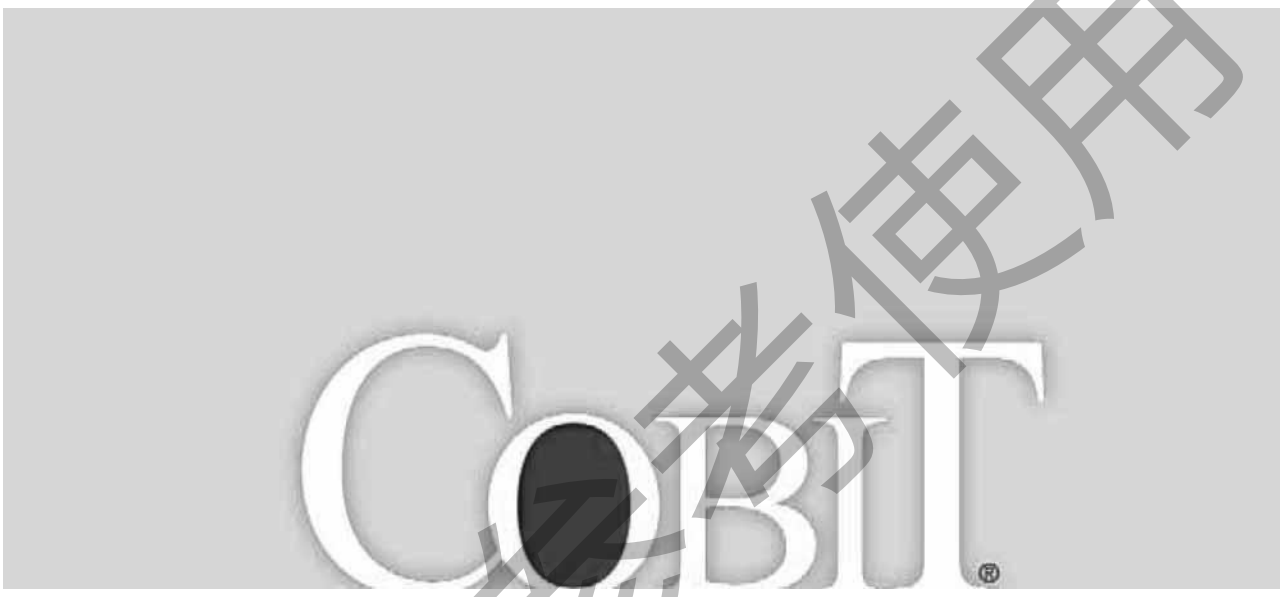
GOVERNANCE INSTITUTE®

LEADING THE IT GOVERNANCE COMMUNITY



4.1

框架

控制目标

管理指南

成熟度模型

COBIT 4.1

The IT Governance Institute®

The IT Governance Institute (ITGI™) (*www.itgi.org*) was established in 1998 to advance international thinking and standards in directing and controlling an enterprise's information technology. Effective IT governance helps ensure that IT supports business goals, optimises business investment in IT, and appropriately manages IT-related risks and opportunities. ITGI offers original research, electronic resources and case studies to assist enterprise leaders and boards of directors in their IT governance responsibilities.

IT治理研究院®

IT 治理研究院（ITGI™，网址：*www.itgi.org*）成立于 1998 年，旨在指导和控制企业信息科技方面，提升国际化的思维与标准。有效的 IT 治理有助于确保 IT 对业务目标的支持，使 IT 投资达到最优，同时能恰当地管理 IT 相关领域风险和机遇。IT 治理研究院提供原始调查、电子资料及案例研究等资源，协助企业领导层、董事会履行 IT 治理职责。

Disclaimer

ITGI created COBIT 4.1 ("Work") primarily as an educational resource for controls professionals. ITGI 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, the controls professional should apply his or her own professional judgment to the specific circumstances presented by the particular systems or information technology environment.

免责声明

ITGI 创建的“COBIT 4.1”（著作）主要作为 IT 控制专业人员的教材。ITGI 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。IT 控制专业人员应该根据具体的系统和信息技术环境，通过自身的专业判断来决定适当的信息、流程或测试。

Disclosure

公开声明

IT Governance Institute
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.590.7491
Fax: +1.847.253.1443
E-mail: *info@itgi.org*
Web site: *www.itgi.org*

ACKNOWLEDGEMENTS 感谢

IT Governance Institute wishes to recognise（ITGI 希望表彰）:

Expert Developers and Reviewers（开发与审核专家）

Mark Adler, CISA, CISM, CIA, CISSP, Allstate Ins. Co., USA
Peter Andrews, CISA, CITP, MCMI, PJA Consulting, UK
Georges Ataya, CISA, CISM, CISSP, MSCS, PBA, Solvay Business School, Belgium
Gary Austin, CISA, CIA, CISSP, CGFM, KPMG LLP, USA
Gary S. Baker, CA, Deloitte & Touche, Canada
David H. Barnett, CISM, CISSP, Applera Corp., USA
Christine Bellino, CPA, CITP, Jefferson Wells, USA
John W. Beveridge, CISA, CISM, CFE, CGFM, CQA, Massachusetts Office of the State Auditor, USA
Alan Boardman, CISA, CISM, CA, CISSP, Fox IT, UK
David Bonewell, CISA, CISSP-ISSEP, Accomac Consulting LLC, USA
Dirk Bruyndonckx, CISA, CISM, KPMG Advisory, Belgium
Don Canilglia, CISA, CISM, USA
Luis A. Capua, CISM, Sindicatura General de la Nación, Argentina
Boyd Carter, PMP, Elegantsolutions.ca, Canada
Dan Casciano, CISA, Ernst & Young LLP, USA
Sean V. Casey, CISA, CPA, USA
Sushil Chatterji, Edutech, Singapore
Edward Chavannes, CISA, CISSP, Ernst & Young LLP, USA
Christina Cheng, CISA, CISSP, SSCP, Deloitte & Touche LLP, USA
Dharmesh Choksey, CISA, CPA, CISSP, PMP, KPMG LLP, USA
Jeffrey D. Custer, CISA, CPA, CIA, Ernst & Young LLP, USA
Beverly G. Davis, CISA, Federal Home Loan Bank of San Francisco, USA
Peter De Bruyne, CISA, Banksys, Belgium
Steven De Haes, University of Antwerp Management School, Belgium
Peter De Koninck, CISA, CFSA, CIA, SWIFT SC, Belgium
Philip De Picker, CISA, MCA, National Bank of Belgium, Belgium
Kimberly de Vries, CISA, PMP, Zurich Financial Services, USA
Roger S. Debreceny, Ph.D., FCPA, University of Hawaii, USA
Zama Dlamini, Deloitte & Touche LLP, South Africa
Rupert Dodds, CISA, CISM, FCA, KPMG, New Zealand
Troy DuMoulin, Pink Elephant, Canada
Bill A. Durrand, CISA, CISM, CA, Ernst & Young LLP, Canada
Justus Ekeigwe, CISA, MBCS, Deloitte & Touche LLP, USA
Rafael Eduardo Fabius, CISA, Republica AFAP S.A., Uruguay
Urs Fischer, CISA, CIA, CPA (Swiss), Swiss Life, Switzerland
Christopher Fox, ACA, PricewaterhouseCoopers, USA
Bob Frelinger, CISA, Sun Microsystems Inc., USA
Zhiwei Fu, Ph. D, Fannie Mae, USA
Monique Garsoux, Dexia Bank, Belgium
Edson Gin, CISA, CFE, SSCP, USA
Sauvik Ghosh, CISA, CIA, CISSP, CPA, Ernst & Young LLP, USA
Guy Groner, CISA, CIA, CISSP, USA
Erik Guldentops, CISA, CISM, University of Antwerp Management School, Belgium
Gary Hardy, IT Winners, South Africa
Jimmy Heschl, CISA, CISM, KPMG, Austria
Benjamin K. Hsaio, CISA, Federal Deposit Insurance Corp., USA
Tom Hughes, Acumen Alliance, Australia
Monica Jain, CSQA, Covansys Corp., US
Wayne D. Jones, CISA, Australian National Audit Office, Australia
John A. Kay, CISA, USA
Lisa Kinyon, CISA, Countrywide, USA
Rodney Kocot, Systems Control and Security Inc., USA
Luc Kordel, CISA, CISM, CISSP, CIA, RE, RFA, Dexia Bank, Belgium
Linda Kostic, CISA, CPA, USA
John W. Lainhart IV, CISA, CISM, IBM, USA
Philip Le Grand, Capita Education Services, UK.
Elsa K. Lee, CISA, CISM, CSQA, AdvanSoft International Inc., USA
Kenny K. Lee, CISA, CISSP, Countrywide SMART Governance, USA
Debbie Lew, CISA, Ernst & Young LLP, USA
Donald Lorete, CPA, Deloitte & Touche LLP, USA
Addie C.P. Lui, MCSA, MCSE, First Hawaiian Bank, USA
Debra Mallette, CISA, CSSBB, Kaiser Permanente, USA
Charles Mansour, CISA, Charles Mansour Audit & Risk Service, UK

ACKNOWLEDGEMENTS CONT. 感谢（续）

Mario Micallef, CPAA, FIA, National Australia Bank Group, Australia
Niels Thor Mikkelsen, CISA, CIA, Danske Bank, Denmark
John Mitchell, CISA, CFE, CITP, FBCS, FIIA, MIIA, QiCA, LHS Business Control, UK
Anita Montgomery, CISA, CIA, Countrywide, USA
Karl Muise, CISA, City National Bank, USA
Jay S. Munnelly, CISA, CIA, CGFM, Federal Deposit Insurance Corp., USA
Sang Nguyen, CISA, CISSP, MCSE, Nova Southeastern University, USA
Ed O'Donnell, Ph.D., CPA, University of Kansas, USA
Sue Owen, Department of Veterans Affairs, Australia
Robert G. Parker, CISA, CA, CMC, FCA, Robert G. Parker Consulting, Canada
Robert Payne, Trencor Services (Pty) Ltd., South Africa
Thomas Phelps IV, CISA, PricewaterhouseCoopers LLP, USA
Vitor Prisca, CISM, Novabase, Portugal
Martin Rosenberg, Ph.D., IT Business Management, UK
Claus Rosenquist, CISA, TrygVesata, Denmark
Jaco Sadie, Sasol, South Africa
Max Shanahan, CISA, FCPA, Max Shanahan & Associates, Australia
Craig W. Silverthorne, CISA, CISM, CPA, IBM Business Consulting Services, USA
Chad Smith, Great-West Life, Canada
Roger Southgate, CISA, CISM, FCCA, CubeIT Management Ltd., UK
Paula Spinner, CSC, USA
Mark Stanley, CISA, Toyota Financial Services, USA
Dirk E. Steuperaert, CISA, PricewaterhouseCoopers, Belgium
Robert E. Stroud, CA Inc., USA
Scott L. Summers, Ph.D., Brigham Young University, USA
Lance M. Turcato, CISA, CISM, CPA, City of Phoenix IT Audit Division, USA
Wim Van Grembergen, Ph.D., University of Antwerp Management School, Belgium
Johan Van Grieken, CISA, Deloitte, Belgium
Greet Volders, Voquals NV, Belgium
Thomas M. Wagner, Gartner Inc., USA
Robert M. Walters, CISA, CPA, CGA, Office of the Comptroller General, Canada
Freddy Withagels, CISA, Capgemini, Belgium
Tom Wong, CISA, CIA, CMA, Ernst & Young LLP, Canada
Amanda Xu, CISA, PMP, KPMG LLP, USA

ITGI Board of Trustees（ITGI 董事会）

Everett C. Johnson, CPA, Deloitte & Touche LLP (retired), USA, International President
Georges Ataya, CISA, CISM, CISSP, Solvay Business School, Belgium, Vice President
William C. Boni, CISM, Motorola, USA, Vice President
Avinash Kadam, CISA, CISM, CISSP, CBCP, GSEC, GCIH, Miel e-Security Pvt. Ltd., India, Vice President
Jean-Louis Leignel, MAGE Conseil, France, Vice President
Lucio Augusto Molina Focazzio, CISA, Colombia, Vice President
Howard Nicholson, CISA, City of Salisbury, Australia, Vice President
Frank Yam, CISA, FHKIoD, FHKCS, FFA, CIA, CFE, CCP, CFSA, Focus Strategic Group, Hong Kong, Vice President
Marios Damianides, CISA, CISM, CA, CPA, Ernst & Young LLP, USA, Past International President
Robert S. Roussey, CPA, University of Southern California, USA, Past International President
Ronald Saull, CSP, Great-West Life and IGM Financial, Canada, Trustee

IT Governance Committee（IT治理委员会）

Tony Hayes, FCPA, Queensland Government, Australia, Chair
Max Blecher, Virtual Alliance, South Africa
Sushil Chatterji, Edutech, Singapore
Anil Jogani, CISA, FCA, Tally Solutions Limited, UK
John W. Lainhart IV, CISA, CISM, IBM, USA
Rómulo Lomparte, CISA, Banco de Crédito BCP, Peru
Michael Schirmbrand, Ph.D., CISA, CISM, CPA, KPMG LLP, Austria
Ronald Saull, CSP, Great-West Life Assurance and IGM Financial, Canada

ACKNOWLEDGEMENTS CONT. 感谢（续）

COBIT Steering Committee（COBIT指导委员会）
Roger Debreceny, Ph.D., FCPA, University of Hawaii, USA, Chair
Gary S. Baker, CA, Deloitte & Touche, Canada
Dan Casciano, CISA, Ernst & Young LLP, USA
Steven De Haes, University of Antwerp Management School, Belgium
Peter De Koninck, CISA, CFSA, CIA, SWIFT SC, Belgium
Rafael Eduardo Fabius, CISA, República AFAP SA, Uruguay
Urs Fischer, CISA, CIA, CPA (Swiss), Swiss Life, Switzerland
Erik Guldentops, CISA, CISM, University of Antwerp Management School, Belgium
Gary Hardy, IT Winners, South Africa
Jimmy Heschl, CISA, CISM, KPMG, Austria
Debbie A. Lew, CISA, Ernst & Young LLP, USA
Maxwell J. Shanahan, CISA, FCPA, Max Shanahan & Associates, Australia
Dirk Steuperaert, CISA, PricewaterhouseCoopers LLC, Belgium
Robert E. Stroud, CA Inc., USA

ITGI Advisory Panel（ITGI咨询小组）
Ronald Saull, CSP, Great-West Life Assurance and IGM Financial, Canada, Chair
Roland Bader, F. Hoffmann-La Roche AG, Switzerland
Linda Betz, IBM Corporation, USA
Jean-Pierre Corniou, Renault, France
Rob Clyde, CISM, Symantec, USA
Richard Granger, NHS Connecting for Health, UK
Howard Schmidt, CISM, R&H Security Consulting LLC, USA
Alex Siow Yuen Khong, StarHub Ltd., Singapore
Amit Yoran, Yoran Associates, USA

ITGI Affiliates and Sponsors（ITGI会员及赞助商）
ISACA chapters
American Institute for Certified Public Accountants
ASIS International
The Center for Internet Security
Commonwealth Association of Corporate Governance
FIDA Inform
Information Security Forum
The Information Systems Security Association
Institut de la Gouvernance des Systèmes d'Information
Institute of Management Accountants
ISACA
ITGI Japan
Solvay Business School
University of Antwerp Management School
Aldion Consulting Pte. Lte.
CA
Hewlett-Packard
IBM
LogLogic Inc.
Phoenix Business and Systems Process Inc.
Symantec Corporation
Wolcott Group LLC
World Pass IT Solutions

感谢中国建设银行组织专业团队完成本书的翻译

团队负责人：

金磐石 CISA 中国建设银行审计部总经理

成员：

杨　军 CISA CIA 中国建设银行审计部副总经理
邱　斌 CISA CISP 中国建设银行审计部
王卫东 CISA 中国建设银行审计部
文　平 CISA 中国建设银行成都审计分部
吴　婷 CISA 中国建设银行审计部
吴　华 CISA CIA 中国建设银行湖南总审计室
贺永班 CISA CISP 中国建设银行新疆总审计室
石洪钧 CISA 中国建设银行武汉审计分部
韩鸿莺 CISA CIA 中国建设银行吉林总审计室
高仁贵 CISA 中国建设银行青岛总审计室
张　震 CISA 中国建设银行沈阳审计分部
冀慎华 CISA CIA 中国建设银行山东总审计室
李　懋 CISA CIA 中国建设银行贵州总审计室
程　斌 CISA 中国建设银行河南总审计室
王凤华 CISA 中国建设银行天津审计分部
陈　青 CISA 中国建设银行厦门总审计室
粟海一 CISA 中国建设银行宜昌总审计室
王华忠 CISA 中国建设银行重庆总审计室
曾繁锋 CISA CIA 中国建设银行广州审计分部
毕力格图 CISA 中国建设银行内蒙古总审计室
薛彦忠 CISA 中国建设银行山西总审计室
李国威 CISA 中国建设银行云南总审计室
孙祥久 CISA CPA 中国建设银行审计部
王明德 CISA 中国建设银行审计部
王　忠 博士　中国国家审计署
高　卓 CISA 中国建设银行审计部
陈晓胜 CISA 中国建设银行西安审计分部
鲁　艺 CISA 中国建设银行河南总审计室
操　祯 CISA CPA 中国建设银行上海审计分部

感谢ISACA香港分会组织专家团队对本书进行了审核

团队总监：

任家明（Mr. Frank Yam） CISA, FHKCS, FHKIoD, FFA, CIA, CFSA, CFE, CCP，任职于科信集团国际有限公司（Focus Strategic Group Limited）

团队负责人：

叶天祐（Mr. Andrew Ip）, CISM,CISA,CIA,FCPA，供职于八达通卡有限公司（Octopus Cards Limited）

成员：

顾向圣（Mr. Peter Koo Heung Shing） CGEIT, CISA, CISM，任职于德勤•关黄陈方会计师行（Deloitte）

马国钧（Mr. Luke Ma） CGEIT, CISA, CISSP，任职于德勤•关黄陈方会计师行（Deloitte）

冼嘉乐（Mr. Samual Sinn） CISA，任职于安永会计师事务所（Ernst & Young）

黎国勇（Mr. Danny Le）CISA, CISM，任职于毕马威会计师事务所（KPMG）

吴剑林（Mr. Philip Ng） CISA, CISSP, AICPA，任职于毕马威会计师事务所（KPMG）

季瑞华（Mr. William Gee） CISA, FCA, FHKICPA，任职于普华永道会计师事务所（PriceWaterhouseCoopers）

陈细明（Mr. Simon Chan）CGEIT,CISA,ASA,CIA，任职于中国银行(香港)有限公司（Bank of China (Hong Kong) Ltd.）

施小贞（Ms. Yantl Sze），任职于Itpreneurs

蒋胜（Mr. Sheng Jiang） PMP, ITIL，任职于Itpreneurs

何廸生（Mr. Dixon Ho） CISM，任职于微软中国有限公司（Microsoft China）

阎振平(Mr. Yan Zhen Ping)，任职于中国光大银行(China Everbright Bank)

朱辉(Mr. Hui Zhu), CGEIT,CISA,CISM，任职于BlueImpact Ltd.

张金城博士(Prof. Zhang Jincheng),任职于南京审计学院(Nanjing Audit University)

王昊博士(Prof. Wang Hao),任职于南京审计学院(Nanjing Audit University)

汪加才博士（Prof. Wang Jiacai）,任职于南京审计学院(Nanjing Audit University)

李庭燎博士（Dr. Li Tingliao） CISA,任职于南京审计学院(Nanjing Audit University)

张耀忠（Stanley Cheung） CISA, CISSP, CBCP，任职于香港商品交易所（HK Mercantile Exchange）

目 录

目录

目录

目录

1. 总体概述

对于许多企业而言，支持其业务的信息与技术是最具价值的资产，但是这些资产通常得不到理解与重视。成功的企业已经意识到信息技术所带来的收益，并利用信息技术为利益相关方创造价值。此外，这些企业也能够理解并管理相关的风险，如增强对法律法规的遵循以及多数业务流程对信息技术（IT）的重要依赖。

人们认识到保障 IT 价值、管理与 IT 有关的风险、增加对信息的控制要求已成为公司治理的关键要素。价值、风险和控制构成了 IT 治理的核心。

IT 治理是董事会和高级管理层的责任，它包括领导能力、组织结构和流程，以确保组织的 IT 能支持和增强组织的业务战略和目标。

此外，为了确保组织的 IT 能支持组织的业务目标，IT 治理融合了许多良好的实践和做法并将其制度化。IT 治理确保企业可以充分利用信息，进而实现收益最大化、充分利用机遇、获得竞争优势。要实现这些结果需要一个 IT 控制框架，该框架可以满足并支持那些广为接受的企业治理、风险管理和其它类似管理的控制框架，如 COSO 的内部控制整体框架。

组织应象保证所有资产一样，保证组织信息的质量、可信和安全要求。管理层应尽可能优化利用可获得的 IT 资源〔包括应用系统、信息、基础设施和人员)。为履行这些职责及实现组织的目标，管理层应了解企业 IT 架构的情况并决定提供什么样的治理和控制。

信息及相关技术控制目标（CobiT®）提供了跨领域和流程框架的良好惯例，并以一个可管理和合理的架构来展示活动。CobiT 的良好实践代表了专家的一致性意见，他们更多的关注于控制而非执行。这些实践将有助于优化 IT 所带动的投资，确保服务交付，并提供措施以便问题出现时可作判断。

为成功交付满足业务要求的 IT 服务，管理层应建立内部控制体系或框架。CobiT 控制框架通过下列措施来满足这些需求：

- 与业务要求保持联系；
- 采用公认的流程模型来组织 IT 活动；
- 识别需要平衡的重要 IT 资源；
- 定义管理层应考虑的控制目标。

CobiT 的业务导向包括：建立 IT 目标与业务目标的联系，提供测量 IT 目标和业务目标成果的度量和成熟度模型，确定业务和 IT 流程所有者的相关职责。

CobiT 通过流程模型来标识其流程的焦点，该流程模型把 IT 进一步细分为与计划、建设、运营和监控领域的职责相一致的 4 个域及 34 个流程，用以提供一个端到端的 IT 视角。企业架构的概念有助于识别流程成功所需的关键资源，即应用系统、信息、基础设施和人员。

总之，为了提供实现企业目标所需的信息，需要通过一系列自然分组化的流程来管理 IT 资源。

但是企业如何使 IT 受控，以便交付企业所需的信息?如何管理风险并保障企业所依赖的关键 IT 资源的安全?企业如何确保 IT 实现其目标并支持企业业务?

首先，管理层需要一个控制目标，该控制目标定义了实施策略、计划和程序、组织结构的最终目标，以提供以下合理保证：

- 实现业务目标；
- 预防或检测和纠正不期望的事件。

其次，在今天复杂的环境下，管理层需要不断搜集简明、及时的信息，快速并成功地做出关于价值、风险和控制的决策，尽管这个决策非常困难。衡量什么，如何衡量?企业需要一个客观的衡量标准，以确定他们处于什么位置，哪些地方需要改进，哪些地方需采取管理工具以监控这种改进。

图 1 所示为管理信息的传统例子，以及曾用来寻求这些问题答案的管理信息工具，但这些仪表盘管理需要指针，平衡记分卡管理需要衡量指标，基准管理需要用于比较的尺度。

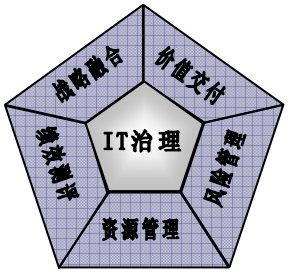
图 1-管理信息

以下的 COBIT 定义回答了上述问题，可以用来确定并监控这些适当的 IT 控制和绩效水平要求：

- **IT 流程绩效和能力的基准管理**：即成熟度模型，源自软件工程学院的能力成熟度模型（CMM）；
- **IT 流程的目标和度量**：基于罗伯特．卡普兰和大卫．诺顿所创建的平衡计分卡的原理，规定并测量相关的成果和绩效；
- **活动目标**：基于 COBIT 的控制目标，对流程进行控制。

基于 COBIT 成熟度模型对流程能力进行评估是 IT 治理实施的关键要素之一。识别关键的 IT 流程和控制后，成熟度模型可以用来识别成熟度的差距并可向管理层显示该差距的具体情况，继而可帮助组织制定相应的行动计划，对这些流程进行改进以达到期望的成熟度级别。

图 2-IT 治理关注领域



- **战略融合**：关注于确保业务计划和 IT 计划的联系；规定、保持和验证 IT 价值建议；使 IT 运营与企业运营一致。
- **价值交付**：在整个交付周期内实施价值建议，确保 IT 实现了预期的战略收益，集中关注成本的优化，提供了 IT 的固有价值。
- **资源管理**：对 IT 资源（应用系统、信息、基础设施和人员）的优化投资并适当管理，关键问题在于知识和基础设施的优化。
- **风险管理**：要求企业的高层管理者具备良好的风险意识，清晰了解企业对风险的承担偏好，了解合规性要求，企业所面临的显著风险的透明化，并将风险管理的职责嵌入组织之中。
- **绩效测评**：追踪并监控战略实施、项目终结、资源使用、流程绩效、服务支付以及诸如平衡记分卡的使用，平衡记分卡将战略转化为措施，这些措施可以实现传统财务管理方面无法测量的目标。

这样，CobiT 为 IT 治理提供了一个框架（**图 2**），进而确保：

- IT 与业务一致；
- IT 保障业务并实现收益最大化；
- IT 资源使用的有效性；
- IT 风险的适当管理。

绩效测评是 IT 治理的关键，CobiT 支持绩效测评。绩效测评包括设定并监控可测量的目标，包括 IT 流程必需交付的目标(流程成果)和 IT 流程如何交付其目标(流程能力和绩效)。多项调研已经表明，IT 成本、价值和风险管理缺乏透明是驱动 IT 治理的最重要的一个因素。相对于其他关注的领域，提高透明度主要通过绩效测评来实现。

这些 IT 治理关注领域描述了高级管理层在企业内部进行 IT 治理时必需考虑的主题。运营管理层利用流程来组织、管理日常的 IT 活动。CobiT 提供了一个通用的流程模型，该模型展示了 IT 职能的通用流程，为 IT 操作人员及业务管理者提供了一个利于理解的通用参考模型。CobiT 流程模型已映射到 IT 治理关注的各个域(见附录 II，IT 流程映射到 IT 治理的关注域、COSO、CobiT IT 资源和 CobiT 信息标准)，这种映射提供了高级管理层期望的管理与运营管理层需要实施的管理之间的桥梁。

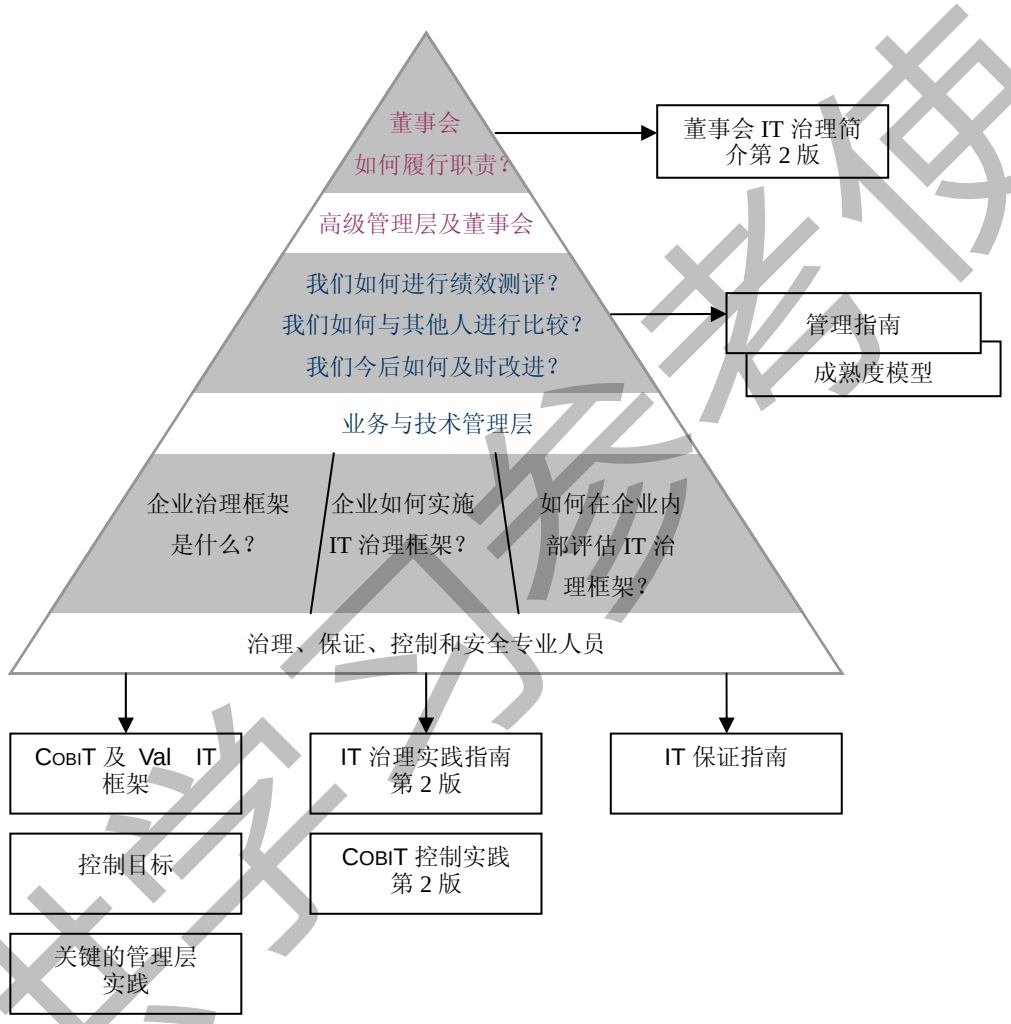
为实现有效治理，高级管理层要求运营管理层在既定的控制框架内对所有的 IT 流程进行控制。CobiT 通过 IT 流程来组织 IT 控制目标，因此，框架建立了 IT 治理要求、IT 流程和 IT 控制之间的清晰联系。

CobiT 定位于一个高级管理层的角度，主要关注于需要采取何种措施才能实现 IT 的适当管理和控制。CobiT 还与其它更为详细的 IT 标准和最佳惯例保持一致和兼容(见附录Ⅳ，CobiT4.1 主要参考资料)。CobiT 作为这些不同参考材料的集大成者，将关键目标归集到一个伞状框架内，并与治理和业务需求建立联系。

COSO(及类似框架)通常作为企业的内部控制框架，COBIT 则是通用的 IT 控制框架。COBIT 的产品族分为三个层次（**图 3**），以支持：

- 高级管理层及董事会；
- 业务管理层和 IT 管理层；
- 从事治理、保证、控制和安全的专业人士。

图 3-COBIT 产品族



该 COBIT 产品图展示了通用的产品族及其主要对象，也包括一些特定目的的衍生产品（IT Control Objectives for Sarbanes-Oxley, 2nd Edition），安全领域的衍生产品（COBIT Security Baseline and Information Security Governance: Guidance for Boards of Directors and Executive Management），或用于特殊的企业的衍生产品（COBIT Quickstart for small and medium-sized enterprises or for large enterprises wishing to ramp up to a more extensive IT governance implementation）。

简要地，COBIT 产品包括：

- Board Briefing on IT Governance, 2nd Edition——用于帮助高级管理层理解IT治理的重要性、主要问题及他们的管理职责；
- Management guidelines/maturity models——用于协助分配职责、测量绩效、基准管

理和阐述能力差距；

• Frameworks——通过 IT 域和流程来组织 IT 治理目标和最佳实务，并将它们与业务需求联系起来；

• Control objectives——提供了管理层对每个 IT 流程进行有效控制需要考虑的高端需求的全集；

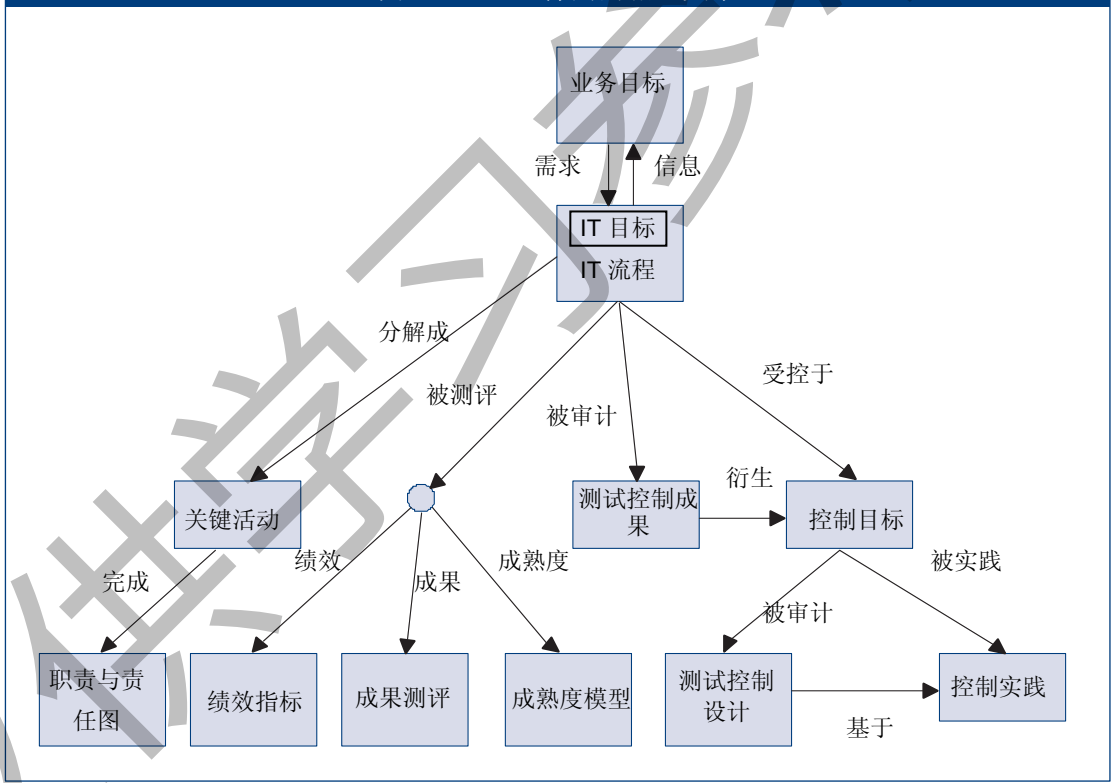
• IT Governance Implementation Guide: Using COBIT® and Val IT TM, 2nd Edition——为使用COBIT、Val IT来实施IT治理提供通用的路线图；

• COBIT® Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance, 2nd Edition——提供了实施这些控制目标的原因和实施方法；

• IT Assurance Guide: Using COBIT®——提供了如何使用 COBIT，用所建议的测试步骤来支持对所有 IT 流程和控制目标的保证活动。

COBIT 的内容图如**图 3** 所示，说明了涉及的主要对象、它们所关注的 IT 治理问题以及为这些问题提供答案的通用的产品。还有一些特殊需求的产品，象安全和特殊企业等。所有的这些 COBIT 组件互相关联，为不同的读者提供治理、管理、控制和保证需求方面的支持，如**图 4** 所示。

图 4-COBIT 组件间的相互关系



COBIT 是一个框架和支持性的工具集，为管理层架起与利益相关方沟通控制需求、技术性问题、业务风险和控制等级的桥梁。COBIT 能够促进在整个企业内建立清晰的 IT 控制策略和良好实践。COBIT 也处于不断的更新当中，并与其他标准和指南相兼容。因此，COBIT 已经变成 IT 最佳实践的集大成者，其伞形的 IT 治理框架有助于理解并管理与 IT 有关的风险及收益。COBIT 的流程结构和其高级别的业务导向的方法提供了一个端到端的 IT 视角，并有助于作出涉及 IT 的决策。

将 COBIT 作为实施 IT 治理框架的价值在于：

- 以业务为中心，IT 与业务较好地保持一致；
- 为管理层提供了一个更好的 IT 视角；
- 在流程导向的基础上，清晰界定的所有者关系及职责；
- 易于被第三方及监管机构所接受；
- 基于通用的语言，可以被所有的利益相关方所理解；
- 满足 COSO 对于 IT 控制环境的要求。

本文档的其它部分描述了 COBIT 体系框架和其他所有的 COBIT 核心组成部分，按照 4 个 IT 域和 34 个 IT 流程进行组织，为其它主要的 COBIT 指南提供了方便易用的参考。后文的附录也提供了有用的参考文献。

最完整和更新及时的有关 COBIT 及相关产品包括：在线工具、实施指南、案例研究、时事通讯和教育资料，可以参见 *www.isaca.org/cobit*。

2. COBIT 框架

COBIT 使命：

研究、制定、发布及促进推广一个权威性的、最新的、国际公认的IT 治理控制框架，该框架可用于企业的业务管理层、IT 专业人士及审计专业人员的日常工作。

2.1. IT 治理控制框架需求

IT 治理控制框架明确了 IT 治理的必要性、利益相关者及其所需完成的任务。

2.1.1. 为什么使用

最高管理层日益重视信息对于企业成功的重大影响。管理层希望加强了解 IT 运营的方式以及调整 IT 资源成功获得竞争优势的可能性。最高管理层尤其需要明确良好的信息管理是否可以使企业：

- 提高目标实现的可能性；
- 更好的学习能力和适应能力；
- 明智地管理所面临的风险；
- 及时发现并抓住机遇。

成功的企业能够理解风险，并充分利用 IT 的优势找到对策以：

- 使 IT 战略与业务战略保持一致；
- 向股东和投资者保证，组织在控制 IT 风险方面满足应有的审慎性标准；
- 将 IT 战略和目标逐层分解到企业；
- 实现 IT 投资价值；
- 建立能够充分实现战略和目标的组织架构；
- 在业务、IT 和外部相关方之间建立建设性的关系及有效的沟通渠道；
- 考评 IT 绩效。

企业如果未采用并实施 IT 治理和控制框架，则无法有效满足以下业务和治理方面的要求：

- 建立 IT 与业务需求的联系；
- 针对这些业务需求制定清晰的 IT 绩效；
- 采用公认的过程模型组织 IT 活动；
- 识别关键 IT 资源以作调整；
- 制定所需的管理控制目标。

此外，IT 治理和控制框架已经变成 IT 管理最佳实践的一部分，并促使建立 IT 治理，符合不断增加的合规性要求。

IT 最佳实践由于以下因素已变得越来越重要：

- 业务管理层和董事会期望获得较好的 IT 投资回报，即 IT 可以满足业务需求以增加利益相关方收益；
- 关注普遍增加的 IT 支出；
- 在隐私保护和金融报告领域（如，the US Sarbanes-Oxley Act, Basel II）以及财政、药品和卫生保健等部门，要求 IT 控制满足有关的合规性要求；
- 选择服务提供商，管理服务外包和采购；
- 更加复杂的 IT 相关风险，如网络安全；

- IT 治理包括采用控制框架和最佳实践以监控和改进关键 IT 活动，进而增加业务价值并降低业务风险；
- 尽可能通过遵循标准的而非特别制定的方法来满足优化成本的需要；
- 逐步成熟并被广泛接受的控制框架，如：COBIT、 ITIL(IT Infrastructure Library) 、ISO27000 系列的信息安全相关标准（ISO9001：2000 质量管理系统需求）、CMMI(Capability Maturity Model® Integration)、PRINCE2（Projects in Controlled Environments 2）和 *A Guide to the Project Management Body of Knowledge* (PMBOK)；
- 企业对遵循公认的标准和基准进行评估的需要。

2.1.2. 谁使用

治理和控制框架适用于不同类型的内外部利益相关方，每一个利益相关方都有特定的需求：

- 关注 IT 投资创造价值的企业内部利益相关方：
  - 投资决策人；
  - 需求制定人；
  - IT 服务对象。
- 提供 IT 服务的内外部利益相关方：
  - IT 组织和流程的管理人员；
  - IT 功能开发人员；
  - IT 运营服务人员。
- 负责控制或风险管理的内外部利益相关方：
  - 负责安全、隐私和/或风险管理的人员；
  - 履行合规职能的人员；
  - 要求或提供保证服务的人员。

2.1.3. 应用方法

为满足上述要求，IT 治理和控制框架应：

- 以业务为中心，确保 IT 目标与业务目标保持一致；
- 采用预定结构的框架，以便易于使用，以流程为导向明确所需覆盖的范围及程度；
- 采纳与 IT 最佳实践和标准一致的做法，并独立于特定的技术；
- 使用能够被所有利益相关方理解的通用术语和定义；
- 通过与公认的公司治理标准(COSO)以及监管机构、外部审计人员所要求的 IT 控制保持一致，帮助组织满足合规性要求。

2.2. COBIT 如何满足要求

为适应上述要求，COBIT 框架基于以下主要特点制定：以业务为中心、以流程为导向、以控制为基础、以绩效测评为驱动。

2.2.1. 以业务为中心

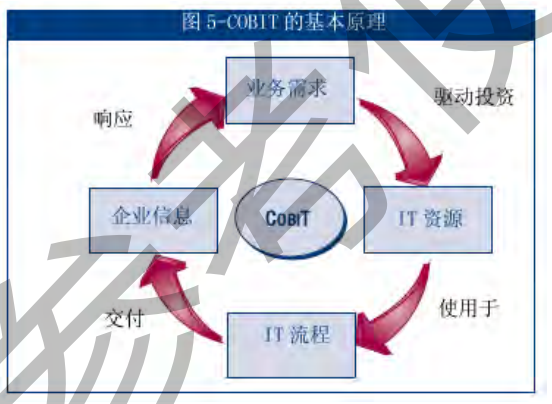
COBIT 的主题是面向业务，除了供 IT 服务人员、用户和审计人员使用外，更重要的是，COBIT 为管理人员和业务流程所有人提供了一个综合指南。

COBIT 框架基于以下原理(**见图 5**)：

为提供实现业务目标所需的企业信息，企业需要采用一套系统化的 IT 流程来投资、管理和控制 IT 资源，来提供企业信息服务。

管理并控制信息是 COBIT 框架的核心，有助于确保与业务需求保持一致。

图 5-COBIT 的基本原理



COBIT 信息标准

为满足业务目标，信息应符合一定的控制标准，COBIT 称之为信息的业务需求。基于一般更广泛的质量、可信和安全要求，七个独立又有所重叠的信息标准定义如下：

- **效果：**涉及到信息与业务流程相关程度的属性，以及信息交付的及时性、正确性、一致性和可用性；
- **效率：**通过优化(生产率最高且符合经济效益)资源使用来提供信息；
- **保密性：**保护敏感信息，避免未经授权的披露；
- **完整性：**与信息的准确度和完全性有关的属性，与业务价值和预期相一致；
- **可用性：**与业务流程对信息的当前或未来可使用性相关的属性，也包括所需资源和相关能力的安全性；
- **符合性：**涉及业务流程与所需遵守的法律、法规及合同约定之间的符合程度的属性，即外部的强制要求和内部政策的遵循性；
- **可靠性：**为管理者提供可靠的信息，以运营相关实体并履行所赋予的职责。

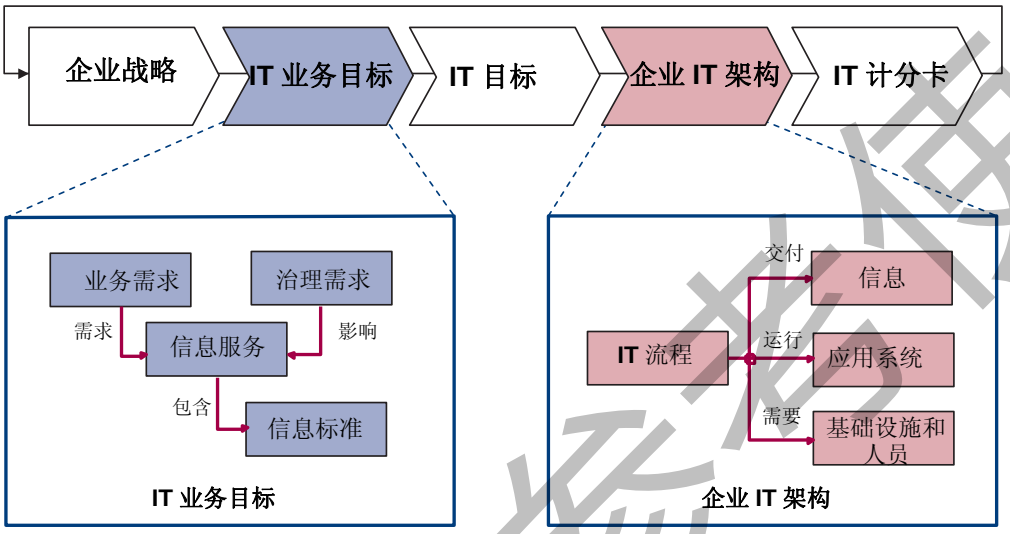
业务目标和 IT 目标

信息标准在为定义业务需求提供一个通用方法的同时，也制订了一系列一般业务目标和 IT 目标，作为与业务相关的、更加细化的基础用以建立业务需求和制定这些目标的衡量指标。企业利用 IT 来激发业务动力，也可以称之为‘IT 的业务目标’。附录 I 提供了一般业务目标和 IT 目标的矩阵，以及他们是如何映射到信息标准的。这一示例可用来指导企业如何确定具体的业务要求、目标和衡量指标。

如果希望 IT 成功交付服务来支持企业战略，那么应明确业务(客户)需求的所有者关系

和需求方向、并清楚理解 IT(供应商)应交付的内容以及如何交付。**图 6** 展示了如何将企业战略转化为 IT 驱动目标(即 IT 的业务目标)，这些目标能清晰地带出 IT 自身目标（IT 目标），进而帮助成功的制订执行 IT 战略（即企业战略的一部分）所需的 IT 资源和能力（企业 IT 架构）[1]。

图 6-定义 IT 目标和企业 IT 架构



一旦确定了一致的目标，接下来便需要监控这些目标以确保实际的交付能够满足预期需求，监控需要通过由目标和 IT 计分卡导出的衡量指标来实现。

为使用户能理解 IT 目标和 IT 计分卡，所有目标和相关衡量指标将以用户能理解的业务术语来表达，这样，一个适当调整目标的层级，使业务部门确信 IT 能可靠地支持企业目标。

附录 I，目标和流程对应表，提供了一般业务目标如何与 IT 目标、IT 流程和信息标准相对应的全局视图。该表将有助于阐述 COBIT 的应用范围，COBIT 和业务驱动力之间的总体业务关系。如**图 6** 所示，这些驱动力来源于企业的业务管理层和治理层，前者注重功能和交付速度，后者更注重成本效益、投资回报（ROI）和合规性。

IT 资源

IT 部门通过一系列清晰的既定流程来达到目标，这些流程利用人员技能、技术基础设施来运行自动化业务应用系统以处理业务信息。这些资源与流程一起构成了企业 IT 架构(**图 6**)。

为满足 IT 的业务需求，企业需投入资源创建充分的技术能力（如企业资源计划[ERP]系统）以支持业务能力（如实施供应链管理），进而获得预期结果（如增加销售和财务收益）。

[1] 需要注意的是：制定和实施企业 IT 架构，也需要制定内部 IT 目标，这些目标并非直接来自业务目标但对业务目标有贡献。

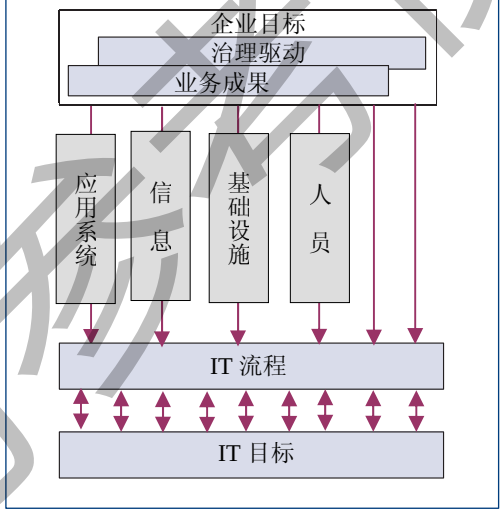
COBIT 对 IT 资源定义如下：

- **应用系统：**是处理信息的自动化系统及操作规程。
- **信息：**是信息系统输入、处理和输出的各种格式的数据，用于业务的各个方面。
- **基础设施：**是保障应用系统处理信息所需的技术和设施(硬件、操作系统、数据库管理系统、网络、多媒体等，以及放置、支持上述设施的环境)；
- **人员：**是计划、组织、获取、实施、交付、支持、监控和评价信息系统及服务的人员。人员可以是内部人员、外包或合同所需人员。

图 7 概述了 IT 的业务目标对如何使用 IT 流程来管理 IT 资源以交付 IT 目标的影响。

2.2.2. 以流程为导向

图 7-管理 IT 资源实现 IT 目标



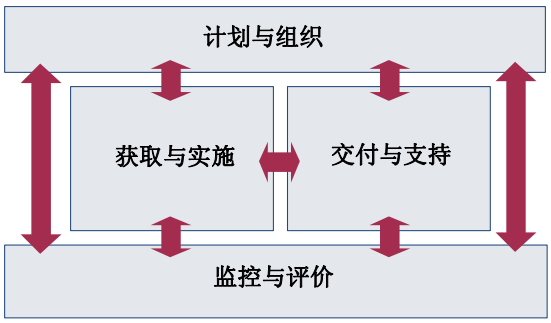
COBIT 在四个域内将 IT 活动定义为一个流程模型。这四个域分别是：计划与组织、获取与实施、交付与支持、监控与评价。这些域映射到传统的 IT 职责域：计划、建设、运行和监控。

COBIT 框架给企业每个成员审视和管理 IT 活动提供了一个参考流程模型和通用语言。其中一个通向最佳治理的重要及初始步骤是把操作模型与通用语言融合到所有涉及 IT 的业务，这样也为衡量和监控 IT 绩效、与服务人员沟通和整合最佳管理实务提供了一个框架。流程模型能强化流程的所有关系，加强责任的界定和追究。

为有效治理 IT，评估 IT 内所需管理的活动与风险是很重要的，这通常归纳为计划、建设、运营和监控四个职责域。如**图 8** 所示，在 COBIT 框架中这些域称为：

- **计划与组织(PO)：**为提供解决方案(AI)和提供服务(DS)落实方针；
- **获取与实施(AI)：**提供解决方案并将其转化成为服务；
- **交付与支持(DS)：**接受解决方案，使之为最终用户所用；
- **监控与评价(ME)：**监控所有流程确保遵循既定方针。

图 8-COBIT 的四个域



计划与组织(PO)

该域涵盖了战略和战术，致力于识别 IT 为实现业务目标作出最佳贡献的途径。实现战略愿景需要从不同的角度和层次去计划、沟通及管理，这需要设立一个适当的组织结构及技术基础设施。

这一领域主要阐述以下管理问题：

- IT 战略与业务战略是否一致?
- 企业是否实现了对资源的最佳利用?
- 组织中每一位成员是否理解 IT 目标?
- 是否理解 IT 风险并加以妥善管理?
- IT 系统的质量能否适当地满足业务需求?

获取与实施(AI)

为实现 IT 战略，应确认、开发/采购、实施 IT 解决方案并将其整合到业务流程中。此外，该域还涵盖了现有系统的变更与维护以确保持续满足业务目标。这一领域主要阐述下列管理问题：

- 新项目所提供的解决方案是否满足业务需求?
- 新项目是否在预算内按时交付?
- 新系统能否按预期运行?
- 系统的更改是否未影响当前的业务运行?

交付与支持(DS)

这一领域主要关注所需服务的实际交付情况，包括服务交付、安全和持续性管理、用户服务支持、数据和操作设施管理。该领域主要阐述下列管理问题：

- 是否按照业务的优先级交付 IT 服务?
- IT 成本是否得到?
- 员工是否能有效和安全地使用 IT 系统?
- 是否充分落实信息安全的机密性、完整性、可用性?

监控与评价(ME)

应定期评估所有 IT 流程的质量以及与控制要求的符合程度。该领域涉及绩效管理、内部控制的监督、合规和治理等内容，主要阐述下列管理问题：

- IT 绩效测评能否及时检查出问题?
- 管理层是否确保内部控制的效果和效率?
- IT 绩效是否能回溯到业务目标?
- 是否对信息安全的机密性、完整性、可用性进行充分控制?

通过这四个领域，COBIT 归纳了 34 个常用 IT 流程（完整列表参照**图 22**）。多数企业已建立了明确的 IT 计划、建设、运行和监控职责，或多数有相同的关键流程，但是很少有企业完整地使用 COBIT 的 34 个流程或建立与之完全一致的流程架构。COBIT 提供一系列完整的流程列表，用于验证活动和职责的完整性；但企业并不需要全部采纳这 34 个流程，更多情况下应按照企业的需要进行裁剪组合。

每一个流程均指明了业务目标与其所支持的 IT 目标之间的联系，同时也提供了如何衡量目标、关键活动和主要交付物以及由谁负责等相关信息。

2.2.3. 以控制为基础

COBIT 定义了 34 个流程的控制目标，在流程与应用控制之间建立了联系。

流程需要控制

控制是指为合理保证业务目标的实现，预防、检查和纠正非预期事件的发生所制定的一系列政策、规程、实务和组织架构。

IT 控制目标提供了一系列完整的高层需求，用于管理层对每个 IT 流程进行有效控制时予以考虑，包括：

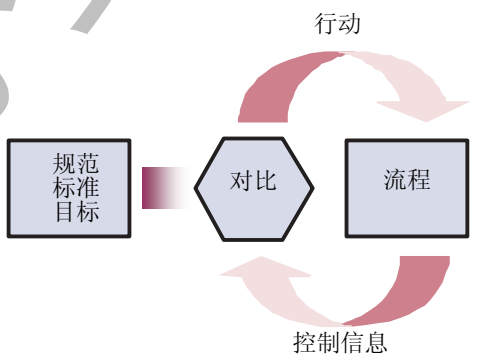
- 管理宗旨是增加价值还是降低风险；
- 政策、程序、实务和组织架构；
- 能否预防、检查和纠正非预期事件的发生以便为业务目标的实现提供合理保证。

针对这些控制目标，企业管理层需要做出以下选择：

- 选择适当的目标
- 确定要实现的目标
- 选择如何实现目标（频率、范围、自动控制等）
- 接受未实现目标可能带来的风险

可以从**图 9** 所示的标准控制模型中得到指引，它遵循以下推理原则：当设定了供暖系统（处理流程）的室温（标准）时，系统会持续检查（比较）房间的环境温度（控制信息）并指示供暖系统提供更多或更少的热量（纠正）。

图 9-控制模型



运营管理层使用流程来组织并管理日常的 IT 活动。COBIT 提供了一个能涵盖 IT 职能所有常见流程的通用流程模型，并为 IT 运营和业务管理层提供了一个易于理解的通用参考模型。为了实现有效治理，运营管理需要在既定的控制框架内对所有 IT 流程实施控制。因为 COBIT 通过 IT 流程来组织 IT 控制目标，它的框架提供了 IT 治理需求、IT 流程和 IT 控制之间清晰的关系。

COBIT 的每个 IT 流程都有一个流程描述和多个控制目标，作为一个整体，是最佳管理流程的基本特征。

控制目标使用两个字母的域缩写（PO、AI、DS 和 ME）加流程号和控制目标号进行标注，除此之外，每一个 COBIT 流程还有用 PCn(流程控制号)标注的一般控制要求，应将他们与流程控制目标共同考虑以形成一个完整的控制要求。

PC1 流程目标

为每个 IT 流程的有效运行制定并传达具体的、可衡量的、可操作的、可实现的、面向

结果的和及时的（SMARRT）流程目标，确保这些目标与业务目标相关联并采用恰当的衡量指标。

PC2 流程所有关系

为每个 IT 流程指定所有者并明确其角色和职责。例如可包括：流程设计职责、与其它流程的交互、对最终结果负责、流程绩效测评和识别改进机遇等。

PC3 流程复用性

设计并建立每一个关键 IT 流程使之能复用并始终产生一致的预期结果，制定一个合乎逻辑但灵活、可伸缩的流程步骤以达到期望结果，并能快速处理例外情况和紧急事件。尽量使用一致的流程，仅在必要时对流程进行裁剪。

PC4 角色和职责

确定关键活动和流程所产生的最终结果，分配并传达明确的角色与职责，以有效果、高效率地执行关键活动并进行记录，同时对流程结果负责。

PC5 政策、计划和程序

制定并贯彻运行 IT 流程相关的所有政策、计划、程序是如何记录、检查、维护、审批、保存、传达和用于培训的。为每一项活动分配职责并在适当的时间检查其执行是否正确。确保政策、计划和程序是可获取的、正确的、可理解的和最新的。

PC6 流程绩效改进

制定一系列衡量指标来监控流程结果和绩效，设立能反映流程目标和绩效的目标值以实现流程目标。确定如何获取数据，比较实际结果与目标值并在必要时纠正偏差，使衡量指标、目标和方法与 IT 整体绩效监控方法保持一致。

有效的控制能导致较少的错误和建立更加一致的管理方式，从而降低风险，增加价值交付和效率提高的可能性。

此外，COBIT 为每个流程提供了一个范例(是说明性的而不是指令性或详尽的)：

- 一般性的输入和输出；
- 使用 RACI 图（执行、负责、商议和通告）描述角色和职责的相关活动和指导
- 关键的活动目标（要做的最重要的事）；
- 衡量指标

除了应知道需要什么控制之外，流程所有者应该理解本流程需要的来自其他流程的输入以及其他流程所需要的本流程的输出。COBIT 为每一个流程提供了关键输入和输出的示例，其中包括外部的 IT 需求。其中一部分输出是其他所有流程的输入，在输出表中标记为“全部”，但是这些输出在所有流程均未包括在输入中，通常包括质量标准和指标要求、IT 流程框架、文档记录角色和职责、企业 IT 控制架构、IT 政策、人员角色和职责。

理解每个流程的角色和职责是有效治理的关键。COBIT 为每个流程提供了一个 RACI 图（执行、负责、商议和告知）。负责代表‘责任止于此’，是为活动提供授权和指导的人；执行是任务的具体执行人；另外两个角色（商议和告知）是提供支持和流程所涉及的每一

个人。

业务控制和 IT 控制

企业的内部控制系统在以下三个层次上影响 IT：

- 在执行管理层：设定企业目标、制定政策、作出关于如何部署和管理企业资源以执行企业战略的决策。董事会确定治理和控制的整体方式并在企业范围内贯彻。IT 控制环境亦受到这些高层目标和政策的控制。
- 在业务流程层：控制具体的业务活动。许多业务流程是自动化的并与 IT 应用系统进行了整合，导致这个层面的许多控制也是自动化的，这些控制被称为应用控制。然而，业务流程中的部分控制仍保留了手工操作，如：交易授权、职责分离和手工核对，因此，业务流程层面的控制是业务人员手工控制与自动化应用控制相结合，虽然应用控制需要 IT 职能予以支持进行设计和开发，但两种控制的建立和管理都是业务部门的职责。
- 为支持业务流程，IT 通常采用共享服务的方式为许多业务流程提供 IT 服务，因为许多的 IT 开发和操作流程需提供给整个企业，并且大多数的 IT 基础设施是公用的(如，网络、数据库、操作系统和存储)。这些应用于所有 IT 服务的控制措施被称为 IT 一般控制。一般控制的可靠运行是保障应用控制可靠性的必备条件，例如：缺乏变更管理将危及（意外或蓄意的）自动化系统完整性检查的可靠性。

IT 一般控制和应用控制

一般控制是指那些嵌入到 IT 流程和服务中的控制，例如：

- 系统开发；
- 变更管理；
- 安全；
- 系统日常运营。

嵌入到业务流程应用系统的控制通常称为应用控制。例如：

- 完整性；
- 准确性；
- 有效性；
- 授权；
- 职责分离。

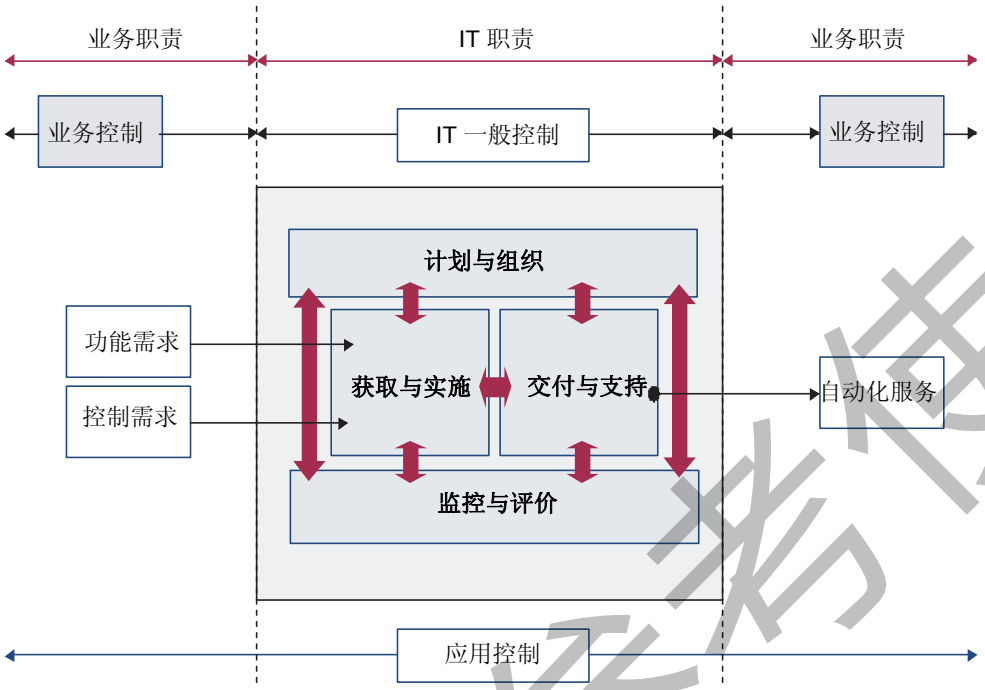
在获取与实施领域中，COBIT 把自动化应用控制的设计和实施定为 IT 的职责，并根据 COBIT 信息标准制定业务需求为基础（**图 10**），但应用控制的运营管理和控制职责不在 IT，应属于业务流程所有人。

因此，应用控制的责任是一个业务与 IT 之间端到端的共同责任，但责任的本质可转变为：

- 业务的责任：定义功能和控制需求，使用自动化服务。
- IT 的责任：实现功能和控制需求的自动化，建立控制以维护应用控制的完整性。

因此，COBIT 的 IT 流程中涵盖了一般 IT 控制，但是只包括应用控制的开发方面；而业务部门则负责制定职责和操作用途。

图 10-业务控制、一般控制和应用控制的边界



下述列表是一系列应用控制目标的建议，用 ACn（应用控制号）进行标注。

AC1 源数据准备和授权

确保由经过授权的和合格的人员遵照既定流程准备源文件，并充分考虑文件创建与审批的职责分离；良好设计的输入格式可减少错误和疏忽；检查输入错误和例外，报告并加以纠正。

AC2 源数据收集和录入

确保经过由授权的合格人员及时录入数据；输入错误数据后的纠正和再次提交应不违背原始交易的授权等级；为能够重建把原始文件保留一段恰当的时间。

AC3 准确性、完全性和真实性检查

确保交易是准确、完全和有效的，尽可能在靠近数据源的位置验证所输入、编辑或返回纠正的数据的有效性。

AC4 处理的完整性和有效性

在整个处理周期保持数据的完整性和有效性，在不中断合法交易的处理过程中检查错误交易。

AC5 输出的检查、核对和错误处理

建立控制程序和制定相应的职责来确保输出的处理是经过授权的，传送给适当的接收人，在传输时提供保护；验证、检查和纠正输出的准确性；并运用所输出的信息。

AC6 交易真实性和完整性

在内部应用系统和业务/运行功能（企业内部或外部）之间传递交易数据之前，检查并适当落实数据源的真实性和内容的完整性，在传输或迁移过程中保持真实性和完整性。

2.2.4. 以测评为驱动

企业的一个基本需求就是了解其自身的 IT 系统状况，决定企业应采取的管理和控制水平。为了确定正确的水平，管理层应该问自己：我们还应该走多远，成本与收益是否匹配？

对于企业自身业绩的客观测评是比较困难的。应该测评什么，如何测评?企业需要衡量他们处于什么位置，哪里需要改进，用什么管理工具来监督改进等。

COBIT 通过以下方式来解决这些问题：

- 采用成熟度模型实施基准管理以识别所需的能力改进；
- IT 流程的绩效目标和指标指明了 IT 流程如何满足业务目标和 IT 目标，并基于平衡记分卡的原理用于测量内部流程的绩效；
- 采用流程活动的目标去促进有效的流程绩效。

成熟度模型

越来越多的公司和公共企业高层管理人员被问到 IT 管理有多好/IT 的管理水平。针对这种情况，需要建立一种业务模式以改进管理使之达到适当的水平，并控制信息基础设施。当前已很少有人质疑这是不是个好议题，但需要考虑好平衡成本收益及下列相关问题：

- 我们的同行在做什么，与他们相比我们处于什么位置?
- 行业公认的最佳实践是什么，与这些最佳实践相比我们处于什么水平?
- 基于这些比较，我们所做的是否充分?
- 为达到适当的管理水平和控制 IT 流程，我们如何确定所需完成的事项？

很难给这些问题提供满意的答案。为了找到高效的管理方式，IT 管理层需不断寻找基准程序和自评估工具。从 COBIT 流程入手，流程所有者可以为控制目标设立逐步改进的基准，来满足以下三方面的需求：

