COBIT 2019

COBIT行业应用系列

银行业IT治理最佳实践

ISACA

银行业 IT 治理最佳实践

关于 ISACA

ISACA® 是享誉全球的信息安全专业机构，在其近 50 年历史中，致力于帮助专业人员和企业实现技术的最大潜力。当今世界为技术所驱动，ISACA 为全球专业人员提供知识、职业认证并打造社群网络，助力其职业进阶，推动他们所在的机构转型，通过技术实现创新。ISACA 全球社区中有 50 多万名从事信息与网络安全、治理、审计与鉴证、风险与创新工作的人员。ISACA 旗下的 CMMI 则专注于企业能力成熟度的评估与改进。ISACA 在全球 188 个国家和地区设有 215 个分会，并在美国和中国开设办公室。

免责声明

ISACA 设计并编制了 IT 治理最佳实践（下称“作品”），主要用作专业人员的学习资料。ISACA 无法保证使用本作品就一定能够实现成功的结果。本作品不应被视为包含所有适用的信息、程序和测试，不排除在其它信息、程序和测试的合理指导下获得同样结果的可能。在确定任何具体信息、程序或测试的适宜性时，专业人员应就具体的情况（特定的系统或信息技术环境）做出自己专业性的判断。

保留权利

ISACA

1700 E. Golf Road, Suite 400, Schaumburg, Illinois 60173, USA

电话 : +1.847.253.1545 传真 : +1.847.253.1443

网站：www.isaca.org

ISACA 中国

北京朝阳区东三环中路 20 号乐成中心 B 座 5 层 505 室

电子邮箱：ISACAChina@isaca.org

ISACA 中国微信公众号

他山之石可以攻玉

—— 将中国的实践经验推广到全球业界

当今 IT 治理专业人士必须面对的课题是，如何让自己所在企业利用技术推动业务表现的实质改善。

无论哪个行业或地区，技术进步在推动业务变革的同时，随之而来的必将是前所未有的挑战。当今的企业都在进行数字化转型以实现效率和创新升级，争取为利益相关方创造非凡价值。随着企业转向新技术，如人工智能、区块链、云平台以及未来几年将涌现的其他技术，发现并采用可靠的治理实践显得日益重要。ISACA 和中国建设银行协作发布的《IT 治理最佳实践》白皮书提供了详实的真知灼见，有助于各种机构利用经过验证、国际公认的框架强化其信息和技术的治理。缺少这样的治理顶层设计，企业组织很难应对挑战，更遑论如何建立应对 IT 风险的防线、有效的汇报机制，以及如何提升企业内部关键利益相关方的风险意识。

今天的技术层出不穷，ISACA 不仅持续优化 COBIT 框架为业者及企业带来巨大价值，并且为良好企业治理得到重视奠定坚实基础。除了支撑企业全方位实施、驱动业务转型以外，COBIT 框架还可以为具体目标和项目等场景解决问题，允许企业量体裁衣，调配治理方案满足自己独一无二的需求。COBIT 内容与时下的相关标准、指南、法规和最佳实践均相关联，因此成为主导企业治理活动的框架。

中国建设银行多年来一直是 COBIT 强有力的支持者和成功的实践者，而《IT 治理最佳实践》白皮书介绍的是其在治理实践中的新经验。屡获殊荣的中国建设银行核心业务系统“新一代”正是基于 COBIT 而打造。新一代系统在多方面均世界领先，系统可用性高，部署的各种新型工具和功能多达 13000 多种，系统手机端用户超过 2.7 亿人。

本最佳实践白皮书由 ISACA、中国建设银行和南京审计大学组成的志愿者团队共同完成，也是 ISACA 推出的基于中国实践的首份 IT 治理最佳实践方面的报告。各种新技术在世界超大型经济体中国普及迅猛，我们迫切期待未来有更多中国从业者、组织和行业实践经验介绍给全球业界。

作为国际性组织，ISACA 全球证书持有人超过 16.5 万，北京办公室于今年年初正式成立，彰显 ISACA 致力分享全球先进知识和经验、支持中国专业人士及机构的力度。《IT 治理最佳实践》白皮书分享的高价值知识资源，帮助我们加深对治理核心原则的理解，助力中国乃至世界各机构在技术转型的进程中释放最大潜能。

Rob Clyde

ISACA 全球董事会主席

本页为空白页

知识分享与中国智慧

IT 治理是一个困扰全球各类组织机构的热门话题之一，国内外相关的理论研究很多，其中以 ISACA（国际信息系统审计协会）推出的 COBIT（信息及相关技术的控制目标）框架标准最为权威。该标准体系已在世界一百多个国家的重要组织与企业中运用，通过建立横跨整个组织的 IT 治理、管理和运营的业务框架，指导这些组织有效利用信息资源，管理与信息相关的风险，通过维持实现收益、优化风险管理及资源利用之间的平衡，从而创造 IT 的最优价值。

中国建设银行的信息化水平在全国乃至全球银行业界均居于领先地位，其基于 COBIT 系列标准的新一代“核心系统建设工程”更是荣获 2017 年度银行科技发展项目特等奖。新一代系统将国际先进的标准与中国银行业的特殊性完美结合，组织信息科技管理全流程建模，构建风险防控体系，完善科技治理体系，获得监管认可和业界肯定，成为中国金融科技创新的典范之作。

本文从 IT 组织、制度、业务框架、IT 架构、科技内控五个方面对建设银行的新一代系统进行了详实的阐述，文中包含了大量易于操作的工具和方法，不仅对 IT 治理在银行业落地提供了切实的指导，对其他行业的 IT 治理实践也有很强的借鉴意义。本文带来的一个更为深远的意义是，中国在采用国际先进标准的过程中创造性地赋予其新的内容和方法，进而向国际业界输出创新的最佳实践，为世界科技的发展贡献中国智慧。从这一点上说，中国建设银行已经走在了知识分享的前列。

陈钟教授
北京大学金融信息化研究中心主任
中国软件行业协会副理事长
中关村智联软件服务业质量创新联盟会长

本页为空白页

目 录

图表目录

第 1 章 IT 治理

科技是第一生产力，信息时代更需要信息科技。随着移动互联、云计算、大数据等新技术与企业经营管理有机融合，信息科技对企业发展已由支撑转为引领，成为现代企业的核心竞争力。然而，影响信息科技的因素众多，企业要想应用信息技术，推动业务持续创新发展，就必须建立保证信息科技“做正确的事”的良好 IT 治理体系。

IT 治理作为一种涉及利益相关者之间关系的制度安排和管理实践，国际信息系统审计协会（以下简称“ISACA”）等知名组织进行了卓有成效的探索，制定了一系列 IT 治理原则和标准。ISACA 认为，企业应从战略、制度、流程、规范和标准等方面，构建适合本企业的 IT 治理框架，提高 IT 治理水平。

1.1 治理理论

ISACA 在信息系统和技术控制目标 5.0（以下简称“COBIT 5”）中指出，IT 治理的目标是为企业利益相关者创造价值（图 1），这意味着在优化风险的同时，以最佳资源成本实现最大收益。

图 1 COBIT 的 IT 治理目标

COBIT5 定义了对企业 IT 治理起到关键性作用的动力因素（图 2），IT 政策和框架体系作为治理的动力载体，通过 IT 资源、流程、组织架构与文化等因素驱动，实现 IT 治理机制，达到治理的目标。

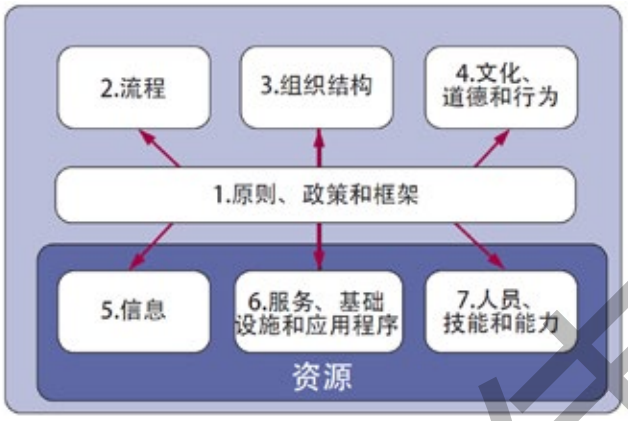

图 2 COBIT 的 IT 治理动力因素

COBIT 5 将治理与管理区分开来，治理流程处理的是利益相关者关注的企业整体目标，将治理的评价、指导与监控作为高效治理体系的关键领域（图 3），主要包括“确保治理框架的设定和维护（EDM01）”、“确保收益交付（EDM02）”、“确保风险优化（EDM03）”、“确保资源优化（EDM04）”、“确保利益相关者的透明度（EDM05）”五个治理流程。

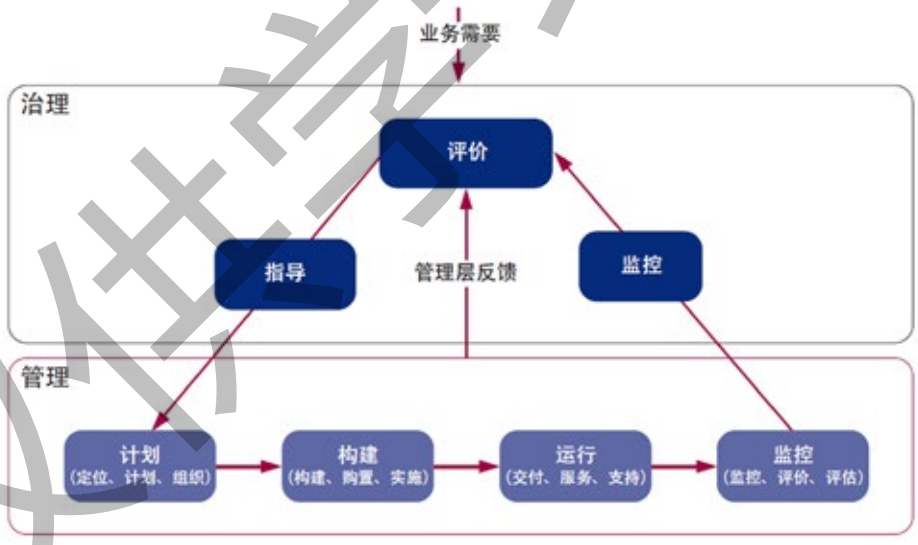

图 3 COBIT5 治理领域

根据 COBIT 5 的 IT 治理理论可以看出，IT 治理确立了整个组织的 IT 基本框架，IT 管理则是在这个既定的框架下驱动组织实现目标。缺乏良好的 IT 治理，企业即使有“很好”的 IT 管理体系，也就像一座地基不牢的大厦，没有真正持续的竞争力；同样，没有有效的 IT 管理，单纯的治理模式也只能是一张美好的蓝图，无法实现企业目标。

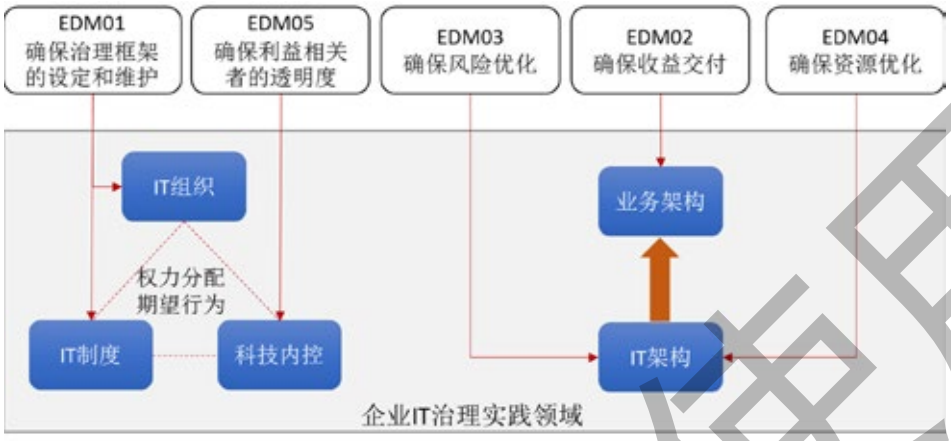

图 4 企业 IT 治理实践领域

IT 治理作为整个组织的 IT 基本框架，首先要明确 IT 决策权的归属和 IT 责任的承担，以及所期望的 IT 行为。其中，IT 组织解决决策权和责任的问题，IT 制度明确“做什么、谁来做、怎么做”，科技内控指导如何监控、评价 IT 行为。同时，IT 要支撑企业的整体战略，需要有企业级的业务架构和灵活的 IT 架构，前者是企业实现价值交付的核心，后者在资源和风险优化的基础上实现业务架构所描述的业务。因此，本实践的 IT 治理主要包括 IT 组织、IT 制度、业务架构、IT 架构、科技内控五个方面。

1.2 治理实践

目前，IT 治理已得到企业管理层的高度关注，但在 IT 治理实施过程中，企业常常面临以下问题或痛点：

- 如何定义董事会、监事会、高管层在 IT 决策中的职责分工？
- 如何设立 IT 组织体系的汇报路径？
- 如何在企业内部构建 IT 风险防线？如何清晰定义各道防线之间的职责界线？
- 如何根据企业治理与管理要求制定 IT 制度框架，并覆盖 IT 活动全生命周期流程？
- 如何确保制度的合理性，避免管理缺失、管理过度或管理不一致？
- 如何建立企业统一的业务架构，实现 IT 与业务的高度融合？
- 如何建立符合企业发展方向的 IT 架构？
- 如何维持内部科技政策与监管要求的一致性，并动态适应业界标准的变化？

本实践通过研究中国建设银行的 IT 治理经验，总结在 IT 组织、IT 制度、业务架构、IT 架构及科技内控等方面的良好实践，提供企业解决上述 IT 治理问题的有效方法和措施。

在 IT 组织方面，构建一个良好的企业 IT 组织体系。在决策层面，明确董事会、监事会、高级管理层以及下设委员会在确定 IT 战略与方向中的职责；在执行层面，明确 IT 部门、业务部门和分支机构在具体落实企业 IT 决策过程中的职责，以及企业 IT 风险三道防线的构成和工作机制；组建专业化团队实现 IT 相关的治理活动；建立培训知识体系和教育机制，持续提升员工信息安全与风险防范意识。

在 IT 制度方面，以 COBIT 5 为指导建立贯穿 IT 活动全生命周期的 IT 制度框架；明确 IT 制度层级划分原则、各层级所包含的制度体例和适用范围、制度制定流程中的重要控制环节和控制要点；运用 IT 监管库、业界标准库、IT 制度库等持续优化 IT 制度。

在业务架构方面，遵循业务统一视图、标准化、模型化等原则，通过企业级业务建模方法，承接企业战略和发展规划，从企业级视角构建端到端流程模型，自顶向下进行设计，形成企业级业务架构。

在 IT 架构方面，遵循面向服务的原则构建企业级 IT 架构。运用结构化和非结构化数据建模方法，建立企业级数据统一视图；遵循层次化、组件化理念，搭建典型的七层十二个平台的企业级应用架构；设计支撑数据和应用的技术架构，创建灵活、松耦合的基础技术平台和组件；提出“安全即服务”理念，建设由服务接入层、应用安全服务层、基础设施安全服务层和安全策略管理中心构成的安全架构，提供集中、统一、灵活、智能的信息安全服务。

在科技内控方面，建立完善的监管合规体系。传导跟踪监管要求，提升企业执行监管要求的水平和学习业界标准的能力；落实 IT 检查监督，明确 IT 检查内容、范围、计划和实施等要素；建立 IT 考核和操作水平管理机制，客观评价企业 IT 管理工作；开展 IT 审计检查问题的跟踪，运用 IT 审计检查库，强化风险管控。

第 2 章 IT 组织

一个良好的 IT 组织需要考虑组织的构成和各方的利益、职责、权限及汇报路径，应与企业整体发展目标保持一致。在支持企业实现业务目标的前提下，通过优化资源、优化风险、实现收益进而创造价值，实现 IT 目标，并监控 IT 方向与目标的绩效与合规性。因此，企业 IT 组织体系的合理与否将直接影响企业 IT 战略的实施，影响到整个企业业务发展战略的实现。

随着企业信息技术的广泛应用，IT 与业务的关系越来越紧密，IT 工作不仅与 IT 部门相关，与企业内各个部门都有关联。在构建企业 IT 组织时，通常会面临以下问题：

- IT 组织体系怎样更有效？
- 如何设立 IT 组织的汇报路径？
- 如何在企业内部构建 IT 风险防线？如何清晰定义各道防线之间的职责界线？

> 如何搭建专业化团队落实企业 IT 管理策略?

