ISACA®
Trust in, and value from, information systems

COBIT®

企业 IT 治理和管理之业务框架

COBIT® 5

AN ISACA® FRAMEWORK

ISACA® 国际信息系统审计协会

国际信息系统审计协会（ISACA®，网址：*www.isaca.org*）是全球公认提供信息系统（IS）鉴证及安全、企业IT 治理与管理，以及 IT 相关风险与合规性之知识、认证、社群、倡导与教育训练的领导组织，会员遍布逾180 个国家，总数超过 100,000 人。ISACA® 成立于 1969 年，是一个非盈利性的独立组织。除了主办国际会议，出版《国际信息系统审计期刊》（*ISACA® Journal*），并制定国际公认的 IS 审计与控制标准，以协助其成员缔造一个信赖可靠，优值的信息系统。同时，为促进与证明个人的 IT 技能及知识，ISACA 还推出了一系列全球公认的专业认证，如：注册信息系统审计师（Certified Information Systems Auditor®, CISA®）、注册信息安全经理（Certified Information Security Manager®, CISM®）、企业信息科技治理认证（Certified in the Governance of Enterprise IT®, CGEIT®）及风险及信息系统监控认证（Certified in Risk and Information Systems Control™, CRISC™）。ISACA 致力于持续更新及扩展根据 COBIT® 框架推出的实务指南和产品系列。COBIT 能协助 IT 专业人员和企业领袖履行其在 IT 治理和管理方面的职责，特别是在鉴证、安全、风险与控制等范畴，使业务价值得以提升。

Quality Statement 质量声明：

This Work is translated into Chinese Simplified from English language version of COBIT® 5 by the ISACA® China/Hong Kong Chapter with the permission of ISACA®. The ISACA® China/Hong Kong Chapter assumes sole responsibility for the accuracy and faithfulness of the translation.

《COBIT® 5》（本著作）经国际信息系统审计协会（ISACA®）许可，ISACA® 中国/香港分会根据其英文版翻译成简体中文，ISACA® 中国/香港分会对翻译文本的准确性和忠实性承担唯一责任。

Disclaimer 免责声明

ISACA has designed this publication, COBIT® 5 (the 'Work'), primarily as an educational resource for governance of enterprise IT (GEIT), assurance, risk and security professionals. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, readers should apply their own professional judgement to the specific GEIT, assurance, risk and security circumstances presented by the particular systems or information technology environment.

国际信息系统审计协会（ISACA®）创建的《COBIT® 5》（著作）主要作为企业 IT 治理（GEIT）、鉴证、风险及安全专业人员的教育资源。国际信息系统审计协会（ISACA®）不承诺使用该著作内容能确保取得成果。该著作并非囊括所有适用的信息、流程和测试，不排除在其它信息、流程或测试的合理指导下获得同样结果的可能。读者应该根据具体的系统和信息技术环境所体现的企业 IT 治理、鉴证、风险与安全状况，通过自身的专业判断来决定采用适当的信息、流程或测试。

ISACA

3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
电话：+1.847.253.1545
传真：+1.847.253.1443
电子邮箱：*info@isaca.org*
网址：*www.isaca.org*

反馈：*www.isaca.org/cobit*
参加使用 ISACA 知识总汇：*www.isaca.org/knowledge-center*
在 Twitter 上关注 ISACA：*https://twitter.com/ISACANews*
在 Twitter 中加入 COBIT 聊天组：#COBIT
在 LinkedIn 加入 ISACA：ISACA（官方），*http://linkd.in/ISACAOfficial*
在 Facebook 上喜欢 ISACA：*www.facebook.com/ISACAHQ*

COBIT® 5
ISBN 978-1-60420-242-7
美利坚合众国印刷

鸣谢

ISACA 希望表彰：

COBIT 5 工作组（2009–2011）
John W. Lainhart, IV, CISA, CISM, CGEIT, IBM Global Business Services, USA, Co-chair
Derek J. Oliver, Ph.D., DBA, CISA, CISM, CRISC, CITP, FBCS, FISM, MInstISP,
Ravenswood Consultants Ltd., UK, Co-chair
Pippa G. Andrews, CISA, ACA, CIA, KPMG, Australia
Elisabeth Judit Antonsson, CISM, Nordea Bank, Sweden
Steven A. Babb, CGEIT, CRISC, Betfair, UK
Steven De Haes, Ph.D., University of Antwerp Management School, Belgium
Peter Harrison, CGEIT, FCPA, IBM Australia Ltd., Australia
Jimmy Heschl, CISA, CISM, CGEIT, ITIL Expert, bwin.party digital entertainment plc, Austria
Robert D. Johnson, CISA, CISM, CGEIT, CRISC, CISSP, Bank of America, USA
Erik H.J.M. Pols, CISA, CISM, Shell International-ITCI, The Netherlands
Vernon Richard Poole, CISM, CGEIT, Sapphire, UK
Abdul Rafeq, CISA, CGEIT, CIA, FCA, A. Rafeq and Associates, India

开发团队
Floris Ampe, CISA, CGEIT, CIA, ISO 27000, PwC, Belgium
Gert du Preez, CGEIT, PwC, Canada
Stefanie Grijp, PwC, Belgium
Gary Hardy, CGEIT, IT Winners, South Africa
Bart Peeters, PwC, Belgium
Geert Poels, Ghent University, Belgium
Dirk Steuperaert, CISA, CGEIT, CRISC, IT In Balance BVBA, Belgium

研讨参与人员
Gary Baker, CGEIT, CA, Canada
Brian Barnier, CGEIT, CRISC, ValueBridge Advisors, USA
Johannes Hendrik Botha, MBCS-CITP, FSM, getITright Skills Development, South Africa
Ken Buechler, CGEIT, CRISC, PMP, Great-West Life, Canada
Don Caniglia, CISA, CISM, CGEIT, FLMI, USA
Mark Chaplin, UK
Roger Debreceny, Ph.D., CGEIT, FCPA, University of Hawaii at Manoa, USA
Mike Donahue, CISA, CISM, CGEIT, CFE, CGFM, CICA, Towson University, USA
Urs Fischer, CISA, CRISC, CPA (Swiss), Fischer IT GRC Consulting & Training, Switzerland
Bob Frelinger, CISA, CGEIT, Oracle Corporation, USA
James Golden, CISM, CGEIT, CRISC, CISSP, IBM, USA
Meenu Gupta, CISA, CISM, CBP, CIPP, CISSP, Mittal Technologies, USA
Gary Langham, CISA, CISM, CGEIT, CISSP, CPFA, Australia
Nicole Lanza, CGEIT, IBM, USA
Philip Le Grand, PRINCE2, Ideagen Plc, UK
Debra Mallette, CISA, CGEIT, CSSBB, Kaiser Permanente IT, USA
Stuart MacGregor, Real IRM Solutions (Pty) Ltd., South Africa
Christian Nissen, CISM, CGEIT, FSM, CFN People, Denmark
Jamie Pasfield, ITIL V3, MSP, PRINCE2, Pfizer, UK
Eddy J. Schuermans, CGEIT, ESRAS bvba, Belgium
Michael Semrau, RWE Germany, Germany
Max Shanahan, CISA, CGEIT, FCPA, Max Shanahan & Associates, Australia
Alan Simmonds, TOGAF9, TCSA, PreterLex, UK
Cathie Skoog, CISM, CGEIT, CRISC, IBM, USA
Dejan Slokar, CISA, CGEIT, CISSP, Deloitte & Touche LLP, Canada
Roger Southgate, CISA, CISM, UK
Nicky Tiesenga, CISA, CISM, CGEIT, CRISC, IBM, USA
Wim Van Grembergen, Ph.D., University of Antwerp Management School, Belgium
Greet Volders, CGEIT, Voquals N.V., Belgium
Christopher Wilken, CISA, CGEIT, PwC, USA
Tim M. Wright, CISA, CRISC, CBCI, GSEC, QSA, Kingston Smith Consulting LLP, UK

鸣谢（续）

专家审核人员

Mark Adler, CISA, CISM, CGEIT, CRISC, Commercial Metals Company, USA
Wole Akpose, Ph.D., CGEIT, CISSP, Morgan State University, USA
Krzysztof Baczkiewicz, CSAM, CSOX, Eracent, Poland
Roland Bah, CISA, MTN Cameroon, Cameroon
Dave Barnett, CISSP, CSSLP, USA
Max Blecher, CGEIT, Virtual Alliance, South Africa
Ricardo Bria, CISA, CGEIT, CRISC, Meycor GRC, Argentina
Dirk Bruyndonckx, CISA, CISM, CGEIT, CRISC, MCA, KPMG Advisory, Belgium
Donna Cardall, UK
Debra Chiplin, Investors Group, Canada
Sara Cosentino, CA, Great-West Life, Canada
Kamal N. Dave, CISA, CISM, CGEIT, Hewlett Packard, USA
Philip de Picker, CISA, MCA, National Bank of Belgium, Belgium
Abe Deleon, CISA, IBM, USA
Stephen Doyle, CISA, CGEIT, Department of Human Services, Australia
Heidi L. Erchinger, CISA, CRISC, CISSP, System Security Solutions, Inc., USA
Rafael Fabius, CISA, CRISC, Uruguay
Urs Fischer, CISA, CRISC, CPA (Swiss), Fischer IT GRC Consulting & Training, Switzerland
Bob Frelinger, CISA, CGEIT, Oracle Corporation, USA
Yalcin Gerek, CISA, CGEIT, CRISC, ITIL Expert, ITIL V3 Trainer, PRINCE2, ISO/IEC 20000 Consultant, Turkey
Edson Gin, CISA, CISM, CFE, CIPP, SSCP, USA
James Golden, CISM, CGEIT, CRISC, CISSP, IBM, USA
Marcelo Hector Gonzalez, CISA, CRISC, Banco Central Republic Argentina, Argentina
Erik Guldentops, University of Antwerp Management School, Belgium
Meenu Gupta, CISA, CISM, CBP, CIPP, CISSP, Mittal Technologies, USA
Angelica Haverblad, CGEIT, CRISC, ITIL, Verizon Business, Sweden
Kim Haverblad, CISM, CRISC, PCI QSA, Verizon Business, Sweden
J. Winston Hayden, CISA, CISM, CGEIT, CRISC, South Africa
Eduardo Hernandez, ITIL V3, HEME Consultores, Mexico
Jorge Hidalgo, CISA, CISM, CGEIT, ATC, Lic. Sistemas, Argentina
Michelle Hoben, Media 24, South Africa
Linda Horosko, Great-West Life, Canada
Mike Hughes, CISA, CGEIT, CRISC, 123 Consultants, UK
Grant Irvine, Great-West Life, Canada
Monica Jain, CGEIT, CSQA, CSSBB, Southern California Edison, USA
John E. Jasinski, CISA, CGEIT, SSBB, ITIL Expert, USA
Masatoshi Kajimoto, CISA, CRISC, Japan
Joanna Karczewska, CISA, Poland
Kamal Khan, CISA, CISSP, CITP, Saudi Aramco, Saudi Arabia
Eddy Khoo S. K., Prudential Services Asia, Malaysia
Marty King, CISA, CGEIT, CPA, Blue Cross Blue Shield NC, USA
Alan S. Koch, ITIL Expert, PMP, ASK Process Inc., USA
Gary Langham, CISA, CISM, CGEIT, CISSP, CPFA, Australia
Jason D. Lannen, CISA, CISM, TurnKey IT Solutions, LLC, USA
Nicole Lanza, CGEIT, IBM, USA
Philip Le Grand, PRINCE2, Ideagen Plc, UK
Kenny Lee, CISA, CISM, CISSP, Bank of America, USA
Brian Lind, CISA, CISM, CRISC, Topdanmark Forsikring A/S, Denmark
Bjarne Lonberg, CISSP, ITIL, A.P. Moller - Maersk, Denmark
Stuart MacGregor, Real IRM Solutions (Pty) Ltd., South Africa
Debra Mallette, CISA, CGEIT, CSSBB, Kaiser Permanente IT, USA
Charles Mansour, CISA, Charles Mansour Audit & Risk Service, UK
Cindy Marcello, CISA, CPA, FLMI, Great-West Life & Annuity, USA
Nancy McCuaig, CISSP, Great-West Life, Canada
John A. Mitchell, Ph.D., CISA, CGEIT, CEng, CFE, CITP, FBCS, FCIIA, QiCA, LHS Business Control, UK
Makoto Miyazaki, CISA, CPA, Bank of Tokyo-Mitsubishi, UFJ Ltd., Japan

鸣谢（续）

专家审核人员（续）
Lucio Augusto Molina Focazzio, CISA, CISM, CRISC, ITIL, Independent Consultant, Colombia
Christian Nissen, CISM, CGEIT, FSM, ITIL Expert, CFN People, Denmark
Tony Noblett, CISA, CISM, CGEIT, CISSP, USA
Ernest Pages, CISA, CGEIT, MCSE, ITIL, Sciens Consulting LLC, USA
Jamie Pasfield, ITIL V3, MSP, PRINCE2, Pfizer, UK
Tom Patterson, CISA, CGEIT, CRISC, CPA, IBM, USA
Robert Payne, CGEIT, MBL, MCSSA, PrM, Lode Star Strategy Consulting, South Africa
Andy Piper, CISA, CISM, CRISC, PRINCE2, ITIL, Barclays Bank Plc, UK
Andre Pitkowski, CGEIT, CRISC, OCTAVE, ISO27000LA, ISO31000LA, APIT Consultoria de Informatica Ltd., Brazil
Dirk Reimers, Hewlett-Packard, Germany
Steve Reznik, CISA, ADP, Inc., USA
Robert Riley, CISSP, University of Notre Dame, USA
Martin Rosenberg, Ph.D., Cloud Governance Ltd., UK
Claus Rosenquist, CISA, CISSP, Nets Holding, Denmark
Jeffrey Roth, CISA, CGEIT, CISSP, L-3 Communications, USA
Cheryl Santor, CISSP, CNA, CNE, Metropolitan Water District, USA
Eddy J. Schuermans, CGEIT, ESRAS bvba, Belgium
Michael Semrau, RWE Germany, Germany
Max Shanahan, CISA, CGEIT, FCPA, Max Shanahan & Associates, Australia
Alan Simmonds, TOGAF9, TCSA, PreterLex, UK
Dejan Slokar, CISA, CGEIT, CISSP, Deloitte & Touche LLP, Canada
Jennifer Smith, CISA, CIA, Salt River Pima Maricopa Indian Community, USA
Marcel Sorouni, CISA, CISM, CISSP, ITIL, CCNA, MCDBA, MCSE, Bupa Australia, Australia
Roger Southgate, CISA, CISM, UK
Mark Stacey, CISA, FCA, BG Group Plc, UK
Karen Stafford Gustin, MLIS, London Life Insurance Company, Canada
Delton Sylvester, Silver Star IT Governance Consulting, South Africa
Katalin Szenes, CISA, CISM, CGEIT, CISSP, University Obuda, Hungary
Halina Tabacek, CGEIT, Oracle Americas, USA
Nancy Thompson, CISA, CISM, CGEIT, IBM, USA
Kazuhiro Uehara, CISA, CGEIT, CIA, Hitachi Consulting Co., Ltd., Japan
Rob van der Burg, Microsoft, The Netherlands
Johan van Grieken, CISA, CGEIT, CRISC, Deloitte, Belgium
Flip van Schalkwyk, Centre for e-Innovation, Western Cape Government, South Africa
Jinu Varghese, CISA, CISSP, ITIL, OCA, Ernst & Young, Canada
Andre Viviers, MCSE, IT Project+, Media 24, South Africa
Greet Volders, CGEIT, Voquals N.V., Belgium
David Williams, CISA, Westpac, New Zealand
Tim M. Wright, CISA, CRISC, CBCI, GSEC, QSA, Kingston Smith Consulting LLP, UK
Amanda Xu, PMP, Southern California Edison, USA
Tichaona Zororo, CISA, CISM, CGEIT, Standard Bank, South Africa

ISACA 董事会
Kenneth L. Vander Wal, CISA, CPA, Ernst & Young LLP (retired), USA, International President
Christos K. Dimitriadis, Ph.D., CISA, CISM, CRISC, INTRALOT S.A., Greece, Vice President
Gregory T. Grocholski, CISA, The Dow Chemical Co., USA, Vice President
Tony Hayes, CGEIT, AFCHSE, CHE, FACS, FCPA, FIIA, Queensland Government, Australia, Vice President
Niraj Kapasi, CISA, Kapasi Bangad Tech Consulting Pvt. Ltd., India, Vice President
Jeff Spivey, CRISC, CPP, PSP, Security Risk Management, Inc., USA, Vice President
Jo Stewart-Rattray, CISA, CISM, CGEIT, CRISC, CSEPS, RSM Bird Cameron, Australia, Vice President
Emil D'Angelo, CISA, CISM, Bank of Tokyo-Mitsubishi UFJ Ltd. (retired), USA, Past International President
Lynn C. Lawton, CISA, CRISC, FBCS CITP, FCA, FIIA, KPMG Ltd., Russian Federation, Past International President
Allan Neville Boardman, CISA, CISM, CGEIT, CRISC, CA (SA), CISSP, Morgan Stanley, UK, Director
Marc Vael, Ph.D., CISA, CISM, CGEIT, CISSP, Valuendo, Belgium, Director

鸣谢（续）

知识委员会
Marc Vael, Ph.D., CISA, CISM, CGEIT, CISSP, Valuendo, Belgium, Chairman
Michael A. Berardi Jr., CISA, CGEIT, Bank of America, USA
John Ho Chi, CISA, CISM, CRISC, CBCP, CFE, Ernst & Young LLP, Singapore
Phillip J. Lageschulte, CGEIT, CPA, KPMG LLP, USA
Jon Singleton, CISA, FCA, Auditor General of Manitoba (retired), Canada
Patrick Stachtchenko, CISA, CGEIT, Stachtchenko & Associates SAS, France

框架委员会（2009-2012）
Patrick Stachtchenko, CISA, CGEIT, Stachtchenko & Associates SAS, France, Chairman
Georges Ataya, CISA, CISM, CGEIT, CRISC, CISSP, Solvay Brussels School of Economics and Management, Belgium, Past Vice President
Steven A. Babb, CGEIT, CRISC, Betfair, UK
Sushil Chatterji, CGEIT, Edutech Enterprises, Singapore
Sergio Fleginsky, CISA, Akzo Nobel, Uruguay
John W. Lainhart, IV, CISA, CISM, CGEIT, CRISC, IBM Global Business Services, USA
Mario C. Micallef, CGEIT, CPAA, FIA, Malta
Anthony P. Noble, CISA, CCP, Viacom, USA
Derek J. Oliver, Ph.D., DBA, CISA, CISM, CRISC, CITP, FBCS, FISM, MInstISP, Ravenswood Consultants Ltd., UK
Robert G. Parker, CISA, CA, CMC, FCA, Deloitte & Touche LLP (retired), Canada
Rolf M. von Roessing, CISA, CISM, CGEIT, CISSP, FBCI, Forfa AG, Switzerland
Jo Stewart-Rattray, CISA, CISM, CGEIT, CRISC, CSEPS, RSM Bird Cameron, Australia
Robert E. Stroud, CGEIT, CA Inc., USA

特别表彰
ISACA Los Angeles Chapter for its financial support

ISACA 及 IT 治理研究院®（ITGI®）会员及赞助商
American Institute of Certified Public Accountants
Commonwealth Association for Corporate Governance Inc.
FIDA Inform
Information Security Forum
Institute of Management Accountants Inc.
ISACA chapters
ITGI France
ITGI Japan
Norwich University
Solvay Brussels School of Economics and Management
Strategic Technology Management Institute (STMI) of the National University of Singapore
University of Antwerp Management School

Enterprise GRC Solutions Inc.
Hewlett-Packard
IBM
Symantec Corp.

目录

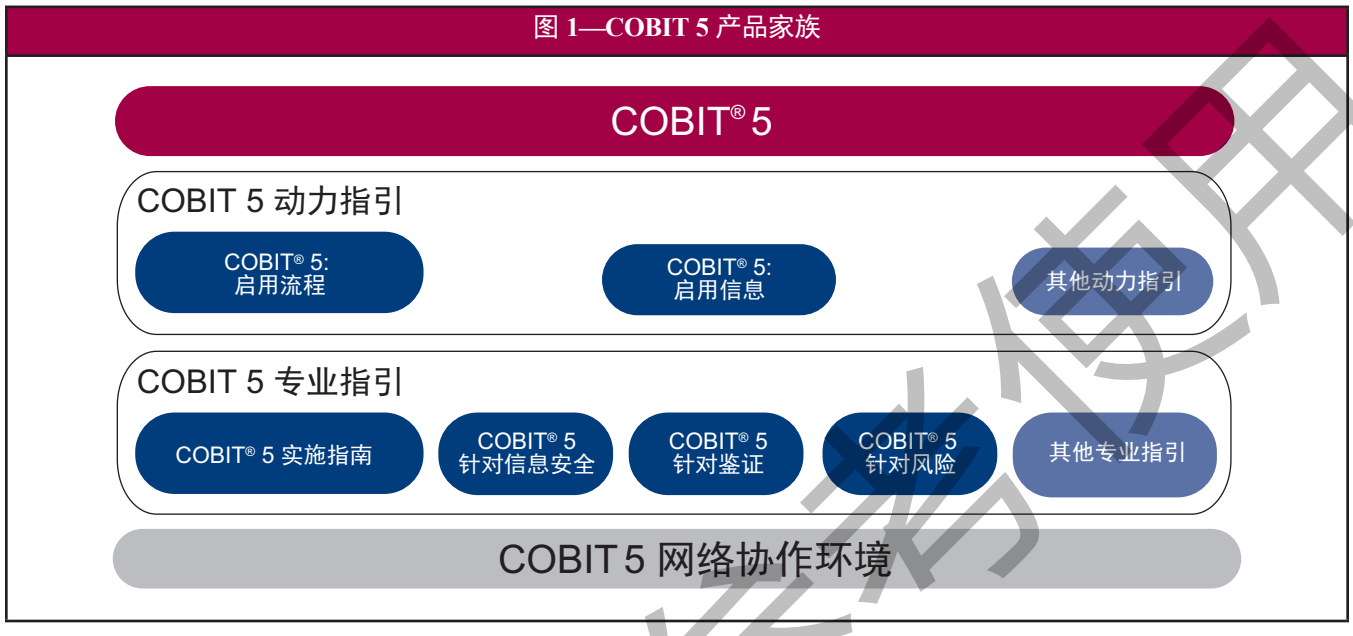
图表目录

本页特此留空

COBIT 5：企业 IT 治理和管理之业务框架

本 COBIT 5 出版物包括 COBIT 5 企业 IT 治理和管理之框架。本出版物属于**图 1** 所示的 COBIT 5 产品家族之一部分。

图 1—COBIT 5 产品家族



COBIT 5 框架是以五个基本原则为本创建而成的，这些原则详细地涵盖并包括对企业 IT治理和管理动力的精细指导。

COBIT 5 产品家族包括以下产品：
- COBIT 5（框架）
- COBIT 5 动力指引, 其中详细讨论了治理和管理动力，具体内容包括：
  - 《COBIT 5：启用流程》
  - COBIT 5：启用信息（开发中）
  - 其他动力指引（参阅 *www.isaca.org/cobit*）
- COBIT 5专业指引，具体内容包括：
  - 《COBIT 5 实施指南》
  - 针对信息安全的 COBIT 5（开发中）
  - 针对鉴证的 COBIT 5（开发中）
  - 针对风险的 COBIT 5（开发中）
  - 其他专业指引（参阅 *www.isaca.org/cobit*）
- 协作的网络环境，这个环境能支持 COBIT 5 的运用

本页特此留空

执行摘要

信息是所有企业的关键资源，从信息创建之日到信息销毁之时，技术无不发挥着至关重要的作用。信息技术日益进步，并已经渗透到企业、社会、公共和商业环境之中的每一个角落。

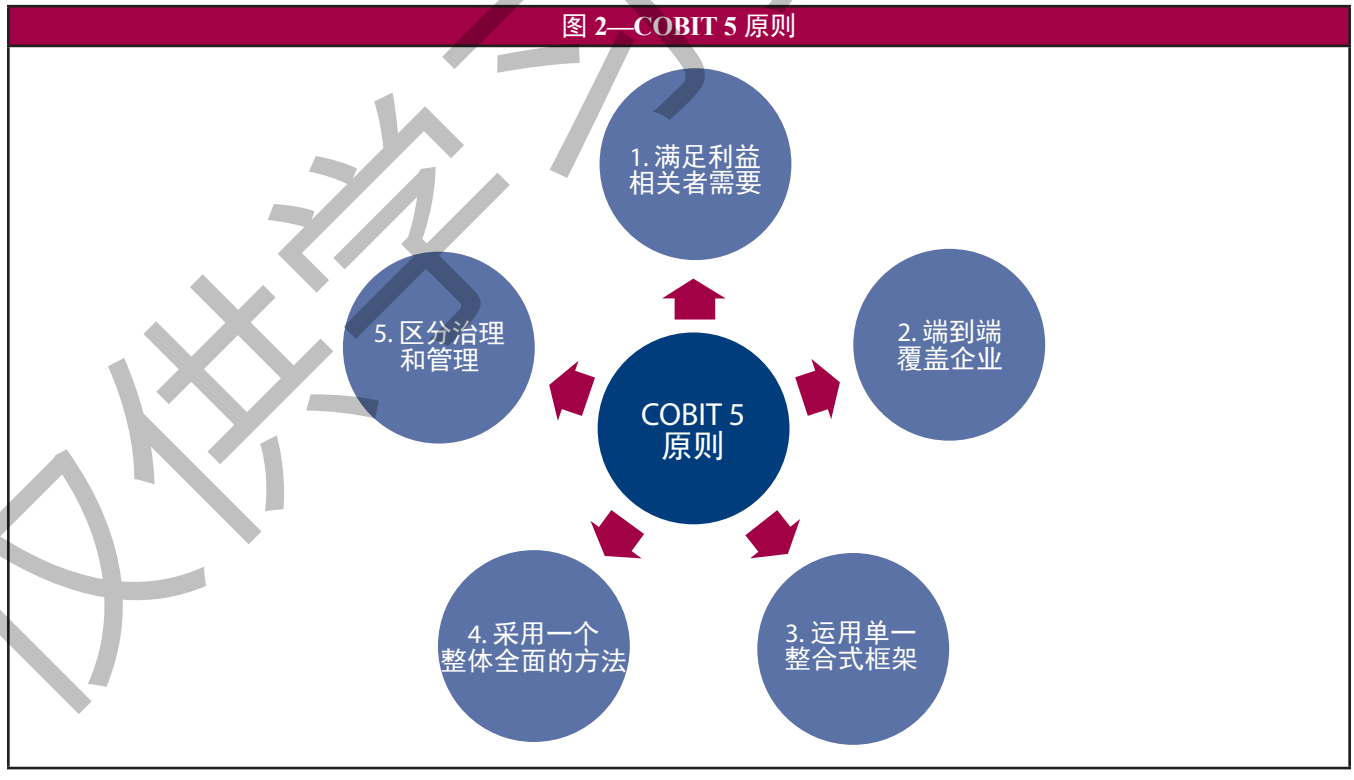
因此，如今，较之于任何历史时期，企业及其管理人员更致力于：
- 维持高质量信息以支持业务决策
- 从信息技术驱动的投资中产生商业价值，例如，通过有效地和创新地运用信息技术达到战略目标和实现商业效益
- 通过可靠的、高效的技术应用实现运营的卓越
- 维持信息技术相关的风险在一个可接受层级上
- 优化 IT 服务和技术的成本
- 遵守不断变化的相关法律法规、契约协议和政策

过去十年以来，“治理”这个词汇已经凸显在商业思维的最前端，以作为对证明良好治理重要性的实例，以及在另一个极端上的全球商务灾难的回应。

成功企业已经认识到，其董事会以及高管层必须像重视业务经营中任何其他重要部分一样地重视信息技术。董事会和管理层无论是在业务经营还是在 IT 功能中都必须通力合作，从而达到将 IT 纳入治理和管理方法之中。此外，为了应对这种需要，日益增加的立法正不断通过，监管条令亦不断实施。

COBIT 5 提供一种全面的框架，以支持企业实现其企业 IT 治理和管理的目标。简而言之，就是帮助企业通过维持实现利益和优化风险等级和资源利用之间的平衡，从而创造源自于 IT 的最佳价值。COBIT 5 能够为整个企业使 IT 在整体上得以治理和管理，并承担整个端到端业务和 IT 功能区域的责任，同时兼顾内外部利益相关者与 IT 相关的利益。COBIT 5 通用和实用于各种规模的机构，无论是商务、非营利、或公共机构。

图 2—COBIT 5 原则



COBIT 5 是以五项关键原则为基础（如**图 2** 所示）进行企业 IT 治理和管理：

- **原则 1：满足利益相关者需要**—企业的存在就是通过在实现收益、优化风险和运用资源之间维持一种平衡，从而为其利益相关者创造价值。COBIT 5 提供所有必需的流程和其他动力以支持通过IT运用来创造业务价值。因为各个企业的目标不尽相同，所以一家企业可以通过目标等级定制 COBIT 5，使其适用于企业的实际情况，将高层次企业目标转化成易于管理的、具体的、与 IT 相关的目标，并将这些目标映射到具体的流程和实践之中。
- **原则 2：端到端覆盖企业**—COBIT 5 将企业 IT 治理整合进企业治理之中：
  – COBIT 5 覆盖企业内所有的职能和流程；并不仅仅只关注“IT 功能”，而且还视信息及相关技术为资产，这种资产就像任何其他资产一样，可由企业内任何人予以处理。
  – COBIT 5 认为，所有与 IT 相关的治理和管理动力是端到端覆盖整个企业范畴的，例如，涉及到内部和外部的任何事和任何人---都与企业信息和相关 IT 的治理和管理形成关联。
- **原则 3：运用单一整合式框架**—IT相关的标准和最佳实践方法很多，每一种都有一种 IT 活动的子集提供指引。COBIT 5 与其他相关标准和框架保持高度一致，因此可以用作企业 IT 治理和管理的首要框架。
- **原则 4：采用一个整体全面的方法**—高效率和有效的企业IT治理和管理需要一种整体解决方案，应考虑到各个互相作用的组件。COBIT 5 定义了一组动力以支持企业IT的综合治理和管理体系的实施。所谓动力在广义上定义为任何能帮助实现企业目标的因素。COBIT 5 定义了七个动力范畴：
  – 原则、政策和框架
  – 流程
  – 组织结构
  – 文化、道德和行为
  – 信息
  – 服务、基础设施和应用程序
  – 人员、技能和能力
- **原则 5：区分治理和管理**—COBIT 5 将治理和管理明确区分开来。这两种科目包含不同类型的活动，需要不同的组织结构，并服务于不同的用途。从 COBIT 5 的角度来看，治理和管理之间的关键区别在于：

  – 治理

  治理确保利益相关者的需要、条件和选项得到评估，以决定平衡、协商一致、需要实现的企业目标；通过优先等级和决策来设定导向；并监控商定的导向和目标的绩效和合规性。

  在大多数企业中，整体治理是董事长领导下的董事会的责任。具体的治理责任可能授予适当级别的特别组织结构，尤其是在较大型综合性企业中更是如此。

  – 管理

  管理层计划，构建、运行和监控与治理机构设立导向一致的活动，以实现企业目标。

  大多数企业中，管理是首席执行官（CEO）领导下行政管理层的责任。

这五项原则结合在一起能够使企业构建一种能优化信息和技术投资的、用于利益相关者收益的、有效的治理和管理框架。

第一章
COBIT 5 概览

COBIT 5 是国际信息系统审计协会（ISACA）为企业IT治理和管理提供的新一代指引，是以来自商务、IT、风险、安全和鉴证团体的众多企业和用户对 COBIT 超过 15 年的实际使用和应用为依据而构建的。开发 COBIT 5 的主要驱动因素包括以下需要：

