — 该企业是中型企业。**图 7.42** 表明，应将中小型企业的焦点领域[43] 用作定义治理系统的基础。

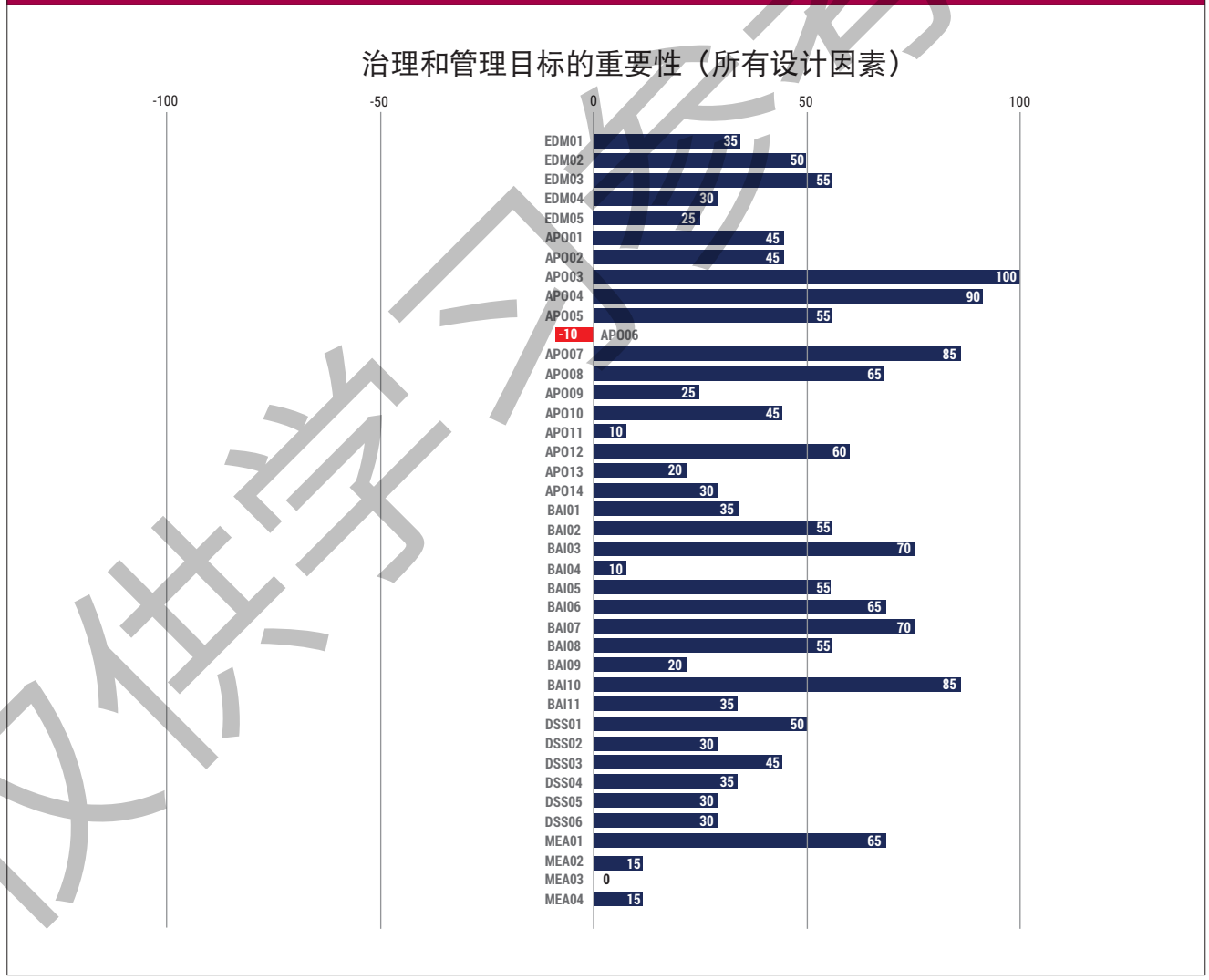
7.3.4 第 4 步：确定治理解决方案的最终设计

设计过程的最后一步需要讨论前述步骤的所有输入，解决冲突，以及达成一致结论。由此产生的治理系统反映了对所有输入的慎重考虑，并且还考虑到了这些输入有时存在冲突，必须做出适当选择。

7.3.4.1 治理和管理目标

此时可将第 3.1 至 3.7 步获得的治理和管理优先级添加到第 2.1 至 2.4 步产生的初步治理系统设计的结果中。综合得出治理体系中下列治理和管理目标优先级调整结果（**图 7.55**）。

图 7.55—示例 2，第 4.1 步：治理和管理目标的重要性（所有设计因素）



[43] *《COBIT® 2019 设计指南：信息和技术治理解决方案的设计》*出版时，中小型企业焦点领域的内容正在制定中，尚未发布。

下列管理目标可能对该企业的治理系统非常重要：

- APO03 *妥当管理的企业架构* (100)
- APO04 *妥当管理的创新* (90)
- APO07 *妥当管理的人力资源* (85)
- BAI10 *妥当管理的配置* (85)
- BAI03 *妥当管理的解决方案识别和构建* (70)
- BAI07 *妥当管理的 IT 变更接受和交接* (70)

与第 2.5 步中的初步范围定义所识别的列表相比，最重要的目标略有变化。

下列管理目标似乎最不重要：

- APO06 *妥当管理的预算和成本*
- MEA03 *妥当管理的外部要求合规性*
- APO11 *妥当管理的项目*
- BAI04 *妥当管理的可用性和容量*

将此结果与初步范围进行比较后，可以得出如下结果：

- 总体而言，在考虑额外设计因素后，大多数治理/管理目标变得更加重要；这可以通过高威胁环境和 I&T 的战略角色进行解释。
- 初步范围定义后评级最高的治理/管理目标，通常在范围优化后的评级仍然很高。

该企业对治理和管理目标的重要性评级表示满意。

经过讨论，该企业认为其第一阶段的治理系统设计将由**图 7.56** 所示的治理和管理目标（和基础流程）组成。

图 7.56—示例 2 治理和管理目标以及目标流程能力级别

参考编号	治理/管理目标	目标流程能力级别
EDM01	确保治理框架的设置和维护	2
EDM02	确保实现效益	3
EDM03	确保风险优化	3
EDM04	确保资源优化	2
EDM05	确保利益相关方参与	2
APO01	妥当管理的 I&T 管理框架	2
APO02	妥当管理的战略	2
APO03	妥当管理的企业架构	4
APO04	妥当管理的创新	4
APO05	妥当管理的组合	3
APO07	妥当管理的人力资源	4
APO08	妥当管理的关系	3
APO09	妥当管理的服务协议	2
APO10	妥当管理的供应商	2
APO12	妥当管理的风险	3
APO14	妥当管理的数据	2

图 7.56—示例 2 治理和管理目标以及目标流程能力级别（续）		
参考编号	治理/管理目标	目标流程能力级别
BAI01	妥当管理的计划	2
BAI02	妥当管理的需求定义	3
BAI03	妥当管理的解决方案识别和构建	3
BAI05	妥当管理的组织变更	3
BAI06	妥当管理的 IT 变更	3
BAI07	妥当管理的 IT 变更接受和交接	3
BAI08	妥当管理的知识	3
BAI10	妥当管理的配置	4
BAI11	妥当管理的项目	2
DSS01	妥当管理的运营	3
DSS02	妥当管理的服务请求和事故	2
DSS03	妥当管理的问题	2
DSS04	妥当管理的连续性	2
DSS05	妥当管理的安全服务	2
DSS06	妥当管理的业务流程控制	2
MEA01	妥当管理的绩效和一致性监控	3

图 7.56 显示了参考资料、治理或管理目标的标题，以及相关流程应实施的目标能力级别。鉴于很多流程都极为重要，所以目标能力级别被设定为更高的值（3 或 4）。该企业运用的逻辑与示例 1 所使用的逻辑相同：

- 如果治理/管理目标的得分为 75 或更高，则表明其重要性相比基准情况至少高 75%，所以需要能力级别 4。
- 得分为 50 或更高的任何治理/管理目标需要能力级别 3。
- 得分为 25 或更高的任何治理/管理目标需要能力级别 2。

7.3.4.2 其他组件

该企业需要特别注意，应强有力地实施治理系统的下列角色和结构（及其他组件）：

- 通过投资办公室来支持投资组合管理角色
- 企业架构师和首席数字官的角色
- 旨在促进自动化和发展以及实现规模经济的服务、基础设施和应用程序组件
- 文化和行为组件对创新的影响
- 重要的组织结构，包括：
  - 安全战略委员会
  - CISO
- 重要的文化和行为领域，包括：
  - 安全意识
- 信息流：
  - 安全政策
  - 安全战略
- 技能和能力：可以在兼具探索和开发的灵活环境中工作的员工
- 流程：投资组合和创新过程，这个过程整合了对数字化转型机会的探索和开发

7.3.4.3 具体焦点领域指南

该企业会将下列指南作为 COBIT 核心指南的补充资料：

- 中小型企业焦点领域指南，因为它是专为小型组织量身定制的
- 信息安全焦点领域指南，考虑到高威胁环境以及风险分析结果和当前的 I&T 相关问题
- DevOps、云和数字化转型焦点领域指南（如适用且可用）

7.4 示例 3：知名政府机构

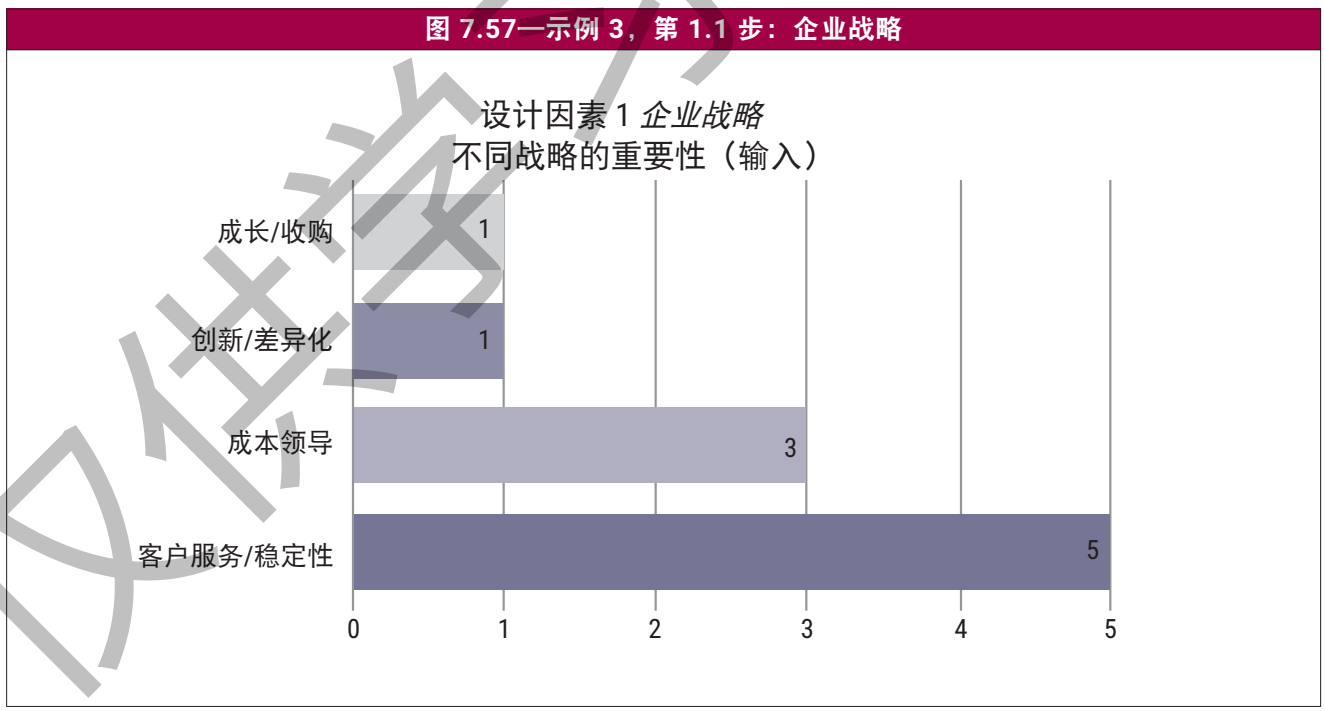
此案例研究旨在展示如何运用工作流程为知名的大型政府机构设计量身定制的治理系统，这些机构致力于向需要帮助的选民提供医疗保健、金融支付、教育和其他必要的服务。该机构的业务遍布范围较广，在全国各地都设有医院、诊所和办事处。该机构的 I&T 预算以及计划和运营预算分布在医院、财务效益和其他业务部门之间，而 IT 商店负责提供基础设施支持、网络运营和安全运营中心。该机构认为 I&T 对组织取得成功至关重要，并且它必须遵守法律法规，尤其是不断出现的新医疗法规。该机构采用传统方法进行开发和运营工作，并且对新技术的采用犹豫不决。该机构的审计职能部门非常活跃，并且有数十个重要审计发现都与该机构如何保护其 I&T有关，尤其是在安全和隐私方面。作为政府机构，它是黑客的主要攻击目标，并且其整个受益人档案刚刚遭受过重大攻击。