> 如何提升不同岗位人员的 IT 风险意识和信息安全技能?

企业 IT 组织体系不能简单地等同为企业的 IT 部门，而应包括企业经营活动中参与 IT 相关活动的所有部门和人员。一个良好的企业 IT 组织体系包含确定 IT 战略与方向的决策体系、具体落实 IT 战略和决策的执行体系以及为实现特定任务而设置的专业化团队。

2.1 决策体系

一般来说，企业 IT 决策体系包括董事会、监事会和高级管理层：董事会负责企业 IT 战略规划，确保与经营管理目标一致；监事会负责监督董事会、高级管理层在企业 IT 方面的履职尽职情况；高级管理层负责企业 IT 管理与流程管理的研究、议事和协调。

2.1.1 董事会

董事会负责企业 IT 战略规划，履行企业 IT 风险管理职责。通常董事会 IT 相关职责为：

1．审查批准企业 IT 战略整体规划，每年至少听取一次 IT 战略规划执行情况的汇报。

2．遵守并贯彻执行国家的法律、法规和技术标准，落实相关监管要求。

3．审议企业 IT 风险管理策略，定期听取企业 IT 风险管理情况汇报，确保 IT 风险管理的总体有效性与合规性。

4．致力于企业的 IT 风险文化建设，规范职业道德行为和廉洁标准，提高全员对 IT 风险管理重要性的认识。

5．确保良好的 IT 治理体系，形成分工合理、职责明确、相互制衡、报告关系清晰的 IT 风险管理组织结构和激励机制。

董事会通常下设若干委员会，其中战略发展委员会负责指导企业信息科技战略规划和执行；风险管理委员会负责指导信息科技风险管理工作，履行 IT 风险相关的规划与管理职责。

2.1.2 监事会

监事会负责监督企业 IT 战略、规划和管理的执行情况。一般来说，监事会 IT 相关职责为：

1．监督董事会、高级管理层在企业 IT 方面的履职尽职情况。

2．监督企业 IT 决策、IT 风险管理的执行与落实情况。

3．指导企业 IT 审计工作。

2.1.3 高级管理层

高级管理层负责企业 IT 管理与流程管理的研究、议事和协调，确保 IT 战略规划有序推进、稳步落实。高级管理层 IT 相关职责为：

1．研究 IT 战略规划，确保其与企业的总体业务战略保持一致。

2．评估 IT 风险管理工作的总体效果和效率。

3．负责 IT 专业队伍的建设，建立人才激励等机制。

首席信息官在高级管理层中负责企业信息科技规划和整合工作，主要职责为：

1．直接参与企业与信息科技运用有关的业务发展决策。

2．确保信息科技战略，符合企业的总体业务战略和信息科技风险管理策略。

3．确保信息科技风险管理的有效性，并使有关管理措施落实到相关的每一个内设机构和分支机构。

4．推动专业培训，提高人才队伍的专业技能。

高级管理层可下设IT委员会，负责企业IT研究、议事和协调，定期召开会议，审议IT相关重大事项。通常，委员会包括 IT 部门、企业战略规划部门、人力资源部门、财务部门、风险管理部门、内控合规部门、质量管理部门及相关业务部门。其主要职责为：

1．研究企业 IT 管理政策。

2．研究企业重大信息系统建设目标和建设方案，推动战略性项目实施。

3．组织制定和落实企业 IT 风险管理策略。

4．组织研究企业整体业务需求的整合，推进全局性业务流程的优化和标准化。

5．组织协调企业年度 IT 开发、运维任务总量计划及配套支持预算，协调推进 IT 项目的实施。

6．分析监管机构重大政策变动对企业流程管理与 IT 管理工作的影响，制定对策和实施方案。

7．定期向董事会、监事会汇报 IT 战略规划的执行、IT 预算和实际支出、IT 建设和运行的整体状况等。

2.2 执行体系

2.2.1 执行机构设置

IT 部门

IT 部门负责企业 IT 规划编制、政策标准制定、计划审核、基础设施建设和管理、应用开发、信息系统运行管理、信息安全管理等。对企业 IT 发展规划、任务落实、制度执行、生产安全等情况进行管理、检查、监督和考核。

一般来说，IT 部门的主要职责为：

1．拟定企业中长期 IT 规划目标和年度计划，拟定 IT 相关规章制度和操作流程，并组织检查、监督和执行。

2．编制企业 IT 开发、运行和维护费用预算。

3．拟定企业 IT 应用管理标准、技术数据标准和信息管理规范。

4．负责企业级网络系统、基础设施建设的管理。

5．牵头组织 IT 应用项目的审批。

6．检查项目开发计划的实施进度，牵头组织对 IT 应用开发项目的验收和知识产权申报，负责开发项目的质量成本控制。

7．负责计算机软件、硬件、服务采购的需求管理。

8．负责信息安全管理，建立健全 IT 风险内控制度并组织落实。

对于规模较大的企业，还可设立开发中心和数据中心，分别承担企业的开发任务和运维任务。其中，开发中心负责企业应用系统开发、测试、推广及技术支持；数据中心负责企业信息系统的技术运行维护和企业基础设施的规划与建设。

业务部门

业务部门作为 IT 系统的需求方和使用方，其主要的 IT 相关职责为：

1．编制、审核 IT 系统业务需求。

2．测试、验证 IT 系统业务功能。

3．负责 IT 信息资产的安全管理，包括识别敏感信息、确定信息资产安全等级、制定信息使用和管理规则。

4．负责将 IT 风险管理要求融入到本部门的业务制度和流程。

分支机构

企业分支机构主要的 IT 相关职责为：

1．落实外部监管和内部控制要求，配合内外部审计和监管检查。

2．负责辖内 IT 系统的日常管理。

3．定期向上级管理层、风险总监及企业总部汇报 IT 风险管理情况。

4．组织开展辖内 IT 风险培训教育。

5．负责辖内计算机软件、硬件、服务采购的需求管理，负责编制分支机构 IT 开发、运行和维护费用预算。

2.2.2 IT 风险三道防线

为确保企业 IT 治理活动的有效执行，落实监管合规要求，应在企业内部构建 IT 治理活动的“三道防线”。

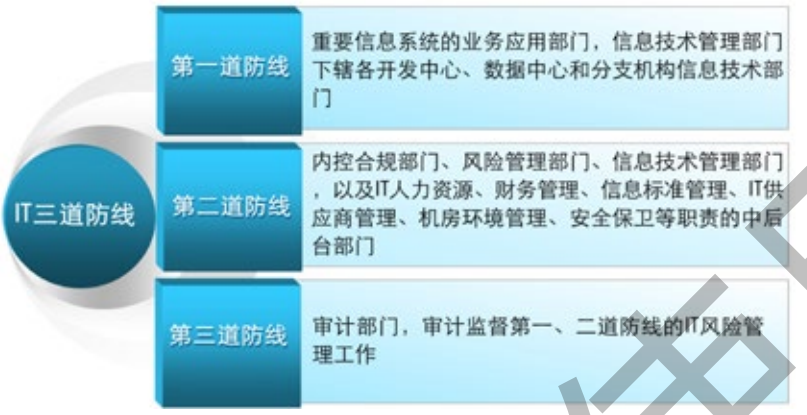

图 5 IT 三道防线

第一道防线是使用信息系统的业务应用部门、以及直接进行信息技术开发、测试、运行和日常基础管理的部门，承担各自领域的 IT 风险控制工作。

第二道防线是承担 IT 风险管理、信息安全和业务连续性管理以及 IT 人力资源和财务、IT 合规和信息标准、IT 供应商管理、机房环境管理、安全保卫等管理职责的中后台部门。第二道防线遵循全面风险管理政策，负责制定 IT 风险管理制度、流程、标准和工具，开展 IT 风险管理工作，定期向董事会、监事会、高级管理层汇报 IT 风险管理情况。

第三道防线是审计部门，审计监督第一、二道防线的 IT 风险管理工作。

2.2.3 沟通汇报机制

良好的沟通与汇报机制，能让企业各利益相关方及时、准确、全面了解企业 IT 及 IT 风险的状况，能确保企业 IT 绩效的透明度，使 IT 目标与企业战略保持一致。

1．IT 风险双线汇报

建立 IT 风险双线汇报机制。在企业总部层面，由 IT 部门负责人每周向首席信息官（CIO）和首席风险官（CRO）双线汇报；总部开发中心、数据中心 IT 风险管理团队向所在部门负责人和总部 IT 部门汇报。在分支机构层面，IT 风险管理团队定期向所在部门负责人和上级 IT 部门汇报。

2．生产事件沟通汇报

通过晨会、安全生产例会和生产事件跟踪会等方式，组织相关方分析生产事件，制定处置措施并跟踪落实。组织生产事件调查和责任认定，向相关方提供事件分析报告和责任认定报告。

IT 运营单位按月将典型事件警示、重要风险提示、系统运行、系统交易、网络运行、系统容量、应用版本上线、IT 服务管理等情况，以通报的形式向管理层汇报，使管理层及时了解企业整体 IT 生产运行状况。

2.3 专业团队

专业团队指为落实 IT 战略与规划、完成 IT 特定任务而组建的团队。专业团队既可以纵跨企业总部与分支机构，也可以横跨 IT 部门与业务部门，可由技术人员或业务人员共同组成。专业团队的设置，能够充分利用企业总部与分支机构的专家资源，发挥其专长，加强总、分机构的联动，完成特定专项任务。

2.3.1 IT 架构管控团队

企业 IT 架构管控团队负责企业级架构设计和管控，包括业务架构、数据架构、应用架构、技术架构和安全架构。在开发中心派驻架构团队，遵循企业级架构标准，指导具体项目方案设计。架构团队的主要职责为：

1．明确架构原则及评审标准。

2．制定架构设计流程，明确架构设计标准和指引。

3．制定架构设计方案和实施计划，组织架构经理、技术专家等人员进行评审。

4．建立架构分析质控流程和架构分析质控清单，编制架构整体方案。

5．建立架构分析变更管理流程，架构分析成果纳入企业级架构资产库进行管理。

2.3.2 新技术研究团队

企业需设立新技术研究团队，持续跟踪 IT 新技术发展，并将相对成熟、适用于企业的新技术纳入研究范围，研究通过后正式在企业进行推广、应用。其主要职责为：

1．建立新技术持续跟踪机制，及时收集分析新技术发展和应用动态。

2．制定新技术研究、选型流程和方法，确定新技术选型的原则和标准。

3．研究新技术应用场景、应用方式，对新技术的功能、性能、安全性等进行测试。

4．制定新技术推广应用方案和计划，提供新技术应用推广过程的专业支持。

2.3.3 信息安全团队

企业总部 IT 部门设立专职的信息安全专业团队，包括运行风险监控团队、安全平台建设团队及渠道安全团队。在企业总部和分支机构之间设立信息安全虚拟团队，通常由一名部门负责人专职管理，从事安全技术研究，提高专业化、精细化水平，为 IT 风险管理提供支持。

运行风险监控团队，其主要职责为：

1．内部风险监控：负责安全监控体系建设和日常运行维护；开展企业网络基础设施、系统平台及应用系统日常安全监控、漏洞检测和安全防范工作；负责安全加固和漏洞处置。

2．外部风险监控：监控并及时应对信息安全威胁和网络攻击，搜索并协调关闭钓鱼网站，监控拦截外发敏感信息，拦截过滤垃圾邮件，监测互联网上侵犯企业知识产权的信息。

3．应急处置：与国家互联网应急中心、运营服务商、网络安全公司等协作，快速、高效响应各

种网络安全事件；建立快速响应的网络攻击联合防御体系，高效完成漏洞补丁、系统修复、流量清洗、攻击溯源等安全响应工作。

4．风险评估：负责运行风险评估、研究内外部威胁变化趋势，关联分析网络、系统、终端等信息安全事件。

安全平台建设团队，其主要职责为建设企业级用户认证、客户认证、密码服务、数据安全、安全监控、终端安全等安全基础设施平台。

渠道安全团队，其主要职责为：

1．追踪和研究互联网、电子商务、移动计算等新技术发展趋势，识别和分析企业电子渠道风险变化趋势。

2．设计电子渠道应用安全技术方案。

3．开发电子渠道安全基础平台，构建电子渠道应用安全体系。

4.分析和应对电子渠道、互联网安全威胁以及黑客最新攻击手段和犯罪手法，防范电子渠道攻击。

为加强企业总部和分支机构之间信息安全和风险管理工作的联动，加快专业人才培养，提升企业信息安全管理水平，企业总部组织各分支机构成立**企业级信息安全虚拟团队**，其主要职责为：

1.承担信息安全管理专项任务: 承担总部下达的信息安全管理专项任务，如IT风险内控制度建设、IT 风险管理专题研究、信息安全新技术试点等。

2．参与信息安全管理工作：参与总部安全制度建设、安全技术管理、风险监控管理、应急灾备管理等工作。

3．信息安全管理工作探索及经验分享：针对日常难点、重点工作，结合工作实践及业界标准，从技术应用、流程控制及管理优化等方面提出工作举措，由总部定期组织审核发布，加强各分支机构之间的工作经验分享和交流。

2.3.4 反欺诈团队

为有效应对外部网络欺诈，金融机构、第三方支付、电子商务等企业应完善网络金融服务的安全保障机制，成立由技术人员和业务人员组成的反欺诈安全团队。

欺诈规则与模型管理团队，其主要职责为：

1．反欺诈规则分析与模型建设：依据网络金融服务业务特点和互联网安全形势，总结网络金融服务风险特征，提炼反欺诈规则，动态调整监测重点。

2．可疑欺诈交易分析：对反欺诈系统识别的大量网络金融服务异常交易，通过经验和相关信息，进行分析、评估，识别高风险交易。

3．调查处理：针对复杂高风险交易，与银行机构、第三方支付等沟通协调，调查网络金融异常交易涉及的客户和账户信息，进行汇总分析和风险处置。

事中控制团队，其主要职责为：

1．大额交易干预：对电子渠道符合大额标准的交易进行实时干预，通过主动外呼客户或者接受客户回拨服务热线等方式，核实客户交易真实性。

2．异常交易干预：对除大额交易以外的达到红色预警标准的异常交易进行实时干预，通过直接阻断、主动外呼客户或者客户回呼等方式进行处置，防范交易风险。

资金追索与事后处理团队，其主要职责为：

与银行机构、第三方支付公司、公安部门、法院等联系、沟通，进行资金追索，及时冻结、划回纠纷涉及的资金；对恶意欺诈的行为进行法律诉讼。

2.3.5 合规培训团队

合规培训团队根据企业 IT 合规总体要求和不同岗位的特点，分析案例，编制专题培训教材，并组织培训。合规培训团队的主要职责为：

1．构建 IT 合规培训知识体系。

2．制定 IT 合规培训计划，明确新入职员工和在职员工年度合规培训要求。

3．组织编写 IT 合规培训教材、开发网络培训课程。

4．负责设计、开发内外部 IT 合规宣传材料。

5．组织实施 IT 合规培训。

2.4 人员意识

在众多风险因素中，内部人员是关键因素。因员工对安全隐患的“不知”，或借职务之便进行恶意操作都将影响企业信息安全，甚至引发严重后果。企业在对员工进行培训时，或忽略了员工岗位、角色的差异，培训内容缺乏针对性；或未将员工绩效与培训质量挂钩，培训效果得不到保证。因此，企业应构建安全培训知识体系，建立相应培训机制，增强员工信息安全意识和风险防范能力。