- 为更多利益相关者能够表明在衡量其对于信息及其相关技术的期望值（在何种风险等级以及何种成本能实现何种收益）以及在确保期望值实际得以交付的过程中他们处于何种优先级。部分人希望的是短期回报，而其他人希望的是长期可持续性；有些人愿意承担高风险，而其他人则不愿意；这些具有分歧的，并有时甚至是冲突性的预期需要予以有效地解决。此外，利益相关者不仅想要更多地参与，而且他们还希望局面的形成和实际结果的实现过程更为透明。
- 解决企业成功日益依赖于外部业务和 IT 技术方的问题，例如，外包商、供应商、顾问方、客户、云运算和其他服务提供商，并通过多样化内部手段和机制来实现预期价值。
- 处理已经大量增长的信息量。企业该如何选择相关及可信的信息以便于作出有效和高效率的决策呢？信息也需要有效地管理，而有效的信息模式就能有所帮助。
- 处理更加广泛深入的信息技术。信息技术越来越多地成为业务的整体部分。通常，即使是与业务保持一致，将 IT 分开不再是令人满意的。IT 必需成为业务项目、组织结构、风险管理、政策、技能、流程等等的整体部分。首席信息官（CIO）和IT职能部门的角色也在不断提升。业务职能部门内越来越多的人掌握了 IT 技能，并且已经或将要涉足于 IT 决策和 IT 运营。因此，IT 和业务需要更好地整合。
- 在创新和新兴技术领域中提供进一步的指引；这就关系到创造性、发明、开发新产品、使现有产品更能吸引消费者，获得新类型的客户。创新也意味着精简产品开发、制造和供应链，从而以不断提升的效率、速度和质量等级，向市场交付产品。
- 覆盖整个端对端业务和 IT 职能责任，并且覆盖形成有效的企业 IT 治理和管理的各个方面，例如，超越流程之外的组织结构、政策和文化。
- 更好地控制日益增长的用户发起的和用户控制的 IT 解决方案。
- 使企业实现：
  – 通过有效和创新地运用企业 IT 创造价值
  – 业务用户对 IT 参与和服务的满意度
  – 与相关法律法规、契约协议和内部政策的合规性
  – 业务需求和 IT 目标之间改善的关系
- 但凡相关之处，连接到或与市场上其他重要框架和标准保持一致性，例如，信息技术基础架构库（ITIL®），开放群组企业架构框架（TOGAF®），项目管理知识体系（PMBOK®），受控环境中的项目 2（PRINCE2®），反虚假财务报告委员会发起人组织委员会（COSO）和国际标准化组织（ISO）等机构的标准。这有助于利益相关者理解各种框架、良好实践和标准是如何互相关联进行定位。以及如何能够协同使用。
- 整合所有重要的 ISACA 框架和指引，主要关注 COBIT，IT 价值管理（Val IT）和 IT 风险管理（Risk IT），但同时也兼顾信息安全业商业模式（BMIS）、IT 鉴证框架（ITAF）和标题为《董事会 IT 治理简报》的出版物和推进治理（TGF）资源，这样COBIT 5就能覆盖整个企业，并提供一种依据将其他框架、标准和实践整合为单一的框架。

不同的产品和覆盖各种利益相关者多样化需要的其他指引，将以 COBIT 5 主要知识库为基础，随着时间的推移予以构建，从而使 COBIT 5 产品架构成为一种富有生命力的文件系统。有关最新 COBIT 5 产品架构可登陆 ISACA 网站 COBIT 页面浏览（*www.isaca.org/cobit*）。

本出版物概览

COBIT 5 框架包括另外的七个章节：

- 第二章详细说明原则 1：**满足利益相关者需要**。本章介绍 COBIT 5 的目标分层。企业 IT 目标可用于规范和建构利益相关者的要求。企业目标可与 IT 相关的目标关联，而这些 IT 相关目标可通过最佳运用和执行包括流程在内的所有动力来实现。这一系列连接的目标称为 COBIT 5 目标分层。本章还提供了利益相关者可能会遇到的有关其企业 IT 治理和管理问题的典型实例。
- 第三章详细说明原则 2：**端到端覆盖企业**。本章详细解释了 COBIT 5 如何以覆盖企业内所有职能和流程的方式将企业 IT 治理整合进企业治理之中。
- 第四章详细说明原则 3：**运用单一整合式框架**，并简单描述了实现整合的 COBIT 5 架构。
- 第五章详细说明原则 4：**采用一个整体全面的方法**。企业 IT 治理是系统性的并得到一系列动力的支持。在本章中，介绍了各种动力和一种查看动力的共同方式：通用动力模型。
- 第六章详细说明原则 5：**区分治理和管理**，并讨论了管理和治理之间的差别，以及它们是如何互相关联的。本章还包括高层级 COBIT 5 流程参考模式的实例。
- 第七章包括**实施指南**的介绍。本章描述了如何才能创建适当的环境、必需的动力、实施中的典型痛点和触发事件和实施以及持续的开发生命周期。本章是以题为《COBIT® 5 实施指南》出版物为依据，其中可了解到有关如何实施基于 COBIT 5 的企业 IT 治理的全部详细资料。
- 第八章详细说明 COBIT 评估程序的方法方案（*www.isaca.org/cobit-assessment-programme*）中的 **COBIT 5 流程能力模型**，该模型与 COBIT 4.1 流程成熟度评估的差异所在，以及用户如何才能迁移到新方法。

附录包括参考信息、映射和关于具体主题更为详细的信息：

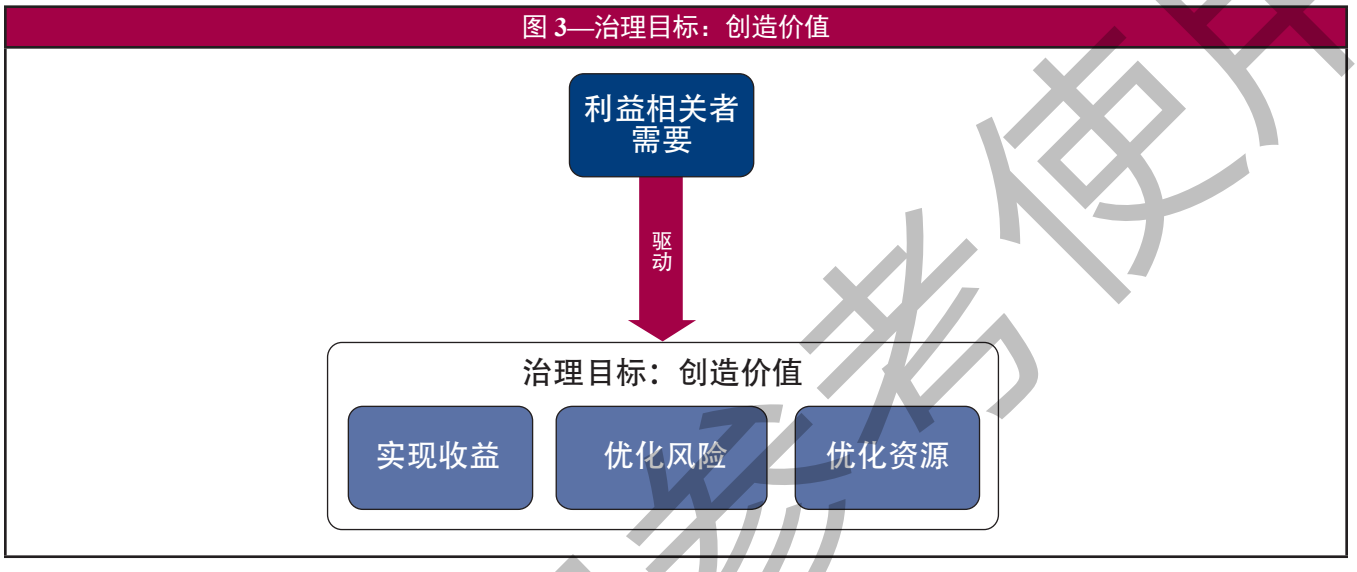
- 附件 A：列示出 COBIT 5 开发中引用的**参考文献**。
- 附件 B：**企业目标与 IT 相关目标之详细映射图**，描述了典型情况下一个或多个 IT 相关目标是如何支持企业目标的。
- 附件 C：**IT 相关目标与 IT 相关流程之详细映射图**，描述了 COBIT 流程是如何支持 IT 相关目标的实现。
- 附件 D：**利益相关者需要与企业目标**，描述了典型的利益相关者需要如何与 COBIT 5 的企业目标相关联。
- 附件 E：**COBIT 5 与最相关的关联标准和框架之映射图**。
- 附件 F：**COBIT 5 信息模型与 COBIT 4.1 信息标准之间的比较**。
- 附件 G：**COBIT 5 动力详细描述**，以第五章为基础，并纳入有关不同动力的更多细节，包括描述具体组件的详细动力模型，并采用大量实例予以说明。
- 附件 H：**词汇表**。

第二章
原则 1：满足利益相关者需要

导言

企业存在就是为了给其利益相关者创造价值。因此，任何企业，无论是商业化的或反之，将以创造价值作为治理目标之一。创造价值就意味着在优化风险的同时，以最佳资源成本实现收益。（见**图 3.**）收益的形式多种多样，例如商业企业的财务收益，或政府机构的公共服务等。

图 3—治理目标：创造价值



企业拥有很多利益相关者，因此“创造价值”就意味着他们之间因人而异，甚至互相冲突。治理就是在面对不同利益相关者的价值利益情况下协商和作决策。因此，在进行收益、风险和资源评估决策时，治理体系应考虑到所有的利益相关者，那么以下问题就可能和应该提出：“收益属于谁？谁承担风险？需要何种资源？”

COBIT 5 目标分层

每一个企业都在不同的环境中运作，而这种环境是由外部因素（市场、行业、地缘政治等）和内部因素（文化、组织、风险偏好等）所决定，并需要一种定制化的治理和管理体系。

利益相关者需要必须转变成企业可行动的战略。COBIT 5 目标分层是一种机制，能将利益相关者的需要转换成具体的、可行动、和定制化的企业目标、IT 相关的目标和动力目标。这种转换允许在企业的每一层级上，每一个方面设定具体目标，以支持整体目标和利益相关者的要求，因此就能有效地支持企业需要和 IT 解决方案及服务之间的一致性。

COBIT 5 目标分层如**图 4** 所示。

步骤 1：利益相关者驱动因素影响利益相关者需要

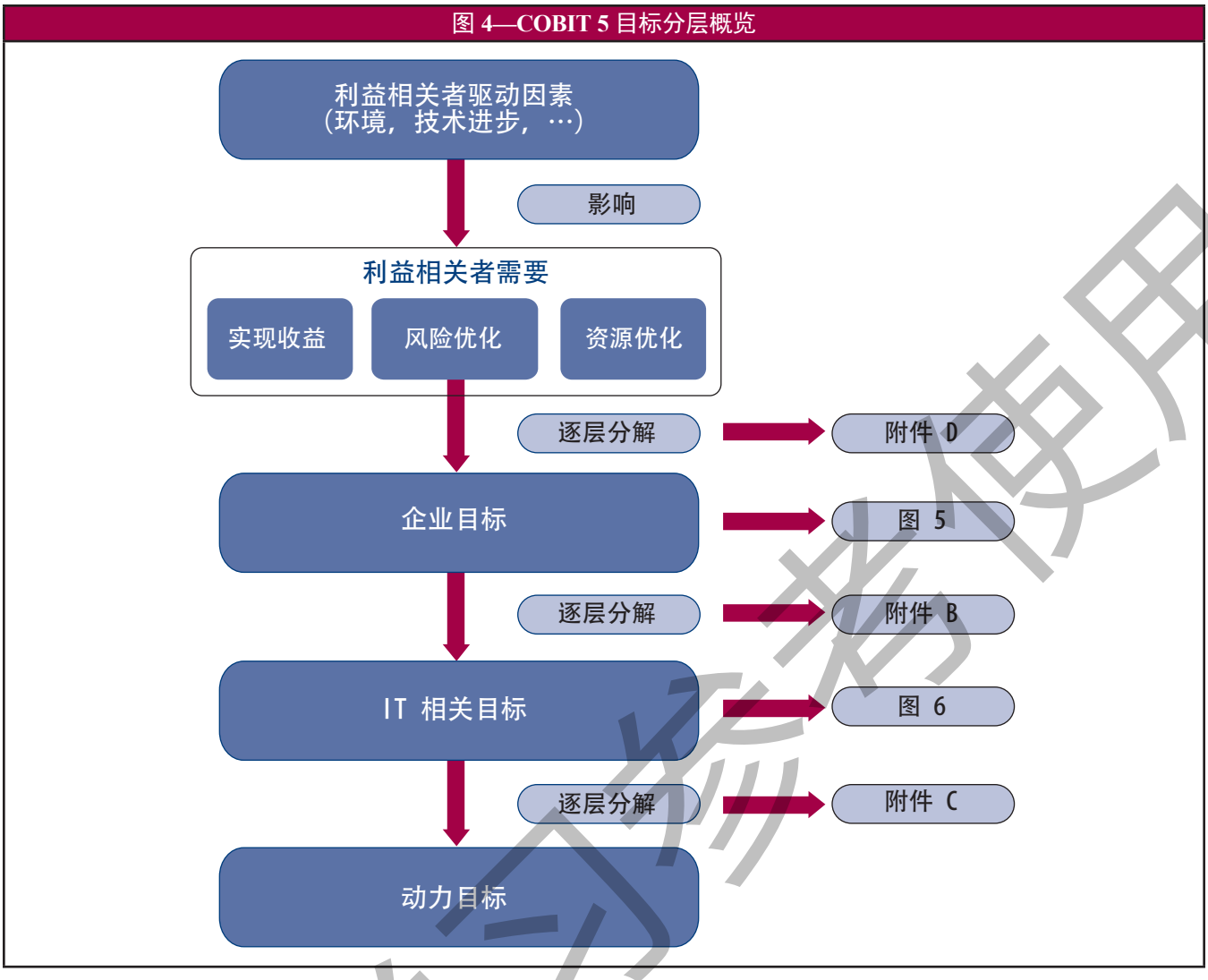
利益相关者需要受到多种驱动因素的影响，例如，战略变化，变化中的商业和监管环境，以及新技术等。

步骤 2：利益相关者需要逐层分解至企业目标

利益相关者需要可以与一系列通用企业目标关联。这些企业目标是运用平衡计分卡 (BSC)[1] 维度开发的，并代表某一企业可能自行定义的常用目标列表。尽管这一列表不甚详尽，但大多数企业特定的目标可以轻而易举地映射到一个或多个通用企业目标之上。利益相关者需要和企业目标表参见附件 D。

[1] Kaplan, Robert S.; David P. Norton; *平衡记分卡：将战略转化成行动*, 美国，哈佛大学出版社，1996 年

图 4—COBIT 5 目标分层概览



COBIT 5 定义了如**图 5** 所示的 17 项通用目标，包括以下信息：
- 平衡记分卡维度，企业目标在该维度下适宜。
- 企业目标
- 与三种主要治理目标的关系——实现收益、风险优化和资源优化。（P 代表主要关系，S 代表次要关系，如，稍弱的关系）。

步骤 3.企业目标逐层分解至 IT 相关的目标

企业目标的实现要求若干个 IT 相关的成果[2]，而这些成果是通过 IT 相关的目标来体现。信息及相关技术的 IT 相关的目标是根据 IT 平衡计分卡（IT BSC）的维度来架构的。COBIT 5 定义了 17 项 IT 相关的目标，如**图 6** 所列示。

IT 相关目标和企业目标之间的映射图纳入在附件 B 中，该图反映了每一个企业目标是如何得到若干个 IT 相关目标的支持的。

步骤 4. IT 相关的目标逐层分解至动力目标

实现 IT 相关的目标要求成功的应用和使用若干个动力。动力的概念在第五章中详细解释。动力包括流程、组织结构和信息，对于每一种动力，可规定一系列具体的相关目标以支持 IT 相关的目标。

流程属于动力之一，附件 C 包含 IT 相关目标和有关 COBIT 5 流程之间的映射图，其中包含有关流程目标。

[2] IT 相关的成果显然并非实现企业目标所要求的唯一中间收益。一个组织内的所有其他职能部门，如财务和营销，也为企业目标的实现做出了贡献，但是，在 COBIT 5 的环境中，仅只考虑到 IT 相关的活动和目标。

图 5—COBIT 5 企业目标

BSC 维度	企业目标	与治理目标的关系		
		实现收益	优化风险	优化资源
财务	1. 商务投资的利益相关者价值	P		S
	2. 竞争性产品与服务的组合	P	P	S
	3. 管理的业务风险（资产保障）		P	S
	4. 外部法律法规的合规性		P	
	5. 财务透明度	P	S	S
客户	6. 以顾客为中心的服务文化	P		S
	7. 业务服务的持续性和可用性		P	
	8. 对变化的企业环境敏捷的反应	P		S
	9. 信息为本的战略性决策	P	P	P
	10. 服务交付成本优化	P		P
内部	11. 业务流程功能性优化	P		P
	12. 业务流程成本优化	P		P
	13. 管理的业务变更方案	P	P	S
	14. 运营及员工生产率	P		P
	15. 内部政策合规性		P	
学习和成长	16. 熟练的有进取心的人员	S	P	P
	17. 产品和业务创新的文化	P		

图 6—IT 相关的目标

IT BSC 维度	信息及相关技术目标	
财务	01	IT 与业务战略的一致性
	02	IT 合规和对业务的外部法律法规合规的支持
	03	行政管理层对进行 IT 相关决策的承诺
	04	管理的 IT 相关业务风险
	05	从 IT 驱动的投资和服务组合中实现的收益
	06	IT 成本、收益和风险的透明度
客户	07	符合业务要求的 IT 服务交付
	08	应用程序、信息和技术解决方案的充分利用
内部	09	IT 敏捷性
	10	信息、处理基础设施和应用程序的安全
	11	IT 资产、资源和能力的优化
	12	通过将应用程序和技术整合进业务流程之中来推动和支持业务流程
	13	准时、按预算提交收益和满足要求及质量标准的项目集交付
	14	用于决策之可靠和有用的信息的可用性
	15	IT 对内部政策的合规性
学习和成长	16	胜任的有进取心的业务和 IT 人员
	17	业务创新的知识、专门技术和首创精神

利用 COBIT 5 目标分层

COBIT 5 目标分层的益处

目标分层[3]之所以重要是因为这样能够以企业的（战略）目标和相关风险为依据来定义企业 IT 治理的实施、改进、和鉴证的优先级。在实践中，目标分层能：

- 规定各责任层级相关的、有形的目的和目标
- 基于企业目标，过滤 COBIT 5 知识库，提取相关指南以纳入具体的实施、改进或鉴证项目之中
- 明确识别和交流恰当的动力（有些为运营必需的）是如何在实现企业目标中发挥重要作用的

谨慎使用 COBIT 5 目标分层

目标分层及其企业目标和 IT 相关目标之间以及 IT 相关目标与 COBIT 5 动力（包括流程）之间的映射图并非万能，因此用户不应以纯粹机械的方式照搬，而应作为一种指引，这样说的理由很多，具体包括：

- 每一个企业的目标优先级不尽相同，而且随着时间推移，优先级也会发生变化。
- 映射图没有区分企业的大小和/或所处的行业，仅只代表一种不同层次目标在整体上如何相互关联的共同特性。
- 映射中采用的指标使用了重要性或相关性两种层级，这就意味着存在相关性的“离散”层级，然而，在现实中，映射接近于对应于各种程度的连续体。

在实践中使用 COBIT 5 目标分层

从上述谨慎使用说明来看，当采用目标分层时，很显然一个企业始终应该运用的第一个步骤是考虑其具体情况来定制映射；换言之，每个企业应该构建其目标分层，并与 COBIT 进行比较，然后予以精炼细化。

例如，企业可能希望：

- 将战略优先级转化成每一个企业目标的具体“权重”或重要性。
- 考虑其具体的环境或行业等，验证目标分层的映射。

[3] 目标分层是以比利时安特卫普大学管理学院 IT 一致性与治理研究所进行的研究为依据。

实例 1—目标分层

某一企业为其规定了若干个战略目标，其中改善客户满意度为重中之重，为此，该企业希望了解到在与 IT 相关的千头万绪中何处需要改进。

该企业认定将客户满意度设定为关键优先级等同于提升以下企业目标的优先级（见**图 5**）：
- 6. 以顾客为中心的服务文化
- 7. 业务服务的持续性和可用性
- 8. 对变化的企业环境敏捷的反应

该企业现在进行目标分层的下一步：分析哪一些 IT 相关的目标与企业目标对应。它们之间推荐的映射列示在附件 B 中。

由此，建议以下 IT 相关的目标应作为重中之重（即所有“P”关联项）。
- 01 IT 与业务战略的一致性
- 04 管理的 IT 相关业务风险
- 07 符合业务要求的 IT 服务交付
- 09 IT 敏捷性
- 10 信息、处理基础设施和应用程序的安全
- 14 用于决策之可靠和有用的信息的可用性
- 17 业务创新的知识、专门技术和首创精神

该企业对本列表予以验证，并确定保留前四项目标作为优先事项。

在下一步分层中，使用动力概念（见第五章），这些 IT 相关的目标驱动若干个动力目标，其中包括流程目标。在附件 C 中，推荐了一份 IT 相关的目标和 COBIT 5 流程之间的映射图。该图可以识别出支持 IT 相关的目标的最有关联性的 IT 相关流程，但是，仅仅只有流程还不充分。其他的动力，如文化、行为和道德、组织结构、或技能和专门技术等同样重要，并需要一系列明确的目标。

当本练习过程完成时，该企业就确定了一套与所有动力一致的，能够使其实现既定战略目的的目标和一套衡量绩效的关联指标。

实例 2—利益相关者需要：可持续性

在进行了利益相关者要求分析之后，某一企业认定可持续性是其战略优先级。为此，可持续性不仅包括环境方面的因素，还包括各种为企业长期成功做出贡献的方方面面。

根据利益相关者需要的分析结果，该企业决定重点关注以下五个目标，并在随后增加部分深层次的目标规范：
1. 商务投资的利益相关者价值，尤其是利益相关者社会的价值
4. 外部法律法规的合规性，重点关注环境相关的法律和外包协议中处理劳动监管条例的法律
8. 对变化的企业环境敏捷的反应
16. 确定企业成功必须依靠熟练的有进取心的人员
17. 产品和业务创新的文化，重点关注长期创新

基于这些优先级，目标分层可像文本中解释的那样得以应用。

关于 IT 的治理和管理问题

因为企业高度依赖于 IT 的关系，任何企业中利益相关者需要的履行将会提出若干个关于企业 IT 治理和管理的问题（**图 7**）。

图 7—关于 IT 的治理和管理问题	
内部利益相关者	**内部利益相关者问题**
• 董事会 • 首席执行官（CEO） • 首席财务官（CFO） • 首席信息官（CIO） • 首席风险官（CRO） • 业务执行经理 • 业务流程所有者 • 业务经理 • 风险经理 • 安全经理 • 服务经理 • 人力资源（HR）经理 • 内部审计师 • 隐私官员 • IT 用户 • IT 经理 • 其他.	• 我如何能从使用 IT 中获得价值?终端用户对 IT 服务的质量满意吗? • 我如何管理 IT 的绩效? • 我如何才能以最佳方式为新的战略机遇开拓新技术? • 我如何才能以最佳方式构建和架构我的 IT 部门? • 我该如何依靠外部提供商？IT 外包协议该如何才能管理好? 我如何获取对外部提供商的保证? • 什么是对信息的（控制）要求? • 我是否解决了所有 IT 相关的风险? • 我是否正在运行一种高效的和灵活的 IT 运营? • 我该如何控制 IT 成本?我怎样才能以最有效的、高效的方式利用 IT 资源? 什么是最有效的、高效的采购选项？ • 我是否有足够的 IT 人员?我该如何发展和维护他们的技能，和如何管理他们的绩效? • 我如何获得 IT 鉴证? • 我正在处理的信息是否足够安全可靠？ • 我该如何通过更为灵活的 IT 环境来改善业务敏捷性？ • IT 项目是否未能交付承诺事项—如果未能，原因何在？IT 是否妨碍着业务战略的执行? • IT 对于企业永续发展的关键程度如何？如果 IT 不能发挥作用，我该怎么办？ • 哪些关键业务流程依赖于 IT，这些业务流程的要求是什么？ • IT 运营预算的平均超限是多少？IT 项目超过预算的频率和程度如何？ • IT 成果有多大部分是用于应急而不是推动业务改善？ • IT 资源是否充足，且基础设施是否可用以满足必需的企业战略目标？ • 重大 IT 决策需要多长时间？ • 整个 IT 投入和投资是否透明？ • IT 是否支持企业符合监管要求和服务等级？我怎样才能知道是否遵循了所有适用法规？
外部利益相关者	**外部利益相关者问题**
• 业务合作伙伴 • 供应商 • 股东 • 监管者/政府 • 外部用户 • 客户 • 标准化组织 • 外部审计师 • 顾问 • 其他.	• 我如何才能知道业务合作伙伴的经营是安全可靠的？ • 我如何才能知道企业遵循了适用的规章和条令？ • 我如何才能知道企业维护着一种有效的外部控制体系？ • 业务合作伙伴之间是否有可控的信息链？

如何找到这些问题的答案

图 7 中提到的所有问题均可与企业目标相关联，并根据问题有效解决的程度，用作目标分层的输入。附件 D 包括一个**图 7** 中所提到的内部利益相关者问题和企业目标之间的映射的实例。

第三章
原则 2：端到端覆盖企业

COBIT 5 是以整个企业、端到端的角度解决信息及相关技术的治理和管理。这就是说，COBIT 5 能：
- 将企业 IT 治理整合进企业治理之中。也就是说，由 COBIT 5 提出的企业 IT 治理体系无缝地整合在任何治理体系之中。COBIT 5 与关于治理的最新观点完全一致。
- 覆盖治理和管理企业信息和相关技术所需要的所有功能和流程，无论该信息在何处处理。鉴于这种扩展的企业范围，COBIT 5 能应对所有相关的内外部 IT 服务以及内外部业务流程。

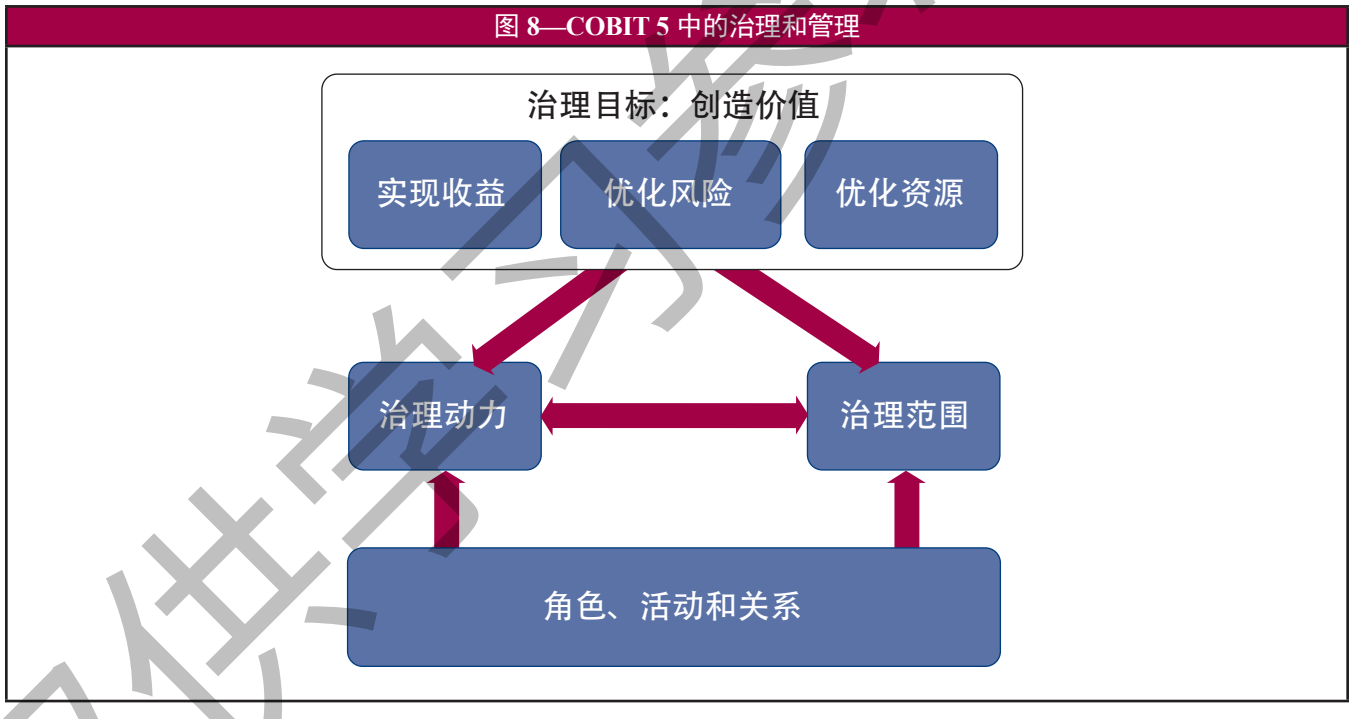
COBIT 5 以若干个动力为基础，提供一种全面性的和系统性的关于企业 IT 治理和管理的观点（见原则 4）。这些动力是端到端和涵盖整个企业的，也就是说，将与企业信息和相关 IT 的治理和管理有关联的内部和外部的任何事及任何人都纳入其中，包括 IT 部门和非 IT 业务部门的活动和职责。

信息属于 COBIT 动力范畴之一。COBIT 5 依照其定义动力的模型允许每一位利益相关者规定有关信息和信息处理生命周期的广泛而完全的需求，因此将业务及其对充分信息的需要与 IT 部门联系起来，并支持业务及其环境中的重点。

治理方法

图 8 描述作为 COBIT 5 基础的端到端治理方法，并展示出一套治理体系的关键组件。[4]

图 8—COBIT 5 中的治理和管理



除了治理目标之外，其他治理方法的要素包括动力、范围和角色、活动和关系。

[4] 本治理系统由 ISACA 的“推动治理前进”（TGF）倡导图解说明。有关 TGF 的详情请访问：*www.takinggovernanceforward.org.*

治理动力

治理动力指治理的组织资源，如框架、原则、结构、流程和实践，通过或朝向这些资源，所采取的行动得以指导，而目标得以实现。动力还包括企业资源—如，服务能力（IT 基础设施、应用程序等）、人员和信息。缺乏资源或动力可能会影响到企业创造价值的能力。

鉴于治理动力的重要性，COBIT 5 包括一种单一的探讨和处理动力的方法（见第五章）。

治理范围

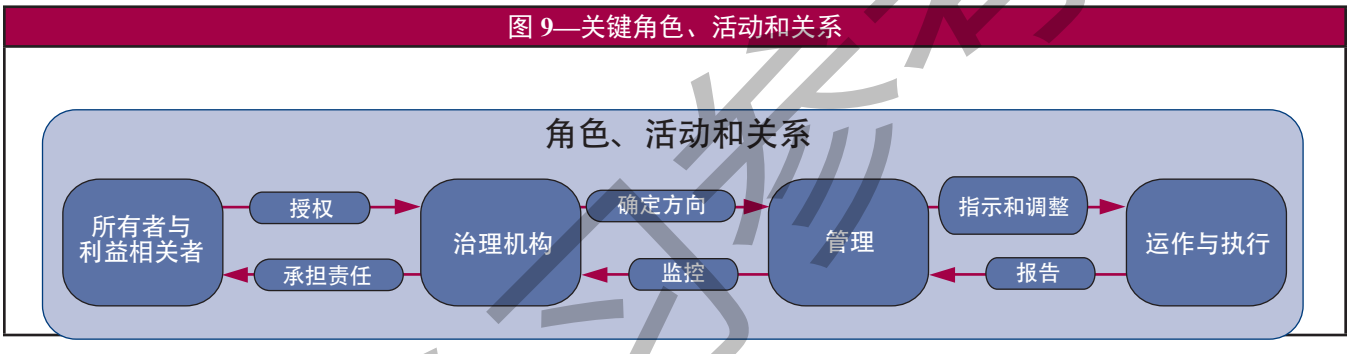
治理可应用到整个企业、某一实体、某一种有形或无形资产等等。也就是说，定义治理应用于企业的不同观点是有可能的，并且定义这种治理系统的范围是至关重要的。COBIT 5 的范围是整个企业---但在本质上，COBIT 5 可处理任何不同的观点。

角色、活动和关系

最后一种要素就是治理的角色、活动和关系，这种要素定义了在任何治理体系范围之内谁参与治理、他们如何参与、他们该做什么，及他们如何互动。在 COBIT 5 中，对在治理和管理域中的治理和管理活动进行了明确的区分，同时也区分了它们之间的界面连接以及所涉及的角色身份。**图 9** 详述了**图 8** 的下半部分，列示出不同角色之间的相互作用。