7.4.1 第 1 步：了解企业环境和战略

首先需要汇总该机构的内外部环境。

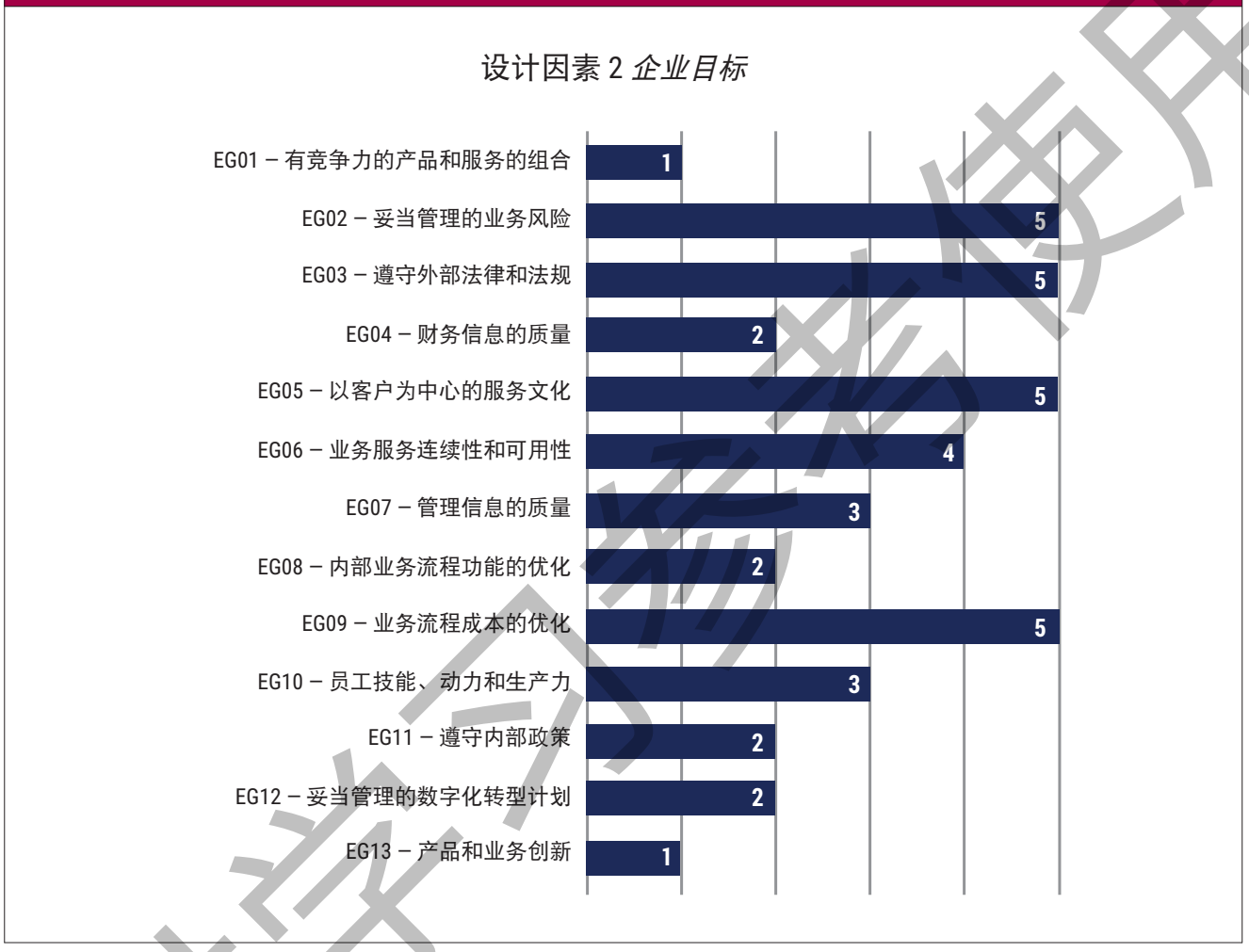
第 1.1 步：了解企业战略 — 该机构专注于为选民提供优质服务（如**图 7.57** 所示）。

图 7.57—示例 3，第 1.1 步：企业战略



第 1.2 步：了解企业目标 — 该机构对**图 7.58** 所示的 13 个通用企业目标进行了评级（评级范围为 1 到 5 分）。该图表明 EG02 *妥当管理的业务风险*、EG03 *遵守外部法律法规*、EG05 *以客户为中心的服务文化*和 EG09 *业务流程成本的优化*是评级最高的企业目标。

图 7.58—示例 3，第 1.2 步：企业目标



第 1.3 步：了解风险概况 — 利用整体风险分析获得的风险状况如**图 7.59** 所示。

图 7.59—示例 3，第 1.3 步：风险概况

风险情景类别	影响 (1-5)	可能性 (1-5)	风险评级
IT 投资决策制定、投资组合定义和维护	4	4	●
计划和项目生命周期管理	4	4	●
IT 成本和监督	2	2	●
IT 专业知识、技能和行为	4	4	●
企业/IT 架构	2	2	●
IT 运营基础设施事故	4	4	●
未授权的行动	4	4	●
软件采用/使用问题	3	3	●
硬件事故	2	2	●
软件故障	3	3	●
逻辑攻击（黑客攻击、恶意软件等）	4	5	●
第三方/供应商事故	2	2	●
违规	3	3	●
地缘政治问题	2	2	●
劳工行动	1	3	●
自然灾害	3	3	●
基于技术的创新	4	3	●
环境	2	3	●
数据和信息管理	4	4	●

●	极高风险
●	高风险
●	中度风险
●	低风险

第 1.4 步：了解当前的 I&T 相关问题 — 对当前状况进行分析可获得**图 7.60** 所述的当前 I&T 相关问题的评估。

图 7.60—示例 3，第 1.4 步：I&T 相关问题

值	重要性 (1-3)	*基准*
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	X	2
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	X	2
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	X	2
IT 外包商的服务交付问题	!	2
不符合 IT 相关法规或合同要求	!	2
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	X	2
重大的隐性和反常的 IT 支出，即用户部门在正常的 IT 投资决策机制控制范围和批准的预算之外的 I&T 支出	X	2
多个举措之间的重复或重叠，或其他形式的资源浪费	X	2
IT 资源不足，员工技能欠缺或员工倦怠/不满	✔	2
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	X	2
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	!	2
复杂的 IT 运营模式和/或缺乏明确的 IT 相关决策机制	X	2
过高的 IT 成本	✔	2
当前 IT 架构和系统导致新举措或创新的实施受阻或失败	✔	2
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	✔	2
各种来源的数据经常出现数据质量和整合方面的问题	✔	2
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、质量控制以及其他问题	X	2
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	X	2
忽视和/或违反隐私法规	✔	2
无法利用新技术或使用 I&T 进行创新	!	2

✔	无问题
!	问题
X	严重问题

7.4.2 第 2 步：确定治理系统的初步范围

可利用第 1 步收集所得的（部分或全部）信息确定治理系统的初步范围。第 2 步会将这些关于企业战略、企业目标、风险概况和 I&T 相关问题的信息转换为相关的治理组件。

第 2.1 步：思考企业战略 — 下图为第 1.1 步中确定的企业战略（**图 7.61**）。**图 7.62** 表明了这些战略对治理和管理目标的相对影响。

图 7.61—示例 3，第 2.1 步：企业战略

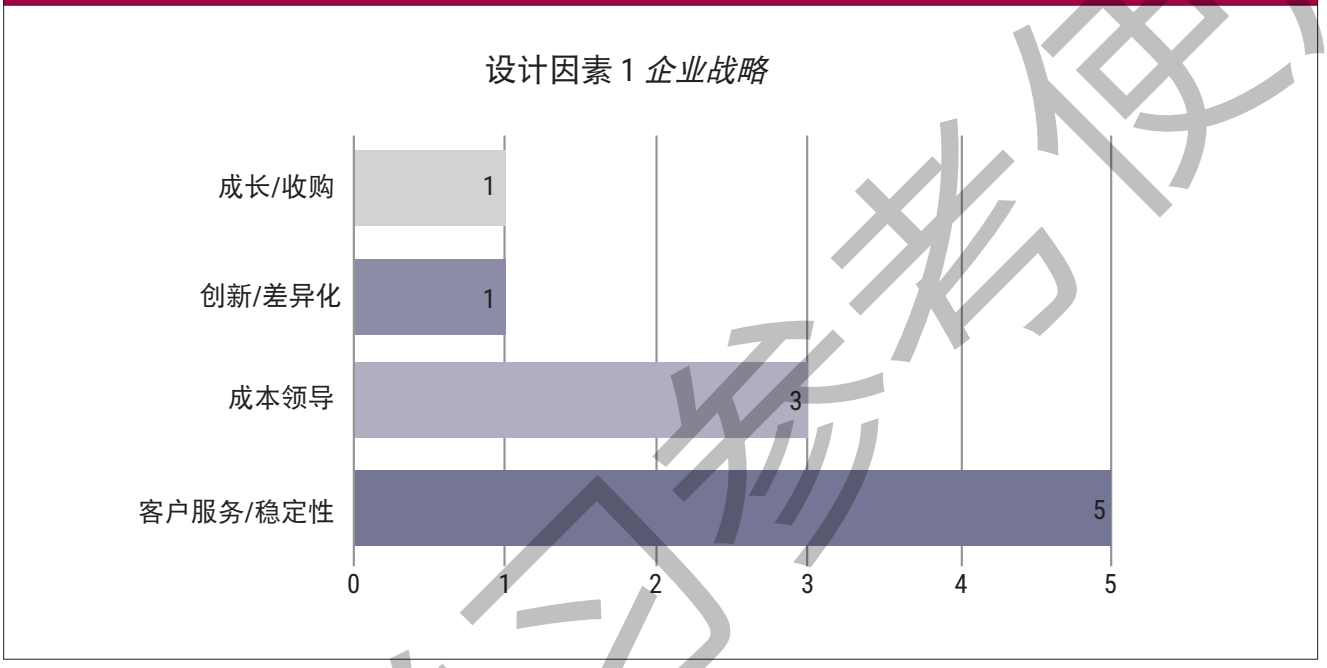
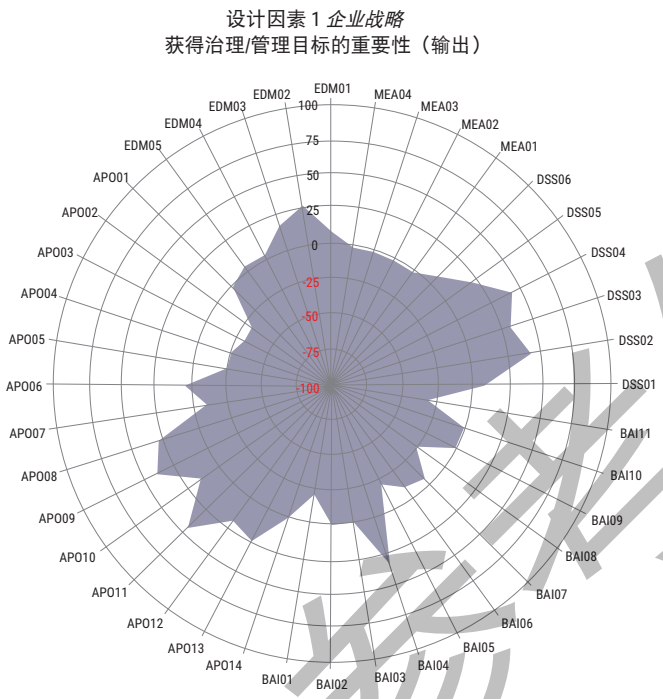