2.4.1 培训知识体系

企业有针对性的分析各岗位面临信息安全风险及防范能力需求，编制面向全体员工、信息技术人员、信息安全人员、客户营销人员的专题培训教材。

1．面向全体员工编制员工信息安全技能手册、信息安全事件警示录

员工信息安全技能手册围绕常见信息安全风险，用简洁的话语、直观的图形传递有效的信息安全防护基础知识。编制信息安全事件警示录，通过收集和分析外部攻击、内控缺陷、系统故障、自然灾害等方面真实的信息安全事件，使员工切身认知安全事件产生的原因、过程和造成的影响。

2．面向技术人员编制信息技术人员安全手册

信息技术人员安全手册帮助技术人员知晓哪些风险需要面对、哪些安全要求必须遵守、哪些安

全手段可以利用，懂得在开发和运维中如何应对、解决安全问题。

3．面向安全人员编制信息安全人员实务手册

信息安全人员实务手册提供安全问题解决思路，介绍软件开发安全、系统建设安全、日常运维安全和安全事件应急处置方法，增强安全人员实务操作技能。

4．面向客户营销人员编制客户营销人员信息安全手册

针对客户营销人员接触客户信息多、外出营销频繁、系统使用环境复杂等特点，以客户营销人员的日常工作活动为主线，梳理其在营销客户、信息系统使用、日常办公等活动中的安全注意事项，明确客户营销人员应知应会的常用安全操作技能，有效保护客户信息和企业资产安全。

2.4.2 培训教育机制

培养各级员工的信息安全意识，鼓励全员参与信息安全建设，力促员工安全地应用信息技术，将低级操作错误和风险隐患抑制在萌芽阶段。

1．建立新员工信息安全培训机制，确保新员工上岗前掌握信息安全知识和制度要求；不同岗位新员工依据培训体系还可进一步接受针对性培训，确保新员工掌握其岗位应知的安全制度和必备的安全技能。

2．制定 IT 风险培训计划，规定不同岗位员工的必修及选修培训课程，明确信息技术关键岗位、信息技术人员、业务人员及相关管理人员应完成培训方式及课时。

3．开展形式多样的培训教育。制作安全技能培训课件、警示教育微课件、信息安全微视频，借助现场、企业网络学习平台、移动设备新媒体应用等多种渠道开展形式多样的 IT 风险管理培训，根据企业需要向员工下达学习任务并进行必要的达标测试。

4．将员工培训与绩效考核结合，对未达到培训要求的员工进行处罚。

5．推行进阶式培训机制，定期组织开展 CISA 等业界信息安全培训及认证考试。

2.5 小结

企业建立包括董事会、监事会、高级管理层在内的 IT 决策体系，包括 IT 部门、业务部门和分支机构在内的 IT 执行体系，从企业 IT 战略和决策的制定、落实到监督，在组织层面保证了 IT 与企业总体目标和战略保持一致。IT 风险双线汇报和生产事件沟通汇报机制，确保了利益相关者的透明度，能够发现企业 IT 面临的问题与风险，及时采取纠偏措施。各专业团队的设立，在保持 IT 架构的先进性、跟踪应用新技术、信息安全管理、有效应对网络欺诈、合规教育培训等方面，发挥了重要作用。构建完备的人员安全培训知识体系和培训机制，实现了不同岗位知识培训的全覆盖，有效提升了员工安全意识和技能。

第 3 章 IT 制度

企业制度是维系企业作为独立组织存在的各种社会关系的总和，是企业赖以生存的体制基础。企业制度传递董事会、监事会和高级管理层的导向和指令、规范企业和员工行为，是企业有序化运行的体制框架。为有效规范 IT 建设、IT 运维和 IT 计划等工作，企业应建立一套完整的 IT 制度体系来管理企业信息化过程中的所有活动，从而创造良好的信息化发展环境。

IT 制度是企业按照自身信息科技发展需要和监管要求，结合 IT 工作实际情况制定的管理办法、实施细则、操作规程、技术标准、手册等规范性文件的总称。在建立 IT 制度体系时，企业通常遇到以下问题：

- 如何根据企业治理与管理要求制定 IT 制度框架，并覆盖 IT 活动全生命周期流程？
- 如何划分制度层级，确保 IT 目标的逐级传导、落实？
- 如何确保制度的合理性，避免管理缺失、管理过度或管理不一致？
- IT 制度如何适应内外部环境变化？

3.1 制度框架

“制”是制约，“度”是尺度，制度即制约之尺度。制度是约束人们行为及其相互关系的一套规则，是一种博弈均衡和合作的机制。制度适用的对象是人，是对人的约束，其主要内容包括两个方面：一是约束个体的行为，明确个体应该做什么，不应该做什么；二是约束人与人之间的关系，明确部门与部门、岗位与岗位之间的职责以及工作衔接，即通常所说的“流程”。制度的目的是在约束人们行为的基础上实现企业目标，其根本作用是解决企业内部从无序到有序和企业员工行为底线的问题。

3.1.1 制度层级

为确保 IT 目标的准确传导、落实，逐级分解 IT 目标，对执行的过程进行规范，并为各流程环节及岗位提供可操作的制度，实现从目标到操作的落地。IT 制度在纵向上可分为三个层级：目标层、方法层和步骤层。

图 6 IT 制度层级

目标层在与企业风险偏好保持一致的前提下，明确管理目标，即明确做什么，包括办法和实施细则两个体例，办法提出宏观要求，细则进一步细化要求。包括：

1．办法：IT 各管理领域均应制定办法级制度，明确此领域的管理目标、管理范围、管理流程以及管理策略。

2．细则：根据管理办法制定细化管理要求的实施细则。

方法层明确谁来做、如何做，包括操作规程、标准和配置基线三个体例，操作规程明确各角色之间的分工及跨角色之间的流程，技术标准和管理标准说明实现要求的方法和程度，配置基线明确 IT 产品的配置标准。包括：

1. 操作规程：一是执行步骤多或涉及专业方法的关键流程，如风险识别等；二是科技重要资产的使用，如生产数据应用、设备使用等；三是 IT 基础服务平台操作，如统一认证服务平台等。

2．标准：技术标准适用于各类基础设施或系统，如互联网平台建设标准；管理标准适用于分类分级或处理过程，如生产事件等级划分标准、数据脱敏标准、科技检查标准等。

3．配置基线：适用于 IT 产品目录中的各产品类型。

步骤层明确各岗位的具体操作步骤，即如何一步步完成所做的工作，涵盖指南、手册等体例。

手册和指南：针对操作方法复杂的环节应制定手册或指南，比如风险识别手册、安全编码指南、预案编制指南等；针对 IT 产品目录中的各型号产品制定操作手册或指南。

3.1.2 框架构建

IT 制度以 COBIT5 为指导，从企业组织和管理的角度出发，形成贯穿 IT 活动全生命周期的完整流程，构建覆盖 IT 建设、IT 运维、IT 计划三个方面的制度框架。

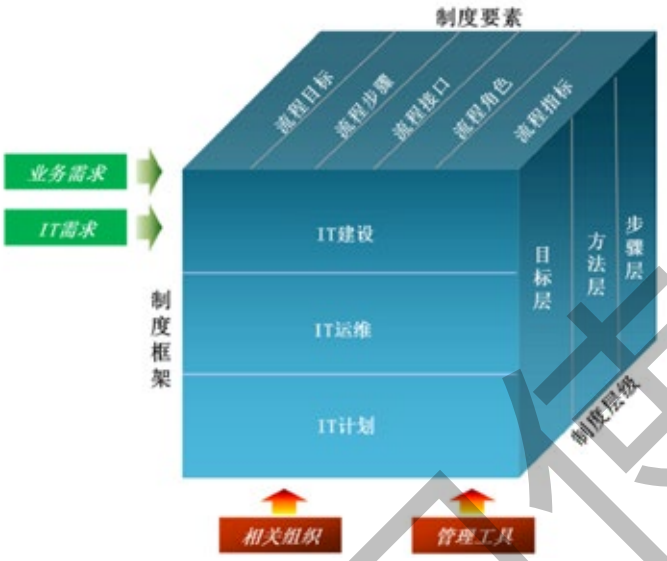

图 7 IT 制度框架

制度框架覆盖 IT 活动的全部管控领域，可划分为：

IT 建设：项目管理、设计管理、测试管理、投产管理和需求管理等领域。

IT 运维：日常运维管理、服务请求管理、事件管理、问题管理、变更管理、容量管理、配置管理、应急管理、数据管理、用户权限管理、系统与网络安全管理、机房管理、知识管理和参数管理等领域。

IT 计划：安全管理、风险管理、服务水平协议管理、架构管理、人力资源管理、制度管理、资产管理、合规管理、创新管理、预算和成本管理、业务关系管理等领域。

IT研发	IT运维	IT管理
项目管理	日常运维管理	安全管理
设计管理	服务请求管理	风险管理
测试管理	事件管理	服务水平协议管理
投产管理	问题管理	规划管理
需求管理	变更管理	架构管理
	容量管理	人力资源管理
	配置管理	外包管理
	应急管理	制度管理
	数据管理	资产管理
	用户权限管理	合规管理
	系统与网络安全管理	创新管理
	机房管理	预算和成本管理
	知识管理	业务关系管理
	参数管理	

图 8 IT 制度管控领域

IT 制度以流程为导向，主要包含以下要素：

流程目标：为总体 IT 服务与每个 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（SMART）流程目标，确保这些目标与业务目标相关联并采用合适的衡量指标。

流程步骤：包括服务设计、建设、运营、监控、改进全部有关的 PDCA 工作环节，具有与其他流程的接口，每一步骤由唯一角色执行。

流程接口：是指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，包括输入输出、接口触发条件、接口管理责任人三项标准内容。

流程角色：清晰定义跨组织边界的流程步骤中不同流程角色的职责，并采用 RACI 模式明确区分角色承担的流程结果总体责任与阶段性执行责任。

流程指标：为支撑总体服务水平和流程的风险控制和持续改进，制定一系列相关联的衡量指标来监控流程结果和效率，设立能反映流程目标和绩效的目标值，使流程指标与总体服务水平指标保持一致。

例如，企业在设计信息安全管理制度框架时，在目标层，制定信息安全管理办法和实施细则，明确信息安全管理的目标、范围及策略；在方法层，制定覆盖用户管理、数据安全、系统安全、终端安全、网络安全、人员安全等信息安全各领域的操作规程，明确各领域分工及领域间的关系；建立相应的技术标准和管理标准，提供达到安全管理目标的方法和程度；在步骤层，明确各岗位的具体操作步骤，针对具有复杂操作方法的环节，制定手册或指南，比如安全运维手册、产品应用指南、安全软件使用手册等。

3.2 制度流程

为保证 IT 制度的科学性和规范性，制度流程应包含制度计划、制度编制、制度评审、制度发布、制度重检、制度修订和制度废止，各环节关系如下图所示：

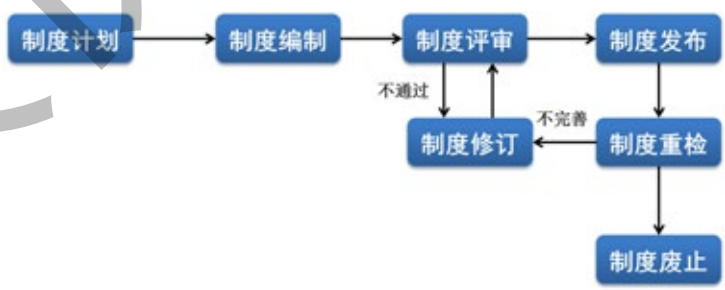

图 9　IT 制度制定流程

制度计划

1. 企业每年组织制定 IT 制度编制计划。

2. 制度计划应依据外部监管要求、业界 IT 标准和实践、企业 IT 发展战略以及企业信息化管理的实际情况进行编制。

3. 制度计划要明确 IT 制度总体框架、编制或修订要点等内容，并落实 IT 制度编制部门。

制度编制

1. 通过情景分析法和建模推演法，充分识别领域中存在的风险，评估风险发生的可能性和影响，确定风险等级。

2. 梳理相应领域的科技监管要求，将监管要求作为制度要求的底线；梳理相应领域的业界标准，将标准中的最佳实践作为制定制度的重要参考。

3. 在制定具体内容时，梳理制度领域中涉及的 IT 资产，分析资产各生命周期中面临的风险，遵从监管要求，参考最佳实践，结合风险识别结果，重点针对中高等级风险，根据企业实际情况，明确生命周期各阶段的管控要求和流程，并落实相应责任人。

4. IT 制度编制部门组织完成制度初稿，并编制科技制度编写说明，明确编制目的、编制依据、编制思路、主要内容、与其它制度关系以及监管要求合规情况等。

5. 将制度初稿和编写说明向相关部门征求意见，并根据征求意见进行修改，形成制度送审稿。

制度评审

1. 企业 IT 制度管理部门对制度送审稿、编写说明、征求意见修改情况进行初步审核，对初审通过的，采取会议评审等形式对制度进行复审。

2. 根据企业内部、业界已发生的风险事件以及 IT 审计发现等，验证制度的管控措施是否能有效控制风险。

3. 企业 IT 制度管理部门将评审后的制度提交法律事务部门进行合法性审查，再提交内控合规部门进行合规性审查。

制度发布

1. 将评审通过的制度按企业规定流程予以发布。

2. 制度发布后，各级 IT 制度管理部门负责对制度进行统一归档。

3. 制度发布后，企业 IT 制度管理部门负责组织 IT 制度培训；各级 IT 制度管理部门负责组织落实本单位的培训。

制度重检

1. 当 IT 相关法律、法规、监管要求发生变化，以及发生重大科技风险事件或发现重大科技隐患时，企业要及时组织制度重检。重检内容分为制度体系重检和具体制度重检两个层面：制度体系重检，包括核查制度缺失和失效情况；具体制度重检，包括检查制度条款是否存在控制不足、控制过当、不同制度之间控制不一致、控制要求不明确等情况。

2. 定期组织制度重检，比如每年组织一次，每次制度重检后将结果报送企业高级管理层。对于重检发现的制度问题，企业组织对制度体系进行完善并修订相应制度。

制度修订

各级 IT 制度管理部门应定期收集整理制度执行中的各类意见、制度重检结果以及制度补充性或修正性的通知，不断更新和维护制度编制和修订要点，作为制度规划和编制工作的主要依据。

制度废止

IT 制度管理部门要定期对制度进行梳理，对于不适用的制度及时下发废止通知。

3.3 制度优化

为了适应企业的内外部 IT 环境的快速变化，保证 IT 制度的全面性和合理性，必须对 IT 制度进行持续优化。制度的持续优化可采用以下工具和方法：

1. 建立并持续完善国内及海外 IT 监管库。IT 监管要求是企业必须遵守的底线，通过 IT 监管库，可快速检索 IT 各领域的所有监管要求，在制度制定和修订时将监管要求融入企业 IT 制度，保持企业制度与监管要求的一致性。

2. 建立并持续完善业界标准库。业界标准是业界对于 IT 管理实践的总结和提炼，为企业认知风险、加强 IT 管理提供了指南。运用业界标准库，可方便查询各领域下的最佳实践和标准，在制度制定和修订时提供重要参考。

3. 建立并持续维护 IT 审计库。IT 审计库是对 IT 审计、检查、测评及评估等发现问题的整理和汇总，便于提炼常见问题、多发问题。运用 IT 审计库，在制度制定和修订时，可针对相应领域中的常见问题、多发问题制定有效的控制措施。

4. 建立并持续维护企业 IT 制度库。IT 制度库是将 IT 制度条款要求整理成规范化的记录，方便员工和技术人员查询管控要求，提供与监管要求、业界标准的对比功能，指导企业优化 IT 制度。

3.4 小结

IT 制度框架覆盖 IT 建设、IT 运维、IT 计划三个方面，贯穿了 IT 活动全生命周期流程。IT 制度在纵向上分为目标层、方法层和步骤层，分别回答了 IT“做什么、谁来做、如何做”等问题，实现了从要求到操作的实际落地。建立并持续完善国内及海外 IT 监管库、业界标准库、IT 审计库、IT 制度库，为 IT 制度持续优化提供参考和依据。

第 4 章 业务架构

企业进行系统开发时，通常根据各部门、各领域的业务需求，用各自不同的方法去分析其流程与数据，往往导致系统功能重复、业务流程与数据不一致等，系统连通和协作成本很高。随着企业 IT 的发展，这种“部门级”的 IT 系统建设模式，越来越难以适应企业的业务创新和发展，有必要通过引进企业级建模方法，在整合业务需求的基础上，建立企业级业务架构，并通过企业级架构管控和集中统一的开发测试实施方法，助力实现企业的发展目标和愿景。企业级 IT 系统建设模式实现企业“一套业务架构、一套 IT 架构、一套实施工艺、一套管理流程”，从根本上改变了以往由部门提出需求，分散设计、分散实施的研发模式，支持企业业务转型发展。

企业级业务架构是保障业务创新和运营、实现价值交付的核心，也是企业级 IT 系统建设模式的关键，任何企业都应构建自己的业务架构，而要构建业务架构必须使用一套有效的业务建模方法。传统的业务建模更多聚焦在某个具体业务的模型拆解和设计，未能上升到企业整个价值链层面，难以形成企业级业务架构。

在企业业务架构方面通常面临以下问题：

- 如何建立企业级统一的业务架构?
- 如何确保企业级业务架构和模型在 IT 建设过程中的有效实现?