有关本治理通用视图的更多信息，请浏览“推动治理前进”：*www.takinggovernanceforward.org.*

图 9—关键角色、活动和关系



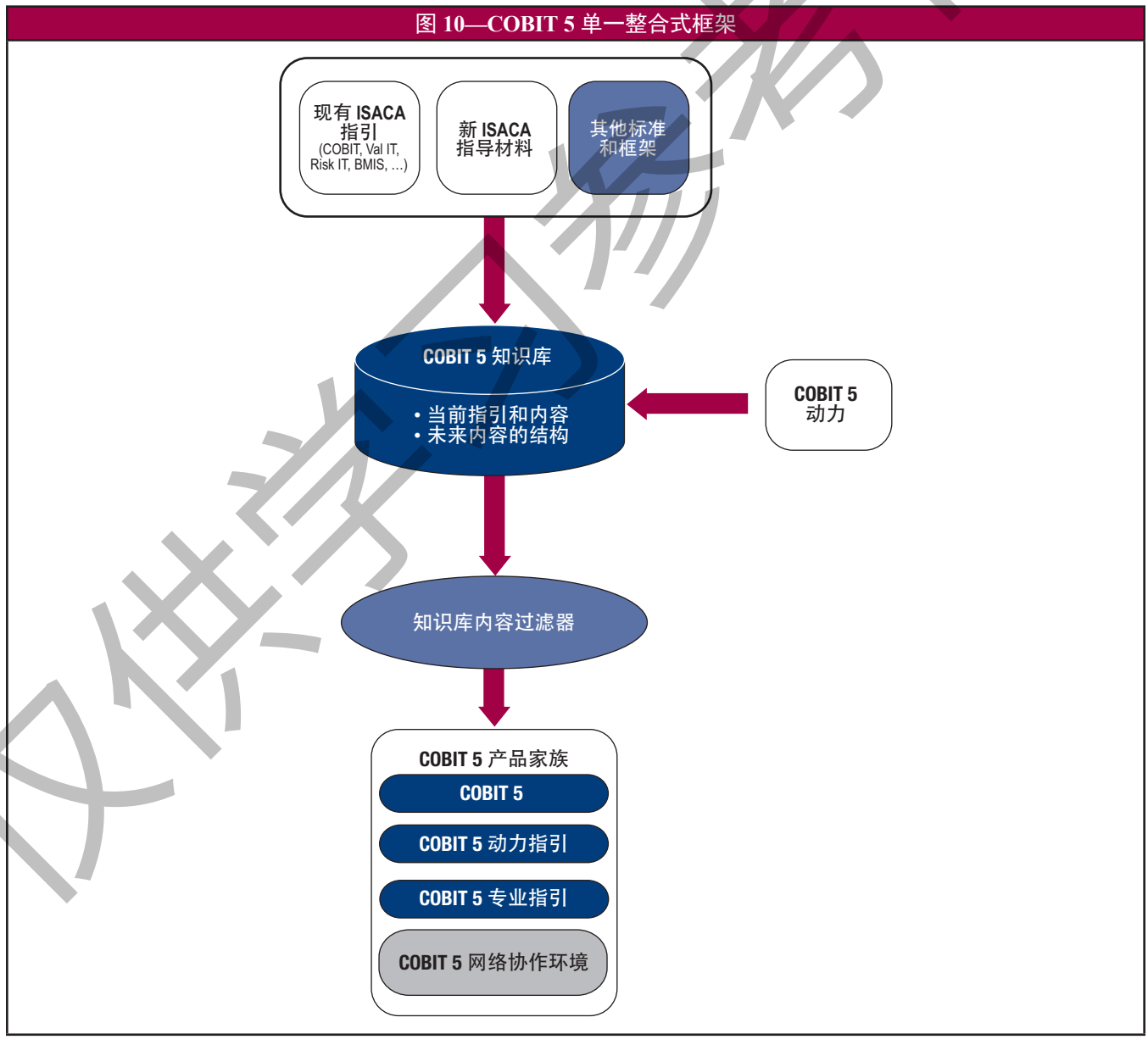
第四章
原则 3：运用单一整合式框架

COBIT 5 是一种单一和整合式框架，其原因在于：
- 保持与其他最新标准和框架一致，从而使企业能够使用 COBIT 5 作为首要的治理和管理框架集成者。
- 完整地覆盖整个企业，为使用中的其他框架、标准和实践提供了有效的整合基础。这种单一的首要框架是综合的非技术性的指导来源以非技术、与技术无关的公用语言表达的，可作为一个一致的、整合的指引资源。
- 为构建指引材料和生成一致的产品集提供一种简单的架构。
- 将以前分散在 ISACA 各种不同框架中的所有知识整合在一起。ISACA 多年以来对企业治理的关键领域进行了研究，并已经开发出诸如 COBIT、IT 价值管理（Val IT）和IT风险管理（Risk IT）、信息安全商业模式（BMIS），出版了《董事会 IT 治理简报》（*Board Briefing on IT Governance*）、信息技术鉴证框架（ITAF）等这些框架，为企业提供指引和帮助，而 COBIT 5 将所有这些知识都整合在一起。

COBIT 5 框架集成者

图 10 提供的是一种图解说明，描述 COBIT 5 是如何实现其一致的整合框架角色。

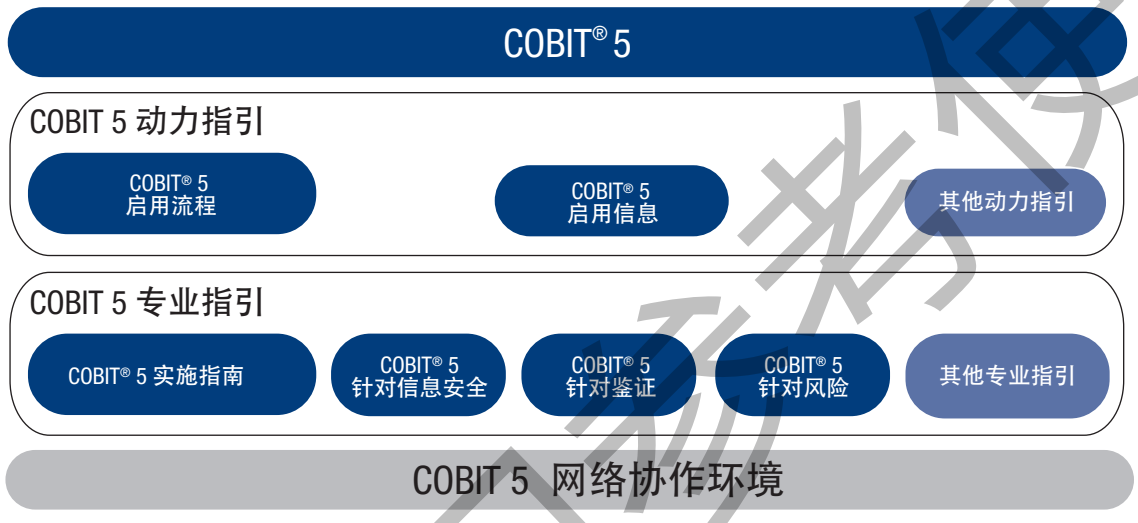
图 10—COBIT 5 单一整合式框架



COBIT 5 框架通过以下方面为其利益相关者提供最完整的、最新的企业 IT 治理和管理的指引（**见图 11**）：

- 研究和运用一套推动新型内容开发的来源，包括：
  - 将现有的 ISACA 指引（COBIT 4.1, Val IT 2.0, Risk IT, BMIS）整合为本单一框架
  - 使本内容与需要进一步完善和更新的领域形成互补
  - 与其他相关标准和框架，例如信息技术基础架构库（ITIL）、开放群组企业架构框架（TOGAF）及国际标准化组织（ISO）标准保持一致。参考文献列表参见附件 A
- 定义一套治理和管理动力，这些动力为所有指引材料提供一种架构。
- 增加 COBIT 5 知识库的内容，该知识库不仅包含所有指引和已生成的内容，并为未来增添内容提供了一个架构。
- 为良好实践提供一种健全全面的参考基础。

图 11—COBIT 5 产品家族



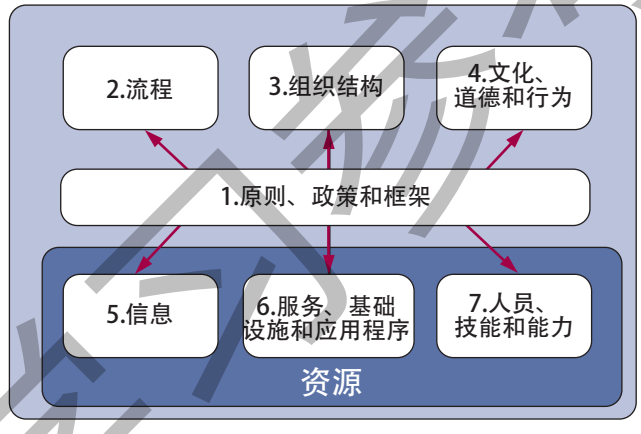
第五章
原则 4：采用一个整体全面的方法

COBIT 5 动力

所谓动力就是单一的或集体的而能影响到某种东西能否起作用的因素——在 COBIT 5 环境中，就是指能对企业 IT 的治理和管理起作用的因素。动力是由目标分级所驱动，例如，较高层级的 IT 相关目标规定了不同的动力所应实现的目标。

COBIT 5 框架描述了动力的七种范畴（**图 12**）：
- **原则、政策和框架**是将欲达到的行为转化成日常管理的实践指引之载体。
- **流程**描述了一套实现某些目的的组织化实践和行动，并生成一套输出以支持实现整体 IT 相关的目标。
- **组织结构**是企业内的关键决策实体。
- 个体或企业的**文化、道德和行为**作为治理和管理活动中的成功因素经常会被低估。
- **信息**，包括所有企业已生成和使用的，渗透在任何组织结构之中。信息对于保证组织结构的运转和良好的治理是必要的，但在运营层级上，信息通常是企业本身的关键产品。
- **服务、基础设施和应用程序**包括为企业提供信息技术处理和服务的基础设施、技术和应用程序。
- **人员、技能和能力**均与人相关，是成功完成各种活动、作出正确决策、和采取纠正措施所必需的。

图 12—COBIT 5 企业动力



部分以前定义的动力也是需要予以管理和治理的企业资源，这可适用于：
- 需要作为资源来管理的信息。某些信息，例如管理报告和商务情报信息，是企业治理和管理的主要动力
- 服务、基础设施和应用程序
- 人员、技能和能力

通过互为联系的动力进行系统的治理和管理

图 12 还传递了企业治理应该采纳的思维模式，这包括：IT 治理是为实现企业的主要目标。任何企业必须始终要考虑到一套互为联系的动力，也就是说，每种动力：
- 需要其他动力的输入才能完全有效，如，流程需要信息，组织结构需要技能和行为；
- 为其他动力的益处提供输入，如，流程提供信息，技能和行为使流程的效率更高。

因此，当涉及到企业 IT 治理和管理时，只有考虑到治理和管理安排的这种系统化性质，才能做出良好的决策。这也就意味着，为满足任何利益相关者的需要，所有相关的动力必须进行相关性分析并在必要时予以处理。这种思维模式必须由企业高层推动，具体由以下实例说明：

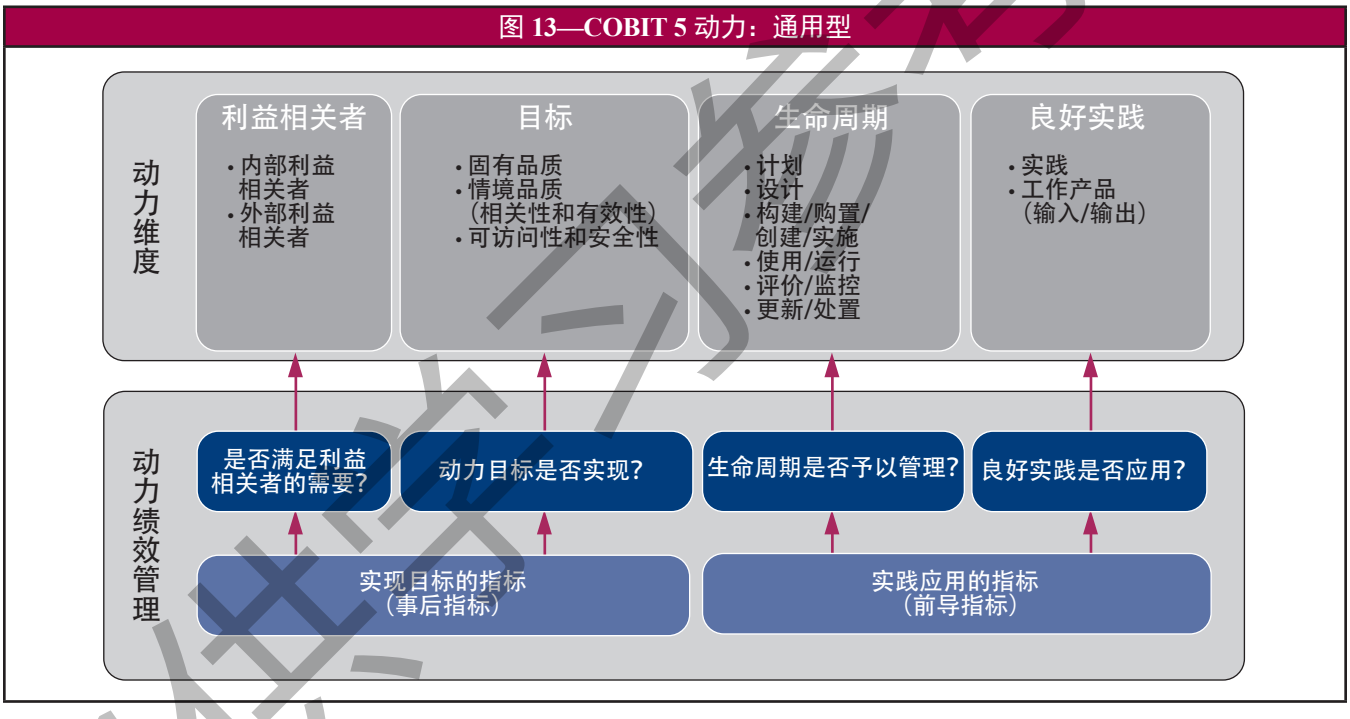
样例 3—企业IT治理和管理
为所有用户提供运营性 IT 服务需要具备的服务能力（基础设施、应用程序等），具有适当技能组合和行为的人员是必需的。同时也需要实施由适当的组织结构支持的一系列服务交付流程。这就表明对于一个成功的服务交付如何需要所有动力的配合。

样例 4—企业IT治理和管理
满足信息安全的要求需要创建一系列政策和程序并将他们实施到位，这些政策会进而要求实施一系列安全相关的实践。然而，如果企业和个人的文化、道德不适宜，信息安全的流程和程序将会无效。

COBIT 5 动力维度

所有动力均有一套共同维度，这套维度（**图 13**）：
- 提供一种共同的、简单的、结构化方式以处理动力
- 允许一个实体管理其复杂的互动关系
- 促进动力的成功结果

图 13—COBIT 5 动力：通用型



动力维度

动力的四种共同维度是：
- 利益相关者— 每一种动力都有利益相关者（起到积极作用的和/或对动力感兴趣的各方）。例如，就流程而言，有执行流程活动的各方，和/或对流程结果感兴趣的各方；对组织结构而言，有在结构中构成各部分的扮演各自的角色或对此感兴趣的利益相关者。利益相关者可能是企业内部或是企业外部的，都有各自的、有时甚至是互相冲突的利益关系。利益相关者的需要转化成企业的目标，这些目标继而转化成企业 IT 相关的目标。**图 7** 所示的是利益相关者列表。
- **目标**—每种动力都有若干个目标，而动力是透过达到这些目标来提供价值。目标可定义为以下方面：
  – 动力的期待结果
  – 动力本身的运用或运营

动力目标是 COBIT 5 层级中的最终步骤，这些目标可进一步细分为不同的范畴：
– **固有品质**—动力精确地、客观地发挥作用，并提供精确的、客观的和规范的结构之程度。
– **情境品质**—考虑到其运行的环境，动力及其结果与目的相适配，例如，结构应该是相关的、完整的、当前的、适当的、一致的、可理解的和易于使用的。
– **访问与安全**—动力及其结果可访问性和安全可靠的程度，例如：
  • 当需要时，动力是可用的
  • 结果是可靠的，例如，访问仅限于有权或需要访问者
• **生命周期**—每一种动力均有生命周期，从运行/使用寿命开始直到处置。这种周期可运用到信息、结构、流程和政策等等。生命周期的各阶段由以下内容构成：
– 计划（包括概念开发和概念选择）
– 设计
– 构建/购置/创建/实施
– 使用/操作
– 评价/监控
– 更新/处置
• **良好实践**— 对于每一种动力，均可定义良好实践。良好实践支持动力目标的实现。良好实践就如何以最佳方式实施动力，或需要何种工作产品或输入和输出等，提供实例和建议。COBIT 5 为其自己提供的部分动力（如流程）提供了良好实践的实例。至于别的动力，亦可采用其他标准，框架的指引。

动力绩效管理

企业都期望能从应用和使用动力中获得积极的成果。为了管理动力的绩效，需要对以下问题进行监控，然后按指标予以回答—并应定期进行：
• 利益相关者的需要是否得以满足？
• 动力目标是否实现？
• 动力生命周期是否予以管理？
• 良好实践是否得以应用？

前两项处理的是动力的实际结果，用于测评目标实现程度之指标可称为“事后指标”。

后两项处理的是动力本身的实际功能性，其测量指标可称之为“前导指标”。

实践中的动力实例

示例 5 说明了动力、其互相的关联性和动力维度，以及如何使用它们来实现收益。

示例 5—动力

一个组织已经为 IT 相关流程任命了一位“流程经理”，负责在良好的企业 IT 治理和管理环境中定义和运行有效和高效的 IT 相关的流程。

首先，流程经理关注流程动力，考虑动力的维度：
• **利益相关者：**流程利益相关者包括所有的流程参与者，例如，为了流程活动或在流程活动期间的执行方、责任方、商议方或告知对象（RACI）等各方。为此，可以使用《COBIT 5：启用流程》中描述的 RACI 图。
• **目标：**就每一个流程而言，恰当的目标和相关的指标需要予以定义。例如，针对某一“关系管理”的流程（《COBIT 5：启用流程》中的 APO08 流程），用户可以发现一套流程目标和指标，如：
  – **目标：**业务策略、计划和要求均得到充分理解、记录和批准。
    • **指标：**与企业业务要求/优先顺序一致的项目集百分比
  – **目标：**存在于企业与 IT 部门之间的良好关系。
    • **指标：**用户和 IT 人员满意度调查的排名
• **生命周期：**每一个流程均有一个生命周期，例如，流程必须被创建、执行和监控，并在必要时予以调整。最终，流程会不复存在。这样，流程经理就需要首先设计和定义流程。流程经理们可以使用《COBIT 5：启用流程》中的若干个要素以设计流程，如定义责任和将流程细分为实践和活动，并定义流程产品（输入和输出）。在后期阶段中，还需要使流程更稳健和高效，而为达到此目的，流程经理可以提高流程的能力等级。受 ISO/IEC 15504 启发的 COBIT 5 流程能力模型和流程能力属性可用于该目的。

示例 5—动力（*续*）

- **良好实践：**如前述要点中提及的，COBIT 5 在《COBIT 5：启用流程》中为各流程非常详细地描述了良好实践，其中可了解到启发和示例流程，并涵盖了良好的企业 IT 治理和管理所要求的各个方面活动。

除了关于流程动力的指引之外，流程经理可以决定研究若干其他的动力，如：

- RACI 图，该图描述了角色和责任。其他动力则便于用户深入钻研这种维度，例如：
  - 在技能和能力动力中，每种角色所必须具备的技能和能力可被定义，及适当的目标（如技术和行为技能等级）和关联的指标都可被定义。
  - RACI 图也包含一系列组织结构。这些结构可以在组织结构动力中予以进一步详述，在此可提供更为详细的架构描述，预期的成果、相关指标（如决策）和良好实践（如控制范围、结构运行原则和授权等级）。
- 原则和政策会使流程正规化，并规定流程为何而存在，可应用的对象以及流程如何使用。这是原则和政策动力的重点领域。

在附件 G 中，对动力的七个范畴进行了详细的讨论。建议阅读该附件以便更好地理解动力，以及动力在组织企业 IT 治理和管理中是如何发挥强而有力的作用。

第六章
原则 5：区分治理和管理

治理和管理

COBIT 5 将治理和管理明确区分开来。这两种科目包含不同类型的活动，需要不同的组织结构，并服务于不同的用途。从 COBIT 5 的角度来看，治理和管理之间的关键区别在于：

- **治理**

> **治理确保利益相关者的需要、条件和选项得到评估，以决定平衡、协商一致、需要实现的企业目标；通过优先等级和决策来设定导向；并监控商定的导向和目标的绩效和合规性。**

在绝大多数企业中，治理是在董事长领导下的董事会的责任。

- **管理**

> **管理层计划、构建、运行和监控与治理机构设定导向一致的活动，以实现企业目标。**

在绝大多数企业中，管理是在首席执行官领导下的执行管理层的责任。

治理和管理之间的互动性

从治理和管理的定义来看，很显然它们构成了不同的活动，并具有不同的责任；然而，鉴于治理的作用——评价、指导和监控——因此需要一组治理和管理之间的互动，以形成一种高效和有效的治理体系。这些互动使用动力结构，在高层次上如图 14 所示。

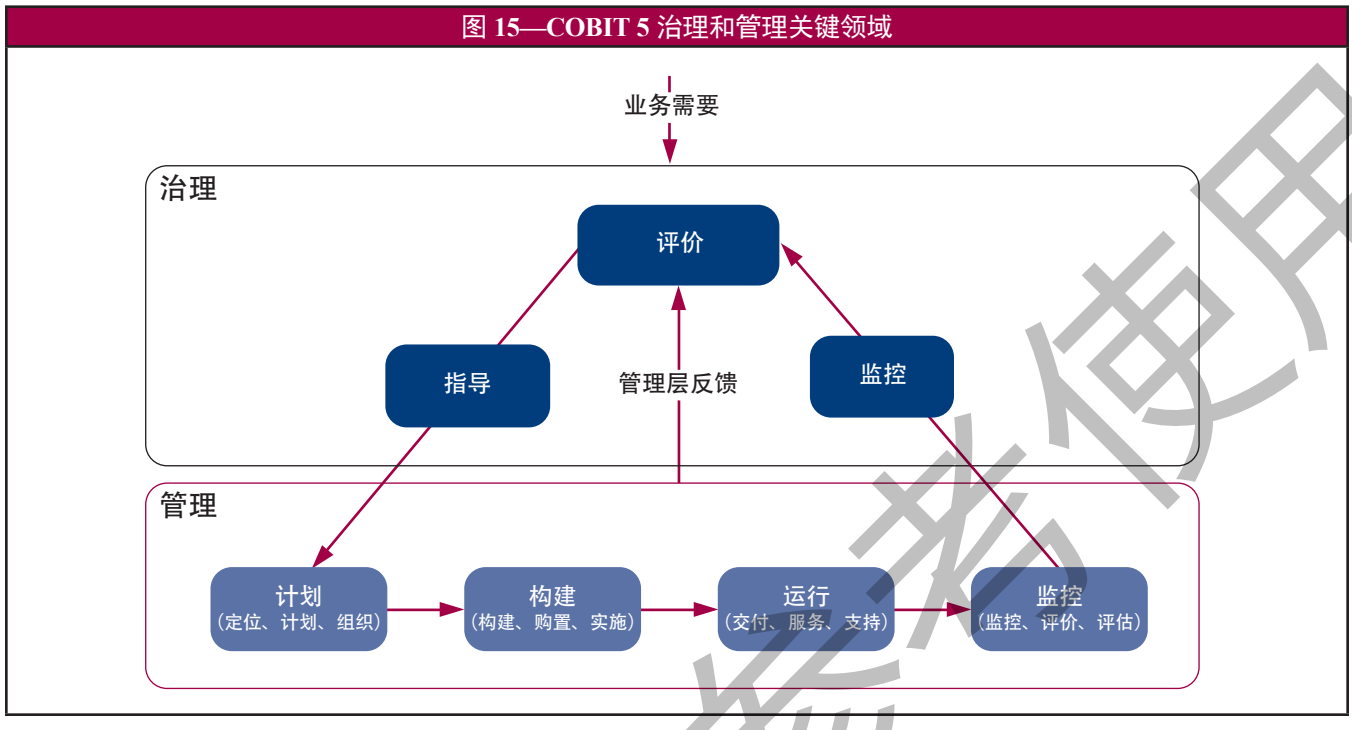
图 4—COBIT 5 治理和管理的互动

动力	治理—管理的互动
流程	在 COBIT 5 流程模型（《COBIT 5：启用流程》）中，治理和管理流程之间存在着区别，包括各自的一系列具体的实践和活动。流程模型还包括 RACI 图，以说明不同组织结构的责任和企业内的角色。
信息	流程模型描述从不同流程实践到其他流程的输入和输出，包括治理和管理流程之间交换的信息。用于评价、指导和监控企业 IT 的信息，以流程模型输入和输出的方式描述在治理和管理之间进行的交换。
组织结构	每一个企业都会定义若干个组织结构；这些结构可参与到治理空间和管理空间之中，取决于其决策的组分和范围。因为治理是关乎设定方向，互动是在治理结构所作出的决策（如，关于投资组合的决策和设定风险偏好）和实施前者所需的决策和运营之间进行。
原则、政策和框架	原则、政策和框架是企业内治理决策制度化的载体，因此，也是治理决策（设定方向）和管理（执行决策）之间的一种互动。
文化、道德和行为	行为也是企业良好治理和管理的关键动力之一，并由高层设定——以榜样为先导——因此也是一项治理和管理之间的重要互动。
人员、技能和能力	治理和管理要求不同的技能组合，但对于治理机构成员和管理层而言，一项根本的技能就是理解各种任务以及任务之间的差异。
服务、基础设施和应用程序	服务需要并由应用程序和基础设施支持，以为治理机构提供充分的信息和支持评价、设定方向和监控治理活动。

COBIT 5 流程参考模型

COBIT 5不是指令性的，但提倡企业实施治理和管理流程以覆盖关键领域，如**图 15** 所示。

图 15—COBIT 5 治理和管理关键领域



只要覆盖所有必要的治理和管理目的，企业可以组织其自视为适当的流程。小型企业可能需要较少的流程；大型和较为复杂的企业可能会需要很多流程，全都是为了达到同一个目的。

COBIT 5 包括一个流程参考模型，该模型详细定义和描述若干个治理和管理流程；并代表所有通常在某一企业内可发现的、与 IT 相关活动的流程，为操作 IT 和业务经理提供一种可理解的共同参考模型。所建议的流程模型是一个完整的、综合的模型，但并不是唯一可行的流程模型。各个企业必须结合其具体情况定义各自的流程集。

将企业涉及到 IT 活动的所有部分使用一种操作模型和一种共同语言结合起来，是迈向良好企业治理的最重要和最关键的步骤之一。这还可以提供一种框架以用于测评和监控 IT 绩效、提供 IT 鉴证、与服务提供商进行交流、以及整合最佳管理实践。

COBIT 5 流程参考模型将企业 IT 治理和管理划分为两大主要流程领域：

- **治理**—包括五个治理流程；在每一个流程中对评价、指导和监控 (EDM)[5] 实践予以定义。
- **管理**—包括四大领域，与计划、构建、运行和监控 (PBRM) 的责任范围一致，并提供端到端的 IT 覆盖。这些领域是 COBIT 4.1 领域和流程结构的演进结果。这些领域的名称选择与其主要的范围指定是一致的，但使用了更多动词对其予以描述：
  - 定位、计划和组织 (APO)
  - 构建、购置和实施 (BAI)
  - 交付、服务和支持 (DSS)
  - 监控、评价和评估 (MEA)

[5] 在治理领域的环境中，“监控”的意思指治理机构检查为管理层设定的方向的实际应用程度之活动。.

每一领域包含若干个流程。尽管如前述，大多数流程需要企业内部的、或在处理特定问题（如质量、安全性）的范围内的“计划”、“实施”、“执行”和“监控”活动，但从企业层次看待 IT 时，这些流程均处于与最相关活动一致的领域之中。

COBIT 5 流程参考模型是 COBIT 4.1 流程模型的继承，但整合 IT 风险管理（Risk IT）和IT价值管理（Val IT）流程。

图 16 显示出 COBIT 5 中全套完整的 37 个治理和管理流程。根据前述的流程模型描述，所有流程的细节均包括在《COBIT 5：启用流程》之中。

图 16—COBIT 5 流程参考模型

本页特此留空

第七章
实施指南

导言

只有通过有效采用并调整 COBIT，使其适应于每个企业的独特环境时，才能借力 COBIT 实现它的最佳价值。每一种实施方法还需要解决包括管理文化和行为变化在内的具体挑战。

ISACA 在其出版的《COBIT 5 实施指南》[6] 中，以持续改进的生命周期为基础提供了实用的和广泛的实施指南。该出版物并非指令性方法，也非完整的解决方案，而只是一种指南，以避免共性常见的误区，发挥良好实践的作用和协助创造成功的结果。本指南还配套有一个实施工具包，该工具包中包含将会持续增强的各种资源，其内容包括：
- 自我评估、测量和诊断工具
- 针对各种受众的介绍
- 相关文章和进一步解释

本章的目的是在较高层面上介绍实施和持续改进生命周期，并突出强调《COBIT 5 实施指南》中的若干个重要话题，例如：
- 就企业 IT 治理和管理的实施和改进进行案例研究
- 确认典型的痛点和触发事件
- 为实施创建适宜的环境
- 借力 COBIT 来发现差距，并指导诸如政策、流程、原则、组织机构和角色及责任等动力的开发

考虑企业的具体环境

企业 IT 治理和管理不可能在真空中进行。每一个企业需要设计自己的实施计划或路线图，这要取决于企业具体的内外部环境中的各种因素。例如企业的：
- 道德和文化
- 适用的法律和法规以及政策
- 使命、愿景和价值观
- 治理政策和实践
- 业务计划和战略意图
- 运作模式和成熟度
- 管理风格
- 风险偏好
- 能力和可用资源
- 行业惯例

同样重要的是要充分利用和构建现有的企业治理中的推动力。

企业 IT 治理和管理的最佳方法因各个企业而异，需要理解和考虑各企业的环境，以便在实施企业 IT 动力的治理和管理时有效地采用和适配 COBIT。COBIT 通常以其他框架、良好实践和标准为依托，而这些也需要予以调整以满足具体的要求。

成功实施的关键成功要素包括：
- 高管层提供及时指导和授权，以及切实有效的承诺和支持
- 所有各方支持治理和管理流程以理解业务和 IT 目标
- 确保对必要变革的推进和有效的沟通
- 根据企业独特的环境量身定制 COBIT 和其他配套的良好实践以及标准
- 注重速赢并优先实施最易实现和的最具效益的改进方案

[6] *www.isaca.org/cobit*

创造适宜的环境

借助 COBIT 在实施举措时给予适当治理和充分管理非常重要。重大 IT 相关的举措常常失败其原因在于各个必需的利益相关者在指导、支持以及监督方面的不足，而利用 COBIT 实施 IT 动力的治理和管理也不例外。来自关键利益相关者的指导和支持非常重要，可以使改进得以采纳和持续进行。在管理薄弱的企业环境中（例如整体业务运行模式不清晰或缺乏企业级的治理动力），这种支持和参与尤其显得重要。

利用 COBIT 驱动的动力应解决实际业务需要和问题，并非仅作用于其本身。管理层应当识别并接受缘于当前问题和驱动因素作为待解决的需求。基于 COBIT 的高层健康度检查、诊断或能力评估是提高意识、达成共识和承诺一致行动的卓越工具。必须从一开始就征求有关利益相关者的承诺和认可。为实现这一点，实施目的和收益需要在业务说明中予以清晰表述，并通过案例概述予以总结。

一旦得到承诺，就需要为该项目集提供充分的资源支持，定义并分派关键角色和责任。需要持续谨慎地维护来自各个受影响的利益相关者的承诺。

应建立和维护适当的监督指导的结构和流程。这些结构和流程还应确保与企业范围内的治理和风险管理方法始终一致。

关键利益相关者应提供明确的支持和承诺，例如，董事会和行政管理层设定“高层基调”并确保各级对项目集的承诺。

识别痛点和触发事件

有若干种因素预示着企业有改善 IT 治理和管理的需要。

采用痛点或触发事件作为实施计划的起始点，企业可以将 IT 改进治理和管理的案例与正在经历的日常实际问题联系起来。这将改善项目的受认可程度，在企业内部营造有必要启动实施的紧迫感。此外，针对企业内最显著或最可识别的问题可以通过确定速赢方案以快速证明增值。这样就会给引进进一步变革提供一个平台，并有助于获得整个高管层对于更深入的变更的决心和支持。

正如在《COBIT 5 实施指南》中所提到的一些典型痛点示例，新建的或修正过的 IT 治理和管理的动力可以作为解决方案（或其中的一部分），这些典型痛点包括：
- 由举措失败、IT 成本上升和低业务价值所导致的业务挫折感
- 与 IT 风险相关的重大事故，如数据泄露或项目失败
- 外包服务的交付问题，如持续违背商定的服务水平
- 未能满足监管或合同要求
- 企业的创新能力和业务敏捷性受限于 IT 水平
- 关于不良 IT 绩效的定期审计结果或报告的 IT 服务质量问题
- 隐藏性的或欺诈性的 IT 费用
- 举措之间存在重复或重叠，或是浪费资源，如未成熟的项目终止
- IT 资源不充足，人员未具备充分的技能，或人员懈怠/不满意
- IT 驱动的变更未能满足业务需要并且交付延迟或超出预算
- 董事会成员、高管或高级经理不愿意参与 IT，或缺乏信守承诺、满意的 IT 业务发起人
- 复杂的 IT 运营模式

除上述痛点外，企业内外部环境中的其他事件也可能昭示或触发对IT治理和管理的关注。《COBIT 5 实施指南》第三章中所给出的示例如下：
- 合并、收购或资产剥离
- 市场、经济或竞争地位的转变
- 业务运行模式或采购协议的变更
- 新的监管或合规要求

- 重大技术变更或范式转移
- 一项全面企业的治理重点或项目
- 一位新的首席执行官、首席财务官、首席信息官等
- 外部审计或咨询评估
- 新的业务战略或优先事项