图 7.62—示例 3，第 2.1 步：针对设计因素 1 *企业战略*获得治理/管理目标的重要性



第 2.2 步：思考企业目标并运用 COBIT 目标级联 — 此时需要按照第 1.2 步指定的评级，运用 COBIT 目标级联来确定哪些治理和管理目标与实现优先的企业目标有关（**图 7.63**）。**图 7.64** 表明了这些已评级的企业目标对治理和管理目标的相对影响。

图 7.63—示例 3，第 2.2 步：企业目标

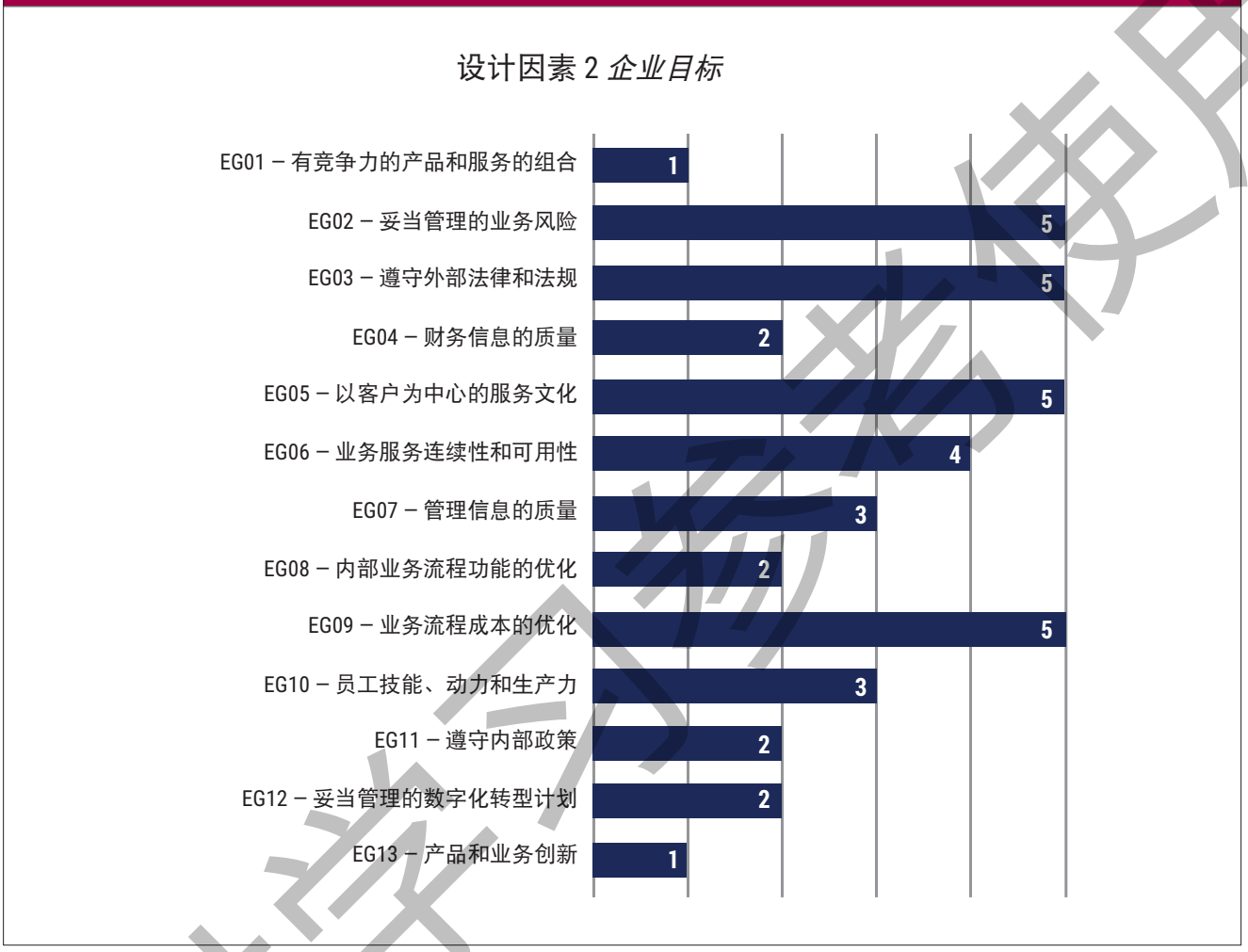
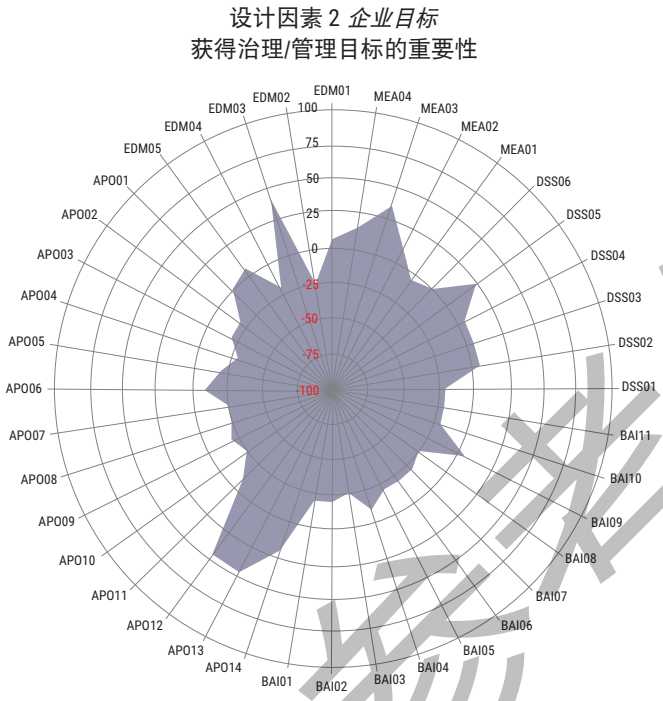


图 7.64—示例 3，第 2.2 步：针对设计因素 2 *企业目标*获得治理/管理目标的重要性



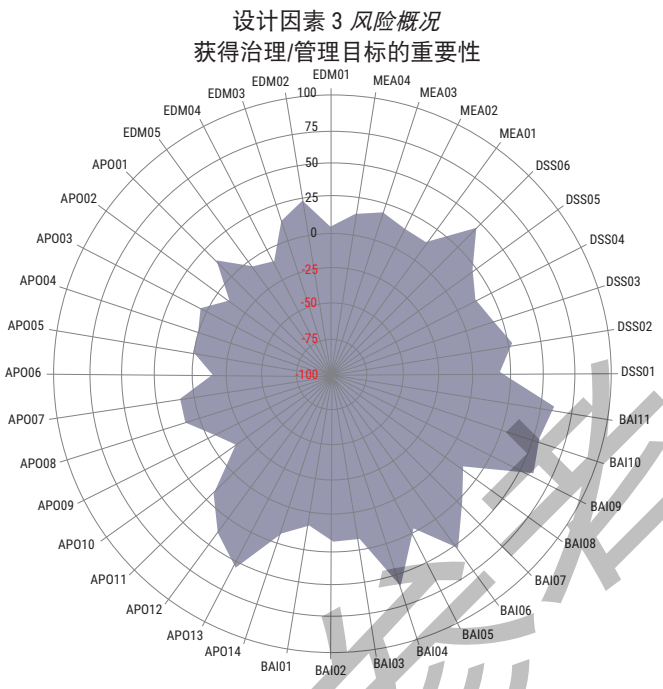
第 2.3 步：思考企业的风险概况 — 第 1.3 步已在总体层面识别和分析 IT 风险类别（**图 7.65**）。基于风险概况与 COBIT 治理和管理目标之间的对应关系（如第 4.2.3 节所述）以及**附录 D** 中的对应关系表，**图 7.66** 已按照风险分析的结果显示治理和管理目标的相对评级。

图 7.65—示例 3，第 2.3 步：风险概况

风险情景类别	影响 (1-5)	可能性 (1-5)	风险评级
IT 投资决策制定、投资组合定义和维护	4	4	●
计划和项目生命周期管理	4	4	●
IT 成本和监督	2	2	●
IT 专业知识、技能和行为	4	4	●
企业/IT 架构	2	2	●
IT 运营基础设施事故	4	4	●
未授权的行动	4	4	●
软件采用/使用问题	3	3	●
硬件事故	2	2	●
软件故障	3	3	●
逻辑攻击（黑客攻击、恶意软件等）	4	5	●
第三方/供应商事故	2	2	●
违规	3	3	●
地缘政治问题	2	2	●
劳工行动	1	3	●
自然灾害	3	3	●
基于技术的创新	4	3	●
环境	2	3	●
数据和信息管理	4	4	●

●	极高风险
●	高风险
●	中度风险
●	低风险

图 7.66—示例 3，第 2.3 步：针对设计因素 3 *风险概况*获得治理/管理目标的重要性



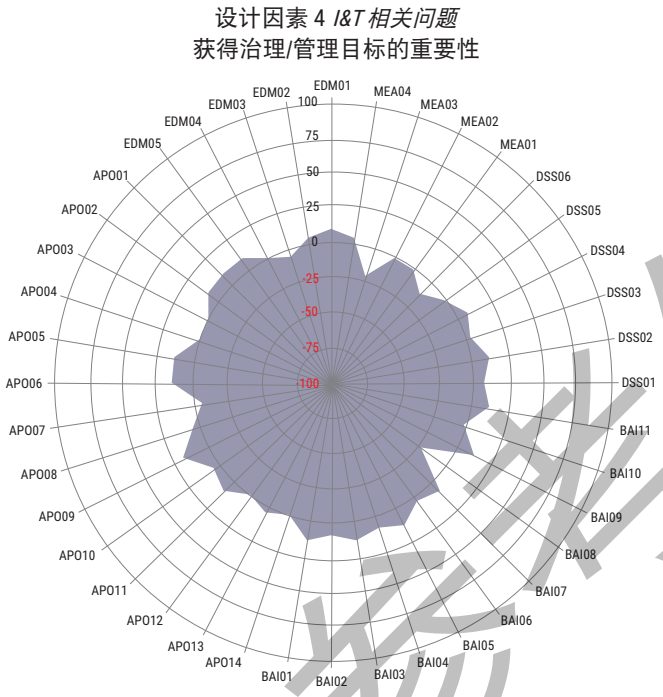
第 2.4 步：思考当前的 I&T 相关问题 — 此步骤利用对应关系表（**附录 E**）将第 1.4 步所识别的问题与 COBIT 治理和管理目标相关联，而该对应关系表又将每个问题与可能影响该问题的一个或多个治理或管理目标进行关联（**图 7.67**）。基于该对应关系（如第 4.2.4 节所述），**图 7.68** 已按照当前 I&T 相关问题的分析结果显示治理和管理目标的相对评级。