4.1 架构定义

业务架构是业务及用于支持业务运行的结构，涵盖了企业的目标、流程、资源、信息以及相互关系，具体包括：业务的结构；业务结构是如何构建的；业务运营是如何组织的；业务的模型和原则；业务的目的、时间、地点、相关干系人、含义及方法。从实施角度看，它不仅包括在业务模型层面对业务流程和信息集合的整体描述，还包括在实施层面提出并落实业务能力解决方案。

业务架构承接企业战略、发展规划，对企业发展起着关键的作用，当企业的战略能力被分解到最细颗粒度并内化整合在业务流程中，且企业的所有员工能够遵循流程、执行流程时，战略才能得以执行并逐步实现。

企业业务模型通常由流程模型、产品模型、数据模型组成，并且作为扩展，还可以包括以提高生产效率和避免操作性错误为核心目的的用户体验模型。其中流程模型体现创造价值的过程，产品模型体现创新和定制化制造，数据模型体现对业务信息的抽象，用户体验模型体现对外部客户、内部用户的友好程度和服务程度。

流程模型、数据模型、产品模型密不可分。流程模型中的产品定义使用产品模型中的基础产品，业务规则明确产品条件的用途。流程模型中业务规则勾稽数据实体，以及对应数据实体操作的类型；数据模型的实体结构参考产品模型确定属性与实例，数据模型的主题域和域值参考产品条件参数。

4.2 架构原则

构建企业级业务架构不仅是一套方法，更是一套全新的企业转型理念。它能够更好的帮助业务部门和 IT 部门认识业务，找出差异，将战略目标融入到日常业务中。企业级业务架构构建应遵循以下原则：

业务统一视图原则

企业级业务架构是业务的统一视图，按照价值链划分创造价值的业务领域，全面识别企业为股东和社会创造价值的标准化流程，清晰、准确的将前、中、后台的流程对接起来，形成端到端的价值链。

构建企业级业务架构的主导思想是从创造价值的角度梳理各业务条线，以价值创造为原则识别关键业务活动，用还原业务本质的分析方法整合标准化业务流程，以模型化的方式描述业务规则。业务模型通过多个维度满足业务运营和管理的需要，主要包括两方面内容：用户视角业务领域和能力视角业务组件。

用户视角业务领域是由一组企业级视角的统一活动构成，用于业务部门完整、清晰的描述其业务流程。它从产品服务和业务管理两方面进行定义，并遵循以下原则：每个用户视角业务领域都是基于具体业务目的的企业级视角统一活动的组合、每个用户视角业务领域都是企业级视角统一活动的子集、用户视角业务领域可反映企业业务的真实状况。

业务组件是从能力角度来洞察企业的商业模式和业务行为，是具有相似资源、人和专业技能的活动组合。业务组件的目标是为帮助客户改进商业模式设计，实现企业级优化，提高业绩与运营效率、控制风险与成本并提高业务灵活性。

标准化原则

标准化是企业业务架构自始至终要坚持的原则，应形成一套唯一的业务术语，统一模型要素的颗粒度，帮助企业各条线有效沟通。按照如下四个原则对要素进行标准化：正确性原则，要素的名称与要素的描述匹配，清楚、准确的表达业务目的；唯一性原则，同一要素的要素名称及其含义必须唯一；完整性原则，要素必须有明确的属性，能支持多个对要素的自由调用，能支持不同的组织、时间、地域等，能支持各种需求；复用性原则，能够清晰的界定要素边界，合并业务目的相似、手段相似、产出相似的情况，满足不同角色在不同流程中自由组合要素的要求。

规则模型化原则

模型化业务规则目的是去除 CPC（客户、产品、渠道）的差异化，整合业务规则，从如何处理业务的角度出发描述在什么条件下可以做什么、不可以做什么。模型化的业务规则是一个全集，反映了业务处理能力和管理水平。

如“检查客户借记卡申请张数”步骤，业务规则中描述“1、银行卡种 A 和银行卡种 B 主卡一人只允许申请一张；2、银行卡种 C 一人只允许申请一张；3、附卡申请张数小于等于两张……”。模型化业务规则是对业务规则进行分析，找出关键变化因子，对业务规则抽象提炼，更好地实现业

务规则重用。接上面例子，模型化业务规则后，可分为 4 个子步骤：1）检查客户持有借记卡产品限制；2）检查子卡附属卡限制；3）检查卡片认证信息限制；4）检查客户参与的可多人共用的亲情卡合约限制。

而子步骤“检查客户持有借记卡产品限制”又可进一步模型化：1）读取借记卡产品信息，获取客户能持有的本产品合约个数限制；2）获取客户已持有的本产品合约数；3）如果已持有产品合约数 = 客户允许合约数，则不允许建立本次合约。

业务规则模型化后，不仅支持现有银行卡种 A、B、C、附卡，还可方便支持未来的各种卡种，既可支持快速产品创新，也方便不断的增加新规则满足差异化服务需求。

关注客户体验原则

企业转型和变革的关键是以客户为中心，与客户实现良好的互动，给客户超出预期的体验，使客户体验成为企业的关键竞争力。业务架构要从外部视角出发定义内部工作流程，定义客户与企业之间的交互，充分结合客户的情感、使用场景、体验等因素，实现具有牢固质量基础的客户体验创新。

4.3 架构设计

随着全球化商业平台的成熟，企业管理层开始关注如何在整个企业层面上进行优化，引入业务架构和企业价值链的概念就显得格外重要。由美国哈佛商学院著名战略学家迈克尔 • 波特（Michael Porter）提出的“价值链分析法”，把企业内外价值增加的活动分为基本活动和支持性活动，基本活动涉及企业生产、销售、进料后勤、发货后勤、售后服务；支持性活动涉及人事、财务、计划、研究与开发、采购等，基本活动和支持性活动构成了企业的价值链。

企业级业务建模以流程建模分析方法为主线，自顶而下从企业战略目标、实践经验和现状问题入手，分析设计业务解决方案和相应的能力需求，通过对具体流程步骤的分析得出改进点，同时识别对应的基础产品和业务信息，实现与数据模型和产品模型的关联。本实践简要介绍了五级流程建模方法以及流程模型如何与其它模型的对接。

五级流程建模对流程层级的颗粒度主要包括以下：

一级——企业领域

二级——业务阶段

三级——业务活动

四级——活动任务

五级——操作步骤

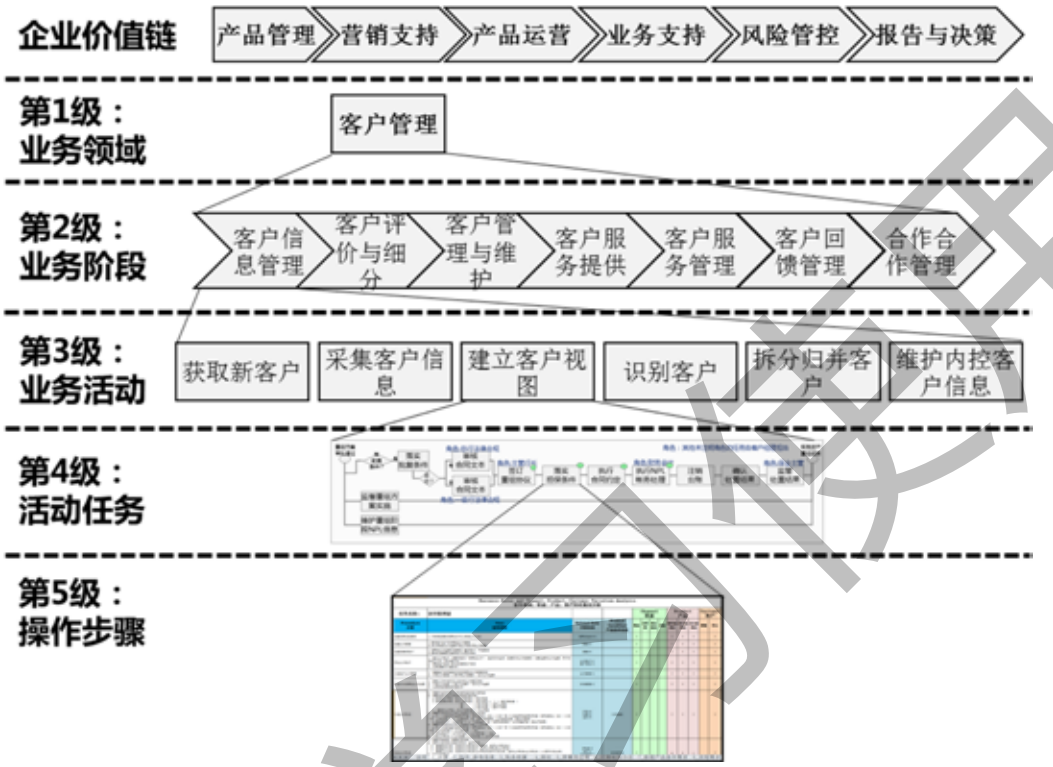

图 10 五级流程建模方法

流程的一级和二级是业务功能的分组，第三级、第四级和第五级流程是执行层的流程。其中第三级（亦称为活动）是企业级视角完成某个具有明确目的、创造价值的端到端流程；第四级（亦称为任务）描述了部门或业务单位为完成三级流程所需要的不同角色完成的具有明确业务目的的事情；第五级（亦称为步骤）描述了员工为完成四级流程所需要执行的具体步骤。业务战略需要细化、具体化并体现在三级、四级和五级执行层面的流程中，才能保证被贯彻执行。

业务建模过程

1．梳理企业高阶业务需求，形成业务能力需求：业务建模承接企业高阶业务需求，从中提炼出业务能力。高阶业务需求主要来源于三方面：一是企业业务战略，提炼出企业发展所需要的业务能力；二是业界领先实践的成果，了解到先进企业所需具备的业务能力；三是现有业务现状，掌握当前企业已经具备的业务能力。

2．整合业务能力，建立业务组件模型：将上述获得的业务能力进行整合，使之变成一个由不同业务模块构成的网络，每个模块中都包含一系列彼此关联的活动。这些模块既能为组织发挥独特作用，又能作为单独实体运行，这些模块称为“业务组件”。业务组件是企业的基本建筑单元，它们彼此松散连接，但可以很灵活的根据业务需要组合起来形成企业的业务能力。

3．逐层细化分解，形成完整业务模型：针对每个业务组件进行逐层流程分解，一直分解到最底层的五级步骤。流程分解到五级步骤意味着这些流程已抽离不稳定的变量因子，成为最基础、也是最稳定的业务操作步骤，最能体现企业的业务价值。将每个业务组件全部剥离 CPC 变量因子后的业务流程，汇总起来就构成此业务组件的价值能力，各业务组件汇总起来就构成企业完整的流程模型。流程模型包括业务领域背景图、流程结构（三级活动）、三级活动的工作流图（四级任务）、流程描述和业务规则（五级步骤）。经过去 CPC 化后的业务操作流程的输入与输出项（如存款的币种、期限、金额）构成了最底层数据模型的输入。全部输入、输出项，按业务对象实体、业务组件进行区分、整合后就形成了企业的数据模型。

流程模型与其它模型对接

1．流程模型与数据模型的对接：在流程模型中，每个步骤均需与数据模型的实体进行关联。步骤中的业务规则描述了需要读取的实体信息（输入项），以及业务规则处理后创建或修改的实体信息（输出项），在关联信息栏中将实体信息以及它的操作类型进行标注，以保持两个模型的一致。每个数据实体都有流程进行创建和读取，每个任务都有数据实体的创建。

2．流程模型与产品模型的对接：流程模型四级任务中抽离变量因子的“产品”是基础产品，如在业务规则上区分不同可售产品执行规则的差异，应通过产品条件，赋予不同的取值执行不同的业务规则。产品条件一定要有流程使用，但反过来，不是所有业务规则都需要产品条件，只有变量因子涉及“产品”时，有可能关联产品条件。

业务建模成果应用

业务建模成果除了展现业务架构、体现业务能力之外，将业务需求中与 IT 相关的内容转化成为应用需求，通过 IT 架构实施落地，实现自身价值。业务建模成果与 IT 架构的对接，目前采用的是业务组件层级的粒度，因为业务组件代表企业的最小业务能力。与业务建模成果相对应，IT 架构中的应用架构建立起应用组件与业务组件的对应关系，并承接业务架构落地实施。

4.4 小结

企业级业务架构是保障整体企业业务创新和运营、实现价值交付的核心，也是企业级 IT 系统建设模式的关键。企业级建模方法遵循业务统一视图、标准化、模型化等原则，构建了从企业级价值链到业务操作步骤的业务全景视图，实现了企业级流程共享，并通过业务规则、产品参数化实现快速支持业务创新。

第 5 章 IT 架构

基于企业的发展愿景和战略规划，企业应有相应的 IT 顶层设计，IT 架构是企业 IT 概要层或顶层的特定结构，通过架构设计将各信息系统有机整合，以符合企业发展需求甚至引领企业发展。

IT 架构是指从企业全局角度建立的，有关 IT 应用的一套完整模型和标准，是描述业务流程、应用、数据和技术等各个方面要素的结构及其关系的总体规划蓝图。业界 IT 架构通常由业务架构、数据架构、应用架构、技术架构组成，其中业务架构更多聚焦业务本身，在上一章中进行了详细介绍。而本实践认为，安全作为 IT 的一个重要属性，贯穿数据、应用、系统等各个层面，为此，将安全架构单独提出，与数据架构、应用架构、技术架构统称 IT 架构。

为更好地服务客户，企业不断创新业务产品，并要求 IT 能支撑新产品的快速部署或调整以满足客户需求。如何构建快速、灵活、易扩展的 IT 架构以提升 IT 价值，已成为企业 IT 部门必须直面的问题。在构建企业 IT 架构时，通常会遇到以下问题：

> 如何构建企业级的数据架构，并保证数据的一致性、完整性和准确性？

> 应用架构如何支持业务产品迅速部署并支撑市场拓展？

> 技术架构如何适应企业架构的变化，保证资源快速调配、应用灵活扩容和一致的客户体验？

> 安全架构如何有效应对企业面临的攻击和威胁、新技术带来的挑战，支持多样化的安全风险防范要求？

为实现企业核心价值，有效解决上述问题，应从整体出发，建立企业级 IT 架构。企业级 IT 架构应站在服务企业整体发展目标的角度，全面支撑业务流程、产品、信息、渠道等，遵循“采用面向服务的架构、业务与 IT 融合、以客户为中心、实现快速产品创新”的原则：

1. 采用面向服务的架构（SOA）：遵循松耦合的原则，采用层次化、组件化的方式，通过组件的共享，达到灵活响应和快速创新的目的。

2. 业务与 IT 融合：IT 架构与业务架构紧密衔接，技术创新的成果为业务模式的创新提供了源泉，为企业创造更大价值。

3. 以客户为中心：具备对客户的深刻洞察能力及灵活应变能力，有针对性、快速地满足客户需求。

4. 实现快速产品创新：实现产品参数化和灵活配置，使得产品创新更便捷、更快速、更灵活。

5.1 数据架构

数据已成为企业的重要资产，数据治理越来越受到重视。而数据架构是企业数据治理的关键，实现了数据标准化，为数据质量保证和数据管控提供基础。为解决数据架构中存在的完整性和一致性问题，应采用系统整体的方法，在企业范围内建立起一种健康、良好的数据生态环境，既解决当前数据问题，也建立长效机制，让数据始终处于一种可控可用的状态，即让数据“生态环境”具有自我调节、适应外部变化的能力。