启动变更

成功实施取决于以适当的方式执行适当的变更（适当的治理和管理动力）。在很多企业中，明显的关注是放在第一方面——即 IT 的核心治理或管理——但不够重视管理变更相关的人员、行为和文化方面以及对利益相关者的激励。

我们不应该侥幸地认为，各种利益相关者在被涉及到或受某些新的或修正的动力影响时会心甘情愿地接收和采纳变更。无视和/或抵制变更的可能性需要以结构化和积极的方法予以解决。同时，应该通过明确的沟通计划达到实施项目的最佳共识，这项沟通计划应界定整个项目集中各个阶段的沟通内容、沟通方式和沟通对象。

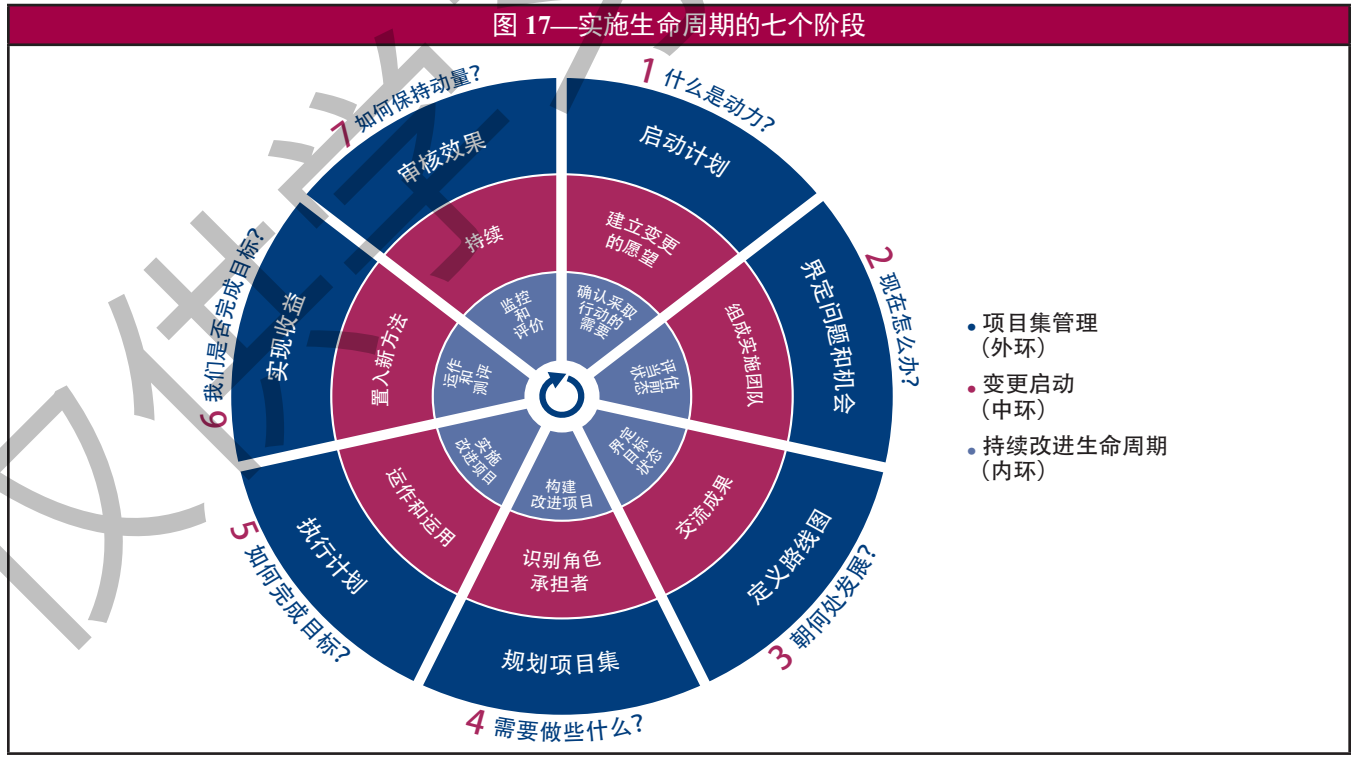
通过获得利益相关者的承诺（在赢得民意、领导的时间、加强沟通和对員工的响应等方面的投入），或如仍有必要，通过强制实施合规要求（对管理、监控和执行流程的投入），可以实现持续性的改进。换言之，需要克服人员、行为、文化等方面的障碍，以便形成合力来适当地采纳变更，灌输采纳变更的意志，并确保采纳变更的能力。

生命周期法

实施生命周期为企业提供了一种利用 COBIT 来解决在实施期间遇到的典型复杂问题以及挑战的方法。生命周期的三个互为联系的组成部分分别是：
1. 核心持续改进生命周期——这不是一次性项目。
2. 启动变更——解决行为和文化方面的问题。
3. 项目集管理。

如上述所讨论的一样，需要创造适当的环境以确保实施或改进计划的成功。生命周期及其七个阶段如图 17 所示。

图 17—实施生命周期的七个阶段



第一阶段开始识别和商定实施或改进计划的需求，这一阶段确定当前的痛点和触发事件，并在行政管理层营造出变更的愿望。

第二阶段关注于如何利用 COBIT 中企业目标与 IT 相关目标以及关联 IT 流程之间的映射关系来界定实施或改进计划的范围，并考虑风险场景来突出需要关注的关键流程。高层诊断对于需要关注的高优先级领域的界定和理解也非常有用。然后进行当前状态的评估，通过执行一项流程能力评估来发现问题和缺陷。大规模计划应根据生命周期的多次迭代予以架构---因为任何超过六个月的实施计划都存在失去利益相关者的动力、关注和全身心投入等方面的风险。

在**第三阶段**中，应设定一项实施目标，然后进行更为详细的分析，利用 COBIT 的指导作用以识别差距和潜在的解决方案。一些解决方案可以是速赢方案，而其余的应该是更具挑战的和长期性的活动。应优先考虑较易于实现的、和有可能产生最大收益的计划。

第四阶段应通过界定合理的业务案例所支持的项目，计划实际的解决方案。还应开发一项实施变更计划。一项完备的业务案例有助于确保项目的收益得到确认和监控。

在**第五阶段**中，建议的解决方案应在日常实践中予以实施。应界定衡量标准并形成监控机制，使用 COBIT 的目标和指标以确保实现和维护业务一致性，并可以测评绩效。要达到成功需要最高管理层的参与和坚定的承诺以及受影响的业务和 IT 利益相关者拥有主人翁精神。

第六阶段关注于新的或改良的动力的持续运行，以及对于其预期收益实现的监控。

在**第七阶段**中，对计划的整体成功进行审验，确认企业 IT 治理和管理的进一步需求，并强化持续改进的要求。

随着时间的推移，在构建企业 IT 治理和管理的可持续性方法的同时，生命周期应循环跟进。

起步：开发业务案例

为确保借力 COBIT 的实施计划成功，在企业内部，对采取行动的需求应广为认识并进行广泛的沟通。可行的方式包括“警钟”式（如前述所讨论，在体验到具体痛点之时），或是表达寻求改善的机会，而且非常重要的一点是，提出有待实现的收益目标。需要逐步灌输一种适当的紧迫感，而且关键利益相关者应意识到不采取措施的风险以及落实这些项目的收益。

计划应属发起人所有，应包括所有关键利益相关者，并应以一个业务案例为基础。首先，可以从高层次战略的角度开始——自上而下——先要明确理解预期实现的业务成果，进而详细描述紧要任务和里程碑以及关键角色和职责。业务案例在管理层指导创造业务价值时是一个非常有价值的工具。业务案例最低限度应包括以下内容：

- 锁定的业务收益目标及其与业务战略的一致性，和相关收益的所有者（业务上负责获取收益者）。这些可以采用痛点和触发事件作为依据。
- 创造预期价值所需的业务变更。这可以基于健康度检查和能力差距分析，并应清楚说明范围内和范围外的具体内容。
- 进行企业 IT 治理和管理变更所需的投资（以必需的项目估算为依据）。
- 持续运营所需的 IT 和业务成本。
- 采用已变更方式运营的预期收益。
- 前述项目中固有的风险，包括任何制约条件和依存关系（基于挑战和成功因素）。
- 计划相关的角色、职责和责任。
- 在整个经济生命周期中如何监控投资和价值创造，以及要使用的指标（基于目标和指标）。

业务案例并非一次性的静态文件，而是一种动态的运营工具，必须持续更新以反映未来的当前视图，从而维护项目可行性的概略图。

量化实施或改进计划的收益可能较为困难，因此应特别注意只关注实际的和能实现的收益。对大量企业进行的研究可以提供关于已实现收益的有用信息。

示例 6—治理的统计

IT 治理研究院（ITGI）委托普华永道（PwC）在二十一个国家中对 800 多个 IT 和业务受访者进行了一次关于 IT 治理的市场研究项目[7]。38% 的受访者列举 IT 治理实践的成果为降低了 IT 成本，28.1% 的受访者认为是改善企业竞争力，而 27.1% 的受访者认为是改善 IT 投资回报。此外，也有若干无形收益的报告，例如改善 IT 相关风险的管理（42.2% 的受访者），改善业务和 IT 之间的沟通和关系（39.6% 的受访者）和改善对业务目标的 IT 交付（37.3% 的受访者）。

ISACA 也进行了有关探索和验证 COBIT 业务价值的研究[8]。从研究得到的数据集提供了很多分析机会，并澄清了企业 IT 治理和业务绩效之间的关系。

一项在全球 250 多家企业中开展的研究表明，就相同的目标而言[9]，那些具有优异的 IT 治理的企业较之于治理较差的企业至少提高了百分之二十以上的收益率。这项研究强调，IT 业务价值直接源自于有效的 IT 治理。

最后，另一项在航空业中进行的研究案例得出的结论是，企业 IT 治理的实施和持续鉴证恢复了业务和 IT 之间的信任，导致投资和战略目标之间的一致性增强。在本案例中还有更实际的收益报告，这包括每一业务生产单元的 IT 持续性成本降低，因而可以抽出资金用于创新。其他在金融界进行的跨案例研究也证明，采用更佳 IT 治理方法的机构明显获得较高的业务/IT 一致性和成熟度分数。[10]

[7] ITGI, *全球企业 IT 治理状况报告(GEIT)*—2011, USA, 美国 2011, *www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Global-Status-Report-on-the-Governance-of-Enterprise-IT-GEIT-2011.aspx*

[8] ISACA, *为 COBIT® 构建业务案例以及 Val IT™ 管理层简报*, 美国, 2009, *www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Building-the-Business-Case-for-COBIT-and-Val-IT-Executive-Briefing.aspx*

[9] Weill, Peter; Jeanne W. Ross; *IT 治理：高层执行者如何管理 IT 决策权以取得优异成果*，哈佛商学院出版社, 美国, 2004

[10] De Haes, Steven; Dirk Gemke; John Thorp; Wim Van Grembergen; '透过 Val IT 分析 KLM 的 IT 价值管理', *ISACA 期刊*, 2011, 第四卷. Van Grembergen, Wim; Steven De Haes; *企业 IT 治理：实现一致性和价值*, 施普林格出版社, 美国, 2009

本页特此留空

第八章
COBIT 5 流程能力模型

导言

COBIT 4.1、IT 价值管理（Val IT）和 IT 风险管理（Risk IT）的用户对包含在那些框架中的流程成熟度模型非常熟悉。这些框架是用于测评当前的或“原样的”企业 IT 相关流程的成熟度，并界定某种必需达到的成熟度的状态，和测定流程之间的差距以及如何改进流程以实现希望达到的成熟度。

COBIT 5 产品集包括一种基于国际公认的《ISO/IEC 15504 软件工程--流程评估标准》的流程能力模型。这一模型将会实现流程评估和流程改进支持的相同整体目标，例如，这种模型可提供一种手段以测评任何治理流程（基于EDM）或管理流程（基于PBRM）的绩效，并为有待识别的改进留有余地。

然而，这种新模型在设计和使用上与 COBIT 4.1 不同，因此有必要讨论以下话题：
- COBIT 5和 COBIT 4.1 模型之间的差别。
- COBIT 5模型的优势。
- COBIT 5用户在实践中会遇到的差别概述。
- 进行基于 COBIT 5模型的能力评估。

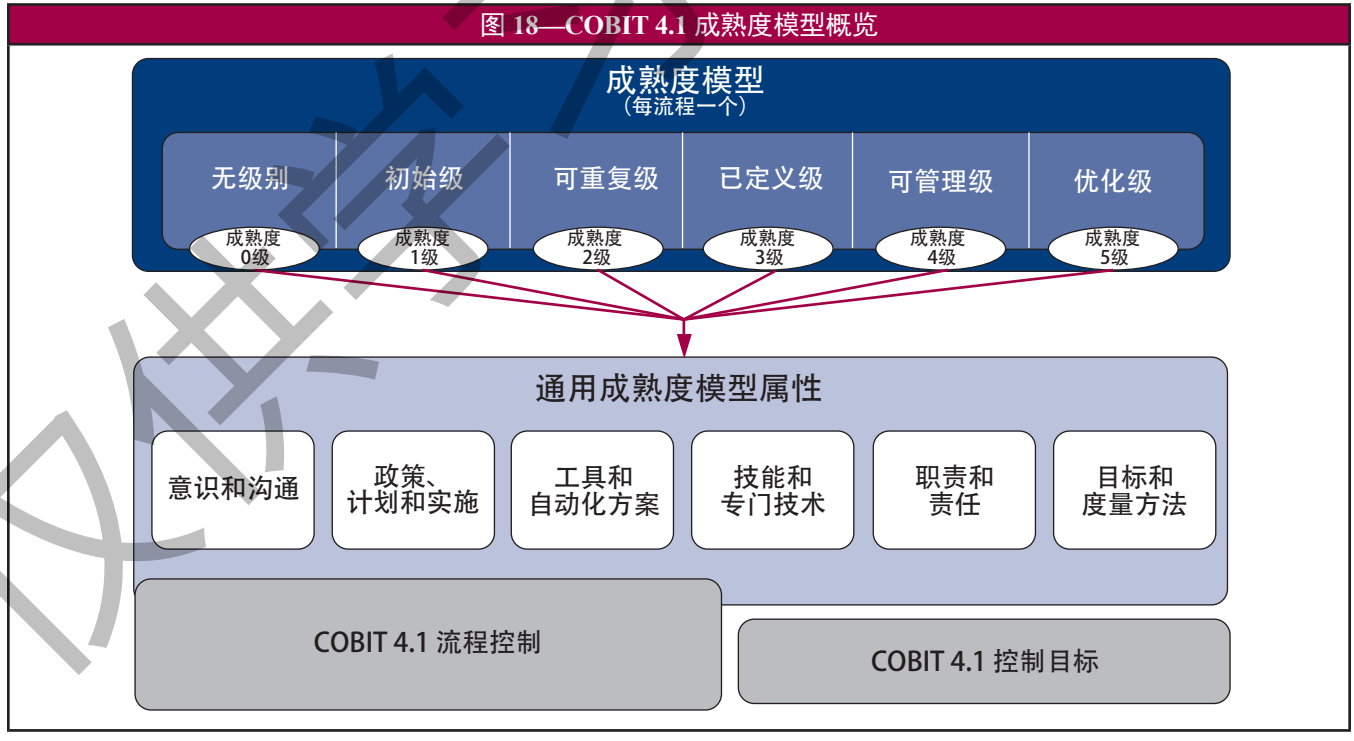
有关COBIT 5能力评估方法的详细情况参见ISACA出版物《COBIT® 流程评估模型（PAM）：使用 COBIT® 4.1》。[11]

虽然本方法将提供有关流程状态的有价值的信息，但流程仅只是七大治理和管理动力之一。因此，流程评估并不代表某一企业治理状态的全局情况。为此，其他动力也需要予以评估。

COBIT 4.1 成熟度模型与 COBIT 5 流程能力模型之间的差别

COBIT 4.1成熟度模型方法要素如**图 18** 所示：

图 18—COBIT 4.1 成熟度模型概览

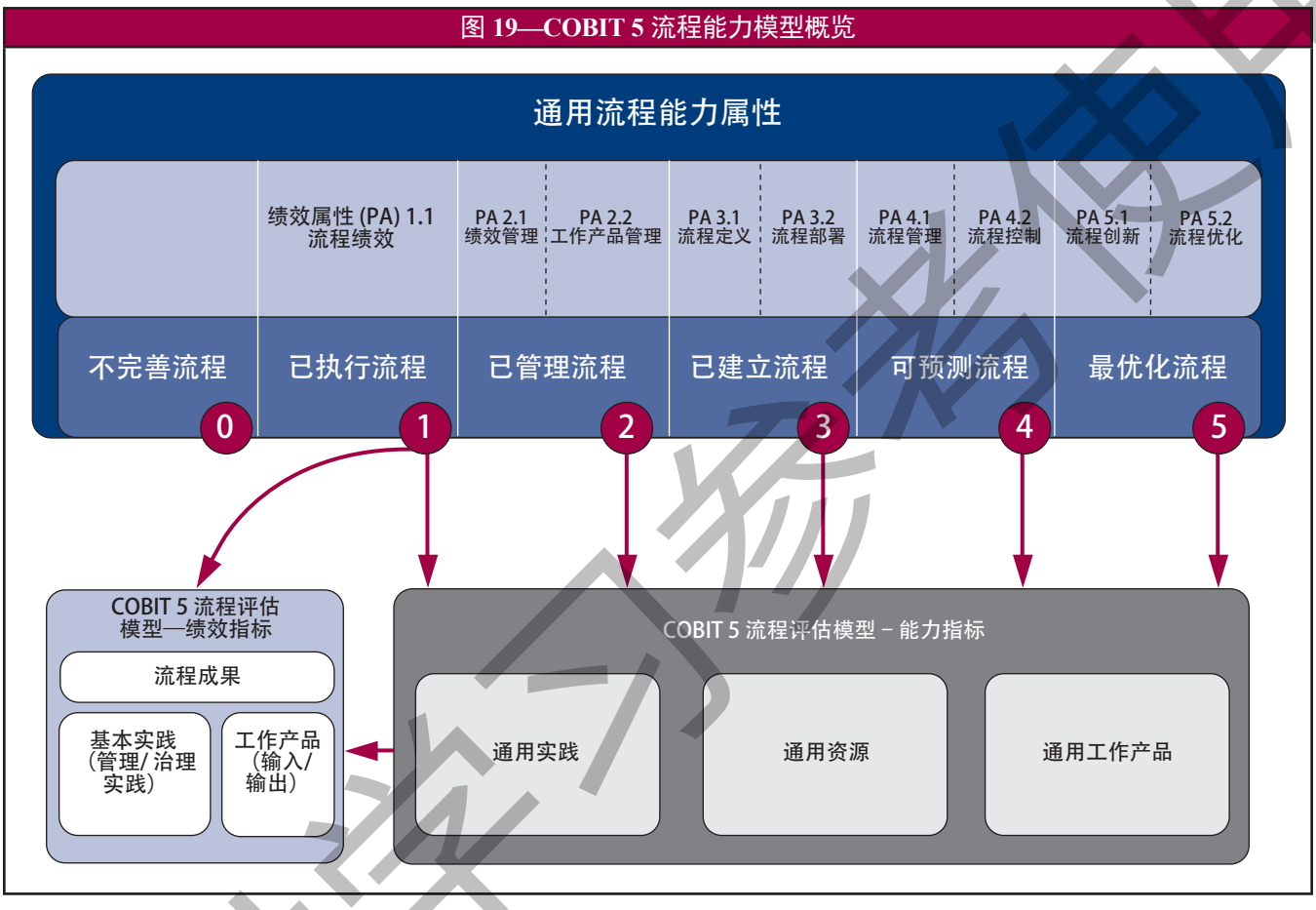


[11] *www.isaca.org/cobit-pam*

运用 COBIT 4.1 成熟度模型来进行流程改进——评估某一流程的成熟度，界定某一目标成熟度等级和识别差距——需要使用以下 COBIT 4.1 组分：
- 首先，需要评估流程控制目标是否满足；
- 其二，包含在每一流程管理指南中的成熟度模型可用于获得流程成熟度概况；
- 此外，COBIT 4.1 的通用成熟度模型提供六种截然不同的属性，适用于每一流程，并协助获得有关流程成熟度等级 的更详细的测评；
- 流程控制为通用控制目标——当评估流程时也需要审核。流程控制可能会与部分成熟度模型属性重叠。

COBIT 5 流程能力方法可总结为如**图 19** 所示：

图 19—COBIT 5 流程能力模型概览



一种流程可能实现的能力分为六个层级，包括所谓的“不完善流程”，这种情况的出现是因为该流程中的实践不能实现试图达到的目的：
- **0 不完善流程**— 流程不可实施或未能实现其目的。处于这种等级时，几乎没有或根本不存在任何流程目的的系统性成绩的证明。
- **1 已执行流程**（一种属性）—已实施流程实现了其流程目的。
- **2 已管理流程**（两种属性）—前述已执行流程已经在管理方式下实施（计划的、监控的和调整的），而且其工作产品已适当建立、控制和维护。
- **3 已建立流程**（两种属性）—前述已管理流程已经采用一种能够实现其目的的规定流程予以实施。
- **4 可预测流程**（两种属性）—前述已建立流程已经在规定限值内运行以实现其流程结果。
- **5 最优化流程**（两种属性）—前述可预测流程正在持续改进以符合有关的当前的或计划了的业务目标。

每一个能力层级只有当下一个层级完全实现后才能实现。例如，一个第三级的流程能力（已建立流程）需要其流程定义和流程部署等属性已大部分完成，并且只有在第二级流程能力（已管理流程）的属性已完全实现后才会得以实现。

在流程能力第一级与较高能力等级之间存在一个重大差别。流程能力第一级的实现要求流程绩效属性大部分得以实现，这实际上就意味着企业正在成功地执行流程并获得了要求的成果。然后，较高的能力等级再添加了不同的属性。在这种评估方案中，实现了一项能力的第一级，乃至达到第五级，就已经是企业的一项重要成绩。需要注意的是，每一个企业应选择（基于成本效益和可行性等理由）其目标或想达到的级别，而且绝少是最高的级别。

在基于 ISO/IEC 15504 的流程能力评估和当前的 COBIT 4.1 成熟度模型（以及类似的基于 Val IT 和 Risk IT 领域的成熟度模型）之间最重要的差别可总结如下：
- 以 ISO/IEC 15504 标准定义的能力等级的命名和含义与当前的 COBIT 4.1 流程成熟度等级截然不同。
- 在 ISO/IEC 15504 标准中，能力等级是由一套九个流程属性予以界定。这些属性覆盖了部分的当前 COBIT 4.1 流程成熟度和/或流程控制覆盖的范围，但在程度上有别和以不同的方式。

对一项 ISO/IEC 15504:2 合规的流程参考模型的要求规定，在描述将要评估的任何流程时，如，任何 COBIT 5 治理和/或管理流程：
- 流程是根据其目的和成果予以描述；
- 流程描述将不包含任何超出测评框架第一级的内容，这就意味着任何超出第一级的流程属性特征均不能出现在流程描述中。无论某一流程是否被测评和监控，或是否正式予以描述等等，均不可能成为其他流程描述或其隶属的管理实践/活动之一部分。这就意味着包括在《COBIT 5：启用流程》中的流程描述仅仅只包含实现实际流程目的和目标的必要步骤。
- 从前述要点来看，适用于所有企业流程的共同属性，原来在《COBIT®》（第三版）出版物中形成重复的控制目标，并被归合于COBIT 4.1的流程控制（PC）目标之中，现在则被定义于评估模型的第二至第五级

实践中的差别 [12]

如前所述，在流程评估模型变更时很显然存在一些实际上的差异。用户需要意识到这些变更，并将这些变更在其行动计划中纳入考虑。

应考虑的主要变更包括：
- 鉴于明显存在著相似的记数法和用于描述的词汇，尽管比较 COBIT 4.1 和 COBIT 5 之间的评估结果非常诱人，但这样的比较并非易事，原因如**图 20** 所示在于范围、重点和意图上的差别。
- 一般而言，COBIT 5 流程能力模型的分数要低些，如**图 20** 所示。在 COBIT 4.1 成熟度模型中，一个流程可能达到第一级或第二级，无需全部实现所有的流程目标；在 COBIT 5 流程能力级别中，这可能或导致 0 或 1 的较低分数。

COBIT 4.1 和 COBIT 5 的能力范围可“映射”大致如**图 20** 所示。
- 在 COBIT 5 中不再在详细流程内容中包含每一流程的具体成熟度模型，因为 ISO/IEC 15504 流程能力评估方法对此不作要求，甚至禁止这种方法。反而，这种方法界定了“流程参考模型”（用于评估的流程模型）所需要的信息：
  - 带目的说明的流程描述；
  - 基本实践，相当于 COBIT 5 词汇中的流程治理和管理实践；
  - 工作产品，相当于 COBIT 5 词汇中的输入和输出。
- COBIT 4.1 成熟度模型生成企业的成熟度概要。这种概要的主要目的就是识别在何种维度中或何种属性中存在具体需要改进的缺点。当着重改进而非需要为报告目的的某一成熟度数字时，企业会使用这种方法。在 COBIT 5 中，评估模型为每一种能力属性提供一种衡量尺度，并指导如何运用，因此对于每一流程，均可就九种能力属性中的任何一种进行评估。
- COBIT 4.1 中的成熟度属性和 COBIT 5 中的流程能力属性并不相同，它们在某种程度上相互重叠或映射，如**图 21** 所示。已经使用 COBIT 4.1 成熟度模型属性法的企业可以重复使用其现有评估数据，并依照**图 21** 的 COBIT 5 属性评估，对这些数据予以重新分类。

[12] 有关更多基于新 ISO/IEC 15504 标准的 COBIT 评估方案，参见 *www.isaca.org/cobit-assessment-programme*.

图 20—成熟度级别（COBIT 4.1）和流程能力级别（COBIT 5）比较表		
COBIT 4.1 成熟度级别	**基于 ISO/IEC 15504 的流程能力**	**应用环境**
5 优化级— 基于持续改进的结果及外部组织的成熟度模型，工作流程已被优化为最佳实践。IT 作为一个整体以使工作流程自动化、提供改进工作质量和效率的工具、使企业快速适应。	**5 级：最优化流程**—4 级可预测流程仍持续改进以符合当前和预期的相关业务目标	**企业角度—公司知识**
4 可管理级—管理层监控和衡量对程序的遵循性，并在流程失效时采取必要的纠正措施；工作流程已处于持续改进中并能作为最佳实践；自动化和工具在有限范围内分散使用。	**4 级：可预测流程**—3 级已建立流程已在规定限值内运营以实现其流程成果。	
3 已定义级—已建立标准化的书面程序，并通过正式的培训进行贯彻；虽已明确要求工作中必须遵循这些流程，但未能检测到偏离流程的现象；程序本身还不尽完善，只是现有工作惯例的正式化。	**3 级：已建立流程**—采用一种能够实现其流程结果的规定流程，已经实施了 2 级已管理流程。	
	2 级：已管理流程— 1 级已执行流程已经在管理方式下实施（计划的、监控的和调整的），而且其工作产品已适当建立、控制和维护。	**实例角度—个人知识**
2 可重复级—已建立工作流程使不同人员在执行相同任务时能够采用类似的操作程序，但组织未对这些流程实施正式的培训和贯彻，其职责仍停留在个人阶段；实际工作对个人知识与能力存在很强的依赖性，错误时有发生。	**1级：已执行流程**—已实施流程实现了其流程目的。 **备注：如果流程结果未能实现，则有可能是，某些分类为成熟度模型 1 的流程根据 15504 标准则被分类为 0 级。**	
1 初始级—组织已意识到问题存在并需要加以解决，但没有标准的工作流程，仍然基于个人与一事一办原则采用临时解决办法；管理缺乏统筹规划。		
0 无级别—完全没有可识别的流程，组织还未意识到需要解决的问题。	**0 级：不完善流程**—流程尚未实施或未能实现其目的。	

图 21—成熟度属性（COBIT 4.1）和流程能力属性（COBIT 5）比较表									
	COBIT 5 流程能力属性								
COBIT 4.1 成熟度属性	**流程绩效**	**绩效管理**	**工作产品管理**	**流程定义**	**流程部署**	**流程管理**	**流程控制**	**流程创新**	**流程优化**
意识和沟通				■	■	■			
政策、计划和实施程序							■		
工具和自动化方案				■					
技能和专门技术				■	■				
职责和责任				■					
目标和度量方法		■				■			

变更的优势

较之于 COBIT 4.1 成熟度模型，COBIT 5 流程能力模型的优势包括：
- 重点更加关注于流程的执行，并确认流程实际达到目的和交付预期所必需的成果。

- 通过消除重复而简化内容，因为 COBIT 4.1 成熟度模型评估需要使用大量的特定组件，包括通用成熟度模型、流程成熟度模型、控制目标和流程控制以支持流程评估。
- 改善的流程能力评估活动和评价的可靠性和可重复性，减少了利益相关者之间就评估结果所产生的争议和分歧。
- 增强的流程能力评估结果的可使用性，因为新模型为出于内外部目的所进行的更正式、更严格的评估建立了一种依据。
- 符合公认的流程评估标准，因此能与市场上的流程评估方法紧密配套。

执行 COBIT 5 流程能力评估

ISO/IEC 15504 标准规定，流程能力评估可基于各种目的和采用不同的严格程度来执行。其目的可以针对内部，重点关注企业各领域间的比较和/或流程改进以增进内部收益，或可针对外部，以正式评估，报告和认证为重点。

COBIT 5 基于 ISO/IEC 15504 的评估方法继续促进实现自 2000 年以来已成为 COBIT 的关键方法的以下目标：
- 使治理机构和管理层能够设定流程能力的基准；
- 使高层级的“现状”和“将来”健康度检查能够支持治理机构和管理层关于流程改进的投资决策；
- 提供差距分析和改进计划信息以支持定义合理的改进项目；
- 为治理机构和管理层提供评估分级以衡量和监控当前能力。

本节描述了如何利用 COBIT 5 流程能力模型进行一种高层级评估以实现这些目标。

评估区分出评估能力 1 级和更高级别之间的差异。实际上，如前所述，流程能力 1 级描述了一个流程是否实现其既定的目的，因此是一个非常重要应实现的级别——并且是达到更高能力水平的基础。

评估流程是否实现其目标—或换言之，达到能力级别 1——可通过以下方面来实现：
1. 根据每一流程的详细流程描述来审核流程结果。并使用 ISO/IEC 15504 评定量表对每一目标达到的程度分级。该评定量表由以下评定指标构成：
   - **N**（未达到）—在评估的流程中几乎或根本没有达到规定属性的证据。（0–15 达到百分比）
   - **P**（部分达到）—在评估的流程中有某种针对的方法或达到规定属性的部分证据。欲达到属性的某些方面则未必能預测。（15–50 达到百分比）
   - **L**（大部分达到）—在评估的流程中有系统性方法和显著达到规定属性的证据。但在评估的流程中可能存在与本属性相关的部分缺点。（50–85 达到百分比）
   - **F**（全部达到）—在评估的流程中有完备的系统性方法和完全达到规定属性的证据。在评估的流程中不存在与本属性相关的重大缺点。（85–100 达到百分比）
2. 此外，使用相同的评定量表，可评估流程（治理和管理）的实践，以体现出基本实践运用达到何种程度。
3. 为进一步精确评估，还可将工作产品纳入考虑范围以确定特定评估属性已经达到的程度。

尽管规定的目标能力级别是由每个企业来决定，但很多企业都雄心勃勃地想使其全部的流程达到能力 1 级。（否则这些流程的意义何在呢？）如果没有达到这一级别，其未能达到的原因就能迅速从上述解释的方法中得到，并可界定一项改进计划：
1. 如果一项必要的流程结果未能一贯达到，则该流程不符合其目标，并需要改进。
2. 流程实践的评估将揭示出哪些实践缺乏或未能奏效，应该实施和/或改进那些实践以使所有要求的流程结果均能达到。