图 7.67—示例 3，第 2.4 步：I&T 相关问题

值	重要性 (1-3)	*基准*
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	✗	*2*
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	✗	*2*
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	✗	*2*
IT 外包商的服务交付问题	!	*2*
不符合 IT 相关法规或合同要求	!	*2*
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	✗	*2*
重大的隐性和反常的 IT 支出，即用户部门在正常的 IT 投资决策机制控制范围和批准的预算之外的 I&T 支出	✗	*2*
多个举措之间的重复或重叠，或其他形式的资源浪费	✗	*2*
IT 资源不足，员工技能欠缺或员工倦怠/不满	✓	*2*
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	✗	*2*
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	!	*2*
复杂的 IT 运营模式和/或缺乏明确的 IT 相关决策机制	✗	*2*
过高的 IT 成本	✓	*2*
当前 IT 架构和系统导致新举措或创新的实施受阻或失败	✓	*2*
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	✓	*2*
各种来源的数据经常出现数据质量和整合方面的问题	✓	*2*
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、质量控制以及其他问题	✗	*2*
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	✗	*2*
忽视和/或违反隐私法规	✓	*2*
无法利用新技术或使用 I&T 进行创新	!	*2*

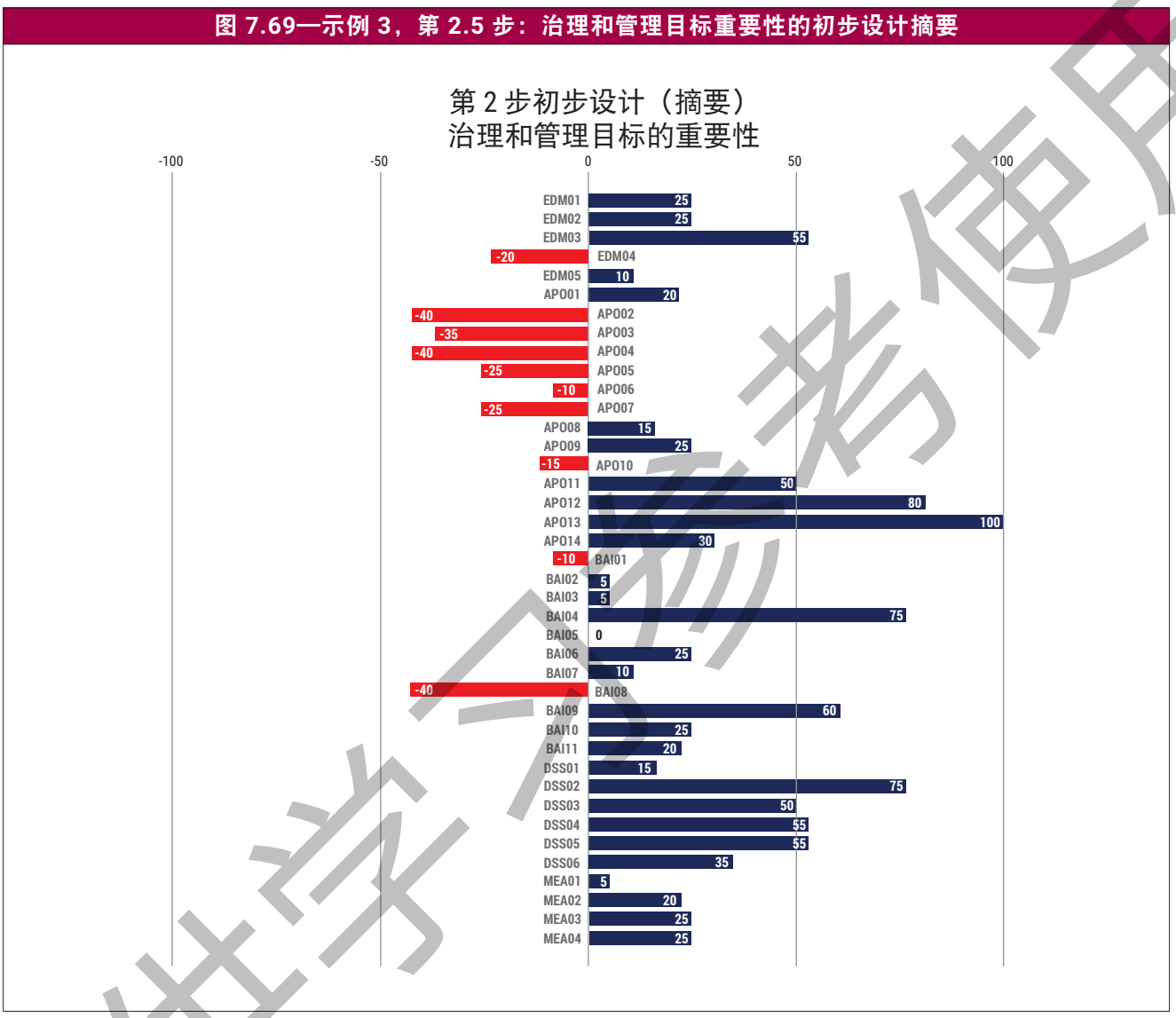
✓	无问题
!	问题
✗	严重问题

图 7.68—示例 3，第 2.4 步：针对设计因素 4 *I&T 相关问题*获得治理/管理目标的重要性



第 2.5 步：治理系统的初步范围 — 此时可将前述步骤中得到的治理和管理优先级相结合。与管理层讨论初步结果，并对两个管理目标进行调整：APO02 *妥当管理的战略*（优先级提高）和 APO09 *妥当管理的服务协议*（优先级降低）。经过这些调整后，获得了治理系统中下列治理和管理目标的初步优先级。

图 7.69—示例 3，第 2.5 步：治理和管理目标重要性的初步设计摘要



综合考虑优先级评分等于或高于 60 的所有治理和管理目标，下列治理和管理目标可能对该机构的治理系统非常重要：

- APO13 *妥当管理的安全* (100)
- APO12 *妥当管理的风险* (80)
- DSS02 *妥当管理的服务请求和事故* (75)
- BAI04 *妥当管理的可用性和容量* (75)
- BAI09 *妥当管理的资产* (60)

下列管理目标似乎（目前而言）最不重要（分数低于 -25）：

- APO02 *妥当管理的战略*
- APO04 *妥当管理的创新*
- BAI08 *妥当管理的知识*
- APO03 *妥当管理的企业架构*

下一步将确定此治理系统的初步范围需要进行哪些优化。

7.4.3 第 3 步：优化治理系统的范围

第 3 步需要根据待分析的一组设计因素来识别初步范围所需的优化。并非所有设计因素都适用于每家企业，所以有时可以忽略其中的某些因素。**图 6.70** 总结了本示例所述中型创新公司适用的第 5 至 11 号设计因素。如不止一个值适用于某个设计因素，则会在该图的数值列中显示该值。

图 7.70—适用于示例 3 的治理系统范围优化表

参考编号	设计因素	数值	治理和管理目标优先级	组件	焦点领域指南
DF5	**威胁环境**				
	高	100%	重要的治理和管理目标包括： • EDM01、EDM03 • APO01、APO03、APO10、APO12、APO13、APO14 • BAI06、BAI10 • DSS02、DSS04、DSS05、DSS06 • MEA01、MEA03、MEA04	重要的组织结构包括： • 安全战略委员会 • CISO 重要的文化和行为领域包括： • 安全意识 信息流： • 安全政策 • 安全战略	信息安全焦点领域[44]
DF6	**合规性要求**				
	低	100%	• *按照初步范围定义*	• *不适用*	COBIT 核心模型
DF7	**IT 角色**				
	支持	5（共 5 分）	• *按照初步范围定义*	• *不适用*	COBIT 核心模型
DF8	**IT 采购模式**				
	内包	100%	• *按照初步范围定义*	• *不适用*	COBIT 核心模型
DF9	**IT 实施方法**				
	传统	100%	• *按照初步范围定义*	• *不适用*	COBIT 核心模型
DF10	**技术采用战略**				
	追随者	100%	重要的治理和管理目标包括： • APO02、APO04、 • BAI01	*可以降速运转的流程*	COBIT 核心模型
DF11	**企业规模**				
	大型		• *按照初步范围定义*	• *不适用*	COBIT 核心模型

前述两则示例已对各设计因素的运用进行了极为详细的介绍。所以此示例将不提供详细的计算和图表，而仅显示最终结果。除了运用**图 7.70** 所述的设计因素以外，还需再次强调确保流程与其 I&T 战略保持一致的重要性。

[44] *《COBIT® 2019 设计指南：信息和技术治理解决方案的设计》*出版时，信息安全焦点领域的内容正在制定中，尚未发布。

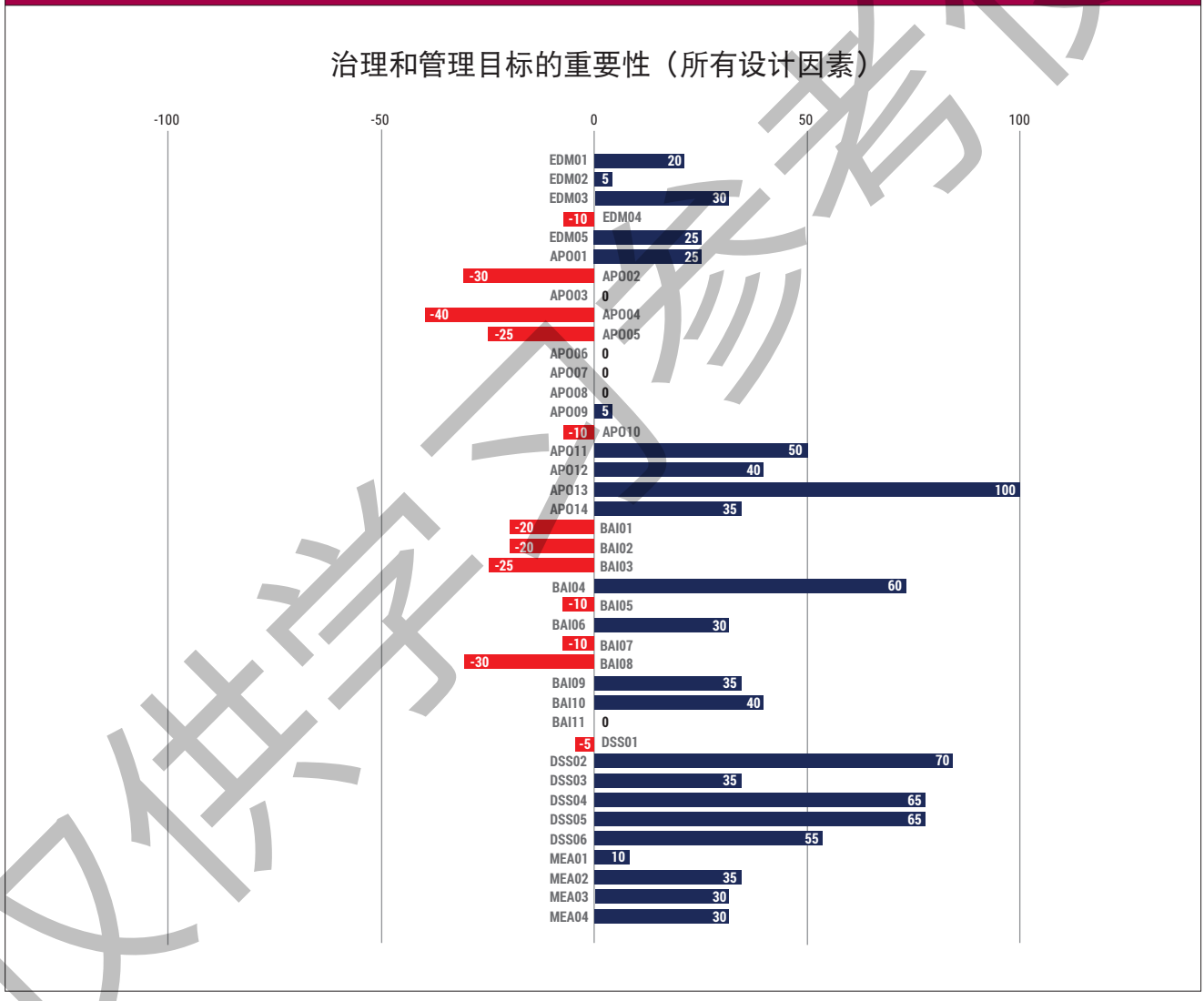
7.4.4 第 4 步：确定治理解决方案的最终设计

设计过程的最后一步需要讨论前述步骤的所有输入，解决冲突，以及达成一致结论。由此产生的治理系统体现了对所有输入的慎重考虑，并且考虑到了这些输入有时存在冲突，必须做出适当的选择，另外也讨论了提高 APO02 *妥当管理的战略*目标的重要性。