5.1.1 数据架构定义

数据架构是企业 IT 架构的基础和核心，它从总体的视角描述了企业经营管理所需数据的整体结构、总体布局、支撑平台、实现方式、主要技术和管控机制等内容。数据架构的目标是“用好数、管好数”，形成良好的企业数据生态环境。

5.1.2 数据架构原则

数据架构要统一数据的规划、存储、计算、服务、接入，为保证数据架构的权威性，在企业的 IT 规划和建设中，数据架构需遵循以下原则：

> 业务认责原则：所有企业重要数据都必须明确业务责任人，业务责任人负责保证数据的准确性、一致性。

> 共享使用原则：数据的企业统筹是实现数据共享原则的基础。共享数据应对所有相关应用开放，并满足不同程度的实时性需求。

> 定义标准化原则：数据定义应满足完整性、正确性、一致性、可理解性、无二义性等要求，每个数据项必须拥有一个一致的、易于理解的业务定义。

> 模型驱动原则：数据模型包括企业级和应用级数据模型，应用级数据模型需在企业级建模方法的指导下建立，且完全融合成为企业级数据模型的一部分。

> 安全性原则：数据在采集、交换和应用过程中，必须采取必要的技术和管理手段确保数据安全。

> 可用性原则：基于业务需求和非功能需求，所有共享数据必须具备连续可用的能力。

> 创建及可信数据源采集唯一性原则：关键数据项必须单点创建，包括外部采集和内部加工形成的数据项；数据要从唯一的、可信的和许可的采集点采集。

5.1.3 数据架构设计

在企业范围内，规范一致的数据定义和描述是采集、加工、使用数据的前提和基础。在设计企业级数据架构时，可采用数据建模的方式，对企业运营中使用和关注的所有业务信息进行分类、抽象和规范描述，确保企业范围内每个数据项具有准确和统一的定义。企业级数据架构还包括对数据实体、实体包含的属性以及实体之间关系的定义，以形成企业级数据统一视图。数据按组织形式可分为结构化数据和非结构化数据，都涉及模型设计方法。

结构化数据建模

结构化数据模型自顶向下可分为若干层次，将企业经营管理所需要的数据从数据的本源出发分为若干主题域，采用层次分类结构对主题域进一步细分和规范，形成企业级的语义模型，采用第三范式的方式按业务对象进行统筹整合，形成逻辑数据模型，逐步按照降范式、实体拆分等形成应用级数据模型。

结构化企业数据模型的设计过程是先确定企业数据主题域以及信息分类和业务分类，再依次确

定各主题域的基础实体、属性实体以及两者之间的关系实体，最后确定实体的关键属性，这样逐级细化，形成层次清晰的企业级逻辑数据模型。逻辑模型的建立，通常采用自上而下与自下而上相结合的方法。

企业逻辑数据模型的构建方法有以下几种：

1. 自上而下：所有业务数据遵循企业概念数据模型的九大业务概念和分类进行建模，并在企业概念数据模型的基础上，对模型进行扩展。

2. 面向对象：在企业概念数据模型的分类模型基础上，选择业务上最稳定的分类方法，建立描述业务对象的实体模型。

3. 自下而上：分析现有系统中的数据结构，与逻辑数据模型实体进行映射，验证逻辑数据模型的正确性以及通用性，并依此修正和完善企业逻辑模型的建模内容。

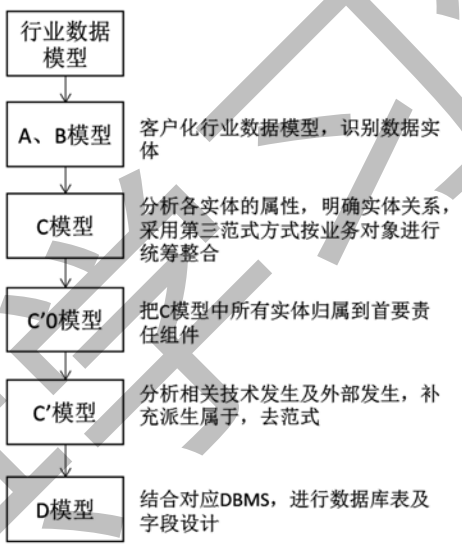

图 11 数据建模方法

结构化的数据模型根据行业数据模型自顶向下可进一步分为 A、B、C、C’0、C’和 D 六个层次的数据模型，其中 A、B、C 模型是概念模型，C’模型是逻辑模型，D 模型是物理模型，C’0 模型是管控模型。A 模型将企业经营管理所需数据分为九大概念，即参与人、合约、条件、产品、地点、分类、业务方向、事件、资源项；B 模型基于 A 模型、采用层次分类结构对数据进一步细分和规范，形成企业级的语义模型；C 模型将 B 模型定义的数据采用第三范式的方式按业务对象进行统筹整合，形成标准规范的数据模型；C’0 模型作为数据管控和应用的基础，将 C 模型从应用的角度按实体粒度划分到相应的应用组件中，实现数据建模和流程建模的关联；C’模型作为应用级数据模型，是在C’0 模型基础之上考虑应用系统具体实施层面的要求，进行降范式和实体拆分等操作后形成的；D 模型则

是在 C’模型基础上考虑系统性能等因素，并结合数据库管理系统的特点进行优化而形成的物理数据模型。

非结构化数据建模

非结构化数据是指在业务开展过程中产生的，无法用关系数据库管理的各种数据。企业内部所产生的非结构化数据，其内涵比较宽泛，通常包括一般的文件、文档、合同、发票、表格、电子邮件、动态 Web 网页、广告、程序、软件、音频、视频以及流媒体等。

为加强非结构化数据的分析和应用，需要对非结构化数据进行统一定义，包括非结构化数据对象本身、对应技术元数据及关键字索引。

在非结构化数据建模过程中，通过建立非结构化数据父类和子类，明确其对应的属性和操作方法，实现可扩展性。

5.2 应用架构

应用架构向上承接了企业战略发展方向和业务模式，向下指导企业 IT 系统的定位和功能，定义了系统的边界和系统间的关系等内容，统一了应用系统建设原则和标准，为企业 IT 治理起到非常重要的作用。企业级 IT 应用架构应依据企业级 IT 架构建设原则，采用业界先进的面向服务架构（SOA），遵循层次化、组件化、微服务设计理念。

5.2.1 应用架构定义

应用架构定义了系统内的基本组织结构和纲要，描述了 IT 系统功能和技术实现的内容。随着 IT 技术的发展，应用系统越来越复杂，应用架构从最初的单机式开始，逐步发展为分布式，到目前比较先进的 SOA 架构。

单机式架构只有一个应用，部署在一台服务器，将应用按照功能分割，降低了业务复杂性，模块之间采用进程内部调用，技术实现简单，容易测试和部署，但代码复杂，难以支持大团队并行开发，后期难以维护。

在分布式架构应用中，每个应用独立开发、独立部署，应用通过有限的 API 接口互相关联，应用内部高内聚，应用之间松耦合。这种架构业务边界清晰，支持大项目并行开发，但一般 API 调用缺乏可靠性保障，大量调用将严重影响系统整体可靠性。

SOA 架构也是分布式架构的一种，但是前端应用不再通过 API 和后端进行关联，而是通过后端提供的服务共享业务逻辑，每个服务都是独立部署，调用灵活。服务间通过定义良好的接口联系起来，使得构建的系统服务以一种统一和通用的方式进行交互。架构组件标准化、专业化、微服务化，以达到松耦合的目标，保持架构的灵活性、稳定性和可扩展性。

5.2.2 应用架构原则

应用架构的设计、规划应遵循统一的原则和要求，形成统一标准体系。尤其大型应用系统的开发设计，需要根据规划对应用服务进行分层，明确系统开发的原则，保障业务目标和 IT 目标的实现。

架构分层是对架构整体复杂性进行解构的方法。其中，“关注点分离”是面向服务的架构的核心原则，用以保持架构的灵活性、稳定性和可扩展性，适应业务的不断变革和发展。架构分层遵循这一重要原则，可对复杂的应用需求进行横向和纵向的分割，使各个服务之间松耦合，内部高内聚，划分成不同的层次和平台。应用的具体开发应该满足特定的架构规范，才能确保符合应用架构的整体要求。

应用系统架构设计原则包括：

> 以客户为中心的原则：围绕外部客户和内部员工，提供方便、简单、便捷的应用服务，满足客户需求、提升客户体验。

> 一体化服务原则：以面向服务的架构设计，采用分层和划分平台的方式，合理规划企业业务需求，把不同系统中同一功能的需求进行整合，满足业务的快速发展需要，为业务创新提供有力支撑。

> 可重用原则：应用系统功能的设计应保证最大可能的可重用性和模块化，并使用现有系统中符合可重用性的功能模块。

> 双模开发原则：对业务成熟的应用系统采用模型和方法论驱动，以及统一方法、工具和流程的开发方法对创新性业务采用敏捷与快速迭代开发方法。

> 支持客户单一视图原则：识别客户行为习惯，为客户提供个性化可定制视图。

5.2.3 应用架构设计

企业应建立以客户为中心、面向服务的应用架构，由应用和应用组件实现，为客户提供产品和服务。架构设计可从两个层面考虑：一是从客户（包括外部客户和内部员工）的角度，需要整合企业产品、服务，提供端到端的完整客户服务流程，建立跨渠道的统一业务流程，提供良好的使用体验；二是从企业角度，需要整合企业级 IT 服务能力，提供专业、深度的产品服务，统一处理渠道、客户、产品之间的差异。

通过业界先进的面向服务的架构模型，遵循层次化、组件化设计理念，对企业业务抽象化，搭建起企业级的应用架构体系。下图为包含七层十二个平台的典型企业级 IT 架构体系。

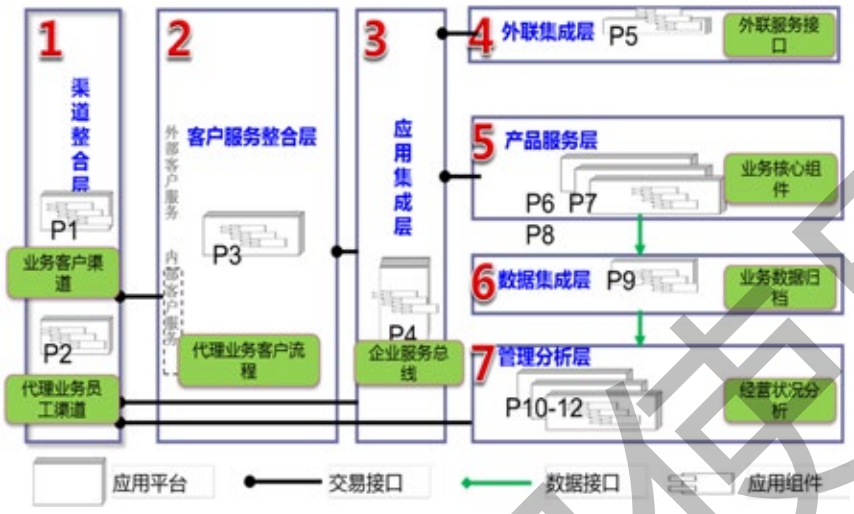

图 12 七层十二个平台企业级应用架构

1. 七层架构实现了渠道与流程、应用与数据、产品操作型和管理分析型处理的分离；通过各平台能力和平台间协同，支持卓越的客户体验、面向客户的集成服务、快速产品部署、高质量的数据服务和优化的企业级管理能力。分别为：

渠道整合层：通过标准化接入手段接受来自不同渠道的业务请求，处理并封装来自不同渠道的数据，调用后台业务服务并返回运行结果。

客户服务整合层：从客户视角出发，整合端到端的客户服务流程，为外部客户提供集成服务，同时为企业内部用户提供操作各类后台业务的集成服务。

应用集成层：通过标准化方式接受来自客户服务整合层的服务请求，为其屏蔽后台业务服务的技术特性，并以一致的形式返回服务结果。

外联集成层：连接各类外部系统，完成协议转换、报文转发等，提供实时和非实时的服务，为内部系统屏蔽技术特性。

产品服务层：支持企业核心业务服务，涉及产品、客户、合约、核算等，提供渠道无关的产品、服务处理组件。

数据集成层：对产品服务层的各类数据，进行整合维度分析，提供一致的面向数据的集成服务和周期性、大规模数据的批量处理，为产品服务层和管理分析层提供一致的数据服务。

管理分析层：包含所有管理分析类应用，所有应用从数据集成层获取交易系统数据，进行加工、处理及分析，为企业内部管理和决策提供支持。

2. 十二个应用平台覆盖七层应用架构，企业 IT 系统基于这十二个统一、标准的平台进行开发，并且通过组件的共享，达到灵活响应和快速创新。

P1 外部客户渠道整合服务平台：受理企业外部客户使用不同终端设备，不同客户端软件的业务请求，对后端业务受理系统屏蔽终端设备和请求协议的差异，统一封装不同的渠道业务数据，调用后台业务服务并接收请求服务返回结果，将结果数据和终端设备、客户端软件的渠道展示特性进行适配转换，返回渠道。

P2 内部员工渠道整合平台：受理企业员工使用不同终端设备，不同客户端软件的业务请求，对后端业务受理系统屏蔽终端设备和请求协议的差异，统一封装不同的渠道业务数据，调用后台业务服务并接收请求服务返回结果，将结果数据和终端设备、客户端软件的渠道展示特性进行适配转换，返回渠道。

P3 客户服务整合平台：整合端到端的客户服务流程，为客户提供集成的服务，提供面向不同用户的流程编排服务，同时也提供面向单一用户的复杂交易的集成服务。

P4 应用集成平台：为客户服务整合层及渠道整合层（其他层）提供标准化的服务调用功能，通过标准化方式接受来自客户服务整合层的服务请求，为其屏蔽后台业务服务的技术特性，并以一致的形式返回服务结果。

P5 外联集成服务平台：提供与外部机构系统间的服务交互，连接各类外部系统服务，完成协议转换、报文转发等，并提供实时和非实时的服务形式，为内部系统屏蔽技术特性，从而保证内部系统的独立性和内外系统的松耦合。

P6-P8 产品服务平台：构建在数据组件、技术组件基础上，由多个公共应用组件和服务组成用以支撑产品服务的应用平台，包括主机平台（P6）、开放 C 平台（P7）和开放 J2EE 平台（P8），主要区别是物理实现技术和特性的不同。

P9 数据集成平台：数据集成服务平台整合企业范围内的各类数据，为产品服务层和管理分析层提供一致的数据服务，具有海量数据存储能力、数据模型能力、大数据量分区能力、大批量处理的计算能力、数据质量的控制能力（数据传输技术检核能力、数据横向检核能力）、高并发处理能力、报表数据存储能力和非结构化数据管理能力。

P10-P12 管理分析平台：按照业务应用需求从数据集成层读取数据，以合适的展现形式支持业务决策和管理，包括：管理分析服务平台（P10）、高效一体化办公服务平台（P11）、在线交易数据服务平台（P12）。

5.3 技术架构

技术架构是支持应用和数据具体需求实现的技术平台和组件的统称。遵循企业级、组件化、面向服务的架构（SOA）设计思想，企业级技术架构实现了技术组件、技术服务、部署模式及运维管控的有机结合，保障 IT 基础设施的稳定运行和 IT 资源的有效供给，支撑业务应用的灵活、快速的部署和扩展。

5.3.1 技术架构定义

技术架构定义了支持应用和数据的基础技术平台和组件，并明确了平台和组件的边界、范围和关联关系。每个应用架构模式代表一种应用部署的典型关系，技术架构可根据不同的应用架构模式明确所需的技术部件，同时根据应用架构分层明确不同的物理技术平台及各平台所需要部署的技术部件，之后考虑用户的性质差异和应用模式推导出所需的系统，最后结合物理应用架构和数据架构定义出物理系统。