就较高流程能力级别而言，可使用 ISO/IEC 15504:2 中的通用实践活动，这些实践为每一个流程能力级别提供了通用的描述。

本页特此留空

附件 A
参考文献

以下框架、标准和其他指南用于 COBIT 5 开发的参考资料和输入。

项目管理协会 (APM)；*APM项目集管理介绍*，Latimer, Trend and Co., 英国，2007

英国标准协会 (BSI)，BS25999:2007 业务连续性管理标准，英国，2007

美国首席信息官委员会，*联邦企业架构* (FEA)，版本 1.0，美国，2005

欧洲委员会，*委员会企业 IT 架构框架 (CEAF)*，比利时，2006

Kotter, John; *领导变革*，哈佛商学院出版社，美国，1996

女王陛下政府，最佳管理实践组合，*管理成功的项目集 (MSP)*，英国，2009

女王陛下政府，最佳管理实践组合，*PRINCE2®*, 英国，2009

女王陛下政府，最佳管理实践组合，信息技术基础设施资料库 (*ITIL®*), 2011

国际标准化组织 (ISO), 9001:2008 质量管理标准，瑞士，2008

ISO/国际电工委员会 (IEC), 20000:2006 IT 服务管理标准，瑞士，2006

ISO/IEC, 27005:2008, 信息安全风险管理标准，瑞士，2008

ISO/IEC, 38500:2008, 信息技术标准的公司治理，瑞士，2008

最高治理原则法典（最高法案 III），南非，2009

经济合作和发展组织 (OECD)，OECD 公司治理原则，法国，2004

开放群组，TOGAF® 9（企业架构框架 9.0 版），英国 2009

项目管理协会，《项目管理知识体系指南》(PMBOK2®)，美国，2008

英国财务报告理事会，‘关于公司治理的合并规范’，英国，2009

本页特此留空

附件 B
企业目标与IT 相关目标之详细映射图

COBIT 5 目标层级解释见第二章。

图 22 中映射图的目的在于证明企业目标是如何得到支持（或转化成） IT 相关的目标。为此，该图包含以下信息：
- 在各列中，所有 17 个 COBIT 5 规定的通用企业目标按平衡计分卡（BSC）维度分组；
- 在各行中，IT 相关目标也按照 IT BSC 维度分组；
- 一份每一企业目标如何得到 IT 相关目标支持的映射图。这份映射图使用以下量度表示：
  - ‘P’ 代表主要，说明存在重要关系，例如，IT 相关目标是企业目标的主要支持。
  - ‘S’ 代表次要，说明存在坚实的但重要性稍弱的关系，例如，IT 相关目标是企业目标的次要支持。

示例 7—映射图

映射图意味着在正常情况下，用户可以期望：
- 企业目标 7. 业务服务持续性和可用性将：
  - 主要取决于 IT 相关目标的实现：
    - 04 管理的 IT 相关业务风险
    - 10 信息，处理基础设施和应用程序的安全
    - 14 用于决策之可靠和有用的信息的可用性
  - 并在较低程度上取决于 IT 相关目标的实现：
    - 01 IT 和业务战略的一致性
    - 07 符合业务要求的 IT 服务交付
    - 08 应用程序、信息和技术解决方案的充分利用
- 反方向使用映射图，达到 IT 相关目标 09. IT 敏捷性将为若干个企业目标的实现做出贡献：
  - 主要的企业目标：
    - 2. 竞争性产品与服务的组合
    - 8. 对变化的企业环境敏捷的反应
    - 11. 业务流程功能性优化
    - 17. 产品和业务创新的文化
  - 在稍次之的程度上，企业目标：
    - 1. 商务投资的利益相关者价值
    - 3. 管理的业务风险（资产保障）
    - 6. 以顾客为中心的服务文化
    - 13. 管理的业务变更方案
    - 14. 运营及员工生产率
    - 16. 熟练的有进取心的人员。

该图依照以下输入创建：
- 安特卫普大学管理学校 IT 配合与治理研究所的研究成果
- COBIT 5 开发和审核过程获得的附加评论和专家意见

当使用图 22 中的映射图时，请考虑第二章中就如何使用 COBIT 5 目标分层所作的备注。

图 22—COBIT 5 企业目标与 IT 相关目标映射图

			企业目标																
			商务投资的利益相关者价值	竞争性产品与服务的组合	管理的业务风险（资产保障）	外部法律法规的合规性	财务透明度	以顾客为中心的服务文化	业务服务的持续性和可用性	对变化的企业环境敏捷的反应	信息为本的战略性决策	服务交付成本优化	业务流程功能性优化	业务流程成本优化	管理的业务变更方案	运营及员工生产率	内部政策合规性	熟练的有进取心的人员	产品和业务创新的文化
			1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.	16.	17.
IT 相关目标			**财务**					**客户**					**内部**					**学习和成长**	
财务	01	IT 与业务战略的一致性	P	P	S			P	S	P	P	S	P	S	P			S	S
	02	IT 合规和对业务的外部法律法规合规的支持			S	P											P		
	03	行政管理层对进行 IT 相关决策的承诺	P	S	S					S	S		S		P			S	S
	04	管理的 IT 相关业务风险			P	S			P	S		P			S		S	S	
	05	从 IT 驱动的投资和服务组合中实现的收益	P	P				S		S		S	S	P		S			S
	06	IT 成本、收益和风险的透明度	S		S		P				S	P		P					
客户	07	符合业务要求的 IT 服务交付	P	P	S	S		P	S	P	S		P	S	S			S	S
	08	应用程序、信息和技术解决方案的充分利用	S	S	S			S	S		S	S	P	S		P		S	S
内部	09	IT 敏捷性	S	P	S			S		P			P		S	S		S	P
	10	信息，处理基础设施和应用程序的安全			P	P			P								P		
	11	IT 资产、资源和能力的优化	P	S						S		P	S	P	S	S			S
	12	通过将应用程序和技术整合进业务流程之中来推动和支持业务流程	S	P	S			S		S		S	P	S	S	S			S
	13	准时、按预算提交收益和满足要求和质量标准的项目集交付	P	S	S			S				S		S	P				
	14	用于决策之可靠和有用的信息的可用性	S	S	S	S			P		P		S						
	15	IT 对内部政策的合规性			S	S											P		
学习和成长	16	胜任的有进取心的业务和 IT 人员	S	S	P			S		S						P		P	S
	17	业务创新的知识、专门技术和首创精神	S	P				S		P	S		S		S			S	P

附件 C
IT 相关目标与 IT 相关流程之详细映射图

本附件包含 IT 相关目标与支持这些目标的 IT 相关流程的映射图，并作为第二章中所解释的目标分层之一部分。

图 23 包括：
- 在各列中，第二章定义的所有 17 个通用 IT 相关目标，并按 IT 平衡计分卡（BSC）维度分组；
- 在各行中，所有 37 个 COBIT 5 的流程按领域分组；
- 每一个 IT 相关目标是如何得到 COBIT 5 IT 相关流程支持的映射图，并使用以下量度来表示：
  - 'P' 代表主要，说明存在重要关系，例如，该 COBIT 5 流程是实现某一 IT 相关目标的主要支持。
  - 'S' 代表次要，说明存在坚实的但重要性稍弱的关系，例如，该 COBIT 5 流程是实现某一 IT 相关目标的次要支持。

示例 8—APO13 管理安全
流程 "APO13- *管理安全*" 将有助于： • 主要对于实现下列 IT 相关目标作出贡献： – 02 IT 合规和对业务的外部法律法规合规的支持 – 04 管理的 IT 相关业务风险 – 06 IT 成本、收益和风险的透明度 – 10 信息、处理基础设施和应用程序的安全 – 14 用于决策之可靠和有用的信息的可用性 • 并在较低程度上，对于 IT 相关目标的实现： – 07 符合业务要求的 IT 服务交付 – 08 应用程序、信息和技术解决方案的充分利用

该图是依照以下输入创建：
- 安特卫普大学管理学校 IT 配合与治理研究所的研究成果
- COBIT 5 开发和审核过程获得的附加评论和专家意见

使用图 23 的映射图时，请考虑第二章中就如何使用 COBIT 5 目标分层所作的备注。

图 23—COBIT 5 IT相关目标与流程之间的映射图

			IT 相关目标																
			IT与业务战略的一致性	IT合规和对业务的外部法律法规合规的支持	行政管理层对进行IT相关决策的承诺	管理的IT相关业务风险	从IT驱动的投资和服务组合中实现的收益	IT成本、收益和风险的透明度	符合业务要求的IT服务交付	应用程序、信息和技术解决方案的充分利用	IT敏捷性	信息、处理基础设施和应用程序的安全	IT资产、资源和能力的优化	过应程和术合业流之来动支业流通将用序技整进务程中推和持务程	准时、预提收和足求质标的目交益满要及量准项集付	用于决策之可靠和有用的信息的可用性	IT对内部政策的合规性	胜任的有进取心的业务和IT人员	业务创新的知识、专门技术和首创精神
			01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17
COBIT 5 流程			财务						客户		内部							学习和成长	
评价、指导和监控	EDM01	确保治理框架的设定和维护	P	S	P	S	S	S	P		S	S	S	S	S	S	S	S	S
	EDM02	确保收益交付	P		S		P	P	P	S			S	S	S	S		S	P
	EDM03	确保风险优化	S	S	S	P		P	S	S		P			S	S	P	S	S
	EDM04	确保资源优化	S		S	S	S	S	S	S	P		P		S			P	S
	EDM05	确保利益相关者的透明度	S	S	P			P	P						S	S	S		S
定位、计划和组织	APO01	管理 IT 管理框架	P	P	S	S			S		P	S	P	S	S	S	P	P	P
	APO02	管理战略	P		S	S	S		P	S	S		S	S	S	S	S	S	P
	APO03	管理企业架构	P		S	S	S	S	S	S	P	S	P	S		S			S
	APO04	管理创新	S			S	P			P	P		P	S		S			P
	APO05	管理投资组合	P		S	S	P	S	S	S	S		S		P				S
	APO06	管理预算和成本	S		S	S	P	P	S	S			S		S				
	APO07	管理人力资源	P	S	S	S			S		S	S	P		P		S	P	P
	APO08	管理关系	P		S	S	S	S	P	S			S	P	S		S	S	P
	APO09	管理服务协议	S			S	S	S	P	S	S	S	S		S	P	S		
	APO010	管理供应商		S		P	S	S	P	S	P	S	S		S	S	S		S
	APO011	管理质量	S	S		S	P		P	S	S		S		P	S	S	S	S
	APO012	管理风险		P		P		P	S	S	S	P			P	S	S	S	S
	APO013	管理安全		P		P		P	S	S		P				P			

图 23—COBIT 5 IT相关目标与流程之间的映射图（*续*）

			IT 相关目标																
			IT与业务战略的一致性	IT合规和对业务的外部法律法规合规的支持	行政管理层对进行IT相关决策的承诺	管理的IT相关业务风险	从IT驱动的投资和服务组合中实现的收益	IT成本、收益和风险的透明度	符合业务要求的IT服务交付	应用程序、信息和技术解决方案的充分利用	IT敏捷性	信息、处理基础设施和应用程序的安全	IT资产、资源和能力的优化	过应程和术合业流之来动支业流通将用序技整进务程中推和持务程	准时、预提收和足求质标的目交益满要及量准项集付	用于决策之可靠和有用的信息的可用性	IT对内部政策的合规性	胜任的有进取心的业务和IT人员	业务创新的知识、专门技术和首创精神
			01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17
COBIT 5 流程			财务						客户		内部							学习和成长	
构建、购置和实施	BAI01	管理项目集和项目	P		S	P	P	S	S	S			S		P			S	S
	BAI02	管理要求定义	P	S	S	S	S		P	S	S	S	S	P	S	S			S
	BAI03	管理解决方案识别和构建	S			S	S		P	S			S	S	S	S			S
	BAI04	管理可用性和容量				S	S		P	S	S		P		S	P			S
	BAI05	管理组织性变更启用	S		S		S		S	P	S		S	S	P				P
	BAI06	管理变更			S	P	S		P	S	S	P	S	S	S	S	S		S
	BAI07	管理变更验收和移交				S	S		S	P	S			P	S	S	S		S
	BAI08	管理知识	S				S		S	S	P	S	S			S		S	P
	BAI09	管理资产		S		S		P	S		S	S	P			S	S		
	BAI10	管理配置		P		S		S		S	S	S	P			P	S		
交付、服务和支持	DSS01	管理运营		S		P	S		P	S	S	S	P			S	S	S	S
	DSS02	管理服务请求和事故				P			P	S		S				S	S		S
	DSS03	管理问题		S		P	S		P	S	S		P	S		P	S		S
	DSS04	管理持续性	S	S		P	S		P	S	S	S	S	S		P	S	S	S
	DSS05	管理安全服务	S	P		P			S	S		P	S	S		S	S		
	DSS06	管理业务流程控制		S		P			P	S		S	S	S		S	S	S	S
监控、评价和评估	MEA01	监控、评价和评估绩效和合规性	S	S	S	P	S	S	P	S	S	S	P		S	S	P	S	S
	MEA02	监控、评价和评估内部控制系统		P		P		S	S	S		S				S	P		S
	MEA03	监控、评价和评估外部要求合规性		P		P	S		S			S					S		S

本页特此留空

附件 D
利益相关者需要与企业目标

第四章显示了从利益相关者的需要到动力目标的目标分层的各个步骤。第二章包括一份典型的IT治理和管理问题表格。从利益相关者的角度来看，明确这些问题是如何与企业目标产生联系是非常有意思的。因此，**图 24** 将其纳入其中；该图显示出一系列内部利益相关者的需要是如何能与企业目标联系起来。

根据具体的利益相关者需要，本表可用于协助设定企业目标或IT相关目标并进行优先排序。在使用这些表格时，应像使用其他目标分层表时一样采用相同的预防措施，例如，每个企业的个体环境大相径庭，而这些表格不应机械套用，而仅仅是作为一种建议性的通用关系合集。在**图 24** 中，如果某种目标需考虑相关的需要，则利益相关者的需要和企业目标之间的交集填在表中。

图 24—COBIT 5 企业目标与治理和管理问题的映射图

利益相关者需要	1. 商务投资的利益相关者价值	2. 竞争性产品与服务的组合	3. 管理的业务风险（资产保障）	4. 外部法律法规的合规性	5. 财务透明度	6. 以顾客为中心的服务文化	7. 业务服务的持续性和可用性	8. 对变化的企业环境敏捷的反应	9. 信息为本的战略性决策	10. 服务交付成本优化	11. 业务流程功能性优化	12. 业务流程成本优化	13. 管理的业务变更方案	14. 运营及员工生产率	15. 内部政策合规性	16. 熟练的有进取心的人员	17. 产品和业务创新的文化
我怎样才能从 IT 使用中获得价值?终端用户对 IT 服务的质量满意吗?	■	■				■	■						■			■	■
我如何管理 IT 绩效?		■			■				■	■	■	■		■			
我怎样才能以最佳方式利用新技术开发新的战略机遇呢?	■	■						■					■			■	■
我怎样才能以最佳方式构建和架构 IT 部门呢?								■		■	■	■		■	■	■	
我在何种程度上依赖于外部提供商? IT 外包协议的管理程度如何? 我如何获得外部提供商的保障?			■	■						■							
对信息的（控制）要求是什么?				■					■						■		
我是否解决所有 IT 相关的风险?			■				■		■						■		
我运营的 IT 是否有效而灵活?					■		■										
我该怎样控制 IT 成本?我该怎样以最为有效和高效的方式使用 IT 资源?什么是最为有效和高效的采购选项?										■		■		■			
我是否有足够的 IT 人员? 我该如何发展和维护他们的技能?我该如何管理他们的绩效?										■		■		■			
我如何得到 IT 鉴证?				■											■		

图 24—COBIT 5 企业目标与治理和管理问题的映射图（*续*）

利益相关者需要	1. 商务投资的利益相关者价值	2. 竞争性产品与服务的组合	3. 管理的业务风险（资产保障）	4. 外部法律法规的合规性	5. 财务透明度	6. 以顾客为中心的服务文化	7. 业务服务的持续性和可用性	8. 对变化的企业环境敏捷的反应	9. 信息为本的战略性决策	10. 服务交付成本优化	11. 业务流程功能性优化	12. 业务流程成本优化	13. 管理的业务变更方案	14. 运营及员工生产率	15. 内部政策合规性	16. 熟练的有进取心的人员	17. 产品和业务创新的文化
我正在处理的信息是否安全可靠?				■			■								■		
我该如何通过更为灵活的 IT 环境来改善业务敏捷性?	■							■					■			■	■
IT 项目是否会不能交付其承诺的结果?——如果是这样, 原因何在? IT 是否妨碍业务战略的执行?	■	■	■					■			■	■	■				
IT 对于企业的永续发展的关键程度如何?如果 IT 不能发挥作用我该怎么办?	■	■					■										
哪些重业务流程依赖于 IT ? 对业务流程的要求是什么?	■	■									■	■					
IT 运营预算的平均超限是多少? IT 项目超过预算的频率以及金额是多少?					■					■		■		■			
IT 成果有多大部分是用于救急而不是推动企业改善?		■	■									■					
IT 资源是否充足，基础设施是否可用以满足必需的企业战略目标?		■	■		■					■		■					
重大 IT 决策需要多长时间?	■	■			■			■									
整个 IT 投入和投资是否透明?		■		■	■										■		
IT 是否支持企业遵守法规和服务等级? 我怎样才知道是否与遵循了所有适用法规?				■											■		

附件 E
COBIT 5 与最相关的关联标准和框架之映射图

导言

本附件将 COBIT 5 与治理范围内最相关的和最常用的标准和框架进行比较。就 ISO/IEC 38500 而言，是通过基于 ISO/IEC 38500 原则的比较来完成；对于其他比较，则采用了一种表格格式，其中 COBIT 5 流程与引用的标准或框架中的等同内容形成映射。

COBIT 5 与 ISO/IEC 38500

以下内容概述了 COBIT 5 是如何支持采用标准的原则和实施方法。《ISO/IEC 38500:2008–信息技术的公司治理》标准是以六个关键原则为基础。每种原则的实际隐含，连同 COBIT 5 指南如何使良好实践成为可能，在此一并予以解释。

ISO/IEC 38500 原则

原则 1—职责

在实践中的意思是：

企业（客户）与 IT （提供商）应以合作伙伴模式进行合作，基于一种积极和互信的关系，进行有效的沟通，明确各自的职责和责任。对于较大型企业，设置一个代表董事会，并由一位董事会成员牵头的 IT 执行委员会（也可称为 IT 战略委员会）是一种非常有效的机制，既可以对企业内的 IT 运用进行评价、指导和监控，又可以就关键 IT 问题为董事会提供建议。在监控 IT 活动时，具有较为简单的指挥机构和较短的沟通路径的中小型企业的主管们需要采用一种更为直接的方法。一概而论，适当的治理组织结构、角色、职责需由治理机构予以授权，为重要决策和任务提供明晰的所有权和问责制。这应包括与关键第三方 IT 服务提供商的关系。

ISACA 的指引如何使良好实践成为可能：

1. COBIT 5 框架为企业 IT 治理定义了一揽子动力。其中“流程”动力和“组织结构”动力连同 RACI[13] 图，在本节所述的环境中尤其具有关联性。这些都非常强烈地倡导责任的指定，并为董事会和管理层就所有关键的相关流程和活动提供角色和责任样板。
2. 《COBIT 5 实施指南》解释了在实施或增强 IT 治理配置时利益相关者和其他涉及方的责任。
3. COBIT 5 的监控分为两级。第一级与治理环境相关联。流程“EDM05 – *确保利益相关者透明度*”解释了主管在监控和评价 IT 治理和 IT 绩效时，利用一种通用方法确定目标和目的以及相关指标等方面的角色。

原则2—战略

在实践中的意思是：

IT 战略规划是一项复杂和关键性的承诺，需要企业范围内各个业务单元以及 IT 战略计划之间的紧密协调。同样至关重要的是将最有可能实现希望达到的收益和有效分配资源的计划摆在优先级别。高层次目标需要转换成可实现的战术计划，确保最低限度的失败和突然性。目标是交付价值以支持战略目标，并同时考虑与董事会风险偏好相关的风险。将计划按自上而下的方式分层固然重要，但计划还必须具有灵活性，适合于满足迅速变化的业务要求和 IT 机遇。

此外，IT 能力的存在与缺失既可驱动也可干扰业务战略；因此，IT 战略规划应包括透明的和恰当的 IT 能力规划。这还应包括当前 IT 基础设施和人力资源能力的评估，以支持未来的业务要求和考虑到未来的技术开发，这些技术可能提高竞争优势和/或优化成本。IT 资源包括与众多外部产品厂商和服务提供商之间的关系，其中部分可能会扮演一个支持业务的关键角色。战略性采购的治理因此也是一项非常重要的战略规划活动，需要高管层的指导和监督。

[13] RACI 图概述了哪些人是一项任务的执行方、责任方、商议方和告知对象。

ISACA 的指引如何使良好实践成为可能：

1. COBIT 5 为管理 IT 投资和（特别是在治理领域中的流程“EDM02–*确保收益交付*”中）适当的业务案例应该如何支持战略目标提供了具体的指引。
2. COBIT 5 APO 领域解释了有效规划和组织内外部 IT 资源所需要的流程，包括战略规划、技术和架构规划、组织规划、创新规划、投资组合管理、投资管理、风险管理、关系管理和质量管理等。同时，还根据行业内研究成果，采用体现出它们是如何支持所有 IT 相关流程的战略目标的通用实例，对业务和 IT 目标的一致性予以解释。
3. 识别出和使企业目标与 IT 相关目标保持一致的实践说明了对企业目标、IT 相关目标和动力，还包括 IT 流程之间的层级关系有着更深入的理解。该指引提出了一份 17 项通用企业目标和 17 项通用 IT 相关目标的列表，该列表内容翔实、联系密切，并在不同部门之间予以验证和优先排序。连同这两者之间关联信息，该列表为构建从业务目标到 IT 目标的通用层级提供了良好的依据。

原则 3—购置

在实践中的意思是：

IT 解决方案的存在就是为了支持业务流程，因此必须注意不要孤立地或只是当作某种“技术”项目或服务来看待IT解决方案。在另一方面，不恰当的技术架构选择、未能维护当前和适当的技术基础设施，或缺失熟练的人力资源，均可能导致项目的失败，以致不能保证业务的持续运营，或减少业务价值。购置 IT 资源应作为更为广泛的 IT 驱动的业务变更之一部分予以考虑。采购的技术必须还要能支持和兼容现有的和已计划的业务流程和 IT 基础设施。其实施并非简单的技术问题，而是组织机构变更、修改的业务流程、培训和启动变更的综合。因此，IT 项目应作为更为广泛的企业范围内变更项目集之一部分予以实施，这些项目集还包括能满足全系列活动的其他项目，以有助于确保得到成功的结果。

ISACA 的指引如何使良好实践成为可能：

1. COBIT 5 EDM 领域通过其完整的生命周期（购置、实施、运行和退役）就治理和管理 IT 驱动的业务投资提供指引。“APO05–*管理投资组合*”流程就是解决如何运用这种投资的有效组合和项目集管理以有助于确保收益得以实现和成本得以优化的问题。
2. COBIT 5 APO 领域为购置规划提供指引，包括投资规划、风险管理、项目集和项目规划以及质量规划。
3. COBIT 5 BAI 领域为采购和实施 IT 解决方案所必需的流程提供指引，其范围涵盖要求定义、识别可行性解决方案、编制文件、培训和使用户和操作机构能运行新系统。此外，还提供了指引以协助确保当变更运用于经营业务和 IT 环境时，解决方案通过测试和适当的控制。
4. COBIT 5 MEA 领域和流程 EDM05 包括有关主管们如何监控和评价购置流程的指引，和确保购置得到适当的管理和执行的内部控制程序。

原则 4—绩效

在实践中的意思是：

有效的绩效测定取决于正要解决的两个关键方面：绩效目标的明确定义和监控目标达成的有效指标的确立。还要求有一种绩效测定流程以帮助确保绩效一致地及可靠地得到监控。只有当目标自上而下设定，并与高层次和批准的业务目标一致，而指标自下而上得以确定，并以各级目标的达成能由各个管理层予以监控的方式形成一致时，治理才能实现。两大关键的治理成功因素是利益相关者对目标的批准和主管们以及经理们对目标达成的责任性的接纳。IT 是一门复杂的及技术性的话题，因此，重要的是要用利益相关者能理解的语言来表示目标、指标和绩效报告以实现透明度，以便能采取适当的措施。

ISACA 的指引如何使良好实践成为可能：

1. COBIT 5 框架为全系列的IT相关流程和其他动力提供目标和指标的通用示例，并说明它们是如何与业务目标形成联系，以便于企业能够对其进行调整以适应企业各自的具体用途。
2. COBIT 5 为管理层就设定与业务目标一致的 IT 目标提供指引，并描述了如何利用目标和指标来监控这些目的的绩效。使用 ISO/IEC 15504 合规能力评估模型可进行流程能力评估。

3. 两个关键 COBIT 5流程提供特定指引：
   – “APO02–*管理战略*”集中在设定目标。
   – “APO09–*管理服务协议*”集中在界定适当的服务和服务目标，并在服务协议层次上予以文件化。
4. 在流程“MEA01–*监控、评价和评估绩效和合格性*”中，COBIT 5 就行政管理层对于本活动的责任提供指引。
5. 计划的《针对鉴证的 COBIT 5》指南解释了鉴证专业人员如何能就 IT 绩效向主管们提供独立的鉴证。

原则 5—合规性
在实践中的意思是：
在当今由互联网和高级技术驱动的全球化市场中，企业需要遵守数量不断增加的法律和监管要求。由于近年来的公司丑闻和财务败笔，公司董事会对以现有的和将要通过的更为严格的法律和条令具有更敏锐的意识。利益相关者对于企业在其经营环境中遵守法律法规并符合良好的公司治理实践的鉴证要求越来越高。此外，由于 IT 使企业之间的无缝业务流程成为可能，因此也出现日益增长的需要以帮助确保合同在诸如隐私、机密、知识产权和安全性等领域中纳入重要的 IT 相关的要求。

主管们需要保证，外部要求合规应作为战略规划的一部分对待，而不是一种付出代价的事后诸葛亮。他们还需要保持高层口径一致，并建立政策和规程供管理层和人员遵守，以确保企业目标得以实现、风险最小化和实现合规。最高管理层必须在绩效和合规之间保持适度平衡，以确保绩效目标不会危及到合规性，相反地，合规性制度要适当，不会形成对业务经营的过分制约。

ISACA 的指引如何使良好实践成为可能：
1. COBIT 5 治理和管理实践为在企业中建立一种适当的控制环境提供了依据。流程能力评估使管理层能够评价 IT 流程能力和对其进行基准管理。
2. COBIT 5 流程“APO02–*管理战略*”有助于确保 IT 计划和整体业务目标之间的一致性，包括治理要求。
3. COBIT 5 流程“MEA02–*监控、评价和评估内部控制系统*”使主管们能够评估控制程序是否足以满足合规要求。
4. COBIT 5 流程“MEA03–*监控、评价和评估外部合规要求*”有助于确保识别出外部合规要求，主管们设定合规方向，和 IT 合规本身得以监控、评估和报告以作为整体符合企业要求的一部分。
5. 计划的《针对鉴证的 COBIT 5》指南解释了审计师如何能够提供独立鉴证，确保合规和遵守源自于内部政令或外部法律、监管或合同要求的内部政策，并确认负责任的流程所有者及时地处理合规差距的任何纠正措施。

原则 6—人类行为
在实践中的意思是：
任何 IT 驱动的变更，包括 IT 治理本身的实施，通常需要在企业内部以及在顾客方和业务合作伙伴方进行重大的文化和行为变更。这可能会在员工之间造成恐惧和误解，因此，若要员工保持积极参与，实施过程就需要谨慎管理。主管们必须旗帜鲜明地对目标进行沟通和交流，并以积极的姿态以示对提议的变更表示支持。人员培训和技能提升是变更的关键要素---尤其是考虑到技术快速发展的性质时更是如此。企业中各个层级的人员，包括利益相关者、管理人员和用户，乃至向企业提供 IT 相关服务和解决方案的专家，均会受到 IT 的影响。在企业范围之外，IT 会影响到顾客和业务合作伙伴，并日益使国内外自助服务和自动化公司间交易成为可能。尽管 IT 驱动的业务流程带来新的收益和机遇，但同时也带来日渐增多的风险类型。诸如私隐和欺诈这样的问题日益成为个人担心的问题，如果要人们信任其使用的 IT 系统，这些问题和其他种类的风险就必须予以管理。信息系统也可能以其将人工程序自动化极大地影响到工作实务。

ISACA 的指引如何使良好实践成为可能：
以下 COBIT 5 动力（包括流程）就与人类行为相关的要求提供指引：
1. COBIT 5 动力包括人员、技能和能力、文化、道德和行为。就每一种动力而言，提出了一种如何处理动力的模型，并以示例说明。

2. COBIT 5 流程“APO07-*管理人力资源*”解释了个人绩效应该如何与公司目标一致，IT 专业人士的技能应该如何维护，和角色和职责应该如何界定。
3. COBIT 5 流程“BAI02-*管理要求定义*”有助于确保应用程序的设计符合人类的操作和使用要求。
4. COBIT 5 流程“BAI05-*管理组织变更的启动*”和“BAI08-*管理知识*”有助于确保用户具备能力有效地使用系统。

此外，ISACA 为专业人员履行IT治理相关的关键角色提供四种认证，这些认证的知识体系在实质上由 COBIT 5 内容所覆盖：
- 企业信息科技管治认证® (CGEIT®)
- 注册信息系统审计师® (CISA®)
- 注册信息安全经理® (CISM®)
- 风险及信息系统监控认证™ (CRISC™)

证书持有者并已证明其具有履行相应角色的能力和经验。

ISO/IEC 38500 标准评价、指导和监控

ISACA 的指引如何使良好实践成为可能：

COBIT 5 流程模型中的治理领域有五个流程，其中每一流程都定义了相应的 EDM 实践。凡与治理相关的活动均主要在此 COBIT 5 中的区域予以界定。

与其他标准的比较

COBIT 5 开发时参考了若干种其他标准和框架；这些标准列示于附件 A 中。

《COBIT 5：启用流程》包含每一个 COBIT 5 流程与含有附加指引的关联标准和框架中最相关部分之间的高层次映射图。

在本节中，包括对每一种标准或框架的简要讨论，并说明在 COBIT 5 中哪些方面和领域与其相关。

ITIL® V3 2011 和 ISO/IEC 20000

以下 COBIT 5 方面和领域由 ITIL V3 2011 和 ISO/IEC 20000 所覆盖：
- 在 DSS 领域中的一个流程子集；
- 在 BAI 领域中的一个流程子集；
- 在 APO 领域中的部分流程。

ISO/IEC 27000 系列

以下 COBIT 5 方面和领域由 ISO/IEC 27000 所覆盖：
- 在 EDM, APO 和 DSS 领域中的安全和风险相关的流程；
- 其他领域中的流程内各种安全相关的活动；
- MEA 领域中监控和评价的活动。

ISO/IEC 31000 系列

以下 COBIT 5 方面和领域由 ISO/IEC 31000所覆盖：
- 在 EDM 和 APO 领域中的风险管理相关的流程

TOGAF®

以下 COBIT 5 方面和领域由 TOGAF 所覆盖：
- 在 EDM（治理）领域中资源相关的流程—架构委员会、架构治理和架构成熟度模型的 TOGAF 组件映射到资源优化。
- 在 APO 领域中的企业架构流程。位于 TOGAF 核心的是架构开发法（ADM）周期，与 COBIT 5 中开发架构愿景（ADM 中的 A 阶段）、界定参考架构（ADM 中的 B,C,D 阶段）、选择机会和解决方案（ADM中的 E 阶段）、和界定架构实施（ADM 中的 F,G 阶段）的实践映射。若干个 TOGAF 组件与 COBIT 5 中提供企业架构服务的实践映射。具体包括：
  – ADM 要求管理
  – 架构原则

– 利益相关者管理
– 企业转型准备评估
– 风险管理
– 基于能力的规划
– 架构合规性
– 架构合约

能力成熟度模型整合 (CMMI)（开发）

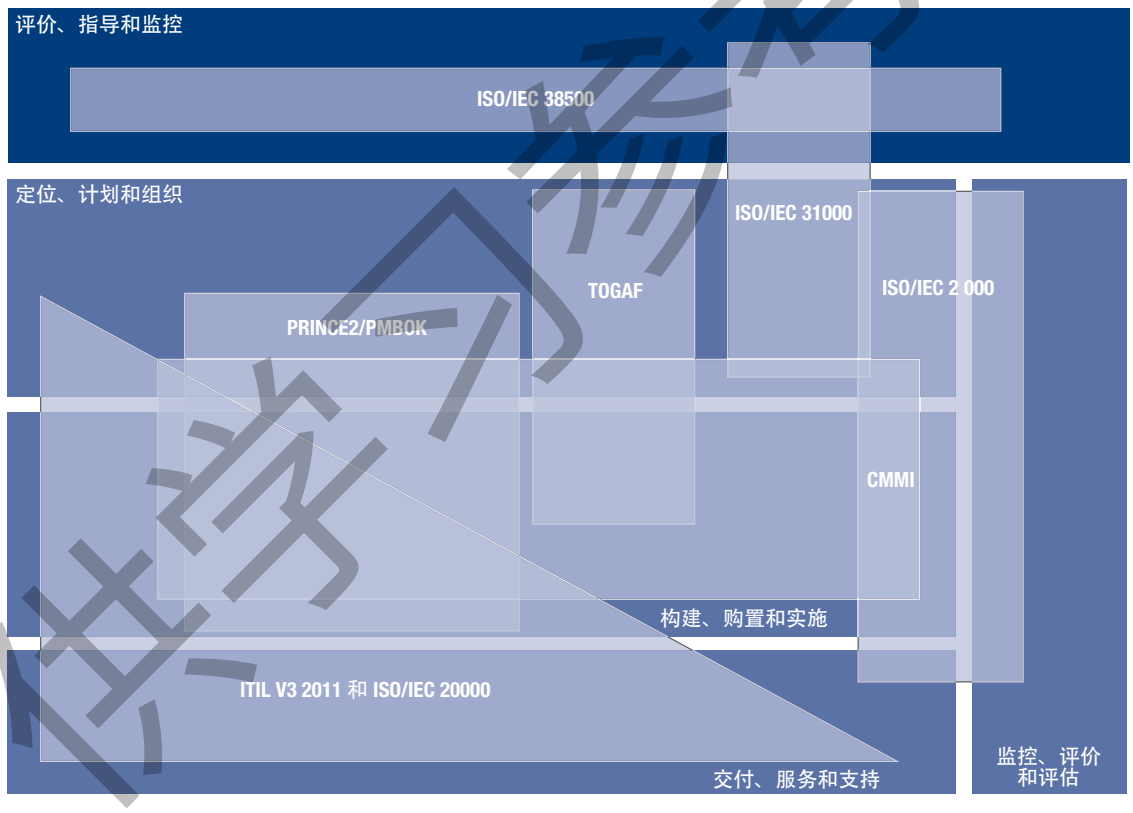
以下 COBIT 5 方面和领域由 CMMI 所覆盖：
• 在 BAI 领域中应用程序–构建和购置相关流程
• 在 APO 领域中部分组织和质量相关的流程。