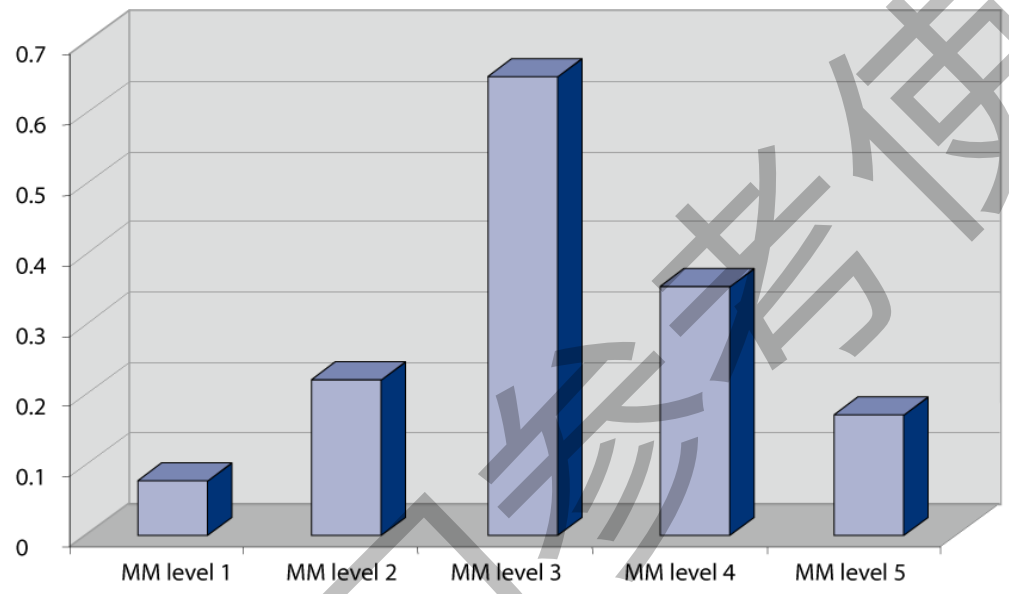
1. 一种衡量方法，以确定企业所处的位置；
2. 一套工作方式，以有效决定将要达到的水平；
3. 一组测量工具，以针对目标评估流程结果。

管理和控制 IT 流程的成熟度模型采用基于组织评价的方法，将成熟度水平划分为从无级别(0)到优化级(5)六个等级，这种方法借鉴了软件工程协会（SEI）对软件开发能力成熟度的定义方式。虽然采纳了 SEI 方法的基本概念，但 COBIT 在实施中与原来的 SEI 有相当的差别。SEI 是面向软件产品工程原理的，组织在这些领域中追求卓越，并通过对成熟度水平的正式评估使软件开发商得到‘认证’；然而，COBIT 给出了成熟度范围的一般性定义（类似于 CMM），但解释了 COBIT IT 管理流程的实质，并从一般定义出发为 34 个 COBIT 流程分别制定了具体模型。无论哪一种模型，范围都不应过细，否则将导致难以实施，而且过于精确的建议也不合情理，因为 COBIT 目标总的来说是识别问题所在和设定改进的优先级，

并非评估与控制目标的符合性水平。

成熟度等级是 IT 流程的概括图，可用于企业识别并记录当前及未来的可能状态，这些等级并非阀值模型（在未充分满足低等级条件时企业不能转向下一个较高等级）。与 SEI CMM 方法不同，使用 COBIT 成熟度模型，无意于准确测量等级或保证完全符合等级要求，其成熟度评估结果以概括图表示可能同时满足几个等级的相关条件（**图 11**）。

图 11-IT 流程的成熟度等级



一个IT流程可能的成熟度等级：此例说明一个总体上处于 3 级的IT流程，虽然已经在绩效管理（4 级）和改进（5 级）开始投资，但是仍有一些低层次的遵循性问题存在

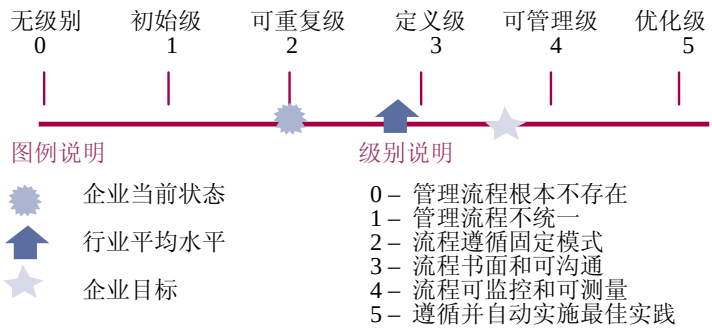
这是因为，当使用 COBIT 模型评估成熟度时，经常会出现这种情况：企业在不同的等级均实施了一部分措施，即使还不完整或不充分，但能促进未来的成熟度改进。例如：虽然不完整，也可以先建立好一部分流程，这也有可能会被误解为流程根本未建立。

使用为每一个 IT 流程设计的成熟度模型，管理层可以找出：

- 企业的实际绩效—当前所处的位置
- 行业的当前状况—比较
- 企业的改进目标—期望达到的位置
- 在‘当前’和‘获取’之间所需的成长路径

为了在管理报告中易于使用，需要采用图形表示方法以支持业务模式的未来规划（**图 12**）。

图 12-图解成熟度模型



制作图表应基于**图 13** 所表述的一般成熟度模型说明。

COBIT 是为 IT 流程管理开发的框架，重点关注控制，其衡量尺度应该实用并易于理解。IT 流程管理的首要问题是其固有的复杂性和主观性，因此，最佳的 IT 流程管理方式是通过推进评估以提高意识，争取董事会的同意并促进改善。可以把成熟度等级作为一个整体，也可以严格针对每一个条款来实施评估，无论哪种方式，都需要被评估流程方面的专家意见。

成熟度模型方法的优点是方便管理层对照等级以察觉提高绩效所需涉及的内容。等级中包括 0，是因为完全有可能不存在任何流程，0-5 的等级基于单一的成熟度水平描述了从无级别到优化级能力的演变过程。

然而，流程管理所需能力并不等同流程绩效。所需能力（取决于业务和 IT 目标）并不需要在整个 IT 环境中处于同样的水平，也就是说，不需要保持一致或只应用于一部分系统；绩效衡量（详见下一段落）对确定企业 IT 流程的真实绩效非常重要。

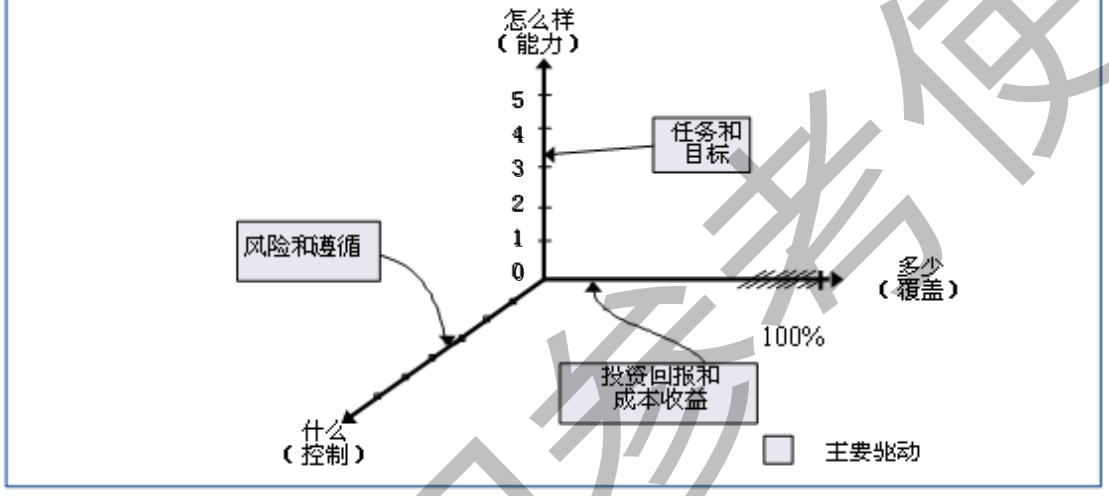
图 13-通用的成熟度模型

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。
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。
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，但未对这些流程组织正式的培训和贯彻，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。
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，但偏离流程的现象仍有发生；程序本身还不尽完善，只是现有工作惯例的正式化。
4–可管理级	管理层监督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。
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。

虽然建立的流程已减少风险，企业仍需分析控制的必要性，以确保降低风险并获得与风险偏好和业务目标相匹配的价值，COBIT 控制目标指出了这些控制。附录 3 提供了内部控制的成熟度模型，并阐明了与内部控制的建立和绩效有关的企业成熟度模型。通常这种分析的目的是为了响应外部要求，理想情况下，应根据 PO6“贯彻管理目标与方针”和 ME2“内部控制的监督与评价”的要求形成制度化的文件。

能力、覆盖面和控制是流程成熟度的所有维度，如**图 14** 所示。

图 14-成熟度的三个维度



成熟度模型是一种衡量管理流程设计效果（即实际应达到能力）的方法，设计效果或应达到能力主要依赖于 IT 目标及其支持的基础业务。能力的实施程度主要取决于企业所期望的投资回报（例如：关键流程和系统相比于其它而言，需要更多、更强的安全管理），另一方面，对流程控制的程度和复杂度则更多取决于企业的风险承受能力和适用的合规要求。

成熟度模型等级将有助于专业人士向管理人员解释 IT 流程管理所存在的缺陷并确定改进的目标。正确的成熟度水平将受企业业务目标、运营环境和行业惯例的影响，特别是管理成熟度水平取决于企业对 IT 的依赖程度、技术的复杂性，及最重要的是企业信息的价值。

企业改进 IT 流程的管理和控制的战略参考模型可以参阅最新的国际标准及最佳惯例。今天的惯例可能变成明天的绩效期望水平，因此对于企业的未来规划也是有帮助的。

成熟度模型是由通用的定性模型（**图 13**）组成并遵循一定的准则，该准则包含下列属性，这些属性随着等级的递增而不断提高：

- 意识和沟通；
- 政策、计划和实施程序；
- 工具和自动化方案；
- 技能和专业经验；
- 职责和责任；
- 目标和度量方法。

图 15 成熟度属性表列出了 IT 流程的管理特征以及从无等级到优化级所涉及的内容。这些属性可用于更全面的评估、差距分析和改进计划中。

总起来说，成熟度模型为企业 IT 流程管理和控制所涉及的各阶段提供了一个概略图，内容包括：

- 一系列针对不同成熟度等级的需求和实现方式
- 一组易于衡量偏差的指标
- 一组衡量实际贡献的指标
- ‘当前是’和‘未来预期’水平的设定基础
- 为达到既定水平而分析差距，以确定所需采取的行动
- 一个如何管理企业 IT 的总体概略图

COBIT 成熟度模型关注的是成熟度，而不是强调控制的覆盖面和深度，成熟度不是为之奋斗的一组数字，也不是用于正式认证的基础，那种分立的认证等级很难交叉使用。COBIT 成熟度模型是可以普遍使用的通用模型，在每个等级中均有被企业认为是最适当流程的情况，正确的等级取决于企业的类型、环境和战略。

确定控制的覆盖面和深度，功能如何使用及实施都应考虑成本效益。例如仅对企业最关键的系统应用高水平的安全管理，另一个例子是在每周进行手工检查和自动化连续控制之间做出抉择。

最后，在较高等级成熟度增加流程控制的同时，企业仍需基于风险和价值驱动进行分析以决定采用哪一种控制机制，框架中定义的一般业务和 IT 目标有助于这种分析。控制机制可参照 COBIT 控制目标重点关注流程中应采取的行动；成熟度模型则主要关注流程管理的程度。附录三提供了一个一般成熟度模型，描述了内部控制环境的状况和企业内部控制的建立。

在落实了成熟度的这三个方面（能力、覆盖面和控制）的问题后，企业将建立一个适当的控制环境。增加成熟度能降低风险和提高效率，从而导致更少的错误、更可预见的流程以及更加符合成本效益的资源利用。

图 15-成熟度属性表

意识和沟通	政策、计划和程序	工具和自动化方案	技能和经验	职责和责任	目标和度量方法
1 已意识到流程的必要性； 很少对问题进行沟通	存在一些非计划的流程和实践对流程和政策没有明确定义	存在一些基于桌面应用的工具；对工具使用没有统筹规划	未识别流程所需的技能；缺乏培训计划和正式的培训	未明确职责和责任，基于依靠个人主动反应去承担问题。	目标不明确，缺乏衡量指标
2 意识到行动的必要性； 管理层沟通整个问题	出现一些相似及通用的流程，但仅倚靠个人经验用直觉进行倚靠个人经验，一些流程已能重复使用，对一些书面要求和政策及流程有非正规了解	通常能使用工具，但只限于关键人员所开发的工具； 已购置了一些工具，但未正确使用甚至闲置未用	已识别少量关键流程所需的技能； 仅在需要时进行培训，而不是根据既定的计划；仅在作业出现时进行非正规培训	个人设定其职责，通常也包括问责，虽然未得到正式批准；问题发生时会出现职责冲突，存在互相指责的倾向。	已设定一些目标，制定了一些财务指标但仅用于高级管理层；在单独的领域内采用不相容的监控方式。
3 理解行动的必要性； 管理层采用更加正式和结构化方式进行沟通	良好实践已能使用已制定及记录所有关键活动的流程，政策及程序	已为自动化流程工具的使用和标准化制定计划； 工具基本得到采用，但未遵循既定计划，也未对工具进行整合	在所有领域制定了书面的技能要求； 已制定正规培训计划，但正规培训仍基于个别人的主观努力	已明确流程职责和责任并指定流程所有者；流程所有者可能还缺乏履行职责所需的完全授权。	已设定一些有效的并与业务目标明确相关的目标和衡量指标，但尚未沟通；已制定考评流程但未得到一致贯彻；开始采用 IT 平衡记分卡概念，偶尔用直觉分析问题的原因。
4 理解所有需求； 采用成熟的沟通技巧和标准化的沟通工具	已有健全及完整的流程，并采用内部最佳实践所有流程已能重复使用及记录，政策經由管理层批准及簽署，已采納标准用以开发和维护流程及程序	能按照标准计划使用工具，部分相关工具已进行整合； 能在自动化流程管理和监控关键活动与控制的主要领域使用工具	能按常规更新所有领域的技能要求，确保所有关键领域的熟练程度并鼓励认证； 按照培训计划应用成熟的培训技巧，鼓励知识共享；所有内部专家均参与其中并对培训效果进行评估	所制定的流程职责和责任能促使流程所有者完全、有效地行使其职责；存在奖励文件，并能促进正面效应。	结合业务目标与 IT 战略规划，来衡量和沟通效率与效果；IT 平衡记分卡已应用于部分领域，管理层记录例外并采用标准化方式分析根本原因；已开始持续改进。
5 能超前、前瞻性地理解需求； 基于当前趋势事先交流问题，采用成熟的沟通技巧和集成沟通工具	已使用外部最佳实践及标准流程的文书處理已建立自动程序，采用标准化和已整合的流程，政策及程序，以求达到端到端管理和改进	在企业范围内使用标准化的系列工具； 完全整相关工具以加强流程的端到端支持； 工具能用于支持流程改进和自动检查控制的例外情况	基于清晰的个人和组织目标提倡技能的持续改进； 使用外部最佳实践、前沿概念和技能组织培训；知识共享是企业文化，并实施以知识为基础的系统； 采用外部专家和行业领先者作指导	授权流程所有者制定决策并采取措施； 职责在全企业范围内按照一致的方式进行层级分解。	已建立全面应用 IT 平衡记分卡的绩效测评系统，把 IT 绩效与业务目标相结合；管理层全面、一致地记录例外情况，并分析根本原因；持续改进是企业的存在方式。

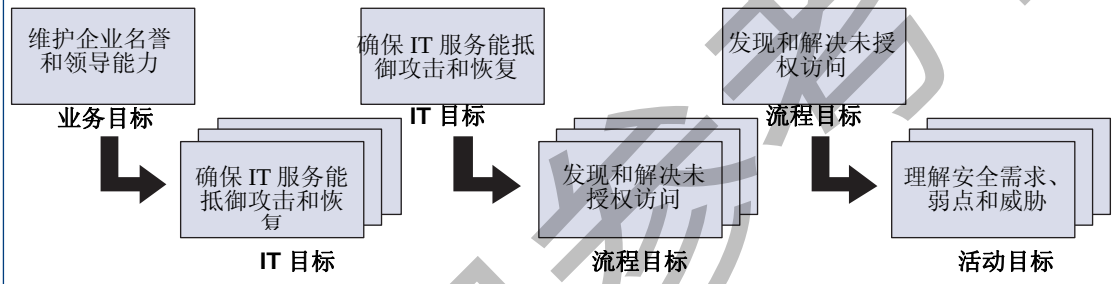
绩效测评

COBIT 在三个层次上制定了目标和衡量指标：

- IT 目标和指标，定义了业务对 IT 的期望和如何测评；
- 流程目标和指标，定义了 IT 流程为了满足 IT 目标必须交付的服务和如何进行评估；
- 活动目标和指标，确定为达到所需性能而采取的流程内活动以及如何测评。

目标自上而下地设立，业务目标确立并支持它的若干个 IT 目标；一个 IT 目标由一个或若干个相互作用的流程来实现，这样，IT 目标帮助确立不同的流程目标；每一个流程目标都需要一系列的活动支持，因此反过来也确立了活动目标。**图 16** 指出了业务、IT、流程和活动目标间的关系。

图 16-目标关系示例

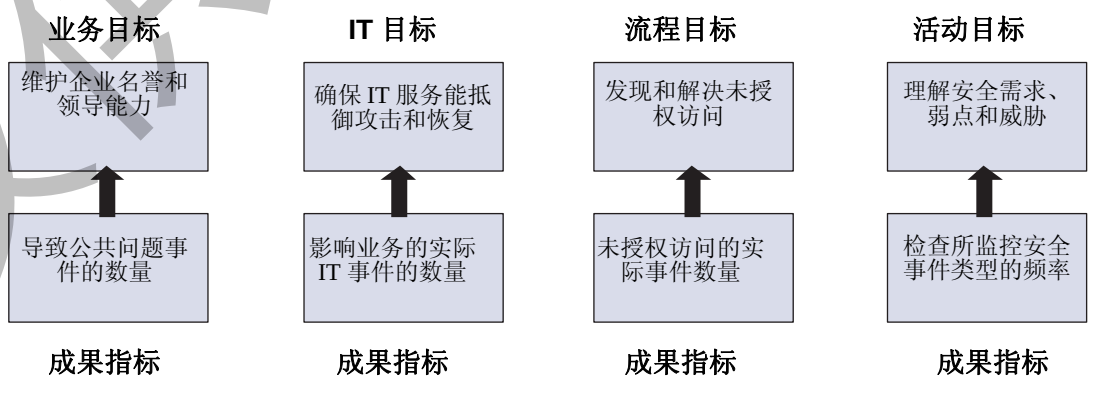


在 COBIT 以前版本中使用的术语 KGI 和 KPI，现已经由两类衡量指标代替。

- 效果指标：即关键目标指标 KGI，指明目标是否已达成，仅在活动结束后测评，因此也称为‘事后指标’。
- 绩效指标：即关键绩效指标 KPI，指明目标的预期实现程度，可以在活动结束之前进行测评，因此也称为‘前导指标’。

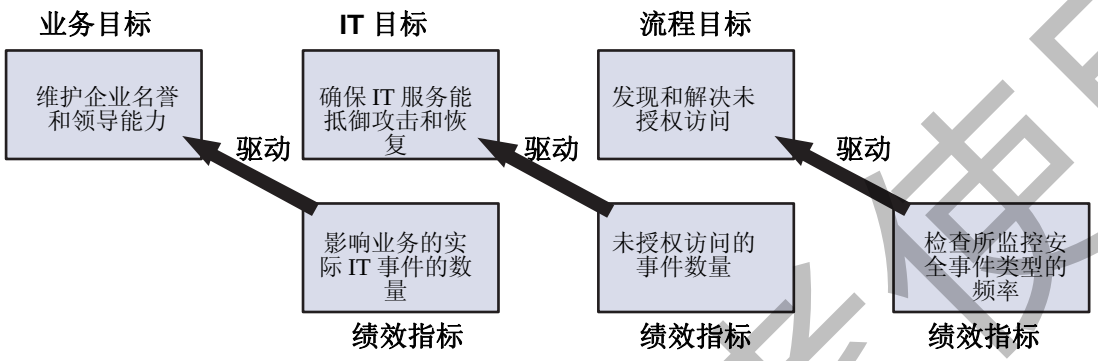
图 17 提供了一些目标或效果指标的示例。

图 17-图 16 示例中可能的成果指标



由低层的效果指标转化出高层的绩效指标，如**图 17** 中的一个例子，“检查并解决非授权访问”这个流程目标的效果指标也支持目标“增强 IT 服务对攻击的抵御和恢复能力”，即：效果指标已转化为高层绩效指标。**图 18** 举例说明了效果指标如何转化为绩效指标。

图 18-图 16 示例中可能的绩效驱动



效果指标定义了信息管理的事后指标，衡量 IT 功能、流程或活动的目标是否已达成，IT 功能的效果指标通常采用下列信息标准术语表示：

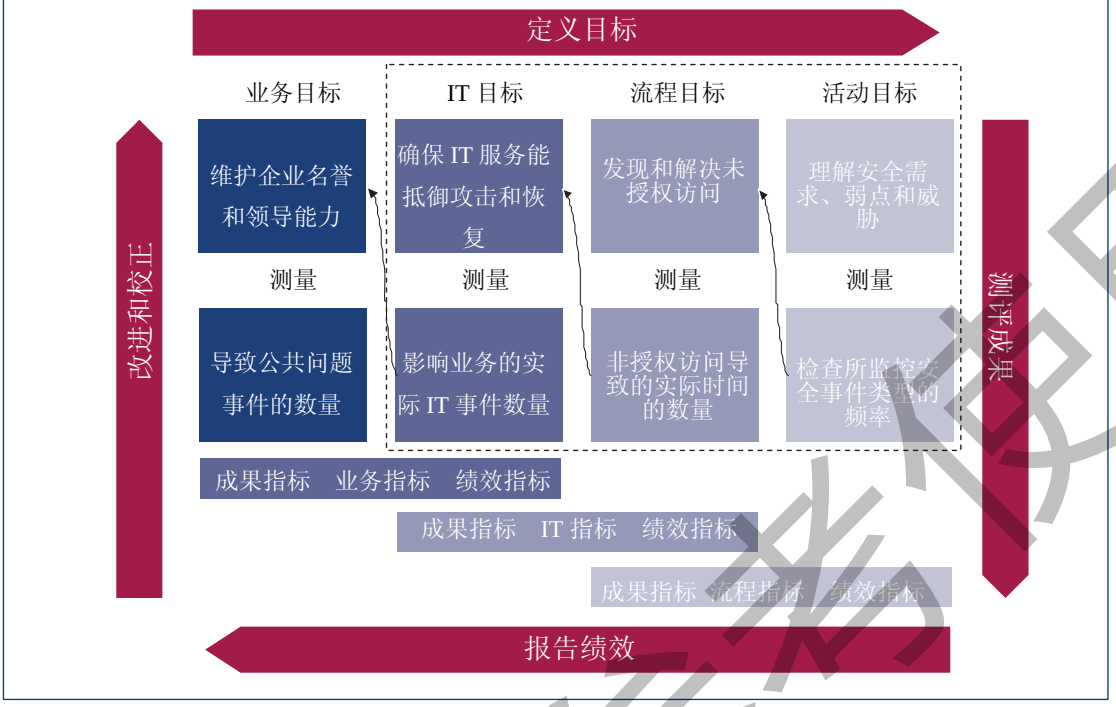
- 支持业务需求的信息可用性；
- 完整性和保密性丧失的风险；
- 流程和运行的成本效率；
- 可靠性、效果和符合性确认。

绩效指标定义了业务、IT 功能或流程促进目标实现的程度，是衡量目标达成可能性的前导指标，以此来推动更高层目标，常用于衡量适用的能力、实务和技能的可用性以及底层支持活动的效果。例如：IT 交付服务是 IT 目标，也是业务的绩效指标及能力。这正是绩效指标时常被引用为绩效推动力的原因，尤其是在平衡记分卡中。

因此，同样的衡量指标既是 IT 功能、流程或活动本身的效果指标，也是推动更高层业务、IT 功能或流程目标的绩效指标。

图 19 描述了业务、IT、流程及活动目标间的关系和各自的衡量指标。从左上到右上，目标逐层分解，目标之下是该目标本身的效果指标，小箭头指出的同一指标同样指标是更高层目标的绩效指标。

图 19-流程、目标和度量之间的关系（DS5）



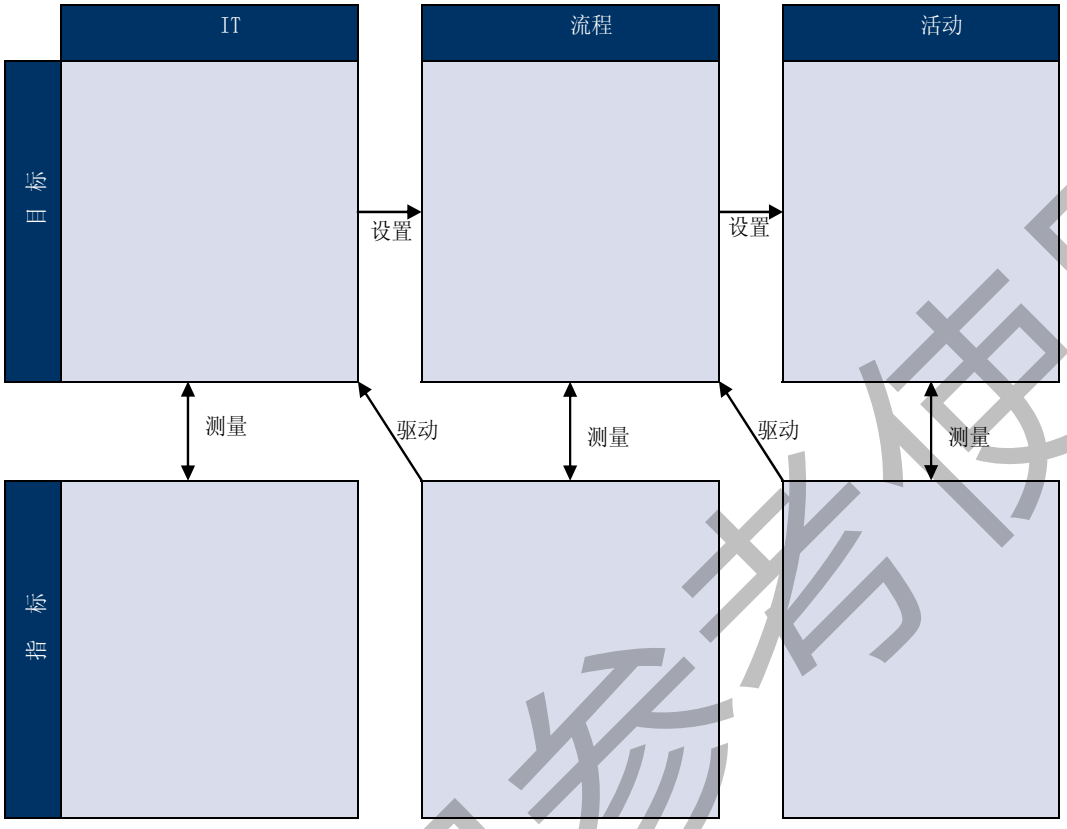
所举示例来自 DS5（确保系统安全），COBIT 只对虚线框内的 IT 目标结果提供效果指标，它们同时也是 IT 业务目标的绩效指标，COBIT 未提供业务目标的效果指标。

在附录 1 中提供了应用于 COBIT 的“目标和测评”章节的业务和 IT 目标，包括他们的关系。**图 20** 为 COBIT 每一个 IT 流程提供了目标和衡量指标。

所制定衡量指标已考虑了以下特点：

- 较高的认知付出比（对绩效和目标达成的认知程度比所需付出的努力）
- 内部可比性（一定时间内相对于某一基准和数量的百分比）
- 不考虑企业规模或行业的外部可比性
- 少而精的指标（甚至是一个可反应不同方面影响的指标），而不是一长串低质量指标
- 易于测评，且不与目标冲突

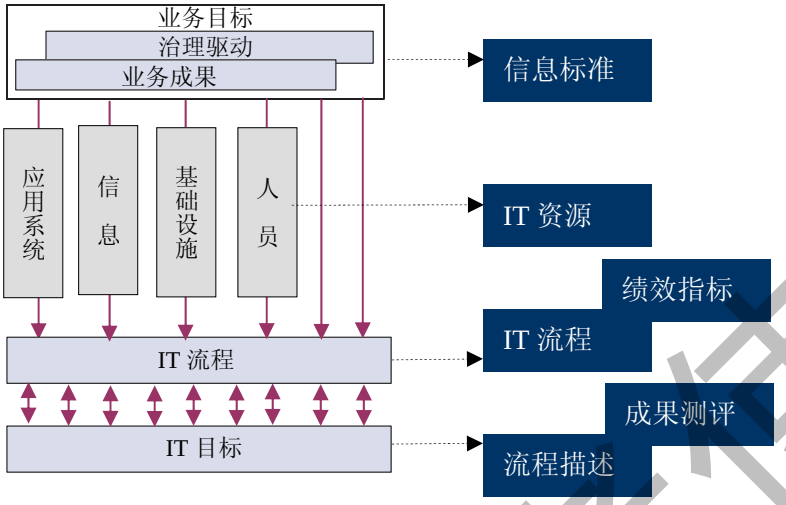
图 20-目标和指标的描述



2.2.5. COBIT 框架模型

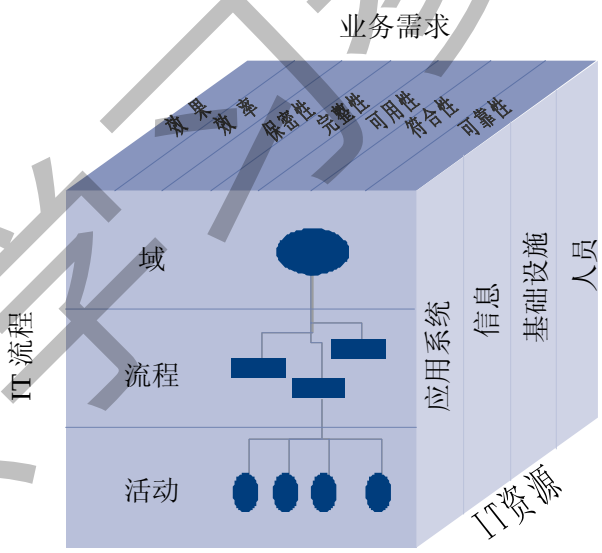
因此，COBIT 框架将信息的业务要求与 IT 服务职能的治理目标紧密结合起来。基于控制目标，COBIT 流程模型可以促进 IT 活动及其资源的适当管理和控制，并协调、监控 COBIT 目标和衡量指标的使用，如**图 21** 所示：

图 21-COBIT 管理、控制、校正和监控

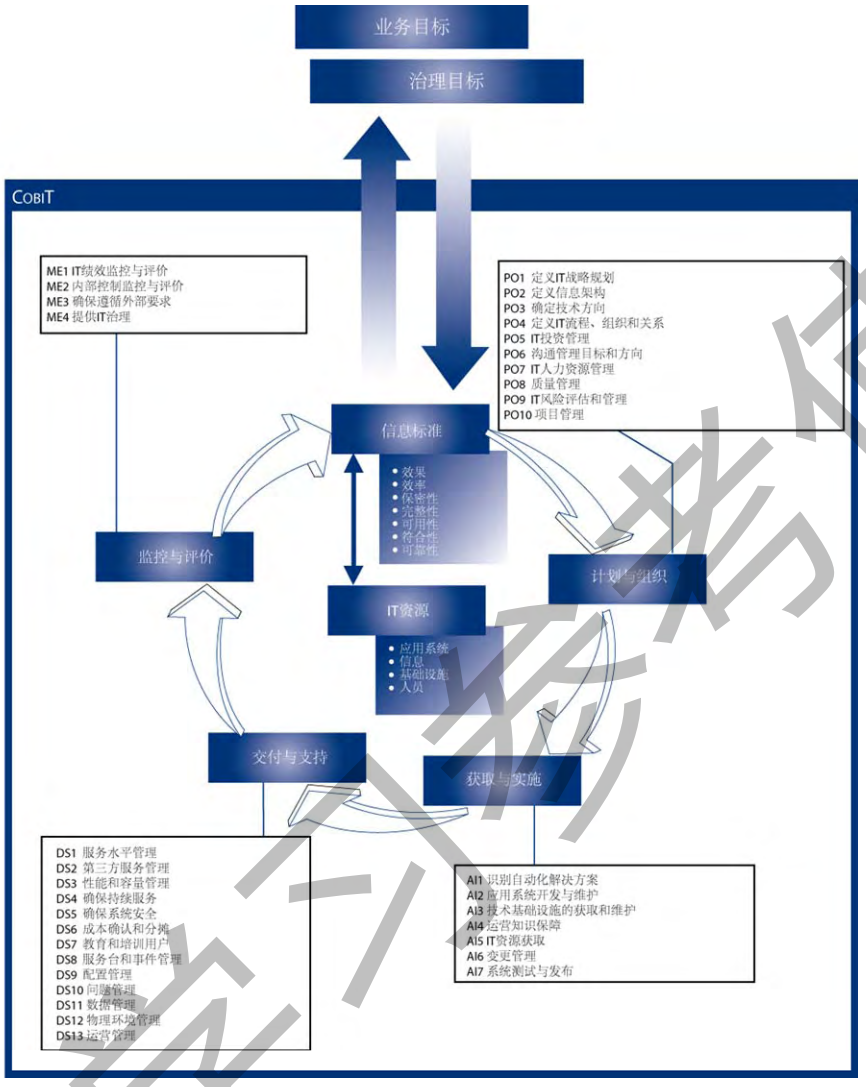


总之，通过 IT 流程管理 IT 资源，来实现 IT 目标以满足业务需求是 COBIT 框架的基本原理。如**图 22** 所示：

图 22-COBIT 立方体



更详细的 COBIT 框架如**图 23** 所示。COBIT 的流程模型包括四个域，34 个通用流程，管理 IT 资源以交付满足业务和治理要求的信息。



2.2.6. COBIT 的公认性

COBIT 建立在对现有 IT 标准和最佳实践的分析和融合基础上，并遵循公认的治理原则。COBIT 定位于高层，由业务需求驱动，覆盖了所有的 IT 活动，关注于应该实现什么而不是如何实现有效的治理、管理和控制。因此，COBIT 是 IT 治理惯例的集大成者，可以为执行管理层，业务和 IT 管理层，治理、保证和安全专业人员及 IT 审计和控制人员所用。COBIT 可以用其他的标准和最佳实践来补充。

实施最佳实践应与企业的治理和控制框架相一致，并适合于组织，也应与其它现有的方法和惯例相结合。标准和最佳实践并不是万能药，其有效性依赖于它们如何被实施并保持最新。当它们作为根据具体情况定制的特定程序的系列准则及起始点时最为有用。为了

避免被束之高阁，管理层及相关人员应理解最佳实践的实施内容、如何实施及它们的重要性。

为了实现最佳实践与业务需求的协调一致，建议将 COBIT 设定为最高层次的整体控制框架，而这框架是基于一个适用于每个企业的 IT 流程模型。个别范围的具体实践和标准可以映射到 COBIT 框架，因此，提供了一个多层次的指导材料的分级。

COBIT 适用于不同的用户：

- 执行管理层--在通常不可预知的 IT 环境中平衡风险和控制投资来获取 IT 投资的回报；
- 业务管理层--获得内部或第三方所提供的 IT 服务的管理和控制的保障；
- IT 管理层--以控制和管理 IT 来提供满足业务需求的 IT 服务；
- 审计人员--支持他们的观点，并为管理人员提供关于内部控制的建议。

COBIT 由一个独立的、非赢利性研究机构开发和维护，并吸取了其会员、行业专家、控制和安全专业人士的经验。其内容是基于对 IT 最佳实践的持续研究和改进，为不同类型的用户提供客观而实用的资源。

COBIT 定位于 IT 治理的目标和范围，确保其控制框架是广泛的，并与企业的治理准则相协调。因此，COBIT 可被董事会、执行管理层、审计人员和监管机构所认可。附录 II 描述了 COBIT 详细控制目标与 IT 治理的 5 个关注领域及 COSO 控制活动之间的对照关系。

图 24 概述了如何把 COBIT 架构图的各类要素映射到 IT 治理重点领域。

图 24-COBIT 框架和 IT 治理关注领域

	目标	指标	实务	成熟度模型
战略融合	**P**	**P**		
价值交付		**P**	**S**	**P**
风险管理		**S**	**P**	**S**
资源管理		**S**	**P**	**P**
绩效测评	**P**	**P**		**S**

P=主要动力　　**S**=次要动力

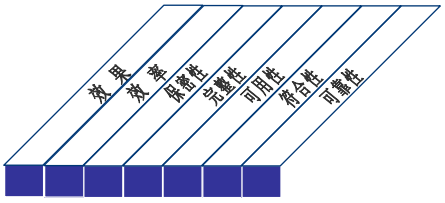
2.3. 如何使用本书

2.3.1. COBIT 框架导航

对于每一个 IT 流程，COBIT 都提供了一个说明和瀑布模式的关键目标和衡量指标，如**图 25** 所示。

图 25-COBIT 导航

在每一个 IT 流程中，控制目标作为管理最佳实践的最低行动说明，以确保流程可控。



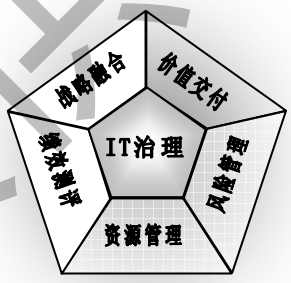
控制 IT 过程：
流程名称

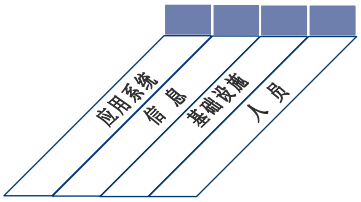
使 IT 满足业务需求：
最重要的 IT 目标概要

通过关注于：
最重要的流程目标的概要

通过下列实现：
活动目标

通过下列衡量
关键指标





主要　次要

2.3.2. COBIT 核心组件概述

COBIT 框架由下列核心组件组成，这些组件包括 34 个 IT 流程，在本书的其他章节完整描述了如何控制、管理和测评每个流程。每个流程都包括四个部分，每个部分通常为一页，内容如下：

- 第 1 部分：流程描述，总结了流程目标并采用瀑布形式描述该流程的主要内容和目标，也描述了流程与信息标准、IT 资源及 IT 治理重点关注领域的映射关系，而用 P 代表主要和 S 代表次要关系；
- 第 2 部分：本流程所包含的详细控制目标；
- 第 3 部分：包括流程输入和输出、RACI 图、目标和衡量指标；
- 第 4 部分：流程的成熟度模型。

审视流程绩效内容的另一种方法是：

- 来自于其他流程的输入符合流程所有者需要；
- 详细控制目标描述了流程所有者需要完成的工作；
- 流程输出符合流程所有者交付需要；
- 目标和衡量指标描述如何对流程测评；
- RACI 图明确了职责分配及分配给谁；
- 成熟度模型描述了改进所需的措施。

所有流程 RACI 图中的角色包括：

- 首席执行官(CEO)；
- 首席财务官(CFO)；
- 业务执行经理；
- 首席信息官(CIO)；
- 业务流程所有者；
- 运营总监；
- 首席架构师；
- 开发总监；
- IT 行政总监(对大型企业来说，人力资源、预算和内部控制等职能的负责人)；
- 项目管理官(PMO)；
- 合规、审计、风险和安全人员(承担控制职责而不是 IT 运营职责的团队)。

特定的流程可能还有其他一些特殊的角色，如 DS8 中的服务台/事件经理。

需要注意的是，尽管这些材料是从众多的专家那里收集而来，且对其进行了细致的研究和评审，但是这些输入、输出、职责、衡量指标和目标并不详尽。他们只是一个专家知识的基础，每个企业都应根据企业的战略、目标和策略自行选择所需的材料。

2.3.3. COBIT 组件的使用

管理层可以用 COBIT 附录 I 的业务目标和 IT 目标来评估 IT 流程，阐明 IT 流程目标和成熟度模型以评估绩效。

实施者和审计师可以从活动或相关 RACI 图中的控制目标和职责识别适当的控制需求。

使用 COBIT 内容作为全面管理和治理 IT 的方法，所有潜在的用户都可以从中受益，另外还可以参考其它更为详细的有关标准，如：

- ITIL 用于提供服务
- CMM 用于提供解决方案
- ISO17799 用于信息安全
- PMBOK 或 PRINCE2 用于项目管理

2.3.4. 附录

本书的结尾部分提供了下列参考资料：

I. 目标和流程关系表(三个表)
II. IT 流程与 IT 治理重点领域、COSO, COBIT IT 资源和信息标准之间的映射关系
III. 内部控制的成熟度模型
IV. COBIT4.1 主要参考资料
V. COBIT3.0 与 COBIT4.1 的交叉引用
VI. 研究和开发方法
VII. 术语表
VIII. COBIT 和相关产品

3. 计划与组织（PO）

PO1 定义 IT 战略规划

PO2 定义信息架构

PO3 确定技术方向

PO4 定义 IT 流程、组织和关系

PO5 IT 投资管理

PO6 沟通管理目标和方向

PO7 IT 人力资源管理

PO8 质量管理

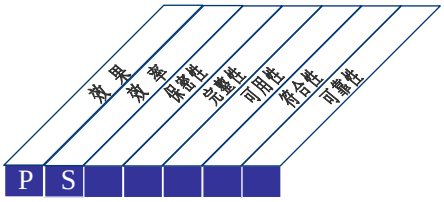
PO9 IT 风险评估及管理

PO10 项目管理

3.1. PO1 定义 IT 战略规划

3.1.1. 流程描述

必须编制符合业务战略及其优先级的 IT 战略规划以管理和指导 IT 资源。IT 部门和业务利益相关方有确保通过项目和服务组合实现最大价值的职责。IT 战略规划关键利益相关方更好理解 IT 机遇及其限制，该规划应评估当前绩效、识别 IT 能力和人力资源的需求，明确必需的投资规模。业务战略和优先级在项目组合中体现，并通过 IT 战术计划实施。IT 战术计划详细描述业务和 IT 都理解和接受的具体目标、行动计划和任务。



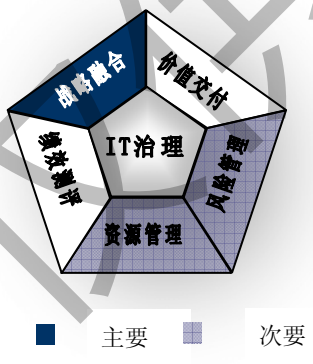
IT 流程中的控制：
定义 IT 战略规划

使 IT 满足业务需求：
在确保收益、成本和风险透明的同时，支持或扩大业务战略和治理要求

通过关注于：
IT 和业务管理层合作，将业务需求转化为服务提供和战略编制，以便透明、有效地交付这些服务

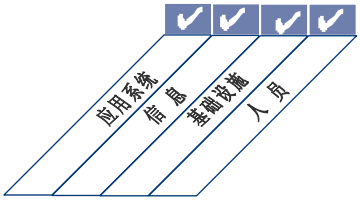
通过下列实现：

- 业务和高级管理层参加 IT 战略规划的编制，以确保该规划满足当前和未来的业务需求
- 了解当前的 IT 能力
- 提供业务目标的优先级划分计划，以量化业务需求



通过下列衡量：

- IT 战略规划中支持业务战略规划的 IT 目标的百分比
- IT 项目投资组合中可以追溯到 IT 战术计划的 IT 项目所占的百分比
- IT 战略规划更新和 IT 战术计划更新之间的延迟



3.1.2. 控制目标

PO1.1 IT 价值管理

与业务部门共同确保企业的 IT 总投资包括了具有确定业务模式的项目群。根据复杂性和自由度的不同来分配资金，以确认强制性、支持性和自主性的投资。IT 流程应确保交付项目 IT 组件的效率和效果，尽早预警可能影响项目组合预期计划成果的偏离，包括成本、进度或功能等。应根据公正、可实施的服务水平协议实施 IT 服务。应清晰分配和监控实现收益和控制成本的责任。应建立透明、公正、可重复和可比较的业务模式评价制度，包括财务价值、未交付所需能力的风险以及未实现预期收益的风险。

PO1.2 IT 与业务的一致性

建立 IT 战略规划和业务战略规划的双向教育和相互协调机制，以实现业务和 IT 的整合和一致。协调业务和 IT 各自单方面意见，以便双方共同确定优先级。

PO1.3 当前能力和绩效的评估

评估解决方案和服务交付的现有能力和绩效，以便建立一个与将来需求可比较的基线。绩效定义包括：IT 对业务目标的贡献、功能性、稳定性、复杂性、成本、优势、劣势。

PO1.4 IT 战略规划编制

与有关的利益相关方共同编制战略规划。该战略规划应指明 IT 目标如何协助达成企业的战略目标及其相应的成本降低和风险控制。战略计划应包括 IT 将如何支持 IT 保障投资项目、IT 服务和 IT 资产。IT 定义了如何满足目标、如何用来测量及如何经过相关方的正式审批。IT 战略计划应涵盖投资/运营预算、资金来源、资源（供应商）战略、采购策略和法律法规需求。战略计划应足够详细以利于 IT 战术计划的制定。

PO1.5 IT 战术计划

根据 IT 战略计划制定一整套组合的 IT 战术计划。这组战术计划包括保障 IT 项目的投资计划、IT 服务和 IT 资产。战术计划应该描述必需的 IT 计划、资源的需求以及资源使用和收益绩效如何被监控和管理。这些战术计划应该足够详细，以便制定项目计划。通过分析项目和服务的组合，主动管理 IT 战术计划和实施。

P01.6 IT 项目组合管理

为实现特定的业务战略目标，采取识别、定义、评价、确定优先级、选择、启动、管理和控制项目群的方式，与业务部门积极管理 IT 推动的投资项目组合。这包括：

阐明期望的业务成果；

确保项目群目标支持这些成果的实现；

理解实现这些成果所需的全部投入；

分配支持衡量指标的清晰的职责；

定义项目群内的项目；

分配资源和资金；

授权；

项目群正式启动时对必需的项目进行试点。

3.1.3. 管理指南

源自	输入
PO5	成本/收益报告
PO9	风险评估
PO10	更新了的 IT 项目投资组合
DS1	新建/更新了的服务需求、更新了的 IT 服务投资组合
*	业务战略和优先级
*	项目群投资组合
ME1	绩效输入到 IT 计划
ME4	IT 治理状况的报告；企业 IT 战略方向

* 输入源自 COBIT 外部

输出	到						
IT 战略计划	PO2…PO6		PO8	PO9	AI1	DS1	
IT 战术计划	PO2…PO6			PO9	AI1	DS1	
IT 项目投资组合	PO5	PO6	PO10	AI6			
IT 服务投资组合	PO5	PO6	PO9	DS1			
IT 资源战略	DS2						
IT 采购战略	AI5						

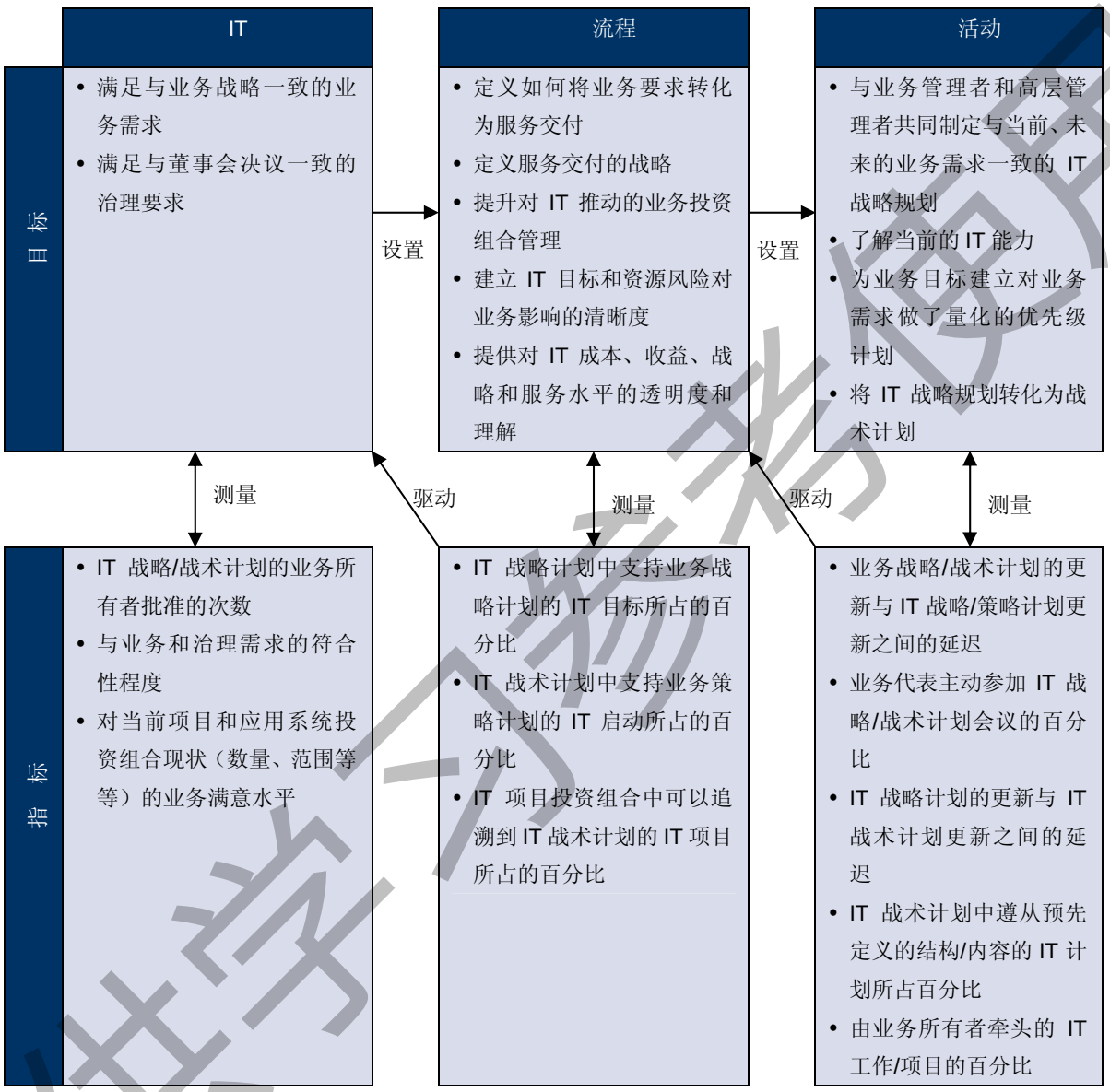
RACI 图

职能

活动	首席执行官	首席财务官	业务执行经理	首席信息官	业务流程所有者	运营总监	首席架构师	开发总监	IT行政总监	项目管理官	合规、审计、风险和安全
建立业务目标和 IT 目标间的关联	C	I	A/R	R	C						
识别关键依赖和当前绩效	C	C	R	A/R	C	C	C	C	C		C
建立 IT 战略规划	A	C	C	R	I	C	C	C	C	I	C
建立 IT 战术计划	C	I		A	C	C	C	C	C	R	I
分析项目群投资组合，并管理项目和服务的投资组合	C	I	I	A	R	R	C	R	C	C	I

RACI 图中，**R**esponsible 代表**执行**，**A**ccountable 代表**负责**，**C**onsulted 代表**商议**，**I**nformed 代表**告知**。

3.1.4. 目标和指标



3.1.5. 成熟度模型

管理“定义 IT 战略规划”流程，使 IT 满足业务需求：在确保收益、成本和风险透明的同时，支持或扩大业务战略和治理需求。

0 级 无级别

未实施 IT 战略规划。管理层未意识到 IT 战略规划需要支持业务目标。

1 级 初始级

IT 管理层认识到 IT 战略规划的需求。在响应特定的业务需求时才进行必要的 IT 规划。IT 战略规划偶尔在 IT 管理层的会议上讨论。业务需求、应用和技术的一致性只是偶尔被动发生而不是组织化的战略。仅仅依据特定项目来非正式地识别战略风险。

2 级 可重复级

业务管理层在必要时才与 IT 管理层共同制定 IT 战略规划。IT 规划在管理层的要求下才做更新。战略决策依据逐个项目来驱动，且与企业的整体战略不一致。靠直觉认定重点战略决策的风险和用户收益。

3 级 定义级

制定了何时及如何实施 IT 战略规划的政策。IT 战略规划遵循员工都知晓的书面的结构化方法。IT 战略规划的流程是合理的，也能够保证规划工作的实施，但在具体的实施过程中却要靠个别管理经理的判断力，且缺乏检查这些流程的方法。整个 IT 战略包括组织想作为创新者或追随者对风险的一致定义。IT 财务、技术及其人力资源策略对新产品和新技术获取的影响日益增加。在业务管理层的会议上讨论 IT 战略规划。

4 级 可管理级

IT 战略规划的制定已经成为标准化活动，管理层注意到 IT 战略规划的例外情况。IT 战略规划工作成为高级管理层的明确职责。管理层可以监控 IT 战略规划流程，依据战略规划做决策并测量其有效性。制定了长、短期 IT 计划并逐层向下分解，同时及时更新。通过强调业务流程、增值能力以及技术和应用系统促成业务流程重组，IT 战略和企业战略将日趋协同。有一个确定在系统开发和运行中使用内、外部资源的良好决策流程。

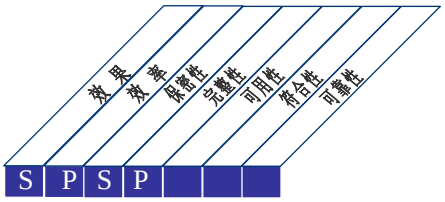
5 级 优化级

IT 战略规划已成为正式文件，而且是一个可以调整的过程。IT 战略规划在业务目标的实现中得到持续重视，并通过对 IT 的投资来实现业务价值。在 IT 战略规划过程中，不断更新对 IT 风险和增加价值的考虑。制定了可实施的长期 IT 计划并不断更新，以满足技术和业务相关的变化。制定了以众所周知、可靠的行业规范为参考的标准，并结合到战略规范化流程中。IT 战略规划包括如何开发新的技术来驱动业务创新，并提高组织的竞争优势。

3.2. PO2 定义信息架构

3.2.1. 流程描述

信息系统部门建立和定期更新业务信息模型并规划适当的系统来优化信息的使用。本流程包括制定与组织的数据语法规则一致的企业级数据字典、数据分类计划和数据安全等级。本流程通过利用可靠和安全的信息来改善管理层决策的质量，能够保障合理的信息系统资源与业务战略匹配。该 IT 流程在以下方面也是必需的：增加数据的安全性和完整性，强化应用系统和用户部门间共享信息的有效性和控制力。



IT 流程中的控制：

定义信息架构

使 IT 满足业务需求：

灵活响应需求，提供可靠和一致的信息，将应用系统与业务流程无缝集成

通过关注于：

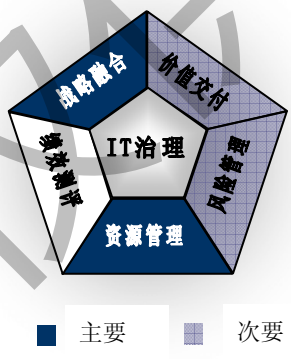
融合了数据分类策略的企业级数据模型的建立，确保所有数据的完整性和一致性

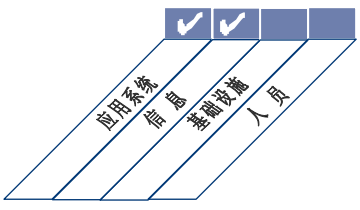
通过下列实现：

- 保证信息架构和数据模型的正确
- 分配数据所有权
- 使用经过审批的分类策略来分类信息

通过下列衡量：

- 数据元重复/冗余的百分比
- 不遵从企业使用的信息架构方法论的应用系统的百分比
- 数据校验活动的频率





3.2.2. 控制目标

PO2.1 企业信息架构模型

建立和维护企业信息模型，使其用于应用开发和决策支持活动，并与 PO1 中描述的 IT 规划保持一致。该模型应易于业务部门创建、使用和共享信息，同时在某种程度上维护其完整性且具有灵活性、功能强、成本效益高、及时、安全和易于故障恢复等特点。

PO2.2 企业数据字典和数据语法规则

维护具备数据语法规则的企业数据字典。该字典使各应用软件和系统间的数据元素共享，加深 IT 人员和业务用户对数据的共同理解，以及防止产生相互冲突的数据元素。

PO2.3 数据分类计划

根据企业数据的关键性和敏感性（如公用的、保密的、绝密的等），建立一个适用于整个企业的分类计划。该计划包括：

数据所有权的详细说明
定义适当的安全等级和保护控制
数据保持和销毁要求的说明
关键性和敏感性的要求

该计划应作为实施诸如访问控制、归档和加密等应用控制的基础。

PO2.4 完整性管理

制定和实施一系列程序，来确保所有存储在电子媒介（例如，数据库、数据仓库和数据档案库）中数据的完整性与一致性。

PO2 定义信息架构

3.2.3. 管理指南

源自	输入
PO1	IT 战略规划和 IT 战术计划
AI1	业务需求；可行性研究
AI7	实施后评审
DS3	性能和容量信息
ME1	绩效输入到 IT 计划

输出	到						
数据分类计划	AI2						
优化的业务系统计划	PO3	AI2					
数据字典	AI2	DS11					
信息架构	PO3	DS5					
分配的数据分类	DS1	DS4	DS5	DS11	DS12		
分类程序和工具	*						

* 输出源自 COBIT 外部

RACI 图

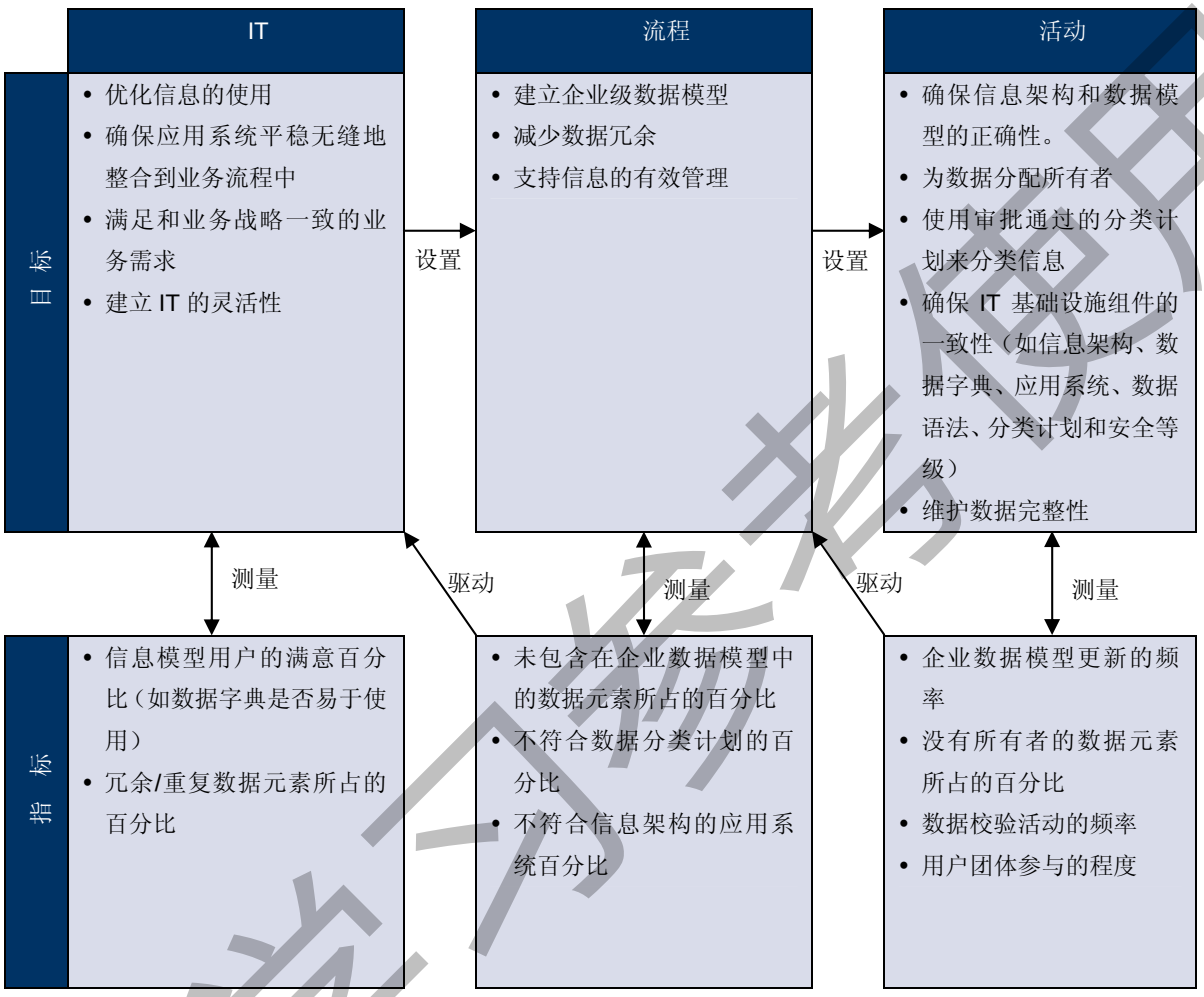
职能

活动

活动	首席执行官	首席财务官	业务执行经理	首席信息官	业务流程所有者	运营总监	首席架构师	开发总监	IT行政总监	项目管理官	合规、审计、风险和安全
创建并维护公司/企业级的信息模型		C	I	A	C		R	C	C		C
创建并维护公司数据字典				I	C		A/R	R			C
建立并维护数据分类计划	I	C	A	C	C	I	C	C			R
为数据所有者提供信息系统分类的程序和工具	I	C	A	C	C	I	C	C			R
利用信息模型、数据字典和数据分类计划来规划最优的业务系统	C	C	I	A	C		R	C			I

RACI 图中，**R**esponsible 代表**执行**，**A**ccountable 代表**负责**，**C**onsulted 代表**商议**，**I**nformed 代表**告知**。

3.2.4. 目标和指标



3.2.5. 成熟度模型

管理“定义信息架构”流程，使 IT 满足业务需求：灵活响应需求，提供可靠和一致的信息，并无缝地将应用系统整合到业务流程中。

0 级 无级别

未意识到信息架构对于组织的重要性。组织未规定开发信息架构所需的知识、经验和职责。

1 级 初始级

管理层认识到信息架构的需要。信息架构一些组件的开发在非计划的基础上实施。这些组件的定义描述的是数据而不是信息，且这些定义是由应用软件供应商所提出。信息架构的沟通是零星的和不一致的。

2 级 可重复级

非正式的、凭直觉的建立了一个信息架构流程，由企业不同的人员和部门遵循。在信息架构的开发中 IT 人员通过实践学习和技术的重复使用获得技能。信息架构组件由个别 IT 人员开发，且由各个项目的需求驱动。

3 级 定义级

管理层接受并理解信息架构的重要性，分派并沟通了信息架构的交付职责。相关的方法、工具和技术虽然不太完善，但已经标准化并成文，并成为非正式培训的一部分。制定了基本的信息架构政策（包括一些战略需求），但政策、标准和工具的合规性没有得到一致遵循。正式明确了数据管理的职能，建立了企业的数据标准，并开始在信息架构的开发和使用中报告标准的遵循情况。开始使用自动化的数据管理工具，但使用流程和规则由数据库软件供应商定义。制定了正式的培训计划，但正式的培训只靠个别部门主动提出。

4 级 可管理级

信息架构的开发和执行有正式的方法和技术。实施了执行信息架构开发流程的问责，对信息架构的成功进行测量。支持信息架构的自动化工具分布广泛但仍没有整合。确定了基本的度量方法并有测量体系。信息架构制定的流程是主动的且关注于将来的业务需求。数据管理部门积极参与到应用开发工作中，以确保数据的一致性。完全建立了自动化的知识库。建立了较为复杂的数据模型以管理数据库的信息内容。执行层的信息系统和决策支持系统使用了可用的数据信息。

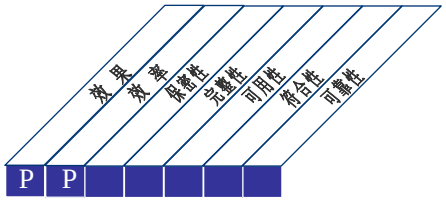
5 级 优化级

信息架构在企业各个层面都得到一致的遵循。持续强调信息架构对业务的价值。IT 人员有专家经验和相应技能，以开发和维护强健和响应良好、可满足所有业务需求的信息架构。信息架构提供的信息一致且应用广泛，在信息架构的开发、维护包括持续的改进流程中广泛使用了行业良好的实践。确定了采用数据仓库和数据挖掘技术管理信息的战略。信息架构持续不断地改进，并考虑了在流程、组织内部和系统中的非传统信息。

3.3. PO3 确定技术方向

3.3.1. 流程描述

信息服务职能部门确定业务支持的技术方向。这需要制定技术基础设施计划和建立架构委员会。架构委员会从产品、服务与交付机制等角度设定和管理清晰并可实现的技术目标，该目标由技术根据提供。该计划应定期更新，包括系统架构、技术方向、获取计划、标准、迁移战略和应急。该计划能及时响应竞争环境的变化、合理安排信息系统人员配置和投资规模，以及改进平台和应用系统的互操作性。