5.3.2 技术架构原则

技术架构设计原则是指为落实 IT 规划，确保技术架构策略和标准的严格贯彻执行，用以指导企业在进行技术架构设计时，需要考虑或遵循的决策规则。设计原则如下：

> 面向 SOA 的技术服务体系：建立面向 SOA 的技术服务体系，提高技术架构的敏捷性和灵活性。实现松耦合的架构，实现技术服务与产品或技术的无关性。

> 集中部署原则：从企业级角度采用集中部署原则，集中利用 IT 资源。同时，应考虑设立多个数据中心以满足容灾需求。

> 系统集中管理原则：确保技术架构从企业级角度出发，实现整体的可管理性，确保技术架构中的全部技术组件实现端到端的”可见”、”可管”和”可控”。

> 基础设施建设的一体化原则：开发、测试、生产和灾备环境的技术架构应遵循一体化分析、设计和建设的原则，以保证端到端的设计一致性，降低实施和支持 IT 项目的成本，实现 IT 技术架构资源的整合和优化。

> 可用性分级原则：技术架构的设计必须支持各应用系统的持续可用。各个系统的可用性需求不一，架构设计需要考虑各个系统、基础设施的可用性保障等级。

> 可扩展设计原则：技术架构应支持灵活扩展，及时响应市场和业务高峰变化。

> 成熟性与先进性平衡原则：在技术选择方面，在保证技术成熟度的同时，要适当引进新技术，以确保技术架构的先进性。

> 组件可管理原则：组件应可测量、可监测、可管理。

5.3.3 技术架构设计

为建立以客户为中心、面向服务的架构，更好地支撑业务应用，提供企业级稳定运行、快速供给能力，技术架构的设计需满足以下几方面要求：

> 集中管理的多中心架构；

> 松散耦合的应用管理；

> 标准化的资源供给体系；

> 统一的应用、数据、基础架构集成管理；

> 合理的网络区域划分与边界控制。

基于面向服务的架构模型，承接企业级应用架构统一设计，技术架构设计包括技术组件和服务、部署模式、资源供给机制等。

技术组件和服务

技术服务是指一组含有非功能性需求“能力”的描述，技术服务的识别来自于业务能力需求和非功能性需求组合。

技术组件是根据技术服务的相似性，以及在一个统一的“容器”内实现技术服务的可能性（包括一些业界最佳实践）所总结并定义，是支持业务和应用的一组技术部件统一视图，一个组件可以实现多个技术服务，以使其可以被统一的描述和有效地部署。

以企业级七层十二个平台应用架构为例，识别并定义出相应的技术组件及服务，具体描述如下：

1. 基础架构层组件为上层提供处理器、存储以及网络资源，采用虚拟化、云计算技术，形成虚拟的资源池，动态地为应用提供服务，资源利用率和可靠性得到进一步提高。

2. IT 服务管理组件是统一调度资源，实现云服务的控制点，从而使得上述的各个体系能够有效地集成在一起。资源调度时通过供应一组服务以及服务集成的体系，并通过预置的配置系统来管理整体的架构运行。

3. 通用服务组件是一组被各应用系统广泛引用的功能性以及非功能性组件。它使运行环境更加易于管理，能够更快地响应应用需求的变化，更好地支持面向服务的架构体系（SOA）。通用服务是可以被共享使用的应用类技术服务，通过对通用技术的服务化和集成，提供符合 SOA 标准或者业界通用标准的接口，支持每个技术服务的企业级部署和服务提供。

部署模式

底层的技术组件经由分解、推导、归纳等过程组合成可被快速部署的部署单元（DU），部署单元又可依据应用模式特性需求结合成各种技术组件的部署模式，最后支持上层 12 个平台的平台服务。

服务主要采用云计算的方式进行部署。部署单元是根据各个不同平台的需求，将多个技术组件组合成为一个新的可以被独立部署并提供某一组功能的组合体，每个部署单元包括应用部署所需要的资源，资源上加载的中间件以及和独立的技术服务集成的服务接口。部署模式是技术服务在部署时可以被选择的拓扑架构，一个技术服务通常会有多种部署模式，每种部署模式有其适用的场景或条件。

服务部署的整个过程由 IT 服务管理组件控制，该组件既管理系统初始化时安装“部署单元”的部署，也管理上层一些预集成系统（如时钟、备份等）配置的部署，还包括运行中动态资源的调度和“部署单元”的生命周期管理。

资源供给机制

当每个部署单元定义明确后，需要从统一的资源池中获得其所需的部署资源。资源池的目标是提供统一的，可被调度的标准资源体系，以使得资源供给和服务集成“快速、标准、可靠”。底层

硬件如服务器，存储和网络资源，这些资源构成了基础架构云（IaaS）环境的基本组成单元；应用运行所需的软件资源如操作系统、数据库和中间件需要从软件的映像资源库中获得，并在分配时完成基础部署，这些资源构成了平台级云（PaaS）环境的基本组成单元。

云服务是面向企业级应用平台的服务供给环节，其目标是在标准的应用模式体系下，提供“预装”的解决方案，从而使得应用的部署和集成实现“随需应变”的运行调度管理。

5.4 安全架构

安全架构是企业 IT 架构不可或缺的内容，能够有效保护企业信息资产，保障信息系统安全稳定运行，保护企业数据安全，构建主动的安全防御体系，适应未来新技术发展趋势，建设面向服务的安全架构体系，有效应对企业面临的攻击和威胁、新技术带来的挑战，满足内外部监管要求。安全架构应践行“安全即服务”的理念，将安全技术、产品以组件化、可定制的安全服务方式提供给应用，形成集中、统一、灵活、智能的信息安全保障体系，支持多样的安全风险防范要求，有力支持企业的业务创新与发展。

5.4.1 安全架构定义

安全架构是指为应对新的安全威胁，以及 IT 技术和业务的发展过程中形成的新安全态势，所提出的安全防护理念、安全技术、安全组件、安全服务及管控模式等应对措施的集合。企业应结合自身特点和业务发展开展安全架构的建设工作。

5.4.2 安全架构原则

安全架构设计遵循以下原则：

> 业务驱动：将适应业务发展作为安全服务、安全基础框架建设的目标和方向。将安全管理由传统的以技术领域划分转变为以业务应用场景和流程划分，从信息系统安全延伸到应用安全、业务安全，从单点控制提升到企业级、全局风险管控的管理高度。

> 安全与用户体验平衡：平衡安全与客户体验，以客户风险等级为基础采取针对性的安全防护措施，提供差异化的安全服务。

> 安全与效率平衡：平衡安全与服务效率，保证业务服务高效的同时提供完备适当的安全服务，实现风险控制与业务发展价值最大化。

> 策略集中管理：将各个业务流程进行统一的标准化管理，针对不同的业务流程制定专属的安全管理策略，并将所有的安全策略集中管理。

> 组件化、可定制：将信息安全技术进行标准化和模块化处理，通过各种统一的标准模块将安全功能灵活、快速组合，以满足各个应用系统的个性化安全需求，提供定制化的安全支撑。

5.4.3 安全架构设计

安全架构实现了建设理念、角色定位、工作方式、实现模式和用户体验等的全面转变，形成了由服务接入层、应用安全服务层、基础设施安全服务层和安全策略管理中心组成的全新“安全架构”。

图 13 安全即服务的安全架构

基础设施安全服务层

基础设施安全组件在终端、网络、系统、云等方面，通过终端设备认证、非法外联、系统安全加固及规范配置、云防病毒、网络隔离、防拒绝服务攻击等各类安全控制机制，保障基础设施安全，延伸企业安全边界，扩展企业业务办理渠道，为应用安全提供基础保障。

网络安全方面，以企业安全策略为总体原则，实现平台安全域划分、不同强度的访问控制、各网络区域的隔离措施等安全要求，满足了管理策略中提出的对基础设施安全的要求。其中网络安全包括网络安全域划分、隔离安全策略、服务器区安全、开发测试网安全、灾备中心安全、接入网安全、互联网服务区安全、外联网服务区安全；终端安全包括资产管理、防恶、软件及补丁管理、系统健康检查等；云安全包括服务器虚拟化安全和桌面云安全，其中服务器虚拟化安全采取了网络隔离并部署防逃逸产品，桌面云安全部署了防病毒和敏感信息监控产品。

应用安全服务层

应用安全服务层提供了信息系统安全的核心功能，包括用户认证、客户认证、密码服务、数据安全和安全监控。将安全功能从应用中解耦，实现了安全功能的组件化、标准化、专业化，面向所有安全对象，建立全面、集中、统一、灵活的安全服务体系，提供全面、透明、高效、可靠、面向服务的安全机制。

1. 用户认证组件

用户认证组件为企业员工多渠道接入提供统一规范、灵活便捷的身份认证和单点登录服务，支持用户多应用一站式登录，支持不同内部办公、业务及管理系统，满足不同员工的安全需求，提升企业内部员工认证效率和安全水平。

企业级身份认证平台，采用多认证方式，灵活支持员工使用多种认证方式进行身份认证，如静态口令、动态口令、指纹、动态令牌等，并为数字证书、人脸识别等认证方式保留扩展接口。实现多协议接入，为 C/S 应用系统提供基于 HTTPS 协议的认证与单点登录接口，为 B/S 应用系统提供统一认证与统一登录服务，为 VPN 接入、网络设备提供 RADIUS、LDAP 协议。

2. 客户认证组件

客户身份认证采用了企业统一的客户认证组件，该组件提供多种方式的身份认证机制，为不同业务系统提供接入安全保证，可满足不同业务需求和业务创新需求。

客户认证组件为企业信息系统提供了静态口令、动态口令、短信验证、数字证书等传统认证方式，针对客户风险等级、交易限额也采取了相应的认证措施，从而有效的提升了企业信息系统的安全性和客户资金的安全性。同时，客户认证组件也实现了生物特征认证方式，如虹膜识别技术，以代替密码、令牌等传统的身份认证方式，解决了企业客户身份的确认难点，为客户提供安全、便捷的企业交易身份认证新模式。

3. 密码服务组件

密码服务组件建立了企业级的密码服务体系，为企业各应用、组件及外联单位提供标准、透明的密码服务和统一集中的密钥管理服务，实现了企业级的密钥统一协商和同步，是确保数据机密性、完整性和防抵赖的重要手段。密码服务组件为企业业务系统提供统一的密钥管理机制，能够有效地提升企业业务系统的安全等级。

4. 数据安全组件

数据安全组件提供数据集散地、数据脱敏、文档权限控制、数据水印、在线浏览、数据销毁等安全功能和服务，有效提升了企业的数据保护能力。多个安全区域的构建实现了数据的分级分类保护和方便使用；数据集散地实现数据在各安全区域内部、安全区域之间、安全区域与数据集散地之间的发布和流转，并集成了数据脱敏、在线浏览等功能以保障数据跨区域流转的安全性；文档权限控制、数据水印和数据销毁等功能实现了对数据本身的安全加固，并保证数据全生命周期权限的统一管理。

数据安全组件为内部员工提供了离线生产数据专用环境、敏感数据在线安全浏览、外发互联网敏感信息拦截等安全服务，既支持了企业管理、营销等业务能合规使用客户信息等敏感数据，又有效防控了敏感数据泄露。

5. 安全监控组件

安全监控组件负责全面采集各类安全监控对象（主机、网络设备、终端设备、安全设备、应用组件、

技术组件、安全组件、运维平台等）的安全日志信息，分析安全风险事件，展示企业 IT 风险态势，及时发现来自内外部的攻击威胁、违规行为，识别潜在风险和安全隐患，保障企业信息系统的持续安全运营。

安全监控组件通过建立统一日志采集平台，提供多样化的日志采集模式，将体系内基础设施日志、应用安全日志、应用业务数据和外部安全数据进行集中管理分析。

安全监控组件充分发挥了关联分析能力，结合外部威胁情报、内部监测发现、交易风控等数据，利用人工智能、大数据挖掘技术，监控窃取客户资金、入侵企业网络、信息泄露、员工违规等事件。

服务接入层

服务接入层将信息安全功能以服务的形式接入到各个业务应用系统中。该层提供安全代理、安全插件和安全客户端，独立于业务应用系统，为业务应用系统提供安全相关功能接口的集合，主要包括加解密运算、数字签名、用户认证等安全功能，是业务系统与安全服务发生直接联系的窗口。另外，服务接入层将业务系统与安全服务进行了解耦，安全服务的调整将不会影响业务系统的运行。下图清晰地展现了使用传统安全架构与使用“安全即服务”（SECaaS）安全架构的对比。

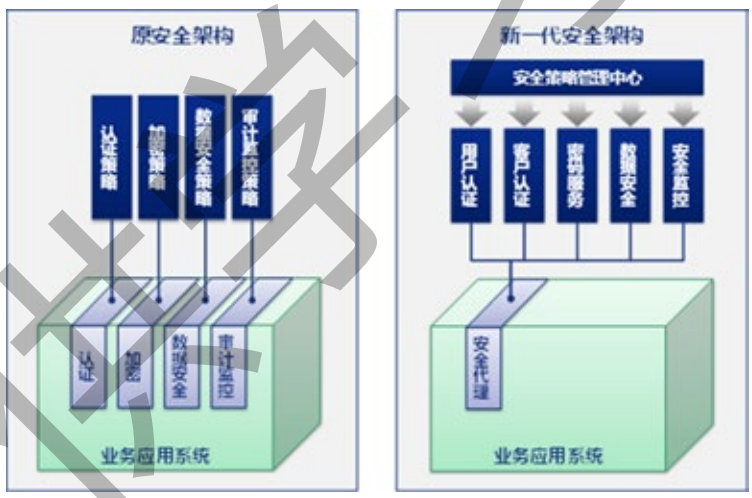

图 14 传统安全架构与 SECaaS 安全架构对比

安全代理和安全插件支持多平台部署，提供安全功能和安全服务的统一接口，实现安全功能的合理分布，达到安全功能部署集中与高效的平衡。

应用系统可依据自身的技术架构选择部署安全代理或安全插件，代理和插件部署在各个应用平台，为应用系统集中提供安全服务。安全代理和安全插件采用颁发给应用系统数字证书的方式绑定应用系统的身份，在提供安全服务的过程中应用系统需要使用数字证书进行身份认证。

安全代理对应用系统提供安全服务的API接口。通过调用接口，应用系统可触发相应的安全服务。安全代理和插件也会定期检查应用系统的安全服务状态，例如自动检测密钥的有效期，在密钥到达有效期后自动发起密钥协商操作，实现对应用的透明服务。同时，安全代理和安全插件也可开启监听服务，接受来自其他安全代理和插件的相关请求。

安全策略管理中心

安全策略管理中心实现企业的统一安全策略管理，为安全架构提供策略支持，建立企业统一的安全管理视图。安全策略管理中心实现了对安全对象（安全节点、客户端、安全代理、插件等）的统一管理，对安全策略（认证策略、凭证策略、密钥策略、终端策略等）的统一发布，提升了安全架构的管控能力。同时，安全策略管理中心通过对认证服务和加密服务等安全服务的可用性监测，提升了安全服务的可用性；通过参数管理，提升了精细化管理的粒度，实现参数化管理安全策略。

5.5 小结

通过自上而下逐步分解的结构化和非结构化数据建模方法，企业级数据架构保证了数据的一致性、完整性和准确性，形成统一的数据视图，能够真正实现以客户为中心的产品推送、个性服务定制等，为大数据分析和应用奠定了坚实的基础。

企业建立的以客户为中心、面向服务的应用架构，由企业级七层十二个平台和应用组件实现。当需要开发新型业务产品时，通过组件快速组装，能够迅速实现业务功能，因此基于该应用架构的开发模式极大程度减少重复开发量，借助平台提供的通用技术组件及服务可达到敏捷开发、快速响应业务需求的目的。

技术架构基于面向服务的架构模型，承接企业级应用架构，创建灵活、松耦合的技术平台和组件，保障 IT 基础设施的稳定运行和 IT 资源的有效供给，支撑业务应用的灵活、快速的部署和扩展。

以“安全即服务”的理念，构建由服务接入层、应用安全服务层、基础设施安全服务层和安全策略管理中心组成的全新“安全架构”。通过 IT 风险态势分析和灵活的安全策略配置，平衡安全控制和客户体验，SECaaS 安全架构可有效防范有组织、有目的的外部攻击，同时快速适应云计算、虚拟化、大数据、移动互联网等新型信息技术手段，为用户提供更为灵活、实用的应用及服务模式。