PRINCE2®

以下 COBIT 5 方面和领域由 PRINCE2 所覆盖：
• 在 APO 领域中与组合相关的流程；
• 在 BAI 领域中的项目集和项目管理流程。

图 25 描述了 COBIT 5 与其他标准和框架之间的相关覆盖。

图 25—COBIT 5 覆盖的其他标准和框架



本页特此留空

附件 F
COBIT 5 信息模型与 COBIT 4.1 信息标准之间的比较

COBIT 4.1七个信息标准——效果、效率、完整性、可靠性、可用性、保密性、和符合性——是如何与 COBIT 5 信息动力的信息质量范畴和维度产生关联？如附件 G 中**图 32** 所示。

下表包含两个栏目：
- 第一栏列示 COBIT 4.1 七个信息标准
- 第二栏列示 COBIT 5 供选方案，例如，对应的信息动力目标。

图 26—COBIT 5 对应于 COBIT 4.1信息标准

COBIT 4.1 信息标准	COBIT 5 相对应的内容
效果	如果信息符合将信息运用特定任务的信息消费者的需要，则信息有效。如果用户利用信息能履行任务，则信息有效。这也符合以下信息质量的目标：适量性、相关性、可理解性、可解释性、客观性。
效率	尽管效率被视为一种产品信息，但效率则更多地与获取和使用信息的流程相关，所以效率与“信息作为一种服务”的观点一致。如果符合用户需要的信息是轻而易举地获取和使用，（例如，几乎不耗费资源——体力、认知能力、时间、和金钱），那么信息的使用是有效率的。这符合以下信息质量的目标：可信性、可达性、易于操作、有信誉。
完整性	如果信息具备完整性，则信息就没有误差而是完整的。这符合以下信息质量的目标：完整、精确。
可靠性	可靠性常被视为精确性的同义词；然而，也可以说，如果是真实和可信的，则信息是可靠的。与完整性相比较，可靠性更为主观，更多地与感知相联系，而不仅仅是事实的。这符合以下信息质量的目标：可信性、有信誉和客观性。
可用性	可用性是可访问和安全性名下的信息质量目标之一。
保密性	保密性与受限存取信息质量目标相对应。
符合性	在某种意义上信息必须符合规范是由任何信息质量目标所覆盖，其程度取决于需求。 监管符合性是使用信息的最常见的一种目标或要求，而并不是信息的固有质量。

本表显示出所有 COBIT 4.1 的信息标准均由 COBIT 5 所覆盖；然而，COBIT 5 信息模型可以界定附加的标准集，因此，为 COBIT 4.1 标准增加了价值。

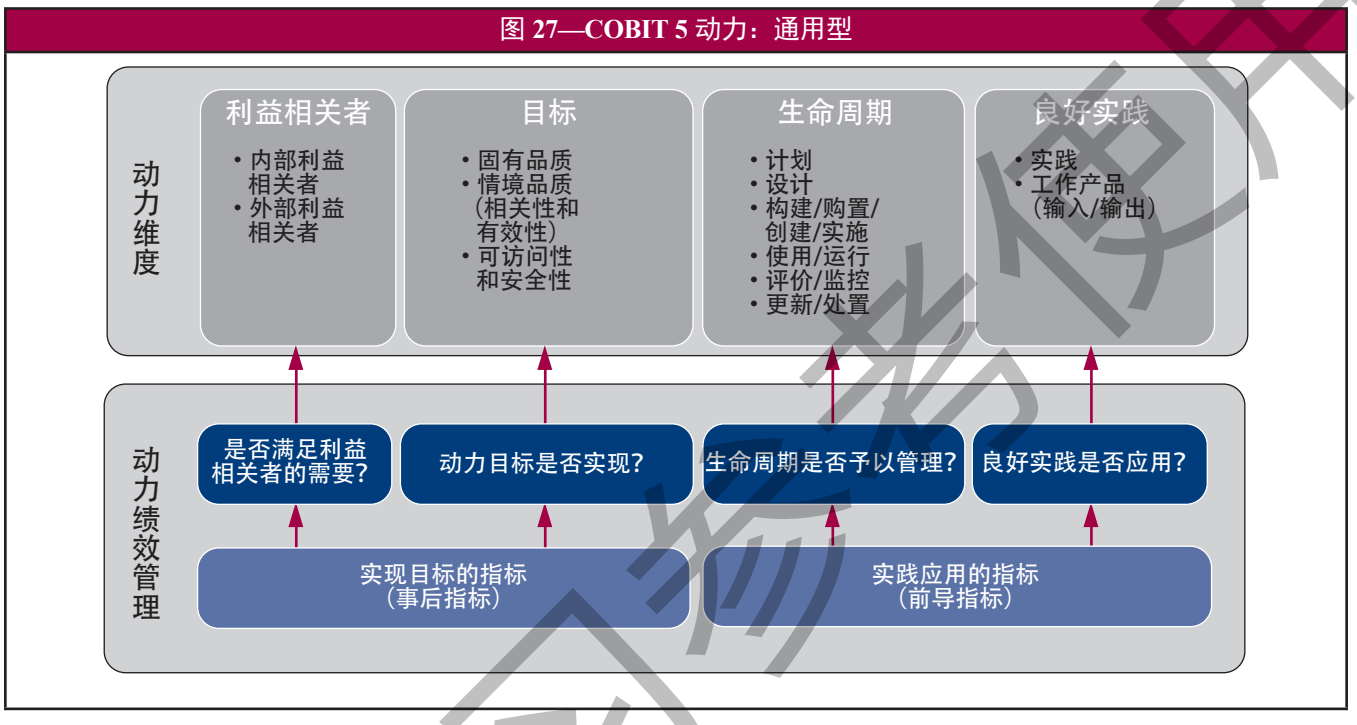
本页特此留空

附件 G
COBIT 5 动力详细描述

导言

本节包含对作为 COBIT 5 框架一部分的动力七个范畴的详细讨论，这些内容最初在第五章中描述，并在**图 27** 中重述。

图 27—COBIT 5 动力：通用型



动力维度

动力的四种共同维度是：

- **利益相关者**—每一种动力都有利益相关者，如，起到积极作用的和/或对动力感兴趣的各方。例如，流程有执行流程活动的各方，和/或对流程结果感兴趣的各方；组织结构也有利益相关者--扮演各自的角色具有各自的利益。利益相关者可能是企业内部的也可能是企业外部的，都有各自的、有时甚至是互相冲突的利益和需要。利益相关者的需要转化成企业的目标，这些目标继而转化成企业 IT 相关的目标。**图 7** 所示是利益相关者列表。
- **目标**—每种动力都有若干个目标，而动力是通过这些目标的达成来提供价值。目标可定义为以下方面：
  - 动力的期待结果；
  - 动力本身的应用或运营。

  动力目标是 COBIT 5 层级中的最终步骤，这些目标可进一步细分为不同的范畴：
  - **固有品质**—动力精确地、客观地发挥作用，并提供精确的、客观的和规范的结构之程度。
  - **关联性品质**—考虑到其运行的环境，动力及其结果与目的相适配，例如，结果应该是相关的、完整的、当前的、适当的、一致的、可理解的和易于使用的。
  - **访问与安全**—动力及其结果可访问性和安全可靠的程度，例如：
    - 当需要时，动力是可用的。
    - 结果是可靠的，例如，访问仅限于有权或需要访问者。
- **生命周期**—每一种动力均有生命周期，从运行/使用寿命开始直到处置。这种周期可运用到信息、结构、流程和政策等等。生命周期的各阶段由以下内容构成：
  - 计划（包括概念开发和概念选择）
  - 设计
  - 构建/购置/创建/实施
  - 使用/操作

  - 评价/监控
  - 更新/处置
- **良好实践**—对于每一种动力，均可定义良好实践。良好实践支持动力目标的实现。良好实践就如何以最佳方式实施动力，或需要何种工作产品或输入和输出等，提供实例和建议。COBIT 5 为 COBIT 5 的部分动力（如流程）提供了良好实践的实例。就其他动力而言，可采用其他的标准、框架等…

动力绩效管理

企业都期望能从应用和使用动力中获得积极的成果。为了管理动力的绩效，需要对以下问题进行监控，然后需要予以回答——并应定期进行：

- 利益相关者的需要是否得以满足？
- 动力目标是否实现？
- 动力生命周期是否予以管理？
- 良好实践是否得以应用？

前两项处理的是动力的实际结果，用于测评目标实现程度之指标可称为“事后指标”。

后两项处理的是动力本身的实际功能性，其测量指标可称之为“前导指标”。

每一种动力均有一个单独的章节，以类似于**图 27** 的图开始，但包括若干个现有动力的特殊要素，以红色和**粗体**表示。

然后，每四个组件一次进行详细讨论，讨论具体的组件和与其他动力的关系。

还采用若干个示例以说明动力的含义和使用。

本节的目的是更为深入地洞察 COBIT 5 框架的内涵，以及动力概念是如何运用于实施和改进企业 IT 的治理和管理。

COBIT 5 动力：原则、政策和框架

原则和政策指的是设置以传递治理机构和管理层的导向和指令的沟通机制。较之于通用动力描述，针对原则、政策和框架动力的具体细节如**图 28** 所示。

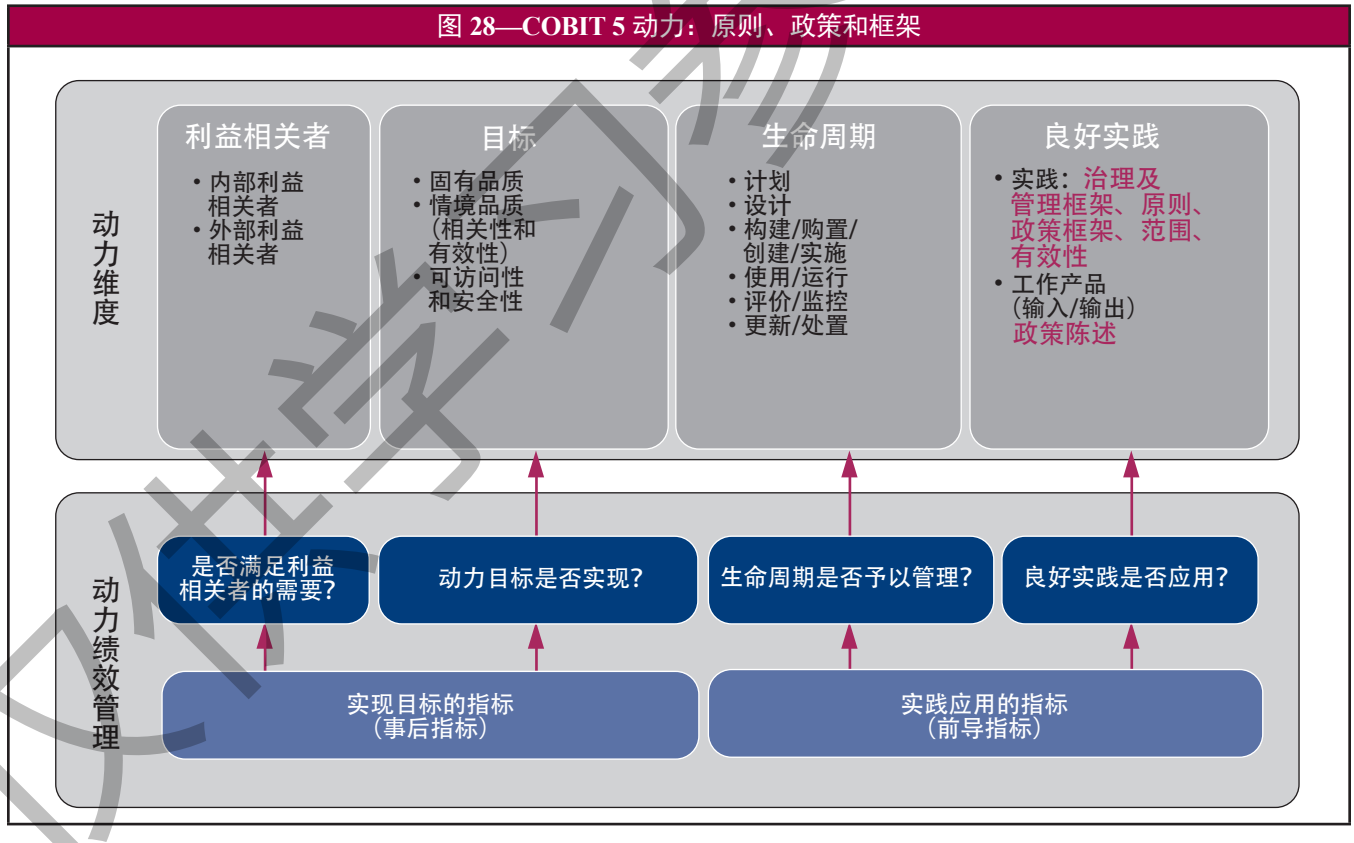
原则、政策和框架模型显示出：

- **利益相关者**—原则和政策的利益相关者可能是企业内部和外部的，包括董事会和行政管理层、合规官员、风险经理、内部和外部审计师、服务提供商和顾客和监管机构。利害关系是双重的：部分利益相关者定义和设定政策。而其他的则必须遵循和与这些政策保持一致。
- **目标和指标**—原则、政策和框架是由董事会和行政管理层界定的交流企业规则，支持治理目标和企业价值的工具。原则必须是：
  – 数量有限
  – 以简单的语言尽可能清晰地表达企业的核心价值观。

政策就如何在实践中运用原则提供更为详细的指南，政策影响到决策如何与原则保持一致。良好的政策是：
– 有效—可以达到规定的目的。
– 高效率—能确保原则以最有效率的方式实施。
– 非侵入性—对于必须遵循政策者而言，具有逻辑性，例如，政策不会形成不必要的阻力。

政策知情权——一种便于所有利益相关者了解政策的机制是否到位？换言之，利益相关者是否知道在何处了解到政策？

图 28—COBIT 5 动力：原则、政策和框架



治理和管理框架应为管理层提供能够进行适当的企业 IT 治理和管理的结构、指引和工具等。框架应该是：
– 综合全面的，涵盖所有要求的领域；
– 开放而灵活的，允许调整适合于企业的具体情况；
– 当前的，例如反映当前企业的导向和当前的治理目标；
– 对于所有利益相关者可用和可访问。

- **生命周期**—政策具有支持达到规定目标的生命周期。框架非常关键，原因在于其通过一种结构以界定兼容一致的指引。例如，一个政策框架一种结构，在这个结构中，可生成和维护一套兼容一致的政策，而且还会提供一种各种政策内部和之间的便利的导航点。

  鉴于企业运作的外部环境，对于强势的内部控制的监管要求的程度可能会不尽相同，因此，就需要一种强势的政策框架。关于框架和政策需要考虑的一个关键关注点是政策的通用型—如果和当政策被审核和更新时，是否有强势的机制到位以保证人们意识到这些更新，最新版本是否易于接入（见前述一点），过时的信息是否适当归档或处置？
- **良好实践：**
  - 良好实践要求政策成为治理和管理框架的一部分，并提供一种（分级的）结构，在这种结构中，所有的政策都应与之适配并且与基本原则形成明确的联系。
  - 作为政策框架的一部分，以下科目需要予以描述：
    - 范围和有效性
    - 未能遵守政策的后果
    - 处理例外的手段
    - 政策合规将能被检查和测评的方式。
  - 公认的治理和管理框架能为纳入政策之内的实际语句提供指引。
  - 政策应与企业的风险偏好保持一致。政策是企业内部控制系统的关键组件之一，其目的在于管理和容纳风险。作为风险治理活动的一部分，企业的风险偏好已经界定，而这种风险偏好应体现在政策之中。规避风险的企业较之于风险进取精神的企业具有更严格的政策。
  - 政策需要每隔一段时间间隔后予以重新生效和/或更新。
- **与其他动力的关系**—与其他动力的联系包括：
  - 原则、政策和框架应反映企业的文化和道德价值观，并应鼓励倡导的行为，因此，与文化、道德和行为动力之间有密切的联系。
  - 流程实践和活动是执行政策最重要的载体。
  - 组织结构可以在其控制范围内界定和实施政策，而组织结构的活动又由政策来界定。
  - 政策也是信息，因此所有应用于信息的良好实践也可应用于政策。

示例 9—社会媒体

企业正在考虑如何应对日益快速增长的社会媒体和其员工能够完全访问这些媒体的压力。迄今为止，各组织机构在授予这种服务的访问权时仍然很保守或是限制，主要是出于安全原因。

来自不同方面的压力代表了对于社会媒体截然不同的立场。员工们希望享有在自己家里一样的访问级别，而组织机构本身也希望使用和开发社会媒体的优势用于营销和提高知名度。

企业已经决定要制定一项关于在企业网络和系统中，包括企业提供给员工的笔记本电脑中使用社会媒体的政策。新政策与“可接受使用政策”类别项下现有政策框架适配，而且比以前的政策更为宽松。因此，通过沟通以解释新政策的原因。同时，也会对部分其他动力产生影响：

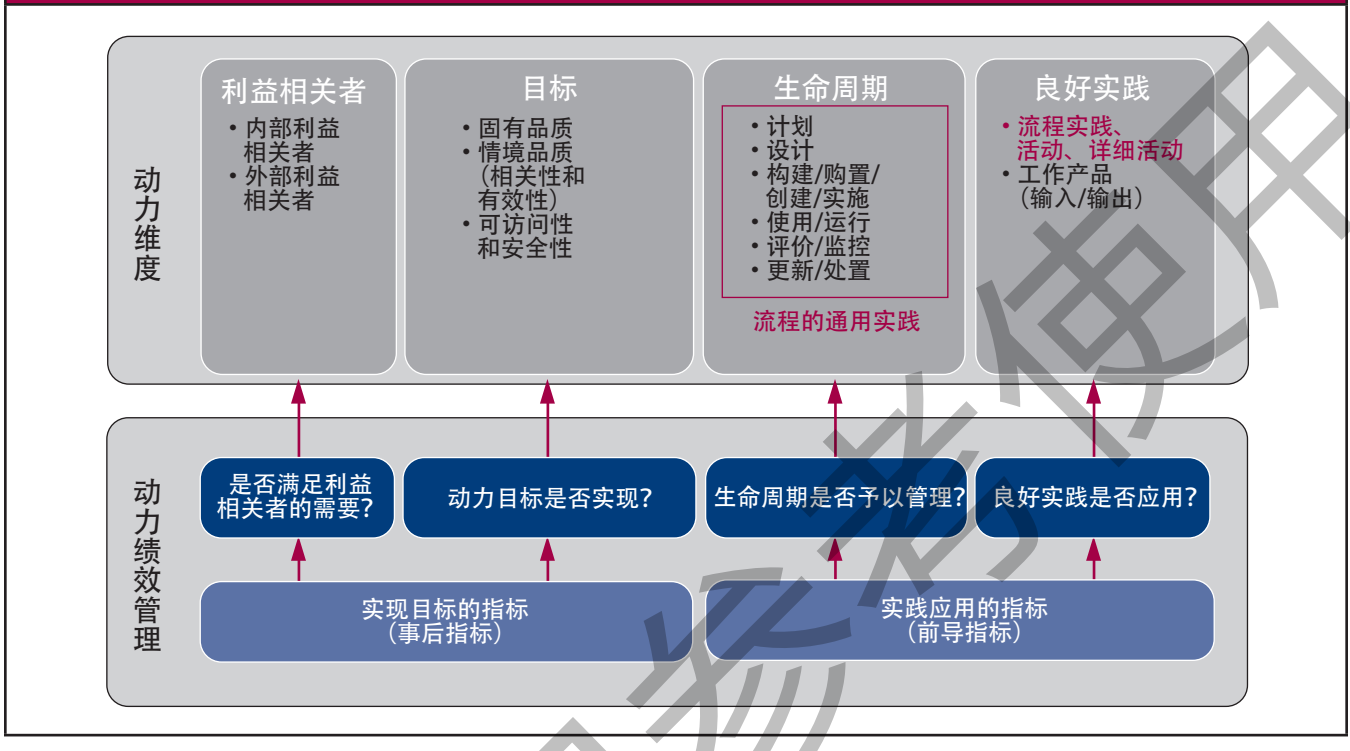
- 员工需要学习如何处理新媒体以避免给企业造成令人尴尬的处境。他们需要学习与企业制定的新导向一致的适当的行为，和发展适当的技能。
- 关于安全的若干个流程需要改变，访问权对这些媒体开放，因此安全设置和配置必须更改，如有可能，需要定义某种补偿措施。

注：COBIT 5 在本动力描述中是一种框架示例。

COBIT 5 动力：流程

较之于通用动力描述，流程动力的具体细节如**图 29** 所示。

图 29—COBIT 5 动力：流程



一个流程定义为**“受从若干个来源（包括其他流程）中接受输入，操纵这些输入并产生输出（如产品和服务）的企业政策和规程所影响的一系列实践的集合”。**

流程模型显示出：

- **利益相关者**—流程拥有内部和外部的具备各自角色的利益相关者；利益相关者及其各自的责任等级在 RACI 图中予以文件化。外部利益相关者包括顾客、业务合作伙伴、股东和监管者。内部利益相关者包括董事会、管理层、员工和志愿者。
- **目标**—流程目标定义为“描述某一流程欲达到的结果之说明。这种结果可能是一种产品、一种重大的其他流程的状态变更或重大的能力改进”。这些目标均属于目标分层的一部分，例如，流程目标支持IT相关的目标，而IT相关目标进而支持企业目标。

流程目标可以分类为：

– **固有目标**—流程是否具有固有品质？是否精确并符合良好实践？是否符合内外部规则？
– **环境目标**—流程是否定制化并适合于企业的具体环境？流程是否具有相关性、可理解性和易于应用？
– **可访问性与安全性目标**—流程在必要时具有保密性，并可按需要获知和访问。

在目标分层中的每一个级别中，参照性地定义了指标以衡量目标达到的程度。指标可以定义为“一种可以量化的实体以便于测评某一流程目标的达成。这些指标应是 SMART——即具体的、可测量的、可操作的、相关的和及时的”。

为了有效地和高效率地管理，需要定义指标以测评预期结果的实现程度。此外，动力绩效管理的第二个方面描述了良好实践的应用程度。同时，定义关联指标以促进动力管理。

- **生命周期**—每一个流程均有一个生命周期。流程会被定义、创建、执行、监控，调整/更新或停用。诸如像基于ISO/IEC 15504 标准的 COBIT 流程评估模型中所规定的那些通用流程均有助于界定、运行、监控和优化流程。
- **良好实践**—《COBIT 5：启用流程》中包含一个流程参考模型，在这个模型中，流程内部良好实践是以详细的成长等级予以描述的：即实践、活动、和详细的活动：[14]

实践：

- 就每一个 COBIT 5 流程而言，其治理/管理实践为有效而实用的企业 IT 治理和管理提供了一整套高层次的要求，具体指：
  - 交付收益、优化风险等级和优化资源使用的措施说明。
  - 与相关公认的标准和良好实践保持一致。
  - 通用性，因此需要调整适合于每个企业。
  - 涵盖流程中的业务和 IT 角色扮演者（端到端）。
- 企业治理结构和管理层需要通过以下方式作出与这些治理和管理实践相关的选择：
  - 选择适用的和决定将要实施的；
  - 在必要的地方增加和/或调整实践；
  - 界定和增加非 IT 相关的实践并在业务流程中整合；
  - 选择如何实施这些实践（频率、跨度、自动化等）；
  - 接受不实施适用的实践可能造成的风险。

活动—在 COBIT 中，操作流程所采取的主要措施：

- 这些活动可定义为“为成功的企业 IT 治理和管理实现管理实践的指引”。COBIT 5 的活动为每种治理或管理实践的实施提供了怎么样、为什么和实施什么的内容，以改进企业的 IT 绩效和/或解决IT解决方案及服务交付的风险。这种材料可为下列人士所应用：
  - 需要计划、构建、运行或监控企业 IT 的管理层、服务提供商、最终用户和 IT 专业人员；
  - 可能需要提供关于当前的、建议实现、或必要改进意见的鉴证专业人士。
- 一整套包含有步骤的通用的或具体的活动是实现关键的治理实践（GP）/管理实践（MP）必要和充分的前提，具体包括：
  - 描述一系列面向行动的必要且充分的实施步骤从而实现治理实践（GP）/管理实践（MP）；
  - 考虑流程的输入和输出；
  - 以公认的标准和良好实践作为依据；
  - 支持确定明确的角色和责任；
  - 非指令性的，需要调整和开发为具体的适合于企业的规程。

详细的活动—这些活动对于实施细节来说可能不够充分，需要从以下方面得到的进一步指引：

- 从具体的相关标准和良好实践中获得，如 ITIL、ISO/IEC 27000 系列和 PRINCE2。
- COBIT 5 产品家族中作为补充开发的更详细或更具体的活动。

输入和输出—COBIT 5 的输入和输出被认为是支持流程运行所必要的流程工作产品。这些输入和输出可以促进关键决策、提供流程活动的记录和审计跟踪，以及当出现事故时实现跟进。这些内容被界定为处于关键治理/管理的实践级别，可能会包括部分仅用于流程之内的工作产品，并且通常是其他流程的必不可少的输入。[15]

> *外部良好实践可能以任何形式及详细程度存在，而且大多数是指其他标准和框架。用户可以随时参考这些外部良好实践，以理解 COBIT 是如何与那些标准在相关方面保持一致，以及映射的可用信息。*

动力绩效管理

企业都期望能从应用和使用动力中获得积极的成果。为了管理动力的绩效，需要对以下问题定期监控和回答（基于指标）：

- 利益相关者的需要是否得以满足？
- 动力目标是否实现？
- 动力生命周期是否予以管理？
- 良好实践是否得以应用？

[14] 仅只有实践和活动是在当前项目中开发。更详细的级别要取决于补充开发，例如，各种专业指引可能为各自领域提供更详细的指南。当然，也可通过相关标准和框架进一步获得指引，正如详细的流程描述中所指明的那样。
[15] 说明性的 COBIT 5 输入和输出不应视为详细清单，因为补充信息流可能会依照某种特定的企业环境和流程框架而予以定义。

就流程动力而言，前两项处理的是动力的实际结果。用于测评目标实现程度的指标可称为“事后指标”。在《COBIT 5：启用流程》中，每一流程目标定义了若干个指标。

后两项处理的是动力本身的实际功能性，其测量指标可称之为“前导指标”。

流程能力等级—COBIT 5 包括一项基于 ISO/IEC 15504 标准的流程能力评估方案。这在 COBIT 5 第八章中进行了讨论，而且其进一步的指引在各种 ISACA COBIT 5 出版物中可以查询。总而言之，流程能力等级衡量目标的实现和良好实践的应用。

与其他动力的关系—流程和其他动力范畴之间的联系是通过以下关系存在：
- 流程需要信息（作为一种类型的输入）并能生成信息（作为工作产品）。
- 流程需要像 RACI 图所表示的组织结构和角色进行运行，例如，IT 督导委员会，企业风险委员会、董事会、审计师、首席信息官、首席执行官等。
- 流程产生并需要服务能力（如基础设施、应用程序等）。
- 流程能够并将依赖于其他流程。
- 流程产生或需要政策和规程以确保连续一致的实施和执行。
- 文化和行为方面决定流程的执行水平。

实践中的流程动力实例

实例 10 说明流程动力及其相互联系和动力维度。实例是根据本文前述的实例 7 所构建。

COBIT 5 流程参考模型

治理和管理流程

COBIT 中指导性原则之一就是区分治理和管理。为符合这一原则，希望每个企业实施若干个治理流程和各个管理流程以提供综合性的企业 IT 治理和管理。

当考虑到企业环境中的治理和管理流程时，各种类型流程之间的区别在于流程的目标：
- **治理流程**—治理流程处理的是利益相关者的治理目标——价值交付、风险优化和资源优化---并包括旨在评价战略选择的实践和活动，提供 IT 指导和结果监控（EDM—符合 ISO/IEC 38500 标准概念）。
- **管理流程**—符合管理的定义，管理流程中实践和活动涵盖 PBRM 企业 IT 的各个责任领域，而且还得提供端到端的 IT 覆盖。

示例 10—流程动力的互相联系

一个组织已经任命了 IT 相关流程的“流程经理”，负责在良好的企业 IT 治理和管理环境中定义和运行有效的和高效的 IT 相关的流程。

首先，流程经理应重点关注流程动力，考虑动力的维度：

- **利益相关者：**流程利益相关者包括所有的流程参与者，例如，在流程活动中的执行方、责任方、商议方或告知对象（RACI）各方。为此，可以使用《COBIT 5：启用流程》中描述的 RACI 图。
- **目标：**就每一个流程而言，需要定义恰当的目标和相关的指标。例如，APO08 流程：管理关系（《COBIT 5：启用流程》），用户可以从中发现一系列流程目标和指标，如：
  - **目标：**业务策略、计划和要求均得到充分理解、文件化和批准。
    - **指标：**与企业业务要求/优先级一致的项目集所占百分比
  - **目标：**存在于企业与IT部门之间的良好关系。
    - **指标：**用户和IT人员满意度调查的排名。
- **生命周期：**每一个流程均有一个生命周期，例如，流程必须创建、执行和监控，并在必要时予以调整。最终，流程会废止。这样，流程经理就需要首先设计和定义流程。流程经理们可以使用《COBIT 5：启用流程》中的若干个要素以设计流程，如定义责任和将流程细分为实践和活动，并定义流程产品（输入和输出）。在后期阶段中，需要使流程更稳健和高效，为达到此目的，流程经理可以提高流程的能力等级。受 ISO/IEC 15504 启发的 COBIT 5 流程能力模型和流程能力属性可用于该目的。
  - 流程能力第二级要求实现两种属性：绩效管理和工作产品管理。第一属性要求若干个规划阶段相关的活动：
    - 界定流程绩效的目标；
    - 规划流程绩效；
    - 界定执行流程的责任；
    - 识别资源；
    - 其他。

    相同的能力等级为“监控”流程生命周期的阶段规定了若干个活动。例如：
    - 流程绩效可以被监控；
    - 流程绩效可以被调整以满足计划；
    - 其他。
  - 可使用相同的方法从逐渐提高的流程能力等级所具备的不同绩效能力属性中来获得整个生命周期中各个不同阶段的指引。
- **良好实践：**在前述要点提及的《COBIT 5：启用流程》一书中，COBIT 5 非常详细地描述了与流程相关的良好实践。其涵盖了一个良好的企业 IT 治理和管理所要求的全面活动，可以从中获得启发或了解示例流程。

除了关于流程动力的指引之外，流程经理可以决定研究若干个其他动力，例如：

- RACI 图描述角色和责任。其他动力允许在这一维度中深入研究，例如：
  - 在技能和能力动力中，可以定义每一角色所必需的技能和能力以及适当的目标（如，技术和行为技能等级）和相关指标也可以予以定义。
  - RACI 图还包含若干个组织结构。这些结构可以在企业架构中进一步精心设计，由此可提供更为详细的结构描述，以定义期望的结果和相关指标（如，决策），良好实践也可以被界定（如，控制跨度、结构操作原则、授权等级）。
- 原则和政策使流程正式化，并规定为什么流程会存在，应用于何种目标以及如何使用。这是原则和政策动力中的重点领域。