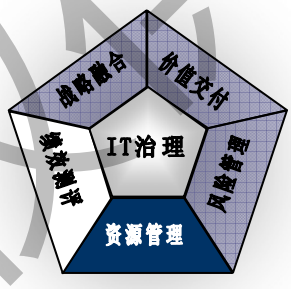


IT 流程中的控制：
确定技术方向

使 IT 满足业务需求：
具有稳定的、低成本的、集成化的和标准的应用系统、资源和能力，以满足现在和将来的业务需求

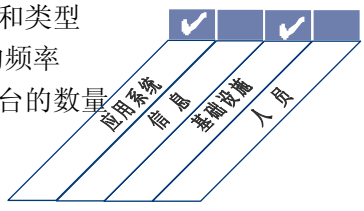
通过关注于：
定义与实施技术基础设施计划、架构和标准，以识别和平衡技术机会。

通过下列实现：
- 建立指导架构和验证架构符合性的论坛
- 建立平衡成本、风险和需求的技术基础设施计划
- 定义基于信息架构需求的技术基础设施标准



主要 次要

通过下列衡量：
- 偏离技术基础设施计划的数量和类型
- 技术基础设施计划评估/更新的频率
- 企业中各部门采用不同技术平台的数量



3.3.2. 控制目标

PO3.1 技术方向计划

通过分析已有的和新兴的技术，计划恰当的技术方向，以利于实现 IT 战略和业务系统架构。在计划中也要也要提出识别计划中潜在的创造业务机会的技术。该计划应阐述系统架构、技术方向、迁移战略和基础设施组件的应急例外考虑。

PO3.2 技术基础设施计划

建立和维护与 IT 战略规划和 IT 战术计划一致的技术基础设施计划。该计划应基于技术方向，并包括应急例外安排和获取技术资源的指南。该计划考虑了竞争环境的变化，合理安排信息系统人员配置和投资规模，改进平台和应用系统的互操作性。

PO3.3 监控未来发展趋势与合规性

建立监控业务部门、同行、技术、基础设施、法律法规环境变化趋势的流程，在开发 IT 技术基础设施计划时同步考虑这些趋势的分析结果。

PO3.4 技术标准

提供企业范围内一致的、高效的、安全的技术解决方案，建立技术论坛以提供技术指导、基础设施产品建议以及技术选择指导，并遵循这些标准和指南的衡量指标。该论坛应基于业务相关性、风险和遵循外部需求来指导技术标准和实践。

PO3.5 IT 架构委员会

建立 IT 架构委员会，以提供架构指导、对架构应用的建议、验证架构的符合性。该委员会应指导 IT 架构设计，确保 IT 架构能满足业务战略、考虑法律法规符合性和持续性需求。可参考 PO2 定义信息架构。

3.3.3. 管理指南

源自	输入
PO1	IT 战略规划和 IT 战术计划
PO2	优化的业务系统计划、信息架构
AI3	技术标准的更新
DS3	绩效和能力信息

输出	到						
技术机会	AI3						
技术标准	AI1	AI3	AI7	DS5			
技术状态的定期更新	AI1	AI2	AI3				
技术基础设施计划	AI3						
基础设施需求	PO5						

RACI 图

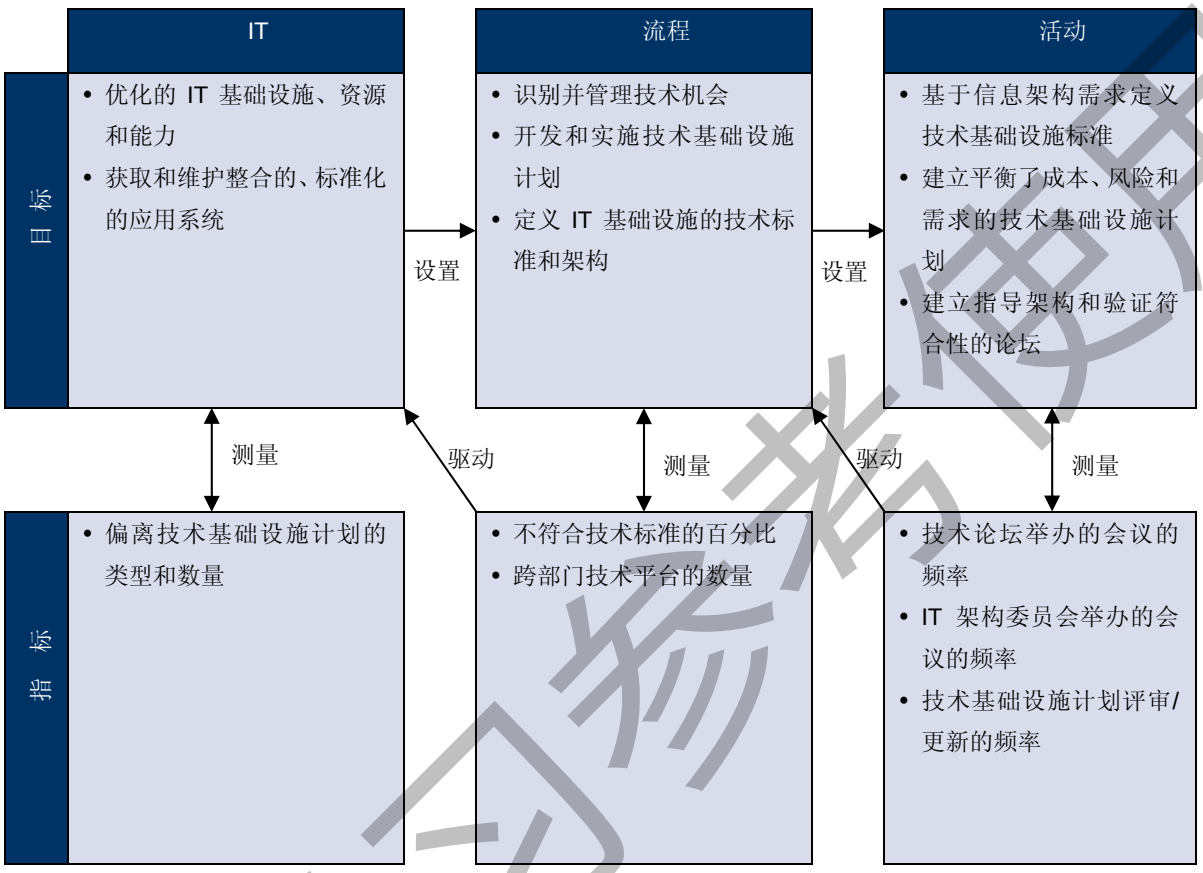
职能

活动

	首席执行官	首席财务官	业务执行经理	首席信息官	业务流程所有者	运营总监	首席架构师	开发总监	IT行政总监	项目管理官	合规、审计、风险和安全
创建并维护技术基础设施计划		I	I	A		C	R	C	C		C
创建并维护技术标准				A		C	R	C	I	I	I
发布技术标准		I	I	A		I	R	I	I	I	I
监控技术发展		I	I	A		C	R	C		C	C
定义新（未来的/战略的）技术的使用		C	C	A		C	R	C		C	C

RACI 图中，**R**esponsible 代表**执行**，**A**ccountable 代表**责任**，**C**onsulted 代表**商议**，**I**nformed 代表**告知**。

3.3.4. 目标和指标



3.3.5. 成熟度模型

管理“确定技术方向”流程，使 IT 满足业务需求：具有满足现在和将来业务需求的稳定的、低成本、整合的和标准化的应用系统、资源和能力。

0 级 无级别

未意识到技术基础设施计划对于企业的重要性。不存在开发技术基础设施计划必需的知识和经验。缺少对利用技术变化编制计划是有效分配资源的关键之理解。

1 级 初始级

管理层认识到技术基础设施规划的必要性。技术组件的开发和现有技术的贯彻是初始的和孤立的。基础设施规划是反应式和只关注于操作层面的。技术方向经常受相互矛盾的硬件、系统软件和应用软件供应商的产品演变计划所左右。对技术变化的潜在影响的沟通相互矛盾。

2 级 可重复级

技术规划的必要性和重要性已经被传达。该计划是战术性的，关注于解决技术难题的所需要的技术解决方案，而非利用技术满足业务需求。对技术变化的评价依赖于不同个体的直觉，但类似的流程。个人通过持续学习和技术的重复应用获得技术规划的经验。通用的技术和标准正在基础设施组件的开发中形成。

3 级 定义级

管理层意识到技术基础设施计划的重要性。技术基础设施计划的开发流程是合理的，并与 IT 战略计划相一致。制定了书面和被良好沟通的技术基础设施计划，但没有得到一致的应用。技术基础设施方向包括在风险和与组织战略相一致的基础上理解组织期望在技术应用上处于领先或落后地位。在了解供应商长期的技术方向和产品开发计划与组织方向保持一致的基础上选择关键供应商。对角色和职责有正式的培训和沟通。

4 级 可管理级

管理层保证技术基础设施计划的开发和维护。IT 人员有开发技术基础设施计划必需的经验和技能。考虑了现有技术和变化的潜在影响。管理层能识别计划的偏离度并预测问题。分配了技术基础设施计划的开发和维护职责。技术基础设施计划的开发流程是复杂的并能响应变化。内部好的实践已被引入到该流程中。人力资源战略和技术方向保持一致，确保 IT 人员能管理技术的变化。为引入新技术制定了迁移计划。通过外部供应商和合作伙伴的协助，取得适当的经验和技能。管理层已利用领先抑或落后的技术在开发新业务机会或运行有效性中的可接受风险进行了分析。

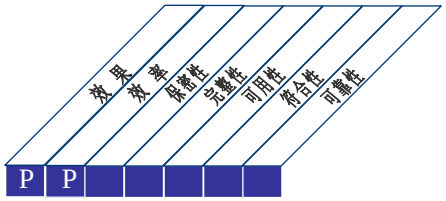
5 级 优化级

有研究部门来评价准备采用和已经使用的技术，并以行业标准作为组织的标杆。技术基础设施计划的方向由行业和国际标准来指导和开发，而非由技术厂商所左右。高级管理层评审技术变化对业务的潜在影响。采用新技术方向和变更技术方向得到管理层的正式批准。企业有一个强健的满足业务需求的技术基础设施计划，对业务环境的变化能够积极响应并及时改进。有持续的和强制的流程来改进技术基础设施计划。行业最佳实践被广泛用于确定技术方向。

3.4. PO4 定义 IT 流程、组织和关系

3.4.1. 流程描述

IT 组织的建立应考虑以下需求：人员、技能、职能、责任、授权、角色、职责和监督。IT 组织应纳入 IT 流程框架以确保透明度和控制、以及高级管理层及业务管理层的参与。IT 战略委员会确保董事会对 IT 的关注，由业务和 IT 部门参与的一个或多个执行委员会确定与业务要求一致的 IT 资源的优先级。所有职能都应有适当的流程、管理政策和程序以特别关注控制、质量保证、风险管理、信息安全、数据及系统所有权和职责分离。为确保能及时支持业务需求，IT 应纳入相关决策流程中。



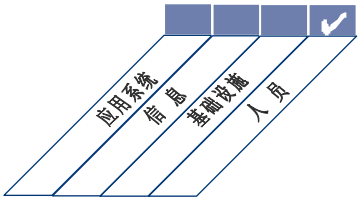
控制 IT 流程：
定义 IT 流程、组织和关系

使 IT 满足业务需求：
在遵从治理需求时灵活响应业务战略，提供确定的、有胜任能力的组织和人员。

通过关注于：
建立明晰的、灵活的、响应及时的 IT 组织架构，所有者定义和实施 IT 流程，IT 的角色和职责整合到业务和决策流程中。

通过下列实现：
- 定义 IT 流程框架
- 建立合适的组织实体和架构
- 定义角色和职责

通过下列衡量：
- 岗位、授权有正式文件描述的角色占比
- 根据战略要求，IT 组织应该支持而未能支持的业务单元/流程的数量
- 没有遵循 IT 组织标准或没有经过批准，在 IT 组织外部的核心 IT 活动数量



3.4.2. 控制目标

PO4.1 IT 流程框架

定义执行 IT 战略规划的 IT 流程框架。该框架应包括 IT 流程结构与相互关系(如，管理 IT 流程的盲点和重复)、所有权、成熟度、绩效测评、改进、合规性、质量目标以及实现它们的计划。该框架应整合面向 IT 的各个流程、企业优化组合管理流程、业务流程和业务变更流程。该 IT 流程框架应整合在质量管理体系（QMS）和内部控制框架之中。

PO4.2 IT 战略委员会

在董事会层面建立 IT 战略委员会。该委员会应确保作为企业治理一部分的 IT 治理得到充分重视，对战略方向提出建议，代表全体董事评审重大投资。

PO4.3 IT 指导委员会

建立由高级管理层、业务管理层和 IT 管理层组成的 IT 指导委员会（或同等机构）以：

根据企业的业务战略和优先级来确定 IT 启用投资项目群（IT-enabled investment programmes）的优先级；

跟踪项目状态，解决资源冲突；

监控服务水平和服务改进。

PO4.4 IT 职能的组织定位

根据在企业内与 IT 重要性有关的业务模型、特别是 IT 对业务战略的重要性和依赖于 IT 的运营水平，在整个组织结构内定位 IT 职能。CIO 的报告路线应该与 IT 在企业内的重要性相当。

PO4.5 IT 组织结构

建立支持业务需要的内部和外部 IT 组织结构。此外，还要建立定期检查 IT 组织结构的流程，以调整人员配备需求和资源战略，满足预期的业务目标和适应环境的变化。

PO4.6 角色和职责的建立

建立和传达 IT 人员和最终用户的角色和职责，以描述 IT 人员和最终用户的授权、职责和责任，以满足组织的需要。

PO4.7 IT 质量保证职责

为履行质量保证（QA）职能分派职责，为 QA 小组提供适当的 QA 系统、控制技巧和沟通专长。确保 QA 小组的组织定位、职责和规模满足组织的需求。

PO4.8 风险、安全和合规性职责

在适当的高层级别上确定业务部门内与 IT 相关风险的所有权和职责。定义和分派管理 IT 风险的关键角色，包括信息安全、物理安全和合规管理的具体职责。在企业级建立风险和安全管理职责以解决组织范围内的问题。额外的安全管理职责可以分派给特定的系统以处理相关的安全问题。从高级管理层获得对 IT 风险偏好的指导和剩余 IT 风险的审批。

PO4.9 数据和系统所有权

为业务部门提供程序和工具，使其业务部门能够履行其数据和信息系统所有者的职责。

所有者应对信息、系统分类作决策，并根据这些分类对信息和系统做保护决策。

PO4.10 监督

在 IT 部门实施适当的监督活动，以确保角色和职责得到正确履行。评估所有职员是否具备充分的授权和资源，以履行其角色和职责并检查其关键绩效指标（KPIs）。

PO4.11 职责分离

实施角色和职责的分离，减少单个成员危及关键流程安全的可能性。确保职员仅限于履行授权给他们的与其工作和职位相关的职责。

PO4.12 IT 职位

定期或在业务部门、运行或 IT 环境发生重大变化时评估 IT 职位需求，确保 IT 部门有足够的资源来充分适当地支持业务愿景和目标。

PO4.13 关键 IT 职员

定义并识别关键 IT 职员（如替代/后备人员），尽量减低因单人履行关键工作而造成的依赖性。

PO4.14 签约职员的政策和程序

确保支持 IT 部门的顾问和签约人员知道并遵守组织的信息资产保护政策，并满足达成一致的合同要求。

PO4.15 关系

在 IT 部门和内部、外部利益相关方之间建立和维护最佳的协调、沟通和联络结构。这些利益相关方如：董事会、高级管理层、业务部门、单独的用户、供应商、安全官员、风险经理、公司合规部门、外包和离场管理者。

3.4.3. 管理指南

源自	输入
PO1	IT 战略和战术计划
PO7	IT 人力资源政策和程序、IT 技能矩阵、工作描述
PO8	质量改进措施
PO9	IT 相关风险整改措施计划
ME1	整改措施计划
ME2	IT 控制有效性报告
ME3	IT 服务交付适用的法律法规需求目录
ME4	流程框架改进

输出	到						
IT 流程框架	ME4						
书面的系统所有者	AI7	DS6					
IT 组织和关系	PO7						
IT 流程框架，书面的角色和职责	ALL						
角色和职责档案	PO7						

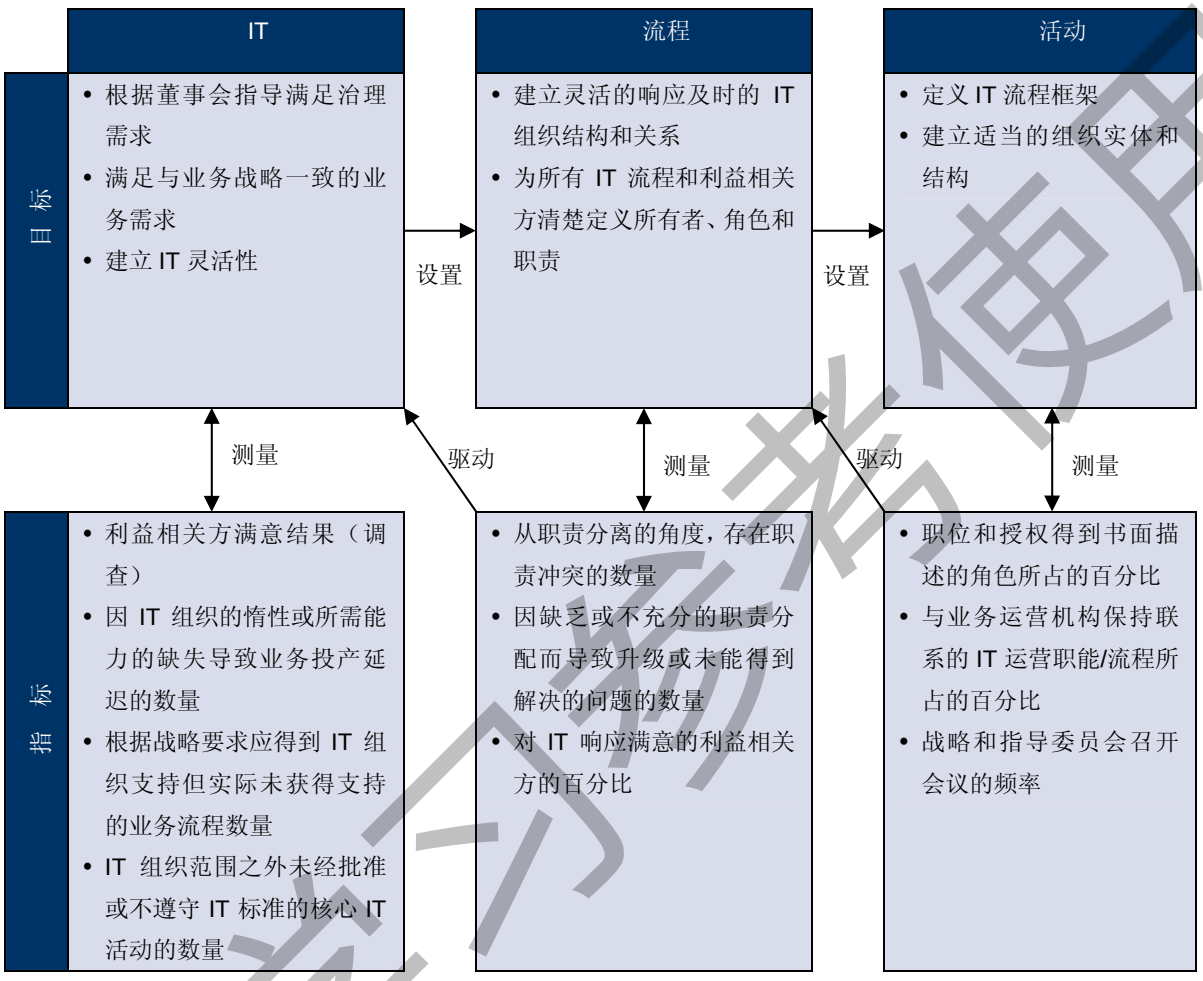
RACI 图

职能

活动	首席执行官	首席财务官	业务执行经理	首席信息官	业务流程所有者	运营总监	首席架构师	开发总监	IT行政总监	项目管理官	合规、审计、风险和安全
建立 IT 组织结构，包括各委员会，与利益相关方、厂商的联系	C	C	C	A		C	C	C	R	C	I
设计 IT 流程框架	C	C	C	A		C	C	C	R	C	C
识别系统所有者		C	C	A	C	R	I	I	I	I	I
识别数据所有者		I	A	C	C	I	R	I	I	I	C
制定并履行 IT 角色与职责，包括监督和职责分离		I	I	A	I	C	C	C	R	C	C

RACI 图中，**R**esponsible 代表**执行**，**A**ccountable 代表**责任**，**C**onsulted 代表商议，**I**nformed 代表**告知**。

3.4.4. 目标和指标



3.4.5. 成熟度模型

管理“定义 IT 流程、组织和关系”流程，使 IT 满足业务需求：在遵从治理需求时灵活响应业务战略，提供确定的、有胜任能力的组织和人员。对该流程的管理有以下分类：

0 级 无级别

没有建立有效的 IT 组织来集中关注业务目标的达成。

1 级 初始级

IT 活动和职能的实施是被动的和不一致的。IT 仅在业务项目的后期才考虑。IT 的职能被考虑为支持职能，缺乏对整个组织远景的考虑。意识到 IT 部门的必要性，但 IT 的角色和职责既没有正式化，也没有得到有效的履行。

2 级 可重复级

IT 职能已组织化，能有序地响应客户需求，并对供应商进行管理，但都缺乏一致性。知道 IT 部门规范化管理和对供应商进行管理的需求，但决策仍然取决于个别关键人员的知识和技能。管理 IT 组织和供应商关系的通用技术开始形成。

3 级 定义级

明确了 IT 部门和第三方的角色和职责。根据 IT 战略建立了 IT 部门并形成文件予以传达。规定了 IT 内部控制环境，与其他相关方（包括各执行委员会、内部审计、供应商管理）的关系正规化。IT 部门在职能上完整。IT 人员和用户需要履行的相关职能定义明确。定义了基本的 IT 人员岗位需求和专家需求，并配备到位。与用户和第三方的沟通协作关系的定义是正式的。对 IT 相关角色和职责的分解进行了定义和实施。

4 级 可管理级

IT 组织架构主动响应变化，IT 组织包含满足业务需求的所有必需的角色。定义并明确了 IT 管理层、流程所有权、职责和权利。内部好的实践已在 IT 部门得到应用。IT 管理层具有定义、实施和监控较佳的 IT 组织架构和沟通协作关系的专家经验和技能。支持业务目标和用户确定的关键成功因素（CSFs）的可测量准则已标准化。建立了 IT 人员的职业技能库以支持项目人员配备和专业发展的需要。定义了平衡 IT 部门内部可用资源、技能与从组织外部获取资源和技能的方法并得到实施。IT 组织架构通过提供与战略业务流程一致而不是与孤立的技术一致的服务来满足业务需求。

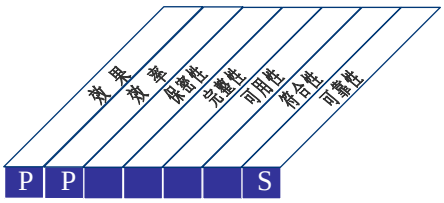
5 级 优化级

IT 组织架构灵活且具有自适应能力。行业最佳实践得到推广。有助于监控 IT 组织架构和流程业绩的技术得到广泛使用。支持复杂的和在地理上分散的 IT 组织架构的技术得到有效使用。具有适当的持续改进流程。

3.5. PO5 IT 投资管理

3.5.1. 流程描述

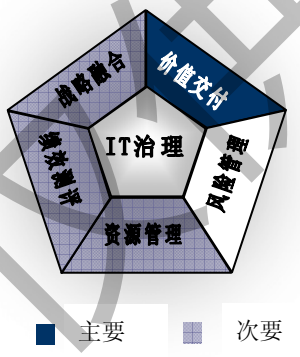
建立和维护管理 IT 投资项目群的框架，该框架包括成本、收益、预算的优先次序、正式的预算编制流程和对预算的管理。和利益相关方商议，以识别和控制在 IT 战略和战术计划中的总成本和收益，且在必要时采取纠正措施。该流程鼓励 IT 和业务利益方的合作，促使 IT 资源使用的效率和效果，为所有者的总成本（TCO）、业务收益的实现以及 IT 投资的回报率（ROI）提供透明度和责任。



控制 IT 流程：
IT 投资管理

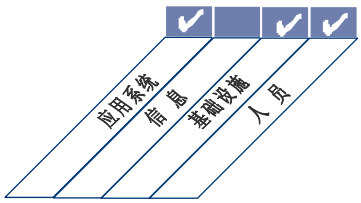
使 IT 满足业务需求：
通过综合的、标准化的服务，扎实并持续地改进 IT 成本有效性，提高对业务收益率的贡献，满足最终用户的期望。

通过关注于：
安排并跟踪 IT 预算与 IT 战略和投资决策的一致性，对 IT 投资和投资组合做有效及时的决策。



通过下列实现：
- 预测并分配预算
- 定义正式的投资标准（ROI，回收期，净现值（NPV））
- 测量并评估预测的业务价值

通过下列衡量：
- 交付的 IT 服务的单位成本的减少占比
- 预算偏离价值与总预算相比的比例
- 用业务价值来表达的 IT 支出比例（如，因连通性增强，销售/服务随之增加）



3.5.2. 控制目标

PO5.1 财务管理框架

建立和维护财务框架，以管理整个 IT 投资组合、业务模式和 IT 预算的 IT 资产和服务的投资和成本。

PO5.2 IT 预算内的优先级

实施一个决策流程，以分配运营、项目和维护等方面所需 IT 资源的优先级，使 IT 对优化 IT 投资项目群、其他 IT 服务和资产的企业投资组合收益的贡献最大化。

PO5.3 编制 IT 预算

建立和实施预算准备流程，该预算应反映企业 IT 投资项目群的投资组合所确定的优先级，并包括运行和维护现有基础设施所需的当期成本。该流程既要支持编制整个 IT 预算，又要能够根据项目内 IT 组件的具体情况，支持编制单个项目群的预算。该流程应允许对整体预算和单个项目群预算的持续检查、细化和审批。

PO5.4 成本管理

实施成本管理流程，比较实际成本和预算。应监控并报告成本。如出现偏差，应及时识别偏差，并评估这些偏差对项目的影响。与项目的业务发起者共同采取适当的整改措施，必要时更新这些项目的业务模式。

PO5.5 收益管理

实施一个流程，以监控提供和保持合适 IT 容量的收益。应识别、监控、报告、认可和在业务模式中阐明 IT 对业务的贡献，该贡献无论是作为 IT 投资项目群的组成部分，还是定期运营支持的一部分。对收益报告做检查，有机会改进 IT 收益贡献时，应制定并采取适当的措施。若 IT 收益的变化影响到项目群，或其他相关项目的变更影响到项目群，则应更新该项目群的业务模式。

PO5 IT 投资管理

3.5.3. 管理指南

源自	输入
PO1	IT 战略和战术计划，项目和服务投资组合
PO3	基础设施需求
PO10	更新了的 IT 项目投资组合
AI1	业务需求可行性研究
AI7	实施后评估
DS3	绩效和能力计划（需求）
DS6	IT 财务
ME4	IT 保障业务投资期望的业务成果

输出	到						
成本收益报告	PO1	AI2	DS6	ME1	ME4		
IT 预算	DS6						
更新了的 IT 服务投资组合	DS1						
更新了的 IT 项目投资组合	PO10						

RACI 图

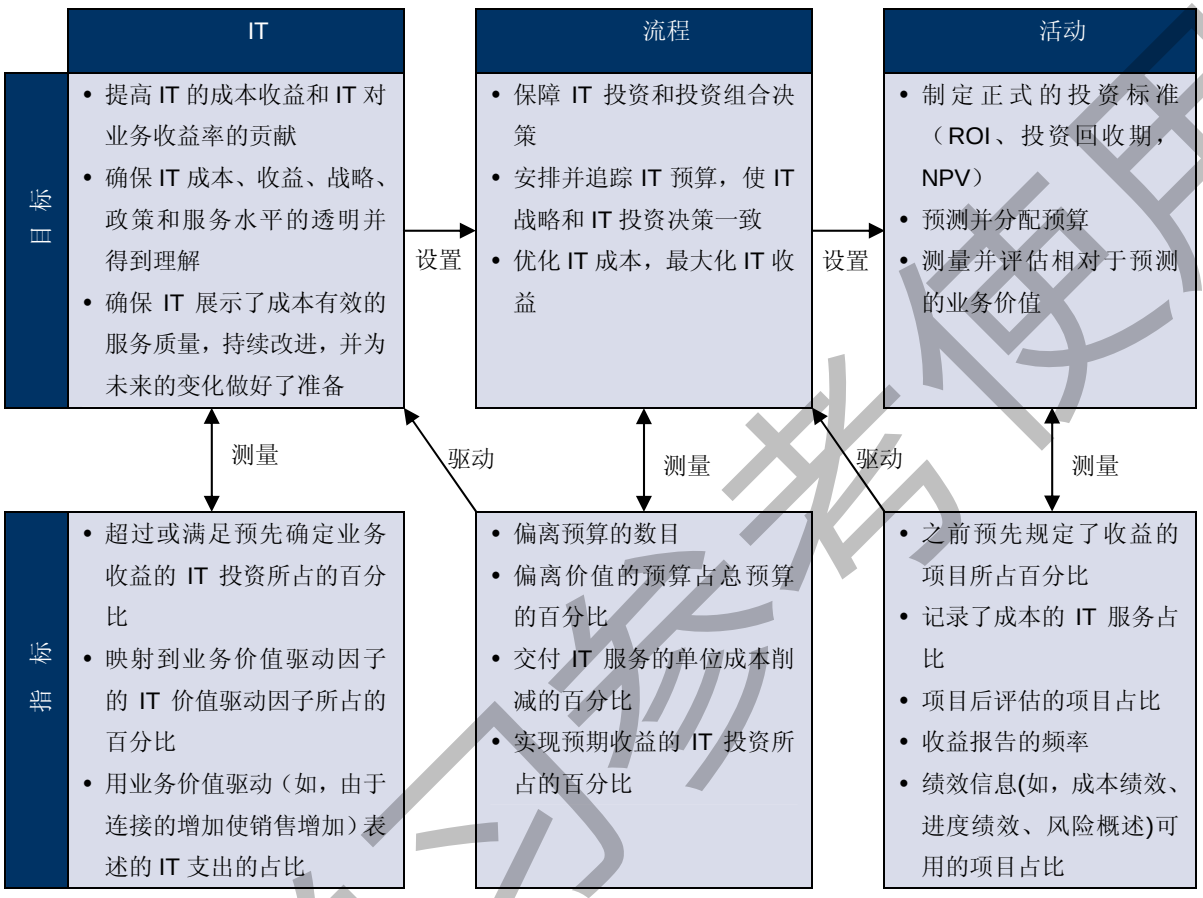
职能

活动

维护项目群投资组合	A	R	R	R	C					I	I
维护项目投资组合	I	C	A/R	A/R	C		C	C		C	I
维护服务投资组合	I	C	A/R	A/R	C	C				C	I
建立并维护 IT 预算编制流程	I	C	C	A		C	C	C	R	C	
识别、沟通并监控 IT 投资、成本及对业务部门的价值	I	C	C	A/R		C	C	C	R	C	C

RACI 图中，**R**esponsible 代表**执行**，**A**ccountable 代表**责任**，**C**onsulted 代表**商议**，**I**nformed 代表**告知**。

3.5.4. 目标和指标



3.5.5. 成熟度模型

管理“管理 IT 投资”流程，使 IT 满足业务需求：通过综合的、标准化的服务，扎实并持续地改进 IT 成本有效性，提高对业务收益率的贡献，满足最终用户的期望，对该流程的管理有以下的分级：

0 无级别

未意识到 IT 投资选择和预算编制的重要性。没有跟踪或监控 IT 投资和花费。

1 初始级

组织认识到管理 IT 投资的必要性，但这一需求没有一致沟通。初步分配了 IT 投资选择和预算编制的职责。没有独立地进行 IT 投资选择和预算，而且没有形成正式的文档。只是偶尔对 IT 投资进行基本判断。编制预算的决策是被动的，仅关注具体的运作。

2 可重复级

对 IT 投资选择和预算编制的必要性有一定理解。沟通了选择和预算编制流程必要性。其符合性主要依赖于组织内个体的自觉性。形成了开发 IT 预算组件的共用技术。编制预算决策是被动的且是策略性的。

3 已定义级

定义了投资和编制预算的策略和流程，并形成文件予以传达，涵盖了关键的业务和技术重点。IT 预算与 IT 战略规划和业务战略规划一致。编制预算和 IT 投资选择流程形成正式的文件并得到沟通。正式培训在进行中，但仍旧主要基于个人的自觉性。正在实行对 IT 投资选择和预算的正式批准。IT 人员具备开发 IT 预算和推荐适当 IT 投资所需的技能和经验。

4 可管理级

将投资选择和编制预算的职责和责任落实到人。识别并解决预算偏差。实施正式的成本分析，分析的内容涵盖了现有运营的直接和间接成本以及被提议的投资，考虑整个生命周期的全部成本。使用预先规定的标准化的预算编制流程。在投资计划中考虑了从硬件、软件到系统集成的开发和运营成本以及 IT 人力资源的开发和运营成本发生变化的影响。采用财务和非财务指标来计算收益和回报。

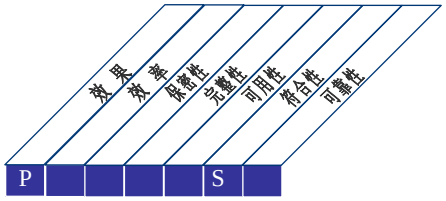
5 优化级

应用行业最佳实践进行成本基准管理，识别了提高投资有效性的方法。在投资选择和编制预算流程中应用技术开发分析。根据实际投资绩效分析中所获取的经验来持续改进投资管理流程。投资决策融合了价格/绩效改进趋势。使用正式的评价方法，在组织现有的资本结构框架内来对融资替代方案进行正式调查和评价。对投资变化有预先的确认。整个生命周期的长期成本和收益分析融入到投资决策中。

3.6. PO6 沟通管理目标和方向

3.6.1. 流程描述

管理层应建立企业的 IT 控制框架并制定和传达制度。通过持续不断的沟通来清晰的传达经过管理层批准并获得其支持的 IT 宗旨、服务目标、制度和流程等。沟通能够支持 IT 目标的实现，并确保对业务风险、IT 风险、IT 目标和方向的认知和理解。该流程应确保遵循相关的法律法规。



控制 IT 流程：

沟通管理目标和方向

使 IT 满足业务要求：

提供关于当前和将来的 IT 服务、相关风险和职责的准确、及时的信息。

通过关注于：

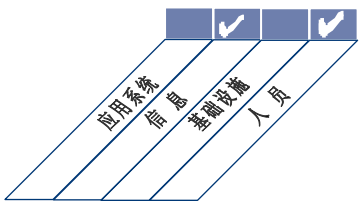
在既定的 IT 框架内，向利益相关方提供正确的、可理解的、经过批准的政策、流程、指南和其他的文档。

通过下列实现：

- 定义 IT 控制框架
- 制定和发布 IT 政策
- 执行 IT 政策

通过下列衡量：

- 因 IT 服务中断导致业务中断的数量
- 理解企业 IT 控制框架的利益相关方所占的百分比
- 未遵循 IT 政策的利益相关方所占的百分比



3.6.2. 控制目标

PO6.1 IT 政策和控制环境

根据企业的管理理念和运营模式，定义 IT 控制环境要素，这些要素包括：对 IT 投资交付价值的预期/要求、风险偏好、完整性、道德价值、职员胜任能力、责任和职责。该 IT 控制环境应基于一种企业文化，这种文化是：在管理重大风险的同时确保价值交付，鼓励跨部门的合作与团队协作，促进合规并持续改进流程，充分处理流程偏差（包括失效）。

PO6.2 企业 IT 风险和控制框架

制定和维护 IT 风险和控制框架，该框架定义了企业 IT 风险和控制的整体方法，并使企业的 IT 政策和控制环境与企业的风险和控制框架一致。

PO6.3 IT 政策管理

制定并维护一系列政策以支持 IT 战略。这些政策应该包括政策目的、角色和职责、例外流程、符合性指引以及参考程序、标准和指南。应定期确认和核准这些政策的适当性。

PO6.4 政策、标准与程序发布

向所有相关的职员发布并实施 IT 政策，因此 IT 政策成为企业运营的一个组成部分。

PO6.5 IT 目标和方向的沟通

通过沟通，让整个企业中适当的利益相关方和用户意识到并理解业务和 IT 的目标和方向。

3.6.3. 管理指南

源自	输入
PO1	IT 战略和战术计划、IT 项目和服务投资组合
PO9	IT 相关风险管理指南
ME2	IT 控制有效性报告

输出	到
企业 IT 控制框架	ALL（所有 COBIT 控制活动）
IT 政策	ALL（所有 COBIT 控制活动）

RACI 图　　职能

活动

	首席执行官	首席财务官	业务执行经理	首席信息官	业务流程所有者	运营总监	首席架构师	开发总监	IT行政总监	项目管理官	合规、审计、风险和安全
建立并维护 IT 控制环境和框架	I	C	I	A/R	I	C		C	C		C
制定并维护 IT 政策	I	I	I	A/R		C	C	C	R		C
沟通 IT 控制框架、IT 目标和方向	I	I	I	A/R					R		C

RACI 图中，**R**esponsible 代表**执行**，**A**ccountable 代表**责任**，**C**onsulted 代表**商议**，**I**nformed 代表**告知**。

3.6.4. 目标和指标

3.6.5. 成熟度模型

管理“沟通管理目标和方向”流程，使 IT 满足业务需求：为当前和将来的 IT 服务、相关风险和职责提供准确、及时的信息。

0 级 无级别

管理层未建立明确的 IT 控制环境。没有认识到需要建立一套 IT 政策、方案、程序和复合性流程。

1 级 初始级

管理层响应式发布信息控制环境的需求。只是当问题发生时，才制定并传达 IT 策略、程序和标准。开发、沟通和符合性流程都是非正式的和不一致的。

2 级 可重复级

管理层已开始意识到建立有效的信息控制环境的必要和需求，但实践大部分是非正式的。管理者沟通了 IT 控制策略、计划和程序的需求，但开发这些需求却仅依赖于个别管理者或业务领域的判断。认识到质量是期望遵循的价值理念，但实践依赖于个别管理者的判断。需要时，才对个体进行培训。

3 级 定义级

管理层制定了完整的信息控制和质量管理环境，并形成文件予以传达，环境中包括 IT 政策、计划和程序方面的框架。IT 政策的开发流程是结构化和可维护的，且为所有成员了解。现有的政策、计划和程序是相对合理的，并覆盖了关键的问题。管理者强调了 IT 安全意识的重要性并有培训计划。有支持信息控制环境的正式培训计划但没有得到严格执行。虽然存在控制策略和程序的整体开发框架，但对这些策略和程序符合性的监控并没有一贯执行。已形成标准的和正式的提升安全意识的途径。

4 级 可管理级

管理层承担沟通内部控制策略的职责，授权职责并分配充分的资源来维护内部控制环境与重大变更的一致性。建立了积极的、主动的信息控制环境，包括质量和 IT 安全意识方面的承诺。开发、维护和传达了一套完整的政策、计划和程序，并构成了内部最佳的实践。建立了发布和随后的符合性检查的框架。

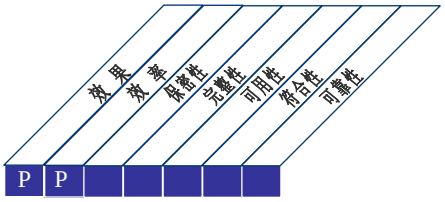
5 级 优化级

信息控制环境与战略管理框架和理念一致，并经常进行评审、更新和持续改进。指派内外部专家以确保采纳控制指导和沟通技巧有关的行业较佳实践。监控、自评估、符合性检查在组织内得到普遍开展。采用办公自动化和基于计算机的培训工具来维护制度、认知知识库及实现沟通优化。

3.7. PO7 IT 人力资源管理

3.7.1. 流程描述

获得、保持并激发具备能力的员工为业务创造和交付 IT 服务。为实现上述目标，应遵循界定的程序，包括招聘、培训、绩效评估、晋升和终止等程序。这一流程很重要，因为人是重要的资产，管理和内部控制环境非常依赖于有胜任能力和工作热情的人员。



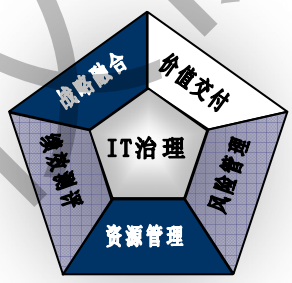
控制 IT 流程：
IT 人力资源管理

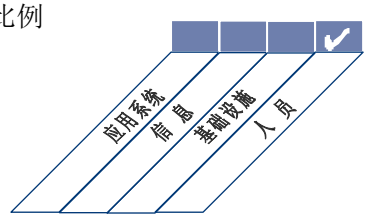
使 IT 满足业务需求：
获得有胜任能力和工作热情的人员来实施并交付 IT 服务

通过关注于：
雇用并培训人员，通过清晰的职业规划来激励，分配与技能相对应的角色，建立规定的评审过程，创建岗位描述，并确保意识到对个体的依赖。

通过下列实现：
- 评审人员绩效
- 雇用并培训 IT 人员以支持 IT 战术计划
- 降低对关键资源过度依赖带来的风险

通过下列衡量：
- 利益相关方对 IT 人员的技能和经验的满意程度
- IT 人员流动率
- 获得资格认证的 IT 人员比例





主要　次要

3.7.2. 控制目标

PO7.1 人员招聘和保持

确保 IT 人员的招聘流程与整个组织的员工制度和流程相一致（即雇用、良好的工作环境和入职培训）。应执行程序以确保组织所雇用的 IT 人员具备实现组织目标所需的技术能力。

PO7.2 人员能力

以人员的教育、培训和/或经验为基础，定期核实人员是否具备履行其职责的能力。定义关键的 IT 能力要求，并通过职业资格和认证方式维持这种能力。

PO7.3 角色分配

规定、监控和管理人员的角色、职责和薪酬框架，包括遵守管理策略和程序的要求，以及道德规范和职业惯例。雇佣的条款和条件应强调雇员在信息安全、内部控制与法律法规符合性方面的职责。监督级别与职位敏感度、分配的职责范围保持一致。

PO7.4 人员培训

雇用时为 IT 人员提供适当的指导，并对其进行持续教育以保持他们的知识、技巧、能力、内部控制和安全意识达到完成组织目标所要求的级别。

PO7.5 对个体的依赖程度

通过知识的获取（文档化）、知识共享、持续性规划和人员备份等方式来最小化对于关键人员过于依赖的风险。

PO7.6 人员选拔程序

IT 人员招聘程序包括背景检查。应根据职能的敏感程度和/或关键程度来确定检查的范围和频率。应对所有的雇员、合同方和供应商进行背景检查。

PO7.7 雇员工作业绩评估

根据个体目标（来源于组织目标）、既定标准、具体的工作要求定期、及时评价工作业绩。雇员应在适当的时候接受履职训练和指导。

PO7.8 工作变更与终止

关于工作变化（尤其是工作终止）时，应采取一些权宜之计。应安排知识的传递、职责的再分配和权限的彻底删除，以实现风险最小化并保障职能的持续性。

3.7.3. 管理指南

源自	输入
PO4	IT 组织和关系；形成文件的角色和职责
AI1	业务需求可行性研究

输出	到						
IT 人力资源策略和程序	PO4						
IT 技能矩阵	PO4	PO10					
工作描述	PO4						
用户的技能和能力，包括个人培训	DS7						
特殊培训需求	DS7						
角色和职责	ALL						

RACI 图

活动 \ 职能	首席执行官	首席财务官	业务执行经理	首席信息官	业务流程所有者	运营总监	首席架构师	开发总监	IT行政总监	项目管理官	合规、审计、风险和安全
识别 IT 技能、职位描述、薪酬范围和个人绩效计分卡		C		A		C	C	C	R	C	
执行与 IT 相关的人力资源策略和程序（招聘、雇用、审查、报酬、培训、评价、晋升和解雇）				A		R	R	R	R	R	C

RACI 图中，**R**esponsible 代表**执行**，**A**ccountable 代表**责任**，**C**onsulted 代表**商议**，**I**nformed 代表**告知**。

3.7.4. 目标和指标

3.7.5. 成熟度模型

管理“IT 人力资源管理”流程，使 IT 满足业务需求：获取有胜任能力和工作热情的人员，以创造和交付 IT 服务。

0 级 无级别

未意识到 IT 人力资源管理和组织技术规划流程保持一致的重要性。没有人员或组织正式的负责 IT 人力资源管理。

1 级 初始级

管理者认识到需要 IT 人力资源管理。IT 人力资源管理流程是非正式的和反应式的。IT 人力资源管理流程运作中关注 IT 人员的雇用和管理。管理层意识到并开始关注因为业务和技术快速以及日益复杂的解决方案，对新的技能和能力水平的需求。

2 级 可重复级

采用策略性的方式来雇用和管理 IT 人员，但只受特定项目需求的驱动，而非基于内外部实用的、能胜任的人员的平衡。对于新员工进行非正式的培训，其后提供的培训仅仅是基于需要的基础之上。

3 级 定义级

建立了明确的、书面的 IT 人力资源管理流程。存在 IT 人力资源管理计划。有一个战略方法以雇佣和管理 IT 人员。设计了正式的符合 IT 人力资源需求的培训计划。建立了轮岗方案，有计划的发展 IT 人员的技术和业务管理能力。

4 级 可管理级

开发和维护 IT 人力资源管理计划的职责被分配给具体的个人或团队，这些个体或团队具备开发和维护计划所需的经验和技能。开发和管理 IT 人力资源管理计划的流程可以响应变更。组织将测量方法标准化，有助于识别与 IT 人力资源管理计划的偏差，并特别的强调 IT 人员增长率和流动率的管理。建立薪酬体系和业绩评审，并与其他 IT 组织和行业最佳惯例相比较。IT 人力资源管理是前瞻性的，并考虑到了职业发展路线。

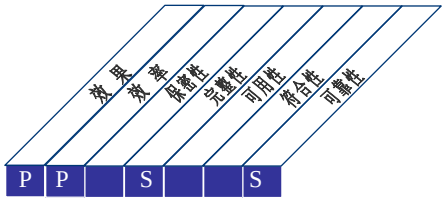
5 级 优化级

持续更新 IT 人力资源管理计划以满足业务需求的变化。IT 人力资源管理与技术计划相结合，确保优化开发并使用可利用的 IT 技能。IT 人力资源管理与企业战略导向相结合，并能响应战略导向的需求。IT 人力资源管理的组件与行业最佳惯例保持一致，例如薪酬、绩效评审、参与行业论坛、知识传递、培训和指导。在组织应用所有新技术标准和产品之前，开发培训方案。

3.8. PO8 质量管理

3.8.1. 流程描述

应建立和维护质量管理体系（QMS），包括已批准的开发与获取的流程和标准。利用清晰的质量需求、程序和政策来编制质量管理计划、实施质量管理和维护质量管理体系。用可实现的定量指标阐述和传达质量要求。通过持续的监控、分析和响应偏差来实现持续改进，并将结果传达给利益相关方。质量管理确保了 IT 为业务交付价值、持续改进和对利益相关方透明。



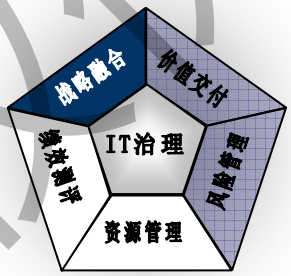
控制 IT 流程：
质量管理

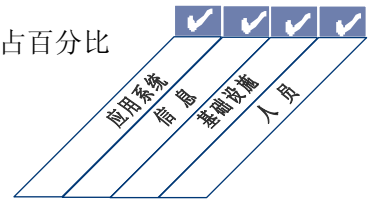
使 IT 满足业务需求：
确保持续改进并测量 IT 交付服务的质量

通过关注于：
定义 QMS，依据既定的目标持续测量绩效，实施持续改进 IT 服务的方案。

通过下列实现：
- 定义质量标准和实践
- 依据既定的标准和实践，监控和测量内外部绩效.
- 持续改进 QMS

通过下列衡量：
- 对 IT 质量满意的利益相关方的百分比（按重要程度衡量）
- 定期进行正式的质量保障评审（QA）且满足质量目标的 IT 过程的百分比
- 接受质量保障评审的过程所占百分比





3.8.2. 控制目标

PO8.1 质量管理体系

建立并维护 QMS，以提供一个标准的、正式的和持续的质量管理方法，该方法与业务需求保持一致。QMS 确定了质量需求和标准、关键 IT 过程及过程间的顺序和交互作用，并确定了定义、检测、纠正和预防不一致性的政策、标准和方法。QMS 应定义质量管理的组织架构、角色、任务和职责。所有的关键职能领域应根据标准和政策制定质量计划，并记录质量数据。监控和测量 QMS 的有效性和接受程度，并在需要时进行改进。

PO8.2 IT 标准与质量实践

识别并保持关键 IT 过程的标准、程序和实践，以指导组织满足 QMS 的目的。当改进和修整组织质量惯例时，可参考行业的最佳惯例。

PO8.3 标准的开发与获取

最终交付物在生命周期内都要采用和维持系统开发和获取的标准，包括在关键里程碑所使用的基于一致的结束标准。要考虑的因素包括：软件编程标准；命名约定；文件格式；规划和数据字典设计标准；用户界面标准；互用性；系统性能效率；可测量性；开发和测试标准；需求验证；测试计划；单元；回归和集成测试。

PO8.4 以客户为中心

通过确定客户需求并将需求整合到 IT 标准和实践中来确保质量管理以客户为关注焦点。定义了在用户/客户与 IT 组织之间产生冲突时的相关角色和职责。

PO8.5 持续改进

保持、定期沟通并持续改进全面质量计划。

PO8.6 质量的测量、监视和评审

规定、策划和实施测量以监控 QMS 持续的符合性，以及 QMS 提供的价值。过程所有者应测量、监控和记录信息，以采取适当的纠正和预防措施。

3.8.3. 管理指南

源自	输入
PO1	IT 战略规划
PO10	详细项目计划
ME1	补救措施计划

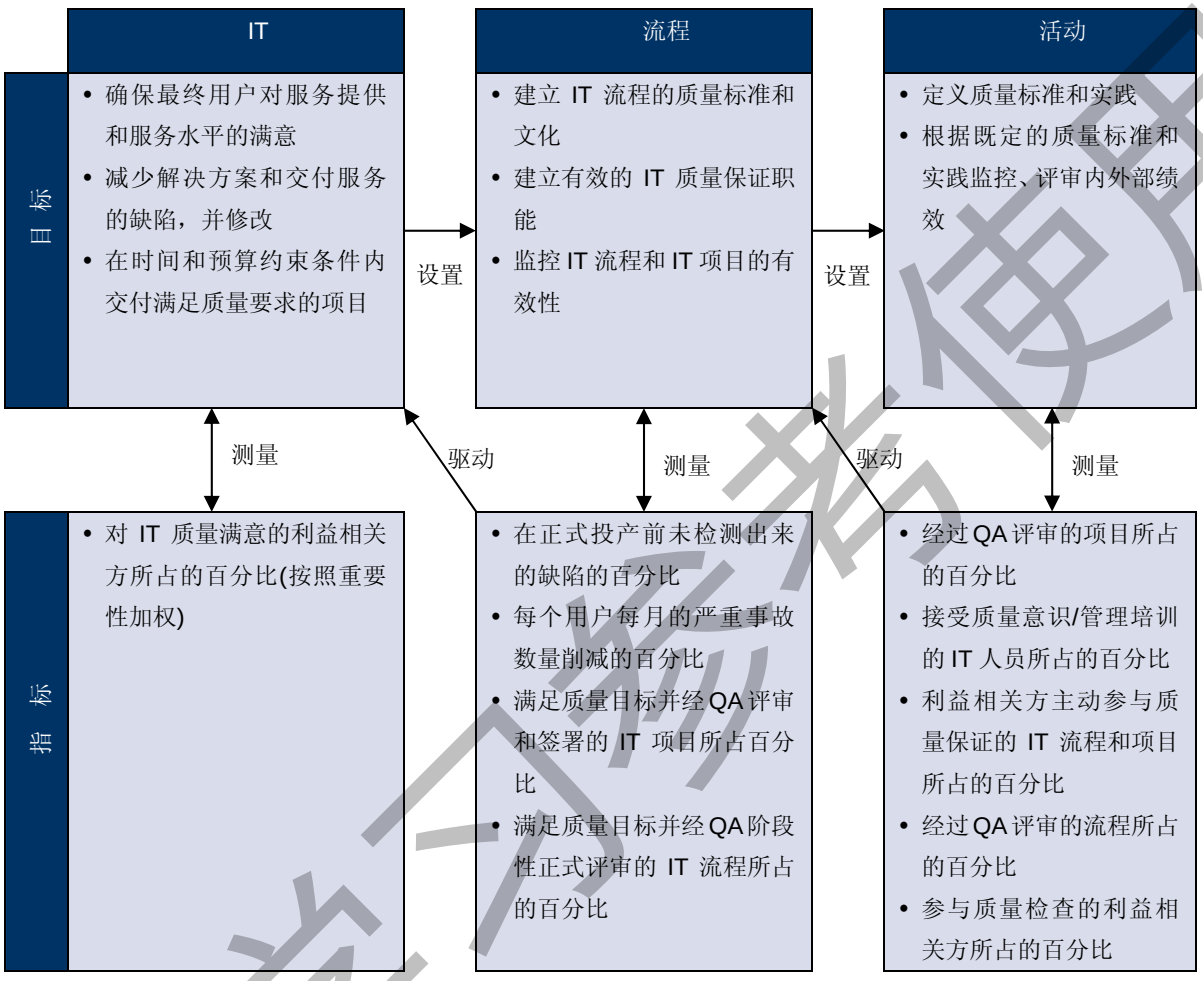
输出	到						
获取标准	AI1	AI2	AI3	AI5	DS2		
开发标准	PO10	AI1	AI2	AI3	AI7		
质量标准和衡量指标要求	ALL（所有 CobiT 控制活动）						
质量改进措施	PO4	AI6					

RACI 图　　职能

活动	首席执行官	首席财务官	业务执行经理	首席信息官	业务流程所有者	运营总监	首席架构师	开发总监	IT行政总监	项目管理官	合规、审计、风险和安全
定义 QMS	C		C	A/R	I	I	I	I	I	I	C
建立并维护 QMS	I	I	I	A/R	I	C	C	C	C	C	C
建立质量标准，并在组织内传达		I		A/R	I	C	C	C	C	C	C
建立并管理持续改进的质量计划				A/R	I	C	C	C	C	C	C
测量、监控并评审与质量目标的符合性				A/R	I	C	C	C	C	C	C

RACI 图中，**R**esponsible 代表**执行**，**A**ccountable 代表**责任**，**C**onsulted 代表**商议**，**I**nformed 代表**告知**。

3.8.4. 目标和指标



3.8.5. 成熟度模型

管理“质量管理”流程，使 IT 满足业务需求：确保持续和可测量的改进 IT 可交付服务的质量。

0 级 无级别

组织缺少 QMS 计划流程和系统开发生命周期方法论。管理层和 IT 人员未认识到质量管理程序的必要性。项目和执行情况从未进行质量评审。

1 级 初始级

管理层意识到需要一个 QMS。QMS 实施由个体驱动，管理层只有非正式的质量判断。

2 级 可重复级

确定了定义和监控在 IT 中 QMS 活动的程序。QMS 活动主要发生在 IT 项目为核心和过程为导向领域，不在整个组织范围的过程中。

3 级 定义级

定义了一个 QMS 过程，并在企业范围内得到管理层和涉及 IT 和最终用户的管理层间的沟通。关于质量的教育和培训方案已经在组织所有层面开展。在项目和 IT 组织中已经定义和共享了基本质量期望。出现了质量管理的通用工具和实践。已计划了质量满意度调查并偶尔实施。

4 级 可管理级

在所有流程内定义了 QMS，包括依赖第三方的那些流程。建立了用于质量度量的标准知识库。成本效益分析方法已被用于调整 QMS 的初始化过程。出现了相对行业和竞争者的基准。创立了针对组织的所有层面开展质量教育和培训的流程。工具和实践已被标准化，并定期应用根本原因分析。持续进行质量满意度调查。已设置结构良好的质量度量的标准程序。IT 管理层为质量度量建立了知识库。

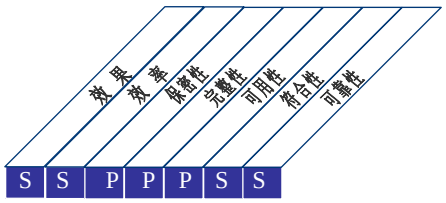
5 级 优化级

质量管理活动（QMS）被整合于所有的 IT 活动领域并充分实施。QMS 过程可根据 IT 环境的变化进行灵活调整。根据外部好的惯例增强质量度量知识库。以外部标准为基准实施测试成为日常工作内容。质量满意度测量是一个持续的过程，引导根本原因分析和改进措施。有正式的质量管理过程级别的保障。

3.9. PO9 IT 风险评估及管理

3.9.1. 流程描述

创建并维护风险管理框架，该框架用书面的方式陈述了一个通用约定的 IT 风险等级、降低战略和剩余风险，应识别、分析并评估任何意外事件对组织目标的潜在影响。应采用风险降低策略来最小化剩余风险并将其降低到可接受的水平。风险评估的结果应易于利益相关方理解，并采用财务数据来表达，以保障利益相关方能够调节风险至可接受的程度。

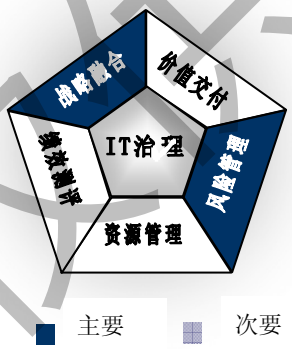


控制 IT 流程：
IT 风险评估及管理

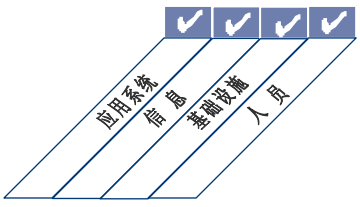
使 IT 满足业务需求：
分析并传达 IT 风险及其对业务流程和目标的潜在影响。

通过关注于：
开发风险管理框架，将其整合到业务和运行风险管理框架之中，进行风险评估、降低风险并传达剩余风险。

通过下列实现：
- 确保内外部的风险管理充分嵌入到风险管理流程之中，并经常实施。
- 履行风险评估
- 推荐并传达风险补救措施计划



通过下列衡量：
- 风险评估所覆盖的关键 IT 目标所占的百分比
- 对识别出的关键 IT 风险已制定措施计划所占的百分比
- 已被批准实施的风险管理措施计划所占的百分比



3.9.2. 控制目标

PO9.1 IT 风险管理框架

将 IT 治理、风险管理和控制框架与企业的风险管理框架整合起来。

PO9.2 建立风险背景

应建立风险评估框架应用的背景，以确保得到适当的结果。这应包括确定每一个风险评估的内外部背景、风险评估的目标以及评定风险所依据的标准。

PO9.3 事件识别

识别对企业目标或运营有潜在影响的事件（实际存在的重要威胁引发的控制弱点），包括业务、法规、法律、技术、贸易伙伴、人力资源和运营等方面。确定影响的种类并维护该信息。在风险登记簿中记录和维护相关的风险。

PO9.4 风险评估

利用定性和定量的方法，定期评估已识别风险的可能性和影响。应在投资组合的基础上，按照分类单独确定固有风险和剩余风险的可能性和影响。

PO9.5 风险响应

制定并维护一个风险响应流程，确保有效成本控制持续缓解风险的暴露。风险响应流程应确定风险战略，比如避免、缓解、分担或者接受，确定相关的职责，考虑风险容忍水平。

PO9.6 风险行动计划的维护和监控

必要时在所有层次上实行风险响应识别的优先和计划控制活动，包括成本、收益和执行的职责。获得经批准的建议措施和可接受的任何剩余风险，确保受影响的流程所有者采取对应的行动。监控计划地执行，向高管层报告执行的偏差。

PO9 IT 风险评估及管理

3.9.3. 管理指南

源自	输入
PO1	IT 战略和战术计划，IT 服务投资组合
PO10	项目风险管理计划
DS2	供方风险
DS4	意外事故测试结果
DS5	安全威胁和弱点
ME1	历史的风险趋势和事件
ME4	企业对于 IT 风险的喜好

输出	到						
风险评估	PO1	DS4	DS5	DS12	ME4		
风险报告	ME4						
IT 相关的风险管理指南	PO6						
IT 相关的风险补救措施计划	PO4	AI6					

RACI 图

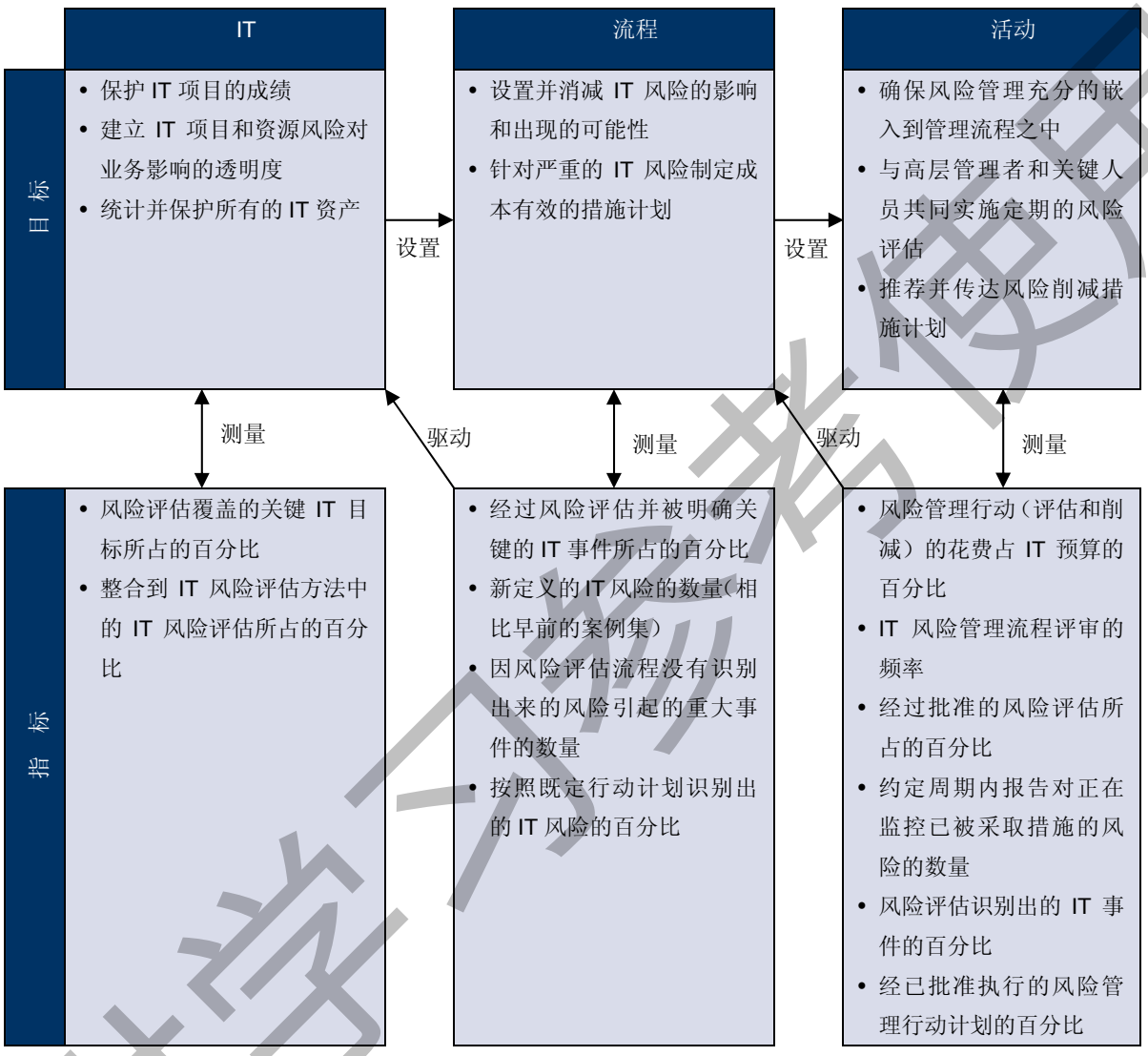
职能

活动

活动	首席执行官	首席财务官	业务执行经理	首席信息官	业务流程所有者	运营总监	首席架构师	开发总监	IT行政总监	项目管理官	合规、审计、风险和安全
确定风险管理合作（如风险评估）	A	R/A	C	C	R/A	I					I
理解相关的业务战略目标		C	C	R/A	C	C					I
理解相关的业务过程目标				C	C	R/A					I
识别内部 IT 目标，并建立风险场景					R/A		C	C	C		I
识别与目标有关的事件[（一些事件是业务为导向的（业务为 A），一些事件是 IT 导向的（IT 为 A,业务是 C））]	I			A/C	A	R	R	R	R		C
评估与事件有关的风险				A/C	A	R	R	R	R		C
评估并选择风险响应措施	I	I	A	A/C	A	R	R	R	R		C
排定控制措施的优先级并制定计划	C	C	A	A	R	R	C	C	C		C
批准并保障风险措施计划的资金		A	A		R	I	I	I	I		I
保持并监控风险措施计划	A	C	I	R	R	C	C	C	C	C	R