第 6 章 科技内控

随着 IT 的作用从业务支持逐渐走向与业务的融合，IT 风险带来的挑战日益严峻，IT 监管要求更加严格，内部控制需求也更加强烈，企业需要更加完善的科技内控机制。完善科技内部控制体系是保障企业健康发展的生命线，同时又是企业提升自身核心竞争力的内在需求。

科技内控应建立一套完善的监管合规体系以满足 IT 监管和企业 IT 内控要求，通过检查监督、考核评价、整改落实等措施不断促进企业 IT 内控管理的执行和改进。在建立科技内控体系方面，企业需要解决的关键问题主要包括：

- 如何有效地使内部科技政策与监管要求保持一致？
- 如何确保科技政策能动态地适应行业监管要求、业界标准的变化形势？
- 如何建立科技监督检查机制，及时发现 IT 违规行为？
- 如何科学合理地评价企业科技合规管理落实情况？
- 如何提升企业 IT 合规问题的整改能力？

6.1 监管传导

6.1.1 监管要求和标准传导

为有效落实 IT 监管要求、实践业界 IT 风险管理先进理念，建立企业统一的 IT 管控领域，梳理监管制度和业界标准数据库，系统、全面地指导和完善企业科技政策，夯实科技内控基础。

1．编制 IT 监管制度导读

监管制度导读按企业统一 IT 管控领域，从本国（地区）、行业、上市公司等层面梳理 IT 监管制度。针对每项制度，介绍出台背景、制度主线、主要内容，并整理需要落实的 IT 任务，指导管理人员学习和落实监管制度，有效促进科技合规管理。

2．编制 IT 监管报告指南

监管报告指南收集涉及报送事项的监管制度，介绍监管机构及其监管重点、报送的事项、内部分支机构适用范围以及报送要求。从重大事件、专项任务、周期性报告等三方面梳理报告事项，指导企业准确及时地向监管机构报告报送。

3．建立国内 IT 监管库

根据 IT 管控领域，梳理 IT 监管要求，建立国内 IT 监管库。国内 IT 监管库通常包括监管制度、监管要求、涉及的企业业务阶段、业务部门、业务领域等要素。

通过 IT 监管数据库，可分析监管机构的监管重点，帮助企业内部不同领域的团队筛选出其涉及或关注的监管制度原文内容，有针对性地学习和落实。

4．建立海外 IT 监管库

为确保海外业务合规拓展，收集各国（地区）监管机构要求和规则，形成海外 IT 监管制度汇编，

建立各国家（地区）IT 监管库。根据 IT 管控领域，综合分析各国（地区）间的监管要求，求同存异，形成整体海外 IT 监管库。海外 IT 监管库通常包括控制领域、监管制度、监管要求、涉及的企业业务阶段、涉及的企业业务部门、业务领域等要素。

通过海外 IT 监管库，企业可针对同一 IT 管控领域的监管制度，分析海外各国（地区）监管差异，加强海外 IT 系统建设、数据保护、电子银行、业务连续性等合规管理。

5. 建立业界 IT 风险标准库

为及时了解业界 IT 风险管理先进理念，系统学习业界 IT 风险管理最佳实践，通过分析如 COBIT5 等业界主流 IT 风险管理标准，企业可建立业界 IT 风险标准库。业界 IT 风险标准库通常包括控制领域、管控要求、标准名称、对应条款编号、涉及的企业业务部门等要素。

通过业界 IT 风险标准库，企业可分析不同业界标准针对 IT 管控领域的管控要求，并根据标准的适用范围和应用场景加以借鉴，增强企业运用最佳实践的能力。

6.1.2 持续跟踪

随着 IT 监管制度和业界标准的不断更新、完善，企业需建立相应的持续跟踪机制，及时收集最新的监管制度及标准，并将其纳入监管和标准数据库，督促内部落地执行。

1．建立国内外监管要求跟踪机制，及时更新 IT 监管库，加强对最新监管要求的传导。

2．建立国内外标准跟踪机制，及时更新 IT 风险标准库，论证纳入企业 IT 管理要求的可行性。

3．分析 IT 监管制度和业界标准更新前后的差异，形成 IT 管理的新思路和新实践，适时修订 IT 制度。

6.2 检查监督

为保障企业业务安全、持续、稳健发展，促进科技内控管理，根据企业 IT 管理制度要求，应定期开展 IT 检查监督工作。

6.2.1 检查范围及内容

检查范围

企业 IT 检查范围包含 IT 工作涉及的所有活动，通常包括以下内容：规划管理、架构管理、项目管理、业务需求管理、开发管理、运维管理、IT 风险管理、服务连续性管理、外包管理、IT 资源管理和合规管理等。

检查内容

1．检查针对企业 IT 工作检查范围中的各个活动，检查其执行过程的合规性和执行结果的正确性，检查内容一般包括：

计划：包括职责分工，策略、方案的制定情况。

执行：对执行过程中关键环节的控制情况。

结果：对执行结果的审核、验证、评估等情况。

定期评估：对流程执行情况的定期回顾，持续改进情况。

2．对审计和检查发现问题处置的及时性、有效性进行检查，检查内容包括：对问题的认知情况和产生原因的分析情况；问题整改工作的落实情况。

3．对监管机构风险提示开展自查的及时性和实施防范措施的有效性进行检查，检查内容包括：自查工作的开展情况；针对自查发现风险的控制情况；风险的持续监测情况。

6.2.2 检查计划

IT 检查计划包括计划管理及检查标准的制定。

检查计划管理

检查组织者应根据 IT 工作总体安排、上年度 IT 工作检查结果、内外部审计发现等情况确定本年度检查对象及检查任务，每年初发布年度 IT 工作检查计划。检查任务包括 IT 全面检查和专项检查。

1．全面检查应每年覆盖全辖一次，其中应对所辖三分之一以上机构进行现场检查。

2．出现以下情况时，检查组织者应结合所辖机构以往工作检查情况，确定是否启动专项 IT 检查工作：新系统上线或已有系统进行重大变更；IT 运行中发现重大纰漏或隐患；涉及 IT 运行的重大任务；内部或同业出现重大 IT 风险事件；IT 审计中发现重大问题；监管部门下发 IT 检查工作要求，或发布 IT 风险提示。

检查标准管理

检查标准是制定 IT 检查方案的基准。检查标准通常包含检查项、检查依据、基本要求、检查手段、标准分值、评分标准等要素。

1．检查项基于检查范围和检查内容确定。

2．检查依据通常包括：国家（地区）层面关于 IT 管理、信息安全管理等相关法律法规；监管机构 IT 监管政策、标准及要求；企业内部各级机构的 IT 相关制度、标准规范及通知要求。

3．结合检查项和检查依据，形成检查的基本要求。

4．检查手段是对检查步骤、检查方法等的详细描述。

5．标准分值是指满足该检查项基本要求的得分，反映了该检查项所占的权重。

6．评分标准是对检查项进行评分的标准。

检查标准制定者应根据 IT 内外部管理要求的变动对检查标准进行动态维护和更新。触发检查标准更新的条件通常包括以下内容：

1．国家（地区）法律法规颁布时，外部监管规定、规范及标准发布时，企业 IT 管理制度、规范、配套细则印发时。

2．下发重大 IT 工作任务，提出新的 IT 管理要求时。

3．检查标准的依据发生修订或废止的情况时。

4．检查标准制定者根据实际检查或反馈情况，发现检查标准不适用或缺失时。

5．检查标准制定者管理职能发生变化时。

6.2.3 检查实施

检查实施包括检查方法及检查流程。

检查方法

IT 工作检查有三种工作方式：现场检查、非现场远程登录检查和非现场信息报送检查。

1．现场检查是通过现场查阅材料、访谈、查看、实测等方法，对被检查者的 IT 工作进行检查。

2．非现场远程登录检查是指通过远程登录相关系统，远程采集数据，对被检查者的 IT 工作进行检查。

3.非现场信息报送检查是指通过收集、分析被检查者报送的信息,对被检查者的IT工作进行检查。

IT 检查流程

IT检查工作流程包括制定检查方案、学习检查方案、下达检查通知、开展检查工作、提交检查结果、下发整改通知书、开展整改等。

1．依据检查标准，组织制定检查方案。检查方案通常包括以下内容：检查对象、检查范围、检查目的、检查方式、检查指南、检查工作安排等。

2．组建检查团队或指定检查人员，组织学习检查方案。

3．向被检查者下达检查通知书。

4．检查团队或检查人员依据检查方案组织开展检查工作。

5.检查团队或检查人员及时总结检查工作情况,向检查执行者汇报检查结果,并提交检查组织者。

6．检查组织者向被检查者下发整改通知书，并监督、跟踪问题的整改。

7．被检查者对检查出的问题开展整改，并将整改情况向检查组织者报告。

6.3 考核评价

为保障企业IT目标与业务目标保持一致,客观有效评价企业IT活动,应建立企业IT考核评价机制。IT 考核评价作为企业 IT 工作的“风向标”和“指挥棒”，可发挥引导作用，推动企业 IT 工作的落实和目标的达成。

6.3.1 IT 考核机制

考核原则

1．全面覆盖原则：企业 IT 工作考核应覆盖企业 IT 工作的各方面，通常包括 IT 建设、IT 运维、IT 计划等企业 IT 相关领域。

2.重点突出原则: 突出企业IT重点关注的领域,如监管机构关注重点、业务创新支持、运维保障等。

3．客观公正原则：严格按照考核标准实事求是、公平合理地确定考核结果。

4．定量定性结合原则：考核指标应以定量指标为主，以定性指标为辅。

考核内容

1.考核指标: 制定考核指标时可将被考核机构或部门进行分类,不同的类别采用不同的考核指标。

2．指标占比：应明确各考核大项的指标占比，考核分项指标的权重。

3．评价标准：通过评价标准明确考核数据的出处、数据运用方法，以及考核数据的主要来源，比如来源于 IT 管理系统、定期 IT 管理通报和考核期内的历史评价结果。

考核实施

1．考核方案编制：考核方案制定者组织 IT 部门职能条线编制考核指标、评价标准及指标占比，形成考核方案，审定后正式发布。

2．自评价：考核实施者组织被考核对象根据考核方案进行自评。被考核对象按时报送自评结果及自评说明材料。

3．考核：考核实施者将被考核单位自评结果及自评说明材料提交给相关职能条线。各职能条线按考核方案，根据 IT 管理系统、IT 管理通报等数据，对被考核单位进行评价，评价结果由考核实施者汇总整理。

4．结果审定：考核实施者将考核汇总结果报送考核审定者审定。

考核结果运用

考核结果是被考核对象 IT 业绩评定、项目审批、检查监督等的重要依据。

6.3.2 IT 操作水平

IT 操作水平是企业 IT 服务质量评价的重要手段，采用正式的、定量的方式明确开发部门、运维部门及分支机构支撑业务需求的 IT 服务能力。操作水平体系的建立有利于保障企业 IT 系统的安全稳定运行和快速恢复生产，帮助企业明确界定 IT 开发、测试、运行的职责界面，引导企业 IT 职能部门主动发现风险隐患并持续改进，不断提升 IT 服务水平。

操作水平管理原则

1．以安全生产为核心：以 IT 服务管理流程为指引建立操作水平指标体系，通过评估体系落实与安全生产相关的内容，强化对安全生产的全过程管理。

2．以服务改进为导向：引入 PDCA 的管理模式，在操作水平体系的落实过程中总结经验，持续提升和逐步深化基于服务的 IT 管理模式，全面提升安全生产能力。

3．以服务管理为框架：从以技术为中心的 IT 管理转向基于服务的管理。以 COBIT 为模型建立整体的服务管理体系框架，以 ITIL 服务生命周期管理的最佳实践为依据，建立服务分解和服务目标的逐级支撑保障。

4．以指标测评为驱动：基于客观事实和数据，建立量化管理评价体系，提升 IT 服务质量。

操作水平协议管理

为有效推行 IT 操作水平协议，有必要制定操作水平协议管理的相关制度，操作水平协议管理制度需要明确以下几方面内容：

1．明确角色职责

服务管理办公室负责组织建立并修订操作水平体系，确定服务接受方的操作水平年度目标要求，完成操作水平协议的最终发布并监督协议的执行情况等。

服务接受方负责组织收集业务部门对 IT 服务的年度目标需求，并将其转换为总体操作水平要求。

服务提供方负责制定机构内部操作水平执行计划，并组织实施。

专家评估委员会负责对生产事件进行事后评估，主要由技术架构、应用架构、开发和运维技术专家、厂商专家等组成。

2．明确操作水平体系建立与修订的内容

服务管理办公室组织签署年度操作水平协议。如有重大调整或特殊需求，由服务管理办公室牵头组织专家评估委员会对操作水平体系进行修订。

操作水平指标

1．指标设计方法

操作水平指标设计通常包括三个步骤：第一步，根据企业业务部门的 IT 服务需求，梳理出所涉及的 IT 管理流程；第二步，根据 IT 管理流程梳理出关键成功因素；第三步，根据关键成功因素设计操作水平指标。

2．常用指标

下图按照开发、测试、运维的分类，列出了 IT 操作水平协议的常见指标。

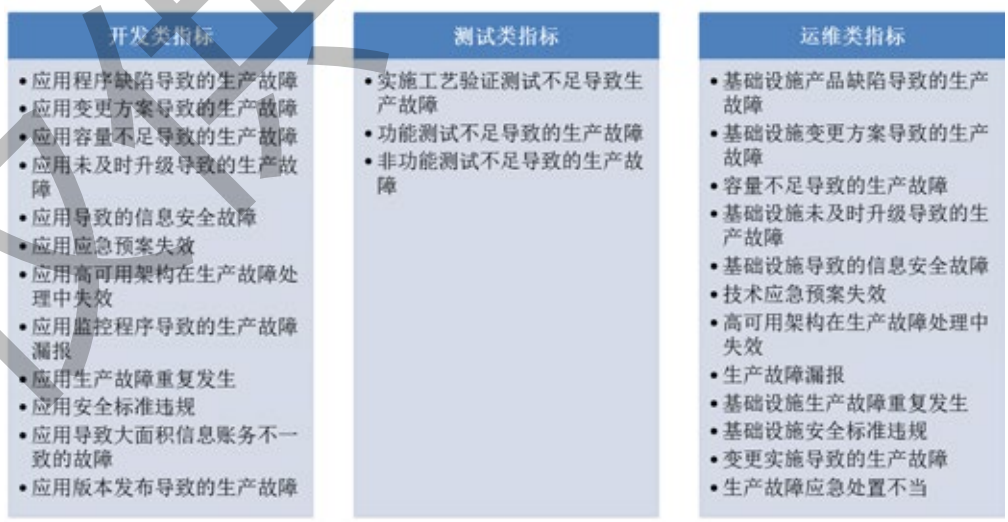

图 15 IT 操作水平协议的常见指标

操作水平评估

操作水平评估体系的总体设计思路以部门对服务目标的支撑能力为衡量目标，以部门所承载的服务内容为基准，以对安全生产造成的影响程度为尺度等几个原则进行设计。简而言之，需要考虑系统的重要性等级、部门维护的系统数量、指标重要程度以及故障严重等级等因素。

操作水平评估体系由两部分构成，评估基准设计和评估方法设计。

1．评估基准设计

首先，从系统对业务影响的重要性对系统进行分级设计，等级越高的系统，基准分值也越高。

其次，从部门层面，建立运维能力基准分值，根据其维护的系统数量及系统等级进行基准分值设计，各部门基准分值不同。

再次，从故障等级层面，以业务部门和监管机构要求为前提，明确定义行内统一的故障等级标准，不同等级故障的扣分基准分值不同。

最后，依据操作水平指标体系的设计结果，从指标违反对服务目标和安全生产的影响程度不同的角度进行设计，将指标赋予不同的权重。

2．操作水平评估算法设计

评估方法的基本设计原则为公平、公正。将操作水平指标、故障等级、责任权重构成评估的三个方面，建立评估算法。

最终每个责任单位扣分总分值相当于故障等级对应的基础分值 × 指标权重 × 责任权重。各责任单位最终评估结果为各单位的基础分值减去所扣分值。

算法综合考虑了各部门的维护能力和发生故障的风险概率，同时引入责任权重的概念避免了多责任单位事件在评估过程中有失偏颇。

操作水平报告

1．操作水平报告方式

操作水平的报告一般采取机构自评和集中测评相结合的方式进行，定期向管理层、首席风险官汇报。

机构自评由企业分支机构、开发部门、运维部门根据评估方案开展；集中测评专家评估委员会对生产事件进行回顾分析，界定责任，并根据责任扣分，同时提出制度、技术标准改进意见。