7.4.4.1 治理和管理目标

此时可将第 3.1 至 3.7 步获得的治理和管理优先级与第 2.1 至 2.4 步所产生的初步治理系统设计的结果相结合。这样可获得治理系统中下列经调整的治理和管理目标优先级。

图 7.71—示例 3，第 4 步：治理和管理目标的重要性（所有设计因素）



综合考虑优先级评分等于或高于 60 的所有治理和管理目标，下列治理和管理目标可能对该机构的治理系统非常重要：

- APO13 *妥当管理的安全* (100)
- DSS02 *妥当管理的服务请求和事故* (70)
- DSS05 *妥当管理的安全服务* (65)
- DSS04 *妥当管理的连续性* (65)
- BAI04 *妥当管理的可用性和容量* (60)

下列管理目标似乎最不重要（分数低于 -50）：

- APO04 *妥当管理的创新* (-40)
- APO02 *妥当管理的战略* (-30)
- BAI08 *管理知识* (-30)
- APO05 *妥当管理的组合* (-25)
- BAI03 *妥当管理的解决方案识别和构建* (-25)

最终结果反映了初步设计中的优先级（在第 2 步之后获得）的若干变化。

经过讨论，该机构认为其治理系统设计将由**图 7.72** 所示的治理和管理目标的优先列表（和基础流程）组成。该图包含所有 COBIT 治理和管理目标、建议的能力级别（基于第 3 步的结果），以及实际决策管理层选择的目标能力级别。

图 7.72—示例 3：治理和管理目标以及目标流程能力级别

参考编号	治理/管理目标	建议的目标流程能力级别	确定的目标流程能力级别
EDM01	确保治理框架的设置和维护	1	**3**
EDM02	确保实现效益	1	**3**
EDM03	确保风险优化	2	**3**
EDM04	确保资源优化	1	**3**
EDM05	确保利益相关方参与	2	**3**
APO01	妥当管理的 IT 管理框架	2	**2**
APO02	妥当管理的战略	1	**3**
APO03	妥当管理的企业架构	1	**2**
APO04	妥当管理的创新	1	**1**
APO05	妥当管理的组合	1	**3**
APO06	妥当管理的预算和成本	1	**3**
APO07	妥当管理的人力资源	1	**2**
APO08	妥当管理的关系	1	**2**
APO09	妥当管理的服务协议	1	**2**
APO10	妥当管理的供应商	1	**2**
APO11	妥当管理的质量	3	**3**
APO12	妥当管理的风险	2	**4**
APO13	妥当管理的安全	4	**4**
APO14	妥当管理的数据	3	**4**
BAI01	妥当管理的计划	1	**3**
BAI02	妥当管理的需求定义	1	**2**

图 7.72—示例 3：治理和管理目标以及目标流程能力级别（续）			
参考编号	治理/管理目标	建议的目标流程能力级别	确定的目标流程能力级别
BAI03	妥当管理的解决方案识别和构建	1	2
BAI04	妥当管理的可用性和容量	3	2
BAI05	妥当管理的组织变更	1	2
BAI06	妥当管理的 IT 变更	2	2
BAI07	妥当管理的 IT 变更接受和交接	1	2
BAI08	妥当管理的知识	1	1
BAI09	妥当管理的资产	2	2
BAI10	妥当管理的配置	2	2
BAI11	妥当管理的项目	1	3
DSS01	妥当管理的运营	1	2
DSS02	妥当管理的服务请求和事故	3	2
DSS03	妥当管理的问题	2	2
DSS04	妥当管理的连续性	3	2
DSS05	妥当管理的安全服务	3	3
DSS06	妥当管理的业务流程控制	2	3
MEA01	妥当管理的绩效和一致性监控	1	2
MEA02	妥当管理的内部控制系统	2	2
MEA03	妥当管理的外部要求合规性	2	2
MEA04	妥当管理的鉴证	2	2

由于对应关系表以及通用目标和情况可能并不总是适合企业的特定环境，所以管理层有权定义不同于（半）自动化方法所建议的目标级别。在**图 7.72** 中，为治理和管理目标建议的目标能力级别和确定的目标级别中，几乎 80% 完全相同或仅变化一级。

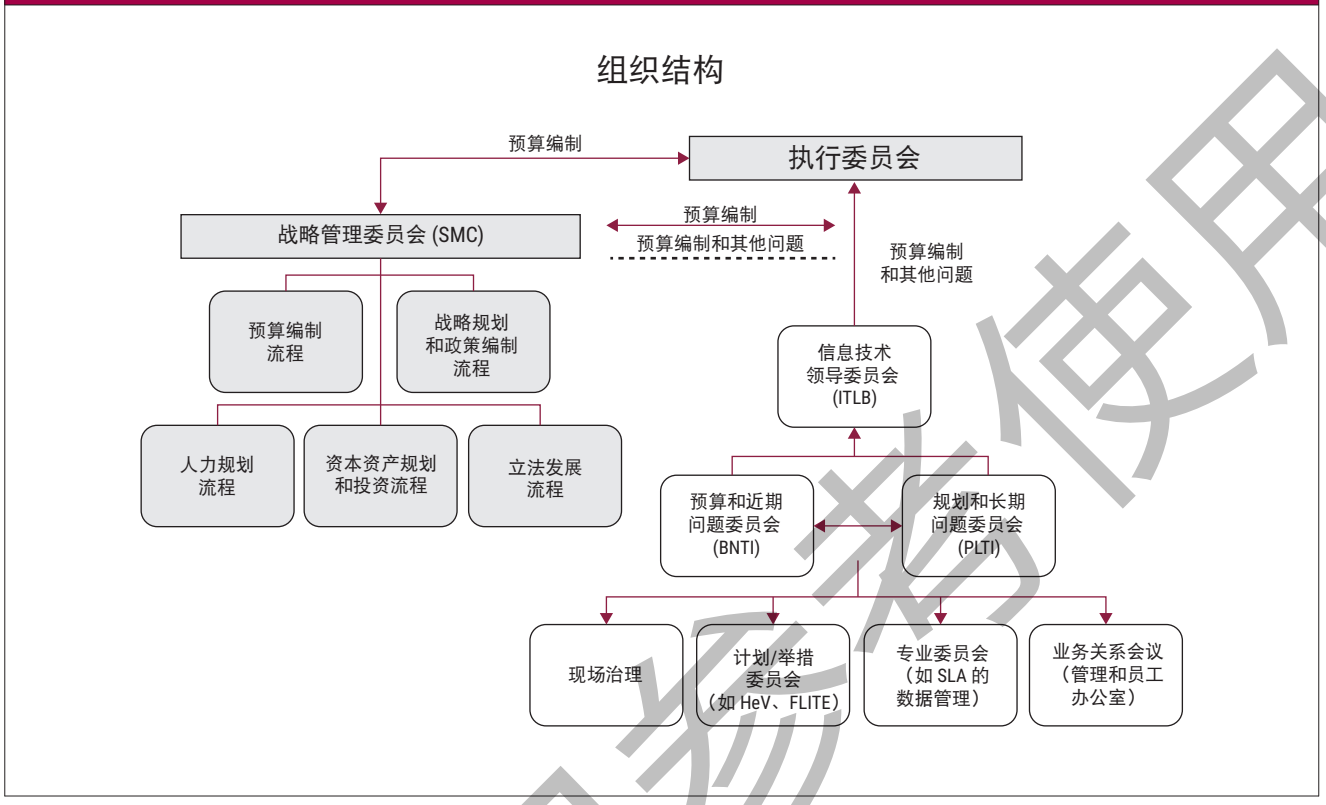
与 IT 成本和预算、计划和项目以及战略有关的治理和管理目标出现的偏差最大。虽然对企业战略、企业目标、风险、I&T 问题和其他设计因素的评估表明治理和管理目标的优先级较低，但管理层还是决定为这些目标指定更高的优先级，以解决该机构的治理问题。

7.4.4.2 其他组件

该机构需要特别注意，应强有力地实施治理系统的下列角色和结构（及其他组件）：

- 该机构将发布一项最高管理层政策，以体现对建立 I&T 治理结构、标准、政策和程序以及实施下列结构和角色的强有力支持。（此备受关注的大型政府机构实施的实际 I&T 治理和组织结构如**图 7.73** 所示。）
- 在组织结构方面，该机构决定实施下列角色：
  - 战略管理委员会
  - IT 领导委员会
  - 预算和短期问题委员会
  - 规划和长期问题委员会
  - 人力规划流程
  - 资本资产规划和投资流程
  - 立法发展流程

图 7.73—示例 3，第 4 步：组织结构



该机构还将确保整个组织拥有足够的风险、安全和隐私意识。

7.4.4.3 具体焦点领域指南

该机构会将下列指南作为核心 COBIT 指南的补充资料：[45]