RACI 图中，**R**esponsible 代表**执行**，**A**ccountable 代表**责任**，**C**onsulted 代表**商议**，**I**nformed 代表**告知**。

3.9.4. 目标和指标



3.9.5. 成熟度模型

管理“IT 风险评估及管理”流程，使 IT 满足业务需求：分析并传达 IT 风险及其对业务流程和目标的潜在影响。

0 级 无级别

没有对流程和业务决议进行风险评估。组织未考虑安全漏洞和开发项目不可靠性对业务的影响。风险管理没有被认为是与获取 IT 解决方案和交付 IT 服务的一致的内容。

1 级 初始级

开始初步考虑 IT 风险。由各项目推动已经出现非正式项目风险评估。风险评估有时在项目计划中被标识，但很少分配到具体的管理者。具体的如安全性，可用性，完整性等与 IT 相关的风险也会在一个项目接一个项目的基础上被考虑到，影响日常的 IT 风险很少在管理层会议上讨论。在考虑到风险的地方，减缓风险的措施并不连续。已初步意识到 IT 风险的重要性并需要去考虑。

2 级 可重复级

存在一个正在开发的风险评估方法，按项目管理人员的判断力实施。认为风险管理通常是很高层级的事，仅应用到较大型项目中或为应对一些问题。识别出风险的地方开始实施风险缓解程序。

3 级 定义级

出现企业级风险管理策略，定义了何时和如何执行风险评估。风险管理遵循既定的书面的流程。对所有员工都有风险管理培训。遵循风险管理流程和接受培训的决意依赖于个人判断。风险评估的方法是有效的、合理的，确保识别出关键的业务风险。一旦识别出风险，缓减关键风险的过程通常就会建立。职位描述里考虑到了风险管理职责。

4 可管理级

风险评估和管理已是标准流程。异常风险管理流程会上报 IT 管理层。IT 风险管理是高管理层的职责。根据不同的项目级别进行风险评估和采取缓解风险措施，同时定期关注整个 IT 运营。管理层被建议更改那些能很大程度影响 IT 相关风险情况的业务和 IT 环境。管理层能够监控风险动态和针对愿意接受的风险水平能做出理智的决定。所有识别出的风险均有任命的所有者，高级管理层和 IT 管理层已确定了组织可接受的风险级别。IT 管理层已制定出针对评估风险和定义风险/回报率的标准测量方法。管理层在标准基础上为可操作的风险管理项目的风险再评估进行了预算。建立了风险管理数据库，部分风险管理过程开始自动化。IT 管理层考虑了风险缓解策略。

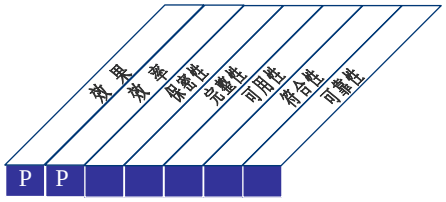
5 优化级

风险管理已发展到了结构化、全组织内实施和具有良好管理的流程级别。最佳实践在整个组织内应用。风险管理数据的捕捉，分析和报告已高度自动化。从各领域和 IT 组织中把领导者抽出来参加同级组中交换经验。风险管理真正整合到各业务和 IT 运营中，被良好接受并广范覆盖 IT 服务的用户。当实施主要的 IT 运营和制定投入决定未考虑风险管理计划时，管理层将发现并采取行动。管理层不间断的评估风险缓解策略。

3.10. PO10 项目管理

3.10.1. 流程描述

为了管理所有的 IT 项目，组织需要建立项目群方案和项目管理框架。这个框架应确保项目间的优先级和相互协调。为了确保项目风险管理的实施以及对业务提供相应价值，框架应包括：主计划、资源分配、交付品的定义、用户的核准、交付方式、质量保证、正式的测试计划以及实施后的评审。这种方法可以减少非预期成本投入和项目被取消的风险，提高业务部门和最终用户的参与和沟通，保证项目交付产品的价值和质量，并最大化它们对 IT 保障投资项目的回报。

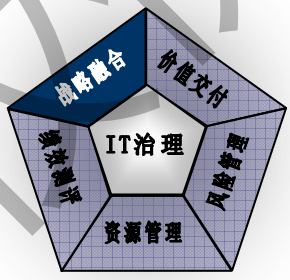


控制 IT 流程：
项目管理

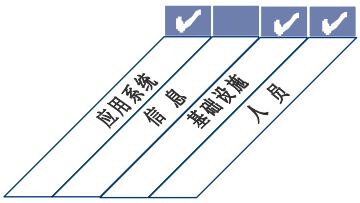
使 IT 满足业务需求：
在约定的时间、预算和质量内完成项目的交付

通过关注于：
将定义的项目群和项目管理办法应用于 IT 项目，确保利益相关方都参与到项目中，并对项目的风险和进度进行监控

通过下列实现：
- 制定并执行项目群和项目管理框架与办法
- 发行项目管理指南
- 对每一个项目，在项目文件包中要完成项目计划编制



通过下列衡量：
- 满足利益相关方期望的项目百分比（按时、按预算、满足需求—根据重要性加权）
- 接受实施后评审的项目百分比
- 遵循项目管理标准和实践的项目百分比



3.10.2. 控制目标

PO10.1 项目群管理框架

通过识别、定义、评估、优先级划分、选择、启动、管理和控制项目，来维护与 IT 驱动投资相关的项目群管理方案。确保单个项目与项目群的目标保持一致。协调多项目间的活动和相互依赖关系，管理项目群内所有项目对期望成果的贡献，解决资源需求和冲突。

PO10.2 项目管理框架

建立并维护项目管理框架，该框架定义了项目管理的范围、边界以及在每个项目中采用的方法。该框架和支持的方法应集成到项目群管理流程之中。

PO10.3 项目管理方法

根据每个项目的规模、复杂程度、规范要求为其制定相应的项目管理方法。项目管理结构包括角色，项目群发起人、项目发起人、执行委员会、项目办公室、项目经理等的职责和责任，以及行使其职责的机制（如报告和阶段评审）。确信所有 IT 项目均能得到授权人员的支持，并在整个战略项目群内实施这些项目。

PO10.4 利益相关的承诺

在整个 IT 驱动投资项目群框架内，项目立项和实施要得到受影响的各利益相关者的承诺和参与。

PO10.5 项目范围说明书

定义并记录项目的性质和范围，以使各利益相关方确认项目范围及项目在整个 IT 驱动投资项目群内与其他项目的关系，并达成共识。在项目启动之前，该范围说明书应经过项目群与项目发起人的正式批准。

PO10.6 项目启动

审批每个重要项目阶段的启动,并与所有利益相关方沟通。启动阶段的批准应基于项目群管理部门的决策。后续阶段的批准应基于前一阶段交付件的评审和接受，以及项目群下一个主要评审上经过更新的业务状况的批准。在项目阶段发生重叠时，项目群和项目发起人应建立审批点，以授权项目往下进行。

PO10.7 集成项目计划

建立一个正式的、经审批的集成项目计划（覆盖了业务和信息系统资源），以便在整个项目生命周期内指导项目实施和项目的控制。应当理解并记录一个项目群内多个项目的活动和相互依赖关系。在整个项目生命周期内要维护该集成项目计划。该项目计划及其变更应依据项目群和项目管理框架来批准。

PO10.8 项目资源

定义项目团队成员的职责、关系、职权和执行标准，并说明获取和分配有胜任能力的职员和合同员工到该项目中的基础。根据组织的获取惯例，对获取每个项目需要的产品和服务编制计划并实施管理，以便完成项目目标。

PO10.9 项目风险管理

通过系统化的流程计划、识别、分析、响应、监控和控制可能引起非期望变化的领域或事件，来消除或最小化单个项目相关的具体风险。应建立和集中记录项目管理流程和项目交付所面临的风险。

PO10.10 项目质量计划

制定一个项目质量管理计划，详细描述项目质量管理体系及其实施方案。该质量管理计划应正式评审并经所有与该项目相关的各方的认可，然后整合到集成项目计划中。

PO10.11 项目变更控制

为每个项目建立项目计划变更控制方案，以便所有项目基线（如成本、进度、范围和质量）的变更都能被适当的评审，这些变更应根据项目群和项目管理框架被核准并整合到集成项目计划中。

PO10.12 保障方法的项目计划

在项目计划编制期间，应识别要求支持新系统或升级系统合格的保障任务， 并将这些任务纳入到集成项目计划中。这些任务应提供满足既定需求的内部控制和安全特性的保障。

PO10.13 项目绩效测评、报告和监控

依据项目范围、进度、质量、成本和风险等关键标准来测量项目的绩效。识别与计划之间的偏差。评估对该项目和项目群的影响，并向关键的利益相关方报告结果。必要时，按照项目群和项目管理框架，推荐、实施和监控补救措施。

PO10.14 项目关闭

每一个项目结束时，都要求该项目的利益相关方确定该项目是否交付了预期的结果和收益。识别并传达每一个完成该项目预期结果和该项目群利益必需的重要措施，并且识别和记录这些经验教训，在将来的项目和项目群中学习使用。

3.10.3. 管理指南

源自	输入
PO1	IT 项目投资组合
PO5	更新的 IT 项目投资组合
PO7	IT 技能矩阵
PO8	开发标准
AI7	实施后评估

输出	到						
项目业绩报告	ME1						
项目风险管理计划	PO9						
项目管理指南	AI1—AI7						
详细的项目计划	PO8	AI1-AI7		DS6			
更新的 IT 项目投资组合	PO1	PO5					

RACI 图

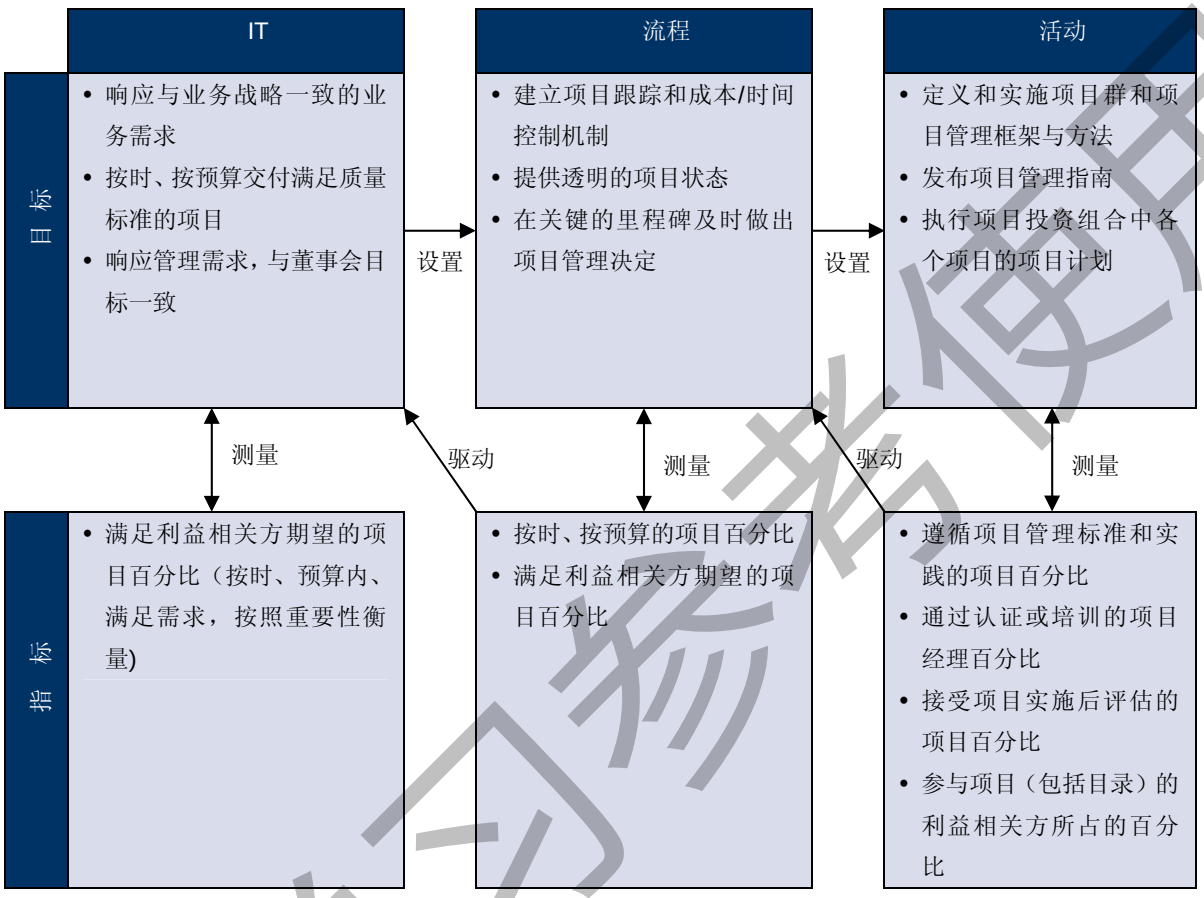
职能

活动

活动	首席执行官	首席财务官	业务执行经理	首席信息官	业务流程所有者	运营总监	首席架构师	开发总监	IT行政总监	项目管理官	合规、审计、风险和安全
定义 IT 投资的项目群/投资组合管理框架	C	C	A	R						C	C
建立并维护 IT 项目管理框架	I	I	I	A/R	I	C	C	C	C	R	C
建立和维护 IT 项目监控、测量和管理系统	I	I	I	R		C	C	C	C	A/R	C
建立项目章程、进度表、质量计划，预算、沟通和风险管理计划			C	C	C	C	C	C	C	A/R	C
确保项目利益相关方的承诺和参与	I		A	R	C						C
确保项目和项目变更的有效控制			C	C		C	C	C		A/R	C
定义和实施项目保障和评审方法			I	C				I		A/R	C

RACI 图中，**R**esponsible 代表**执行**，**A**ccountable 代表**责任**，**C**onsulted 代表**商议**，**I**nformed 代表**告知**。

3.10.4. 目标和指标



3.10.5. 成熟度模型

管理“项目管理”流程，使 IT 满足业务需求：确保在规定的时间、预算和质量内完成项目的交付。

0 级 无级别

没有采用项目管理技术，组织没有考虑因缺少项目管理和开发项目的失败对业务的影响。

1 级 初始级

由 IT 经理决定是否在 IT 部门中使用项目管理技巧和方法。项目所有者和管理者缺乏管理委员会的支持。在没有用户管理层参与或缺乏客户需求的情况下就对项目管理做关键决策。编制 IT 项目时只有极少或没有客户和用户的参与。在 IT 部门内没有清晰的组织来管理项目。没有定义项目管理的角色和职责。项目、项目进度表和里程碑定义缺乏或根本没有定义。没有跟踪项目人员的时间和费用，也没有与预算做比较。

2 级 可重复级

高级管理层意识到 IT 项目管理的必要性。组织处于逐个项目开发和使用一些技巧和方法的过程中。为 IT 项目中正式地定义了业务和技术目标。有限的利益相关方参与 IT 项目管理中。在项目管理的多数方面开发了初级的指南。项目管理指南的应用仅限于个别项目经理的判断力。

3 级 定义级

建立并发布了 IT 项目管理流程和方法。IT 项目定义了适当的业务和技术目标。业务部门和 IT 部门的高级管理者开始参与项目管理。在 IT 部门内建立了项目管理办公室，并定义了初级的角色和职责。根据确定的、最新的里程碑、进度表、预算和业绩评价来监控 IT 项目。制定了项目管理培训计划，但主要是个别职员发起的。定义了质量保证方法和系统实施后活动，但没有得到 IT 管理人员的广泛使用。项目开始以组合优化的方式进行管理。

4 级 可管理级

管理层要求正式的标准化的项目度量，在项目完成时马上进行经验总结和评审。在整个企业内而不是仅仅在 IT 部门内部对项目管理进行衡量和评估。项目管理流程的增强是正式的，与项目组成员做了沟通。IT 管理部门建立了项目管理组织架构，并以文档形式确定了其中的角色、职责和人员考核准则。制定了评估每个里程是否成功的标准。在项目开始、实施中和完成后对 IT 价值和风险进行测量和管理。项目日益强调企业整体目标而不限于 IT 部门的目标。高级管理层和各利益相关方都强烈的、积极的支持项目管理。为项目管理办公室和 IT 部门的员工提供了相关的项目管理培训计划。

5 级 优化级

强制执行一个证明有效的、全生命周期的项目和项目群管理方法，并整合到整个组织的文化中。实施了持续主动的识别和制定最佳的项目管理实践的活动。定义并实施了获得开发和运行项目的 IT 战略。从项目启动到项目后评估，有集成的项目管理办公室负责项目和项目群的管理。为支持战略启动。在组织范围内计划项目和项目群确保用户和 IT 资源的最佳使用。

4. 获取与实施（AI）

AI1 识别自动化解决方案

AI2 应用系统开发与维护

AI3 技术基础设施的获取与维护

AI4 运营知识保障

AI5 IT 资源获取

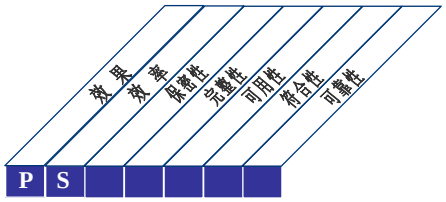
AI6 变更管理

AI7 系统测试与发布

4.1. AI1 识别自动化解决方案

4.1.1. 流程描述

为了确保有效地满足业务需求，在获取和研发新的应用系统或功能之前，需进行需求分析。分析过程包括：定义需求、考虑替代资源、评审技术与经济可行性、执行风险评估及成本效益分析，最终决定‘研发’还是‘购买’。所有这些步骤使得组织在确保达到业务目标的同时，把获取和实现这些解决方案的费用减到最小。

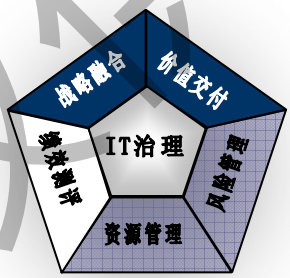


控制 IT 流程：
识别自动化解决方案

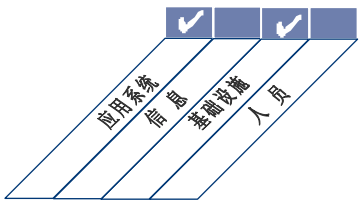
使 IT 满足业务需求：
把业务功能和控制需求转化成有效的自动化解决方案设计

通过关注于：
识别技术可行且有成本效益的解决方案

通过下列实现：
- 定义业务和技术需求
- 按照既定的开发标准进行可行性研究
- 批准（或否决）需求和可行性研究结果



通过下列衡量：
- 由于错误的可行性假设而导致未达到预期收益的项目数量
- 经业务流程的所有者批准的可行性研究的百分比
- 对所提交功能满意的用户百分比



4.1.2. 控制目标

AI1.1 定义和维护业务功能与技术需求

识别、划分优先等级、详细说明并批准业务功能及技术需求，涵盖了为达到 IT 保障投资项目预期成果所需的全部因素。

AI1.2 风险评估报告

作为组织的需求开发流程的一部分，识别、评述和分析与业务流程和解决方案设计相关的风险。

AI1.3 可行性研究和形成方案改进建议

进行可行性研究以验证实现业务需求的可能性。应由业务管理部门在 IT 部门的支持下对可行性及供选择的行动方案进行评估并推荐给业务主办人。

AI1.4 需求与可行性研究的决策和批准

验证存在一个流程，要求在预定的关键阶段，业务主办人批准和签署业务需求、技术方案和可行性研究报告。业务主办人应该做出对选择解决方案及获取方法的最终决定。

4.1.3. 管理指南

源自	输入
PO1	IT 战略规划
PO3	定期的“技术状况”更新
PO8	采购和开发标准
PO10	项目管理指南和项目详细计划
AI6	变更处理描述
DS1	服务水平协议
DS3	性能和容量计划（需求）

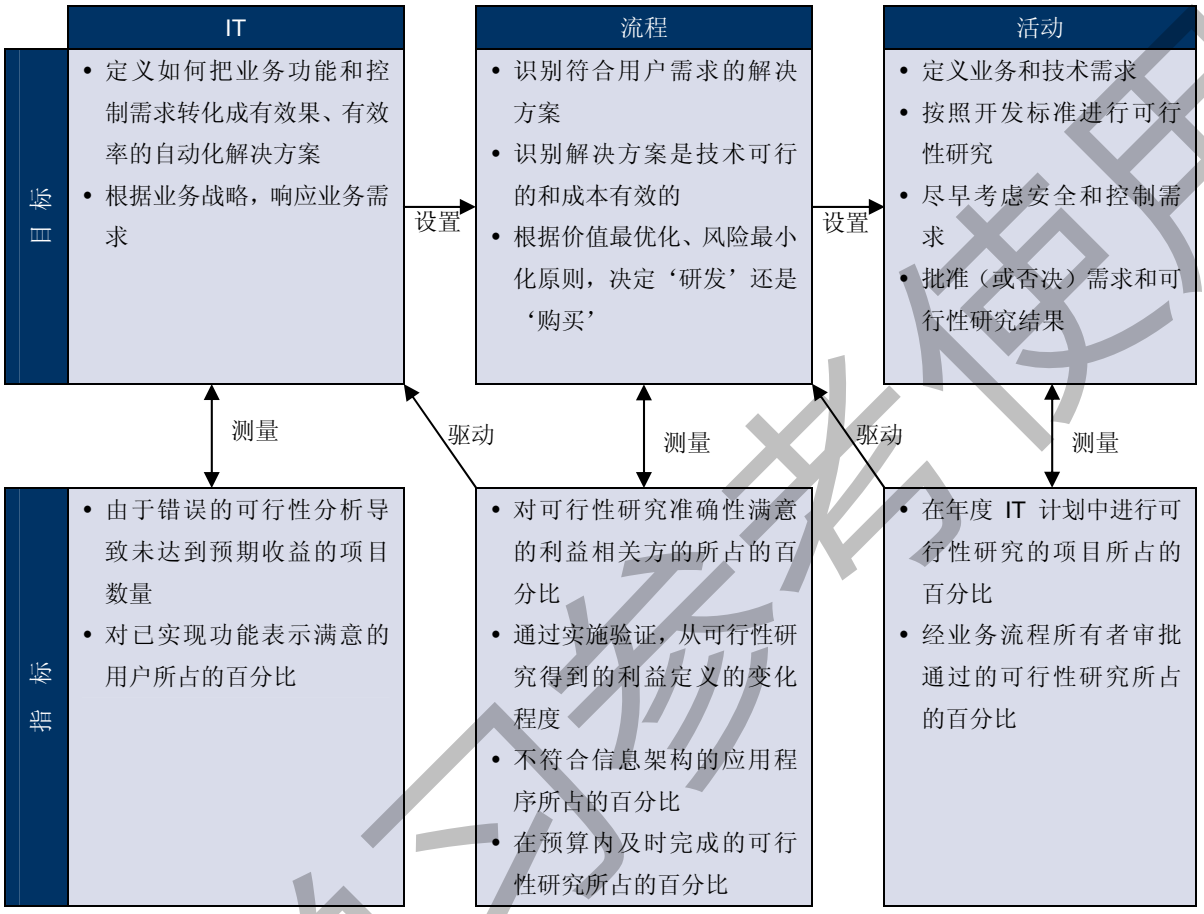
输出	到						
业务需求可行性研究	PO2	PO5	PO7	AI2	AI3	AI4	AI5

RACI 图

活动 \ 职能	首席执行官	首席财务官	业务执行经理	首席信息官	业务流程所有者	运营总监	首席架构师	开发总监	IT行政总监	项目管理官	合规、审计、风险和安全
定义业务和技术需求			C	C	R	C	R	R		A/R	I
建立完整的、通用的需求流程				C		C		C		A/R	C
识别、记录和评估业务流程相关的风险			A/R	R	R	R	C	R		R	C
对实现业务需求进行可行性研究/影响评估			A/R	R	R	C	C	C		R	C
评估所提出的解决方案在 IT 运行方面的益处		I	R	A/R	R	I	I	I		R	
评估所提出的解决方案的在业务上的益处			A/R	R		C	C	C	I	R	
形成需求审批流程			C	A		C	C	C		R	C
审批所提出的解决方案		C	A/R	R	R	C	C	C	I	R	C

RACI 图中，**R**esponsible 代表**执行**，**A**ccountable 代表**责任**，**C**onsulted 代表**商议**，**I**nformed 代表**告知**。

4.1.4. 目标和指标



4.1.5. 成熟度模型

管理“识别自动化解决方案”流程，使 IT 满足业务需求：把业务功能和控制需求转化为有效果、有效率的自动化解决方案。

0 级 无级别

组织在开发、执行或变更解决方案时不要求识别功能和操作需求，如系统、服务、基础设施、软件、硬件和数据。组织没有维持与业务有潜在关系的可用技术解决方案的意识。

1 级 初始级

意识到需求定义和 IT 解决方案识别是必需的。个别小组非正式地进行需求讨论，需求有时记录在案。基于个人对市场的有限了解或对供应商提供资料的反馈来识别解决方案。很少对可利用的技术进行结构化研究或分析。

2 级 可重复级

存在一些凭直觉的识别 IT 解决方案的方法，并随业务不同而变化。依靠内部经验和知识，采用非正规方式识别解决方案。每个项目的成功依赖一些个别关键人员的经验。项目文档及制定决策的质量变化相当大。使用非结构化的方法来定义需求和识别技术解决方案。

3 级 定义级

存在清晰和结构化的决定 IT 解决方案的方法。确定 IT 解决方案的方法需要考虑业务或用户需求、技术环境、经济可行性、风险评估以及其他因素对备选方案的评估结果。部分项目中决定 IT 解决方案的流程基于以下因素：个别项目成员所做的决定、管理部门承诺的时间长短、最初需求的大小和优先级别。使用结构化的方法来定义需求和识别 IT 解决方案。

4 级 可管理级

识别和评估 IT 解决方案的既定方法论存在并将之应用于大多数项目。项目文档质量良好，且每一个阶段都得到适当的审批。需求符合预定的结构并具有良好的关联关系。考虑了备选方案，方案中包括有成本和收益分析。所采用的方法论是清晰、明确、易于理解和可度量的。对 IT 解决方案进行筛选和评估时，IT 部门和业务部门之间有明确的协调分工。

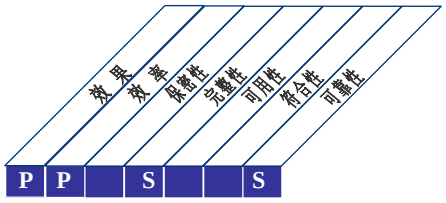
5 级 优化级

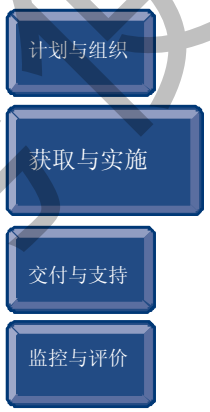
识别和评估 IT 解决方案的方法论得到持续改进。获取和实施的方法论根据项目规模的大小灵活变化，并得到包含各类 IT 解决方案参考资料的内外部知识库的支持。方法论以既定的结构产生可行性研究和需求分析文档，并能有效维护。识别新的机遇，能够利用技术来获取竞争优势，对业务流程再造有所触动，提高整体效率。如果 IT 解决方案在没有考虑技术或业务功能需求供选方案的情况下被批准，管理部门能够及时发现并采取行动。

4.2. AI2 应用系统开发及维护

4.2.1. 流程描述

应用系统必须按照业务需求予以实现，实现过程涵盖了应用系统设计、适当考虑应用系统的控制及安全要求、按照标准进行实际开发和配置。这使得组织能以恰当的自动化应用系统充分支持业务运行。



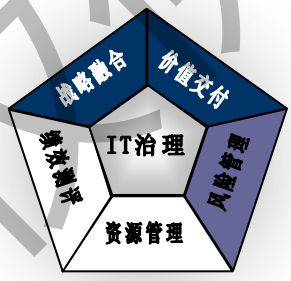


控制 IT 流程：
应用软件开发及维护

使 IT 满足业务需求：
及时并以合理成本提供满足业务需求的应用软件

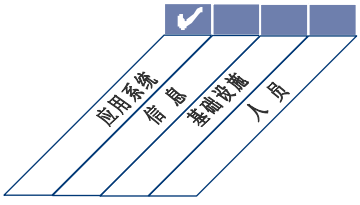
通过关注于：
确保是一个及时和成本合理的开发流程

通过下列实现：
- 转化业务需求成为设计说明
- 对于所有的变更坚持遵循开发标准
- 开发、运行和测试活动分离



主要　次要

通过下列衡量：
- 每一个应用系统中导致明显故障时间产品的问题数量
- 对所提交功能满意的用户百分比



4.2.2. 控制目标

AI2.1 高层设计

把业务需求转化成软件开发的高层设计说明书需要考虑组织的技术方向及信息架构。设计说明书应获得管理层批准以确保高层设计体现业务需求。开发或维护过程中出现重大技术或逻辑偏差时应进行再评估。

AI2.2 详细设计

准备详细设计和技术软件应用需求。定义需求可接受的标准。确保拥有高层设计符合的业务需求。在开发过程中时，出现重大技术或逻辑偏差时应进行再评估。

AI2.3 应用控制和可审计性

在适当的位置，利用自动控制手段来执行业务控制，例如处理是准确的、完整的、及时的、被授权的和可审计的。

AI2.4 应用安全和可用性

落实应用安全和可用性的需求，响应已识别的风险，协调数据的分类、企业信息架构、企业信息安全架构和风险容忍度。

AI2.5 外购应用软件的配置和实施

配置和执行已获取软件以满足业务目标。

AI2.6 现有系统的重大升级

对于当前系统出现设计和功能重大变化事件发生的情况，需要执行一个类似于新系统开发的流程。

AI2.7 应用软件开发

确保在开发自动化系统功能时，能遵循设计说明书、开发及文档标准、质量要求和认证标准。对于第三方开发的应用软件，确保已识别和落实所有法律和合同方面的问题。

AI2.8 软件质量保证

建立、提供资源和执行软件质量保证计划以获得需求所定义的和企业质量策略、程序所要求的软件质量。

AI2.9 应用系统需求管理

跟踪并记录设计、开发及实施过程中每一个需求（包括所有被拒绝的需求）的状态，按照既定的变更管理流程审批需求变更。

AI2.10 应用系统维护

对应用软件的维护建立一个策略和计划。

4.2.3. 管理指南

源自	输入
PO2	数据字典；数据分类表；优化的业务系统计划
PO3	定义技术规定的升级
PO5	成本收益报告
PO8	获取和开发标准
PO10	项目管理指南；详细项目计划
AI1	业务需求的可行性研究
AI6	变更流程描述

输出	到						
应用安全控制说明书	DS5						
应用和软件包的知识开发标准	AI4						
采购决策	AI5						
初始计划的服务水平协议	DS1						
可行性、连续性和可恢复性说明书	DS3	DS4					

RACI 图

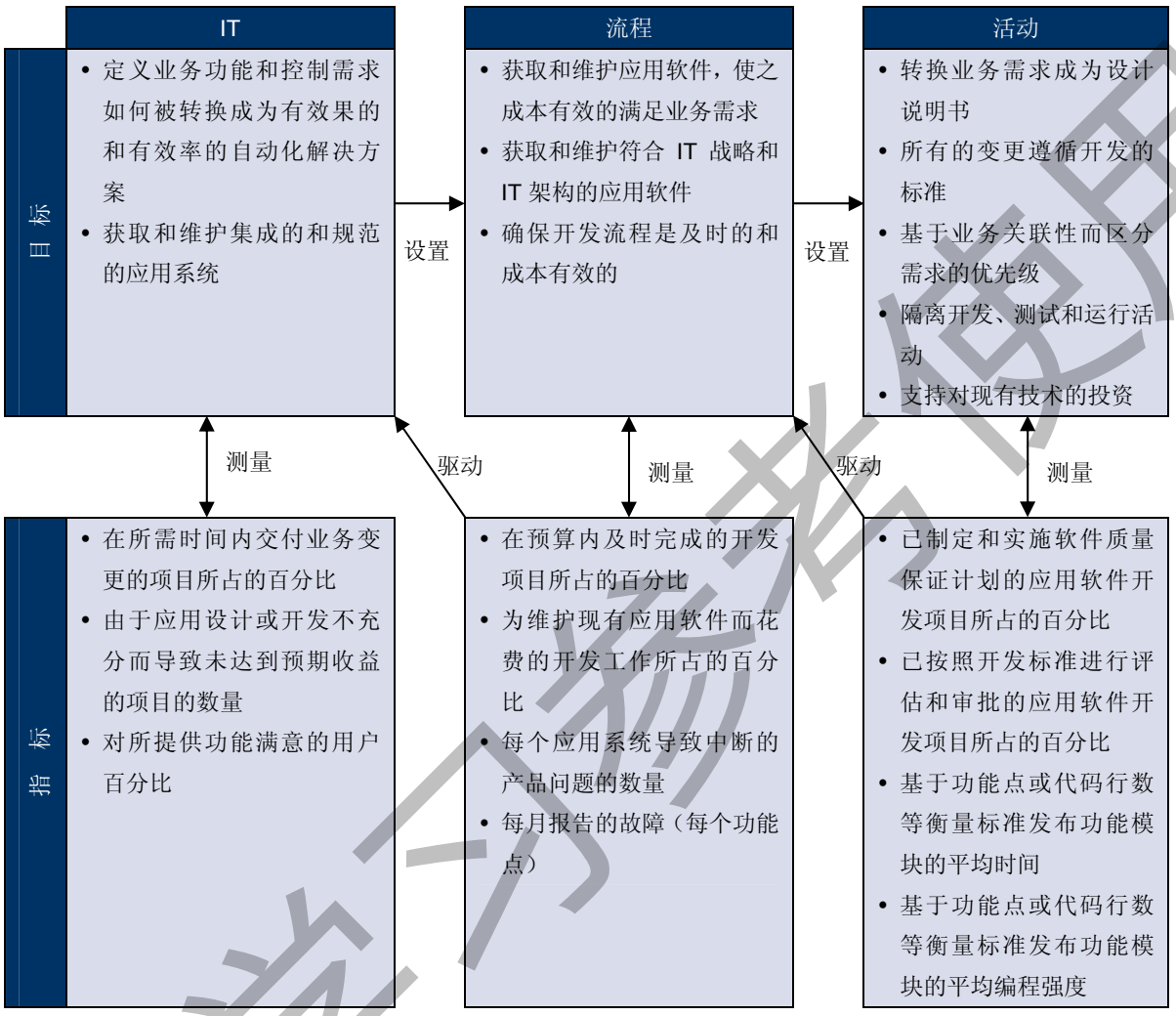
职能

活动

活动	首席执行官	首席财务官	业务执行经理	首席信息官	业务流程所有者	运营总监	首席架构师	开发总监	IT行政总监	项目管理官	合规、审计、风险和安全
转化业务需求成为高层设计说明书				C		C	A/R		R	C	
准备详细设计和技术软件应用系统的需求			I	C	C	C	A/R		R	C	
在设计中描述应用控制				R	C		A/R		R	R	
客户化和实施所获取的自动化功能				C	C		A/R		R	C	
建立正式方法和流程来管理应用开发流程			C		C	C	A	C	R	C	
建立项目的软件质量保证计划				I		C	R		A/R	C	
记录和管理应用系统需求							R		A/R		
建立软件应用系统的维护计划			C		C		A/R		C		

RACI 图中，**R**esponsible 代表**执行**，**A**ccountable 代表**责任**，**C**onsulted 代表**商议**，**I**nformed 代表**告知**。

4.2.4. 目标和指标



4.2.5. 成熟度模型

管理“应用软件开发及维护”流程，使 IT 满足业务需求，必须使可用的应用系统符合时间要求、成本合理，与业务需求保持协调一致。

0 级 无级别

没有为设计和应用说明设置流程。有代表性的情况是，应用被获取是基于卖方的驱动、品牌的公认或者 IT 人员对某些特殊产品的熟悉，而很少甚至没有考虑实际的需求。

1 级 初始级

意识到应用系统开发和维护流程是必需的，开发和维护应用系统的方法随项目的不同而不同。对于特殊的业务需求，有可能独立地获得一些个别的解决方案，但导致维护和支持缺乏效率。

2 级 可重复级

基于 IT 部门的经验，建立了一些不同但类似的流程来处理应用系统的开发及维护。应用系统的成功在很大程度上依靠于 IT 部门人员的技巧和经验。组织中内部知识的流失通常会给维护工作带来问题并遭受损失。在设计或开发过程中，很少考虑应用软件的安全性和可用性。

3 级 定义级

存在一个清晰、明确和被广泛理解的应用系统开发和维护流程，并且这个流程符合 IT 和业务战略。在不同的应用系统开发和维护项目中，尝试使用文档化的流程，但很难应用于所有的项目，因此既定的步骤有可能被绕过。维护活动得到计划和统筹安排。

4 级 可管理级

存在一个正式的和易于理解的方法论，包括设计和说明的流程、获取的标准、测试的过程和文档化的要求。存在文档化的批准认可机制，以确保所有的步骤被遵循，例外的处理被授权。实践和流程不断得到改进，以适应组织的要求，同时也适用于大部分的应用系统需求，并被所有成员采用。

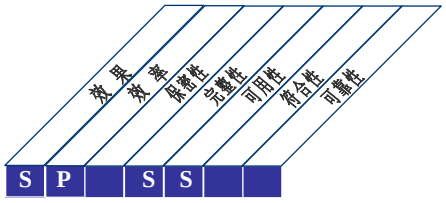
5 级 优化级

应用软件的获取和维护活动符合既定的流程要求。所用方法论是基于组件的，以预定的和标准的应用系统来满足业务需求，并且适用于整个组织的范围。获取和维护的方法是相当先进的，能够快速进行部署，对业务需求的变更能够做出快速、灵活的反应；获取及实施的方法服从于持续改进的需要，并且有内外部知识库（包含相关资料和最佳实践）的支持。按照既定的结构生成文档，使应用软件及其维护更加有效。

4.3. AI3 技术基础设施的获取和维护

4.3.1. 流程描述

组织应当建立一个获取、实施和升级技术基础设施的流程，这要求组织应当针对基础设施的获取、维护及保护制定一个计划方案，该方案要与已经批准的技术战略和开发及测试环境的有关规定相一致。这确保了为业务应用系统提供持续的技术支持。



控制 IT 流程：
获取并维护 IT 基础设施

使 IT 满足业务需求：
获得并维持一个完整的、标准的 IT 基础设施

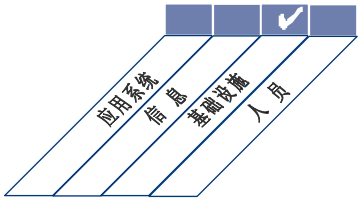
通过关注于：
为业务应用系统提供与既定 IT 架构和技术标准相一致的合适平台

通过下列实现：

- 制定一个和技术基础设施计划相符的技术获取计划
- 制定技术基础设施维护计划
- 实施内部控制、安全和审计措施

通过下列衡量：

- 与既定的 IT 架构和技术标准不相符的平台所占的比例
- 过时（或即将过时）的基础设施所支持的关键业务过程的数量
- 已经不再受支持（或即将不受支持）的基础设施组件的数量



■ 主要 ▦ 次要

4.3.2. 控制目标

AI3.1 技术基础设施的获取计划

制定一个获得、实施和维护技术基础设施的计划，满足既定的业务功能及技术需求，并符合组织的技术发展方向。

AI3.2 基础设施资源的保护和可用性

在硬件和基础设施软件的配置、集成和维护过程中，执行内部控制、安全和审计措施以保护资源并确保其可用性和完整性。明确定义使用敏感基础设施组件的职责，让开发和集成基础设施组件的人员理解这些职责，并且监控和评估他们的使用情况。

AI3.3 基础设施维护

制定一个基础设施维护的策略和计划，并确保按照组织的变更管理程序控制基础设施的变更。内容包括：定期审核业务需求、补丁管理及升级战略、风险、脆弱性评估及安全需求。

AI3.4 可行性验证环境

建立一个开发和验证环境以支持对基础设施组件的可行性（效果、效率）及集成测试。

4.3.3. 管理指南

源自	输入
PO3	技术基础设施计划，技术标准和有利的环境；定期的“技术状况”更新
PO8	采购和开发标准
PO10	项目管理指南和项目详细计划
AI1	业务需求可行性研究
AI6	变更处理描述
DS3	性能和容量计划（需求）

输出	到						
采购决议	AI5						
用于测试/安装的配置系统	AI7						
物理环境需求	DS12						
技术标准更新	PO3						
系统监控要求	DS3						
基础设施知识	AI4						
初步计划的营运水平协议	DS1						

RACI 图

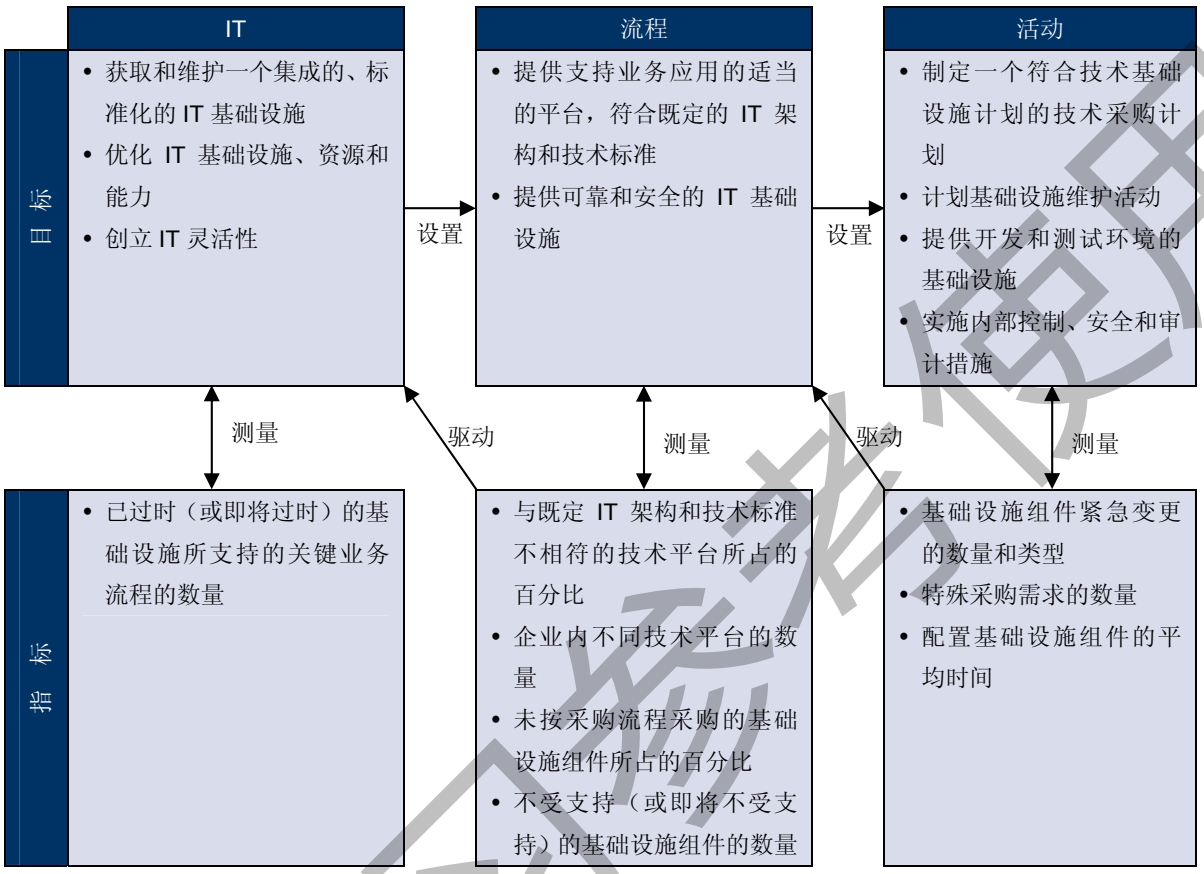
职能

活动

活动	首席执行官	首席财务官	业务执行经理	首席信息官	业务流程所有者	运营总监	首席架构师	开发总监	IT行政总监	项目管理官	合规、审计、风险和安全
制定采购程序及流程		C		A		C	C	C	R		I
与供应商讨论经批准的基础设施需求		C/I		A	I	R	C	C	R		I
制定基础设施维护策略及规划				A		R	R	R	C		
配置基础设施组件				A		R	C				I

RACI 图中，**R**esponsible 代表**执行**，**A**ccountable 代表**责任**，**C**onsulted 代表**商议**，**I**nformed 代表**告知**。

4.3.4. 目标和指标



4.3.5. 成熟度模型

管理“技术基础设施获取与维护”流程，使 IT 满足业务需求：获取与维护一个完整的、标准的 IT 基础设施。

0 级 无级别

没有把管理技术基础设施看作一个十分重要的主题予以落实。

1 级 初始级

缺乏全面规划，对每一个新应用系统都需要对基础设施做改动。虽然意识到 IT 基础设施很重要，但缺少全面一致的方法。维护活动仅仅是为了响应短期需求，生产环境同时也是测试环境。

2 级 可重复级

在策略层面上对获取和维护 IT 基础设施有一个一致的方法，但未基于任何既定的战略，也没有考虑必须支持的业务应用系统的需求。已经理解 IT 基础设施是重要的，并且有一些正式的活动所支持。部分维护工作已经事先安排，但缺乏全面的统筹计划。部分情况下已经建立了单独的测试环境。

3 级 定义级

已经建立一个清晰、确定并被广泛理解的 IT 基础设施的获取和维护流程，该流程能够支持关键业务应用系统的需求，并且符合企业的 IT 和业务战略，但是还没有得到一致的贯彻。维护工作已经列入计划并被事先安排和协调。测试环境与生产环境已经分离。

4 级 可管理级

技术基础设施的获取与维护过程在大多数情况下运行良好，能够得到一致贯彻并且关注可复用性。IT 基础设施能够充分支持业务应用系统。该流程的组织合理、运行主动。为达到可测量性、适应性、整体性的预期水平所需的成本与研制周期已经得到部分优化。

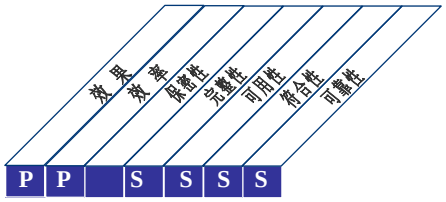
5 级 优化级

技术基础设施的获取与维护过程运行主动，并且与关键业务应用系统和技术架构紧密结合。遵循关于采用技术解决方案的良好实践，同时也考虑了最新的平台发展与管理工具。通过合理化、标准化基础设施组件和利用自动化降低了费用。高水平对技术的认知理解能够选择最优方式主动提高性能，包括考虑配件的外购。IT 基础设施被看作是支撑 IT 应用系统的关键能动力。

4.4. AI4 运营知识保障

4.4.1. 流程描述

使有关新系统的知识具备可用性。这个流程要求为用户和 IT 部分人员编制相关文件和手册，并提供培训，以确保应用系统和基础设施的正确使用和操作。



控制 IT 流程：

运营知识保障

使 IT 满足业务需求：

确保最终用户对服务内容和服务水平满意，把应用程序及技术解决方案与业务流程紧密结合

通过关注于：

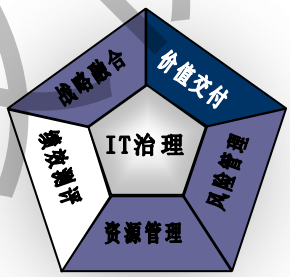
提供有效的用户及操作手册和培训资料，为成功的系统操作转移必要的知识

通过下列实现：

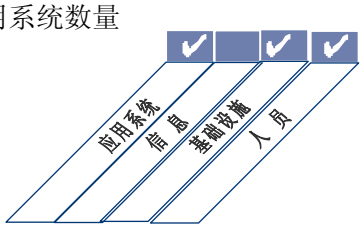
- 建立并完成知识转移文档
- 对用户、业务管理人员、运营操作和技术人员提供培训和沟通
- 编制培训资料

通过下列衡量：

- IT 流程与业务流程实现无缝整合的应用系统的数量
- 对应用系统培训和支持资料表示满意的业务所有者所占百分比
- 得到足够用户及操作培训的应用系统数量



主要　次要



4.4.2. 控制目标

AI4.1 运营知识保障方案

制订运营知识保障方案，以识别和记录所有技术、运营和使用方面的知识，确保运营、使用和维护人员能够行使职责。

AI4.2 向业务管理层转移知识

向业务管理层转移知识，以确保他们掌握应用系统和数据的所有权，并对服务的交付与质量、内部控制、应用系统的管理行使职责。

AI4.3 向最终用户转移知识

向最终用户转移知识，以确保他们在支持业务流程的过程中能够有效地和有效率地使用应用系统。

AI4.4 向运营维护人员转移知识

向运营维护人员转移知识，以他们能够根据服务水平要求，有效地且有效率地交付、支持和维护应用系统及相关的基础设施。

4.4.3. 管理指南

源自	输入
PO10	项目管理指南和项目详细计划
AI1	业务需求可行性研究
AI2	应用和软件包知识
AI3	基础设施知识
AI7	已知和可以接受的缺陷
DS7	必要的文档更新

输出	到					
用户、运营、支持、技术和管理手册	AI7	DS4	DS8	DS9	DS11	DS13
解决方案实施的知识转移要求	DS7					
培训教材	DS7					

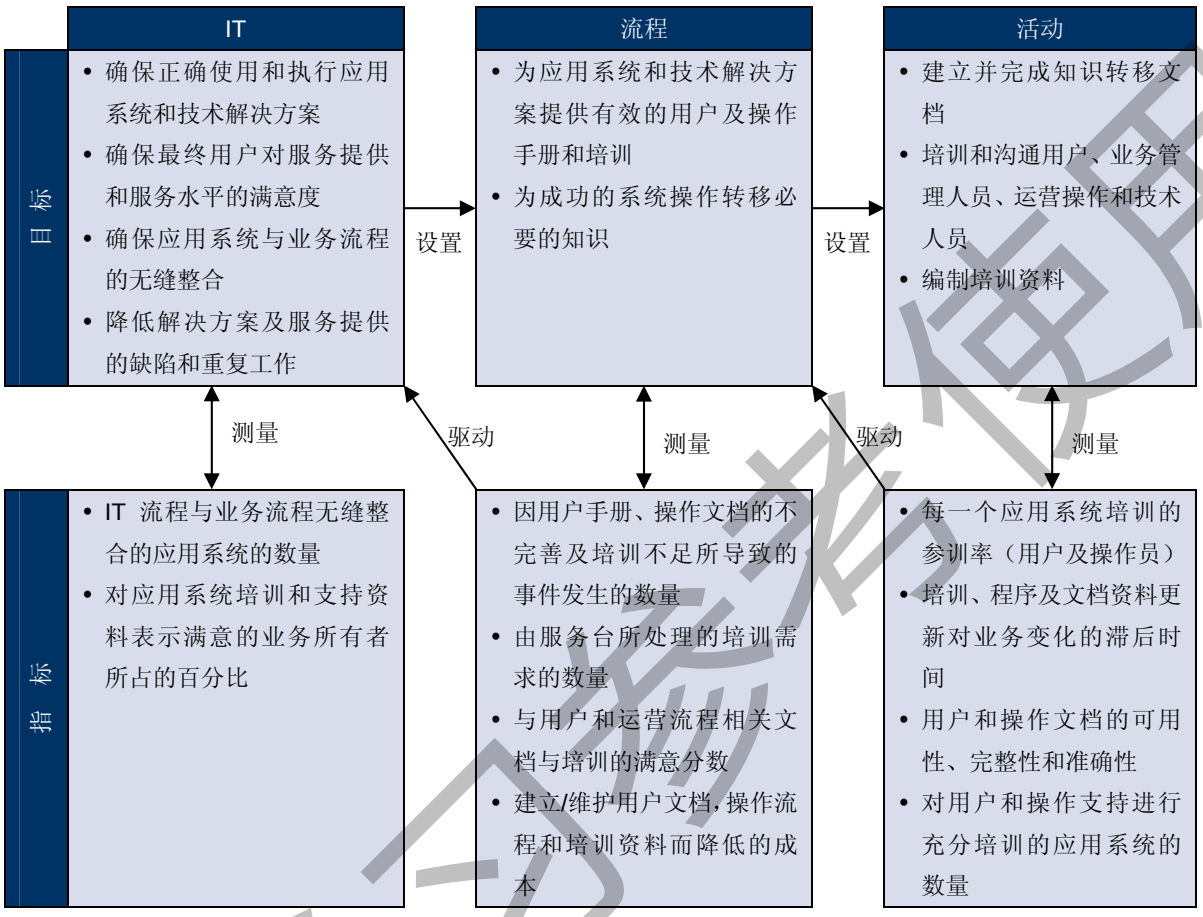
RACI 图　　职能

活动

活动	首席执行官	首席财务官	业务执行经理	首席信息官	业务流程所有者	运营总监	首席架构师	开发总监	IT行政总监	项目管理官	合规、审计、风险和安全	开发团队	培训部门
建立一个策略,使解决方案可操作				A	A	R		R			I	R	C
建立一个知识转移方法论				C	A							C	R
建立最终用户程序手册					A/R			R			C	C	
为运营支持维护人员建立技术支持文档						A/R		C			C		
建立和实施培训					A	A		R					R
评估培训结果并加强文档管理					A	A						R	R

RACI 图中，**R**esponsible 代表**执行**，**A**ccountable 代表**责任**，**C**onsulted 代表**商议**，**I**nformed 代表**告知**。

4.4.4. 目标和指标



4.4.5. 成熟度模型

管理“运营知识保障”流程，使 IT 满足业务需求：确保最终用户对服务提供和服务水平的满意度以及应用系统、技术解决方案与业务流程的无缝整合。

0 级 无级别

组织缺少编制用户文档、操作手册和培训资料的流程，仅有外购系统的相关资料。

1 级 初始级

意识到流程文档是必需的，但是有时候编制文档，只在有限范围内分享，且内容不一致，大多数文档及操作程序编制不及时。培训资料往往是一次性的且质量好坏不一。没有针对不同系统及业务部门进行操作程序整合。在培训程序设计时，没有从业务单位收集相关的要求。

2 级 可重复级

使用大致相同的方法编制文档和操作程序，但不是基于结构化的方法或框架。没有采用统一的方法建立用户及操作程序。由个人或项目组编制培训资料，其质量取决于编制人员。对用户支持的质量和操作程序由差转为好，但在整个组织内缺乏整合和一致性。针对业务和用户能够提供或推进培训项目，但没有全面的培训展示和交付的计划。

3 级 定义级

有一个明确界定的、可接受的并被广泛理解的用户文档、操作手册和培训资料的编制框架。操作程序在一个正式的知识库中保存和维护，任何需要的人都可以访问；能够根据反馈情况对文档及操作程序进行更正。当发生事故时，操作程序是可以离线访问和维护的。对于变更项目，存在一个流程以确保相关的操作程序得到更新，同时相关的培训资料得到明确的交付。尽管存在既定的方法，但由于没有对是否强制遵循标准进行控制，导致实际内容的差异。用户非正式地参与到流程中。逐渐使用自动化手段编制和分发操作程序。已制订了业务及用户的培训计划和时间安排。

4 级 可管理级

存在既定的培训资料及操作程序维护框架，并得到 IT 管理层支持；所采用的方法涉及所有系统和业务部门，因而可以从业务角度来考虑流程；同时，培训资料及操作程序是集成在一起并相互关联的。存在确保遵循相关标准的控制，同时针对全部流程来编制和维护操作程序。作为持续改进流程的一部分，能够收集和评估业务及用户对文档和培训的反馈。文档及培训资料通常具有很好的预见性、可靠性和可用性。建立自动化程序将之日益集成到应用系统开发过程中，并促进两者的结合，方便用户访问。根据业务需要进行业务和用户的培训。IT 管理层正为提供文档及培训资料和培训程序确定度量标准。

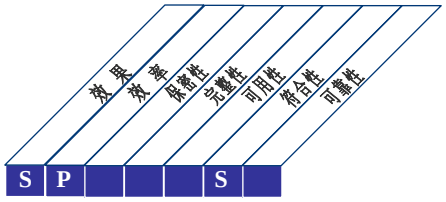
5 级 优化级

能够通过采用新的工具或方法来持续改进用户及操作文档的编制流程。操作程序及培训资料作为可以持续更新的知识库，能够通过采用最新的知识管理、流程图及分享技术等电子化手段进行维护，并使其易于访问。文档及培训资料能够根据组织结构、操作模式以及软件的变更而得到更新。文档、培训资料的编制和培训项目的实施完全与业务及业务流程定义结合，能够满足整个组织的需求而不仅仅是面向 IT 流程。

4.5. AI5 IT 资源获取

4.5.1. 流程描述

必须取得包括人员、硬件、软件和服务在内的 IT 资源，这需要对获取程序、供应商的选择、签订合同以及获取过程本身进行明确规定并切实执行。这确保组织能以及时、有成本效益的方式获取所需的全部 IT 资源。



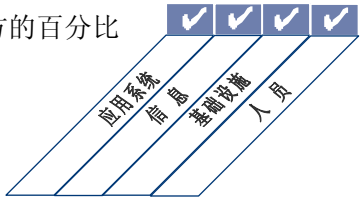
控制 IT 流程：
IT 资源获取

使 IT 满足业务需求：
改善 IT 的成本效益性和对业务收益的贡献

通过关注于：
获知并维持以下 IT 工作能力：交付策略、完整及标准的 IT 基础设施、降低 IT 获取风险

通过下列实现：
- 获得法律专家及合同专家的建议
- 规定获取程序和标准
- 按照即定程序获得所需的硬件、软件和服务

通过下列衡量：
- 获取合同引起争议的次数
- 降低的采购成本
- 对供应商满意的关键利益相关方的百分比



主要　次要

4.5.2. 控制目标

AI5.1 采购控制

制定和遵守一系列与组织的集中采购流程及策略相一致的程序及标准，以获取业务所需的 IT 相关基础设施、工具、硬件、软件和服务。

AI5.2 供应商合同管理

制定全部供应商合同的签订、修改和终止程序，程序中至少应涉及以下内容：法律、财务、组织、文档、性能、安全、知识产权、终止责任及义务（包括处罚条款）。所有合同及其变更应通过法律顾问的审查。

AI5.3 选择供应商

采取公平、正规的方式选择供应商，确保选出基于指定需求的最佳可行方案，需求应当在潜在的供应商中进行优选。

AI5.4 IT 资源采购

确保组织利益在所有获取合同中受到保护，在软件、开发资源、基础设施和服务的合同条款中，应明确相关各方的权利和义务。

4.5.3. 管理指南

源自	输入
PO1	IT 采购战略
PO8	采购标准
PO10	项目管理指南和项目详细计划
AI1	业务需求可行性研究
AI2-3	采购决议
DS2	供应商目录

输出	到						
第三方关系管理要求、合同管理	DS2						
已采购细目	AI7						
合同安排	DS2						

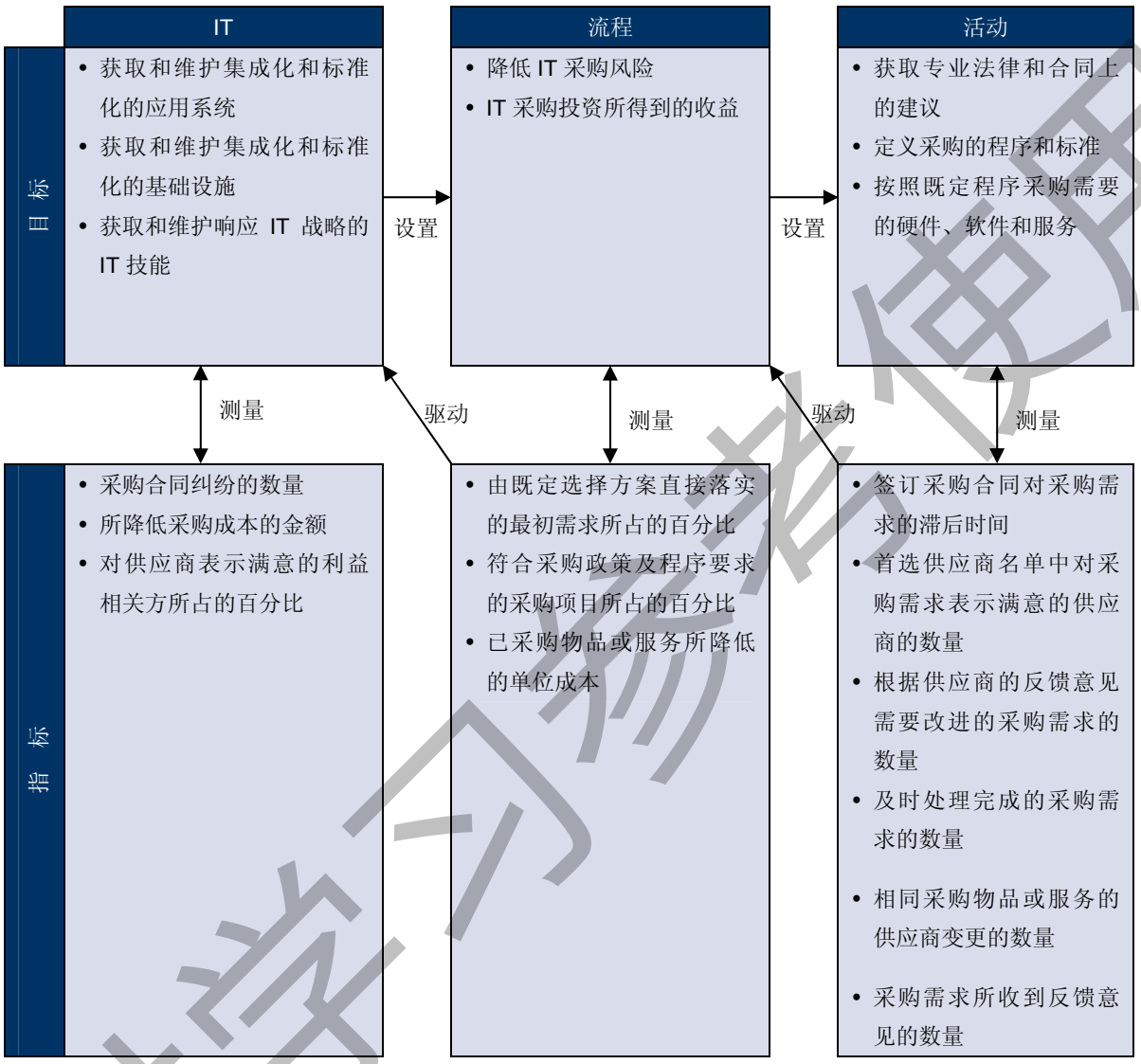
RACI 图　　职能

活动

	首席执行官	首席财务官	业务执行经理	首席信息官	业务流程所有者	运营总监	首席架构师	开发总监	IT行政总监	项目管理官	合规、审计、风险和安全
制定符合组织集中采购政策的采购程序	I	C		A		I	I	I	R		C
建立并维护供应商信息库									A/R		
通过正规的流程评估和选择供应商	C	C		A		R		R	R	R	C
签订保护组织利益的合同	R	C		A		R		R	R		C
按照既定的流程执行采购任务				A		R		R	R		C

RACI 图中，**R**esponsible 代表**执行**，**A**ccountable 代表**责任**，**C**onsulted 代表**商议**，**I**nformed 代表**告知**。

4.5.4. 目标和指标



4.5.5. 成熟度模型

管理“IT 资源获取”流程，使 IT 满足业务需求：改善 IT 的成本效益性和对业务收益的贡献。

0 级 无级别

没有定义适当的 IT 资源采购流程。组织还未意识到要确保能够及时、有成本效益地获取全部 IT 资源需要制定明确的采购政策及流程。

1 级 初始级

组织已意识到需要制定书面政策和程序把 IT 采购纳入组织的集中采购流程中。IT 资源采购合同由项目经理或其他职员根据个人判断来签订和管理，而不是依靠正规的流程和政策；在企业采购及合同管理流程和 IT 职能之间仅存在极少关联，采购合同仅作为项目总结的一部分，缺乏持续管理方式。

2 级 可重复级

组织已经意识到需要制定 IT 采购的基本政策与程序，部分政策与程序已经与集中采购流程进行了整合。采购流程主要应用于大型且引人注目的项目中，IT 采购的职责、责任以及合同管理还依赖于管理人员的经验。意识到供应商的管理与合作关系管理的重要性，但其落实工作仍基于个人能动性。合同流程主要应用于大型或引人注目的项目。

3 级 定义级

管理层制定了在集中采购流程指导下的 IT 采购政策和程序，大部分 IT 采购已经纳入集中采购程序。制定了 IT 资源的采购标准，对 IT 资源供应商的管理已从单纯的合同管理统一到企业项目管理机制中。IT 管理部门通过行使 IT 职能来沟通适度采购及合同管理的需求。

4 级 可管理级

IT 采购已完全纳入企业集中采购程序，IT 资源采购标准已应用在所有采购中。IT 采购合同及采购管理的衡量指标已经与相关业务事项建立关联。报告 IT 采购活动来支持业务目标的可用性，管理层通常能知道未按政策和程序执行的 IT 采购事项。正在建立与供应商的战略伙伴关系。IT 管理层通过检查执行效果的方式要求对所有采购事项应用既定的采购及合同管理流程。