2．操作水平报告内容

操作水平报告可以按事件分析、指标分析、重点问题分析三个维度进行，事件分析又可以从产品原因、业务原因、内部原因、第三方原因等几个维度进行分析；指标分析又可以从开发指标、运维指标、测试指标三个维度展开。

6.4 整改落实

外部监管、内外部审计和内部检查评估充分发挥了监管和内部二、三道防线的作用，问题的有效整改对于企业提升 IT 治理水平、提高 IT 服务能力具有重要意义。企业应建立体系化、规范化、流程化的整改机制，避免出现问题分析不充分、整改不及时和督促不到位。

6.4.1 问题成因

事出必有因，深入分析审计问题才能对症下药，有效解决问题。通过剖析历年已发现的问题，根据不同的成因采取不同的整改方案。

主要成因分为人为因素和外部限制两类：

1．人为因素：问题是由人为因素造成的，需要进一步通过人的思想和行为来分析。思想上认识不足或存在恶意，体现在安全意识不强甚至是恶意行为等所导致；行为上可能存在风险隐患或已经导致风险，如参数配置时的误操作。

2．外部限制：主要分为技术和流程因素。在技术方面，主要体现为未通过技术手段控制或控制不足，如系统未设置双人复核；在流程方面，主要体现为控制缺失、控制不足或控制过严。

6.4.2 整改原则

> 风险导向：问题整改应以问题背后的风险为基础，确定满足风险管控策略的整改措施，实现控制成本与风险的平衡。

> 全面性：应针对问题的产生进行全面分析，从制度流程、人员意识、技术管控等多个角度提出整改措施，避免陷入“就事论事，此查彼犯”的困境。

> 长效性：应对问题进行深入分析，针对多发难点问题展开专题研究，提出长效整改措施，避免“一事一改，屡查屡犯”。

6.4.3 整改方法

以内外部检查和审计发现的 IT 问题为源头，按 IT 管控领域建立 IT 审计库，分析并制定完善制度、优化流程、改进技术等整改措施，建立问题追踪机制，确保问题整改落实到位。

1. 建立 IT 审计库

IT 审计库将问题整改和分析融为一体，不仅可跟踪检查发现问题的整改情况，也可作为全面评估和专项评估的输入，还可重点分析问题集中的领域，形成多发问题热点地图，突出管理重点。

IT 审计库由 IT 审计检查清单和 IT 审计检查跟踪库两部分组成。IT 审计检查清单用于登记 IT 相关的审计检查报告，主要包含文号、审计检查任务下达单位、执行单位、审计检查对象、审计检查范围等。IT 审计检查跟踪库用于记录问题、分析问题，跟踪整改计划措施和整改进度，通常包括问题描述、标签词条、所属机构（责任部门）、成因分析、整改措施、整改计划、整改进度等。其中，标签词条与 IT 管控领域相对应，便于问题的归纳分析，帮助企业依据内部管控领域定位整改重点。

2．建立问题跟踪机制

充分运用 IT 审计库，对企业历年审计检查问题进行集中管控，明确整改责任人、整改措施，做好更新维护，定期督促，确保及时完成整改。具体地说，就是从及时录入问题、分析问题成因、明确整改责任、定期状态追踪、实施监督考核等方面建立问题跟踪机制。

3．强化风险管控

运用IT审计库，从企业内部管控领域、风险源、作用方式、保护对象、造成的影响等方面进行分析，形成直观的审计检查风险地图，针对风险项采取针对性、多形式的管控措施。

建立问责机制：根据问题性质，对责任方进行追究，落实分级惩罚措施，强化人员风险意识和责任意识，从源头上解决问题。

开展专项问题研究：组建虚拟专家团队或选定辖内分支机构承担专项问题研究，针对高发和严重问题研究长效解决措施，提出针对性整改方案。

完善控制措施：加强制度重检、优化管理流程，以制度形式固化整改成效；加强机控，减少人为管控，达到长效整改目的。

整改经验交流：定期审核并发布 IT 风险管理重点工作举措，促进企业内部知识共享；定期提炼并汇编实践效果较好的高发问题整改经验，组织专题会议或培训开展交流，促进企业整体风险整改能力的提高。

建立风险通报机制：加强日常风险指标监测，研判风险趋势，定期通报监测结果；对专项审计检查报告进行分析并通报；针对热点风险发布风险提示；定期对监管动态、业界动态、信息安全热点事件等进行监测，发布 IT 风险事件及管理动态监测周报。

提升员工意识：通过开展现场、远程在线培训、竞赛等多种形式，提高员工知识水平和风险管控意识，督促员工自觉整改。

6.5 小结

在监管传导方面，编制了 IT 监管制度导读和 IT 监管报告指南，建立了国内 IT 监管库、海外 IT 监管库及业界 IT 风险标准库。通过 IT 监管数据库的建立，企业可及时分析监管机构的监管重点，帮助不同领域的团队筛选出其涉及或关注的监管制度原文，调整科技政策并加以落实，提升执行监管要求的水平和学习业界标准的能力。通过制定覆盖全面的检查提纲，实施检查，督促落实制度要求，纠正不合规问题，发现制度偏差并及时更新修订。通过制定考核机制，指引企业 IT 发展方向，推动企业 IT 工作的落实和目标的达成。通过对问题的深入分析、建立 IT 审计库和问题跟踪机制，有效落实问题整改，强化问责机制，组织整改经验交流，引导企业培养合规文化，全方位提升员工合规知识水平和风险管控意识。

附录 1 与 COBIT5 映射关系

最佳实践	COBIT5
2.1.1--- 董事会	EDM01、APO01.01
2.1.2--- 监事会	EDM01、APO01.01
2.1.3--- 高管层	EDM01、APO01.01
2.2.1--- 执行机构设置	EDM01、APO01.02
2.2.2---IT 风险三道防线	EDM01、APO11.01
2.2.3--- 沟通汇报机制	EDM05、APO08.04
2.3.1---IT 架构管控团队	EDM04、APO01.01、APO01.02
2.3.2--- 新技术研究团队	EDM04、APO01.01、APO01.02
2.3.3--- 信息安全团队	EDM04、APO01.01、APO01.02
2.3.4--- 反欺诈团队	EDM04、APO01.01、APO01.02
2.3.5--- 合规培训团队	EDM04、APO01.01、APO01.02
2.4.1--- 培训知识体系	EDM04、APO07.03
2.4.2--- 培训教育机制	EDM04、APO07.03
3.1.1--- 制度层级	EDM01、APO01.03、APO01.08
3.1.2--- 框架构建	EDM01、APO01.03、APO01.08
3.2--- 制度流程	EDM01、APO01.03、APO01.07
3.3--- 制度优化	EDM01、APO01.03、APO01.07
4.1--- 架构定义	EDM04、APO03.02
4.2--- 架构原则	EDM04、APO03.02
4.3--- 架构设计	EDM04、APO03.02
4.2--- 模型管理	EDM04、BAI01.09
5.1.1--- 数据架构定义	EDM04、BAI03.01
5.1.2--- 数据架构原则	EDM04、BAI03.01
5.1.3--- 数据架构设计	EDM04、BAI03.02
5.2.1--- 应用架构定义	EDM04、BAI03.01
5.2.2--- 应用架构原则	EDM04、BAI03.01
5.2.3--- 应用架构设计	EDM04、BAI03.02
5.3.1--- 技术架构定义	EDM04、BAI03.01
5.3.2--- 技术架构原则	EDM04、BAI03.01
5.3.3--- 技术架构设计	EDM04、BAI03.02
5.4.1--- 安全架构定义	EDM04、BAI03.01

5.4.2--- 安全架构原则	EDM04、BAI03.01
5.4.3--- 安全架构设计	EDM04、BAI03.05
6.1.1--- 监管要求和标准传导	EDM01、EDM05、APO01.03
6.1.2--- 持续跟踪	EDM03、APO01.03、APO01.08
6.2.1--- 检查范围及内容	EDM03、MEA02.01、MEA03.03、MEA02.03
6.2.2--- 检查计划	EDM03、APO12.02、MEA02.03
6.2.3--- 检查实施	EDM03、MEA02.04、MEA03.03
6.3.1---IT 考核机制	EDM02、APO01.08、MEA01.01、MEA01.03
6.3.2---IT 操作水平	EDM02、APO11.01、APO11.02、APO11.04
APO07.04、MEA01.01、MEA01.03	
6.4.1--- 问题成因	EDM03、APO12.02、MEA03.04
6.4.2--- 整改原则	EDM03、APO12.06、MEA03.04
6.4.3--- 整改方法	EDM03、APO12.06、MEA03.04

附录 2 词汇表

名词	解释
CPC	是 Customer、Product、Channel 的首字母缩写，即客户、产品、渠道。
SOA	是 Service-Oriented Architecture 的缩写，即面向服务的架构。
安全即服务（SECaaS）	安全即服务是安全架构的设计理念，即由服务接入层、应用安全服务层、基础设施安全服务层和安全策略管理中心组成全新的“安全架构”。
操作水平	指采用正式的、定量的方式明确开发部门、运维部门及分支机构支撑业务需求的内部服务能力。
国内 IT 监管库	指通过梳理国内 IT 监管要求，形成的包括监管制度、具体的监管要求、涉及的企业业务阶段、涉及的企业业务部门、涉及的企业业务领域等要素在内的 IT 监管库。
海外 IT 监管库	指通过梳理海外 IT 监管要求，形成的包括控制领域、监管制度、具体的监管要求、涉及的企业业务阶段、涉及的企业业务部门、涉及的企业业务领域等要素在内的 IT 监管库。
价值链	指以企业内部价值活动为核心所形成的价值体系，分为基本活动和支持活动两类，基本活动包含：生产、营销、运输和售后服务等，支持活动包含：物料供应、技术、人力资源或支持其他生产管理活动的基础功能等。
七层应用架构	七层架构实现了渠道与流程，应用与数据，产品操作型和管理分析型处理的分离；通过各平台能力和平台间协同，可以支持卓越的客户体验、面向客户的集成服务、快速产品部署、高质量的数据服务和优化的企业级管理能力
三道防线	为防范内部风险设置的内部制衡与监督机制，通常业务部门和职能部门是风险管理的第一道防线，具有风险管理职责的部门是风险管理的第二道防线，审计部门是风险管理的第三道防线。
十二个应用平台	十二个应用平台覆盖七层应用架构，所有应用都部署在这十二个应用平台之上，企业 IT 系统都基于这十二个统一、标准的平台上进行开发，并且通过组件的共享，达到灵活响应和快速创新。
五级流程建模	五级流程建模是构建企业级业务架构的方法。五级流程建模对流程层级的颗粒度主要包括以下： 1 级——企业级价值链或主题领域 2 级——在业务领域的价值链 3 级——活动 4 级——任务 5 级——操作步骤
业界 IT 风险标准库	是指通过整理业界 IT 风险管理标准、最佳实践，形成的包括控制领域、管控要求、标准名称、对应条款编号、涉及的企业业务部门等要素在内的标准库。

鸣谢

开发团队

金磐石，CISA，中国建设银行，中国
庄玉良，CISA，南京审计大学，中国
杨　军，CISA，中国建设银行，中国
郭汉利，中国建设银行，中国
林磊明，中国建设银行，中国
王立新，中国建设银行，中国
曹文中，CISA，中国建设银行，中国
张　辉，CISA，中国建设银行，中国
邱　斌，CISA，中国建设银行，中国
余小兵，CISA，南京审计大学，中国
李家伟，CISA，中国建设银行，中国
陈　成，CISA，中国建设银行，中国
吴　静，CISA，中国建设银行，中国
李庭燎，CISA，南京审计大学，中国
郭红建，CISA，南京审计大学，中国

参与研讨人员

韦有华，中国建设银行，中国
张晓东，中国建设银行，中国
刘爱辉，中国建设银行，中国
刘瑞胜，中国建设银行，中国
陈　铭，CISA，中国建设银行，中国
孙春霞，CISA，中国建设银行，中国
杨宝辉，CISA，中国建设银行，中国
顾呈页，CISA，中国建设银行，中国
汤　阳，CISA，中国建设银行，中国
尹丹娜，CISA，中国建设银行，中国
王三九，CISA，中国建设银行，中国
黄烨华，CISA，中国建设银行，中国

刘宝忠，CISA，中国建设银行，中国
唐艳萍，CISA，中国建设银行，中国
郭卫军，中国建设银行，中国
陈一心，中国建设银行，中国
包航宇，中国建设银行，中国

专家审核人员

杨　**竑**，中国人民银行，中国
单继进，中国银行业监督管理委员会，中国
王　忠，中华人民共和国审计署，中国
华　宁，电气电子工程师学会（IEEE）亚洲区，中国
兰　瑜，CISA，安永华明会计事务所，中国

专家评审

刘涤西，CISA，全国海关信息中心，中国
彭劲松，CISA，中国化工集团，中国
冼嘉乐，CISA，普华永道会计师事务所，中国
陈　伟，CISA，北京谷安天下科技有限公司，中国

《IT治理最佳实践》是ISACA的COBIT框架与中国企业IT治理最佳实践相结合的良好典范，也是中国建设银行历时六年、参考借鉴COBIT标准着力打造的新一代系统顺利上线的经验总结（中国建设银行的《核心系统建设工程》2018年9月获中国银监会银行科技发展项目特等奖）。

《IT治理最佳实践》为中国企业在数字经济时代构建良好的IT治理机制提供了科学的、可借鉴的指导方法，同时对ISACA的知识库进一步完善和在中国的落地做出了重要贡献。

——陈伟，CISA，COBIT、ITIL认证培训讲师，北京谷安天下科技有限公司副总经理、首席咨询顾问

“看了首两章，就忍不住一直看下去。书中所述的IT治理与一般的IT治理书籍所述的不一样，非常有实践的借鉴。整部书的架构也非常简洁及有条理，还包括科技合规的实践，这是企业目前面对的重大挑战之一，尤其是走出去的企业。”

——冼嘉乐，CISA，CRISC，CISP，普华永道合伙人、网络安全与隐私保护服务

ISACA在信息及相关技术控制目标（COBIT）中提出IT治理的概念、原则和标准，并不断发展完善。《IT治理最佳实践》是中国建设银行与南京审计大学团队IT治理理论应用与实践探索的共同成果，是企业构建IT治理框架、提高IT治理水平的生动体现和系统反映，立意新颖，理念先进，逻辑严密，内涵丰富，极具推广价值。

——庄玉良，南京审计大学商学院院长

今天中国的信息化建设在百花齐放、锐意创新的奔跑中，还需要科学的指引。ISACA与中国建设银行合作推出的《IT治理最佳实践》或许对致力于数字化转型的企业能够有所启发。

——彭劲松，CISA，原中国化工集团CIO

总是从不同渠道听闻建行科技之强，后有幸结识金先生，就近聆听“新一代系统”之成就和问题，受益良多。自己做IT三十年，提前拜读此书，会更多一份珍惜与感动。在此，愿把此书推荐给同学们，更好地理解所学之价值及社会之发展；愿把此书推荐给各行业之同行，它山之石可以攻玉，创新发展共同进步；愿把此书推荐给IT企业，有助于理解用户之口味，提升自身服务之品位；也希望专家们能看到，总结行业实践经验，增强标准推广信心。此前，专委会委员们也都珍藏了一本，感谢建行同仁的创造与分享。

———刘涤西，全国海关信息中心

ISACA中国
电子邮箱：isacachina@isaca.org
办公地址：北京朝阳区东三环中路20号乐成中心B座5层505室