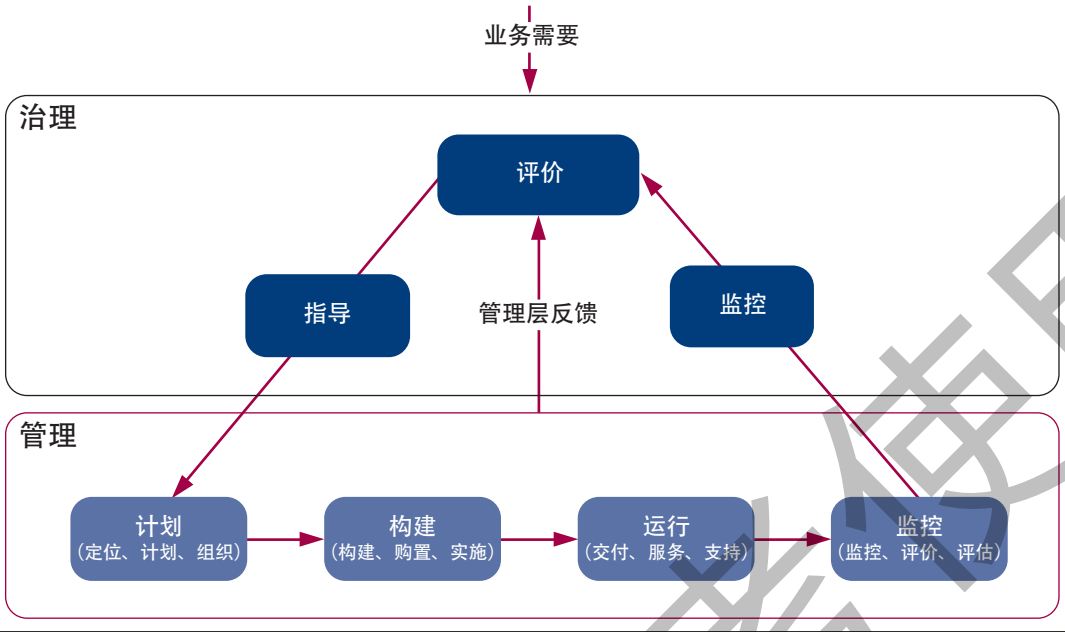
尽管两种类型流程的结果不尽相同，并涉及不同的受众，但实质上，从流程本身的环境来看，所有流程均要求有流程范围中的“规划”、“构建或实施”、“执行”和“监控”活动。

COBIT 5 流程参考模型

COBIT 5 不是指令性的，但从上文来看，COBIT 5 很显然倡导企业实施治理和管理流程，以便覆盖关键领域，如**图 30** 所示。

在理论上，只要基本治理和管理目标得以覆盖，一个企业可以组织其自认为适当的流程。较小型企业可能流程较少；较大型和更为复杂的企业可能流程更多，但均覆盖相同目标。

图 30—COBIT 5 治理和管理的关键领域



尽管如上文所述，COBIT 5 包括一个流程参考模型，该模型详细定义和描述若干个治理和管理流程，针对所有在企业内常规的、与 IT 相关活动的流程为 IT 运营和业务经理提供了一种可理解的共同参考模型。所建议的流程模型是一个完全的、综合的模型，但并不是唯一可能的流程模型。各个企业必须结合其具体情况定义各自的流程集。

结合运营模型和企业内涉及到 IT 活动所有部分的共同语言是迈向良好治理的最重要和最关键的步骤之一。它也提供了一种框架以用于测评和监控 IT 绩效、与服务提供商进行交流和整合最佳管理实践。

COBIT 5 流程参考模型将企业 IT 治理和管理细分为两种主要领域的活动——治理和管理——划分为两大流程领域：

- **治理**—本领域包括五个治理流程；在每一个流程中对评价、指导和监控（EDM）实践予以定义。
- **管理**—这四大领域与计划、构建、运行和监控（PBRM）的责任范围一致（COBIT 4.1 领域的演进结果），并覆盖 IT 的端到端。像 COBIT 4.1 及以前版本一样，每个领域包含若干个流程。尽管如前文所述，大多数流程需要进行企业内部的、或在处理特定问题（如质量、安全性）时进行 “计划”、“实施”、“执行”和“监控”活动，但当涉及到企业层面时的 IT 管理时，根据与其最相关的领域确定其所在的域。

在 COBIT 5 中。流程全面覆盖了企业 IT 治理和管理相关的业务和 IT 活动的整个范围，因此，流程模型是真正意义上的覆盖整个企业。

COBIT 5 流程参考模型是 COBIT 4.1 流程模型的延续，但整合了 IT 风险管理（Risk IT）和IT价值管理（Val IT）流程。**图 31** 显示出 COBIT 5 中全套完整的 37 个治理和管理流程。根据前述的流程模型描述，所有流程的细节均包括在《COBIT 5：启用流程》之中。

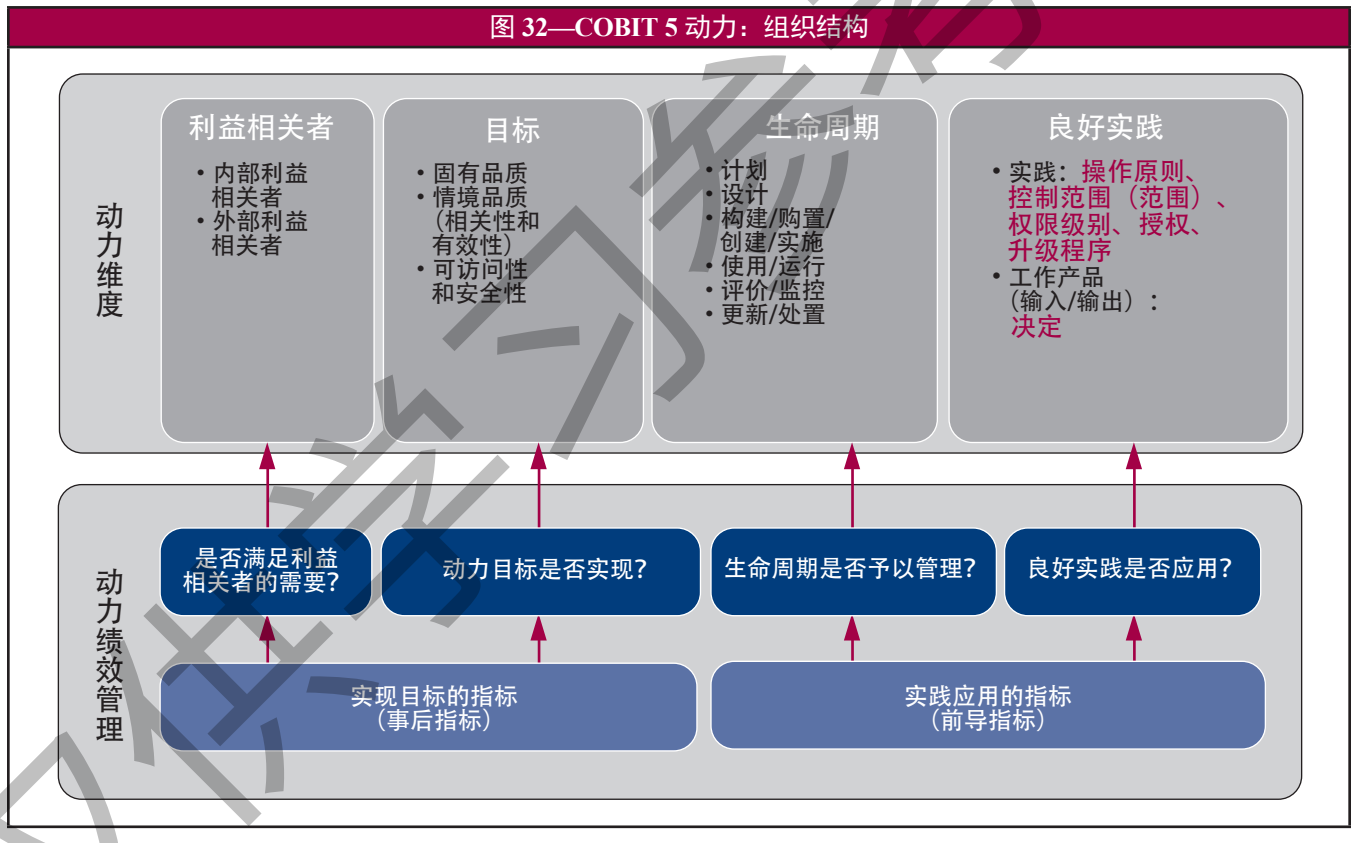
图 31—COBIT 5 流程参考模型

COBIT 5 动力：组织结构

较之于通用动力描述，组织结构动的具体细节如**图 32** 所示。

组织结构模型显示出：
- **利益相关者**—组织结构利益相关者可能是企业内部或外部的，包括机构本身、其他机构、组织实体、客户、供应商和监管者等各种成员；他们的角色各异，包括决策、游说和顾问。利益相关者的利益也各不相同，例如，在机构所作出的决策中他们的利益何在呢？
- **目标**—组织结构动力本身的目标包括适当的指令、定义明确的操作原则和其他良好实践的应用。组织结构动力的成果应包括若干个良好的行动和决定。
- **生命周期**—组织结构有其生命周期，该周期包括：被创建、存在、被调整而直到最后解散。从一开始起，应界定一项指令作为其存在的理由和目的。
- **良好实践**—若干个组织结构的良好实践可区分为：
  - 操作原则—关于机构如何运作，例如，会议次数、文档编制和内务管理规则等的实际安排。
  - 构成—机构的成员，即那些内部的或外部的利益相关者。
  - 控制范围—组织结构决策权的界限。
  - 权限/决策权级别—机构被授权进行的决策。
  - 授权—机构可将其（子集的）决策权授予向其报告的其他机构。
  - 升级规程—一个机构的升级路径描述了在决策过程中出现问题时需要采取的措施。

图 32—COBIT 5 动力：组织结构



与其他动力的关系—与其他动力的联系包括：
- RACI 图将流程活动与组织结构和/或企业内的个人角色联系起来，并描述了针对每种流程实践的每个角色的参与程度：即执行方、责任方、商议方或告知对象。
- 文化、道德和行为决定组织结构及其决策的效率和有效性。
- 组织结构的构成应考虑并要求各成员具有适当的技能组合。
- 组织结构的指令和操作原则应由现有的政策框架指导。
- 输入和输出—在能够进行正式决策之前，一个机构需要输入（典型信息），然后能生成输出，例如，决策、其他信息、或要求附加输入。

COBIT 5 中的列举的组织结构

正如关于 COBIT 5 流程模型讨论中所提到的，一个 COBIT 5 流程参考模型已经创建并列举在《COBIT 5：启用流程》中详细描述。这一模型包括采用了若干个角色和结构的 RACI 图。**图 33** 描述了这些预定义的角色和结构。

注：

- 这些角色定义并不一定要与企业已经实施的实际功能相一致。不过，尽管如此，从对结构或角色所描述的作用对于大多数企业仍然适用上来看，它们提供了价值。
- 本表的目的不是为每个企业规定一种万能的组织机构图，而应视为举例。

图 33—COBIT 5 角色和组织机构	
角色/结构	**定义/描述**
董事会	企业中最高行政管理人员和/或非执行董事构成的团体，他们负责企业的治理并掌控企业的整个资源。
首席执行官（CEO）	负责企业整个管理的最高级别官员。
首席财务官（CFO）	企业中负责全面财务管理，包括财务风险和控制以及可靠和精确的会计管理的最高级别官员。
首席营运官（COO）	企业中负责营运的最高级别官员。
首席风险官（CRO）	企业中负责全面风险管理的最高级别官员。可设置一个 IT 风险职能岗位以监督 IT 相关的风险。
首席信息官（CIO）	企业中负责 IT 与业务战略一致的最高级别官员，还负责规划、提供资源、和管理支持企业目标的 IT 服务和解决方案的交付。
首席信息安全官（CISO）	企业中负责企业各种信息安全的最高级别官员。
企业主管人员	负责某一具体业务单位或子公司运营的高级管理人员。
业务流程所有者	负责实现流程目标、推动流程改进和批准流程变更等流程绩效的人员。
战略（IT 执行）委员会	由董事会委任的高级管理人员构成的团体，以确保董事会参与到和始终知晓重大 IT 相关的事务和决定。该委员会负责管理 IT 驱动的投资组合、IT 服务和 IT 资产，保证交付价值和管理风险。正常情况下该委员会由一名董事会成员而不是首席执行官主持。
（项目或项目集）督导委员会	由负责项目集和项目指导的利益相关者和专家构成的团体，包括管理和监控计划、资源配置、收益和价值交付以及项目集和项目风险管理
架构委员会	由负责对企业架构相关的事务和决策予以指导的利益相关者和专家构成的团体，还负责设定架构政策和标准。
企业风险委员会	由负责支持企业风险管理（ERM）活动和决策所必需的企业层面协调和一致同意的企业管理人员构成的团体。可以成立一个 IT 风险理事会，以便更详细地考虑 IT 风险，并为企业风险委员会提供建议。.
人力资源负责人	负责企业中关于人力资源的规划和政策的最高级别官员。
合规部	企业中负责法律、监管和合约合规指导的职能部门。
审计部	企业中负责提供内部审计的职能部门。
架构负责人	负责企业架构流程的高级人员。
开发负责人	负责 IT 相关解决方案开发流程的高级人员。
IT 运营负责人	负责 IT 运营环境和基础设施的高级人员。
IT 行政管理负责人	负责 IT 相关记录和支持 IT 相关行政管理事务的的高级人员。
项目集和项目管理办公室(PMO)	负责支持项目集和项目经理的职能部门，并负责收集、评估和报告关于其项目集和构成项目的信息。
价值管理办公室(VMO)	充当管理投资和服务组合秘书处的职能部门，其职能还包括对投资机会和业务案例进行评估和提供建议，推荐价值治理/管理方法和控制手段，并报告投资和服务可持续和创建价值的进展情况。
服务经理	为特定客户（用户）或客户（用户）团体管理开发、实施、评价和持续管理新建和现有产品和服务的人员。

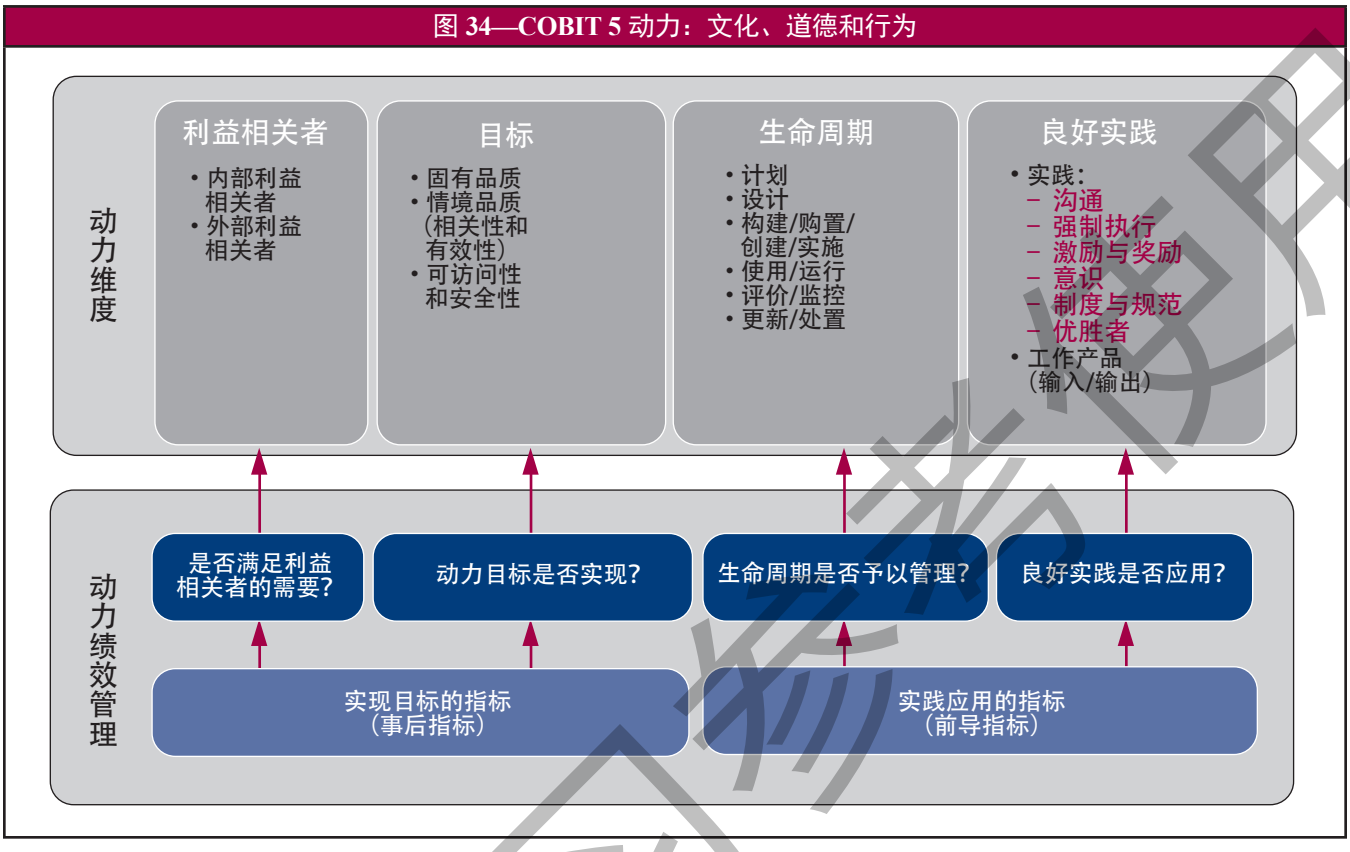
图 33—COBIT 5 角色和组织机构（续）	
角色/结构	**定义/描述**
信息安全经理	管理、设计、监督和/或评估企业信息安全的人员。
业务持续性经理	管理、设计、监督和/或评估企业业务持续性能力的人员，以保证企业的关键职能部门能在破坏性事件之后持续运行。
隐私官	负责监控隐私法律的风险和对业务的影响的人员，并且还将指导和协调实施符合隐私保护条例的政策和活动。也称为数据保护官。

本页特此留空

COBIT 5 动力：文化、道德和行为

文化、道德和行为指的是企业内一系列个人的或集体的行为。
较之于通用动力描述，针对文化、道德和行为动力的具体细节如**图 34 所**示。

图 34—COBIT 5 动力：文化、道德和行为



文化、道德和行为模型表现为：

- **利益相关者**—文化、道德和行为的利益相关者可能是企业内部或外部的。内部利益相关者包括整个企业，外部利益相关者包括监管者，例如，外部审计师或监督机构。利益是双重的：部分利益相关者，如，法律专员、风险经理、人力资源经理、薪酬委员会及其官员等，负责处理定义、实施和强制执行欲达到的行为，而其他的则必须遵守规定的制度和规范。
- **目标**—文化、道德和行为动力的目标涉及到以下方面：
  - 由企业赖以生存的价值观所决定的组织性道德；
  - 由企业每个个人的价值观所决定的个人道德，取决于诸如宗教、种族、社会经济背景、地域和个人经历等外部因素的重要程度。
  - 个人行为，可在整体上决定一个企业的文化。有很多因素，例如上述提及的外部因素，也有企业内的人际关系、个人目标和志向等，驱动着行为。与这种环境相关的部分行为类型包括：
    - 承担风险的行为—企业觉得能承受多大的风险？愿意承担哪种风险？
    - 遵循政策的行为—人员在何种程度上拥护和/或遵守政策？
    - 应对负面结果的行为—企业如何处理负面结果，如，损失事故或错失良机？企业是否能从中吸取教训并试图调整，或抱怨而不分析深层原因？
- **生命周期**—组织机构的文化、道德立场和个人行为等等，均有其生命周期。从现有文化开始，企业可以识别出必要的变更并努力完成其实施。在良好实践中描述的几种工具可以使用。
- **良好实践**—在整个企业中，为创建、激励和维护欲达到的行为所需的良好实践包括：
  - 在整个企业内沟通欲达到的行为和强调的公司价值观。
  - 通过高管层和其他优胜者的表率行为加强的倡导的行为意识。

– 对欲达到的行为的鼓励诱因和强制威慑。在个人行为和企业设置到位的人力资源奖励方案之间有明确的联系。
– 制度和规范，可为欲达到的组织性行为提供更多指引。这与企业设置到位的原则和政策有着明显联系。

• **与其他动力的关系**—与其他动力的联系包括：
– 流程可能会设计为完美的等级，但如果流程的利益相关者不希望像预期的那样执行流程，例如，如果他们的行为是某种不合规的现象之一时，则流程结果难以实现。
– 同样道理，组织结构可以按照教科书设计和构建，但如果决策未能实施——由于不同的个人实际行为或缺乏激励机制等——就不可能实现真正的企业 IT 治理和管理。
– 对于企业价值观和欲达到的行为而言，原则和政策是非常重要的沟通机制。

示例 11—质量改进

一家企业面临着使用新应用程序时不断出现的严重质量问题。尽管事实上健全的软件项目开发方法已经到位，但过于频繁的软件问题导致日常业务的操作问题。

调查表明，基于项目的及时交付和未超出预算，对开发团队成员和管理层进行了考核并予以奖励。但没有按质量标准或业务收益标准对他们进行测评。因此，在开发过程中，他们勤勉地专注于交付时间和削减成本，如，准时测试。调查还表明，与已建立的方法和规程的合规性实际上不存在，因为这样做要从开发预算（有利于质量）中拿出更多的时间。此外，当开发移交至操作团队时，组织结构实际上终止了正式的开发参与。从此以后，参与开发仅只是间接地通过已建立的事故管理和问题管理流程。

由此得到的教训是，必须为解决方案开发管理层和团队采用更好的激励机制，以鼓励关注质量工作。

示例 12—IT 相关的风险

与 IT 相关风险有关联的不健全或有问题的文化的部分症状包括：

- 实际风险偏好与政策转化之间不一致。管理层对待风险的真正价值观可以合理地积极些和敢于承担风险，然而，创建的政策则反映出相当保守的态度。因此，价值观和实现价值观的手段之间不配套，不可避免地导致冲突。例如，为管理层设定的激励机制和不一致的政策的强制执行之间会出现冲突。
- 存在一种“责备文化”。这种文化无论如何都应该避免；这种文化是相关的有效的沟通的最大障碍。在责备文化中，如果项目未能如期交付或未能满足预期，则业务单位倾向于指责IT部门。这样一来，他们就不能认识到业务单位的预先参与会影响到项目的成功。在极个别的情况下，业务单位会推卸未能满足预期的责任，而该单位则从未就其预期进行过明确的沟通。这种“责备游戏”仅只能损害跟单位之间的有效沟通，从而更进一步为延误火上浇油。如果要想在整个企业内培养协作精神，高层管理团队必须识别并迅速控制这种责备文化。

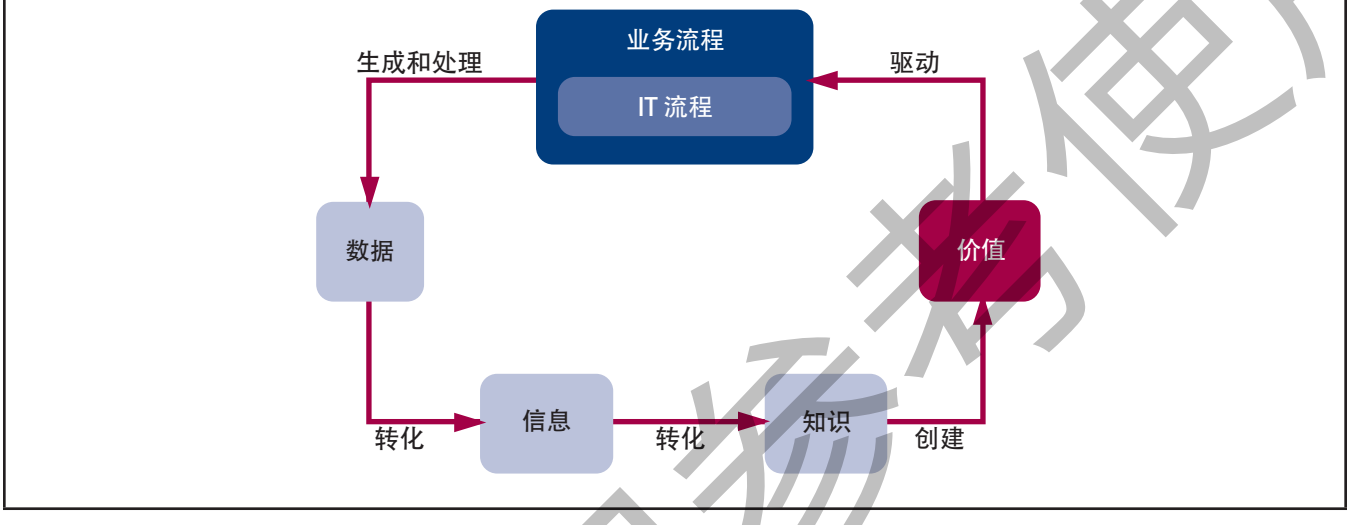
COBIT 5 动力：信息

导言—信息周期

信息动力处理的不仅是自动化信息，还包括所有与企业相关的信息。信息可能是结构化的，也可能是非结构化的，可能是正式化的，也可能是非正式化的。

信息可视为是处于企业的“信息周期”中的一个阶段。在信息周期中（**图 35**），业务流程生成和处理数据，并将其转化成信息和知识，并最终生成企业价值。信息动力的范围主要关注处于“信息周期”中的“信息”阶段，但 COBIT 5 也涵盖了数据和知识等方面。

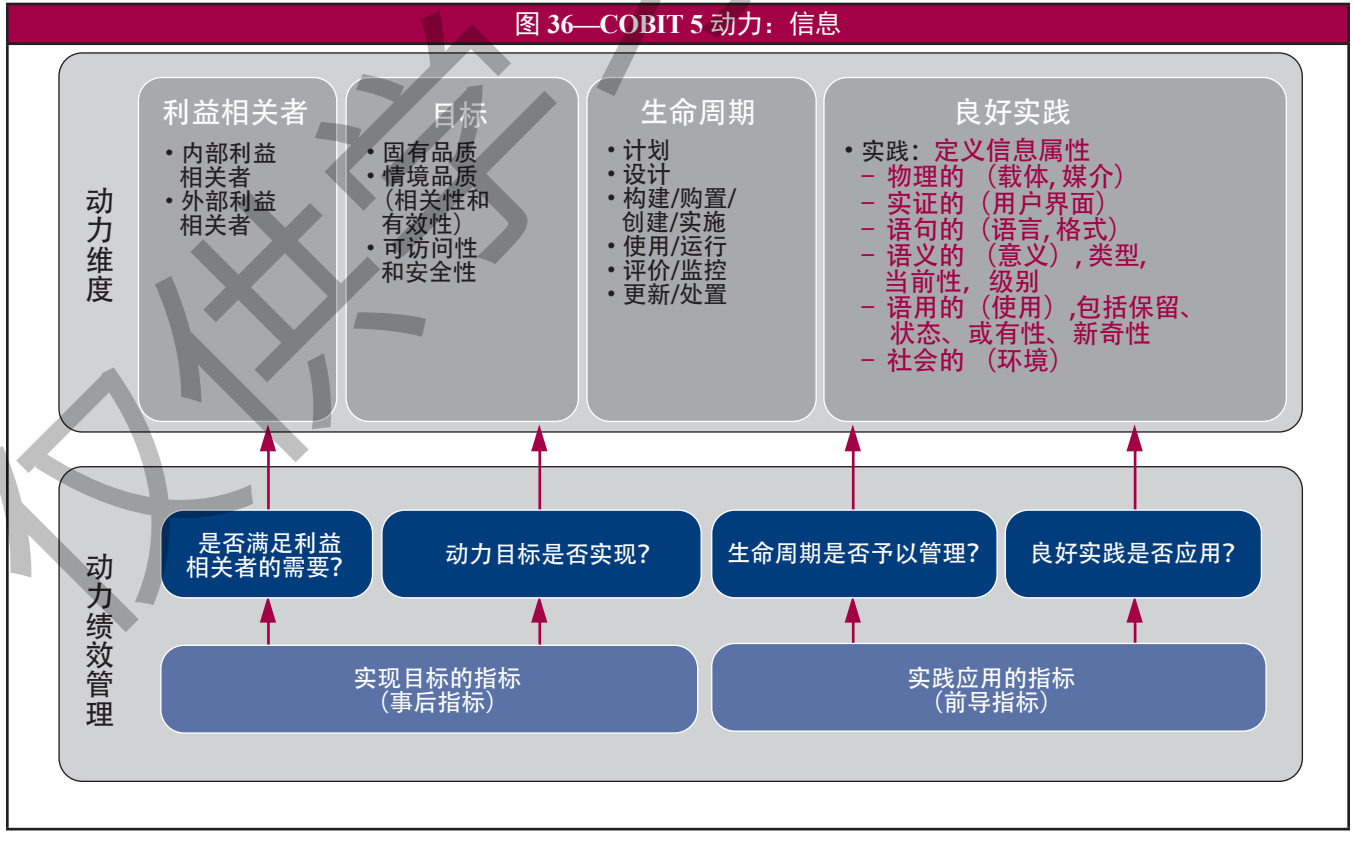
图 35—COBIT 5 元数据—信息周期



COBIT 5 信息动力

较之于通用动力描述，信息动力的具体细节如**图 36** 所示。

图 36—COBIT 5 动力：信息



信息模型（IM）表现出：

- **利益相关者**—可能是企业内部或外部的。通用模型还意味着除了识别利益相关者外，其利益也需要识别，例如，他们为什么关注或对信息感兴趣。

  就利益相关者存在的信息而论，处理信息中角色可能有不同的范畴，其范围包括详细的信息建议——如，建议具体数据或信息的角色，例如架构师、所有者、部门代表、托管人、供应商、受益人、模型师、质量经理、安全经理—到较通泛的信息建议——例如，信息生成者、信息管理者和信息消费者等之间的区别。
  – 信息生成者，负责创建信息。
  – 信息管理者，负责储存和维护信息。
  – 信息消费者，负责使用信息。

  这些范畴涉及到与信息资源相关的具体活动。这些活动又取决于信息的生命周期阶段；因此，为了发现具有适当信息模型粒度级别的角色范畴。可使用信息模型的信息生命周期维度。这就意味着信息利益相关者角色可以按照信息生命周期阶段来定义，例如，信息策划师、信息获得者、信息用户。同时，这也意味着信息利益相关者维度并不是独立的维度；不同的生命周期阶段拥有不同的利益相关者。

  鉴于相关角色取决于信息生命周期阶段，其利益可以与信息目标关联。
- **目标**—信息目标可分成三种品质的次级维度：

  固有品质—数据价值符合实际或真实价值的程度，这包括：
  – 精确性—信息正确与可靠的程度。
  – 客观性—信息无偏见、公正、不偏不倚的程度。
  – 可信性—信息被认为是真实可信的程度。
  – 公认性—信息就其来源或内容受到高度尊重的程度。

  环境性和表现性品质—信息运用于信息用户任务，并以可理解的和明确的方式表现的程度，可识别出信息品质取决于使用环境，具体包括：
  – 关联性—信息运用于并有助于现有任务的程度。
  – 完整性—信息没有缺失，具有针对当前任务的足够深度和广度之程度。
  – 当前性—信息针对当前任务是充分全新的程度。
  – 信息适量—信息量适合于当前任务的程度。
  – 简洁的表现性—信息紧凑表现的程度。
  – 一致的表现性—信息以相同格式表现的程度。
  – 可解读性—信息采用适当的语言、符号和单位并具有清晰的定义的程度。
  – 可理解性—信息易于理解的程度。
  – 易操作性—信息易于操作和应用于不同任务的程度。

  安全性/可访问性品质—信息可用或可获得的程度，具体包括：
  – 可用性/及时性—信息在需要时可用并能快速检索的程度。
  – 访问限制—信息限制于授权方的适当访问的程度。

  附件 F 中详细的描述了 COBIT 5 信息品质标准如何与 COBIT 4.1 信息标准进行比较。例如，完整性和精确性的信息目标覆盖了 COBIT 4.1 所定义的完整性。
- **生命周期**—信息的全生命周期需要予以考虑，而生命周期中不同阶段中的信息可能需要采用不同的方法。COBIT 5 动力区分出以下阶段：
  – **计划**—信息资源的创建和使用准备到位的阶段。在本阶段中的活动可能会涉及到目标识别，信息架构的规划以及标准和定义的开发，例如，数据定义、数据采集程序。
  – **设计**
  – **构建/购置**—信息资源购置的阶段。在本阶段中的活动可能涉及到创建数据记录、采购数据和载入外部文件。
  – **使用/操作**，具体包括：
    - 存储—信息电子化持有或硬盘保存的阶段（或仅仅是人为记忆）。在本阶段中的活动可能涉及到电子格式的信息储存（如，电子文件、数据库、数据仓库），或硬拷贝（如，纸质文件）。
    - 分享—信息通过分发方式可供使用的阶段。在本阶段中的活动可能涉及到牵涉将信息配置到可以访问和使用的场所等流程。例如。通过电子邮件发布文件。就电子持有的信息而言，这一生命周期可能会大量与储存阶段重叠，例如，通过数据库存取、文件/文档服务器分享信息。