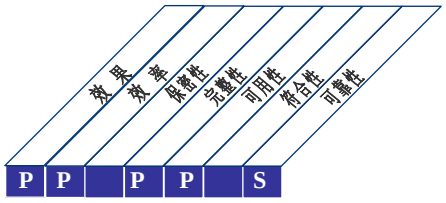
5 级 优化级

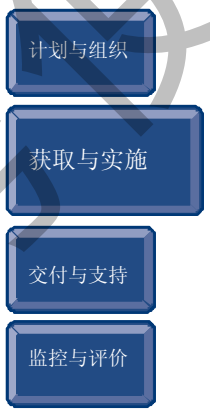
管理层通过 IT 采购流程建立健全资源采购，要求所有 IT 采购遵从政策及程序。采用与相关业务事项相关联的指标来衡量 IT 采购合同及采购管理。已经与大多数供应商及合作商建立了良好的合作关系并进行衡量和监督，合作关系已经提到战略层面进行管理。IT 资源采购标准、政策和程序已经纳入战略管理和流程评价。IT 管理部门通过行使 IT 职能来沟通适当采购及合同管理的战略重要性。

4.6. AI6 变更管理

4.6.1. 流程描述

所有变更（包括紧急维护和补丁，以及与生产环境相关的基础设施和应用系统的变更）均以正式的、可控制的方式进行管理。变更实施前（包括对程序、流程、系统和服务参数变更）均获记录、评估和授权；变更实施后，按既定的计划审核变更的结果。确保变更对生产环境的稳定性及完整性造成负面影响的风险降至最低。





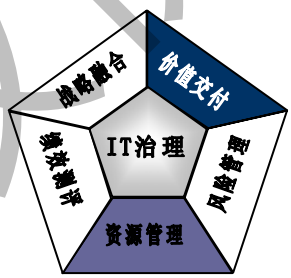
控制 IT 流程：
变更管理

使 IT 满足业务需求：
服务于业务需求，与业务策略保持一致，同时减少解决方案及服务交付的缺陷和返工的机率。

通过关注于：
控制所有变更的影响评估、授权和执行，包括 IT 基础架构、应用和技术解决方案的变更，最小化因变更请求规格说明书的不完整所引发的错误，中止未经授权的变更执行。

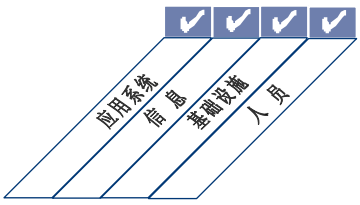
通过下列实现：

- 确定和沟通包括紧急变更在内的变更流程
- 变更评估、优先级排序和授权
- 变更状态跟踪和报告



通过下列衡量：

- 因不精确的变更请求规格说明书或不完整的影响评估引起的业务中断或数据错误的数量
- 因不充分的变更请求规格说明书引发的应用和基础设施返工重做的数量
- 遵循正式变更控制流程处理变更的百分比



4.6.2. 控制目标

AI6.1 变更标准和流程

建立正式的变更管理流程，以标准化的方式处理所有的变更请求（包括维护和补丁），包括应用系统、程序、流程、系统及服务参数和基础平台的变更。

AI6.2 影响评估、优先级和授权

以结构化的方式评估所有的变更请求，确定变更对运营系统及其功能的影响。确保对变更进行分类、优先级划分和授权。

AI6.3 紧急变更

建立一个非常规的变更流程，用于处理紧急变更的提出、测试、记录、评估和授权。

AI6.4 变更状态跟踪和报告

建立一个跟踪和报告系统以记录未获批准的变更和完成的变更，并与已获批准和正在执行中的变更进行信息沟通。确保获准的变更按计划执行。

AI6.4 变更的结束和文档

一旦变更实施，确保相关的系统和用户文件及程序得到更新。

4.6.3. 管理指南

源自	输入
PO1	IT 项目投资组合
PO8	质量改进措施
PO9	IT 相关风险整改措施计划
PO10	项目管理指南和项目详细计划
DS3	所要求的变更
DS5	对变更的安全需求
DS8	服务请求/变更请求
DS9-10	变更请求(在何处以及如何实施处理)
DS10	问题记录

输出	到						
变更处理描述	AI1…AI3						
变更状态报告	ME1						
变更授权	AI7	DS8	DS10				

RACI 图

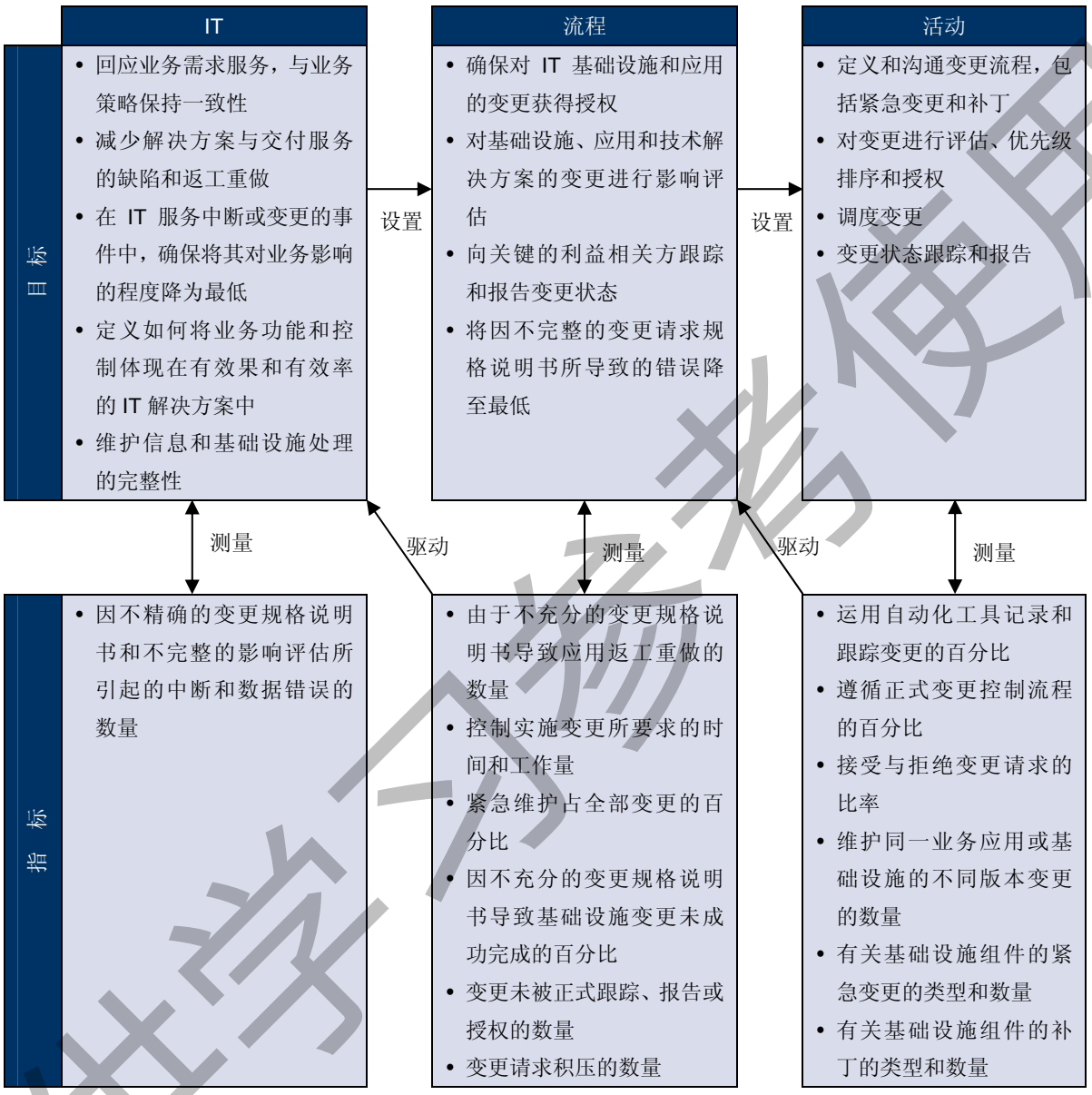
职能

活动

活动	首席执行官	首席财务官	业务执行经理	首席信息官	业务流程所有者	运营总监	首席架构师	开发总监	IT行政总监	项目管理官	合规、审计、风险和安全
制定和实施始终如一的对变更请求记录、评估和优先级排序的流程				A	I	R	C	R	C	C	C
基于业务需求对变更进行影响评估和优先级排序				I	R	A/R	C	R	C	R	C
确保任何紧急和重大变更遵循业已核准的变更处理流程				I	I	A/R	I	R			C
变更授权				I	C	A/R		R			
管理和发布有关变更的信息.				A	I	R	C	R	I	R	C

RACI 图中，**R**esponsible 代表**执行**，**A**ccountable 代表**责任**，**C**onsulted 代表**商议**，**I**nformed 代表**告知**。

4.6.4. 目标和指标



4.6.5. 成熟度模型

管理“变更管理”流程，使 IT 满足业务需求：服务于业务需求，与业务策略保持一致，同时减少解决方案及服务交付的缺陷和返工的机率。

0 级 无级别

变更管理流程未被定义，变更实质上未受控。没有意识到变更可能引起 IT 和业务营运的不一致，也未意识到优良的变更管理会带来益处。

1 级 初始级

意识到变更应被管理和控制。但实际情况经常变化，类似未经授权的变更经常发生。变更文档质量低或不存在，配置文件不完整和不可靠。由于缺乏变更管理，可能发生类似生产环境中断的错误。

2 级 可重复级

建立了非正式的变更管理流程，大部分变更遵循此流程；但流程尚未结构化，基本处于初级和易出错的阶段；配置文件内容的准确性不一致，变更之前仅进行有限的计划和影响评估。

3 级 定义级

建立了正式变更管理流程，包含分类、确定优先次序、应急程序、变更授权和版本管理等内容，并开始得到遵照执行。变更处理经常绕过变更流程，采用临时性变更措施处理。差错可能发生，未经授权的变更偶尔也会发生。IT 变更对业务运营的影响分析逐渐趋于正式，以支持新应用和技术的发布推广。

4 级 可管理级

建立良好的变更管理流程，所有的变更均遵循此流程，管理层确信可将例外情况降至最低。流程是有效的，但主要依赖人工程序和控制来保证变更质量。对所有变更进行全面的管理规划和影响评估，以降低变更实施后发生问题的可能性。存在变更的审批流程。变更管理文档准确及并反映了当前最新的状态，文档中包含变更正式实施轨迹。配置文件通常是准确的。IT 变更管理计划及实施与业务流程变更之间的集成越来越完善，以确保培训、组织变革及业务连续性方面的问题得到落实。IT 变更管理与业务流程再造之间的一致性日益增强。存在持续一致的流程，用于监控变更管理流程性能和质量。

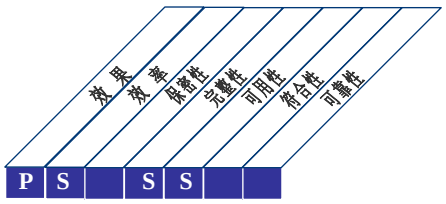
5 级 优化级

定期评审和升级变更管理流程，与最佳实践保持一致。评审流程反映了监控结果。配置信息由计算机管理，并提供版本控制。变更轨迹记录完善，使用工具检测未经许可和非法的软件。IT 变更管理与业务变更管理集成，确保 IT 成为企业生产力增长和创造新业务机会的推动力。

4.7. AI7 系统测试与发布

4.7.1. 流程描述

新系统开发完成后需要在生产环境进行实施和运营，这就需要首先在专用的测试环境下，使用相应的测试数据对新系统进行充分的测试，然后定义产品的首次发布和迁移说明，制定产品发布计划并进行实施，相应地还要进行实施后评审。确保运营系统达到与预期一致的结果。



控制 IT 流程：

解决方案和变更的上线和批准

使 IT 满足业务需求：

新开发或变更的系统上线后不会出现大的问题

通过关注于：

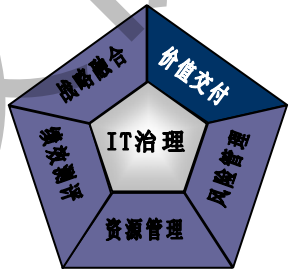
测试应用系统和基础设施解决方案是否满足预期目标，减少错误发生，并对产品的发布做出计划

通过下列实现：

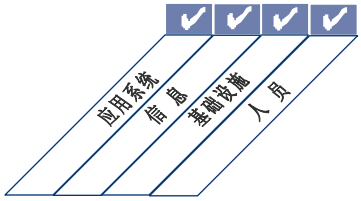
- 建立测试方法论
- 进行发布计划
- 测试结果被业务部门评估并批准
- 实施系统上线后评审

通过下列衡量：

- 由于不充分的测试而导致的应用系统故障时间或数据修复次数的总数
- 通过实施后评估达到预期收益的系统所占的百分比
- 文档化并经批准的测试计划的项目所占的百分比



■ 主要 ▦ 次要



4.7.2. 控制目标

AI7.1 用户培训

作为每一个信息系统开发、实施或修改项目的一部分，应按照既定的培训及实施计划和相关资料对用户部门及 IT 运营组织的人员进行培训。

AI7.2 测试方案

制定基于组织范围的标准的测试计划，此标准包括已定义的任务、职责和输入输出标准等，并确保该计划被相关部门正式批准。

AI7.3 实施方案

建立实施和回退/撤销方案，并获得相关部门正式批准。

AI7.4 测试环境

定义和建立安全的测试环境，测试环境能够代表预计生产环境中的安全性、内部控制、操作习惯、数据质量、保密要求和工作负载。

AI7.5 系统切换和数据转换

作为组织开发方法论的一部分，制定数据转换和基础设施迁移计划，并且包括审计轨迹、回退和撤销。

AI7.6 变更测试

在迁移到生产环境前，根据已定义的测试计划独立进行变更测试。确保测试计划考虑了安全和性能因素。

AI7.7 最终验收测试

确保业务流程拥有者和 IT 利益相关方根据测试计划确定的测试流程的结果进行评估。在测试流程中修正已识别的重大错误，错误已完成了在测试计划中识别的一整套测试和任何必须的压力测试。对验收测试结果进行评估后，批准在生产环境上线。

AI7.8 系统上线

测试完成后，遵照实施方案，控制系统转换到生产环境的迁移。获得诸如用户、系统拥有者、运营管理部门等关键利益相关方的正式批准。如有必要，新、旧系统应并行运行一段时间，并且比较运行情况和结果。

AI7.9 实施后评审

按照组织的变更管理标准制定一个程序，规定把实施后评审列入实施计划。

4.7.3. 管理指南

源自	输入
PO3	技术标准
PO4	记录系统所有者
PO8	开发标准
PO10	项目管理指南和项目详细计划
AI3	用于测试/安装的配置系统
AI4	用户、运营、支持、技术和管理手册
AI5	已采购细目
AI6	变更授权

输出	到						
发布的配置项	DS8	DS9					
已知和可接受缺陷	AI4						
上线	DS13						
软件版本和发布计划	DS13						
实施后评估	PO2	PO5	PO10				
内部控制监控	ME2						

RACI 图

职能

活动

活动	首席执行官	首席财务官	业务执行经理	首席信息官	业务流程所有者	运营总监	首席架构师	开发总监	IT行政总监	项目管理官	合规、审计、风险和安全
制定和评审实施计划			C	A	I	C	C	R		C	C
定义、评审测试策略（输入和输出标准）和执行测试计划方法论			C	A	C	C	C	R		C	C
为系统认证，建立和维护业务、技术需求知识库和测试案例				A				R			
在测试环境中完成系统切换和集成测试			I	I	R	C	C	A/R		I	C
部署测试环境并且执行最终验收测试			I	I	R	A	C	A/R		I	C
通过达成一致的鉴定标准，提交产品上线运行			I	R	A	R	C	R		I	C

RACI 图中，**R**esponsible 代表**执行**，**A**ccountable 代表**责任**，**C**onsulted 代表**商议**，**I**nformed 代表**告知**。

4.7.4. 目标和指标

4.7.5. 成熟度模型

管理“系统测试与发布”流程，使 IT 满足业务需求：新开发或变更的系统上线后不出现大的问题。

0 级 无级别

完全缺乏正式的安装和验收流程，无论是高级管理层还是 IT 人员都没有意识到需要验证解决方案是否满足预期的目标。

1 级 初始级

已经意识到验证和证实实施方案服务既定的目标是必需的。在部分项目中执行了测试，但是否测试由具体的项目组决定，且测试方法经常变化。正式的批准和审批很少或不存在。

2 级 可重复级

在测试和认证方法之间存在一定的一致性，但通常不是基于任何既定方法论。通常由单独的开发团队决定测试的方法，并且往往缺乏集成测试。有一个非正式的审批流程。

3 级 定义级

在安装、移植、转换、验收环节存在正式的方法论。IT 的安装和验收流程集成在系统生命周期中并且在一定程度上是自动化的。个人的决定可能导致培训、测试、上线和验收与既定的流程不符。已上线系统的质量缺乏一致性，新系统在实施后产生了重大问题。

4 级 可管理级

建立了正式的流程，对既定的测试环境和验收程序进行很好的组织和实践。在实际操作中，所有重要的系统变更都遵循正式的方法。满足用户需求的评估是标准化和可度量的，产品的规格也是能够被管理层评估和分析的。已上线系统的质量是令管理层满意的，实施后出现的问题也在合理的水平上。流程的自动化是特定的并且是基于项目的。尽管缺乏实施后评估，管理层对当前系统的效率水平仍可能是满意的。测试系统能充分反映生产环境。新系统的压力测试和现有系统的回归测试被应用于重大项目。

5 级 优化级

作为持续改进和精细化的结果，安装和验收流程已经达到最佳实践的水平。IT 安装和验收流程完全统一于系统的生命周期，并在适当的时候自动化的，推进有效培训，新系统向生产状态的测试和转化。建立良好的测试环境、问题记录和故障分析流程，以确保产品有效率和有效果地迁移到生产环境。验收通常一次成功，不需要返工，实施后问题仅限于微小的改动。实施后评估是标准化的，并且得来的经验教训被重新引入流程，确保持续的质量改进。一贯采用新系统的压力测试和改进系统的回归测试。

5. 交付与支持（DS）

DS1 服务水平的定义和管理

DS2 第三方服务管理

DS3 性能和容量管理

DS4 确保持续服务

DS5 确保系统安全

DS6 成本确认和分摊

DS7 教育和培训用户

DS8 服务台和事件管理

DS9 配置管理

DS10 问题管理

DS11 数据管理

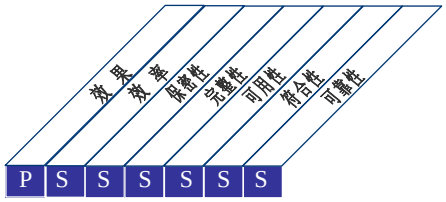
DS12 物理环境管理

DS13 运营管理

5.1. DS1 服务水平的定义和管理

5.1.1. 流程描述

通过 IT 服务及服务水平的书面定义和协议，IT 管理者和业务客户之间能够就需要的服务进行有效沟通。该流程还包括监控服务水平的完成情况并及时向利益相关方报告，使 IT 服务和相关的业务需求保持一致。



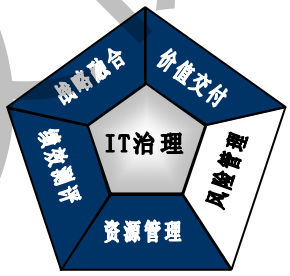
控制 IT 流程：
服务水平的定义和管理

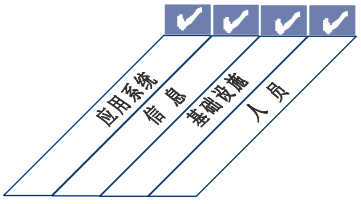
使 IT 满足业务需求：
确保关键 IT 服务和业务策略的一致性

通过关注于：
识别服务需求，约定服务水平并监控服务水平的完成情况

通过下列实现：
- 与需求和交付能力一致的内、外部正式协议
- 服务水平完成情况报告(报告和会议)
- 在制定战略规划时识别并考虑新出现的、已更新的服务需求。

通过下列衡量：
- 对符合约定水平的服务交付满意的业务利益相关方的百分比
- 不在约定范围内交付的服务数量
- 每年同业务客户召开的正式的服务水平协议评审会议的次数





■ 主要 ▦ 次要

5.1.2. 控制目标

DS1.1 服务水平管理框架

定义一个框架，在客户和服务提供者之间提供一个正式的服务水平管理流程。该框架应当和业务需求与优先级保持持续一致，并促进用户和服务提供者达成共识(facilitate common understanding)。该框架应当包括以下流程：建立服务需求、服务定义、服务水平协议(SLAs)、运营水平协议(OLAs)和资金来源。这些内容属性应安排在服务目录（service catalogue）中。该框架应当为服务水平管理者定义组织架构，包括内外部服务提供者和客户的角色、任务和职责。

DS1.2 服务定义

IT服务定义以服务特征和业务需求为基础。以服务目录形式将这些服务集中组织和存储起来。

DS1.3 服务水平协议

基于客户需求和 IT 容量，为所有的关键 IT 服务定义并签署服务水平协议。协议应当包括客户承诺、服务支持需求、经利益相关方签署的衡量这些服务的定性和定量标准、融资和商务安排、角色和责任，以及该 SLA 协议可能的监督。需要考虑的内容有:可用性、可靠性、性能、容量的增长、支持水平、可持续性计划、安全和需求约束。

DS1.4 运营水平协议

定义OLAs，以说明技术上如何交付这些服务，以便最好地支持SLA(s)。OLAs应当向服务提供者详细说明有针对性的技术流程并可以支持多份SLAs。

DS1.5 服务水平绩效的监控和报告

持续监控指定的服务水平执行标准。服务水平完成报告应当有针对性的提供给利益相关方。分析监控统计结果，识别个别服务和整体服务的负面和正面趋势。

DS1.6 服务水平协议和合同的审阅

定期审阅SLAs和与内外部服务提供者签署的基础合同（UCs），以确保它们是有效的和最新的，并且已经考虑了需求的变化。

5.1.3. 管理指南

源自	输入
PO1	战略和战术的 IT 计划，IT 服务目录
PO2	指定的数据分类
PO5	更新的 IT 服务组合
AI2	初始计划的 SLAs
AI3	初始计划的 OLAs
DS4	包括角色和职责的灾难服务需求
ME1	绩效输入到 IT 计划编制

输出	到						
合同评审报告	DS2						
流程绩效报告	ME1						
新的/更新的服务需求	PO1						
SLAs	AI1	DS2	DS3	DS4	DS6	DS8	DS13
OLAs	DS4	DS5	DS6	DS7	DS8	DS11	DS13
更新的IT服务组合	PO1						

RACI 图

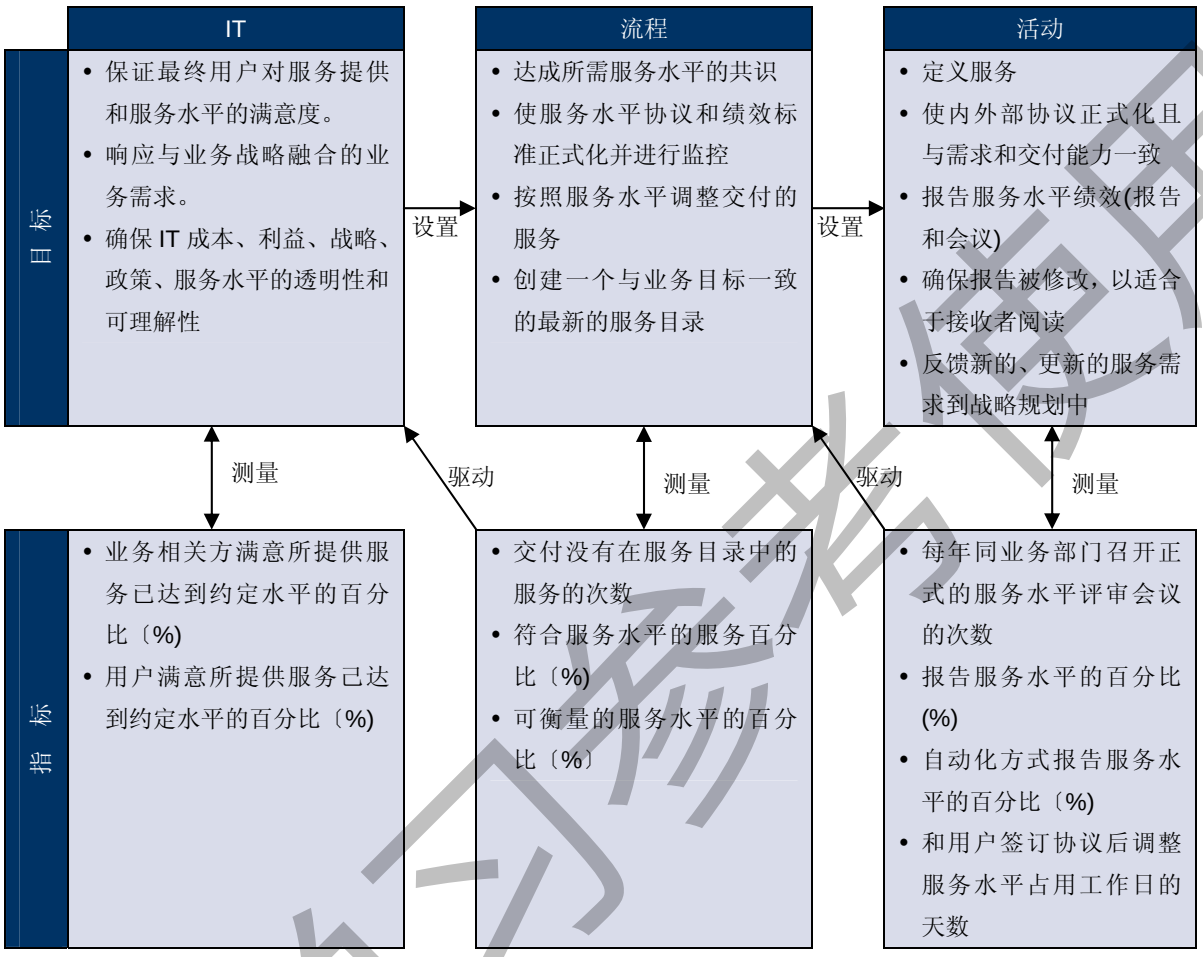
职能

活动

活动	首席执行官	首席财务官	业务执行经理	首席信息官	业务流程所有者	运营总监	首席架构师	开发总监	IT行政总监	项目管理官	合规、审计、风险和安全	服务管理者
为定义IT服务创建一个框架			C	A	C	C	I	C	C	I	C	R
建立 IT 服务目录			I	A	C	C	I	C	C	I	I	R
为关键 IT 服务定义 SLAs		I	I	C	C	R	I	R	R	C	C	A/R
定义符合 SLAs 的 OLAs				I	C	R	I	R	R	C	C	A/R
监控和报告端对端服务水平绩效				I	I	R		I	I		I	A/R
审阅 SLAs 和 UCs		I		I	C	R		R	R		C	A/R
审阅和更新服务目录			I	A	C	C	I	C	C	I	I	R
创建服务改进计划			I	A	I	R	I	R	C	C	I	R

RACI 图中，**R**esponsible 代表**执行**，**A**ccountable 代表**责任**，**C**onsulted 代表**商议**，**I**nformed 代表**告知**。

5.1.4. 目标和指标



5.1.5. 成熟度模型

管理“服务水平的定义和管理”流程，使 IT 满足业务需求：保证关键 IT 服务与业务战略的一致性。

0 级 无级别

管理层没有意识到定义服务水平流程的需求，没有分配监测服务水平的责任和义务。

1 级 初始级

有管理服务水平的意识，但是流程是非正式的和被动的。没有详细说明定义和管理服务的责任及义务。即使有绩效测评，也仅仅是定性的，没有严格定义目标。报告是非正式的、少量的和不一致的。

2 级 可重复级

存在达成一致的服务水平，但它们是非正式的、没有审阅过的。服务水平报告是不完整的，可能是不切题或误导客户的。服务水平报告依赖于个体管理者的技能和主动性。服务水平协调者被指定并赋予定义的职责，但是权力有限。即使存在一个符合服务水平协议（SLAs）的流程，也仅是自发的，而不是强制执行的。

3 级 定义级

已定义好责任，但是授权很随意。SLA 开发流程设置了检查点，用于再评估服务水平和客户满意度。利用一个标准流程，服务和服务水平被定义、文档化并达成共识。服务水平的不足被识别，但是解决这些不足的过程是非正式的。预期服务水平成果和资金提供之间有清晰联系。服务水平虽然达成了共识，但可能没有满足业务需求。

4 级 可管理级

在系统需求定义阶段，越来越多地考虑到服务水平定义，并且整合到应用和操作环境的设计中。客户满意度被定期衡量和评估。绩效测评反映用户需求，而不是 IT 目标。评估服务水平的衡量标准变得正规化，并反映了行业标准。以关键业务作为定义服务水平的标准的基础，同时包括可用性、可靠性、性能、增长的容量、用户支持、持续性计划和安全考虑。当服务水平没有达到要求时，根本原因分析被例行完成。监控服务水平的报告流程正在日趋自动化。与不符合约定服务水平相关联的操作和金融风险被定义和清晰理解。一个正式的测量系统被建立和维护。

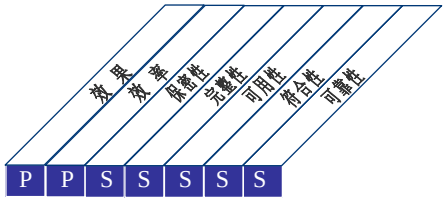
5 级 优化级

在利用技术优势,包括成本效益比的同时，服务水平得到持续的重新评估以保证与 IT 目标和业务目标的一致。所有服务水平管理流程都在持续改进。客户满意度被持续地监控和管理。预期服务水平反映了业务单元战略目标，同时依照行业标准进行评估。IT 管理层拥有达到服务水平目标所需的资源和义务，并建立实现目标的激励机制。作为持续改进流程的一部分，高管层监控绩效测评。

5.2. DS2 第三方服务管理

5.2.1. 流程描述

为了保证由第三方（供应商、合作伙伴）提供的服务满足业务需求，需要一个有效的第三方管理流程。这个流程既通过在第三方协议中清晰的定义角色、责任和期望来完成，又通过审阅和监控协议的有效性和遵循性来完成。有效的第三方服务管理能使不履约供应商相关的业务风险降到最低。



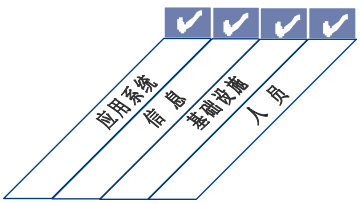
控制 IT 流程：
第三方服务管理

使 IT 满足业务需求：
通过明确的收益、成本和风险，提供满意的第三方服务

通过关注于：
和有资格的第三方服务供应商建立关系和双边责任，监控服务的交付，以验证并确保符合服务协议

通过下列实现：
- 识别和分类供应商服务
- 识别和减小供应商风险
- 监控和测评供应商绩效

通过下列衡量：
- 用户对签约服务的投诉次数
- 符合明确定义的服务需求和服务水平的主要供应商的百分比
- 受监控的主要供应商百分比



5.2.2. 控制目标

DS2.1 所有供应商关系的识别

识别所有供应商服务，并通过供应商类型、重要性、关键性加以分类。维护正式的技术和组织关系文档，这些文档包括供应商的角色、职责、目标、预期的交付成果、主要资质证书。

DS2.2 供应商关系管理

对每个供应商都有正式化的供应商关系管理流程。关系所有者应当保持与客户和供应商的联系，并确保关系的质量是建立在信任和透明的基础之上（例如，通过签订 SLAs）。

DS2.3 供应商风险管理

持续识别和减小与供应商能力相关的风险，以便安全、高效的持续交付有效的服务。确保合同符合遵循法律法规要求的业务标准。风险管理层应进一步关注保密协议（NDAs）、第三方存管合同、供应商持续的发展能力、安全要求的遵循、供应商变更、惩罚和奖励等。

DS2.4 供应商绩效监控

建立监控服务交付的流程，确保该供应商满足目前的业务需求并继续履行合同协议和 SLAs，而且该供应商的绩效与其他供应商和市场环境相比是有竞争力的。

5.2.3. 管理指南

源自	输入
PO1	IT 资源策略
PO8	获取标准
AI5	合同方案，第三方关系管理需求
DS1	SLAs，合同评审报告
DS4	灾难服务要求，包括角色和职责

输出	到						
流程绩效报告	ME1						
供应商目录	AI5						
供应商风险	PO9						

RACI 图

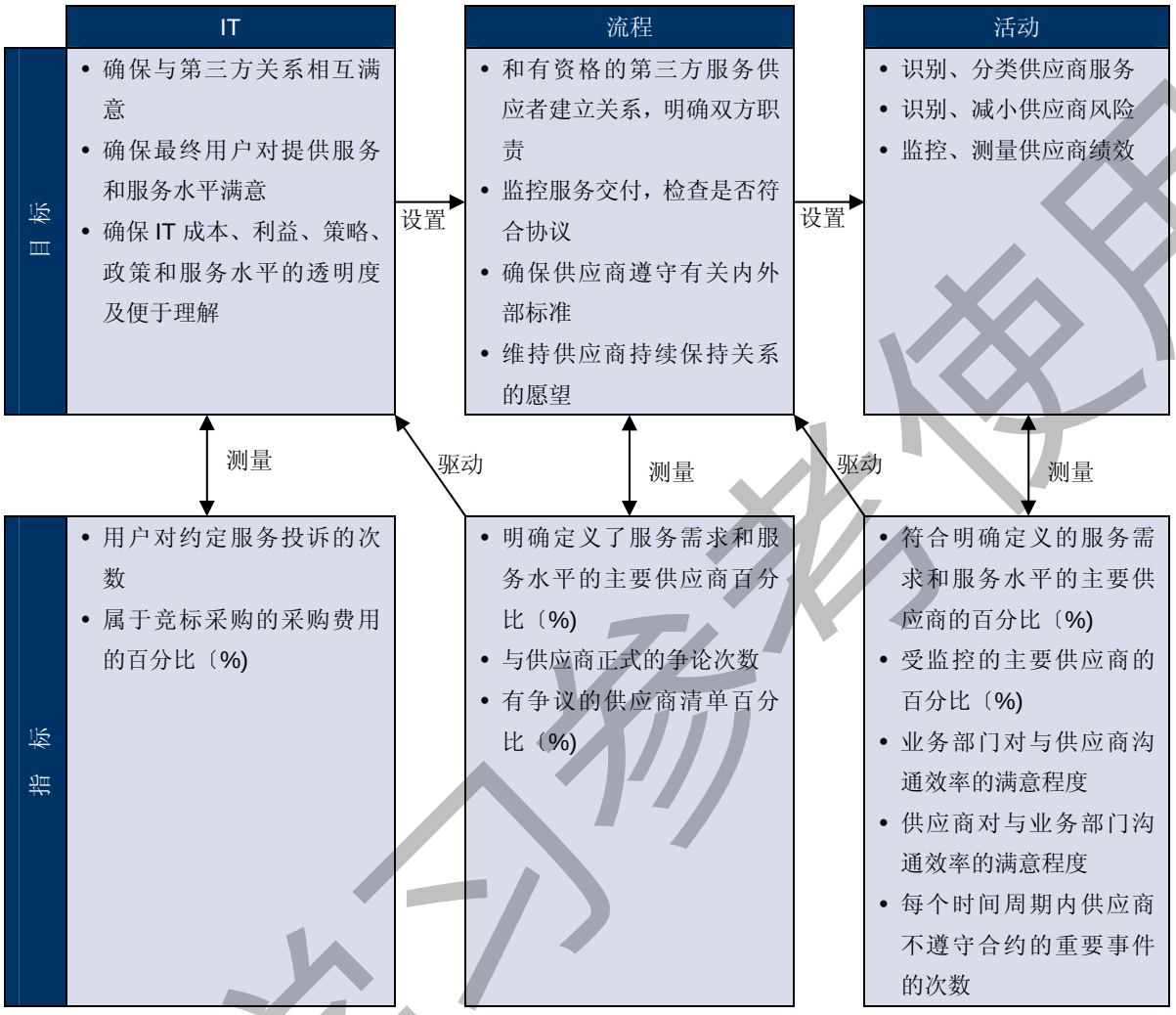
职能

活动

活动	首席执行官	首席财务官	业务执行经理	首席信息官	业务流程所有者	运营总监	首席架构师	开发总监	IT行政总监	项目管理官	合规、审计、风险和安全
识别、分类第三方服务关系				I	C	R	C	R	A/R	C	C
定义、文档化供应商管理流程		C		A	I	R	I	R	R	C	C
建立供应商评估、选择规则和流程		C		A	C	C		C	R	C	C
识别、评估和减小供应商风险		I		A		R		R	R	C	C
监控供应商服务交付				R	A	R		R	R	C	C
为所有业务利益相关方评估服务关系的长期目标	C	C	C	A/R	C	C	C	C	R	C	C

RACI 图中，**R**esponsible 代表**执行**，**A**ccountable 代表**责任**，**C**onsulted 代表**商议**，**I**nformed 代表**告知**。

5.2.4. 目标和指标



5.2.5. 成熟度模型

管理“第三方服务管理”流程，使 IT 满足业务需求：提供满意的第三方服务的同时使利益、成本和风险是透明的。

0 级 无级别

未定义职责和义务，缺少关于与第三方签约的正式政策和流程，第三方服务未经管理层批准和审阅。不存在测量活动，没有来自第三方的报告。在缺乏约定报告职责的情况下，高级管理层不清楚服务的交付质量。

1 级 初始级

管理层意识到需要通过文档化的政策和程序进行第三方管理，包括签订合同。与服务提供者没有标准的协议条款。提供的服务的测评是不正式和被动的。操作实践是依赖于个体和供应商的经验（例如，在要求时）。

2 级 可重复级

监控第三方服务供应商、相关风险以及服务交付的流程是非正式的。与标准的供应商条款和条件一起被使用的签署的、形式上的合同（例如，提供服务的描述）。有关于提供服务的报告，但不支持业务目标。

3 级 定义级

具有良好的管理第三方服务的文档化流程，并且有与供应商进行检查和谈判的清晰的流程。服务提供合同签订时，与第三方的关系是完全建立在合同基础上的。提供服务的特性在合同中详细说明，包括法律法规、操作和控制需求。指定了第三方服务的监督责任。合同条款基于标准模板。有关第三方服务的业务风险被评估和报告。

4 级 可管理级

建立正式和规范的标准来定义保证条款，条款包括工作范围、提供的服务和交付内容、前提、计划、成本、付款方式和职责。明确了合同和供应商管理的职责。供应商资格、风险和能力被持续审查。结合业务目标定义服务需求。存在一个依照合同条款检查服务绩效的流程，为评估当前和未来第三方服务提供依据。在采购流程中使用了转让定价模型。所有相关方都清楚服务、成本和里程碑期望值。存在约定好的监控服务供应商的目标和指标。

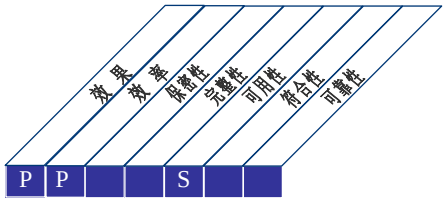
5 级 优化级

按预定的间隔，定期审阅与第三方签订的合同。明确了管理供应商及其提供服务的质量的职责。从可操作性、合法性和可控性方面监控合同的遵从情况，并强行执行纠正。独立地周期性审核第三方，并提供绩效反馈信息用于改进服务交付。采用的测量方法根据业务条件的改变而变化。存在支持潜在问题早期发现的措施。广泛的、已定义的服务水平绩效报告与第三方补偿相关联。管理者基于测量员调整第三方服务的获取和监控流程。

5.3. DS3 性能和容量管理

5.3.1. 流程描述

管理 IT 资源的性能和容量必须有一个定期检查当前 IT 资源的性能和容量的流程。该流程基于工作负载、储存需求和例外需求来预测未来需求。该流程为支持业务需求的信息资源持续可用提供保证。

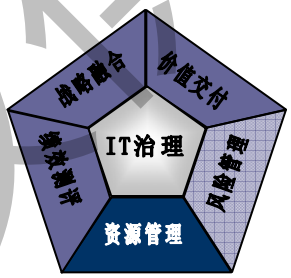


控制 IT 流程：
性能和容量管理

使 IT 满足业务需求：
优化 IT 基础设施、资源和容量的性能以响应业务需要

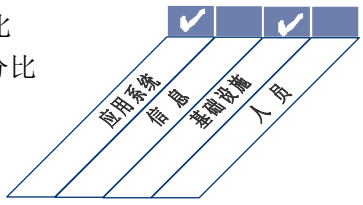
通过关注于：
满足 SLAs 要求的响应时间，减小停机时间，通过监控和测评持续改进 IT 的性能和容量

通过下列实现：
- 系统容量和可用性的计划和提供
- 系统性能的监控和报告
- 系统性能的模拟和预测



■ 主要 ▦ 次要

通过下列衡量：
- 由于不充足的容量计划，每个用户每月损失的机时数量
- 超过目标利用率峰值的百分比
- 不符合 SLAs 响应时间的百分比



5.3.2. 控制目标

DS3.1 性能和容量计划

建立一个审阅 IT 资源性能和容量的计划流程，确保合理成本的容量和性能能够有效处理由 SLAs 确定的、达成一致的工作负载。容量和性能计划应采用适当的模型，该模型考虑了 IT 资源当前和未来的性能、容量和吞吐量。

DS3.2 当前性能和容量

评估当前 IT 资源的性能和容量是否能够满足已达成协议服务水平的交付要求。

DS3.3 未来性能和容量

定期进行 IT 资源的性能和容量预测，把由于容量不足和性能退化引起服务中断的风险降低到最低程度，同时为可能的重新部署识别出额外的容量。识别工作负载趋势，确定在性能和容量计划中考虑了这些预测数据。

DS3.4 IT 资源的可用性

考虑正常的工作负载、突发事件、存储需求和 IT 资源的生命周期等因素，提供所需的容量和性能。应当做好如下安排：区分任务优先级、容错机制、资源分配实践。管理层应当确保应急计划正确描述了个别 IT 资源的可用性、容量和性能。

DS3.5 监控和报告

持续监控 IT 资源的性能和容量。收集的数据应该为以下两个目的服务：

- 维持和调整当前的 IT 性能，处理诸如恢复能力、紧急事件、当前和计划工作负荷、存储计划和资源获得等问题。
- 按照 SLAs 要求向业务部门报告交付服务的可用性。

附有所有的例外报告及整改建议。

5.3.3. 管理指南

源自	输入
AI2	可用性、连续性和恢复详细说明
AI3	系统监控要求
DS1	SLAs

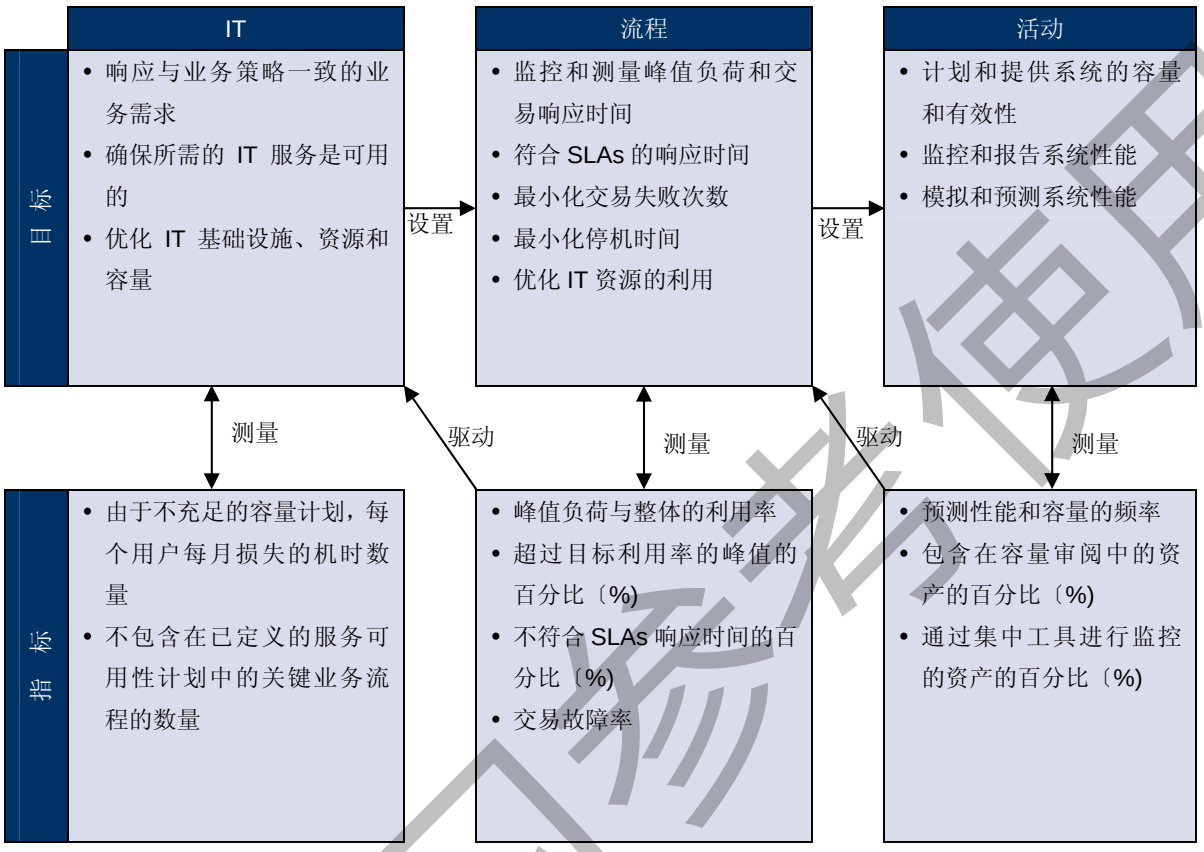
输出	到						
性能和容量信息	PO2	PO3					
性能和容量计划（需求）	PO5	AI1	AI3	ME1			
需求变更	AI6						
流程绩效报告	ME1						

RACI 图

活动 \ 职能	首席执行官	首席财务官	业务执行经理	首席信息官	业务流程所有者	运营总监	首席架构师	开发总监	IT行政总监	项目管理官	合规、审计、风险和安全
建立一个计划流程以审阅 IT 资源的性能和容量				A		R	C	C	C	C	
审阅当前 IT 资源的性能和容量				C	I	A/R		C	C	C	
预测 IT 资源的性能和容量				C	C	A/R	C	C	C	C	
进行差异分析以识别 IT 资源的不匹配				C	I	A/R		R	C	C	I
为 IT 资源的潜在失效建立应急计划				C	I	A/R		C	C	I	C
持续性地监控和报告 IT 资源的可用性、容量和性能。				I	I	A/R		I	I	I	I

RACI 图中，**R**esponsible 代表**执行**，**A**ccountable 代表**责任**，**C**onsulted 代表**商议**，**I**nformed 代表**告知**。

5.3.4. 目标和指标



5.3.5. 成熟度模型

管理“性能和容量管理”流程，使 IT 满足业务需求：优化 IT 基础设施、资源和容量以响应业务需要。

0 级 无级别

管理层没有意识到关键业务流程可能需要高水平的 IT 性能，或者全部的业务对 IT 服务的需求可能超过了容量。没有合适的容量计划流程。

1 级 初始级

用户为性能和容量限制设计临时解决方法。不鼓励业务流程所有者对性能和容量计划的需要。性能和容量的管理行为是典型被动的。容量和性能计划流程是非正式的。对 IT 资源当前和将来的性能和容量理解有限。

2 级 可重复级

业务和 IT 管理层意识到没有性能和容量管理所带来的影响。基于个体系统的评估、支持和项目团队的知识，性能需求通常能够满足。使用一些单独的工具来诊断性能和容量问题，但是结果的一致性是依赖于关键个体的专业知识的。不存在对于 IT 性能和容量的整体评估或者对于最高的和最不利的负荷情况的考虑。可用性问题通常以意外和随机的方式发生，而且需要花费相当长的时间来诊断和改正。任何的性能测量都主要是以 IT 需求为基础而不是客户需求。

3 级 定义级

性能和容量需求的定义贯穿于系统的整个生命周期。定义了服务水平需求和标准，可以用来衡量运行性能。按照确定的流程，跟随一个已定义流程，未来性能和容量需求被模型化。

提供性能统计报告。与性能和容量相关的问题仍然可能发生，需要花费一定时间来改正它。虽然发布了服务标准，用户和客户仍然可能对服务能力表示怀疑。

4 级 可管理级

具有用于衡量系统的使用、性能、容量的流程和工具，并且把结果和确定的目标进行比较。最新的信息是可用的，提供了标准化性能统计，并且对因为性能和容量不足引起的事件进行报警。性能和容量不足引起的事故被按照已定义的和标准的流程来处理。自动化工具被用于监控特定资源，比如磁盘空间、网络、服务器和网关。在业务处理期间报告性能和容量的统计信息，以使用户和客户了解 IT 服务水平。用户对于现行的服务能力普遍满意，并且可能要求新的改善的可用性水平。测量 IT 性能和容量的标准已经达成一致，但是可能仅仅被偶尔地和不一致地应用。

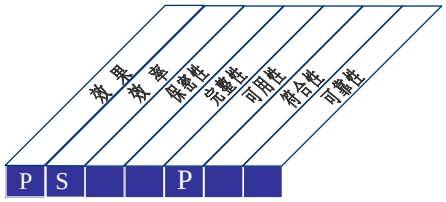
5 级 优化级

性能和容量计划与业务需求预测完全同步。IT 基础设施和业务需求取决于定期的审阅，以确保花费可能的最低成本达到最优的容量。监控关键 IT 资源的工具被标准化，能够跨平台使用，并且和组织范围内的事件管理系统关联。监控工具检测，并且能自动修正与性能和容量相关的问题。趋势分析被执行，并且显示由于业务量的增加而马上出现的性能问题，促使制定计划和避免非预期的问题发生。测量 IT 性能和容量的标准被细致引入到所有关键业务流程的结果测量和性能指标中，并且被一贯地执行。根据这些测量分析，管理层调整性能和容量计划。

5.4. DS4 确保持续服务

5.4.1. 流程描述

为了提供持续性的 IT 服务，需要开发、维护和测试 IT 持续性计划，利用异地备份存储，提供定期的持续性计划的培训。一个有效的持续性服务流程最大程度减少主要 IT 服务中断的可能性和对关键业务功能和流程的影响。



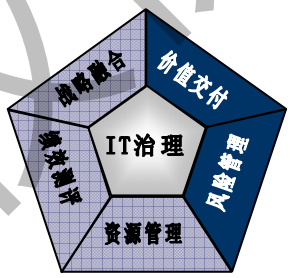
控制 IT 流程：
确保持续服务

使 IT 满足业务需求：
如果发生 IT 服务中断，确保对业务的影响最小

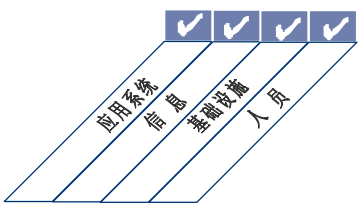
通过关注于：
建立了灵活的自动化解决方案，并开发、维护、演练 IT 持续性计划

通过下列实现：
- 开发和维护（改善）IT 应急计划
- 培训和演练 IT 应急计划
- 异地存储应急计划和数据的拷贝

通过下列衡量：
- 由于无计划的停机，每个用户每月损失的小时数
- IT 持续性计划中未覆盖依赖于 IT 的关键业务流程的数量



主要　　次要



5.4.2. 控制目标

DS4.1 IT 持续性框架

建立了一个 IT 持续性框架，使用一致的流程支持企业级的业务持续性管理。框架的目标应当是辅助决定基础设施所需的恢复力和推动灾难恢复和 IT 应急计划的制定。框架应当说明持续性管理的组织结构，包括内外部服务提供者以及他们的管理者和客户的角色、任务和职责，以及计划流程，该流程建立规则和结构来记录、测试和执行灾难恢复和 IT 应急计划。计划还应当包括关键资源的识别、关键影响因素的说明、关键资源可用性的监控和报告、替代的处理以及备份和恢复原则。

DS4.2 IT 持续性计划

IT 持续性计划基于框架建立，旨在降低关键业务功能和流程中断带来的影响。计划应当根据潜在业务影响的风险理解，明确所有 IT 关键服务对破坏承受能力、替代的处理和恢复能力的需求。它们还应当包括使用指南、角色和职责、程序、沟通流程和测试方法。

DS4.3 关键 IT 资源

把注意力集中在 IT 持续性计划所指定的最关键项目上，在恢复情形下建立恢复能力和优先级。避免恢复次要项目对注意力的分散，确保响应和恢复与业务需求的优先排序一致，成本保持在可接受的水平并与法规和合同要求一致。考虑不同等级的承受能力、响应和恢复需求（比如 1～4 小时，4～24 小时，超过 24 小时）以及关键业务的运营周期。

DS4.4 IT 持续性计划的维护

鼓励 IT 管理层定义和执行变更控制程序，确保 IT 持续性计划保持最新版本并持续反映实际的业务需求。清晰、及时地传达程序和职责的变更信息。

DS4.5 IT 持续性计划的测试

定期测试 IT 持续性计划，确保 IT 系统能有效恢复，发现计划的缺陷，保持计划的相关性。这需要细致的准备、文档资料、测试结果报告，以及根据测试结果实施相应的行动计划。将单一应用的测试恢复的范围与端对端测试的集成测试方案和集成供应商测试一起考虑。

DS4.6 IT 持续性计划的培训

向所有相关方提供定期的培训会议，培训内容是关于假设事件或灾难发生时的程序和他们的角色和职责。通过应急测试结果来检验和提升培训。

DS4.7 IT 持续性计划的分发

定义和管理了分发策略，确保计划被适当和安全地分发，对于合适的经授权的团体来说，计划随时随地都是可用的。应当关注使计划在所有灾难情形下都容易得到。

DS4.8 IT 服务恢复和重新开始

计划 IT 恢复和重新开始服务期间将要采取的行动。这可能包括备份站点的激活、替代处理的开始、客户和利益相关方的沟通以及重新开始的程序。确保业务部门理解 IT 恢复时间和必要的技术投资以支持业务恢复和重新开始的需要。

DS4.9 异地备份存储

异地存储在 IT 恢复和业务持续性计划中需要的所有关键备份介质、文档和其它 IT 资源。业务流程所有者和 IT 人员共同决定备份存储的内容。异地存储设施的管理应该符合数据分类政策和企业的介质存储惯例。IT 管理层应该确保周期性地评估异地存储安排，至少每年一次，评估内容包括环境保护和安全。确保用于恢复归档数据的硬件和软件的兼容性，并且周期性地测试和更新归档数据。

DS4.10 恢复后审查

确定 IT 管理层是否建立了评估关于灾难后 IT 功能成功恢复的计划充分性的流程，并相应更新计划。

5.4.3. 管理指南

源自	输入
PO2	制定数据分类
PO9	风险评估
AI2	可用性、持续性和恢复的详细说明
AI4	用户、运行、支持、技术和管理手册
DS1	SLAs 和 OLAs

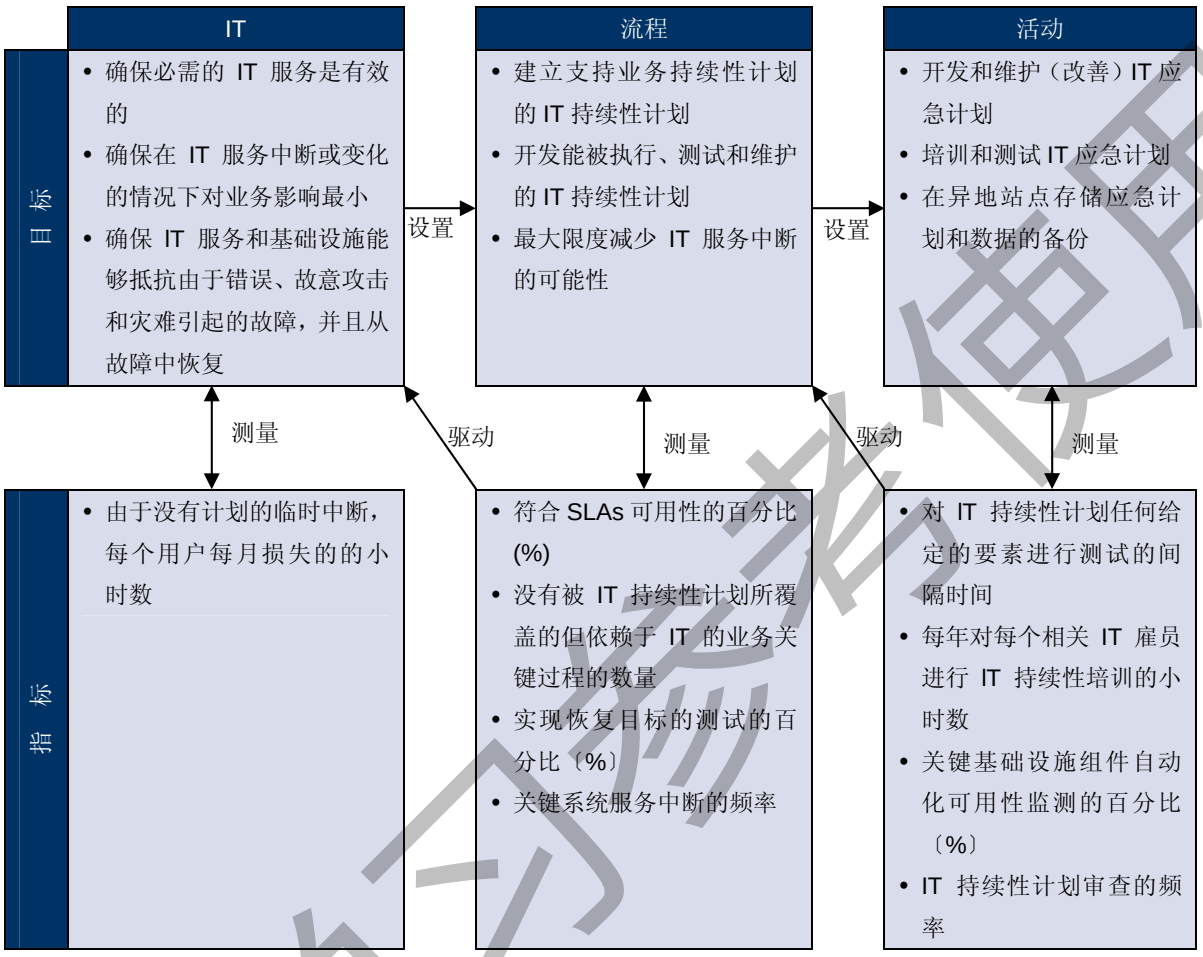
输出	到						
应急测试结果	PO9						
IT 配置项的关键程度	DS9						
备份存储和保护计划	DS11	DS13					
事件/灾难的阈值	DS8						
包括角色和职责的灾难服务需求	DS1	DS2					
流程绩效报告	ME1						

RACI 图

活动 \ 职能	首席执行官	首席财务官	业务执行经理	首席信息官	业务流程所有者	运营总监	首席架构师	开发总监	IT行政总监	项目管理官	合规、审计、风险和安全
开发 IT 持续性框架		C	C	A	C	R	R	R	C	C	R
进行业务影响分析和风险评估		C	C	C	C	A/R	C	C	C	C	C
开发和维护 IT 持续性计划	I	C	C	C	I	A/R		C	C	C	C
基于恢复目标的识别和分类 IT 资源				C		A/R		C	I	C	I
定义和执行变更管理流程确保 IT 持续性计划符合当前实际				I		A/R		R	R	R	I
定期测试 IT 持续性计划				I	I	A/R		C	C	I	I
根据测试结果开发一个后续的行动计划				C	I	A/R	C	R	R	R	I
计划和实施 IT 持续性培训				I	R	A/R		C	R	I	I
计划 IT 服务的恢复和重新开始		I	I	C	C	A/R	C	R	R	R	C
计划和实施备份存储和保护				I		A/R		C	C	I	I
建立执行恢复后审查的流程				C	I	A/R		C	C		C

RACI 图中，**R**esponsible 代表**执行**，**A**ccountable 代表**责任**，**C**onsulted 代表**商议**，**I**nformed 代表**告知**。

5.4.4. 目标和指标



5.4.5. 成熟度模型

管理“确保持续服务”的流程，使 IT 满足业务要求：确保 IT 服务中断事件对业务的影响最小。

0 级 无级别

没有 IT 运行的风险、漏洞和威胁的认识，或没有失去 IT 服务对业务的影响的认识。服务的持续性没有认识到需要管理层关注。

1 级 初始级

持续性服务的责任是非正式的，执行这个责任的授权是有限的；管理层开始意识到持续性服务的相关风险以及对持续性服务的需求；在持续性服务方面，管理层关注的焦点是基础设施资源，而不是 IT 服务；用户采取变通的办法响应服务中断；对于重大的业务中断，IT 部门的响应是被动的、没有准备的；停机计划考虑了 IT 需要，但是没有考虑业务需求。

2 级 可重复级

分配了确保持续服务的责任，但保证持续服务的方法是零碎的；系统可用性的报告是零星的、可能是不完整的，并且没有考虑业务影响；尽管有持续性服务可用性的承诺，并且它的主要原理也众所周知，但是没有文档化的 IT 持续性计划；有一个关键系统和组件的清单，但是可能不可靠；规范化的持续性服务实践正在逐步形成，但是成功与否依赖于个体。

3 级 定义级

管理持续性服务的责任是明确的。对持续性服务进行计划和演练的责任进行了清晰的定义和分配；IT 持续性计划已经文档化，并且是基于系统重要性和业务影响；周期性地报告持续性服务测试结果；在处理重大事件和灾难时，依靠个体的主动性来遵守标准和接受培训；管理层一贯地沟通确保持续服务计划的需要；高可用性组件和系统冗余正在被应用，关键系统和组件的清单得到维护。

4 级 可管理级

持续性服务的责任和标准被强制执行；分派了维护持续性服务计划的责任；维护活动是基于持续性服务测试的结果、内部好的实践经验以及不断变化的 IT 和业务环境；有关持续性服务的结构化数据被收集、分析、报告和执行；提供了关于持续服务流程的正式的、强制的培训，系统可用性的好的实践经验正在被统一推广实行；可用性实践和持续服务计划相互影响；对中断事件进行分类，相关的每一个人都清楚每一类事件的升级途径；制定了持续服务的目标和指标，并得到认可，但可能是不一致的测量。

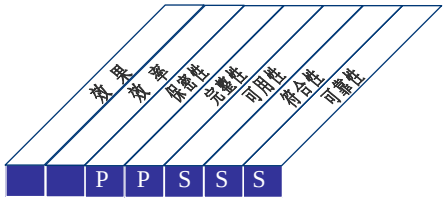
5 级 优化级

集成的持续服务流程考虑了基准和最佳外部实践；IT 持续性计划与业务持续性计划进行了整合，并且得到例行维护；确保持续服务的需求得到销售商和主要供应商的保障；进行了 IT 持续性计划的整体测试，并将测试结果用于更新计划；通过收集和分析数据，对流程进行持续改进；可用性实践和持续服务计划完全一致；管理层确信灾难或者主要事件不因单点故障而引发；升级实践得到理解，并且被彻底地强制执行；关于持续服务效果的目标和指标被系统地测量，管理层根据测量结果对计划进行调整。

5.5. DS5 确保系统安全

5.5.1. 流程描述

为了维护信息的完整性和保护 IT 资产，需要一个安全管理流程。这个流程包括建立和维护 IT 安全的角色、职责、政策、标准和程序。安全管理也包括执行安全监控、定期测试和对识别的安全弱点和事件进行纠正。有效的安全管理通过保护所有的 IT 资产来最小化安全漏洞和事件对业务的影响。



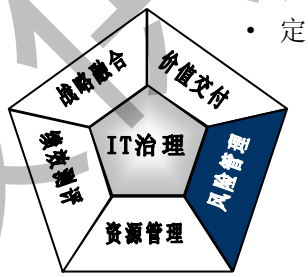
控制 IT 流程：
确保系统安全

使 IT 满足业务需求：
维护信息的完整性和基础设施运行，最小化安全弱点和事件对业务的影响

通过关注于：
定义 IT 安全政策、计划和程序，并且监控、检测、报告和解决安全漏洞和事件

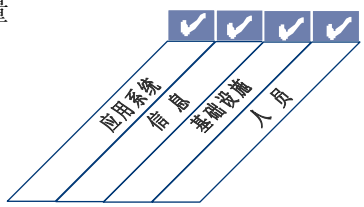
通过下列实现：

- 理解安全需求、漏洞和威胁
- 以标准方式管理用户认证和授权
- 定期测试安全



通过下列衡量：

- 损害组织公共声誉的事件数量
- 不符合安全需求的系统数量
- 违反职责分离的数量



■ 主要　▦ 次要

5.5.2. 控制目标

DS5.1 IT 安全管理

在最高的适当的组织层面管理 IT 安全，使对安全行为的管理符合业务需求。

DS5.2 IT 安全计划

把业务、风险和遵从性需求转化为一个总体安全计划，同时考虑 IT 基础设施和安全文化。确保这个计划和在服务、人员、软件和硬件方面的适当投资一起，应用到安全政策和程序中。将安全政策和程序传达给利益相关方和用户。

DS5.3 身份管理

确保所有用户（内部的、外部的和临时的）和他们在 IT 系统中的行为（业务应用、IT 环境、系统操作、开发和维护）能够唯一确认。通过验证机制授予用户身份。证实用户访问系统和数据的权限与定义的和签订的业务需求一致，而且工作要求被附加在用户身份上。确保用户访问权限是由用户管理员申请，由系统所有者批准，由安全责任人执行。将用户身份和访问权限保存在中央存储库中。部署成本效益技术和程序测量，并且保持最新，以建立用户身份、执行身份认证和强制访问权限。