- 风险焦点领域的内容，考虑到高威胁环境以及风险分析结果和当前的 I&T 问题
- 信息安全焦点领域指南，考虑到高威胁环境以及风险分析结果和当前的 I&T 问题

[45] *《COBIT® 2019 设计指南：信息和技术治理解决方案的设计》*出版时，风险和信息安全焦点领域正在制定中，尚未发布。

本页特意留白

附录

下列附录包含治理和管理目标与第 2.6 节所识别的设计因素之间的对应关系表。

这些对应关系表示设计因素值对治理或管理目标的重要性的影响程度。

这些对应关系使用零 (0) 到四 (4) 分进行评级：4 表示影响最大，0 表示毫无关系。

示例：当企业为 DF2 *企业战略*选择成长战略时，附录 A 对应关系表明管理目标 APO03 *妥当管理的企业架构*将极为重要（值为 4）。

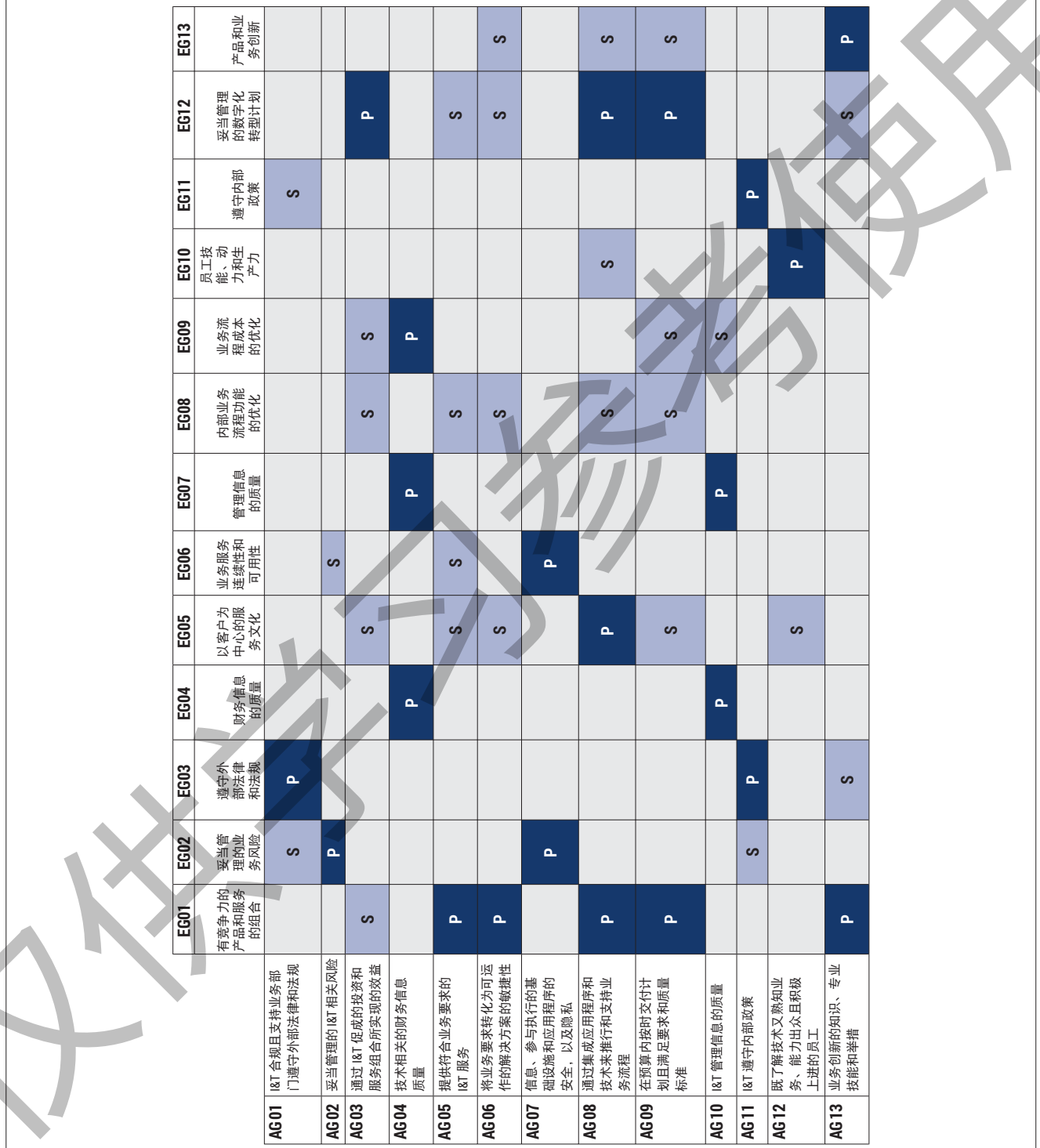
附录 A：对应关系表 — 企业战略与治理和管理目标

图 A.1—企业战略与治理和管理目标的对应关系				
DF1	成长/收购	创新/差异化	成本领导	客户服务/稳定性
EDM01	1.0	1.0	1.5	1.5
EDM02	1.5	1.0	2.0	3.5
EDM03	1.0	1.0	1.0	2.0
EDM04	1.5	1.0	4.0	1.0
EDM05	1.5	1.5	1.0	2.0
APO01	1.0	1.0	1.0	1.0
APO02	3.5	3.5	1.5	1.0
APO03	4.0	2.0	1.0	1.0
APO04	1.0	4.0	1.0	1.0
APO05	3.5	4.0	2.5	1.0
APO06	1.5	1.0	4.0	1.0
APO07	2.0	1.0	1.0	1.0
APO08	1.0	1.5	1.0	3.5
APO09	1.0	1.0	1.5	4.0
APO10	1.0	1.0	3.5	1.5
APO11	1.0	1.0	1.0	4.0
APO12	1.0	1.5	1.0	2.5
APO13	1.0	1.0	1.0	2.5
APO14	1.0	1.0	1.0	1.0
BAI01	4.0	2.0	1.5	1.5
BAI02	1.0	1.0	1.5	1.0
BAI03	1.0	1.0	1.5	1.0
BAI04	1.0	1.0	1.0	3.0
BAI05	4.0	2.0	1.0	1.5
BAI06	2.0	2.0	1.0	1.5
BAI07	1.5	2.0	1.0	1.5
BAI08	1.0	3.5	1.0	1.0
BAI09	1.0	1.0	1.0	1.0
BAI10	1.0	1.0	1.0	1.0
BAI11	3.5	3.0	1.5	1.0
DSS01	1.0	1.0	1.0	1.5
DSS02	1.0	1.0	1.0	4.0

图 A.1—企业战略与治理和管理目标的对应关系（续）				
DF1	成长/收购	创新/差异化	成本领导	客户服务/稳定性
DSS03	1.0	1.0	1.0	3.0
DSS04	1.0	1.0	1.0	4.0
DSS05	1.0	1.0	1.0	2.5
DSS06	1.0	1.0	1.0	1.5
MEA01	1.0	1.0	1.0	1.0
MEA02	1.0	1.0	1.0	1.0
MEA03	1.0	1.0	1.0	1.0
MEA04	1.0	1.0	1.0	1.0

附录 B：对应关系表 — 企业目标与一致性目标

图 A.2—企业目标与一致性目标的对应关系



		EG01	EG02	EG03	EG04	EG05	EG06	EG07	EG08	EG09	EG10	EG11	EG12	EG13
		有竞争力的产品和服务的组合	妥当管理的业务风险	遵守外部法律和法规	财务信息的质量	以客户为中心的服务文化	业务服务连续性和可用性	管理信息的质量	内部业务流程功能的优化	业务流程成本的优化	员工技能、动力和生产力	遵守内部政策	妥当管理的数字化转型计划	产品和业务创新
AG01	I&T 合规且支持业务部门遵守外部法律和法规		S	P								S		
AG02	妥当管理的 I&T 相关风险		P				S							
AG03	通过 I&T 促成的投资和服务组合所实现的效益	S				S			S	S			P	
AG04	技术相关的财务信息质量				P			P		P				
AG05	提供符合业务要求的 I&T 服务	P				S	S						S	
AG06	将业务要求转化为可运作的解决方案的敏捷性	P				S			S				S	S
AG07	信息、参与执行的基础设施和应用程序的安全，以及隐私		P				P							
AG08	通过集成应用程序和技术来推行和支持业务流程	P				P			S		S		P	S
AG09	在预算内按时交付计划且满足要求和质量标准	P				S			S	S			P	S
AG10	I&T 管理信息的质量				P			P		S				
AG11	I&T 遵守内部政策		S	P								P		
AG12	既了解技术又熟知业务、能力出众且积极上进的员工					S					P			
AG13	业务创新的知识、专业技能和举措	P		S									S	P

附录 C：对应关系表 — 一致性目标与治理和管理目标

图 A.3—一致性目标与治理和管理目标的对应关系

		AG01	AG02	AG03	AG04	AG05	AG06	AG07	AG08	AG09	AG10	AG11	AG12	AG13
		I&T 合规且支持业务部门遵守外部法律和法规	妥当管理的 I&T 相关风险	通过 I&T 促成的投资和服务组合所实现的效益	技术相关的财务信息质量	提供符合业务要求的 I&T 服务	将业务要求转化为可运作的解决方案的敏捷性	信息、参与执行的基础设施和应用程序的安全，以及隐私	通过集成应用程序和技术来推行和支持业务流程	在预算内按时交付计划且满足要求和质量标准	I&T 管理信息的质量	I&T 遵守内部政策	既了解技术又熟知业务、能力出众且积极上进的员工	业务创新的知识、专业技能和举措
EDM01	确保治理框架的设置和维护	P	S	P					S			S		
EDM02	确保实现效益			P		S	S		S					S
EDM03	确保风险优化	S	P					P				S		
EDM04	确保资源优化			S		S	S		S	P			S	
EDM05	确保利益相关方参与				S						P	S		
APO01	妥当管理的 I&T 管理框架	S	S	P		S		S	S	S	S	P		
APO02	妥当管理的战略			S		S	S		P				S	S
APO03	妥当管理的企业架构			S		S	P	S	P					
APO04	妥当管理的创新			S			P		S				S	P
APO05	妥当管理的组合			P		P	S		S	S				
APO06	妥当管理的预算和成本			S	P					P	S			
APO07	妥当管理的人力资源			S		S				S			P	P
APO08	妥当管理的关系			S		P	P		S	S			P	P
APO09	妥当管理的服务协议					P			S					
APO10	妥当管理的供应商					P	S			S				
APO11	妥当管理的质量			S	S	S				P	P			
APO12	妥当管理的风险		P					P						
APO13	妥当管理的安全	S	S					P						
APO14	妥当管理的数据	S	S		S			S			P			
BAI01	妥当管理的计划			P			S		S	P				
BAI02	妥当管理的需求定义			S		P	P		S	P			S	
BAI03	妥当管理的解决方案识别和构建			S		P	P		S	P				
BAI04	妥当管理的可用性和容量					P		S		S				
BAI05	妥当管理的组织变更			P		S	S		P	P			S	
BAI06	妥当管理的 IT 变更		S			S	P		S					
BAI07	妥当管理的 IT 变更接受和交接		S				P			S				
BAI08	妥当管理的知识			S			S		S	S			P	P
BAI09	妥当管理的资产				P						S			
BAI10	妥当管理的配置					S		P						
BAI11	妥当管理的项目			P		S	P			P				
DSS01	妥当管理的运营					P			S					
DSS02	妥当管理的服务请求和事故		S			P		S						
DSS03	妥当管理的问题		S			P		S						
DSS04	妥当管理的连续性		S			P		P						
DSS05	妥当管理的安全服务	S	P			S		P				S		
DSS06	妥当管理的业务流程控制		S			S		S	P			S		
MEA01	妥当管理的绩效和一致性监控	S		S		P				S	P	S		
MEA02	妥当管理的内部控制系统	S	S		S	S		S		S	S	P		
MEA03	妥当管理的外部要求合规性	P										S		
MEA04	妥当管理的鉴证	S	S		S	S		S			S	P		

附录 D：对应关系表 —IT 风险与治理和管理目标

图 A.4—IT 风险与治理和管理目标的对应关系

DF3	RISKCAT01 IT 投资决策制定、投资组合定义和维护	RISKCAT02 计划和项目生命周期管理	RISKCAT03 IT 成本和监督	RISKCAT04 IT 专业知识、技能和行为	RISKCAT05 “企业/IT 架构”	RISKCAT06 IT 运营基础设施事故	RISKCAT07 未授权的行动	RISKCAT08 “软件采用/使用问题”	RISKCAT09 硬件事故	RISKCAT10 软件故障
EDM01	3	2	3	0	0	0	2	0	0	0
EDM02	3	2	0	0	2	0	0	0	0	0
EDOM3	2	2	0	0	0	0	0	0	0	1
EDM04	3	0	4	3	2	0	0	0	0	0
EDM05	3	1	3	0	0	0	2	0	0	1
APO01	2	3	2	0	2	2	4	2	0	2
APO02	2	0	0	0	3	0	0	2	1	0
APO03	2	0	0	0	4	0	0	2	0	2
APO04	0	0	0	0	1	0	0	0	0	0
APO05	4	2	2	0	2	0	0	2	2	0
APO06	2	3	4	0	0	0	0	0	0	0
APO07	0	0	0	4	0	2	3	3	0	0
APO08	0	0	0	2	2	0	0	4	0	0
APO09	0	0	2	0	0	0	2	3	0	1
APO10	0	2	3	0	0	0	2	2	3	2
APO11	0	3	0	0	0	0	0	2	0	4
APO12	0	0	0	0	0	0	3	0	0	2
APO13	0	0	0	0	0	0	4	0	0	0
APO14	0	0	0	0	0	0	3	2	0	0
BIA01	0	4	0	0	2	0	0	3	0	0
BAI02	2	2	0	0	2	0	0	3	0	2
BAI03	0	3	0	0	2	0	0	2	0	3
BAI04	0	1	0	0	0	0	0	0	0	0
BAI05	0	2	0	2	0	0	0	4	0	0
BAI06	0	0	0	0	0	3	4	0	0	2
BAI07	0	0	0	0	0	2	3	2	0	4
BAI08	0	0	0	2	0	3	0	3	0	3
BAI09	0	0	0	0	0	1	3	0	0	0
BAI10	0	0	0	0	0	2	4	0	0	2
BAI11	0	4	0	0	0	0	0	0	0	0
DSS01	0	0	0	0	0	4	3	0	4	0
DSS02	0	0	0	0	0	3	2	3	2	2
DSS03	0	0	0	0	0	3	1	4	0	3
DS0S4	0	0	0	0	0	3	3	0	3	0
DSS05	0	0	0	0	0	3	4	0	2	0
DSS06	0	0	0	0	0	3	4	2	0	0
MEA01	1	2	2	0	0	2	2	0	0	2
MEA02	1	2	2	0	0	3	3	0	0	2
MEA03	0	1	0	0	0	1	2	0	0	0
MEA04	1	2	0	0	0	0	3	0	0	2