- 使用—使用信息以完成目标的阶段。在本阶段中的活动可能涉及到所有相关信息的使用（如，管理决策、运行自动化流程），也可能包括诸如信息检索和信息形式转换。

根据《推动治理前进》中的观点，信息是一种企业治理的动力；因此，信息模型中规定的信息使用可以是企业治理的利益相关者在承担其角色、履行其活动和互动时需要信息的目的。

图 8 中涵盖了这些角色、活动和关系。利益相关者之间的互动需要信息流，这些信息流的目的在图解中予以说明：问责、授权、监控、设定导向、一致性、执行和控制。

– 监控—确保信息资源持续适当发挥作用的阶段，如具有价值。在本阶段中的活动可能涉及到保持信息的最新时效和各种信息管理的活动，例如，在数据仓库中增强、清理、合并、和移除重复的信息数据。
– 处置—当不再使用时对信息资源删除的阶段。在本阶段中的活动可能涉及到信息归档和销毁。

- **最佳实践**—在诸如经济、通讯理论、信息科学、知识管理等不同的学科中分别理解信息的概念不同；因此关于什么是信息没有万能一致的定义。然而，信息的性质可通过界定和描述其属性予以分类。

现提出以下方案以构建信息的不同特性：信息由六个级别或层次以界定和描述其属性，这六个层级体现出属性的连续统一体，其范围起始于信息的物理范畴，即这些属性与信息技术和信息采集、储存、处理、分配和展现的媒介相关，到信息使用、理解和作为的社会范畴。

以下是对层次和信息属性的描述：

- **物理范畴层**—凭经验可以观察到发生的所有现象的范畴。
  – 信息载体/媒介—能识别出信息的物理载体的属性，如，纸张、电子信号、声波等。
- **实证层**—对用于解码信息及其相互之间和来自背景噪音中进行区分的标示的实证观察。
  – 信息访问渠道—能识别出信息访问渠道的属性，如，用户界面。
- **语句层**—自然或人工语言的创建语句意义的规则和原则。语句指的是信息形式。
  – 代码/语言—能识别出用于信息解码的标识项语言/格式以合并形成语句结构的符号的规则之属性。
- **语义层**—从语句结构中创建意义的规则和原则。语义指的是信息的意义。
  – 信息类型—能识别出信息之类的属性，例如，财务与非财务信息、内部与外部信息源头、预知的/预测的与观察值，计划的与实现值。
  – 信息当前性—能识别出信息参照的时间范围的属性，例如，过去的信息、当前的和未来的。
  – 信息级别—能识别出信息详细等级的属性，例如，每年、每季度、每月的销售额。
- **语用层**—创建在人际交流中能履行具体目的的较大型语句结构的规则和架构。语用指的是信息使用。
  – 保留期—能识别出信息在销毁前信息可以保留时间的属性。
  – 信息状态—能识别出信息是可供使用还是历史性的属性
  – 新奇性—能识别出信息是否能创造出新知识或确认现有知识的属性，例如，信息与确认。
  – 或有性—能识别出必需先于本信息（才能视为信息）的信息的属性。
- **社会范畴层**—通过在语义的语用等级上使用语言结构，社会化构建的范畴，例如，合同、法律和文化。
  – 语境—能识别出信息有意义、被使用、有价值等的语境的属性，例如，文化语境、主题域语境。

关于信息的进一步思考—对信息和相关技术的投资是以业务案例为基础，其中包括成本效益分析。成本和效益不仅指有形的、可衡量的因素，还可以考虑到诸如竞争优势、客户满意度和技术不确定性等无形因素。只有当信息资源被应用或使用时，企业才能从中生成效益，因此，信息的价值仅只有通过使用（内部的或售出）才能测定，而信息没有内在价值。只有通过将信息灌输到行动中，才能生成价值。

信息模型是一种新模型，并且各种组件非常丰富。我们将在单独的出版物中对其进行开发。为了使 COBIT 5 用户觉得其更为具体，使其相关性在整体 COBIT 5 框架的环境中更为明确，我们提供了信息模型可能使用的示例 13, 14 和 15。

示例 13—用于信息规范的信息模型

当开发一项新应用程序时，信息模型可用于协助应用程序和相关信息或数据模型的规范。

信息模型的信息属性可用于定义将要使用到信息的应用程序和业务流程的规范。

例如，新系统的设计和规范需要明确：
- **物理层**—信息储存在何处？
- **实证层**—信息如何才能访问？
- **语句层**—信息如何创建和编码？
- **语义层**—这是何种信息？信息是何种等级？
- **语用层**—保留要求是什么？需要哪些其他信息才能使本信息有用和可用？

研究与信息生命周期结合的利益相关者维度，就能定义谁在信息生命周期的哪一个阶段需要何种数据访问权限。

当进行应用程序测试时，测试人员可以研究信息质量标准以开发一套综合的测试案例。

示例 14—用于确定必要保护的信息模型

企业内的安全团队可以从信息模型属性维度中收益。的确，需要对信息保护负责时，他们需要从以下方面查考：
- **物理层**—信息在物理上是如何及储存在何处？
- **实证层**—信息的访问渠道是什么？
- **语义层**—信息是何种类型？信息是否是当前的、或与过去相关的或是未来？
- **语用层**—保留要求是什么？信息是历史的还是可操作的？

使用这些属性将便于用户确定保护等级和必要的保护机制。

研究信息模型的另一种维度时，安全专业人员还可以考虑信息生命周期的阶段，因为需要在其各个生命周期阶段中予以保护。实际上，安全始于信息的规划阶段，并意味着有不同的储存、分享和配置信息的保护机制。信息模型能够确保信息在其全生命周期中得到保护。

示例 15—用于确定易于数据使用的信息模型

当执行业务流程（或应用程序）审核时，信息模型可用于协助执行一个对信息处理和交付以及其基础信息系统的一般性审核。质量标准可用于评估何种信息可用的程度——信息是否为完整的、及时可用的、真实正确的、相关的、和适量的。用户还可以考虑可访问性标准——当需要信息时是否可以访问并能得到充分保护。

这种审核甚至还可以进一步扩展以纳入表现标准，例如，那种信息的方便程度可以理解、解释、使用和操纵。

使用信息模型的信息质量标准进行的审核可为企业提供一份关于某项业务流程内当前信息质量的综合性和全面的视图。

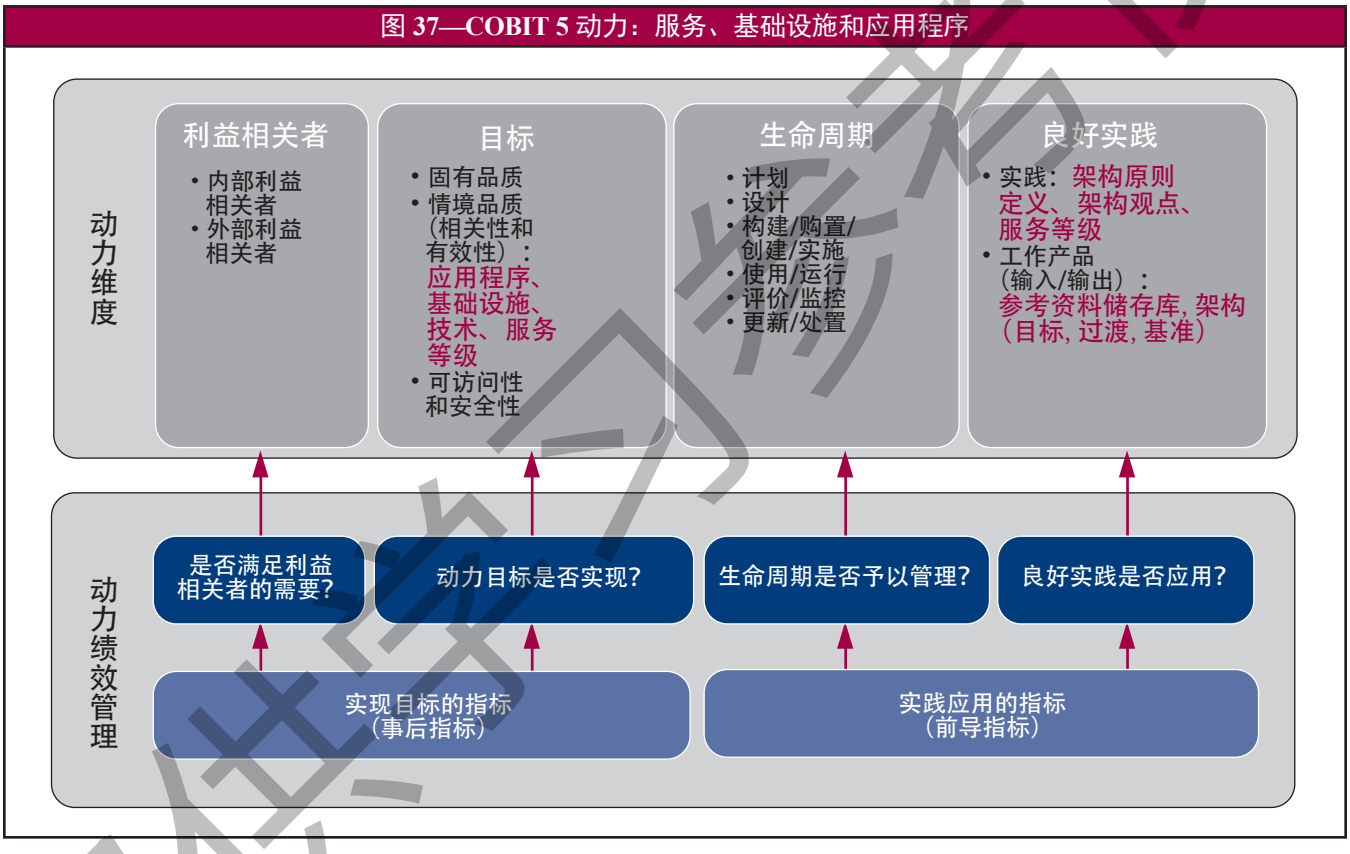
COBIT 5 动力：服务、基础设施和应用程序

服务能力指的是在交付 IT 相关服务中发挥作用的应用程序和基础设施等资源。

较之于通用动力描述，服务能力动力的具体细节如**图 37** 所示。

服务、基础设施和应用程序模型表现为：
- **利益相关者**—服务能力（服务、基础设施和应用程序的合称）利益相关者可能是内部的或外部的。服务可能由内部或外部各方提供——内部的IT部门、运营经理、外购提供商等。服务用户可能是内部的——业务用户——也可能是外部企业——合作伙伴、客户、供应商等。每一个利益相关者的利益需要确认，并要么是集中在交付充分的服务，或者是从提供商处接收所要求的服务。
- **目标**—服务等级能力的目标将以服务来表示—如应用程序、基础设施、技术---和服务等级，这是考虑到服务和服务等级对企业是最经济的。此外，目标与服务和服务如何提供及其结果相关联，例如，对成功支持的业务流程作出贡献。
- **生命周期**—服务能力具备生命周期。未来的或计划的服务能力在目标架构中予以典型描述。服务能力涵盖了诸如未来应用程序和目标基础设施模型等构建块，并且还描述了这些构建块之间的连锁和关系。

图 37—COBIT 5 动力：服务、基础设施和应用程序



使用或运行以交付当前 IT 服务的当前服务能力是以一个基线架构来描述。取决于目标架构的时间框架，可以定义一个过渡架构，而该架构显示出企业处于目标和基线架构之间的增长状态。
- **良好实践**—服务能力的良好实践包括：
  - 架构原则定义—架构原则是企业内管辖实施和 IT 相关资源使用的整体指导方针。潜在架构原则的实例包括：
    - **再利用**—作为目标或过渡架构之一部分，当设计和实施解决方案时，架构的共同组件应予以使用。
    - **购买与构建**—除非有内部进行开发的已批准的理论原则，否则应购买解决方案。

  - **简单性**—在满足企业要求的同时，企业架构的设计和维护应尽可能简单。
  - **敏捷性**—企业架构应将敏捷性整合以有效和高效率的方式满足不断变化的业务需要。
  - **开放性**—企业架构应利用开放性的行业标准。
- 企业定义最适当的架构观点以满足不同利益相关者的需要。其内容包括用模型、目录和指标来描述的基准、目标或过渡架构；例如，可通过应用程序界面图解描述一项应用程序的架构，该图解会显示出使用中（或计划的）应用程序以及其中的界面。
- 设置一个架构储存库，该库可用于储存不同类型的架构输出，包括架构原则和标准、架构参考模型和其他架构可交付项，这些内容将界定服务的构建块，例如：
  - 提供业务功能性的应用程序；
  - 技术基础设施，包括硬件、系统软件和网络基础设施；
  - 物理基础设施。
- 需要服务提供商定义和实现的服务等级。

架构框架和服务能力的外部良好实践已经存在，这包括可用于快速跟踪架构可交付项创建的指引、模板或标准。实例包括：

- TOGAF[16]（开放群组企业架构框架）提供了一个“技术参考模型”和一个“整合的信息基础设施参考模型”。
- ITIL（信息技术基础架构资料库）就如何设计和运行服务提供了综合指引。

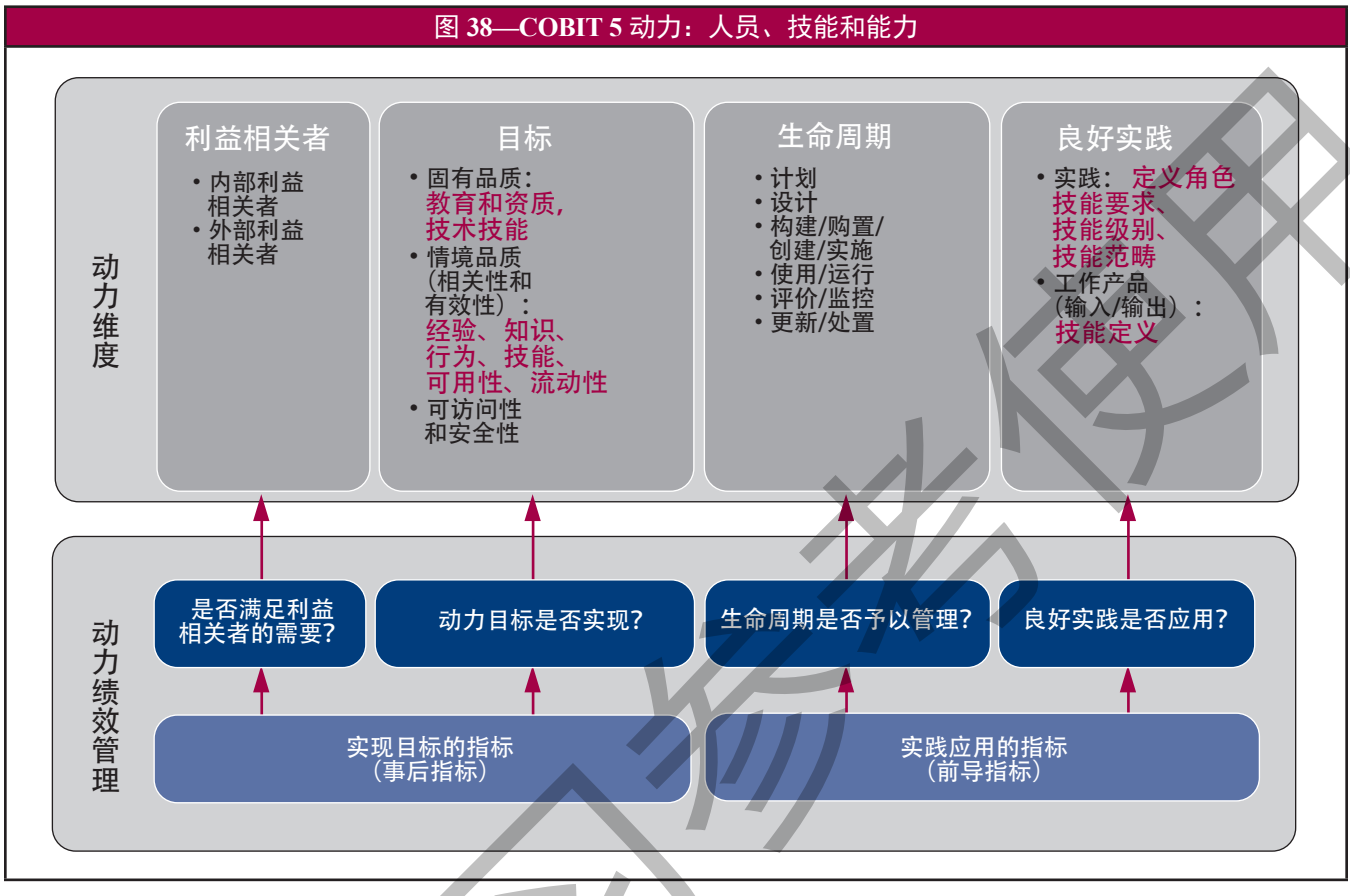
- **与其他动力的关系**—与其他动力的联系包括：
  - 信息是服务能力之一，而服务能力是通过流程驱动以交付内外部服务。
  - 当需要构建服务导向的文化时，文化和行为方面也具有相关性。
  - 在 COBIT 5 之内，管理实践和活动的输入和输出可能包括服务能力，这需要将服务能力输入或交付作为输出。

[16] *www.opengroup.org/togaf*

COBIT 5 动力：人员、技能和能力

较之于通用动力描述，针对人员、技能和能力动力的具体细节如**图 38** 所示。

图 38—COBIT 5 动力：人员、技能和能力



人员、技能和能力模型表现为：

- **利益相关者**—技能和能力利益相关者是内部的也可能是企业外部的。不同的利益相关者承担不同的角色---业务经理、项目经理、合作伙伴、竞争对手、招聘专员、培训师、系统开发员、技术IT专家等---每种角色要求具备一套截然不同的技能组合。
- **目标**—技能和能力目标相关于教育和资质等级、技术技能、经验等级知识和行为技能，这些都是提供和执行成功的流程活动、组织结构角色等所必需的。人员目标包括员工可用性和流动率的正确等级。
- **生命周期：**
  - 技能和能力具有生命周期。一个企业必须明白其当前的技能基础是什么，并计划需要什么。这受到企业战略和目标以及其他方面的影响。技能需要发展（如，通过培训）或获得（如，通过招聘），并部署在组织结构内各种不同的角色中。如果某项获得自动化或外包，则技能可能需要出卖。
  - 定期地，如每年度地，企业需要评估技能基础以了解已经出现的进化，而这种进化将会注入到下一阶段计划的流程中。
  - 这种评估还可注入到人力资源的奖励和表彰流程。
- **良好实践：**
  - 技能和能力的良好实践包括为各利益相关者扮演的每种角色界定所需的客观的技能要求。这可以通过不同的技能级别和技能范畴予以描述。就每一技能范畴中的每种适当的技能级别而言，应有可用的定义。技能范畴与所进行的IT相关活动相对应，例如信息管理、业务分析。

– 其他良好实践：
  • 良好实践还有外部来源，例如“信息时代的技能框架” (SFIA),[17] 该框架提供了综合的技能定义。
  • 映射于 COBIT 5 流程领域的潜在技能范畴实例如**图 39** 所示。

图 39—COBIT 5 技能范畴

流程领域	技能范畴实例
评价、指导和监控 (EDM)	• 企业 IT 治理
定位、计划和组织 (APO)	• IT 政策制订 • IT 战略 • 企业架构 • 创新 • 财务管理 • 投资组合管理
构建、购置和实施 (BAI)	• 业务分析 • 项目管理 • 使用性评价 • 要求定义和管理 • 编程 • 系统人体工程学 • 软件调试 • 容量管理
交付、服务和支持 (DSS)	• 可用性管理 • 问题管理 • 服务台与事故管理 • 安全管理 • IT 运营 • 数据库管理
监控、评价和评估 (MEA)	• 合规审核 • 绩效监控 • 控制审计

• **与其他动力的关系**—与其他动力的联系包括：
  – 需要技能和能力在组织结构内履行流程活动和作出决策。相反的，部分流程旨在支持技能和能力的生命周期。
  – 通过行为技能与文化、道德和行为形成一种联系，这会驱动个人行为，并受到个人道德和组织机构道德的影响。
  – 技能定义也是信息，因此需要考虑到信息动力的最佳实践。

[17] *www.sfia.org.uk*

附件 H
词汇表

英文	中文	定义
Accountable party (RACI)	责任方(RACI)	对某一主题、流程、或范围最终负责的个人、团体或实体。 在 RACI 图（执行、负责、商议和告知）中，回答的问题是：**谁对任务的成功负责？**
Accountability of governance	治理责任	治理应保证通过评价利益相关方之需求、条件和选项，通过优先次序和决策确定方向，并监控计划的绩效、合规、及进度，从而实现企业的目标。在大多数企业中，治理是董事长领导下的董事会之责任。
Activity	活动	在 COBIT 中，针对流程操作所采取的主要行动，为实现成功的企业 IT 治理和管理的管理实践準则，这些活动应： • 描述一套必要的、充分的、以行动为导向的实施步骤，以实现一项治理实践或管理实践； • 考虑流程的输入和输出； • 是以公认接受的标准和最佳实践为基础； • 支持确定明确的角色和责任； • 非惯例性，且需要不时修改和开发以适合于企业的具体程序。
Alignment	一致性	企业 IT 治理和管理的动力支持企业目标和战略的一种状态。
Application architecture	应用架构	对于管理对象所必需的处理信息和支持企业目标的能力的逻辑分组描述。
Architecture board	架构委员会	负责对企业架构相关事务和决策予以指导、并确定架构政策和标准的利益相关者和专家构成的团队。
Authentication	身份认证	指验证用户身份和用户的对计算机信息有适当的访问权限的行为。 范围注解：鉴证：身份认证旨在防止欺诈登录的行为，也可以用于验证数据的正确性。
Baseline architecture	基准架构	进入一个架构循环评审和重新设计之前，对业务系统元素的总体和基础设计的现有描述。
Benefits realisation	收益实现	治理的目标之一。为企业带来新的收益，维护和扩展现有收益形式，和消除那些不再能创造足够价值的计划和资产。
Business continuity	业务持续性	预防、减轻业务中断或从中断中恢复。相关的术语“业务恢复计划”、“灾难恢复计划”和“应急计划”也可用于此类情形之中，且都集中在持续性的恢复方面；因此，“可恢复性”方面也应予以考虑。
Business goal	业务目标	将企业使命从意图说明转变成绩效目标和结构的具体体现。
Business process control	业务流程控制	旨在为一个业务流程实现其目的提供合理保障的系列政策、程序、实务、和组织结构。
Chargeback	借项冲回	一个公司内部各单位所发生的经费的重新分配。 范围注释：借项冲回非常重要，其原因在于如果没有这样一项政策，则会导致对某一项产品或服务的收益性的误解，因为某些关键经费会被忽略或是根据任意公式计算。

英文	中文	定义
COBIT	信息及相关技术控制目标	1. COBIT 5：即以前所称的“信息及相关技术控制目标”（COBIT），现在仅用作其第五迭代的缩略词。这是一套完整的、全球公认的、用于治理和管理企业信息和技术（IT）的框架，该框架支持企业行政层和管理层确定和实现其业务目标和相关的 IT 目标。COBIT 描述了五项原则和七项动力，用以支持企业开发、实施、和持续改进以及监控良好的 IT 相关的治理和管理实践。 范围注释：COBIT 较早的版本集中于 IT 流程、及其管理和控制，以及 IT 治理等方面。采纳和使用 COBIT 框架是经由一系列不断增加的支持产品家族的指导予以支持。（详情参见：www.isaca.org/cobit.） 2. COBIT 4.1 及较早版本：即以前所称的“信息及相关技术控制目标”（COBIT），这是一套完整的、全球公认的、IT 流程框架，以提供一种综合的 IT 治理、管理、控制和鉴证模型的方式，支持业务和 IT 行政层及管理层确定和实现其业务目标和相关的 IT 目标。COBIT 描述了 IT 流程和所关联的控制目标、管理指南（活动、职责、责任和绩效矩阵）、以及成熟度模型。COBIT 支持企业管理层开发、实施、和持续改进以及监控良好的 IT 相关的实践。 范围注释：采纳和使用 COBIT 框架是经由以下方面的指导予以支持：为行政层和管理层（《董事会 IT 治理简报》（第 2 版））、为 IT 治理实施者（《COBIT 快速入门》（第 2 版）、《IT 治理实施指南：使用 COBIT 和Val IT》（第 2 版）、《COBIT 控制实践：指导实现成功 IT 治理的控制目标》）和为 IT 鉴证和审计专业人员（《IT 鉴证指南：使用 COBIT》）。还有支持其适用于某些立法和监管要求（如：《针对萨班斯-奥克斯利法案的 IT 控制目标》、《针对‘巴塞尔新资本协议’的 IT 控制目标》）和信息安全相关的（如：《COBIT 安全基准》）的指南。COBIT 还映射到其他框架和标准，以阐明 IT 管理生命周期的整个覆盖面，并在企业采用多重 IT 相关的框架和标准中支持其使用。
Code of ethics	道德规范	旨在通过规定运用于某些情形中的组织价值观和规则，以影响员工的个人和组织行为的文件；此类文件的采用旨在帮助企业中需要作出决策的那些人理解何为“对”和“错”，并将这种理解运用到其决策之中。
Competence	胜任	成功履行某项具体任务、行动或职能的能力。
Consulted party (RACI)	商议方 (RACI)	指在活动中应寻求其意见的人（双向沟通）。 在 RACI 图中，回答的问题是：**谁提供输入（信息）？**关键角色提供输入（信息）。应注意的是，还要由责任或执行角色从其他单元或外部合作伙伴处获得信息；然而，从列示的角色处获得的输入应予以考虑，并且如有必要，可采取适当的行动逐步升级，这包括流程所有者和/或指导委员会的信息。

英文	中文	定义
Context	上下文	一整套可能会影响到或决定一个企业、实体、流程或个体如何行动的内部和外部因素。 范围注释：上下文包括： • 技术上下文—影响一个机构从数据中提取价值的能力之技术因素； • 数据上下文—数据的准确性、可用性、当前性和质量； • 技能和知识—一般经验、和分析性、技术性以及业务技能； • 组织性和文化性上下文—政治因素和某个机构是否更看重数据而不是直觉； • 战略性上下文—企业的战略目标。
Control	控制	管理风险的手段，包括具有行政、技术、管理、或法律属性的政策、程序、指南、实践和组织结构；也可用于安全措施或对策的同义词。
Culture	文化	一种行为、信仰、设想、态度和行事方式的模式。
Driver	动因	激发或影响某一企业或个人如何行动的外部和内部因素。
Enterprise goal	企业目标	参见业务目标。
Enterprise governance	企业治理	董事会和高管层为提供战略方向而制定的一整套的职责和实践，以确保目标的实现、风险可控和企业资源的有效利用。也可以指一种聚焦于整个企业的治理观；所有其他方面必须与之保持一致的最高等次的治理观念。
Full economic life cycle	全经济生命周期	指一个时间段，在这个时间段中预计会从一项投资计划中获得实质性业务收益，和/或这项投资计划中预计会发生的实质性费用（包括投资、运行和资产报废费用）。
Good practice	良好实践	经证实并让多个企业成功使用、并产生可靠结果的活动或流程。
Governance	治理	治理确保利益相关者的需要、条件和选项得到评估，以决定平衡、协商一致、需要实现的企业目标；通过优先等级和决策来设定导向；并监控商定的导向和目标的绩效和合规性。
Governance/management practice	治理/管理实践	就每一项 COBIT 流程而言，治理和管理实践为有效和务实的企业 IT 治理和管理提供了一整套高层次要求，也就是治理机构和管理层行为的体现。
Governance enabler	治理动力	某些（有形或无形）能帮助实现有效治理的因素。
Governance framework	治理框架	框架是一种基本的概念结构，用于解决和处理复杂问题；是一项治理动力；是一套概念、设想、和实践，规定某件事情是如何得以处理或理解，确定所涉及的实体之间的关系和所涉及各方的角色，以及界限（什么包含在、或未包含在治理体系之内）。 实例：COBIT 和 COSO 的内部控制--均为整体框架。
Governance of enterprise IT	企业 IT 治理	一种治理观，能确保信息及其相关技术支持企业战略并使企业能够实现其目标，也包括 IT 功能性治理，如，保证能高效率和有效地提供 IT 能力。
Information	信息	像其他重要的业务资产一样，是一种企业业务上不可或缺的资产，其存在的形式多种多样：书面打印或书写、电子方式存储、通过邮寄或电子方式传递、在胶片上显示、或交谈中口述等等。

英文	中文	定义
Informed party (RACI)	告知对象 (RACI)	指应被告知最新活动进展情况的人（单向沟通）。 在 RACI 图中，回答的问题是：**谁接收信息？** 即被告知任务的成果和/或接收可交付项的角色。作为“责任方”的角色应当总是接收适当的信息以监督任务的进程，就像“执行方”角色在其负责的领域中接收适当的信息一样。
Inputs and outputs	输入和输出	被认为是支持流程运行所必需的流程工作产品/产物；能启动关键决策，提供流程活动的记录和审计轨迹，并能在出现事故时启动后续跟进。输入和输出是在关键管理实践层面上予以定义，可能会包括仅在流程被使用的某些工作产品，并且通常是其他流程的关键输入。COBIT 5 中说明的输入和输出不应视为详尽无遗的，因为附加的信息流可能根据某一特定企业的环境和流程框架额外予以定义。
Investment portfolio	投资组合	已经考虑的和/或已经进行的投资集合。
IT application	IT 应用	利用或借助于 IT 所构成为业务流程一部分的电子功能。
IT goal	IT 目标	描述企业 IT 在支持企业目标中欲达到的成果的说明。这种成果可能是一种产物、一项重大的变更、或一项重大的能力改进。
IT service	IT 服务	每日为客户提供的 IT 基础设施、应用和客户使用的支持，具体实例包括服务台、设备供应和迁移、和安全授权。
Management	管理	管理层计划、构建、运行和监控与治理机构设定导向一致的活动，以实现企业目标。
Model	模型	一种方式去描述一套既定组件以及这些组件相互之间是如何产生关联，用以说明一个对象、系统或概念的主要工作方式。
Metric	度量	一种可量化的实体，能够对一个流程目标的实现进行测评。度量应具备 SMART 特征，即具体性、可测性、可行动性、相关性、和及时性。完整的度量指导定义使用的单元、测量频度、理想的目标值（如适用）和实施测量的程序以及对评估判读的程序。
Objective	目标	一种对欲达到结果的表述。
Organisational structure	组织结构	一种治理和管理的动力，包括企业及其结构，层级和从属机构。 例如：指导委员会。
Output	输出	参见“输入和输出”。
Owner	所有者	持有或拥有某一企业、实体或资产权利和责任的个人或群体，如，流程所有者、系统所有者。
Policy	政策	由管理层正式表述的整体意图和方向。
Principle	原则	一种治理和管理的动力，由企业持有的价值观和根本设想、以及用以指导和限定企业决策界限、企业内部和外部沟通、托管（代为保管他人拥有的资产）的信念等构成。 例如：伦理章程、社会责任章程。

英文	中文	定义
Process	流程	通常是受企业政策和程序影响的一系列实践的集合，这种集合从若干资源（包括其他流程）中获得投入，并且利用这些投入去得到产出（如，产品、服务）。 范围注释：流程对于现有的、负责任的所有者具有清晰的业务原由，对于流程的执行中具有明确的角色和责任，和测量绩效的手段。
Process (capability) attribute	流程（能力）属性	ISO/IEC 15504: 适用于任何流程的可测量的流程能力特征。
Process capability	流程能力	ISO/IEC 15504: 一种能满足当前或预估的业务目标的流程能力的特征。
Process goal	流程目标	一种描述某一流程欲达到的成果的阐述；所体现的成果可能是某一产物、某一重大状态变更或其他流程的重大能力改进。
Programme and project management office (PMO)	规划和项目管理办公室 (PMO)	负责支持规划及项目经理，收集、评估和报告有关规划和项目的行为信息之职能部门。
Quality	质量	达到目的（实现既定价值）的结构。
RACI chart	RACI 图	描述在组织框架内哪些人是执行方、责任方、商议方和告知对象的图表
Resource	资源	能帮助组织实现其目标的任何企业资产。
Resource optimisation	资源优化	治理目标之一，涉及到有效地、高效地、负责任地使用全部资源——人力、财务、设备、设施等。
Responsible party (RACI)	执行方 (RACI)	指必须确保活动能成功完成的人。 在 RACI 图中，回答的问题是：**谁在完成任务？** 在履行列示的活动中承担主要运行职责，并创造出欲达到的结果的角色。
Risk	风险	发生某一事件及其后果概率的组合 (ISO/IEC 73)
Risk management	风险管理	治理目标之一，必需识别风险、评估该风险的影响和可能性、和制订策略，如规避风险、减少风险的负面影响和/或转移风险，并遵循企业的风险偏好予以管理。
Service catalogue	服务目录	关于所有客户可运用的 IT 服务的结构性信息。
Services	服务	参见 IT 服务。
Skill	技能	为实现预定结果所习得的能力。
Stakeholder	利益相关者	任何对企业负有责任、或具有预期或某些利益的人，如，股东、用户、政府机构、供应商、客户和公众。
System of internal control	内部控制体系	旨在提供合理保证使企业的目标得以实现，使得意外事件得以预防、或探知并被纠正的政策、标准、计划、程序和组织结构。
Value creation	创造价值	当三种基本目标（收益实现、风险优化和资源优化）得以平衡时，一个企业所实现的主要治理目标。

本页特此留空