DS5.4 用户账户管理

采取一套用户账户管理程序来处理请求、建立、发布、暂停、更改和关闭用户账户及其相关用户权限。包括一个概述数据或系统的所有者分配访问权限的批准程序。这些程序应该应用到所有用户，包括管理者（特权用户）、内部和外部用户，应用到正常和紧急情况。与访问公司系统和信息相关的权利和职责被依照合同授予所有类型的用户。定期检查所有的账户及其相关的权限。

DS5.5 安全测试与监控

主动的测试和监控 IT 安全的实施。为确保被批准的企业信息安全基线得到维持，IT 安全应该被定期重新确认达标。日志和监控功能能够及早防止和/或检测并随后及时报告需要定位的不寻常和/或异常的活动。

DS5.6 安全事件定义

清晰定义和传达潜在安全事件的特征，以使它们能够被事件和问题管理流程正确的分级和处理。

DS5.7 安全技术保护

使得与安全相关的技术可以防止篡改，并且没有不必要地泄露安全文档。

DS5.8 密钥管理

确定管理密钥的生成、更换、收回、注销、分配、认证、储存、登录、使用和存档的政策和程序是适当的，以确保受到保护的密钥不被更改和未经授权的泄露。

DS5.9 恶意软件的预防、检测和纠正

在整个组织内部采取适当的（尤其是最新的安全补丁和病毒控制）预防性、检测性和纠正性的措施，保护信息系统和技术免受恶意软件（例如，病毒、蠕虫、间谍软件、垃圾邮件）的侵害。

DS5.10 网络安全

使用安全技术和相应的管理程序（例如，防火墙、安全设备、网络隔离、入侵检测）来授权访问和控制网络上的信息流。

DS5.11 敏感数据交换

通过可信任的途径或媒介交换敏感交易数据，对交换的数据采取相应的控制技术，这些控制应该能提供数据内容、数据提交证据、数据接收证据的真实性和不可抵赖性。

5.5.3. 管理指南

源自	输入
PO2	信息架构；数据分类
PO3	技术标准
PO9	风险评估
AI2	应用安全控制规范
DS1	OLAs

输出	到						
安全事件定义	DS8						
安全意识方面的具体培训需求	DS7						
流程绩效报告	ME1						
安全变更需求	AI6						
安全威胁和漏洞	PO9						
IT 安全计划和政策	DS11						

RACI 图

活动 \ 职能	首席执行官	首席财务官	业务执行经理	首席信息官	业务流程所有者	运营总监	首席架构师	开发总监	IT行政总监	项目管理官	合规、审计、风险和安全
定义和维护 IT 安全计划	I	C	C	A	C	C	C	C	I	I	R
定义、建立和操作一个身份（账户）管理流程			I	A	C	R	R	I			C
监控潜在的和当前的安全事件				A	I	R	C	C			R
定期检查和确认用户访问权限				I	A	C					R
为维护和保护密钥建立和维护程序				A		R			I		C
应用和维护技术和程序化控制以保护网络中的信息流				A	C	C	R	R			C
执行定期的脆弱性评估		I		A	I	C	C	C			R

RACI 图中，**R**esponsible 代表**执行**，**A**ccountable 代表**责任**，**C**onsulted 代表**商议**，**I**nformed 代表**告知**。

5.5.4. 目标和指标

5.5.5. 成熟度模型

管理“确保系统安全”流程，使 IT 满足业务需求：维护信息的完整性，处理基础设施，最小化安全漏洞和事件对业务的影响。

0 级 无级别

组织没有认识到 IT 安全的必要性。责任和义务没有被分配以确保安全。没有应用支持 IT 安全管理的测量。没有 IT 安全报告，并且对 IT 安全破坏没有响应流程。完全缺乏一个可识别的系统安全管理流程。

1 级 初始级

组织认识到需要 IT 安全。需要 IT 安全的意识主要依赖于个体。IT 安全还是被动处理。IT 安全没有测量。由于责任不清，被检测到 IT 安全破坏时会导致相关部门互相推诿扯皮。对 IT 安全破坏的响应是不可预测的。

2 级 可重复级

IT 安全的责任和义务被分配给了 IT 安全协调员，尽管安全协调员的管理权是有限的。需要 IT 安全的意识是零散而有限的。虽然与安全相关的信息由系统产生，但是这些信息没有被分析。第三方服务不能处理组织的具体安全需要。制订了安全政策，但是技能和工具不足。IT 安全报告是不完整的、误导的或者不相关的。安全培训是有效的，但是主要由个体主动承担。IT 安全主要被看作是 IT 部门的责任和事情，业务部门认为 IT 安全与他们无关。

3 级 定义级

存在安全意识并由管理层进行促进。定义了符合 IT 安全策略的 IT 安全程序。IT 安全的责任被分配和理解，但没有被一贯地强制执行。由于风险分析的驱动，存在一个 IT 安全计划和安全解决方案。安全报告中没有包括清晰的业务重点。实施了专门的安全测试(例如，入侵测试)。为 IT 和业务部门提供了有效的安全培训，但是没有正式的计划和管理。

4 级 可管理级

IT 安全的责任被明确分配、管理和强制执行。持续进行 IT 安全风险和影响分析。安全策略和程序与具体的安全基线一起被完善。提升安全意识的方法是强制性的。用户识别、认证和授权是规范化的。要求负责审计和安全管理的员工进行安全认证。按照标准和正式的流程进行安全测试，并且有助于安全水平的提高。IT 安全流程和组织的整体安全功能相协调。IT 安全报告与业务目标相关联。业务和 IT 部门都进行 IT 安全培训。根据业务需求和定义的安全风险概要，制订计划并管理 IT 安全培训。已经定义了安全管理的目标和指标，但是没有测量。

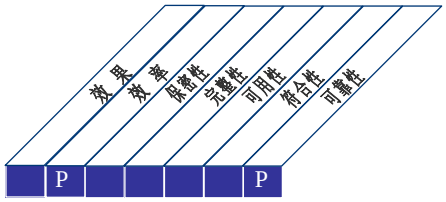
5 级 优化级

IT 安全是业务部门和 IT 管理部门的共同责任，并且被整合到公司的安全业务目标中。IT 安全需求被清晰的定义、优化并被包括在一个已批准的安全计划中。用户和客户对定义安全需求的责任感日益增强，并且安全功能在设计阶段就被整合到应用中。安全事件能够被自动化工具支持下的正式的事件响应程序迅速定位。定期实施安全评估，以评价安全计划的实施效果。有关威胁和漏洞的信息被系统的收集和分析。降低风险的充分的控制措施得到快速沟通和执行。安全测试、对安全事件的根本原因分析和对风险的预先识别被用于持续的流程改进。安全流程和技术在组织范围内被整合。安全管理的标准被测量、收集和沟通。管理层利用这些测量结果在持续改进流程中调整安全计划。

5.6. DS6 成本确认和分摊

5.6.1. 流程描述

为建立一个可以公平和公正地分摊 IT 成本到业务部门的体系，需要精确地测量 IT 成本并且和业务用户在分配的公平性方面达成一致。这个流程包括建立和运营一个体系，用于获取、分摊和报告 IT 成本给服务的用户。一个公平的分摊体系能够使业务部门对 IT 服务的使用做出更多正确的判断和明智的决定。



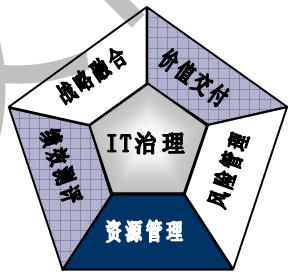
控制 IT 流程：
成本确认和分摊

使 IT 满足业务需求：
确保 IT 成本的透明性和可理解性，并通过使用快速广泛的 IT 服务改进成本效益

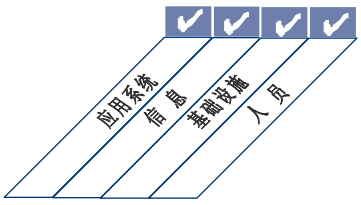
通过关注于：
IT 成本完整和准确的获取，经业务用户同意的公平的分摊体系，和及时报告 IT 使用和成本分摊的体系

通过下列实现：
- 根据提供服务的数量和质量调整收费
- 建立并同意一个完整的成本模型
- 按照协商一致的政策实施收费

通过下列衡量：
- 业务管理部门承认/支付 IT 服务账单的百分比
- 预算、预测和实际成本不一致的百分比
- 全部 IT 成本中按照协商一致的成本模型分摊的百分比



■ 主要 ■ 次要



5.6.2. 控制目标

DS6.1 服务的定义

识别所有的 IT 成本，并将它们映射到 IT 服务中，以支持一个透明的成本模型。IT 服务应该连接到业务流程中，使得业务部门能够识别相关的服务账单级别。

DS6.2 IT 成本核算

依据企业成本模型获取和分摊实际成本。预测与实际成本之间的差异应该遵照企业的财务测量体系进行分析和报告。

DS6.3 成本模型和收费

建立和使用基于服务定义的 IT 成本模型，以支持按服务进行内部收费率的计算。IT 成本模型应该确保用户可以识别、计量和预测服务的收费，促进资源的合理利用。

DS6.4 成本模型的维护

定期审查和校准成本/计费模型的适当性，维护不断发展的业务和 IT 活动的相关性和适当性。

DS6 成本确认和分摊

5.6.3. 管理指南

源自	输入
PO4	文档记录的系统所有者
PO5	成本-收益报告，IT 预算
PO10	详细的项目计划
DS1	SLAs 和 OLAs

输出	到						
IT 财务	PO5						
流程绩效报告	ME1						

RACI 图

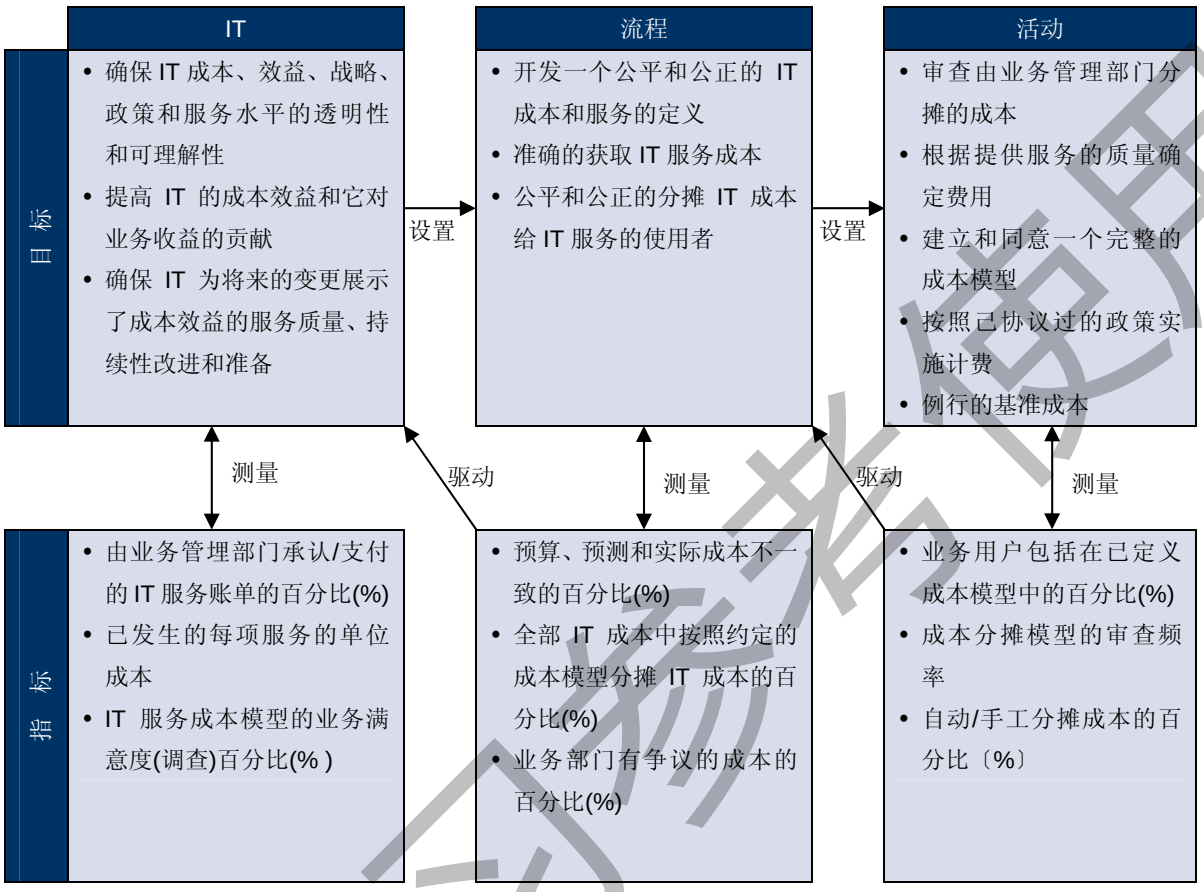
职能

活动

活动		首席执行官	首席财务官	业务执行经理	首席信息官	业务流程所有者	运营总监	首席架构师	开发总监	IT行政总监	项目管理官	合规、审计、风险和安全
将 IT 基础设施映射到提供的服务/支持的业务流程中		C	C	A	C	C	C	C	R	C		
识别所有的 IT 成本（例如，人员，技术）并以单位成本为基础将它们映射到 IT 服务中		C		A		C	C	C	R	C		
建立和维护 IT 会计和成本控制流程		C	C	A	C	C	C	C	R	C		
建立和维护计费政策和程序		C	C	A	C	C	C	C	R	C		

RACI 图中，**R**esponsible 代表**执行**，**A**ccountable 代表**责任**，**C**onsulted 代表**商议**，**I**nformed 代表**告知**。

5.6.4. 目标和指标



5.6.5. 成熟度模型

管理“成本确认和分摊”流程，使 IT 满足业务要求：确保 IT 成本的透明性和可理解性及通过 IT 服务快速广泛的使用改进成本效益。

0 级 无级别

完全缺乏任何可识别的流程，用于确认和分摊所提供信息服务的成本。组织甚至没有意识到，关于成本核算存在有待处理的问题，并且该问题没有得到任何传达。

1 级 初始级

对信息服务的整体成本有一个大致的了解，但是没有按照每一用户、客户、部门、用户组、服务功能、项目或可交付的服务对成本进行细分。事实上不存在成本监控，仅仅把整体成本报告给管理层。把 IT 成本做为一般运行开销分摊。不向业务部门提供有关 IT 服务成本或效益的任何信息。

2 级 可重复级

对需要确认和分摊成本有一个整体的认识。成本分摊是基于非正式的或原始的成本假设，如硬件成本，而且事实上没有与价值驱动连接起来；成本分摊流程是可重复的。对标准的成本确认和分摊程序没有进行正式的培训和传达；没有分配收集和分摊成本的责任。

3 级 定义级

有一个已定义和文档化的信息服务成本模型。定义了将 IT 成本与提供给用户的服务联系起来的流程。对将 IT 成本分摊到 IT 服务有一个适当水平的认识。向业务部门提供成本的原始信息。

4 级 可管理级

信息服务成本管理的责任和义务被定义且被各级管理层充分理解，并得到正式的培训支持。直接和间接的成本被及时和自动地确认并报告给管理层、业务流程的所有者和用户。通常情况下，对成本进行了监控和评估，并且在发现成本偏离预算时采取了相应的措施。将信息服务成本的报告与业务目标和 SLAs 联系起来，并且得到业务流程所有者的监控。财务部门审核成本分摊流程的合理性。有一个自动的成本核算系统，但它更关注于信息服务功能，而不是业务流程。对成本测量的目标和指标达成了一致，但未得到一致性测量。

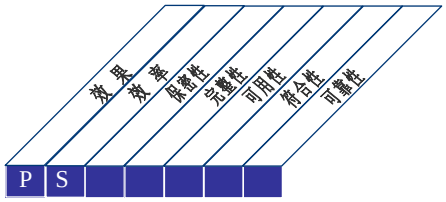
5 级 优化级

所提供服务的成本被识别、收集、总结并报告给管理层、业务流程所有者和用户。成本被识别为可计费项，并支持一个内部服务计费系统，基于用户的使用情况对提供的服务进行适当的收费。成本的详细说明支持 SLAs。服务成本的监控和评估被用于优化 IT 资源的成本。获得的成本数据用于确认组织的预算流程中所实现的效益。通过智能报告系统，信息服务成本的报告对业务需求的变化提供早期预警。由于每个服务的处理量不同，而采用了一个可变的成本模型。基于持续改善和借鉴其他组织的成果，成本管理被细化到一个行业实践的水平。成本优化是一个持续进行的流程。管理层审核成本管理的目标和指标，并将其作为在重新设计成本测量系统时持续改善流程的一部分。

5.7. DS7 教育和培训用户

5.7.1. 流程描述

IT 系统所有用户（包括 IT 内部的用户）的有效培训，需要识别每个用户组的培训需求。除了识别培训需求外，这个流程还包括为有效的培训和衡量培训结果制定和执行一套策略。一个有效的培训计划可以通过减少用户差错、提高生产力和提高关键控制的遵循性来提高技术的有效使用，例如用户安全措施。



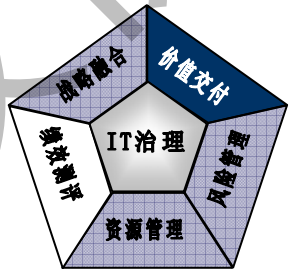
控制 IT 流程：
教育和培训用户

使 IT 满足业务需求：
有效和高效的使用应用和技术解决方案，确保用户遵循政策和程序

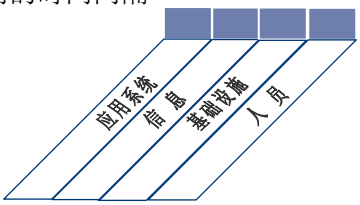
通过关注于：
清晰地理解 IT 用户的培训需求，有效的培训策略的实施和培训结果的评估

通过下列实现：
- 制定培训课程
- 组织培训
- 实施培训
- 监控并报告培训的有效性

通过下列衡量：
- 由于用户缺乏培训而呼叫服务台的次数
- 利益相关者对实施培训的满意度的百分比
- 识别培训需求和实施培训之间的时间间隔



主要　次要



5.7.2. 控制目标

DS7.1 教育和培训需求的识别

为每个目标团队的员工制定课程并定期更新时要考虑如下因素：

- 当前和未来业务需要和战略
- 信息作为一种资产的价值
- 公司价值（包括道德价值、控制和安全文化等）
- 新 IT 基础设施和软件的应用（例如，软件包、应用软件）
- 当前和未来的技能、个人竞争能力、证书和证书授予的需求以及要求资格的重新认证
- 提供培训的方式（例如，教室，基于网络的）、目标团队的规模、培训目标的可达性和培训时间安排

DS7.2 教育和培训的交付

以识别出的教育和培训需求为基础，确定培训目标团队和团队的人数、有效的培训机制、教师、培训师和顾问。任命培训师并及时组织培训。记录注册信息(包括资格条件)、出勤情况和培训效果评价。

DS7.3 培训评估

根据培训的实用性、质量、有效性、知识的掌握程度、成本和效益等方面的完成情况，评价教育和培训内容的交付。评价的结果为今后制定培训方案和培训计划和交付培训提供依据。

5.7.3. 管理指南

源自	输入
PO7	用户的技能和上岗资格，包括个人培训；特定培训的需求
AI4	培训教材，为落实解决方案的知识转移需求
DS1	OLAs（运营水平协议）
DS5	在安全意识方面特定的培训需求
DS8	用户满意度报告

输出	到						
流程绩效报告	ME1						
所需文档的更新资料	AI4						

RACI 图

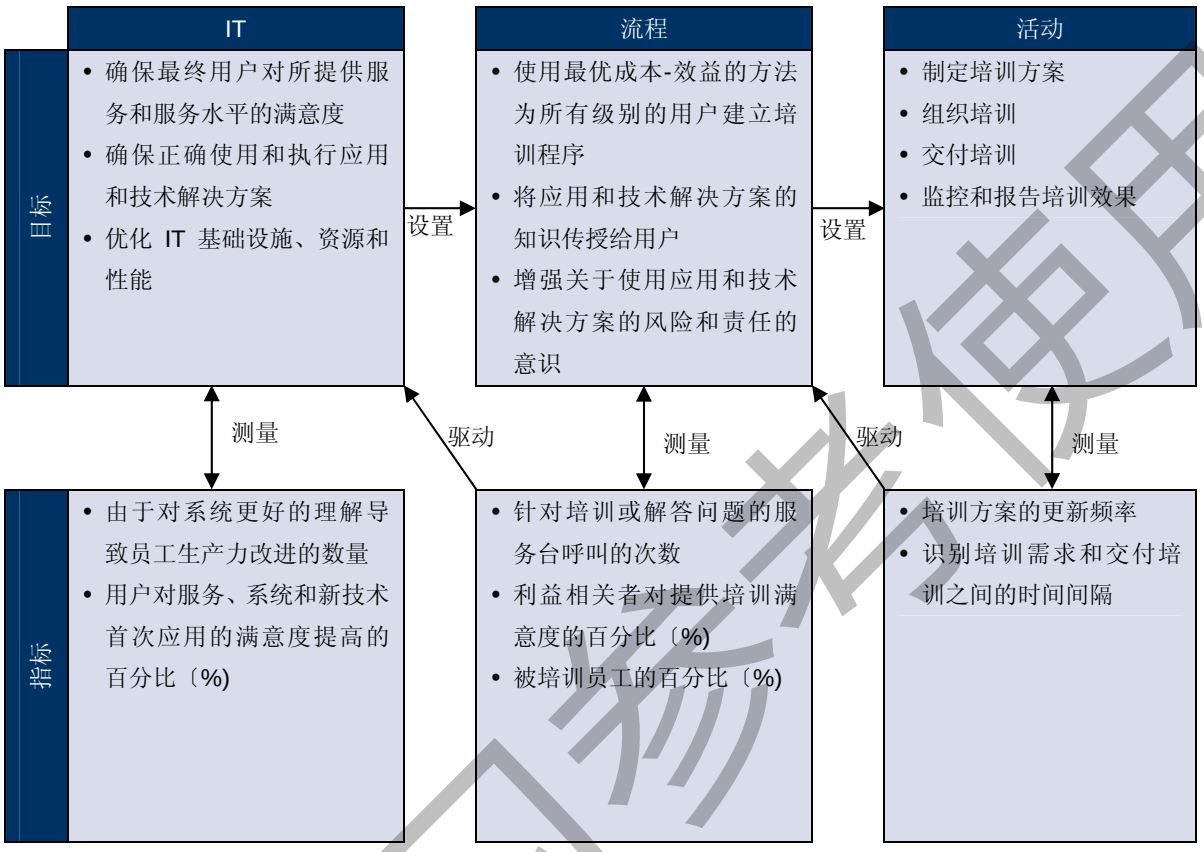
职能

活动

活动	首席执行官	首席财务官	业务执行经理	首席信息官	业务流程所有者	运营总监	首席架构师	开发总监	IT行政总监	项目管理官	合规、审计、风险和安全	培训部
识别和区分用户的培训需求			C	A	R	C	C	C	C	C	C	R
建立培训计划			C	A	R	C	I	C	C	C	I	R
传达意识、教育和培训活动			I	A	C	C	I	C	C	C	I	R
执行培训评估			I	A	R	C	I	C	C	C	I	R
识别并评估最佳的培训交付方法和工具			I	A/R	R	C	C	C	C	C	C	R

RACI 图中，**R**esponsible 代表**执行**，**A**ccountable 代表**责任**，**C**onsulted 代表**商议**，**I**nformed 代表**告知**。

5.7.4. 目标和指标



5.7.5. 成熟度模型

管理“教育和培训用户”流程，使 IT 满足业务需求：为有效地和高效率地使用应用系统和技术解决方案，确保用户与培训政策和程序的符合性。

0 级 无级别

组织内部完全没有教育和培训计划。组织甚至未意识到存在培训的问题需要解决，并且对培训的问题缺乏沟通。

1 级 初始级

有证据证明，组织已经意识到了对教育和培训计划的需求，但是没有形成标准化的流程。在缺少组织计划的情况下，员工自发的识别并参与培训课程。其中一些培训课程讲述道德规范、系统安全意识和安全实践等课题。整个培训的管理方法缺少凝聚力，在处理有关教育和培训的问题和方法上，仅仅存在零星和不一致的沟通。

2 级 可重复级

有贯穿组织的需要教育和培训计划以及与该计划相关流程的意识。培训开始在员工的个人绩效计划中被识别。教育培训流程发展到不同的教师用不同的方法讲授相同主题的非正式培训教育课程的阶段。其中一些培训课程讲述道德规范、系统安全意识和实践等课题。培训高度依赖个人的知识。但在所有问题和处理这些问题的需求上的沟通是一致的。

3 级 定义级

制定并传达了教育和培训计划。员工和管理人员识别并文档化培训需求。培训和教育流程被标准化和文档化。确定了预算、资源、设施和培训师来支持培训和教育计划。给员工开设了道德规范、系统安全意识和实践方面的正式课程。大部分培训和教育流程受到监控，但不是所有的偏离都能被管理层检测到。偶尔对培训和教育中出现的问题进行分析。

4 级 可管理级

有一个可测量结果的全面的培训和教育计划。培训职责清晰，确定了培训流程所有权。培训和教育成为员工职业生涯的组成部分。管理层支持并参与培训和教育会议。所有的员工都接受了道德规范和系统安全意识的培训。为保护系统免受影响可用性、机密性和完整性的故障的侵害，所有员工都接受了适当级别的系统安全实践培训。管理层通过不断地审阅和更新培训和教育计划及流程来监控遵循性。培训和教育流程不断地改进，并强制执行最佳的内部实践。

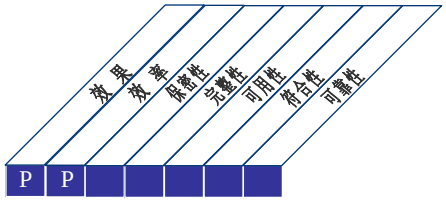
5 级 优化级

培训和教育导致个人绩效的改进。培训和教育成为员工职业生涯发展的关键组成部分。为培训和教育计划提供了充足的预算、资源、设施和讲师。利用外部最佳实践和其他组织的成熟度模型作为评价基准，培训和教育流程被精细化并实施持续改进。分析了产生问题和偏差的根本原因，适当地识别和采取了有效的行动。对道德规范和系统安全法则有正确的态度。IT 被以广泛的、综合的和优化的方式用于自动化操作，并为培训和教育计划提供工具。有不同类别的外部培训专家参与，并且采用同业基准作为指引。

5.8. DS8 服务台和事件管理

5.8.1. 流程描述

为及时有效地响应 IT 用户的查询和问题，需要一个精心设计和有效执行的服务台和紧急事件管理流程。这个流程包括设定服务台的功能，用来登记、处理事件升级、进行趋势和根本原因分析，以及提供解决方案。企业利益包括通过快速的响应用户的查询来提高生产率，另外，企业可以通过有效的报告找到根本原因（例如，用户培训不足）。



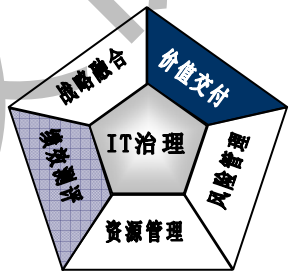
控制 IT 流程：
服务台和事件管理

使 IT 满足业务需求：
通过确保对最终用户的查询、问题和事件的解决和分析，能够使 IT 系统有效的使用

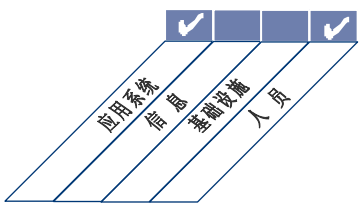
通过关注于：
具有快速响应、清晰的升级程序、解决问题和趋势分析等专业的服务台功能

通过下列实现：
- 安装和运行服务台
- 监控和报告趋势
- 定义清晰的逐步升级的标准和程序

通过下列衡量：
- 一线支持的用户满意度
- 在约定的/可接受的时间周期内事件解决的百分比
- 呼叫放弃率



■ 主要　▦ 次要



5.8.2. 控制目标

DS8.1 服务台

建立服务台功能，它是用户与 IT 系统的接口，用来进行登记、沟通、调度和分析所有呼叫、报告的事件、服务请求和信息需求。应该有监控和逐步升级程序，它们基于预先签订的与适当服务水平协议（SLA）相关的服务水平，这些程序允许对任何报告的问题，例如，事件、服务请求或信息需求进行分类和排定不同优先级。通过服务台和 IT 服务的质量测量最终用户的满意度。

DS8.2 登记客户查询

建立一个功能和系统，以记录和跟踪呼叫、事件、服务请求和信息需求。这个系统应该与事件管理、问题管理、变更管理、容量管理和可用性管理等流程一起紧密工作。事件应该按照业务和服务的优先级分类，并且在需要的地方传递给适当的问题管理团队。客户应该被告知他们的查询的状态。

DS8.3 事件的逐步升级

建立服务台程序，使不能立即解决的事件按照 SLA 中定义的限度适当地逐步升级，如果合适的话，应该提供临时解决方法。确保基于用户的事件（无论该事件是否有 IT 团队正在研究解决途径）的归属和生命周期的监控依然保留在服务台。

DS8.4 事件关闭

建立及时监控客户查询解除的程序。当事件已经被解决，确保服务台记录了问题解决的步骤，确认客户已经同意所采取的行动。也记录和报告未解决的事件（已知错误和临时解决方法）为问题管理团队提供信息。

DS8.5 报告和趋势分析

产生服务台的运行报告，使管理者能够测量服务绩效、服务响应时间，识别趋势或重复发生的问题，使服务得到持续的改进。

5.8.3. 管理指南

源自	输入
AI4	用户、运营、支持、技术和管理手册
AI6	变更授权
AI7	发布配置项目
DS1	SLAs 和 OLAs
DS4	事件/灾难的阈值
DS5	安全事件的定义
DS9	IT 配置/资产列表
DS10	已知问题、已知错误和临时解决方法
DS13	事件标签

输出	到						
服务请求/变更要求（RFC）	AI6						
事件报告	DS10						
流程绩效报告	ME1						
用户满意度报告	DS7	ME1					

RACI 图

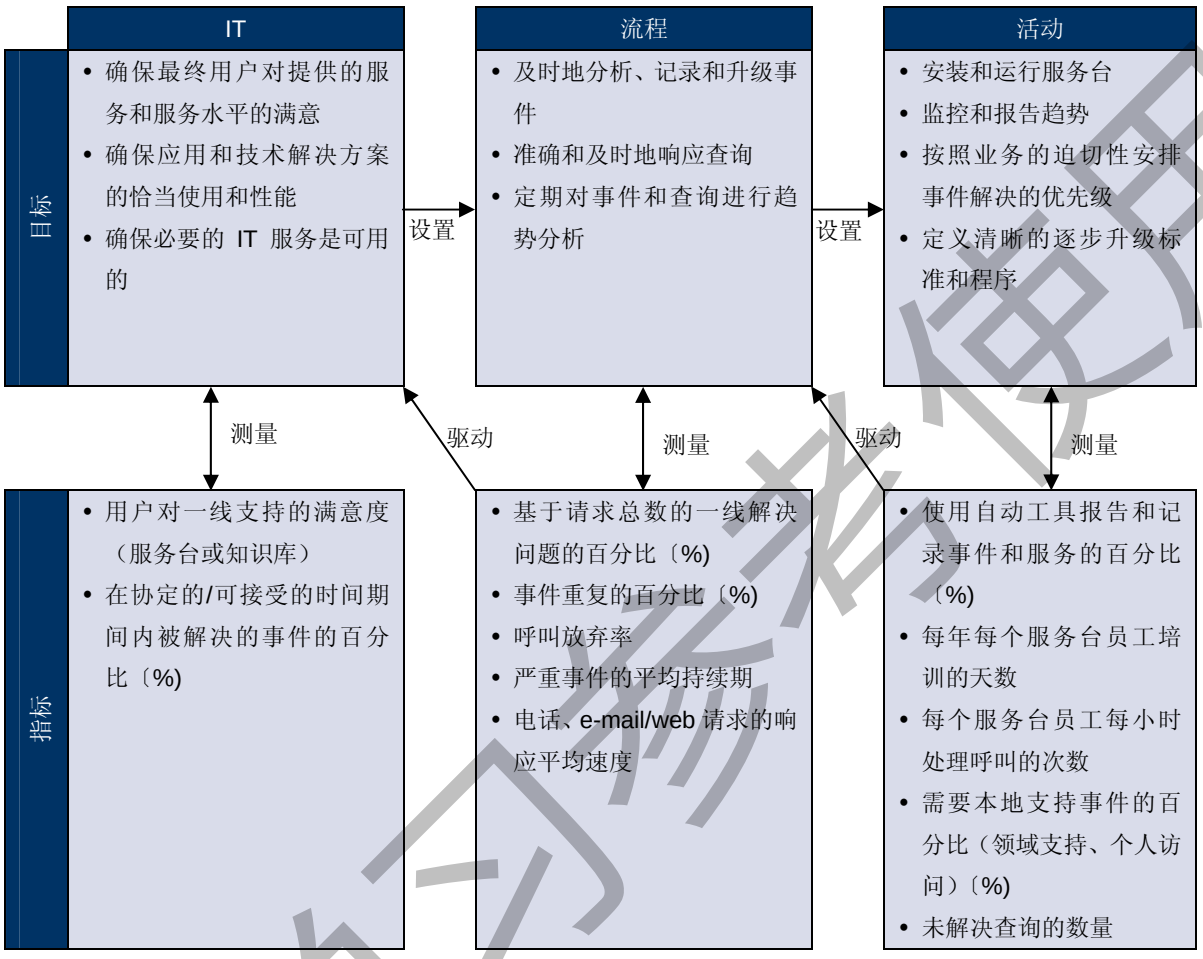
职能

活动

活动	首席执行官	首席财务官	业务执行经理	首席信息官	业务流程所有者	运营总监	首席架构师	开发总监	IT行政总监	项目管理官	合规、审计、风险和安全	服务台和事件管理者
建立分类（严重性和影响）和逐步升级程序（功能和等级）				C	C	C	C	C	C		C	A/R
检测和记录事件/服务需求/信息需求												A/R
分类、调查和诊断查询				I		C	C	C			I	A/R
解决、复原和关闭事件					I	R	R	R			C	A/R
通知客户（例如问题更新状态）				I	I							A/R
生成管理报告	I			I	I	I			I		I	A/R

RACI 图中，**R**esponsible 代表**执行**，**A**ccountable 代表**责任**，**C**onsulted 代表**商议**，**I**nformed 代表**告知**。

5.8.4. 目标和指标



5.8.5. 成熟度模型

管理“服务台和事件管理”流程，使 IT 满足业务需求：通过确保对最终用户的查询、问题和事件的解决和分析，使 IT 系统得到有效的使用。

0 级 无级别

不存在解决用户疑问和问题的支持。完全缺乏一个事件管理流程。组织没有意识到这个问题需要解决。

1 级 初始级

管理层认识到需要一个由各种工具和员工来支撑的流程，以便响应用户查询并管理事件的解决。然而没有标准化的流程，并且仅提供被动支持。管理层没有监控用户查询、事件或趋势。没有逐步升级流程，以确保问题得到解决。

2 级 可重复级

组织意识到需要服务台功能和事件管理流程。由经验丰富的个体组成的非正式网络能够提供有用的帮助。这些个体拥有一些可用的常用工具来辅助解决事件。没有对标准程序进行正规培训和传达，并且责任由个体承担。

3 级 定义级

对服务台功能和事件管理流程的需要被识别和接受。程序被标准化和文档化，并正在进行非正规培训。然而是否获得培训和遵守标准要依赖于个体。开发了常见问题库（FAQs）和用户指引手册，但是个体必须找到它们并且可能不遵守它们。查询和事件被以人工方式跟踪和个别地监控，但是没有一个正式的报告系统。查询和事件的及时响应情况没有被测量，事件可能未被解决。用户已经得到明确的沟通，知道在哪里和怎么报告问题和事件。

4 级 可管理级

在组织的所有层面，充分认识到事件管理流程的好处，并且在合适的组织单元中建立了服务台功能。通过集中式知识库，实现技术和工具的自动化使用。服务台员工与问题管理员工密切合作。职责清晰，有效性受到监控。建立并使相关人员知晓传递、升级和解决事件的程序。服务台员工经过培训，并且流程被运用专用软件进行了改进。管理层制定了服务台性能评价指标。

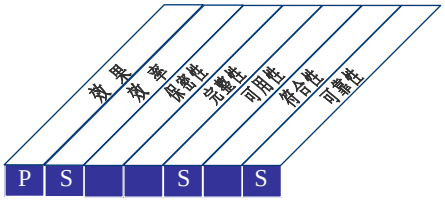
5 级 优化级

事件管理流程和服务台功能被建立和精心组织，并且具有知识化、以客户为中心和有帮助的客户服务定位。标准被系统地测量和报告。广泛而全面的常见问题库是知识库的主要部分。提供适当的工具使用户能够自我诊断并解决事件。建议是一致的，并且事件在结构化的升级流程中得到快速解决。管理层运用一个集成化工具进行事件管理流程和服务台功能的绩效统计。基于性能指标分析结果、持续改进和其它组织基准，流程已经被改进到最佳行业实践的水平。

5.9. DS9 配置管理

5.9.1. 流程描述

需要建立和维护一个准确和全面的配置库，确保硬件和软件配置信息的完整性。这个流程包括收集初始配置信息、建立基线、验证和审计配置信息，并在需要的时候更新配置库。有效的配置管理能促进更高的系统可用性、生产问题最小化和更快的解决问题。



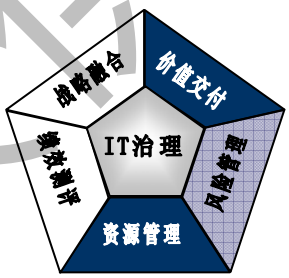
控制 IT 流程：
配置管理

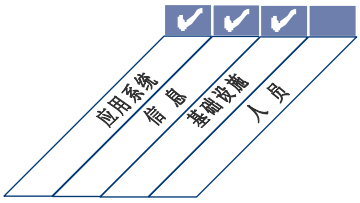
使 IT 满足业务需求：
优化 IT 基础设施、资源和容量，核算 IT 资产

通过关注于：
建立和维护一个包括资产配置属性和基线的准确和完整的配置库，并与实际资产配置进行比较

通过下列实现：
- 建立一个包括所有配置项的中心配置库
- 识别和维护配置项
- 检查配置数据的完整性

通过下列衡量：
- 由不适当的资产配置引起的业务遵循性问题的数量
- 已经识别的配置库和实际资产配置之间的偏差的数量
- 已购买但没有在配置库中核算的许可证的百分比





主要　　次要

5.9.2. 控制目标

DS9.1 配置库和基线

建立一个支持工具和中心配置库，以便包含配置项中的所有相关信息。监控和记录所有的资产和资产的变更。为每一个系统和服务保留一个配置项基线作为变动后返回的检查点。

DS9.2 配置项的标识和维护

建立配置程序以支持对配置库的所有改变的管理和记录。将这些程序与变更管理、事件管理和问题管理程序集成。

DS9.3 配置的完整性检查

定期检查配置数据以便检验和确认当前和历史配置的完整性。参照软件使用政策定期检查已安装的软件，以识别私自安装的、没有许可证的或者任何超出当前许可协议的软件的事例。报告、应对并纠正错误和偏差。

5.9.3. 管理指南

源自	输入
AI4	用户、运营、支持、技术和管理手册
AI7	发布的配置项
DS4	IT 配置项的重要性

输出	到						
IT 配置/资产明细	DS8	DS10	DS13				
变更请求（在何处和如何实施调整）	AI6						
流程绩效报告	ME1						

RACI 图

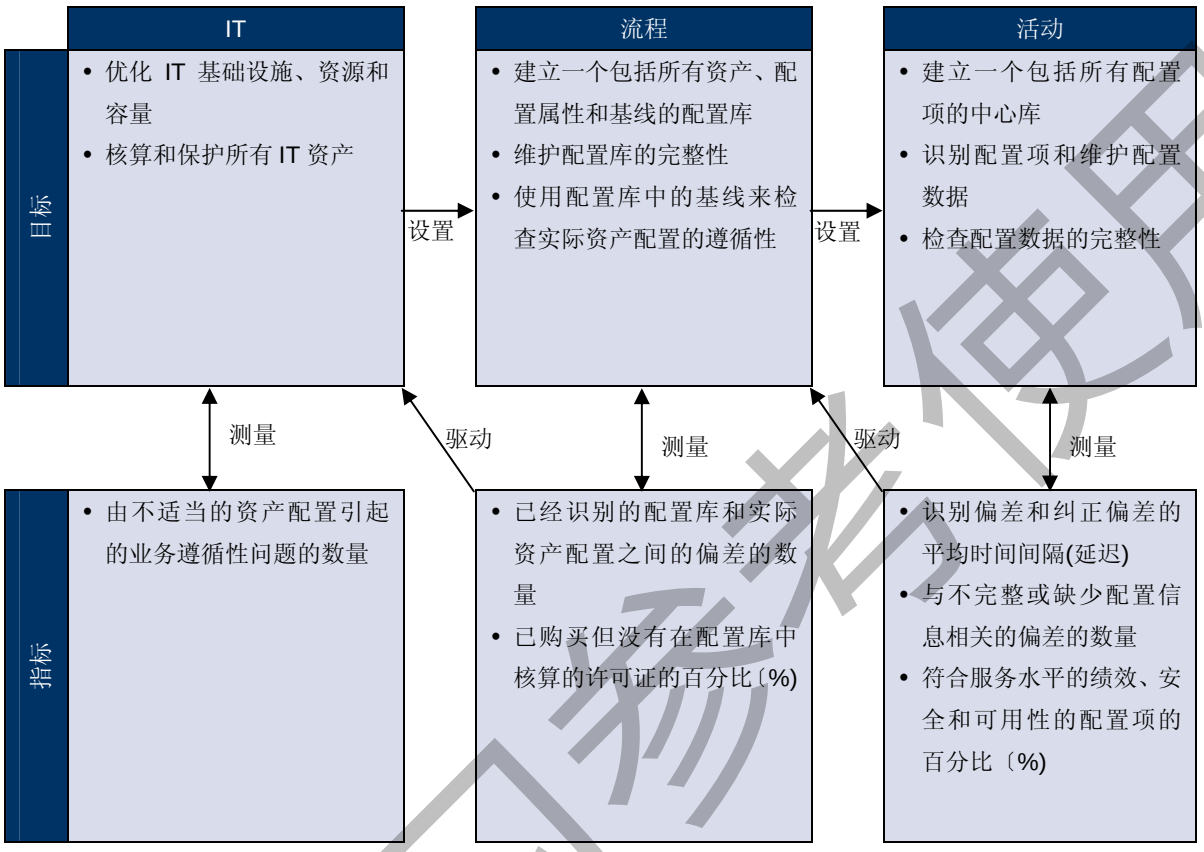
职能

活动

	首席执行官	首席财务官	业务执行经理	首席信息官	业务流程所有者	运营总监	首席架构师	开发总监	IT行政总监	项目管理官	合规、审计、风险和安全	配置管理经理
开发配置管理计划程序					C	A	C	I	C		C	R
收集初始配置信息和建立基线						C	C	C			I	A/R
检验和审计配置信息（包括检测未许可软件）		I				A			I		I	A/R
更新配置库						R	R	R			I	A/R

RACI 图中，**R**esponsible 代表**执行**，**A**ccountable 代表**责任**，**C**onsulted 代表**商议**，**I**nformed 代表**告知**。

5.9.4. 目标和指标



5.9.5. 成熟度模型

管理“配置管理”流程，使 IT 满足业务需求：优化 IT 基础设施、资源和容量，并核算 IT 资产。

0 级 无级别

管理层不了解拥有一个可以报告和管理 IT 基础设施（包括硬件和软件配置）的流程的好处。

1 级 初始级

认识到配置管理的需要。在个体行为的基础上执行基本的配置管理任务，例如维护软硬件的目录。没有定义标准作法。

2 级 可重复级

管理层认识到控制 IT 配置的需要并理解到准确和全面配置信息的好处，但是存在对技术人员知识和专家经验的绝对依靠。配置管理工具的使用达到了一定程度，但是在各个平台上有所不同。没有规定标准的工作法。配置数据内容是有限的，而且没有被诸如变更管理和问题管理等相关的流程使用。

3 级 定义级

程序和工作法被书面化、标准化和传达，但是标准的培训和应用依赖于个体。相似的配置管理工具正在被跨平台使用。程序的偏差未必能被发现，而且物理验证被不一致地执行。出现一些协助追踪设备和软件变更的自动化工具。配置数据正在被相关的流程使用。

4 级 可管理级

管理配置的需要被组织的所有层面认可，并且好的实践得到持续推进。程序和标准被传达和并入到培训，而且偏差被监控、追踪和报告。自动化的工具，例如推送技术，被利用来实施标准和提高稳定性。配置管理系统覆盖了几乎所有的 IT 资产而且允许适当的发布管理和分发控制。跟物理验证一样，例外分析被一贯地应用，而且这些例外发生的根本原因得到调查。

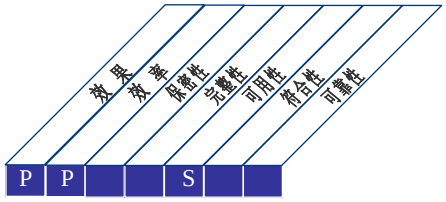
5 级 优化级

所有 IT 资产在一个中心配置管理系统中管理，这个系统包含着关于组件、组件的相互关系和事件的所有必需的信息。配置数据与厂商目录相一致。存在对相关的流程充分的整合，而且相关流程用自动化的方式使用和更新配置数据。基线审计报告为每一个个体单元的修理、维护、授权、升级和技术评估提供了必须的硬件和软件数据。限制安装未经授权软件的规定是强制性的。管理层利用分析报告来预测修理和升级，并提供预定的升级和技术更新能力。对个体 IT 资产进行跟踪和监控，保护它们不被偷窃、错用和滥用。

5.10. DS10 问题管理

5.10.1. 流程描述

有效的问题管理需要识别和分类问题，分析问题根本原因并解决问题。问题管理流程也包括改进建议的制定、问题记录的维护和纠正操作状态的审阅。一个有效的问题管理流程能最大化系统的可用性，改进服务水平，减少成本和改进客户方便性和满意度。



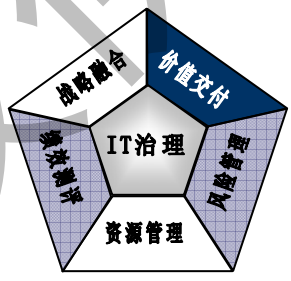
控制 IT 流程：
问题管理

使 IT 满足业务需求：
确保最终用户对服务提供和服务水平的满意度，并且减少处理和服务交付的过失和返工

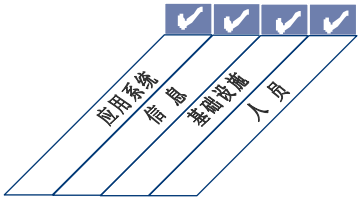
通过关注于：
记录、跟踪和解决运营问题；研究所有重要问题的根本原因；为识别出运营问题而制定解决方案

通过下列实现：
- 执行已报告问题的根本原因分析
- 分析趋势
- 获取问题所有权并且促进问题的解决

通过下列衡量：
- 对业务有影响的复发问题的数量
- 规定期限内解决的问题的百分比
- 基于问题严重程度，持续的问题报告和升级频度



■ 主要 ▦ 次要



5.10.2. 控制目标

DS10.1 问题识别和分类

执行流程来报告和分类已经被识别为事件管理一部分的问题。问题分类的步骤和事件分类的步骤相类似；这些步骤分别是确定种类、影响、紧急程度和优先级。将问题正确的分类到相关的组或者域（举例，硬件、软件、支持软件）。这些组能够匹配用户和客户群的组织职责，并且这些职责应该是将问题分配给支持员工的基础。

DS10.2 问题跟踪和解决

确保问题管理系统提供了足够的审计追踪工具，来允许跟踪、分析和确定所有下述报告问题的根本原因：

- 所有关联的配置项
- 未解决的问题和事件
- 已知的和可疑的错误
- 问题趋势的跟踪

识别和启动可以接受的解决方案，查找根本原因，通过已建立的变更管理流程提出变更请求。在整个解决流程中，问题管理应该从变更管理获得问题和错误处理进程的定期报告。问题管理应该监控问题和已知错误对用户服务的持续影响。在一个影响变得严重的事件中，问题管理应该升级该问题，可能将它提交给一个适当的委员会来提高变更请求的优先级或者执行一个适当的紧急变更。根据服务水平协议来监控问题解决的进展。

DS10.3 问题关闭

在证实成功排除已知错误后，或者在与业务部门对如何处理问题达成一致后，引入适当的程序来关闭问题记录。

DS10.4 配置、事件和问题管理的集成

集成配置、事件和问题管理相关的流程以确保问题的有效管理，并且管理能够得到改进。

5.10.3. 管理指南

源自	输入
AI6	变更授权
DS8	事件报告
DS9	IT 配置/资产明细
DS13	错误日志

输出	到						
变更请求(何时和怎么应用修改)	AI6						
问题记录	AI6						
流程绩效报告	ME1						
已知问题、已知错误和临时解决方法	DS8						

RACI 图

职能

活动

活动	首席执行官	首席财务官	业务执行经理	首席信息官	业务流程所有者	运营总监	首席架构师	开发总监	IT行政总监	项目管理官	合规、审计、风险和安全	问题管理经理
识别和分类问题			I	I	C	A	C	C			I	R
执行根本原因分析						C		C				A/R
解决问题					C	A	R	R		R	C	C
审阅问题的状态			I	I	C	A/R	C	C		C	C	R
提出改进建议，并且创建相关变更请求					I	A	I	I		I		R
维护问题记录					I	I		I			I	A/R

RACI 图中，**R**esponsible 代表**执行**，**A**ccountable 代表**责任**，**C**onsulted 代表**商议**，**I**nformed 代表**告知**。

5.10.4. 目标和指标

5.10.5. 成熟度模型

管理“问题管理”流程，使 IT 满足业务需求：确保最终用户对服务提供和服务水平的满意度，并且减少问题解决和服务提供的不足和返工。

0 级 无级别

没有意识到问题管理的必要性，如问题和事件没有区别。因此，也没有尝试去识别事件的根本原因。

1 级 初始级

员工认识到管理问题并解决其根本原因的需求。拥有关键知识的员工提供一些与他们专业领域相关的问题的帮助，但是没有被分配问题管理的职责。信息没有共享，导致在寻找答案的过程中另外的问题发生和生产时间的损失。

2 级 可重复级

在业务单元和信息服务功能中，存在管理与 IT 相关问题所带来的利益和需求的广泛共识。解决流程已经发展到一定程度，少数关键人员为识别和解决问题负责。信息以非正式的和被动的方式在员工中共享。对用户的服务水平是不稳定的，并且受到问题管理的结构化知识缺乏的牵制。

3 级 定义级

有效的集成问题管理系统的需要被管理层接受和支持，人员配备和培训的预算是可用的。问题解决和升级流程被标准化。在响应团队内，问题和解决过程的记录和跟踪是散乱的，使用可用的未集成化工具。偏离已建立的规范和标准的情况可能没有检测出。信息以主动的和正式的形式在员工中共享。管理层对事件的检查，以及对问题识别和解决的分析是有限的和非正式的。

4 级 可管理级

问题管理流程得到组织内部所有层面的理解。建立了清晰的职责和所有权。方法和程序被文档化和传达，有效性得到测量。大多数问题被识别、记录和报告，并且问题的解决方案被启动。知识和专业技术被培养、维护，并且发展到较高水平，这种功能被视为实现 IT 目标和改进 IT 服务的一种资产和主要贡献者。问题管理流程与事件、变更、可用性和配置管理等相关流程适当整合，并且帮助客户管理其数据、工具和操作。商定了问题管理流程的目标和指标。

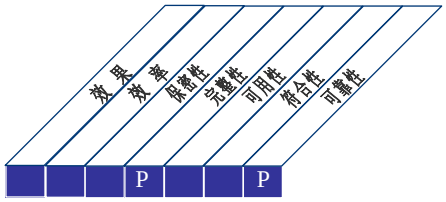
5 级 优化级

问题管理流程发展到一个有前瞻性的和主动的流程，有助于 IT 目标的实现。问题可以被预测和预防。通过与厂商和专家的定期联系，维护有关过去和未来问题模式的知识库。问题和解决过程的记录、报告和分析是自动化的，并且完全与配置数据管理整合在一起。目标始终被测量。绝大多数系统装备了自动检测和报警装置，以便持续地追踪和评估。基于对测量的分析，问题管理流程被持续改进，并且报告给利益相关方

5.11. DS11 数据管理

5.11.1. 流程描述

有效的数据管理需要识别数据需求，数据管理流程也包括建立有效的管理程序，以管理介质库、数据的备份和恢复、介质的恰当处理。有效的数据管理有助于确保业务数据的质量、及时性和有效性。



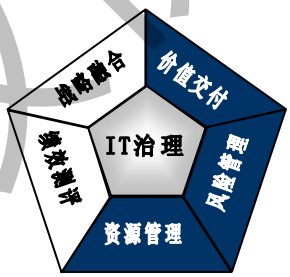
控制 IT 流程：
数据管理

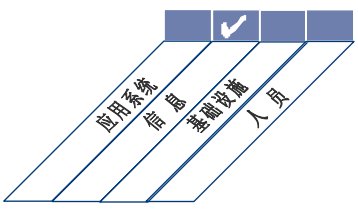
使 IT 满足业务需求：
优化信息的使用，确保在需要时信息的可用性

通过关注于：
维护数据的完整性、准确性、可用性和保护

通过下列实现：
- 备份数据和测试恢复
- 管理本地和异地的数据存储
- 数据和设备的安全处理

通过下列衡量：
- 用户对数据有效性的满意度
- 数据成功恢复的百分比
- 在介质被处理之后敏感数据被恢复的事件的数量





■ 主要 ■ 次要

5.11.2. 控制目标

DS11.1 数据管理的业务需求

检验所有预期处理的数据被完整、准确、及时的接收和处理，所有已交付的输出符合业务需求。支持重新开始和重新处理的需求。

DS11.2 存储和保管方案

制定和实施有效的数据存储、保留和归档流程以满足业务目标、组织的安全政策和控制需求。

DS11.3 介质库管理系统

制定和实施程序，以维护一个被存储和归档的介质目录，确保介质的可用性和完整性。

DS11.4 销毁

制定和实施程序，确保数据和硬件的销毁或转移符合敏感数据和软件保护的业务需求。

DS11.5 备份和恢复

制定和实施符合业务需求和持续性计划的程序，以备份和恢复系统、应用程序、数据和文档。

DS11.6 数据管理的安全需求

制定和实施政策和程序，以识别和应用数据的接收、处理、存储和输出的安全需求，满足业务目标、组织的安全策略和规章的要求。

5.11.3. 管理指南

源自	输入
PO2	数据字典；划分数据类别
AI4	用户、操作、支持、技术和管理手册
DS1	运营水平协议
DS4	备份存储和保护计划
DS5	IT 安全计划和政策

输出	到						
流程绩效报告	ME1						
数据管理的操作指南	DS13						

RACI 图

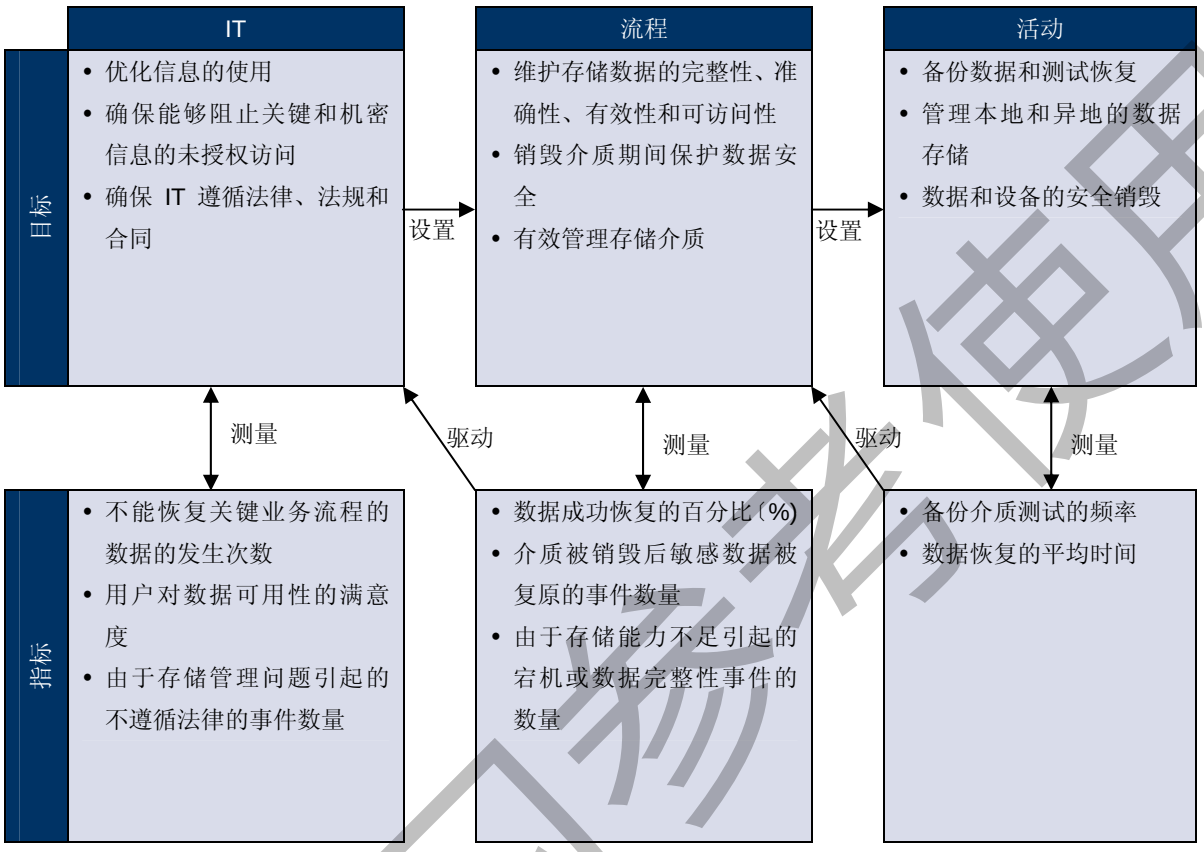
职能

活动

活动	首席执行官	首席财务官	业务执行经理	首席信息官	业务流程所有者	运营总监	首席架构师	开发总监	IT行政总监	项目管理官	合规、审计、风险和安全
把数据存储和保存需求转变成程序				A	I	C	R				C
定义、维护和实施管理介质库的程序				A		R	C	C	I		C
定义、维护和实施介质和设备安全销毁的程序				A	C	R			I		C
根据计划备份数据				A		R					
定义、维护和实施数据恢复程序				A	C	R	C	C			I

RACI 图中，**R**esponsible 代表**执行**，**A**ccountable 代表**责任**，**C**onsulted 代表**商议**，**I**nformed 代表**告知**。

5.11.4. 目标和指标



5.11.5. 成熟度模型

管理“数据管理”流程，使 IT 满足业务需求：优化信息的使用，确保在需要时信息是可用的。

0 级 无级别

没有认识到数据是公司资源和资产。没有为数据管理指定数据所有权或个体职责。数据质量和安全性很差或不存在。

1 级 初始级

组织认识到有效数据管理的需要。有一个专门方法来详细说明数据管理的安全需求，但没有一个正式的沟通程序。没有进行数据管理的具体培训。数据管理的职责不清晰。有恰当的备份/恢复程序和销毁方案。

2 级 可重复级

整个组织都有需要有效的数据管理的意识。高级别的数据所有权开始出现。数据管理的安全需求由关键个体文件化。对数据管理的关键活动(例如，备份、恢复、销毁）进行了一些 IT 内部的监控。数据管理职责被非正式的分配给关键 IT 人员。

3 级 定义级

在 IT 内部和整个组织范围内数据管理的需要被理解和认可。已建立数据管理职责。数据的所有权被分配给控制数据完整性和机密性的可靠团队。数据管理程序在 IT 内部被正式化，并且一些备份/恢复数据的工具和销毁设备被使用。有一些适当的数据管理监控。定义了基本性能指标。正在开展数据管理人员的培训。

4 级 可管理级

数据管理的需要被理解，并且所需的操作在组织内部被认可。组织内部已经对数据所有权和管理职责进行清晰定义、分配和传达。程序是正式的和广为人知的，而且知识被共享。正在使用最新工具。与客户约定好目标和性能指标，并通过定义明确的流程来监控。有适当的针对数据管理人员的正式培训。

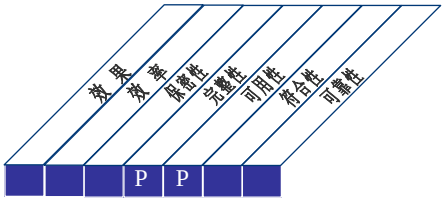
5 级 优化级

组织内部了解和认可数据管理的需要和对所有需求行动的理解。主动研究未来的需要和需求。数据所有权和数据管理的责任被明确建立，在组织内部广为人知，并得到及时更新。程序是正式和广为人知的，并且知识共享是标准实践。运用使数据管理最大程度自动化的成熟工具。与客户约定好目标和性能指标，与业务目标联系在一起，并通过定义明确的流程持续性的监控。持续探索改进的时机。建立了数据管理人员的培训机制。

5.12. DS12 物理环境管理

5.12.1. 流程描述

计算机设备和人员的保护需要有良好设计和管理的基础设施。管理物理环境的流程包括定义物理地点的需求、选择合适的设施和设计有效的流程来监控环境因素以及管理物理访问。物理环境的有效管理减少了由于对计算机设备和人员的侵害而引起的业务中断。



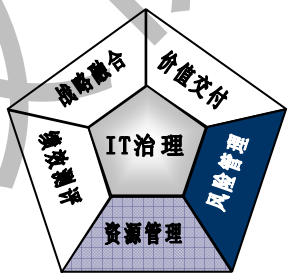
控制 IT 流程：
物理环境管理

使 IT 满足业务需求：
保护计算机资产和业务数据，使业务中断的风险降为最低

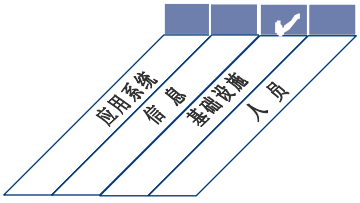
通过关注于：
提供和维护一个适当的物理环境来保护 IT 资产免受非法访问、毁坏或偷窃

通过下列实现：
- 实施物理安全措施
- 选择和管理设施

通过下列衡量：
- 物理环境事件引起的停机故障时间
- 由于物理安全破坏或故障引发的事件数量
- 物理风险评估和审查的频率



主要　次要



5.12.2. 控制目标

DS12.1 地点的选择和规划

IT 设备物理地点的定义和选择策略支持与企业战略相关的技术战略。地点的选择和规划设计应该考虑自然和人为灾难的风险，同时要考虑相关法律法规，例如职业健康和安全的规定。

DS12.2 物理安全措施

制定和执行符合业务需求的物理安全措施，确保 IT 地点和物理资产的安全。物理安全措施必须能够有效地预防、检测和减少与偷窃、温度、火灾、烟尘、水灾、振动、恐怖袭击、人为破坏、电力中断、化学污染、爆炸相关的风险。

DS12.3 物理访问

根据业务需要（包括紧急事件）制定和实施对场所、建筑物和区域的物理访问权限的授予、限制、取消流程。对场所、建筑物和区域的访问必须被证明、授权、记录和监控。这种访问控制适用于进入场所的所有人员，包括正式员工、临时员工、客户、供应商、来访者或者其它第三方访问人员。

DS12.4 依据环境因素的保护

设计和实施保护环境因素的措施。安装专业的装置和设备来监控和控制环境。

DS12.5 物理设施的管理

管理设施，包括电力和通讯设施，要与法律和法规、技术和企业的需求、供应商的说明书及健康和安全指南相符。

5.12.3. 管理指南

源自	输入
PO2	确定的数据分类
PO9	风险评估
AI3	物理环境需求

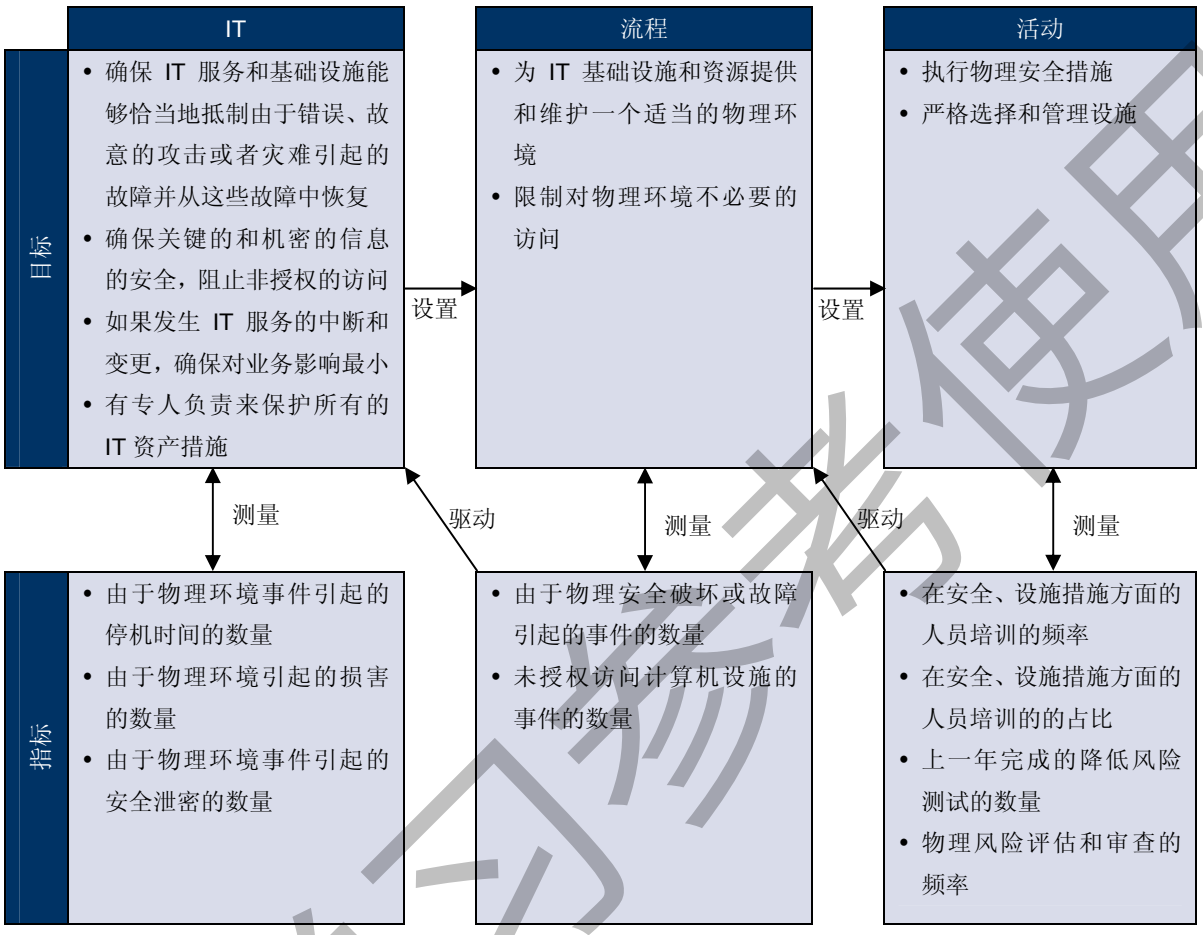
输出	到						
流程绩效报告	ME1						

RACI 图

活动 \ 职能	首席执行官	首席财务官	业务执行经理	首席信息官	业务流程所有者	运营总监	首席架构师	开发总监	IT行政总监	项目管理官	合规、审计、风险和安全
定义物理保护的需求水平					C	A/R	C				C
选择和启用场所（数据中心、办公室等）	I	C	C	C	C	A/R	C		C	C	C
执行物理环境措施					I	A/R	I	I			C
管理物理环境（包括维护、监控和报告）						A/R	C				
制定和执行物理访问授权和维护流程				C	I	A/R	I	I	I		C

RACI 图中，**R**esponsible 代表**执行**，**A**ccountable 代表**责任**，**C**onsulted 代表**商议**，**I**nformed 代表**告知**。

5.12.4. 目标和指标



5.12.5. 成熟度模型

管理“物理环境管理”流程，使 IT 满足业务需求：以保护计算机资产和业务数据，并最小化业务中断风险。

0 级 无级别

没有意识到保护设施或计算机资源投资的需要。环境因素，包括防火、防尘、防电力中断、温度湿度控制等，既没有被监控也没有被控制。

1 级 初始级

组织认识到提供适当的物理环境的业务需求，以保护资源和人员免受人为和自然灾害的威胁。设施和设备的管理依靠关键个体的技能和能力。人员可以在设施内不受限制地活动。管理层没有监控设施环境的控制或者人员的活动。

2 级 可重复级

操作人员实施了环境控制和监控。物理安全是一个非正式的流程，是由一个小团队来管理具有高水平安全级别的物理设施。设施维护流程没有明文规定，只是依赖于有良好实践经验的少数人员进行维护。物理安全目标的制定没有基于任何正式的标准，管理层不能确保达到所有安全目标。

3 级 定义级

维护一个可控制的计算机环境的需要得到组织内部的理解和接受。环境控制、预防性维护和物理安全都是经管理层批准和追踪的预算项目。应用了访问限制，只有被授权的人员才允许访问计算设施。访客是否要作登记和有人陪同取决个体。物理设施的标识不引人注意并且不容易识别。民间权威人士监控健康和安全规章的符合性。为优化保险成本，风险被以最低成本进行投保。

4 级 可管理级

在组织结构和预算分配上体现出对维护一个受控的计算机环境的需求的完全理解。环境和物理安全需求被文档化，访问被严格控制和监控。建立并传达了责任和所有权。管理设施的全体成员在紧急情况下得到了充分锻炼，如同在健康和安全实践中一样。在限制对设施的访问、登记环境和安全因素方面存在适当的标准化控制机制。管理层负责监控控制措施的效果和已建立标准的符合性。管理层已经建立了测量计算机环境管理的目标和指标。计算机资源的可恢复性被合并到组织的风险管理流程中。完整的信息被用于优化保险范围和相关成本。

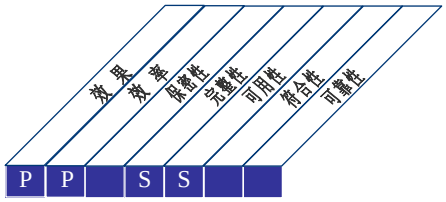
5 级 优化级

存在达成一致的所需设施的长期计划来支持组织的计算机环境。为所有的设施定义了标准，包括选址、建设、安保、人员安全、机械和电子系统、依据环境因素(如火、照明和水患)的保护。所有的设备都建立了清单并按照组织当前的风险管理流程进行分类。访问被基于工作需要进行严格控制，并受到持续监控，在访问的各个时间点所有来访者都有人陪同。通过专业设备，环境得以监控和控制，并且监控设备间可以无人值守。目标被始终如一的测量和评估。预防性维护计划强制要求严格按照时间表进行，对敏感设备进行常规测试。设施策略和标准与 IT 服务可用性目标相一致，并与业务持续性计划和危机管理一起被整合。管理层持续地使用目标和指标对所有设施进行审阅和优化，抓住有利时机来提高对业务的贡献度。

5.13. DS13 运营管理

5.13.1. 流程描述

完整准确地处理数据需要数据处理流程的有效管理和硬件的认真维护。这个流程包括定义操作规程来有效管理预处理、敏感信息输出的保护、基础设施的性能监控以及确保硬件的预防性维护。有效的运营管理帮助维护数据的完整性，并减少业务中断和 IT 运营成本。



控制 IT 流程：
运营管理

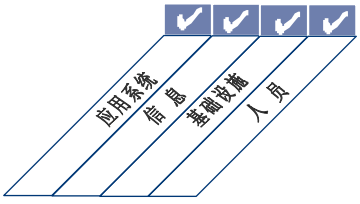
使 IT 满足业务需求：
维护数据的完整性，确保 IT 基础设施能够抵御错误和故障，并且能从错误和故障中恢复

通过关注于：
符合运营服务水平预定的数据处理，保护敏感信息的输出，监控和维护基础设施

通过下列实现：
- IT 环境的运营符合签订的服务水平和定义的操作指南
- 维护 IT 基础设施

通过下列衡量：
- 影响服务水平的运营事件的数量
- 运营事件引起的非计划停机的小时数
- 包括在预防性维护计划中的硬件资产的百分比

■ 主要 ▦ 次要



5.13.2. 控制目标

DS13.1 运营流程和操作指南

制定、实施和维护 IT 运营流程，确保全体运营人员熟悉与其相关的运营任务。运营流程应当包含交接班（运营活动的正式移交、状态更新、运营问题、升级流程、当前职责的报告），以支持签定的服务水平，确保持续性运营。

DS13.2 作业调度

按照最高效的序列组织作业、进程和任务的调度，使吞吐量和利用率最大化，以满足业务需求。

DS13.3 IT 基础设施的监控

制定和实施对 IT 基础设施和相关事件进行监控的流程，确保运营日志中记载了充分的按时间发生顺序排列的信息，以便运营以及与运营活动相关的时间顺序能够重建、审查和测试.