图 A.4—IT 风险与治理和管理目标的对应关系（*续*）

DF3	RISKCAT11 逻辑攻击（黑客攻击、恶意软件等）	RISKCAT12 “第三方/供应商事故”	RISKCAT13 违规	RISKCAT14 地缘政治问题	RISKCAT15 劳工行动	RISKCAT16 自然灾害	RISKCAT17 基于技术的创新	RISKCAT18 环境	RISKCAT19 数据和信息管理
EDM01	0	0	3	2	0	0	2	2	2
EDM02	0	0	1	0	0	0	3	1	3
ED0M3	2	0	3	3	0	0	0	2	3
EDM04	0	2	1	0	2	0	0	2	3
EDM05	0	1	3	3	0	0	0	2	2
APO01	3	3	3	0	0	0	3	2	3
APO02	1	2	0	0	0	0	2	2	1
APO03	2	2	0	0	0	0	2	0	3
AP0O4	0	0	0	0	0	0	4	0	0
APO05	0	0	0	0	0	0	2	0	0
APO06	0	2	0	2	0	0	2	2	0
APO07	2	0	0	2	4	0	2	2	0
APO08	2	2	0	0	0	0	3	0	2
APO09	2	3	0	0	0	0	0	0	0
APO10	2	4	2	2	0	0	0	0	0
APO11	0	0	0	0	0	0	0	0	2
APO12	3	0	0	0	0	2	0	0	0
APO13	4	0	3	0	0	0	0	0	0
APO14	2	0	3	0	2	4	2	0	4
BIA01	0	0	0	0	0	0	0	0	0
BAI02	2	0	0	0	0	0	0	0	0
BAI03	3	0	0	0	0	0	0	0	0
BAI04	0	0	0	0	0	0	0	0	0
BAI05	0	0	0	0	0	0	0	0	0
BAI06	3	0	0	0	0	0	0	0	3
BAI07	2	0	0	0	0	0	0	0	0
BAI08	0	0	0	0	2	0	0	0	2
BAI09	0	0	0	0	0	0	0	0	0
BAI10	3	0	0	0	0	0	0	0	0
BAI11	0	0	0	0	0	0	0	0	0
DSS01	2	0	0	0	0	0	0	2	0
DSS02	4	0	0	0	0	0	0	0	0
DSS03	1	0	0	0	0	0	0	0	0
DS0S4	4	0	2	0	3	4	0	0	2
DSS05	4	0	3	0	3	2	0	0	3
DSS06	2	0	2	0	0	0	0	0	3
MEA01	3	2	2	2	0	2	0	0	2
MEA02	3	2	2	3	0	2	0	0	2
MEA03	3	2	4	2	0	0	0	0	2
MEA04	3	2	2	4	0	2	2	0	2

附录 E：对应关系表 — I&T 相关问题与治理和管理目标

图 A.5—I&T 相关问题与治理和管理目标的对应关系

DF4	由于被认为对业务价值的实现没有起到应有的作用，整个组织的挫败感不断增加	由于举措失败或被认为对业务价值的贡献极低，业务部门（用户）和 IT 部门受挫	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	IT 外包商的服务交付问题	不符合 IT 相关法规或合同要求	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	重大的隐性前后不一的 IT 支出，即用户部门在正常的行投资决策机制范围之外的 I&T 支出	多个举措之间的重复或重叠、或其他形式的资源浪费	IT 资源不足、员工技能欠缺员工倦怠/不满	IT 促成的变革或项目经常无法满足业务对成超过预算
EDM01	3.0	3.0	1.0	1.0	2.0	2.0	2.0	1.0	1.0	1.0
EDM02	2.5	3.0	1.0	1.0	1.5	2.5	2.0	1.5	0.5	2.5
EDM03	1.0	1.0	2.0	1.0	2.0	2.0	1.0	1.0	0.0	0.5
EDM04	1.0	1.0	1.0	1.0	1.0	2.0	3.0	3.5	3.5	1.0
EDM05	1.0	1.0	1.0	1.0	1.5	2.0	1.0	1.0	0.0	1.0
AP001	2.0	1.0	2.0	1.0	2.0	2.0	1.0	1.0	0.0	0.5
AP002	1.5	1.5	1.5	1.5	1.0	1.5	1.0	1.0	0.0	1.0
AP003	1.0	1.5	1.0	2.0	0.5	1.5	2.0	1.5	1.0	3.5
AP004	1.0	1.0	1.0	1.0	0.5	0.5	0.5	0.5	0.0	0.0
AP005	3.0	3.0	1.0	1.5	2.0	2.0	1.5	3.5	0.5	2.0
AP006	3.5	2.0	1.0	1.5	1.5	2.0	4.0	3.0	1.0	2.0
AP007	1.5	1.0	1.0	1.0	1.0	1.5	2.0	2.0	4.0	1.0
AP008	2.5	2.0	1.0	2.5	1.5	1.0	2.5	2.0	1.5	1.0
AP009	2.0	1.5	2.0	4.0	1.0	2.5	1.5	2.0	0.5	1.0
AP010	1.0	1.0	2.0	4.0	1.5	1.5	1.5	0.0	1.5	1.0
AP011	1.0	1.0	3.0	1.5	1.0	3.0	0.0	0.0	0.0	2.0
AP012	1.0	0.5	2.5	1.5	2.0	2.0	1.0	1.0	0.5	1.0
AP013	0.0	0.0	3.5	1.0	2.0	1.0	0.0	1.0	0.0	0.5
AP014	1.0	1.5	3.0	1.0	2.5	1.5	1.0	1.5	0.0	1.5
BAI01	0.0	1.0	1.5	0.0	0.0	0.0	0.0	3.0	1.0	3.5
BAI02	0.0	3.0	0.0	0.0	0.5	2.0	0.0	2.0	0.0	3.5
BAI03	1.0	2.0	2.0	0.0	0.0	2.0	0.0	1.0	0.0	3.0
BAI04	0.5	0.0	2.0	3.0	0.0	2.0	0.0	0.0	0.0	0.0
BAI05	1.0	3.0	0.0	0.0	0.0	0.0	0.0	0.5	0.0	3.0
BAI06	0.0	0.0	2.5	3.0	0.5	1.5	0.0	1.0	0.0	1.5
BAI07	0.0	1.0	2.0	2.0	0.5	1.5	0.0	0.5	0.0	2.0
BAI08	0.0	0.0	0.0	1.5	0.5	0.5	0.0	1.0	2.0	0.5
BAI09	0.5	0.5	1.0	0.0	0.0	0.0	2.0	2.0	0.0	0.0
BAI10	0.0	0.0	2.5	2.0	0.5	0.0	0.0	0.5	0.0	0.0
BAI11	1.0	2.0	2.5	0.0	0.0	0.0	2.0	3.0	1.0	4.0
DSS01	0.0	0.0	2.5	2.0	1.0	2.0	0.0	0.5	0.0	0.0
DSS02	1.0	1.0	4.0	3.0	1.0	2.5	0.0	0.0	0.0	0.0
DSS03	0.0	1.0	3.0	3.0	0.0	3.0	0.0	0.0	0.0	0.0
DSS04	0.0	0.0	3.0	1.0	2.0	0.0	0.0	0.0	0.0	0.0
DSS05	0.0	0.0	4.0	2.0	2.0	0.0	0.0	0.0	0.0	0.0
DSS06	0.0	1.0	0.5	0.0	3.0	0.5	0.0	0.0	0.0	1.0
MEA01	1.0	1.5	2.0	2.0	2.5	3.0	1.0	2.0	1.5	1.0
MEA02	0.0	0.0	2.0	2.0	2.5	2.0	2.0	0.0	0.5	2.0
MEA03	0.0	0.0	2.0	2.0	4.0	0.5	0.0	0.0	0.0	0.0
MEA04	1.0	1.0	3.0	1.5	3.0	4.0	2.0	1.0	1.0	0.5

图 A.5—I&T 相关问题与治理和管理目标的对应关系 （续）

DF4	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	复杂的 IT 运营模式和/或缺乏明确的 IT 相关决策机制	过高的 IT 成本	当前 IT 架构和系统导致新举措或创新的实施受阻或失败	业务和技术知识之间的鸿沟导致业务用户与信息和/或技术专家难以交流	各种来源的数据经常出现数据质量和整合方面的问题	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、质量控制以及其他问题	业务部门在企业 IT 部门极少或者根本没有参与的情况下实施自己的信息解决方案	忽视和/或违反隐私法规	无法利用新技术或使用 I&T 进行创新
EDM01	3.0	3.5	1.0	1.0	1.0	1.0	2.0	3.0	1.5	1.0
EDM02	1.5	1.0	3.0	2.0	1.0	1.0	2.0	2.0	1.0	2.5
EDM03	1.0	0.0	1.0	1.5	1.0	2.0	1.0	1.0	2.5	1.0
EDM04	1.5	0.0	4.0	2.0	1.0	1.5	2.0	2.5	0.0	1.0
EDM05	3.0	1.5	1.5	0.5	0.0	0.5	1.0	1.0	1.0	0.0
APO01	1.5	4.0	1.0	2.0	1.0	1.0	1.5	2.0	0.5	1.0
APO02	2.5	0.5	0.5	1.5	1.5	0.5	2.0	2.0	0.0	2.5
APO03	0.5	0.5	1.0	4.0	1.0	3.5	2.0	3.0	0.0	2.0
APO04	0.5	1.0	0.5	2.0	1.0	0.0	0.5	0.5	0.0	4.0
APO05	2.0	1.5	2.0	1.0	0.5	0.0	2.5	2.5	0.0	2.0
APO06	1.0	1.5	4.0	0.0	0.0	0.0	1.0	2.0	0.0	0.0
APO07	0.0	0.0	1.0	0.0	3.0	0.0	0.5	0.5	1.5	1.0
APO08	3.0	1.0	0.5	1.0	4.0	1.0	3.0	3.5	0.0	0.5
APO09	0.0	0.0	1.0	0.0	0.0	0.0	1.0	1.5	0.0	0.0
APO10	0.0	0.0	1.0	0.0	0.0	0.0	0.5	2.0	1.0	0.0
APO11	0.0	0.0	0.0	0.5	0.5	3.0	2.0	2.0	0.0	1.0
APO12	1.0	1.0	1.0	1.0	1.0	2.0	1.0	1.5	2.5	1.0
APO13	0.0	0.0	0.0	0.0	0.0	1.5	2.0	1.0	2.0	1.0
APO14	0.0	0.0	0.5	2.5	0.5	4.0	2.5	2.0	3.0	0.5
BAI01	0.0	0.0	1.5	0.5	1.0	0.0	1.5	2.0	0.0	1.0
BAI02	0.0	1.0	1.0	2.0	2.0	1.5	2.5	3.0	0.5	1.0
BAI03	0.0	0.5	1.0	1.0	1.0	0.5	2.0	2.0	1.0	0.5
BAI04	0.0	0.0	0.5	0.0	0.0	1.0	1.0	1.0	0.0	0.5
BAI05	1.0	0.0	0.0	0.5	2.0	0.0	0.5	1.5	0.0	1.0
BAI06	0.0	1.0	0.5	1.0	0.5	2.0	2.0	2.0	1.0	1.0
BAI07	0.0	1.0	0.0	1.0	0.5	2.0	2.0	2.0	0.0	1.0
BAI08	0.0	0.5	0.0	1.0	3.0	2.0	1.0	1.5	0.0	0.5
BAI09	0.0	0.0	2.0	1.0	0.0	0.0	1.0	1.5	0.0	0.0
BAI10	0.0	0.0	1.0	1.5	0.0	1.5	1.0	2.0	0.0	0.0
BAI11	0.0	0.0	1.5	2.0	0.5	0.0	1.0	1.5	0.0	0.5
DSS01	0.0	0.0	1.0	0.0	0.0	1.5	1.0	2.0	0.0	0.0
DSS02	0.0	0.0	1.0	0.0	0.0	1.0	1.0	1.0	0.0	0.0
DSS03	0.0	0.0	0.0	1.0	1.5	1.0	1.0	1.0	0.5	0.0
DSS04	0.0	0.0	0.0	0.0	0.0	1.5	1.0	2.0	0.0	0.0
DSS05	0.0	0.0	0.0	0.0	0.0	1.5	1.0	2.0	2.0	0.0
DSS06	0.0	0.0	0.0	0.0	1.5	2.5	1.5	1.0	2.0	0.0
MEA01	1.0	1.0	2.0	1.0	1.0	1.0	1.5	1.0	2.5	1.0
MEA02	1.0	1.0	1.5	1.0	0.0	2.0	1.0	1.0	2.5	0.0
MEA03	0.0	0.0	0.0	0.0	0.0	2.0	0.0	0.0	4.0	0.0
MEA04	1.0	1.0	1.5	0.0	1.0	1.0	1.0	1.0	2.5	1.0