DS13.4 敏感资料和输出设备

建立适当的物理安全设施、会计核算和库存管理手段对 IT 敏感资产进行管理，例如，专用表格、流通票据、特别目的的打印机和安全令牌。

DS13.5 硬件的预防性维护

制定和实施确保基础设施得到及时维护的的流程，减少硬件失效或性能下降的频率和影响。

5.13.3. 管理指南

源自	输入
AI4	用户、操作、支持、技术和管理手册
AI7	产品上线、软件发布和分配计划
DS1	SLAs 和 OLAs
DS4	备份存储和保护计划
DS9	IT 配置/资产详细资料
DS11	数据管理的操作指南

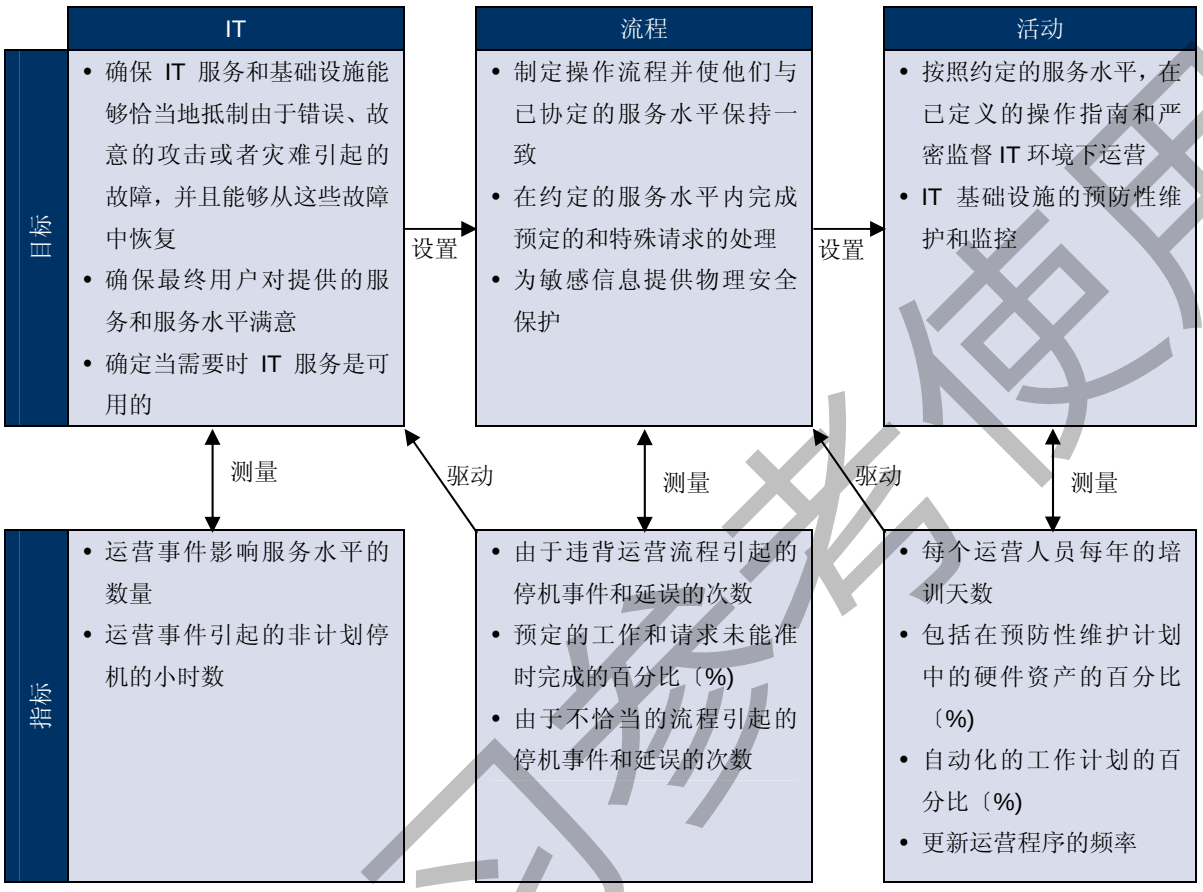
输出	到						
事件故障单	DS8						
错误日志	DS10						
流程绩效报告	ME1						

RACI 图　　职能

活动	首席执行官	首席财务官	业务执行经理	首席信息官	业务流程所有者	首席运营官	首席架构师	首席开发官	首席行政经理	项目管理办公室	合规、审计、风险和安全
建立和修订运营流程（包括手册、列表清单、轮班计划、移交文档、升级流程等）					A/R						I
安排作业负荷和批作业				C	A/R	C	C				
监控基础设施、处理过程和解决问题					A/R						I
管理和保护物理输出（如纸张、介质）					A/R						C
通过时间表和基础设施，申请维修或更换				C	A/R	C	C				C
建立/实施一个保护认证设备免受干扰、遗失和偷窃的流程			A		R			I			C
计划和执行预防性维护					A/R						

RACI 图中，**R**esponsible 代表**执行**，**A**ccountable 代表**责任**，**C**onsulted 代表**商议**，**I**nformed 代表**告知**。

5.13.4. 目标和指标



5.13.5. 成熟度模型

管理“运营管理”流程，使 IT 满足业务需求：以维护数据的完整性，确保 IT 基础设施能够抵制错误和故障并且能从错误和故障中恢复。

0 级 无级别

组织没有投入时间和资源来建立基础的 IT 支持和运营活动。

1 级 初始级

组织认识到建立 IT 支持职能的需求。建立了很少数的标准流程，运营活动实际上都是被动的。大多数运营流程没有正式计划，没有任何事先批准就接受处理请求。支持业务流程的计算机、系统、应用软件经常中断、延迟和失效。时间都浪费在等待资源的过程中。输出介质有时出现在非预期或者不受控制的地方，或者根本不出现。

2 级 可重复级

组织意识到了 IT 运营活动在 IT 支持职能中发挥了关键作用。工具的预算根据具体情况分配。IT 支持操作是非正式的，依靠直觉的。高度依赖个体技能和能力。覆盖该做什么、何时做、以何种顺序做的操作指南没有形成文件。开展了一些操作培训，有一些正式的操作标准。

3 级 定义级

对计算机操作管理的需求在组织内部得到理解和接受。资源得到分配，开展了一些在职培训。可重复职能被正式的定义、标准化、文档化并被传达。事件和已完成任务的结果都得到记录，只有有限的记录结果向管理层做了报告。引进和使用自动调度和其他工具来限制操作人员干预。在操作中有新作业的地方都引入了控制。开发了正式政策以减少非调度事件的数量。在实际中与供应商的维护和服务协议仍然是非正式的。

4 级 可管理级

计算机操作和支持职责被清晰的定义，所有者被分配。通过有关资本支出和人力资源的资源预算，以支持运营。培训是正式的，并且正在执行中。调度和任务都被文件化，并传达给内部的 IT 职能部门和业务客户。有可能使用标准化的绩协议和已建立的服务水平来测量并监控每日的活动。任何背离已建立的规范的行为都能得到快速的定位和改正。管理层监控计算机资源的使用情况以及工作或已分配任务的完成情况。存在一种持续性的努力，以提高自动化处理水平，做为持续改进的方法。与供应商建立起了正式的维护和服务协议。有完全一致的问题、容量和可用性管理流程，该流程被错误和故障原因的分析所支持。

5 级 优化级

IT 支持操作是有效的、高效率的和充分灵活，以最低限度损失的生产力来满足服务水平要求。IT 操作管理流程以知识库为基础被标准化和文件化，并得到持续改进。支持系统的自动化流程连续地运转，并有助于一个稳定的环境。所有的问题和故障都得到分析，以识别根本原因。确保变更管理的例行会议及时讨论了在生产调度中的变更。在与供应商的合作过程中，对设备的使用年限和故障症状进行分析，并且在实际工作中对设备主要做预防性的维护。

6. 监控与评价（ME）

ME1 监控与评价 IT 绩效

ME2 监控与评价内部控制

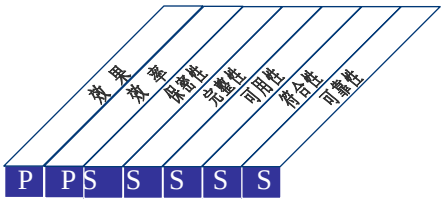
ME3 确保遵循外部要求

ME4 提供 IT 治理

6.1. ME1 监控与评价 IT 绩效

6.1.1. 流程描述

有效的 IT 绩效管理需要一个监控流程。这个流程包括定义相关的绩效指标、有系统的和及时的绩效报告以及对偏差的快速反应。必需实施监控，以确保已设定的工作能够被落实并与已设定方向和策略保持一致。



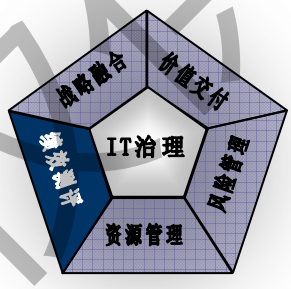
控制 IT 流程：
IT 绩效监控与评价

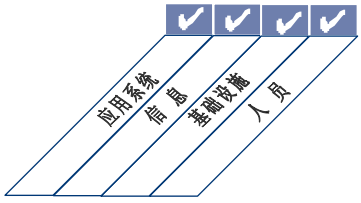
使 IT 满足业务需求：
符合治理要求的 IT 成本、利益、战略、策略和服务水平的透明度和可理解程度。

通过关注于：
监控和报告流程衡量指标，识别和执行绩效改进活动。

通过下列实现：
- 将流程绩效报告整理和转化到管理报告中
- 审查已确定目标的绩效并启动必要的整改措施

通过下列衡量：
- 管理层和治理层对绩效报告的满意度
- 由于监控活动所引起的改进行为的数量
- 关键流程监控的比例





■ 主要 ■ 次要

6.1.2. 控制目标

ME1.1 监控体系

创建一个通用的监控框架和方法，以便定义需要遵循的范围、方法论和流程，用以监控 IT 对业务的贡献，以及衡量 IT 解决方案和服务交付水平对业务的贡献。并把这一监控体系整合到整个公司的绩效管理体系当中。

ME1.2 监控数据的收集和识别

与业务部门一起设定一套绩效目标，并使这个目标得到业务部门和其他利益相关方的认可。定义比较这些目标的基准，识别采集来衡量这些目标的可用数据。建立一个流程，以收集这些目标的及时、准确的数据，并报告其进展。

ME1.3 监控方法

履行一个绩效监控方法（如，平衡记分卡），以记录目标、获取测量情况、提供简洁、全视角的 IT 绩效，且适合企业监控体系。

ME1.4 绩效评价

定期评估目标的绩效，分析偏差产生的原因，启动整改措施以寻找深层次原因。适当的时候，实施偏差根本原因分析。

ME1.5 董事会和管理层报告

编纂高级管理层报告，描述 IT 对业务的贡献，尤其在企业项目组合、IT 保障投资项目群、个别项目群的解决方案和可交付的服务等方面的绩效。现状报告应包括以下内容：已实现的计划目标、已使用的预算资源、已达到的绩效目标、已缓释的可识别风险。期望高级管理层审阅的主要问题的整改建议。将报告提供给高级管理层并请其审阅后回馈意见。

ME1.6 整改措施

根据绩效监控、评估和报告结果来识别和采取整改措施。通过采取以下措施来确保全部监控、报告和评估工作的连续性：

- 对管理层回馈意见的审阅、协商和接受
- 对整改职责的分配
- 对整改措施执行结果的追踪

6.1.3. 管理指南

源自	输入
PO5	成本收益报告
PO10	项目绩效报告
AI6	变更状态报告
DS1-13	流程绩效报告
DS3	性能和容量计划（需求）
DS8	用户满意度报告
ME2	IT 控制的有效性报告
ME3	IT 活动遵循外部法律和法规需求的报告
ME4	IT 治理状况报告

输出	到						
绩效作为 IT 计划编制的参考	PO1	PO2	DS1				
整改措施计划	PO4	PO8					
历史风险趋势和事件	PO9						
流程绩效报告	ME2						

RACI 图

活动 \ 职能	董事会	首席执行官	首席财务官	业务执行经理	首席信息官	业务流程所有者	运营总监	首席架构师	开发总监	IT行政总监	项目管理官	合规、审计、风险和安全
建立监控方法		A	R	C	R	I	C	I	C	I		C
识别关键的依赖性及当前绩效		C	C	C	A	R	R		R			
建立记分卡					A		R	C	R	C		
评估绩效			I	I	A	R	R	C	R	C		
报告绩效	I	I	I	R	A	R	R	C	R	C		I
识别和监控绩效改进措施					A	R	R	C	R	C		C

RACI 图中，**R**esponsible 代表**执行**，**A**ccountable 代表**责任**，**C**onsulted 代表**商议**，**I**nformed 代表**告知**。

6.1.4. 目标和指标

6.1.5. 成熟度模型

管理“IT 绩效监控与评价”流程，使 IT 满足业务需求：符合治理要求的 IT 成本、利益、战略、策略和服务水平的透明度和可理解程度。

0 无级别

组织没实施任何监控过程，IT 也无独立执行项目和流程的监控，缺少有效的、及时的和准确的报告，未意识到清晰的可理解的过程目标的必要。

1 初始级

管理层意识到收集和评估有关监控流程信息的必要性。但没有定义标准的收集和评估过程。实施监控和选择度量标准是基于每个特定的 IT 项目和流程需求。监控通常是在可能导致一定损失或阻碍企业发展的情况下得到执行。会计功能监控是基于 IT 财务措施。

2 可重复级

已建立基本的监控措施。存在收集和评估的方法及技术，但未在整个组织中采纳。监控结果的解释依赖关键个人的经验判断。在收集信息时选择和使用了有限的工具，但数据收集过程缺少规划。

3 定义级

管理层已发布并制度化了标准监控流程，已实施了监控所需的教育与培训工作，已形成了与历史绩效信息相关的规范化知识基础。评估仅仅在每个单独的 IT 流程和项目中进行，并没有整合到所有流程中去。规定了监控 IT 流程和服务水平的工具。通过使用传统的财务和经营标准定义了组织绩效的信息服务水平贡献度的测量标准。也规定了 IT 特定的绩效度量方法、非财务的测量方法、战略度量方法、客户满意度的度量方法和服务水平的测量方法。规定了测量绩效框架。

4 可管理级

管理层已规定了在流程发挥作用情况下的容错度。监控报告结果已标准化和规范化。在所有 IT 项目和流程中都有一个整合的度量标准。IT 组织的管理报告体系已正规化。在整个组织内整合和使用了自动化的工具，这些工具被用来收集和监控应用、系统和流程中的操作信息。管理层已能够基于所有利益相关者确认后的统一的标准来评估绩效。IT 功能度量与整个组织目标相一致。

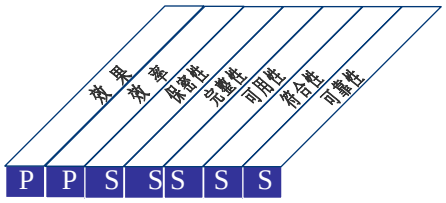
5 优化级

开发了连续的质量改进过程，用来更新整个组织的监控标准和策略，以及合并具体的行业最佳实践。所有监控过程都被优化且支持组织目标。业务驱动的衡量标准被常规性地用来测量绩效，并整合到战略评估框架中，例如 IT 平衡计分卡体系。流程监控不断优化，并与组织中的业务过程改进计划相一致。针对行业和主要竞争者的基准已按易于理解的对比标准进行了规范化。

6.2. ME2 监控与评价内部控制

6.2.1. 流程描述

建立有效的 IT 内部控制程序需要清晰的监控流程。此流程包括监控和报告控制例外事件、自我评估结果和第三方评审。内部控制监控的关键好处是为以下内容提供保证：运营的效率和效果、遵循适用的法律和法规。



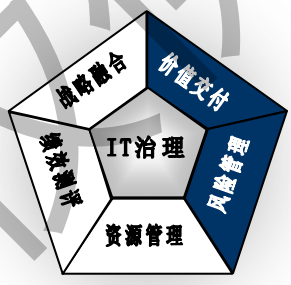
控制 IT 流程：
内部控制监控与评价

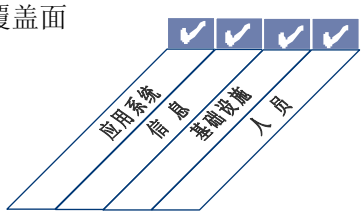
使 IT 满足业务需求：
确保 IT 目标的实现以及符合 IT 相关的法律、法规和合同。

通过关注于：
监控 IT 相关活动的内部控制流程，并制定改进措施

通过下列实现：
- 定义一个嵌入在 IT 流程框架的一个内部控制体系
- 监控和报告 IT 内部控制的有效性
- 向管理层报告控制例外情况以采取措施

通过下列衡量：
- 主要内部控制违规的数量
- 主动改进控制的数量
- 自我评估控制的数量和覆盖面





主要　次要

6.2.2. 控制目标

ME2.1 监控内部控制框架

持续监控 IT 控制环境和控制框架。使用行业最优方法和基准去评估及改进 IT 控制环境和控制框架持续监控以满足企业目标。

ME2.2 管理评价

监控和评价 IT 内部控制管理的效率和效果。

ME2.3 控制例外事件

识别控制例外事件，分析并找出其潜在根源。逐步升级控制例外事件并报告给合适的利益相关者。提出必要的整改措施。

ME2.4 控制自我评估

通过持续的自我评估流程，评价管理层对于 IT 流程、政策、协议控制的完整性和有效性。

ME2.5 内部控制保证

必要时可通过第三方评审以获得内部控制完整性和有效性的进一步保证。

ME2.6 对第三方的内部控制

评估外部服务提供者的内部控制状态。确定外部服务提供者遵循了法律、法规要求以及合同约定。

ME2.7 整改措施

依据控制评估和报告，定义、启动、追踪并执行整改措施。

ME2 监控与评价内部控制

6.2.3. 管理指南

源自	输入
AI7	内部控制监控
ME1	流程绩效报告

输出	到						
IT 控制的有效性报告	PO4	PO6	ME1	ME4			

RACI 图

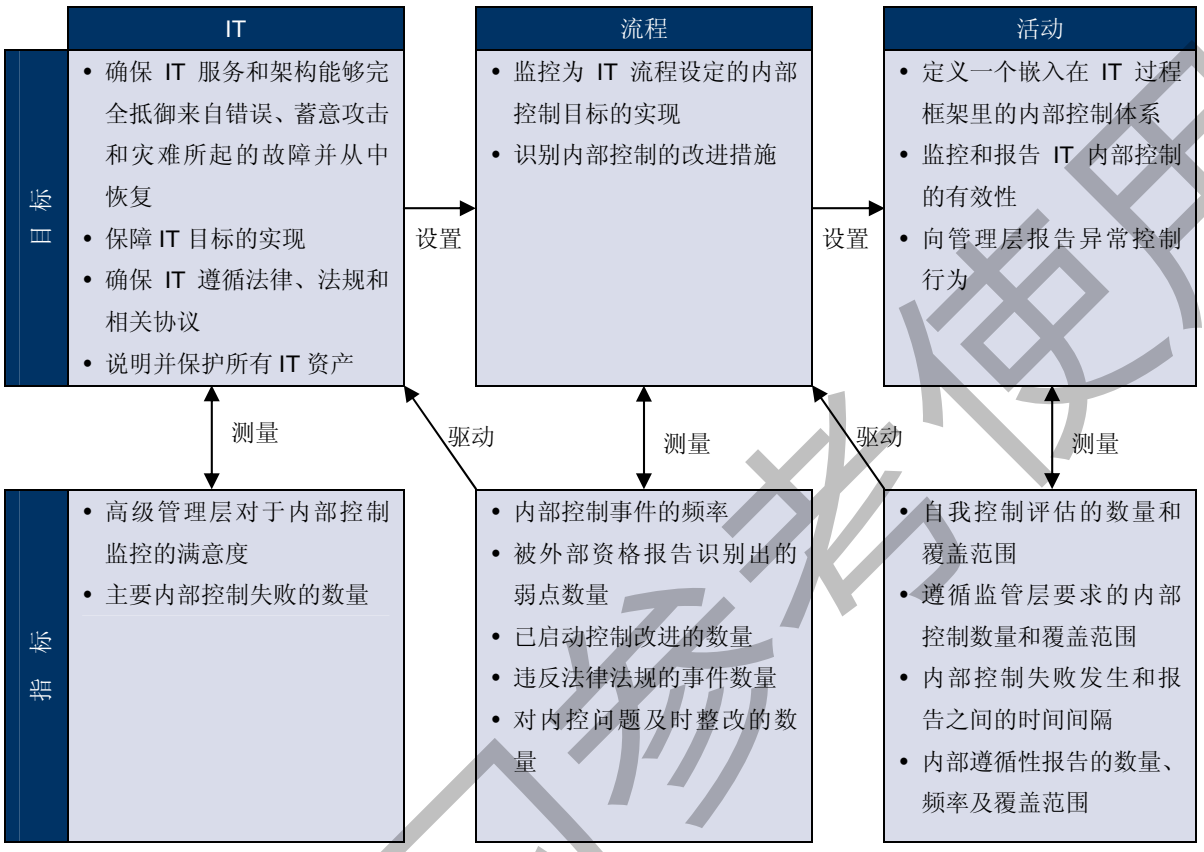
职能

活动

活动	董事会	首席执行官	首席财务官	业务执行经理	首席信息官	业务流程所有者	运营总监	首席架构师	开发总监	IT行政总监	项目管理官	合规、审计、风险和安全
监督和控制 IT 内部控制活动					A		R		R	R		R
监控自评估流程				I	A		R		R	R		C
监控独立的审阅、审计和检查				I	A		R		R	R		C
监控第三方执行的控制保证流程		I	I	I	A		R		R	R		C
监控识别和评估控制异常的流程		I	I	I	A	I	R		R	R		C
监控识别和补偿控制异常的流程		I	I	I	A	I	R		R	R		C
向关键利益相关者报告	I	I	I		A/R							I

RACI 图中，**R**esponsible 代表**执行**，**A**ccountable 代表**责任**，**C**onsulted 代表**商议**，**I**nformed 代表**告知**。

6.2.4. 目标和指标



6.2.5. 成熟度模型

管理“监控和评价内控控制”，使 IT 满足业务需求：保证 IT 目标符合 IT 相关的法律、法规和合同。

0 无级别

组织缺乏监控内部控制有效性的流程，管理层缺少内部控制的报告方法，普遍没有意识到 IT 运行安全和内部控制保证。管理层和员工普遍缺乏内部控制意识。

1 初始级

管理层意识到常规的 IT 管理和控制保证的必要性。评估内部控制适当性方面特别依赖个别专家意见。IT 管理层没有正式分派监控内部控制有效性的职责。IT 内部控制评价仅作为传统财务审计的一部分来执行，使用的方法和技能没有体现出信息服务功能。

2 可重复级

组织采用非正式内部控制报告的形式启动整改措施。内部控制评估依赖关键个人的技能。组织逐渐对内控监控有了意识。信息服务管理层仅对认为重要的内部控制执行一些有效性监控。开始使用内部控制监控的方法和工具，但处于无计划状态。通过个人的技能能够识别 IT 环境所特有的风险要素。

3 定义级

管理层支持并制度化了内部控制的监控。形成了评价和报告内部控制监控行为的政策和措施。规定了内部控制监控的培训教育程序。设定了自我评估和内部控制审阅过程，并为可依赖的业务和 IT 管理者分配角色。使用了工具但未整合到整个过程当中去。在控制框架中使用了 IT 流程风险评估策略，此框架是为 IT 组织所特别开发。规定了特别流程的风险及其缓释策略。

4 可管理级

管理层已实施了内部控制的监控框架。组织也建立了内控监控过程的容错级别。使用工具实施了标准化评估，并自动监测出控制例外事件。专业人员利用高级管理者所批准的正式的控制框架，建立了正规的 IT 内部控制职责。技能熟练的 IT 员工定期参加内部控制评估。基于内部控制评估的历史信息，建立了有关衡量指标的知识体系。建立了与上述内容相当的内部控制监控的评审机制。

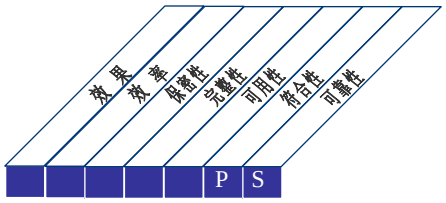
5 优化级

管理层在整个组织中建立了持续改进流程，该流程充分考虑了 IT 内部控制监控经验和行业最佳实践。组织适时使用了整合的和最新的工具，该工具能够对下述内容做出有效评估：关键 IT 控制内容、快速发现控制监控事件情况。正式实施了为信息服务所设计的知识分享体系。针对行业标准基和最佳实践所设计的标准已正规化。

6.3. ME3 确保遵循外部要求

6.3.1. 流程描述

有效的合规监管需要建立一个保证遵循法律、法规和合同要求的审阅流程。该流程包括：确定合规要求，优化和评价对这些合规要求的响应情况，确保完全遵循了这些要求，最后，将 IT 的遵循报告与业务遵循报告合并。



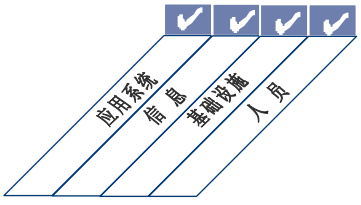
控制 IT 流程：
确保遵循外部要求

使 IT 满足业务需求：
确保遵循法律、法规和合同要求

通过关注于：
识别所有适用的法律、法规、合同要求以及相应的 IT 遵循性水平要求，并优化 IT 流程以降低违规风险。

通过下列实现：
- 识别与 IT 相关的法律、法规和协议性要求
- 评估遵循性要求所带来的影响
- 监控、报告这些要求的遵循情况

通过下列衡量：
- IT 违规成本，包括和解费用和罚金
- 外部遵循性问题的确定与解决之间的平均滞后时间
- 合规评审的频率



主要　次要

ME3 确保遵循外部要求

6.3.2. 控制目标

ME3.1 识别外部法律、法规和合同的合规性要求

不断收集确定国内和国际法律、法规和其他外部要求，在制定组织的 IT 政策、标准、程序和方法论时体现这些要求。

ME3.2 优化对于外部要求的应对措施

审阅和调整 IT 政策、标准、流程和方法论，以确保法律、法规和协议要求得到落实。

ME3.3 评估外部要求的合规性

确认 IT 政策、标准、流程和方法论遵循了法律、法规要求。

ME3.4 积极保证合规性

获取并报告所有的内部政策得到遵循，这些政策来自于内部规定外部法律要求、监管要求或合约要求，以确保流程所有者能够适时采取整改措施。

ME3.5 整合报告

将来自其他业务部门的涉及法律、法规和合同需求合规性的内容与 IT 的法律、法规和合同需求合规性报告进行整合。

6.3.3. 管理指南

源自	输入
*	与法律法规需求的符合性
PO6	IT 政策

输出	到						
与 IT 服务交付相关的法律法规需求目录	PO4	ME4					
与外部法律法规需求相关的 IT 活动符合性报告	ME1						

* 输入来自于 COBIT 外部

RACI 图

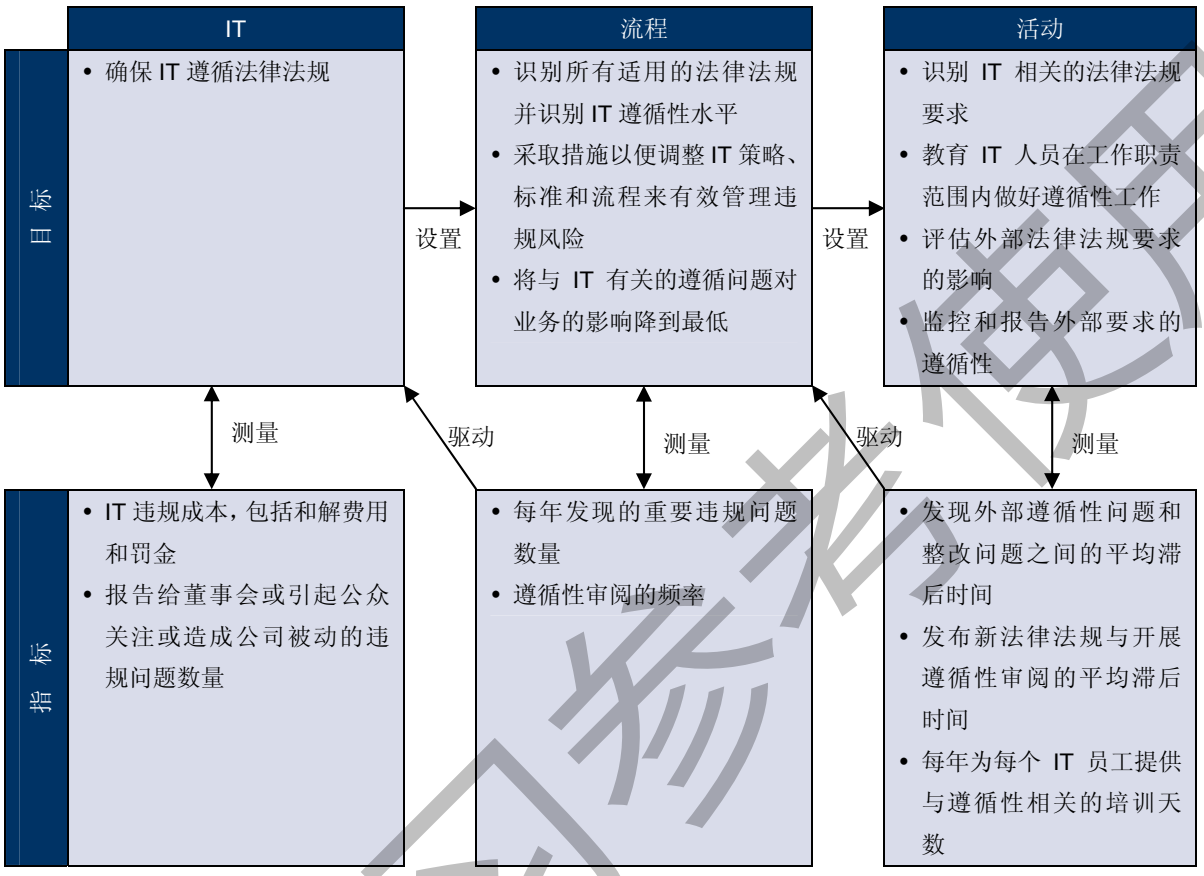
职能

活动

活动	董事会	首席执行官	首席财务官	业务执行经理	首席信息官	业务流程所有者	运营总监	首席架构师	开发总监	IT行政总监	项目管理官	合规、审计、风险和安全
规定和执行一个可识别法律、合同、策略、法规需求的流程					A/R	C	I	I	I	C	I	R
评估遵循 IT 政策、标准和程序的 IT 活动	I	I	I	I	A/R	I	R	R	R	R	R	R
有效的遵循性保证报告，即 IT 活动对 IT 政策、标准和程序的遵循性保证					A/R	C	C	C	C	C	C	R
为调整 IT 政策、标准和程序提供输入，使其满足遵循性需求					A/R	C	C	C	C	C		R
将来自其他业务部门涉及法规要求的内容与 IT 的法规需求报告整合					A/R		I	I	I	R	I	R

RACI 图中，**R**esponsible 代表**执行**，**A**ccountable 代表**责任**，**C**onsulted 代表**商议**，**I**nformed 代表**告知**。

6.3.4. 目标和指标



6.3.5. 成熟度模型

管理“确保遵循外部要求”流程，使 IT 满足业务需求：确保遵循法律、法规和合同要求。

0 级 无级别

对影响 IT 的外部需求基本没有意识，缺少专门针对法律、法规和合同要求的遵循性流程。

1 级 初始级

对影响组织的法律、法规及协议的遵循性需求有了意识，采用非正式的流程保持遵循性，但仅在新项目或应对审计和审阅时使用。

2 级 可重复级

对遵循外部需求的必要性有了理解，而且这种需求已经得到显现。在遵循性已经成为持续需求的领域中，如财务制度或隐私立法，个别遵循性工作已按年度开展。然而没有标准的方法。高度依赖个人知识和职责，错误也在所难免。有了一些非正式的有关外部要求和遵循性问题的培训。

3 级 定义级

已开发了策略、计划和程序，并且进行了文档化和宣传，以确保和法律、法规、合同的遵循性，但有些没有一贯执行，有些已经过期或不适用而需要修订。没有开展监控工作，而且没有突出遵循性要求。在影响组织的外部法律法规需求和已规定好的遵循性流程方面提供了培训。为减少合同性责任的风险已制定了标准的、形式上的协议和法律流程。

4 级 可管理级

对来自外部要求的问题暴露以及确保在各层面都存在遵循性的必要有全面的理解。已有正式的培训计划来保证所有员工意识至自己的遵循性职责。职责和流程所有权清晰明了。流程包括对外部环境的审阅，以便能够识别外部要求及其改变。建立了一个适当的机制，以便能够监控违反外部要求的行为、加强内部操作、开展整改工作。用标准化的方式深层次分析违规问题，以便找到可行的解决方案。在某些特殊方面采用了标准化的内部最佳实践，例如章程和持续服务合同。

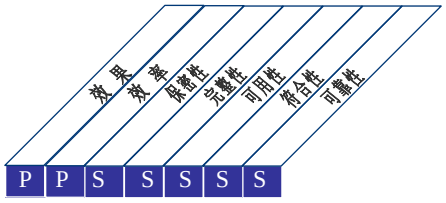
5 级 优化级

为了确保遵循外部要求，制定有协调的、高效的和强制实施的流程，这个流程是基于能够对整个组织提供指引和协作的核心功能所设计。存有针对外部要求所适用的大量知识，包括外部要求的未来趋势、有可能发生的变化、新解决方案的需求。组织参与外部立法机构和行业机构的讨论，以便理解和影响外部要求。已开发了最佳实践确保有效遵循外部要求，使得极少有遵循性方面的问题。存有核心的、遍布组织范围内的追踪体系，使管理达到工作流文档化，量化和提高遵循性监控流程的质量和效果。实施了外部要求的自我评估过程，并达到一个良好的实践水准。组织在遵循性方面的管理风格和文化是非常强大的，并且流程运转非常通畅，以致于对新员工或发生重要变更时只需提供有限培训即可。

6.4. ME4 提供 IT 治理

6.4.1. 流程描述

建立有效的治理框架，包括定义组织结构、流程、领导力、角色和职责，以确保企业 IT 投资在遵循企业战略和目标的前提下运作。



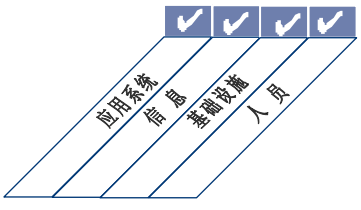
控制 IT 流程：
提供 IT 治理

使 IT 满足业务需求：
整合 IT 治理与公司治理目标，并遵从法律和法规

通过关注于：
制订关于 IT 策略、绩效、风险的董事会报告，响应与董事会目标一致的治理要求

通过下列实现：
- 建立整合在公司治理中的 IT 治理框架
- 获得 IT 治理现状的独立保证

通过下列衡量：
- 董事会向利益相关者报告 IT 情况的频率（包括成熟度）
- IT 部门向董事会报告的频率（包括成熟度）
- 独立评估 IT 遵循性的频率



主要　次要

6.4.2. 控制目标

ME4.1 建立 IT 治理框架

定义、建立和调整 IT 治理框架，并使其与组织的整体公司治理和控制环境相一致。以这个框架为基础建立合适的 IT 流程和控制模型，提供明确的责任和实践以避免内部控制失败和其他缺陷。确保 IT 治理框架符合法律法规要求，并与公司的战略目标保持一致。报告 IT 治理的现状和问题。

ME4.2 战略融合

让董事会和高级管理层能够理解 IT 战略，例如 IT 角色、技术认知和技术能力。确保 IT 部门和业务部门在 IT 对业务战略的潜在贡献方面能够达成共识。与董事会及其建立的治理机构如 IT 战略委员会一起确定战略方向，管理 IT 有关事项，确保 IT 战略和目标层层落实到业务部门和 IT 部门，并在业务部门和 IT 部门间建立信心和信任。IT 部门和业务部门共同实施 IT 战略和运营，以便制定战略决策、获取 IT 投资的收益。

ME4.3 价值交付

管理 IT 项目及其它 IT 资产和服务，保证在支持企业战略和目标上的最大可能价值。确保以下内容：清楚 IT 项目投资的预期业务成果以及为实现这些成果必需的全部付出；利益相关方创建和同意了全面的和一致的业务模式；对资产和投资的管理贯穿其整个经济生命周期；动态管理收益的实现，如对新服务的贡献、效率增加、改善对客户需求的响应等。对投资组合、项目群和项目管理执行严格的方法，强调业务部门对所有 IT 项目投资的所有权，IT 部门确保交付的 IT 功能和服务的成本最优。

ME4.4 资源管理

定期评估 IT 实施工作和运营，检查 IT 资源的投资、使用和分配情况，确保资源分配的适当性并符合当前和未来战略目标和业务需要。

ME4.5 风险管理

与董事会一起确定企业的 IT 风险偏好，保证采取了适当的 IT 风险管理活动，以确保实际 IT 风险没有超出董事会的风险偏好。组织中明确风险管理的职责，确保业务部门和 IT 部门定期评估和报告 IT 相关的风险及其影响，所有利益相关方都清楚企业的 IT 风险偏好。

ME4.6 绩效测评

确定已实现或超出了事先设定的 IT 目标，或者 IT 目标的进展满足期望要求。如果事先设定的目标没有实现或进展不理想，需检查管理层的整改措施。向董事会报告有关的投资组合、项目群和 IT 绩效，以便高级管理层审查向既定目标的进展情况。

ME4.7 独立保证

获取以下 IT 合规性的独立保证（内部的或外部的）：相关法律和法规；组织的政策、标准和程序；公认的实践和做法；IT 绩效的效率和效果。

ME4 提供 IT 治理

6.4.3. 管理指南

源自	输入
PO4	IT 流程框架
PO5	成本/收益报告
PO9	风险评估和报告
ME2	报告 IT 控制的有效性
ME3	与 IT 服务交付相关的法律法规要求的目录

输出	到						
流程框架改进	PO4						
IT 治理现状报告	PO1	ME1					
IT 驱动的业务投资的预期业务成果	PO5						
企业为 IT 制定的战略方向	PO1						
企业的 IT 风险偏好	PO9						

RACI 图

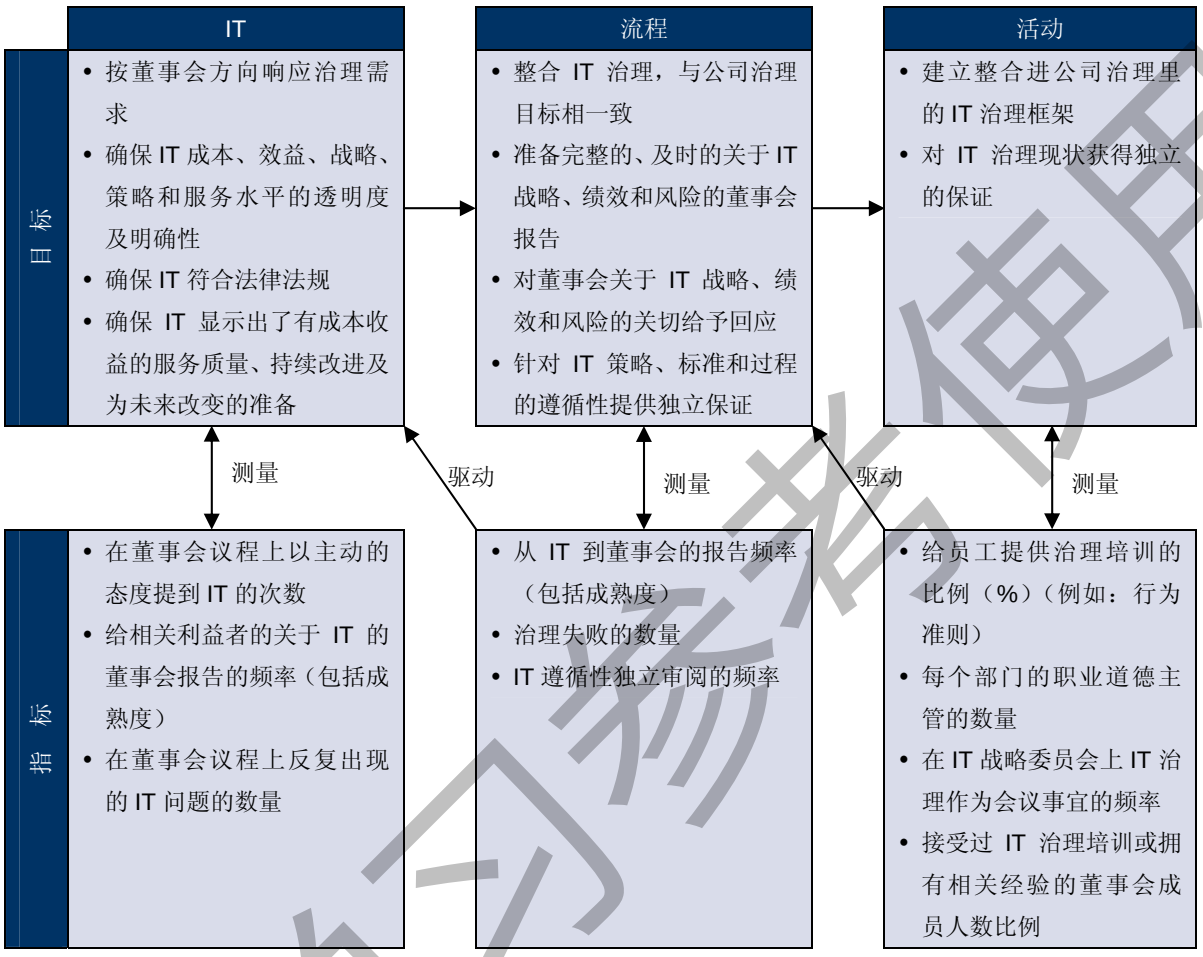
职能

活动

活动	董事会	首席执行官	首席财务官	业务执行经理	首席信息官	业务流程所有者	运营总监	首席架构师	开发总监	IT行政总监	项目管理官	合规、审计、风险和安全
建立管理层和董事会对于 IT 活动的监督和促进机制	A	R	C	C	C							C
审查、签署、调整和沟通与业务战略相适应的 IT 绩效、IT 战略、资源和风险管理	A	R	I	I	R							C
获取定期的、独立的绩效评估和政策、计划和程序的遵循情况	A	R	C	I	C		I	I	I	I	I	R
解决独立评估的发现，确保管理层实施已达成一致的建议	A	R	C	I	C		I	I	I	I	I	R
形成 IT 治理报告	A	C	C	C	R	C	I	I	I	I	I	C

RACI 图中，**R**esponsible 代表**执行**，**A**ccountable 代表**责任**，**C**onsulted 代表**商议**，**I**nformed 代表**告知**。

6.4.4. 目标和指标



6.4.5. 成熟度模型

管理“提供 IT 治理”流程，使 IT 满足业务需求：整合 IT 治理与公司治理目标，并遵从法律和法规。

0 没有级

完全缺乏对 IT 治理过程的认识，组织甚至没有意识到这样存在问题，因此对这个问题也缺少交流。

1 初始级

对 IT 治理问题有了认识，也认识到有必要强调 IT 治理。在个别具体工作中或使用了一些特别的方法。管理层的方法具有创造性，但也存在一些问题，如孤立、沟通的不一致。关于如何使 IT 为业务绩效服务，管理层仅有大致的方向。管理层仅对组织造成损失或难以应对的事件有积极的反应。

2 可重复级

对 IT 治理问题有了意识。正在开发 IT 治理活动和绩效指标，包括 IT 计划、传递和监控过程。部分 IT 流程的改善依赖于个人意志。管理层也规定了基本的 IT 治理度量方法、评估方法以及技术。但这些过程还没有完全应用在组织内。关于治理标准和职责的沟通在个人之间进行。在不同的 IT 项目和过程中是个人驱动治理过程。测量 IT 治理过程、工具和方法有限，由于缺少专业知识这些内容不能得到充分应用。

3 定义级

管理层理解 IT 治理的重要性和必要性，并在组织内传播。书面确定了成果指标和绩效指标的关联，定义了 IT 管理的基线。形成了标准化和书面的程序。管理层已沟通了标准化的程序，建立了培训机制。利用工具协助检查 IT 治理情况。定义了仪表盘，作为 IT 平衡计分卡的一部分。但仅有个别人得到培训，个别人遵循和使用这些标准。各流程被监控，但主要是个别人的自发行为，且管理层不大可能发现其中的偏差。

4 可管理级

在所有层面，对 IT 治理都有全面理解。对于谁是客户这个问题有清晰的理解，并且通过 SLAs 明确和监控了职责。职责清晰且建立了流程所有者。IT 流程和 IT 治理整合进了业务和 IT 战略中。在 IT 流程方面的改进主要基于定量的理解，为流程标准的遵循性监控和度量提供了可能性。所有流程的利益相关者都意识到了风险、IT 重要性和它所能提供的机遇。管理层定义了可操作流程的可容忍度。但也是有局限性使用了技术，主要是战术上的、且基于成熟方法和标准工具的技术。IT 治理已经整合到战略和操作计划和监控的流程当中。所有 IT 治理活动的绩效指标都被记录和追踪，这些指标引导了整个公司的改进。关键流程绩效的所有职责是清晰的，基于关键流程度量的管理的回报是丰厚的。

5 优化级

对 IT 治理问题和解决方案有着深刻的和前瞻性的理解。先进的概念和技术支撑了培训和沟通。流程已经被总结提炼到一个最佳的行业实践水平，并主要基于持续改进结果和模仿其他组织的成熟度。IT 政策的实施促使组织、个人和流程很快适应并充分支持 IT 治理需求。所有问题和偏差都能够从根本上分析原因，并寻找和采取恰当的措施解决。IT 以广泛的、整体的、优化的方式自动处理工作流，且提供工具改进质量和效果。在整个公司范围内定义了、平衡了和沟通了 IT 流程的风险收益关系。外部专家作用较大，基准被用作指南。组织中广泛存在治理预期的监控、自我评估和沟通交流，积极利用技术去测量、分析、沟通和培训。公司治理和 IT 治理在战略上紧密相连，充分利用技术、人力、财务资源提升企业竞争力。IT 治理活动与企业治理过程融合。

附录 I 目标和流程关联表

该附录提供了一个展示通用业务目标与 IT 目标、IT 流程和信息标准之间关系的整体视图。共有三张表：

1. 第一张表展示了依照平衡记分卡确定的业务目标与 IT 目标、信息标准的映射关系。对一个给定的通用业务目标，表中列示了典型支持该业务目标的 IT 目标和与该业务目标相关的 COBIT 信息标准。表中所列的 17 个业务目标不应看作是所有可能的业务目标的全集；所选择的是那些对 IT 有显著影响的业务目标（与 IT 相关的业务目标）。
2. 第二张表展示了 IT 目标与 COBIT 的 IT 流程、IT 目标所依据的信息标准之间的映射关系。
3. 第三张表展示了 IT 流程与它所支持的 IT 目标之间的反向映射关系。

这些表展示了在 COBIT 与业务驱动之间、COBIT 描述的范围与所有业务之间的关系，使典型的与 IT 相关的业务目标通过 IT 目标映射到支持其所需要的 IT 流程。该表基于通用的目标，因此，对一个具体的企业来说，可作为参考或选择性使用。

在 COBIT 第三版的后面提供了一个用于业务需求的信息标准的链接，这些表也指出了那些业务和 IT 目标所支持的重要的信息标准。

备注：

1. 在业务目标图中，信息标准是一个相关标准的集合，这些标准是基于 IT 目标和对业务目标相关的主观评估，无意区分主次，仅仅为了表述和便于用户使用一个相似的流程去分析自己的业务目标。
2. 在 IT 目标图中，所列主要和次要的信息标准，是基于每一个 IT 流程和对 IT 目标与业务目标之间主次关系的主观评估。这些仅仅是指导性的，用户在评估他们自己的 IT 目标的时候，可以参考相似流程。

附录 I—目标和流程关联表

业务目标到 IT 目标的关联

		业务目标	IT目标								COBIT信息标准						
											效果	效率	保密性	完整性	可用性	符合性	可靠性
财务视角	1	为IT保障业务投资提供良好投资回报		24								4					
	2	管理IT相关业务风险	2	14	17	18	19	20	21	22			4	4	4		
	3	改进公司治理和透明度	2	18													4
客户视角	4	改善客户倾向和服务	3	23							4						
	5	提供有竞争力产品和服务	5	24							4	4					
	6	建立持续和可用的服务	10	16	22	23					4				4		
	7	对业务需求变更提供灵活快捷的响应	1	5	25						4	4					
	8	完成服务交付的成本最优化	7	8	10	24						4					
	9	为战略决策提供可靠的和有用的信息	2	4	12	20	26				4			4			4
内部流程视角	10	改善和维护业务流程的功能	6	7	11						4	4					
	11	降低流程成本	7	8	13	15	24					4					
	12	提供与外部法律、法规及合同的合规性	2	19	20	21	22	26	27				4			4	
	13	提供与内部政策的符合性	2	13									4			4	
	14	管理业务变更	1	5	6	11	28				4	4					
	15	改善和维持运营和员工生产力	7	8	11	13					4	4					
学习与成长视角	16	管理产品和业务创新	5	25	28						4	4					
	17	获得和维持技能熟练的和上进的人	9								4	4					

IT 目标到 IT 流程的关联

	IT目标	流程											CobiT信息标准						
													效果	效率	保密性	完整性	可用性	符合性	可靠性
1	响应符合业务战略的业务需求	PO1	PO2	PO4	PO10	AI1	AI6	AI7	DS1	DS3	ME1		P	P		S	S		
2	响应符合董事会方向的管理需求	PO1	PO4	PO10	ME1	ME4							P	P					
3	确保最终用户对服务提供和服务等级的满意	PO8	AI4	DS1	DS2	DS7	DS8	DS10	DS13				P	P		S	S		
4	最优化信息的利用	PO2	DS11											S		P			S
5	创建IT灵活性	PO2	PO4	PO7	AI3								P	P		S			
6	确定如何将业务功能和控制需求转化为自动化解决方案的效率和效果	AI1	AI2	AI6									P	P				S	
7	获取和维护整合的和标准化的应用系统	PO3	AI2	AI5									P	P				S	
8	获取和维护完整和标准的IT基础设施	AI3	AI5										S	P					
9	获得并维持响应IT战略的IT技能	PO7	AI5										P	P					
10	确保与第三方之间的相互满意	DS2											P	P	S	S	S	S	S
11	确保应用系统与业务流程的完美结合	PO2	AI4	AI7									P	P		S	S		
12	确保IT成本、收益、战略、策略和服务等级的透明度和被理解	PO5	PO6	DS1	DS2	DS6	ME1	ME4					P	P				S	S
13	确保应用系统和技术解决方案的合理使用和性能	PO6	AI4	AI7	DS7	DS8							P	S					
14	登记和保护所有IT资产	PO9	DS5	DS9	DS12	ME2							S	S	P	P	P	S	S
15	优化IT基础设施、资源和性能	PO3	AI3	DS3	DS7	DS9							S	P					
16	减少解决方案和服务交付的过失和返工	PO8	AI4	AI6	AI7	DS10							P	P		S	S		
17	保护IT目标的达成	PO9	DS10	ME2									P	P	S	S	S	S	S
18	清楚源自IT目标及资源的风险对业务的影响	PO9											S	S	P	P	P	S	S
19	确保关键和机密信息与不应该访问的人的隔离	PO6	DS5	DS11	DS12										P	P	S	S	S
20	确保自动化的业务交易和信息交换是可信的	PO6	AI7	DS5									P			P	S	S	
21	确保IT服务和基础设施能适当抵御和恢复因失误、恶意攻击和灾难而导致的故障	PO6	AI7	DS4	DS5	DS12	DS13	ME2					P	S		S	P		
22	确保因IT服务中断或变更而对业务影响的最小	PO6	AI6	DS4	DS12								P	S		S	P		
23	确保所必需的IT服务是可用的	DS3	DS4	DS8	DS13								P	P			P		
24	提高IT的成本效益和对业务收益的贡献	PO5	DS6										S	P					S
25	项目按时、按预算、满足质量标准地交付	PO8	PO10										P	P		S			S
26	维持信息和基础设施的完整性	AI6	DS5										P	P		P	P		S
27	确保IT遵循法律、法规和合同	DS11	ME2	ME3	ME4										S	S		P	S
28	确保IT显示出有成本效益的服务质量、持续改进和适应未来变化	PO5	DS6	ME1	ME4								P	P					P

IT 流程与目标矩阵

	响应配合业务战略的业务需求	响应符合董事会的方针的管理需求	确保最终用户对服务提供和服务等级的满意	优化信息利用	创建IT灵活性	确定如何将业务功能和控制需求能被高效传递和自动化解决	获取和维护完整和标准的应用系统	获取和维护完整和标准的IT基础设施	获得并维持能够响应IT战略的IT技能	确保与第三方的相互满意	确保应用系统与业务流程的完美结合	确保IT成本、收益、战略、策略和服务等级的透明度和被理解	确保应用系统和技术解决方案的合理使用和性能	登记和保护所有IT资产	优化IT基础架构、资源和性能	减少解决方案和服务交付的过失和返工	保护IT目标的实现	建立透明的、由IT目标和资源风险与可接受的业务影响	确保关键和机密信息与不应被访问的人隔离	确保自动化业务处理和信息交换信息可信	确保IT服务和基础设施能适当抵御和从人为失误、恶意攻击和灾难而导致的故障	确保IT服务中断或变更对业务影响的最小化	确保所必需的IT服务是可用的	提高IT成本效益和对业务收益的贡献	及时、按照预算和符合质量标准地完成项目	维持信息和基础设施的完整性	确保IT遵循法律、法规和合同	确保IT具有基于成本效益的服务质量、持续改进和对未来变化的准备
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
计划和组织																												
P01 定义IT战略规划	4	4																										
P02定义信息架构	4			4	4						4																	
P03确定技术方向							4								4													
P04 定义IT流程、组织和关系	4	4			4																							
P05 IT投资管理												4												4				4
P06 沟通管理目标和方向												4	4						4	4	4	4						
P07 IT人力资源管理					4				4																			
P08质量管理			4													4									4			
P09 IT风险评估及管理														4			4	4										
P010项目管理	4	4																							4			
获取和实施																												
AI1识别自动化解决方案	4					4																						
AI2应用系统开发与维护						4	4																					
AI3技术基础设施的获取与维护					4			4							4													
AI4运营知识保障			4								4		4			4												
AI5 IT资源获取							4	4	4																			
AI6变更管理	4					4										4						4				4		
AI7系统测试与发布	4									4			4			4				4	4							
服务提供和支持																												
DS1服务水平管理	4		4									4																
DS2第三方服务管理			4							4		4																
DS3性能和容量管理	4														4								4					
DS4 确保持续服务																					4	4	4					
DS5确保系统安全														4					4	4	4					4		
DS6成本确认和分摊												4												4				4
DS7教育和培训用户			4										4		4													
DS8服务台和事件管理			4										4										4					
DS9配置管理														4	4													
DS10问题管理			4													4	4											
DS11数据管理				4															4								4	
DS12物理环境管理														4					4		4	4						
DS13运营管理			4																		4		4					
监控与评价																												
ME1 IT绩效监控与评价	4	4										4																4
ME2内部控制监控与评价														4			4				4						4	
ME3 确保遵循外部要求																											4	
ME4提供 IT治理		4										4															4	4

附录 II 流程与 IT 治理关注领域、COSO、COBIT IT 资源和 COBIT 信息标准的映射表

本附录提供了一个在 COBIT IT 管理流程和五个 IT 管理关注领域、COSO 的组件 IT 资源和信息标准之间的映射表。该表也提供了基于 COBIT 在线（COBIT ONLINE）的关联重要性程度（高，中和低）。这个矩阵利用一页的篇幅概要地阐述了 COBIT 框架是如何落实 IT 治理、COSO 的要求，展示 IT 流程与 IT 资源和信息标准之间的关联关系。P 标识主要相关，S 标识次要相关，既没有 P 也没有 S 并不意味着它们之间没有关系，而仅仅表示不重要或者关系不大。该重要程度值是基于调查和专家的意见，仅供参考。使用者应该考虑在他们的组织当中哪些流程是最重要的。

附录 II—IT 流程与 IT 治理关注领域、COSO、CobiT IT 资源和 CobiT 信息标准映射表

控制点	重要性	IT 治理关注领域					COSO					CobiT IT 资源				CobiT 信息标准						
		战略整合	价值交付	资源管理	风险管理	绩效考评	控制环境	风险评估	控制活动	信息和交流	监控	应用系统	信息	基础设施	人员	效果	效率	保密性	完整性	可用性	符合性	可靠性
计划和组织																						
PO1 定义 IT 战略规划	H	P		S	S			P		S	S	√	√	√	√	P	S					
PO2 定义信息架构	L	P	S	P	S				P	P		√	√			S	P	S	P			
PO3 确定技术方向	M	S	S	P	S			S	P	S		√		√		P	P					
PO4 定义 IT 流程、组织和关系	L	S		P	P		P			S	S				√	P	P					
PO5 IT 投资管理	M	S	P	S		S		S	P			√		√	√	P	P					S
PO6 沟通管理目标和方向	M	P			P		P			P			√		√	P					S	
PO7 IT 人力资源管理	L	P		P	S	S	P			S					√	P	P					
PO8 质量管理	M	P	S		S		P		P	S	P	√	√	√	√	P	P		S			S
PO9 IT 风险评估及管理	H	P			P			P				√	√	√	√	S	S	P	P	P	S	S
PO10 项目管理	H	P	S	S	S	S	S	S	P		S	√		√	√	P	P					
获取和实施																						
AI1 识别自动化解决方案	M	P	P	S	S				P			√		√		P	S					

控制点	重要性	IT 治理关注领域					COSO					CobiT IT 资源				CobiT 信息标准						
		战略整合	价值交付	资源管理	风险管理	绩效考评	控制环境	风险评估	控制活动	信息和交流	监控	应用系统	信息	基础设施	人员	效果	效率	保密性	完整性	可用性	符合性	可靠性
AI2 应用系统开发与维护	M	P	P		S				P			√				P	P		S			S
AI3 技术基础设施的获取与维护	L			P					P					√		S	P		S	S		
AI4 运营知识保障	L	S	P	S	S				P	S		√		√	√	P	P		S	S	S	S
AI5 IT 资源获取	M		S	P					P			√	√	√	√	S	P				S	
AI6 变更管理	H		P	S				S	P		S	√	√	√	√	P	P		P	P		S
AI7 系统测试与发布	M	S	P	S	S	S			P	S	S	√	√	√	√	P	S		S	S		
服务提供和支持																						
DS1 服务水平的定义和管理	M	P	P	P		P	S	P		S	S	√	√	√	√	P	P	S	S	S	S	S
DS2 第三方服务管理	L		P	S	P	S	P	S	P		S	√	√	√	√	P	P	S	S	S	S	S
DS3 容量和性能管理	L	S	S	P	S	S			P		S	√		√		P	P			S		
DS4 确保持续服务	M	S	P	S	P	S	S		P	S		√	√	√	√	P	S			P		
DS5 确保系统安全	H				P				P	S	S	√	√	√	√			P	P	S	S	S
DS6 成本确认和分摊	L		S	P		S			P			√	√	√	√		P					P
DS7 教育和培训用户	L	S	P	S	S		P			S					√	P	S					
DS8 服务台和事件管理	L		P			S	S			P	P	√			√	P	P					

控制点	重要性	IT 治理关注领域					COSO					CobiT IT 资源				CobiT 信息标准						
		战略整合	价值交付	资源管理	风险管理	绩效考评	控制环境	风险评估	控制活动	信息和交流	监控	应用系统	信息	基础设施	人员	效果	效率	保密性	完整性	可用性	符合性	可靠性
DS9 配置管理	M		P	P	S				P			√	√	√		P	S			S		S
DS10 问题管理	M		P		S	S			P	S	S	√	√	√	√	P	S			S		
DS11 数据管理	H		P	P	P				P				√						P			P
DS12 物理环境管理	L			S	P			S	P					√					P	P		
DS13 运营管理	L			P					P	S		√	√	√	√	P	P		S	S		
监控与评价																						
ME1IT 绩效监控与评价	H	S	S	S	S	P				S	P	√	√	√	√	P	P	S	S	S	S	S
ME2 内部控制监控与评价	M		P		P						P	√	√	√	√	P	P	S	S	S	S	S
ME3 确保遵循外部要求	H	P			P				P	S	S	√	√	√	√						P	S
ME4 提供 IT 治理	H	P	P	P	P	P	P	S		S	P	√	√	√	√	P	P	S	S	S	S	S

备注：这个 COSO 映射图是基于最初的 COSO 框架。该映射图通常也适用于随后的 COSO 企业风险管理—完整的框架，它被推广用于内部控制，更好和更广阔的关注企业风险管理领域。同时，它并非致力于也没有替代原有的 COSO 内部控制框架，只是在其中内嵌了内部控制框架，CobiT 用户可以选择参照这个企业风险管理框架来满足他们的内部控制需求并转向一个完整的风险管理流程。

附录 III 内部控制成熟度模型

这个附录提供了通用的成熟度模型，它展示了企业内部控制环境的状态和内部控制的建立。该附录说明了内部控制如何管理，建立良好内部控制的必要性，以及如何将内部控制从初始级发展为优化级。该模型提供高端指南，有助于 COBIT 用户清楚 IT 有效的内部控制需要什么，并定位企业的成熟度等级。

附录 III－内部控制成熟度模型

成熟等级	内部控制环境状态	内部控制的建立
0 无级别	没有认识到内部控制的必要性。控制不是组织文化或使命的一部分。存在控制缺乏和事件的高风险。	没有评估内部控制必要性的意识。事件升级时才被处理。
1 初始级	对内部控制必要性有一定认识。风险和控制需求的方法是非正式和无组织的，没有沟通或监控。不足没有被识别出来。雇员不知道他们的职责。	没有评估需要什么 IT 控制的意识。当执行高层次评估时，对重要事件的反应只是在非正式的基础之上。评估只涉及实际发生的事件。
2 可重复级	控制适当但是没有文件化。运营依靠的是个人的认识和动机。有效性没有得到充分的评价。存在较多控制缺陷并且没有充分的定位；可能有严重影响。解决控制问题的管理行为没有前瞻性或一致性。雇员可能不知道他们的职责。	控制必要性的评估只是在需要选择 IT 流程以测量当前控制成熟度水平、应当达到的与现有的控制水平的差距时发生。一个非正式的研讨方法，包括 IT 管理者和参与这个流程的团队，被用来定义一个适当的方法来控制这个流程并且推动一个商定的行动计划。
3 定义级	控制适当而且被充分的文件化。运营的有效性被定期评价并且有问题的平均数量。然而，评估流程没有文件化。当管理层能够处理预期的大部分控制问题时，存在一些控制弱点而且影响仍然严重。雇员知道他们的有关控制的职责。	基于价值和风险驱动来识别关键 IT 流程。通过详细分析来识别控制需求、差距的根本原因和开发改进的时机。除专题研讨会外，使用工具和访谈以支持分析结论，确保 IT 流程所有者拥有并且推动评估和改进流程。
4 可管理级	存在有效的内部控制和风险管理环境。定期进行正式的文件化控制评估。很多控制是自动化的并且被定期审查。管理层很可能检测到大部分控制问题。一致致力于已识别控制缺陷的解决。有限的、战术层面的技术被应用到自动化控制中。	IT 流程关键程度在相应业务流程所有者的充分的支持和协商下被定期的定义。控制需求的评估是基于这些流程的政策和实际成熟度，根据一个包括关键利益相关方的全面和标准的分析。这些评估的责任是清晰和强制性的。改进策略得到业务支持。达到期望结果的绩效被一贯地监控。有时组织外部控制审阅。
5 优化级	整个企业的风险和控制程序提供了持续和有效的控制及风险问题的解决方法。内部控制和风险管理与企业实践整合在一起，企业实践由自动化的实时监控所支持，该监控全面负责控制监控、风险管理和合规执行。控制评估是持续的，是基于自我评估、差距和根本原因分析的。雇员主动参与控制改进。	业务变更考虑 IT 流程的关键性，并且包含任何重新评估流程控制能力的必要性。IT 流程的所有者定期执行自我评估，确认控制处于符合业务需要的正确的成熟度水平，考虑了成熟度的属性以找到使控制更加有效和高效的途径。组织根据外部最佳实践来制定标准，并寻求内部控制有效性的外部建议。对于关键流程，采取独立的审阅，以提供控制在所需的成熟度水平和按计划工作的保证。

附录 IV 主要参考资料

在早期的 COBIT 开发和更新活动中，使用了超过 40 个国际上详细的 IT 标准、框架、指南和最佳实践，以确保 COBIT 在 IT 治理和控制的所有领域中的完整性。

因为 COBIT 专注于需要“什么”以达到足够的 IT 管理和控制，所以其定位在高层次。更多详细的 IT 标准和最佳实践处于详细描述“如何”去管理和控制 IT 具体方面的低层次。COBIT 将与治理和业务需求相关的理论框架之下的这些不同指引、概括性关键目标进行了整合。

这次 COBIT 更新（COBIT4.1），主要参考了 6 个与 IT 相关的全球标准、框架和实践，以确保适当的覆盖、持续性和一致性。它们是：

- COSO：

  Internal Control—Integrated Framework(内部控制—整合框架)，1994

  Enterprise Risk Management—Integrated Framework(企业风险管理—整合框架)，2004

- Office of Government Commerce（OGC®,英国商务部）：

  IT Infrastructure Library®（ITIL®），1999—2004

- International Organisation for Standardisation(ISO/IEC 27000,国际标准化组织)：
- Software Engineering Institute（SEI®,软件工程协会）：

  SEI Capability Maturity Model（CMM®），1993

  SEI Capability Maturity Model Integration（CMMI®），2000

- Project Management Institute（PMI®,美国项目管理协会）：

  A Guide to the Project Management Body of Knowledge（PMBOK），2004

- Information Security Forum（ISF，互联网安全研讨会）：

  The Standard of Good Practice for Information Security，2003

此外还参考了：

- IT Control Objectives for Sarbanes-Oxley(萨班斯-奥克斯利法案的IT控制目标)：*The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting, 2nd Edition,* IT Governance Institute, *USA (2006)*
- *CISA Review Manual*, ISACA (2006)

附录 V CobiT 第三版与 CobiT4.1 之间的对照

框架标准的变更

CobiT4.0的升级结果，对CobiT框架最主要的变更如下：

- M域变成ME,代表“监控和评价”。
- 删除了M3和M4，因为它们被许多的IT审计标准充分涵盖，是审计流程并不是IT流程,但索引被保留在本次升级后的框架中，以突出管理层对保证部门的需要和使用。
- ME3是与监管失察相关的流程，以前曾被PO8涵盖。
- ME4是与IT治理失察相关的流程，作为一个IT治理治理框架与CobiT的目的一致。该流程定位为IT治理链的最后一环，它强调为在企业中实施有效的IT治理最终目标，对前面的每一个流程提供支持。
- 由于PO8的删除，使得PO9*风险评估*和PO10*项目管理*与CobiT第三版的编号一致，PO8变成了质量管理，即原来的PO11流程。PO域现在有10个流程，取代了原来的11个流程。
- AI域有两处变更：获取流程的增加和包含在AI5的版本管理。后者在本次升级时放在了AI域的最后一个流程，即AI7中。AI5中“获取流程”这部分作为一个新的获取流程单独增加。AI域现在有7个流程，替代了原来的6个流程。

CobiT4.1,对CobiT4.0作了增量更新，包括:

- 增强了高级管理层的总体视角
- 在框架部分对目标和指标的说明
- 核心概念更好的定义。着重叙述变更的控制目标的定义，更强调管理层实践的叙述。
- 通过控制实践和VAL IT开发活动，对控制目标进行改进。一些控制目标被整合和/或重述以避免交迭，并且使控制目标的各个要点在一个流程中更加一致。这些变更使得剩余的控制目标重新编号。其他的一些控制目标被重述，使其更具行动导向，并保持措辞一致。具体修订包括：
  - AI5.5和AI5.6被组合到AI5.4中
  - AI7.9、AI7.10 和 AI7.11被组合到AI7.8中
  - ME3被修订，包括遵循除法律和法规需求之外的合同需求
- 基于支持控制有效性评估和报告，应用控制被改写得更有效。即用6个应用控制代替了CobiT4.0中18个应用控制，更详细的细节在CobiT控制实践第二版中提供。
- 根据安特卫普管理大学（比利时）验证研究得到的新观点，改进了附录1中的业务目标和IT目标要点。
- 扩大了提供CobiT流程的快捷参考目录活页，修订了包括CobiT框架的各个流程和应用控制要素的描述域的概述图。
- 对CobiT用户(CobiT 4.0和CobiT Online)提出的改进建议进行了评审，并适当合并在正文中。

控制目标

从上述控制标准的变更和阐明及关注控制目标内容可以看出，CobiT框架的升级已经大大改变了该框架内部的控制目标。控制目标已经从215个减少到了210个，因为所有的普通素材现在仅在框架标准中保留，并在每一个流程中没有重复。而且，所有应用控制参考移到框架和具体控制目标中，这些框架和具体控制目标被合并到新的陈述中。支持与控制目标相关的过渡活动，下面两套表格说明了新旧控制目标之间的交叉参考。

管理指南

添加了输入和输出，以表示该流程需要其他流程输入什么，该流程主要提供什么。也描述了活动和相关的职责。输入和活动目标取代了COBIT第三版的关键成功因素。衡量指标现在基于业务目标、IT目标、流程目标和活动目标的层层细化并保持一致。评审并增强了COBIT第三版的衡量指标集，以使其更具代表性和可测量性。

交叉参考：COBIT 第 3 版到 COBIT4.1

COBIT3.0	COBIT4.1
PO1 定义 IT 战略规划	
1.1IT 作为组织长短期计划的一部分	1.4
1.2IT 长期计划	1.4
1.3IT 长期计划编制-方法和结构	1.4
1.4IT 长期计划变更	1.4
1.5IT 部门的短期计划编制	1.5
1.6IT 计划的沟通	1.4
1.7IT 计划的监控和评价	1.3
1.8 现有系统的评估	1.3
PO2 定义信息架构	
2.1 信息架构模型	2.1
2.2 公司数据字典和数据语法规则	2.2
2.3 数据分类计划	2.3
2.4 安全级别	2.3
PO3 确定技术方向	
3.1 技术基础设施计划编制	3.1
3.2 监控未来趋势和监管要求	3.3
3.3 技术基础设施例外	3.1
3.4 硬件和软件获取计划	3.1，AI3.1
3.5 技术标准	3.4，3.5
PO4 定义 IT 组织和关系	
4.1IT 计划编制或执行委员会	4.3
4.2IT 部门的组织定位	4.4
4.3 组织达成的评审	4.5
4.4 角色和职责	4.6
4.5 质量保证职责	4.7
4.6 逻辑和物理安全职责	4.8
4.7 所有权和管理权	4.9
4.8 数据和系统所有权	4.9
4.9 监督	4.10
4.10 职责分离	4.11
4.11IT 职位	4.12
4.12IT 人员的工作或职位描述	4.6
4.13 关键 IT 人员	4.13
4.14 签约人员政策和程序	4.14
4.15 关系	4.15
PO5 IT 投资管理	
5.1 年度 IT 运行预算	5.3
5.2 成本收益监控	5.4
5.3 成本收益评判	1.1，5.3，5.4,5.5
PO6 沟通管理目标和方向	
6.1 信息控制环境	6.1
6.2 管理层的政策职责	6.3，6.4，6.5
6.3 组织政策的沟通	6.3，6.4，6.5
6.4 政策实施资源	6.4
6.5 政策维护	6.3，6.4，6.5
6.6 政策、程序和标准的符合性	6.3，6.4，6.5
6.7 质量承诺	6.3，6.4，6.5
6.8 安全和内部控制框架政策	6.2
6.9 知识产权	6.3，6.4，6.5
6.10 特殊问题政策	6.3，6.4，6.5
6.11IT 安全意识的沟通	6.3，6.4，6.5
PO7 人力资源管理	
7.1 人员招聘	7.1
7.2 人员资格	7.2
7.3 角色和职责	7.4
7.4 人员培训	7.5
7.5 交叉培训或人员备份	7.6
7.6 人员解雇程序	7.7
7.7 雇员工作绩效评估	7.8
7.8 工作变更和终结	7.8
PO8 确保遵循外部需求	
8.1 外部需求评审	ME3.1
8.2 遵循外部需求的实践和程序	ME3.2
8.3 安全和人文环境符合性	ME3.1
8.4 私有、知识产权和数据流	ME3.1

COBIT4.1

COBIT 3.0	COBIT 4.1
8.5 电子商务	ME3.1
8.6 遵循保险合约	ME3.1
PO9 评估风险	
9.1 业务风险评估	9.1，9.2，9.4
9.2 风险评估方法	9.4
9.3 风险识别	9.3
9.4 风险测量	9.1，9.2，9.3，9.4
9.5 风险行动计划	9.5
9.6 风险接受	9.5
9.7 安全措施选择	9.5
9.8 风险评估承诺	9.1
PO10 项目管理	
10.1 项目管理框架	10.2
10.2 用户部门参与项目启动	10.4
10.3 项目团队成员与职责	10.8

COBIT 3.0	COBIT 4.1
10.4 项目定义	10.5
10.5 项目审批	10.6
10.6 项目阶段审批	10.6
10.7 项目主计划	10.7
10.8 系统质量保证计划	10.10
10.9 计划编制的保证方式	10.12
10.10 正式的项目风险管理	10.9
10.11 测试计划	AI7.2
10.12 培训计划	AI7.1
10.13 实施后评估计划	10.14（部分）
PO11 质量管理	
11.1 总体质量计划	8.5
11.2QA 方法	8.1
11.3QA 计划编制	8.1
11.4IT 标准和程序的评审	8.1，8.2

COBIT 3.0	COBIT 4.1
11.5 系统开发生命周期方法论	8.2，8.3
11.6 现有技术重大变更的 SDLC 方法论	8.2，8.3
11.7SDLC 方法论更新	8.2，8.3
11.8 联合分类和沟通	8.2
11.9 获取和维护技术基础框架	8.2
11.10 第三方实施关联	8.2，DS2.3
11.11 程序文档标准	AI4.2, AI4.3, AI4.4
11.12 项目群测试标准	AI7.2，AI7.4
11.13 系统测试标准	AI7.2，AI7.4
11.14 并行/现场测试	AI7.2，AI7.4
11.15 系统测试文档	AI7.2，AI7.4
11.16 开发标准的 QA 评估	8.2
11.17IT 目标达成的 QA 评审	8.2
11.18 质量度量	8.6
11.19QA 评审报告	8.2

COBIT 3.0	COBIT 4.1
AI1 识别自动化解决方案	
1.1 信息需求定义	1.1
1.2 实施路线选择说明	1.3，5.1，PO1.4
1.3 获取战略说明	1.3，5.1，PO4.1
1.4 第三方服务需求	5.1，5.3
1.5 技术可行性研究	1.3

COBIT 3.0	COBIT 4.1
1.6 经济可行性研究	1.3
1.7 信息架构	1.3
1.8 风险分析报告	1.2
1.9 成本有效的安全控制	1.1，1.2
1.10 审计轨迹测试	1.1，1.2
1.11 功效学	1.1

COBIT 3.0	COBIT 4.1
1.12 系统软件的选取	1.1，1.3
1.13 采购控制	5.1
1.14 软件产品获取	5.1
1.15 第三方软件维护	5.4
1.16 合同应用程序	5.4
1.17 设施的接收	5.4

COBIT 3.0	COBIT 4.1
1.18 技术的接收	3.1，3.2，3.3，5.4
AI2 获取和维护应用软件	
2.1 设计方法	2.1
2.2 现存系统的主要变更	2.1，2.2，2.6
2.3 设计批准	2.1
2.4 文件需求定义和相关文档	2.2
2.5 程序说明书	2.2
2.6 源数据收集设计	2.2
2.7 输入需求定义和文档化	2.2
2.8 接口定义	2.2
2.9 人机接口	2.2
2.10 流程需求定义和相关文档	2.2
2.11 输出需求定义和相关文档	2.2
2.12 可控能力	2.3，2.4
2.13 作为关键设计因素的可用性	2.2
2.14 应用程序软件的 IT 完整性规定	2.3，DS11.5
2.15 应用软件测试	2.8，7.4
2.16 用户参考和支持资料	4.3，4.4
2.17 系统设计的重评估	2.2
AI3 获取和维护技术基础设施	
3.1 新硬件和软件评估	3.1，3.2，3.3
3.2 硬件预防性维护	DS13.5

COBIT 3.0	COBIT 4.1
3.3 系统软件安全	3.1，3.2，3.3
3.4 系统软件安装	3.1、3.2、3.3
3.5 系统软件维护	3.3
3.6 系统软件变更控制	6.1，7.3
3.7 系统功用的使用和监控	3.2，3.3，DS9.3
AI4 开发和维护程序	
4.1 运营需求和服务等级	4.1
4.2 用户流程手册	4.2
4.3 操作手册	4.4
4.4 培训材料	4.3，4.4
AI5 系统上线和发布	
5.1 培训	7.1
5.2 应用系统软件性能分配	7.6，DS3.1
5.3 实施方案	7.2，7.3
5.4 系统转化	7.5
5.5 数据转换	7.5
5.6 测试的策略和方案	7.2
5.7 变更测试	7.4，7.6
5.8 并行/初步标准和性能的测试	7.6
5.9 最终接收测试	7.7
5.10 安全测试和上线	7.6
5.11 运营测试	7.6

COBIT 3.0	COBIT 4.1
5.12 系统上线	7.8
5.13 满足用户需求的评估	7.9
5.14 管理层的实施后评审	7.9
AI6 变更管理	
6.1 变更管理发起和控制	6.1，6.4
6.2 影响评估	6.2
6.3 变更控制	7.9
6.4 紧急变更	6.3
6.5 文档和程序	6.5
6.6 授权的维护	DS5.3
6.7 软件版本策略	7.9
6.8 软件发布	7.9

COBIT 3.0	COBIT 4.1
DS1 定义和管理服务水平	
1.1 服务水平协议架构	1.1
1.2 服务水平协议的情况	1.3
1.3 性能程序	1.1
1.4 监控和报告	1.5
1.5 服务水平协议和合同评估	1.6
1.6 责任条款	1.3
1.7 服务改进程序	1.6
DS2 管理第三方服务	
2.1 供应商接口	2.1
2.2 所有者关系	2.2
2.3 第三方合同	AI5.2
2.4 第三方资格	AI5.3
2.5 外购条款	AI5.2
2.6 服务的连续性	2.3
2.7 安全关系	2.3
2.8 监控	2.4
DS3 性能和容量管理	
3.1 可用性和性能需求	3.1
3.2 可用性方案	3.4
3.3 监控和报告	3.5

COBIT 3.0	COBIT 4.1
3.4 模型工具	3.1
3.5 未来性能管理	3.3
3.6 工作量预测	3.3
3.7 资源的容量管理	3.2
3.8 资源的可用性	3.4
3.9 资源调度	3.4
DS4 确保持续服务	
4.1IT 持续性框架	4.1
4.2 持续性计划策略和哲理	4.1
4.3IT 持续性计划的内容	4.2
4.4IT 持续性需求的最小化	4.3
4.5 维护 IT 持续性计划	4.4
4.6 测试 IT 持续性计划	4.5
4.7IT 持续性计划培训	4.6
4.8IT 持续性计划发布	4.7
4.9 用户部门可选流程备份程序	4.8
4.10 关键 IT 资源	4.3
4.11 备份场所和硬件	4.8
4.12 异地备份存储	4.9
4.13 恢复程序	4.10
DS5 确保系统安全	

COBIT 3.0	COBIT 4.1
5.1 管理安全措施	5.1
5.2 识别、授权和访问	5.3
5.3 联机访问数据的安全	5.3
5.4 用户账户管理	5.4
5.5 用户账户评估管理	5.4
5.6 用户账户的用户控制	5.4，5.5
5.7 安全监控	5.5
5.8 数据分级	PO2.3
5.9 一般性识别和访问权力管理	5.3
5.10 违反和安全活动报告	5.5
5.11 事件处理	5.6
5.12 重新认证	5.1
5.13 相对人的信任	5.3AC6
5.14 交易授权	5.3
5.15 不可抵赖	5.11
5.16 可信路径	5.11
5.17 安全功能的保护	5.7
5.18 关键密码的管理	5.8
5.19 恶意软件的防范、发现和纠正	5.9
5.20 与公网的连结和防火墙的建设	5.10
5.21 电子交易的防护	13.4

CobiT 3.0	CobiT 4.1
DS6 确认和分摊成本	
6.1 责任条款	6.1
6.2 成本程序	6.3
6.3 用户计费和分发程序	6.2，6.4
DS7 教育和培训用户	
7.1 培训需求的识别	7.1
7.2 培训组织	7.2
7.3 安全原则和对培训的了解	PO7.4
DS8 辅助和建议客户	
8.1 服务台	8.1，8.5
8.2 客户队列登记	8.2，8.3，8.4
8.3 客户队列升级	8.3
8.4 清除监控	10.3
8.5 报告和趋势分析	10.1
DS9 配置管理	
9.1 配置记录	9.1
9.2 配置基线	9.1
9.3 状态检查	9.3
9.4 配置控制	9.3
9.5 未授权软件	9.3

CobiT 3.0	CobiT 4.1
9.6 软件存储	AI3.4
9.7 配置管理程序	9.2
9.8 软件责任性	9.1，9.2
DS10 问题和事件管理	
10.1 问题管理系统	10.1，10.2，10.3，10.4
10.2 问题升级	10.2
10.3 问题跟踪和审计轨迹	8.2，10.2
10.4 紧急和临时访问授权	5.4，12.3，AI6.3
10.5 紧急流程的优先级	10.1，8.3
DS11 数据管理	
11.1 数据准备程序	AC1
11.2 源文件授权程序	AC1
11.3 源文件数据收集	AC1
11.4 源文件错误处理	AC1
11.5 源文件保留	DS11.2
11.6 数据输入授权程序	AC2
11.7 准确性、完整性和授权检查	AC3
11.8 数据输入错误处理	AC2，AC4
11.9 数据处理的完整性	AC4
11.10 数据处理的确认和编辑	AC4
11.11 数据处理的错误处理	AC4

CobiT 3.0	CobiT 4.1
11.12 输出处理和保留	AC5，11.2
11.13 输出分布	AC5，AC6
11.14 输出平衡和调节	AC5
11.15 输出评估和错误处理	AC5
11.16 对输出报告的安全保护	11.6
11.17 在转送和运输中对敏感数据的保护	AC6，11.6
11.18 敏感数据倾向性保护	11.4，AC6
11.19 存储管理	11.2
11.20 保留时间和存储期限	11.2
11.21 媒体库管理系统	11.3
11.22 媒体库管理职责	11.3
11.23 备份和恢复	11.5
11.24 备份工作	11.4
11.25 备份存储	4.9，11.3
11.26 归档	11.2
11.27 敏感消息的管理	11．6
11.28 授权和完整性	AC6
11.29 电子交易的完整性	5.11
11.30 存储数据连续的完整性	11.2

COBIT 3.0	COBIT 4.1
DS12 设施管理	
12.1 物理环境安全	12.1，12.2
12.2IT 场所的低配置	12.1，12.2
12.3 参观者护送	12.3
12.4 职员健康和安全	12.1、12.5、ME3.1
12.5 环境因素的保护	12.4，12．9

COBIT 3.0	COBIT 4.1
12.6 不间断电源	12.5
DS13 运营管理	
13.1 运营流程和操作指南	13.1
13.2 流程启动和其他运营文档	13.1
13.3 作业调度	13.2
13.4 与标准作业调度的偏差	13.2

COBIT 3.0	COBIT 4.1
13.5 处理的持续性	13.1
13.6 运营日志	13.1
13.7 维护的特殊形式和输出设备	13.4
13.8 远程运营	5.11

COBIT 3.0	COBIT 4.1
M1 监控流程	
1.1 收集监控数据	1.2
1.2 评定性能	1.4
1.3 评定客户满意度	1.2
1.4 报告管理	1.5
M2 内部控制评价	
2.1 内部控制监控	2.2
2.2 内部控制的及时使用	2.1
2.3 内部控制水平报告	2.2，2.3
2.4 运营安全和内部控制保证	2.4

COBIT 3.0	COBIT 4.1
M3 获得独立保障	
3.1 独立安全和内部控制 IT 服务的认可/认证	2.5，4.7
3.2 独立安全和内部控制的第三方服务供应商的认可/认证	2.5，4.7
3.3 独立有效的 IT 服务评估	2.5，4.7
3.4 独立的有效的第三方供应商的评估	2.5，4.7
3.5 与法律、管理需求和和合同条款的符合性的独立保证	2.5，4.7
3.6 与第三方服务供应商之间的法律、管理需求和和合同条款的符合性独立保证	2.5，2.6，4.7
3.7 独立保证功能的能力	2.5，4.7
3.8 未来审计的内含	2.5，4.7

COBIT 3.0	COBIT 4.1
M4 提供独立审计	
4.1 审计章节	2.5，4.7
4.2 独立性	2.5，4.7
4.3 专业的道德规范和标准	2.5，4.7
4.4 完整性	2.5，4.7
4.5 规划	2.5，4.7
4.6 审计工作的表现	2.5，4.7
4.7 报告	2.5，4.7
4.8 后续活动	2.5，4.7

CobiT4.1 对照 CobiT 第 3 版

CobiT 4.1	CobiT 3.0
PO1 定义 IT 战略规划	
1.1 IT 价值管理	5.3
1.2 IT 与业务的一致性	New
1.3 当前能力和绩效的评估	1.7, 1.8
1.4 IT 战略计划	1.1、1.2、1.3、1.4、1.6 、AI1.2 、AI1.3
1.5 IT 战术计划	1.5
1.6 IT 投资组合管理	new
PO2 定义信息架构	
2.1 企业信息架构模型	2.1
2.2 企业数据字典和数据语法规则	2.2
2.3 数据分类计划	2.3, 2.4, DS5.8
2.4 完整性管理	New
PO3 确定技术方向	
3.1 技术方向计划	3.1, 3.3, 3.4
3.2 技术基础设施计划	New
3.3 监控未来发展趋势与合规性	3.2
3.4 技术标准	3.5
3.5 IT 架构委员会	3.5
PO4 定义 IT 流程、组织和关系	
4.1 IT 流程框架	New
4.2 IT 战略委员会	New
4.3 IT 执行委员会	4.1

CobiT 4.1	CobiT 3.0
4.12 IT 职位	4．11
4.13 关键 IT 职员	4．13
4.14 签约职员的政策和方法	4．14
4.15 关系	4．15
PO05 IT 投资管理	
5.1 财务管理框架	New
5.2 IT 预算内的优先级	New
5.3 编制 IT 预算	5.1, 5.3
5.4 成本管理	5.2, 5.3
5.5 收益管理	5．3
PO6 沟通管理目标和方向	
6.1 IT 策略和控制环境	6.1
6.2 企业 IT 风险和控制框架	6.8
6.3 IT 策略管理	6.2,6.3,6.5, 6.6, 6.7,6.9,6.10, 6.11
6.4 策略、标准与程序发布	6.2,6.3,6.5, 6.4, 6.6, 6.7, 6.9, 6.10, 6.11
6.5 IT 目标和方向的沟通	6.2,6.3,6.5, 6.6, 6.7, 6.9, 6.10, 6.11
PO7 IT 人力资源管理	
7.1 人员招聘和保持	7.1
7.2 人员能力	7.2
7.3 角色分配	New

CobiT 4.1	CobiT 3.0
8.3 标准的开发与获取	11.5, 11.6, 11.7
8.4 以客户为中心	New
8.5 持续改进	New
8.6 质量的测量、监视和评审	11.8
PO9 IT 风险评估及管理	
9.1 IT 风险管理框架	9.1,9.4,9.8
9.2 建立风险背景	9.1,9.4
9.3 事件识别	9.3,9.4
9.4 风险评估	9.1,9.2,9.4
9.5 风险响应	9.5,9.6,9.7
9.6 风险行动计划的维护和监控	New
PO10 项目管理	
10.1 项目群管理框架	New
10.2 项目管理框架	10.1
10.3 项目管理方法	New
10.4 利益相关的承诺	10.2
10.5 项目范围说明书	10.4
10.6 项目启动	10.5, 10.6
10.7 集成项目计划	10.7
10.8 项目资源	10.3
10.9 项目风险管理	10.10

4.4 IT 职能的组织定位	4.2
4.5 IT 组织结构	4.3
4.6 角色和职责的建立	4.4, 4.12
4.7 IT 质量保证职责	4.5
4.8 风险、安全和合规性职责	4.6
4.9 数据和系统所有者	4.7, 4.8
4.10 监督	4.9
4.11 职责分离	4.10

7.4 人员培训	7.3, DS7.3
7.5 对个体的依赖程度	7.4
7.6 人员选拔程序	7.5
7.7 雇员工作业绩评估	7.6
7.8 工作变更与终止	7.7, 7.8
PO8 质量管理	
8.1 质量管理体系	11.2,11.3,11.4
8.2 IT 标准与质量实践	11.5,11.6, 11.7, 11.8,11.9, 11.10, 11.16, 11.17,11.19

10.10 项目质量计划	10.8
10.11 项目变更控制	New
10.12 保障方法的项目计划	10.9
10.13 项目绩效测量、报告和监控	New
10.14 项目关闭	10.13 (part)

COBIT4.1	COBIT3.0
AI1 识别自动化解决方案	
1.1 定义和维护业务功能与技术需求	1.1, 1.9, 1.10, 1.11, 1.12
1.2 风险评估报告	1.8, 1.9, 1.10
1.3 可行性研究和供选的行动方案的简述	1.3, 1.7, 1.12
1.4 需求与可行性研究的决策和批准	new
AI2 应用系统开发及维护	
2.1 高层设计	2.1, 2.2
2.2 详细设计	2.2, 2.4, 2.5,2.6, 2.7, 2.8, 2.9, 2.10, 2.11,2.13, 2.17
2.3 应用控制和可审计性	2.12, 2.14

COBIT4.1	COBIT3.0
AI3 技术基础设施的获取和维护	
3.1 技术基础设施的获取计划	PO3.4, 1.18, 3.1, 3.3, 3.4
3.2 基础设施资源的保护和可用性	1.18, 3.1, 3.3, 3.4, 3.7
3.3 基础设施维护	1.18, 3.1, 3.3, 3.4, 3.5, 3.7
3.4 可行性验证环境	New
AI4 运营知识保障	
4.1 运营知识保障方案	4.1
4.2 向业务管理层知识转移	PO11.11, 4.2
4.3 向最终用户转移知识	PO11.11, 2.16, 4.4

COBIT4.1	COBIT3.0
AI6 变更管理	
6.1 变更标准和流程	3.6, 6.1
6.2 影响评估、优先级和授权	6.2
6.3 紧急变更	DS10.4, 6.4
6.4 变更状态跟踪和报告	6.1
6.5 变更的结束和文档	6.5
AI7 系统测试与发布	
7.1 用户培训	PO10.11, PO10.12, 5.1
7.2 测试方案	PO10.11, PO11.12, PO11.13, PO11.14, PO11.15, 5.3, 5.6

2.4 应用安全和可用性	2.12
2.5 外购应用软件的配置和实施	New
2.6 现有系统的重大升级	2.2
2.7 应用软件开发	New
2.8 软件质量保证	2.15
2.9 应用系统需求管理	New
2.10 应用系统维护	New

4.4 向运营维护人员转移知识	PO11.11, 2.16, 4.3, 4.4
AI5 IT 资源获取	
5.1 采购控制	1.2, 1.3, 1.4, 1.13, 1.14
5.2 供应商合同管理	DS2.3, DS2.5
5.3 选择供应商	1.4, DS2.4
5.4 IT 资源采购	1.15, 1.16, 1.17, 1.18

7.3 实施方案	3.6, 5.3
7.4 测试环境	PO11.12, PO11.13, PO11.14, PO11.15, 2.15, 5.7
7.5 系统切换和数据转换	5.4, 5.5
7.6 变更测试	5.2, 5.7, 5.8, 5.10, 5.11
7.7 最终验收测试	5.9
7.8 系统上线	5.12
7.9 实施后评审	5.13, 5.14

CobiT4.1

CobiT4.1	CobiT3.0
DS1 服务水平的定义和管理	
1.1 服务水平管理框架	1.1, 1.3
1.2 服务定义	New
1.3 服务水平协议	1.2, 1.6
1.4 运营水平协议	New
1.5 服务水平绩效的监控和报告	1.4
1.6 服务水平协议和合同的审阅	1.5、1.7
DS2 第三方服务的管理	
2.1 所有供应商关系的识别	2.1
2.2 供应商关系管理	2.2
2.3 供应商风险管理	PO11.10, 2.6, 2.7
2.4 供应商绩效监控	2.8
DS3 性能和容量管理	
3.1 性能和容量计划	AI5.2, 3.1, 3.4
3.2 当前性能和容量	3.7
3.3 未来性能和容量	3.5, 3.6
3.4 IT 资源的有效性	3.2, 3.8, 3.9
3.5 监控和报告	3.3
DS4 确保持续服务	
4.1 IT 持续性框架	4.1, 4.2
4.2 IT 持续性计划	4.3
4.3 关键 IT 资源	4.4, 4.10
4.4 IT 持续性计划的维护	4.5

CobiT4.1	CobiT3.0
DS5 确保系统安全	
5.1 IT 安全管理	5.1, 5.12
5.2 IT 安全计划	New
5.3 身份管理	5.2, 5.3, 5.9, 5.14, AI6.6
5.4 用户账户管理	5.4, 5.5, 5.6, 5.13, 10.4
5.5 安全测试与监控	5.6, 5.7, 5.10
5.6 安全事件定义	5.11
5.7 安全技术保护	5.17
5.8 密钥管理	5.18
5.9 恶意软件的预防、检测和纠正	5.19
5.10 网络安全	5.20
5.11 敏感数据交换	5.15, 5.16 11.29, 13.8
DS6 确认与分摊成本	
6.1 服务的定义	6.1
6.2 IT 会计	6.3
6.3 成本模型和收费	6.2
6.4 成本模型的维护	6.3
DS7 教育和培训用户	
7.1 教育和培训需求的识别	7.1
7.2 教育和培训的交付	7.2
7.3 培训评估	New
DS8 服务台和事件管理	
8.1 服务台	8.1

CobiT4.1	CobiT3.0
9.2 配置项的标识和维护	9.7, 9.8
9.3 配置的完整性检查	9.3, 9.4, 9.5
DS10 问题管理	
10.1 问题识别和分类	8.5, 10.1, 10.5
10.2 问题跟踪和解决	New
10.3 问题关闭	8.4, 10.1
10.4 配置、事件和问题管理的集成	New, 10.1
DS11 数据管理	
11.1 数据管理的业务需求	New
11.2 存储和保管方案	11.12, 11.19, 11.20, 11.26, 11.30
11.3 介质库管理系统	11.21, 11.22, 11.25
11.4 销毁	11.18, 11.24
11.5 备份和恢复	AI2.14, 11.23
11.6 数据管理的安全需求	11.16, 11.17, 11.27
DS12 物理环境管理	
12.1 地点的选择和规划	12.1, 12.2, 12.4
12.2 物理安全测量	12.1, 12.2
12.3 物理访问	10.4, 12.3
12.4 依据环境因素的保护	12.5
12.5 物理设施的管理	12.4, 12.6, 12.9
DS13 运营管理	
13.1 运营流程和操作指南	13.1, 13.2, 13.5, 13.6
13.2 作业调度	13.3, 13.4

4.5 IT 持续性计划的测试	4.6
4.6 IT 持续性计划的培训	4.7
4.7 IT 持续性计划的分发	4.8
4.8 IT 服务恢复和重新开始	4.9, 4.11
4.9 异地备份存储	4.12, 11.25
4.10 恢复后审查	4.13

8.2 登记客户质疑	8.2, 10.3
8.3 事件的逐步升级	8.2, 8.3, 10.5
8.4 事件关闭	8.2
8.5 报告和趋势分析	8.1
DS9 配置管理	
9.1 配置库和基线	9.1, 9.2, 9.8

13.3 IT 基础设施的监控	new
13.4 敏感资料和输出设备	5.21, 13.7
13.5 硬件的预防性维护	AI3.2

COBIT4.1	COBIT 3.0
ME1 IT 绩效监控与评价	
1.1 监控体系	1.0*
1.2 监控数据的收集和识别	1.1, 1.3
1.3 监控方法	New
1.4 业绩评价	1.2
1.5 董事会和管理层报告	1.4
1.6 整改措施	New
ME2 内部控制监控与评价	
2.1 监控内部控制框架	2.0*, 2.2
2.2 管理的评价	2.1, 2.3

COBIT 4.1	COBIT 3.0
2.3 控制例外事件	new
2.4 控制自我评估	2.4
2.5 内部控制保证	New
2.6 关于第三方的内部控制	3.6
2.7 整改措施	New
ME3 确保遵循外部要求	
3.1 识别外部法律、法规和协议的遵循性要求	PO8.1, PO8.3, PO8.4, PO8.5, PO8.6, DS12.4
3.2 优化对于外部要求的应对措施	PO8.2
3.3 评估外部要求的遵循性	New
3.4 积极保证遵循性	New
3.5 整合报告	New

COBIT 4.1	COBIT 3.0
ME4 提供 IT 治理	
4.1 制定 IT 治理框架	New
4.2 战略一致性	New
4.3 价值交付	New
4.4 资源管理	New
4.5 风险管理	
4.6 绩效测量	New
4.7 独立保障	New

附录 VI—研究与开发方法

COBIT 框架内容的开发受到 COBIT 指导委员会的监督，该委员会由来自工业、学术界、政府，以及 IT 治理、保证、控制和安全行业的国际代表组成。为了项目的临时研究与开发的可交付成果的质量保证和专家评审，建立了国际工作组。整个项目的指导由 ITGI 提供。

前期的 COBIT 版本

从在第一版中定义的 COBIT 框架入手，国际准则、指南和研究在最佳实践中的应用导致了控制目标的开发。审计指南随之被开发以评估这些控制目标是否被适当地实现。对第一和第二版的研究包括识别的国际原始资料的收集和分析，由在欧洲（阿姆斯特丹自由大学）、美国（加州科技大学）和澳大利亚（新南威尔士大学）的团队完成。研究人员负责编辑、审阅、评估和适当的合并了国际技术准则、行为规范、质量准则、审计专业准则以及产业实践和需求，因为这些标准规范等与框架和单个的控制目标有关。收集和分析完后，研究人员被要求深入地检验每个领域和流程，并且对特殊的 IT 流程提出新的或者改进的适用的控制目标建议。最终结果的合并整理由 COBIT 指导委员会来完成。

COBIT 第三版的修订工作包括根据新的和修订的国际参考文献编写管理指南，对 COBIT 第二版做升级。此外，修订完善了 COBIT 框架以支持不断增加的管理控制、引入绩效管理和促进 IT 治理。为管理层提供该框架的应用方法，以便能够评估和选择信息和相关技术的控制实施和改进，并测评绩效，管理指南包括成熟度模型、关键的成功因素、和控制目标有关的 KGIs 和 KPIs。

管理指南由来自世界范围的工业、学术界、政府，以及 IT 治理、保证、控制和安全行业的 40 位专家组成的研究小组开发完成。这些专家参与一个寄宿制的研究小组，研究小组由专业促进者进行指导，使用 COBIT 指导委员会定义的开发指南。该研究小组得到 Gartner Group 和 ricewaterhouseCoopers 的有力支持，他们不仅提供思路而且派出多名他们在控制、绩效管理和信息安全方面的专家。研究小组的成果是 COBIT 的 34 个流程描述的成熟度模型、CSFs、KGIs 和 KPIs 的草稿。最初可交付成果的质量保证由 COBIT 指导委员会执行，成果被发布在 ISACA 的网站上。当给完整性和一致性提供 COBIT 框架时，管理指南文件提供一个面向管理的新的工具集。

对 COBIT 第三版中控制目标的更新，以新的和修订的国际参考文献为基础，由 ISACA 分会成员在 COBIT 指导委员会会员的指导下进行。目的不是为了进行控制目标的所有内容的一个全面分析或者一次重新开发，而是为了提供一个增量更新流程。管理指南的开发结果被用于修订 COBIT 框架，尤其是流程描述的思考、目标和引擎语句。COBIT 第三版于 2000 年 7 月公开发表。

最近的修订活动

在不断发展 COBIT 知识体系的努力下，COBIT 指导委员会在过去的两年里已经启动了 COBIT 细节方面的研究。这些焦点研究项目陈述了控制目标和管理指南的组成。一些具体范围说明如下。

控制目标研究

- COBIT—IT 治理自底向上调整
- COBIT—IT 治理自顶向下调整
- COBIT 和其他详细准则—在 COBIT 和 ITIL、CMM、COSO、PMBOK、ISF’s *Standard of Good Practice for Information Security*（ISF 的信息安全最佳实践准则）和 ISO27000 之间的详细映射使得 COBIT 与这些准则在语言、定义和概念上保持一致。

管理指南研究

- KGI-KPI 临时关系分析
- KGIs/KPIs/CSFs 的质量的审阅—基于 KPI/KGI 临时关系分析，把 CSFs 划分成“你需要从别人那里得到什么”和“你自己需要做什么”
- 指标概念的详细分析—指标专家为升级指标概念而进行的详细开发，建立起一连串“流程-IT-业务”指标，并且为这些指标定义了质量标准。
- 业务目标、IT 目标和 IT 流程的链接—在 8 个不同行业的详细研究导致一个更详细的领悟，COBIT 流程如何支持具体 IT 目标的实现，扩展到如何支持业务目标的实现；结果随后被归纳
- 成熟度模型内容的审阅—确保流程之间和内部的成熟度水平的一致性和质量，包括更好的成熟度模型属性的定义

所有这些项目被 COBIT 指导委员会启动和监管，而日常管理和追踪则被一个较小的 COBIT 核心团队执行。大部分上述研究项目的实施基于 ISACA 会员、COBIT 用户、专家顾问和学术界人士的经验和志愿团队。本地开发组设立在布鲁塞尔（比利时）、伦敦（英格兰）、芝加哥（美国），坎培拉（澳大利亚首都地区）、开普敦（南非）、华盛顿（美国）和哥本哈根（丹麦），每个小组有 5 到 10 位 COBIT 用户，每年平均集中工作 2 到 3 次，完成由 COBIT 核心团体分配的具体研究和审阅任务。另外，一些具体的研究项目被分配给一些类似安特卫普管理大学（UAMS）和夏威夷大学的商业学校。

这些努力研究的结果，与历年来 COBIT 用户提供的反馈意见和象控制实践这样的新产品开发过程中记录的问题一起被加进主要的 COBIT 项目，以更新和改进控制目标、管理指南和框架。保留两个主要的开发实验室，每个包括超过 40 名来自全世界的 IT 治理、管理和控制方面的专家（经理、顾问、学术界人士和审计师），来审阅和全面升级控制目标和管理指南的内容。此外一些小的团队细化和完成由这些主要事件产生的有意义的输出。

最终的草稿受到一个有大约 100 个参与者的完全公开审阅流程的支配。收到的大量意见由 COBIT 指导委员会在一个最终审阅研讨会内进行分析。

这些研讨会的结果被 COBIT 指导委员会、COBIT 核心团队和 ITGI 加工以在这个卷内创造出新的 COBIT 素材。COBIT 在线的存在意味着现在有技术能够更容易的保持 COBIT 内容为最新，并且这种手段将被用作 COBIT 内容的主要知识库。它将被具体内容领域的定期审阅和来自用户库的反馈所维护。定期出版物（纸质和电子的）将被生成以为 COBIT 内容提供离线参考。

附录 VII 词汇表

序号	英文	中文	中文解释
1	Access control	访问控制	限制及控制访问计算机系统资源的规程，包括逻辑或物理控制以防止未经授权进入或使用。
2	Accountable	负责（责任人）	在 RACI 图中，指对执行活动进行授权和审批的人或团队
3	Activity	活动	针对 CobiT 流程所进行的主要行动
4	Application program	应用程序	对业务数据（如数据录入、更新或查询）进行处理的程序。应用程序是相对系统程序（如操作系统或网络控制程序）和实用程序（如排序或复制）而言的。
5	Audit charter	审计章程	经董事会批准的，定义内部审计活动目的 、授权和责任的文档
6	Authentication	鉴别	是指验证系统实体的身份（如，用户、系统、网络节点）和实体对计算机信息有适当的访问权限。用于防止欺诈登录的行为，也可以确保数据的正确性。
7	Automated application control	自动化的应用控制	一整套内嵌入自动化解决方案（应用系统）中的控制
8	Balanced scorecard	平衡记分卡	一整套的绩效考核指标，共分为四类，包括财务、客户新增、内部业务流程、学习与创新。由 Robert S. Kaplan and David P. Norton 92 年创建。
9	Benchmarking	标杆管理	与同业或竞争对手进行业绩比较的一套系统的方法，从而去学习最好的业务运作的方法（如，质量、后勤效率或其它的标杆管理）。
10	Best practice	最佳实践	成功用于多个企业的、经过验证的活动或流程。
11	Business process	业务流程	参考 Process
12	Capability	能力	履行或完成工作所需具备的特征
13	Capability Maturity Model (CMM)	能力成熟度模型	美国软件工程研究所（SEI）开发的、针对软件的成熟度模型。是许多组织用来识别最佳实践，帮助评估和提高软件开发过程中的成熟度的模型。
14	CEO	首席执行官	首席执行官，一个组织里职位最高的人
15	CFO	首席财务官	首席财务官，主要负责组织的财务风险管理的人
16	CIO	首席信息官	首席信息官，负责组织的 IT 团队的人。有些时候，CIO 角色扩大变成首席知识官（CKO），负责处理知识，而不仅仅是信息。也参见 CTO。
17	CTO	首席技术官	首席技术官，一个组织中关注技术保障的人。CTO 的头衔通常与 CIO 是一个意思。

序号	英文	中文	中文解释
18	Configuration item (CI)	配置项	在配置管理控制中的基础架构组件或者项目，如基础架构相关的变更需求。从完整的一个系统（包括所有硬件、软件和文档）到单个模块或小的硬件组件，配置项的复杂度、大小和类型都有很大的不同。
19	Configuration management	配置管理	在系统的生命周期中，对一组配置项变更进行的控制。
20	Consulted	商议	在 RACI 图中，指在活动中应寻求其意见的人（双向沟通）
21	Continuity	持续性	预防、减轻故障或从故障恢复。相关的术语“业务恢复计划”、“灾难恢复计划”和“持续性计划”也用在这，这些都集中在持续性的恢复方面。
22	Control framework	控制框架	对按照详细步骤执行控制过程所实现的预期结果或目标的描述。
23	Control objective	控制目标	通过在详细流程中实施控制规程而达成期望的结果和目的描述
24	Control practice	控制实践	通过合理的资源利用、适当的风险管理、保持 IT 与业务的一致性，从而实现控制目标的关键控制机制。
25	COSO	COSO	反虚假财务报告委员会（Tradeway）下属的发起人委员会，1992 年发布了内部控制总体框架并被国际广泛作为公司治理的标准。参阅 www.coso.org
26	CSF	关键成功因素	关键成功因素，在 IT 流程之内实现控制的最重要的观点或活动。
27	Dashboard	仪表板	为组织设定各个等级的目标，以实现对预期目标进行连续监控的工具
28	Data classification scheme	数据分级计划	根据关键程度、敏感度和所有权等因素，确定企业数据分类的计划
29	Data dictionary	数据字典	包括数据库每个数据元素的名字、类型、取值范围、源、访问授权的数据库。同时也指出哪个应用程序使用这些数据，所以当数据结构调整时，能生成其所影响的程序清单。数据字典可以是用于管理或记录目的的独立的信息系统或是对数据库操作的控制。
30	Data owners	数据所有者	对计算机数据的完整性、正确性和可用性负责的个人、一般为管理人员或主管。
31	Detective control	检查性控制	用来识别企业已经定义的、对流程或最终产品造成实质性影响的事件（预期或非预期）、错误或其它事情
32	Domain	域	在 COBIT 中， IT 生命周期中一组控制目标（PO、AI、DS、ME）的逻辑阶段
33	Enterprise	企业	为了共同目标一起工作的一组个体，通常的组织形式，如公司、公共机构、慈善机构或公信机构。
34	Enterprise architecture	企业架构	描述业务系统的组件、或业务系统的元素（如，技术）及相互关系和支持组织目标的方式等的总体和基础的设计

附录 VII

序号	英文	中文	中文解释
35	Enterprise architecture for IT	企业 IT 架构	描述有关业务的 IT 组件、组件间关系以及它们支持组织目标的方式等的总体和基础的设计
36	Enterprise governance	企业治理	董事会和高管层为维护战略方向而制定的一整套的职责和操作规程，以确保目标的实现、风险可控和企业资源的有效利用。
37	Framework	框架	参阅控制框架
38	General computer controls	一般控制	相对应用控制而言，与应用系统部署、维护、运行以确保系统可用等相关的环境。一般控制的目标是确保应用系统、完整的程序和数据文件以及操作系统得到合理的开发和实施。与应用控制一样，一般控制可能是人工的和自动的。比如，一般控制包括对按照信息系统策略和信息安全规定所做的开发和实施、对不相容岗位进行分离、灾难预防和恢复计划。
39	Guideline	指南	描述完成一件事情的详细方法，比规程少一些指令性的内容。
40	Information architecture	信息架构	IT 架构（包括应用系统和技术）的组件之一。参阅 IT 架构。
41	Informed	通告对象	在 RACI 图中，指应将最新活动进展情况通知到的人（单向沟通）
42	Internal control	内部控制	政策、计划和规程，以及确保实现业务目标和预防或发现并纠正非预期事件的组织架构。
43	ISO 17799	ISO 17799	定义信息机密性、完整性和可用性的国际标准
44	ISO 27001	ISO 27001	信息安全管理-详细的用户指南，替代 BS7799-2。意在向第三方审计提供基础，并与其它管理标准（如，ISO/IEC9001 和 14001）协调。
45	ISO 9001:2000	ISO 9001:2000	由国际标准化组织（ISO）发布的质量管理实践规则。ISO9001.2000，描述了针对任何一个需要证明有能力提供符合质量目标的产品或服务的组织所要执行的质量管理体系的详细要求。
46	IT	IT	信息技术，硬件、软件、通讯和其它用于不同形式数据的输入、存储、处理、传输和输出的设备
47	IT architecture	IT 架构	描述业务的 IT 组件及关系，支持组织目标的方式的总体和基础设计
48	ITIL	ITIL	英国官方商业治理（OGC）IT 基础库，一套用于管理和提供 IT 运营服务的指南。
49	IT incident	IT 事件	所有由非正常的操作，导致或可能导致中断或降低服务质量的事情
50	IT investment dashboard	IT 投资监控	设置组织不同层次的预期并对照支出目标和按照商业价值标准衡量的 IT 保障投资项目收益进行持续监控的工具。
51	IT strategic plan	IT 战略规划	一个长期的计划，如 3 至 5 年，业务与 IT 部门共同描绘 IT 资源如何为企业战略目标做出贡献。

序号	英文	中文	中文解释
52	IT strategy committee	IT 战略委员会	董事会层面的委员会，以确保落实董事会所关心的重大的 IT 困难/决议。委员会主要负责 IT 保障投资组合、IT 服务和其它 IT 资源。委员会是投资组合的所有者。
53	IT tactical plan	IT 战术计划	一个中期的计划，一般 6 至 18 个月，将 IT 战略规划转换为必要的提议、资源需求以及监管和管理资源及收益的方法。
54	IT user	IT 用户	运用 IT 去支持或实现业务目标的人
55	Key management practices	关键管理实践	成功执行业务流程所必需的管理实践
56	KGI	KGI	关键目标指标：事后向管理层报告 IT 流程是否完成业务需求、是否符合信息标准的约定的指标
57	KPI	KPI	关键绩效指标：衡量流程达到预期目标的程度。衡量是否达到预期目标的主要指标，是能力、实践和技术方面非常好的指标。它们衡量活动目标，以确定流程所有人是否为有效完成绩效采取了必要措施。
58	Maturity	成熟度	在业务领域，显示业务流程达到预期目标的可靠程度或可信赖程度
59	Measure	测评指标	用于评价和沟通绩效的标准。评价通常以自然数、金额、百分比等来计量，同时也可以采取如用户满意度等其它信息。报告和监控评价指标将帮助一个组织促进流程有效执行企业战略。
60	Metrics	度量	详细描述了如何对绩效进行定量地、周期性地评估。一个完整的试题定义使用的单元、频度、理想的目标值、实施测量的流程以及对评估流程的阐述。
61	OLA	OLA	运营水平协议:一个涵盖内部服务交付的协议，支持在服务交付内的 IT 运营。
62	Organisation	组织	企业的构成方式，也指实体。
63	Outcome measures	成果测量	测量描述了之前实施活动的结果，并且经常作为一个滞后的指标被提及。它们常常关注时间周期结束时的结果并描述历史绩。它们也经常作为关键目标指标（KGI）被提及，并被用来显示目标是否完成。这些只能在事后进行测量，因此被称作“滞后指标”。
64	Performance	绩效	在 IT 领域指一个流程实际的执行和成绩。
65	Performance drivers	绩效驱动	测量考虑到了滞后指标的驱动，它们在结果清楚之前可以被测量，因此被称作“提前指标”。在这两个指标之间存在一种假定的联系，即改良提前指标获得的绩效可以驱动滞后指标获得更好的绩效。它们也作为关键绩效指标（KPI）被提及，并被用来显示目标是否有可能完成。
66	Performance management	绩效管理	IT 领域管理所有测量类型的能力，包括职工、团队、流程和财务测量的。该术语意味着闭环控制和测量的规范化监控。
67	PMBOK	PMBOK	项目管理知识体系：项目管理协会（PMI）制定的一个项目管理标准。
68	PMO	PMO	项目管理官：该个体职责是为支持项目管理任务及推进项目管理纪律的具体措施的执行负责。

附录 VII

序号	英文	中文	中文解释
69	Policy	政策	通常，指一个记录了活动和做法的高级别的原则，这些活动和做法是通过决议的。政策的显著意图在于影响和指导目前和将来的决策要与企业管理团队建立的价值体系、目标和战略计划保持一致。
70	Portfolio	投资组合	一个程序、项目、选定的服务或者资产的组合，被管理和监控以使业务回报达到最优。
71	Preventive control	预防控制	一个内部控制，被用来预防不良事件、错误和其他组织已经确认对流程和最后结果有负面影响的事件。
72	PRINCE2	PRINCE2	OGC 制定的控制环境中的计划：项目管理方法涵盖项目的管理、控制和组织。
73	Problem	问题	在 IT 领域，一个或多个未知事件潜在的原因。
74	Procedure	程序	一份包含指定如何实现活动步骤的文件。程序作为流程的一部分被定义。
75	Process	流程	通常是受组织政策和规程影响的一系列程序的集合，流程需投入若干资源和利用这些投入，这些投入和资源可能来自于其他的流程。流程对现有系统、负有责任的流程所有者，围绕流程执行而制定的明确的角色和职责具有明确的业务动机和衡量绩效的方法。
76	Programme	规划	一组结构化相互依赖的项目，涵盖了所要求的业务、流程、人员和组织活动的全部范围（是必要的并充分的）以实现明确且详细的业务成果。
77	Project	项目	一系列结构化的活动，此活动关系到交付给组织既定的功能（对于实现所需的业务成果此活动是必要的但不是充分的）基于一致同意的时间表和预算。
78	QMS	QMS	质量管理体系：此体系概述了必要的政策和程序，以改进和控制的各种进程，最终会导致改善组织的表现。
79	RACI chart	RACI 图	描述在组织框架内哪些人是执行人、责任人、咨询者和通告对象的图表
80	Resilience	可伸缩性	系统或网络中断后的自动恢复能力，通常以最小影响为目标。
81	Responsible	执行人	在 RACI 图中，指必须确保活动能成功完成的人
82	Risk	风险	利用资产或资产组的弱点造成损失/破坏的潜在的可能性。通常是从影响和发生的可能性来评价。
83	Root cause analysis	问题根源分析	诊断事件源头的过程，可被用于从结果着手研究典型的错误或问题。
84	SDLC	系统开发生命周期	系统开发生命周期，软件开发或获取的各个阶段。典型的阶段包括可行性研究、需求分析、需求定义、 详细设计、编程、测试、安装和实施后检查，不包括服务交付或收益实现的活动。
85	Segregation/ separation of duties	职责分离	一个基本的内部控制措施，为预防和发现错误和异常，将初始化和记录交易、资产保管的职责分配给不同的个人。通常应用于大型 IT 组织，以避免单独一个人植入欺诈或恶意代码而未被发现。

序号	英文	中文	中文解释
86	Service desk	服务台	在 IT 组织内部、与 IT 服务的用户进行联系的一个点。
87	Service provider	服务提供方	向组织提供服务的外部实体
88	SLA	SLA	服务水平协议，在服务提供方与客户或用户签定的协议，定义了最低的服务指标以及如何衡量这些指标。
89	Standard	标准	强制的要求，如，ISO/IEC2000（国际标准），UNIX 配置的内部安全标准，或者是财务记录如何进行维护的官方标准。“标准”也通常指由如 ISO、BSI 等标准组织发布的实践准则或规范。
90	TCO	TCO	总成本，在 IT 方面包括： 计算机及软件的初始费用 硬件和软件升级 维护 技术支持 培训 用户执行的特定活动。
91	Technology infrastructure plan	技术基础设施计划	关于确保现在或今后处理或应用系统使用的技术、人力资源和设施的计划。

附录 VIII CobiT 及相关产品

在 4.0 及以上版本的 CobiT 体系中，包括：

- **框架**—描述 CobiT 是如何组织 IT 治理管理和从 IT 域、流程以及它们与业务需求的关系的控制目标及最佳实践。
- **流程描述**—包括 34 个覆盖 IT 所有领域的 IT 流程。
- **控制目标**—介绍通用的 IT 流程所对应的最佳管理目标。
- **管理指南**—介绍帮助划分责任、考核绩效、确定基准和落实差距的工具
- **成熟度模型**—描述 IT 流程现在和未来可能所处的状态

自 CobiT 诞生以来，CobiT 的核心内容得到持续优化，基于 CobiT 派生的著作数量一直在增加。下面是基于 CobiT 的出版物：

- *Board Briefing on IT Governance, 2nd Edition*(《供董事会参考的 IT 治理简介》（第 2 版）)——帮助管理人员理解 IT 治理为什么重要，结果是什么，他们的管理责任是什么？
- CobiT® Online（CobiT 在线）——允许用户为其企业定制自己的 CobiT，可以存储和应用所需要的版本。它可以提供在线的、实时的查询、随时提问，建立基线和新建一个便捷的、分享经验与问题的讨论。
- *CobiT® Control Practices*（CobiT 控制实践）：*Guidance to Achieve Control Objectives for Successful IT Governance, 2nd Edition*（《指导实现成功 IT 治理的控制目标》（第 2 版））——指导在实施控制目标时规避风险和获取价值，指导如何实现目标。强烈推荐与 *IT Governance Implementation Guide: Using CobiT® and Val ITTM, 2nd Edition*（《IT 治理实施指南：应用 CobiT 和 VAL IT 2.0 版》）一起使用。
- *IT Assurance Guide: Using CobiT®*(《IT 鉴证指南：使用 CobiT》)——介绍 CobiT 如何应用于支持多样的保证活动和对所有 CobiT IT 流程和控制目标所建议的测试步骤。它替代了《IT 审计指南》中的内容，用于对 CobiT4.1 的控制目标的审计和自评估。
- *IT Control Objectives for Sarbanes-Oxley: The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting, 2nd Edition*（《针对萨班斯-奥克斯利法案的 IT 控制目标：设计和执行基于财务报告的内部控制的 IT 角色》（第 2 版））——介绍如何保证遵循基于 CobiT 控制目标的 IT 环境的指南。
- *IT Governance Implementation Guide: Using CobiT® and Val ITTM, 2nd Edition*（《IT 治理实施指南：使用 CobiT 和 Val IT》（第 2 版））——介绍通用的、使用 CobiT 和 Val IT 及配套的工具包去开展 IT 治理的路线图。
- *CobiT® Quickstart, 2nd Edition Quickstart, 2nd Edition*（《CobiT 快速入门》）

——针对小企业和大企业的第一次应用，提供控制基线。

- *COBIT® Security Baseline, 2nd Edition*（《COBIT 安全基线》）——描述在企业内部开展信息安全工作的基本步骤。第二版正在编写。
- COBIT 映射图—当前发表在 www.isaca.org/downloads:
  - Aligning COBIT, ITIL and ISO 17799 for Business Benefit
  - COBIT Mapping: Overview of International IT Guidance, 2nd Edition
  - COBIT Mapping: Mapping of ISO/IEC 17799:2000 With COBIT, 2nd Edition
  - COBIT Mapping: Mapping of PMBOK With COBIT 4.0
  - COBIT Mapping: Mapping of SEI's CMM for Software With COBIT 4.0
  - COBIT Mapping: Mapping of ITIL With COBIT 4.0
  - COBIT Mapping: Mapping of PRINCE2 With COBIT 4.0
- *Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition*（《信息安全管理：董事会和高管层使用指南》（第 2 版））——介绍信息安全的业务条款、帮助发现与安全相关的问题的工具和技术。

Val IT 是总括术语，用于描述说明 Val IT 框架的出版物和将来补充的产品和活动。当前与 Val IT 相关的出版物有：

- *Enterprise Value: Governance of IT Investments—The Val IT™ Framework 2.0*（《企业价值：IT 投资管理—Val IT 框架》，介绍企业如何基于 COBIT 框架，从 IT 保障投资获取最理想的收益）。包括：
  - 三个流程—价值管理、投资组合管理 和投资管理
  - IT 关键管理实践—对实现预期结果或特定目标产生积极作用的最佳管理实践。它们支持 Val IT 流程，与实施 COBIT 控制目标发挥大致相同的作用。
- *Enterprise Value: Governance of IT Investments—The Business Case*（《企业价值：IT 投资管理—业务模式》），聚焦于投资管理流程的关键元素。
- *Enterprise Value: Governance of IT Investments—The ING Case Study*（《企业价值：IT 投资管理—ING 案例研究》），介绍一个全球性的金融服务企业如何在 Val IT 框架的背景下管理 IT 投资组合。

要获取更全面、更新的关于 COBIT、Val IT 以及相关著作、案例研究、培训信息、时事通讯和其它具体框架的信息，请访问 www.isaca.org/cobit 和 www.isaca.org/valit。