附录 F：对应关系表 — 威胁环境与治理和管理目标

图 A.6—威胁环境与治理和管理目标的对应关系		
DF5	高	正常
EDM01	3.0	1.0
EDM02	1.0	1.0
EDM03	4.0	1.0
EDM04	1.0	1.0
EDM05	2.0	1.0
APO01	3.0	1.0
APO02	1.0	1.0
APO03	3.0	1.0
APO04	1.0	1.0
APO05	1.0	1.0
APO06	1.0	1.0
APO07	2.0	1.0
APO08	1.0	1.0
APO09	2.0	1.0
APO10	3.0	1.0
APO11	2.0	1.0
APO12	4.0	1.0
APO13	4.0	1.0
APO14	3.0	1.0
BAI01	1.0	1.0
BAI02	1.0	1.0
BAI03	1.0	1.0
BAI04	2.0	1.0
BAI05	1.0	1.0
BAI06	3.0	1.0
BAI07	1.0	1.0
BAI08	1.0	1.0
BAI09	1.0	1.0
BAI10	3.0	1.0
BAI11	1.0	1.0
DSS01	1.0	1.0
DSS02	3.0	1.0
DSS03	2.0	1.0
DSS04	4.0	1.0
DSS05	3.0	1.0
DSS06	3.0	1.0
MEA01	3.0	1.0
MEA02	2.0	1.0
MEA03	3.0	1.0
MEA04	3.0	1.0

附录 G：对应关系表 — 合规性要求与治理和管理目标

图 A.7—合规性要求与治理和管理目标的对应关系			
DF6	高	正常	低
EDM01	3.0	2.0	1.0
EDM02	1.0	1.0	1.0
EDM03	4.0	2.0	1.0
EDM04	1.0	1.0	1.0
EDM05	1.5	1.0	1.0
APO01	2.0	1.5	1.0
APO02	1.0	1.0	1.0
APO03	1.0	1.0	1.0
APO04	1.0	1.0	1.0
APO05	1.0	1.0	1.0
APO06	1.0	1.0	1.0
APO07	1.0	1.0	1.0
APO08	1.0	1.0	1.0
APO09	1.0	1.0	1.0
APO10	1.5	1.0	1.0
APO11	1.0	1.0	1.0
APO12	4.0	2.0	1.0
APO13	1.5	1.0	1.0
APO14	2.0	1.5	1.0
BAI01	1.0	1.0	1.0
BAI02	1.0	1.0	1.0
BAI03	1.0	1.0	1.0
BAI04	1.0	1.0	1.0
BAI05	1.0	1.0	1.0
BAI06	1.0	1.0	1.0
BAI07	1.0	1.0	1.0
BAI08	1.0	1.0	1.0
BAI09	1.0	1.0	1.0
BAI10	1.0	1.0	1.0
BAI11	1.0	1.0	1.0
DSS01	1.0	1.0	1.0
DSS02	1.0	1.0	1.0
DSS03	1.0	1.0	1.0
DSS04	1.5	1.0	1.0
DSS05	2.0	1.0	1.0
DSS06	1.0	1.0	1.0
MEA01	1.0	1.0	1.0
MEA02	1.0	1.0	1.0
MEA03	4.0	2.0	1.0
MEA04	3.5	2.0	1.0

附录 H：对应关系表 — IT 角色与治理和管理目标

图 A.8—IT 角色与治理和管理目标的对应关系				
DF7	支持	工厂	整顿	战略
EDM01	1.0	2.0	1.5	4.0
EDM02	1.0	1.0	2.5	3.0
EDM03	1.0	3.0	1.0	3.0
EDM04	1.0	1.0	1.0	2.0
EDM05	1.0	1.0	1.0	2.0
APO01	1.0	1.5	1.5	2.5
APO02	1.0	1.0	3.0	3.0
APO03	1.0	1.0	2.0	2.0
APO04	0.5	1.0	3.5	4.0
APO05	1.0	1.0	2.5	3.0
APO06	1.0	1.0	1.0	2.0
APO07	1.0	1.0	1.0	1.5
APO08	1.0	1.0	2.0	2.5
APO09	1.0	2.0	1.5	2.0
APO10	1.0	2.5	1.5	2.0
APO11	1.0	1.5	1.5	2.0
APO12	1.0	2.5	1.0	3.0
APO13	1.0	2.0	1.5	3.0
APO14	1.0	1.5	1.5	2.5
BAI01	1.0	1.0	2.0	2.5
BAI02	1.0	1.0	3.0	3.0
BAI03	1.0	1.0	3.0	3.0
BAI04	1.0	2.5	1.5	2.0
BAI05	1.0	1.0	1.0	2.0
BAI06	1.0	2.5	1.0	2.0
BAI07	1.0	1.0	2.0	2.0
BAI08	1.0	1.0	1.0	2.0
BAI09	1.0	1.0	1.0	2.0
BAI10	1.0	1.5	1.0	2.0
BAI11	1.0	1.0	2.0	2.0
DSS01	1.0	3.5	1.0	3.0
DSS02	1.0	3.0	1.5	3.0
DSS03	1.0	3.0	1.5	3.5
DSS04	1.0	3.0	1.5	3.5
DSS05	1.5	2.5	1.5	3.5
DSS06	1.0	1.0	1.0	2.5
MEA01	1.0	1.0	1.0	2.0
MEA02	1.0	1.0	1.0	2.0
MEA03	1.0	1.0	1.0	1.5
MEA04	1.0	1.0	1.0	2.0

附录 I：对应关系表 — IT 采购模式与治理和管理目标

图 A.9—IT 采购模式与治理和管理目标的对应关系			
DF8	外包	云	内包
EDM01	1.0	1.0	1.0
EDM02	1.0	1.0	1.0
EDM03	1.0	2.0	1.0
EDM04	1.0	1.0	1.0
EDM05	1.0	1.0	1.0
APO01	1.0	1.0	1.0
APO02	1.0	1.0	1.0
APO03	1.0	1.0	1.0
APO04	1.0	1.0	1.0
APO05	1.0	1.0	1.0
APO06	1.0	1.0	1.0
APO07	1.0	1.0	1.0
APO08	1.0	1.0	1.0
APO09	4.0	4.0	1.0
APO10	4.0	4.0	1.0
APO11	1.0	1.0	1.0
APO12	2.0	2.0	1.0
APO13	1.0	1.0	1.0
APO14	1.0	1.0	1.0
BAI01	1.0	1.0	1.0
BAI02	1.0	1.0	1.0
BAI03	1.0	1.0	1.0
BAI04	1.0	1.0	1.0
BAI05	1.0	1.0	1.0
BAI06	1.0	1.0	1.0
BAI07	1.0	1.0	1.0
BAI08	1.0	1.0	1.0
BAI09	1.0	1.0	1.0
BAI10	1.0	1.0	1.0
BAI11	1.0	1.0	1.0
DSS01	1.0	1.0	1.0
DSS02	1.0	1.0	1.0
DSS03	1.0	1.0	1.0
DSS04	1.0	1.0	1.0
DSS05	1.0	1.0	1.0
DSS06	1.0	1.0	1.0
MEA01	3.0	3.0	1.0
MEA02	1.0	1.0	1.0
MEA03	1.0	1.0	1.0
MEA04	1.0	1.0	1.0

附录 J：对应关系表 — IT 实施方法与治理和管理目标

图 A.10—IT 实施方法与治理和管理目标的对应关系			
DF9	敏捷	DevOps	传统
EDM01	1.0	1.0	1.0
EDM02	1.0	1.0	1.0
EDM03	1.0	1.0	1.0
EDM04	1.0	1.0	1.0
EDM05	1.0	1.0	1.0
APO01	1.0	1.0	1.0
APO02	1.0	1.0	1.0
APO03	1.0	2.0	1.0
APO04	1.0	1.0	1.0
APO05	1.0	1.0	1.0
APO06	1.0	1.0	1.0
APO07	1.0	1.5	1.0
APO08	1.0	1.0	1.0
APO09	1.0	1.0	1.0
APO10	1.0	1.0	1.0
APO11	1.0	1.0	1.0
APO12	1.0	1.5	1.0
APO13	1.0	1.0	1.0
APO14	1.0	1.0	1.0
BAI01	2.0	1.5	1.0
BAI02	3.5	2.0	1.0
BAI03	4.0	3.0	1.0
BAI04	1.0	1.0	1.0
BAI05	2.5	1.5	1.0
BAI06	3.5	2.0	1.0
BAI07	2.5	2.5	1.0
BAI08	1.0	1.0	1.0
BAI09	1.0	1.0	1.0
BAI10	1.5	2.0	1.0
BAI11	2.5	1.0	1.0
DSS01	1.0	2.5	1.0
DSS02	1.0	1.5	1.0
DSS03	1.0	1.5	1.0
DSS04	1.0	1.0	1.0
DSS05	1.0	1.0	1.0
DSS06	1.0	1.0	1.0
MEA01	1.5	1.5	1.0
MEA02	1.0	1.0	1.0
MEA03	1.0	1.0	1.0
MEA04	1.0	1.0	1.0

附录 K：关系对应表 — 技术采用战略与治理和管理目标

图 A.11—技术采用战略与治理和管理目标的对应关系			
DF10	先行者	追随者	滞后者
EDM01	3.5	2.5	1.5
EDM02	4.0	2.5	1.5
EDM03	1.5	1.0	1.0
EDM04	2.5	2.0	1.5
EDM05	1.5	1.0	1.0
APO01	2.5	1.5	1.0
APO02	4.0	3.0	1.5
APO03	2.0	1.0	1.0
APO04	4.0	3.0	1.0
APO05	4.0	2.5	1.0
APO06	1.0	1.5	1.0
APO07	2.5	1.0	1.0
APO08	3.0	1.5	1.0
APO09	1.5	1.5	1.0
APO10	2.5	1.5	1.0
APO11	1.5	1.5	1.0
APO12	2.0	1.5	1.0
APO13	1.0	1.0	1.0
APO14	2.5	2.0	1.0
BAI01	4.0	3.0	1.5
BAI02	3.5	2.5	1.0
BAI03	4.0	2.5	1.0
BAI04	1.5	1.5	1.0
BAI05	3.0	2.0	1.0
BAI06	2.5	2.0	1.0
BAI07	3.5	2.5	1.0
BAI08	1.5	1.0	1.0
BAI09	1.0	1.0	1.0
BAI10	1.5	1.0	1.0
BAI11	3.5	2.5	1.0
DSS01	1.0	1.0	1.0
DSS02	1.0	1.0	1.0
DSS03	1.5	1.0	1.0
DSS04	1.5	1.0	1.0
DSS05	1.5	1.0	1.0
DSS06	1.0	1.0	1.0
MEA01	3.0	2.0	1.0
MEA02	1.0	1.0	1.0
MEA03	1.0	1.0	1.0
MEA04	1.0	1.0	1.0