CAICT 中国信通院

企业数字化治理应用发展报告

（2021 年）

中国信息通信研究院云计算与大数据研究所

2021 年 7 月

版权声明

编制说明

本报告的编写得到如下企业的支持，在此一并感谢（排名不分先后）：

阿里云计算有限公司、蚂蚁科技集团股份有限公司、北京奇虎科技有限公司、北京百度网讯科技有限公司、中国联通软件研究院、美团商企通、北京字节跳动科技有限公司、360 政企安全集团、度小满科技（北京）有限公司、小米科技有限责任公司、华为技术有限公司、中国移动江苏公司、中移（杭州）信息技术有限公司、中国移动通信集团内蒙古有限公司、贝壳找房（北京）科技有限公司、北京谷安天下科技有限公司、大家保险集团有限责任公司、大家信科有限责任公司、西安恩耐博人工智能科技有限公司、中冶宝钢技术服务有限公司、上海宝信软件股份有限公司、上海速擎软件有限公司、上海精鲲计算机科技有限公司、东华软件股份公司。

前　言

数字经济时代，科技革命和产业变革日新月异，深刻改变着社会生产生活方式和社会治理体系。企业作为社会治理体系中重要的一环，在数字经济时代加速数字化转型的过程中，同时面临着严峻的治理挑战。当前，企业数字化转型使得企业治理环境和治理对象数字化，治理活动也需要走向数字化，建立数字化治理机制，受到企业管理者的关注。越来越多的企业决策者认为运用技术手段对组织内部人员、组织、业务、流程、基础设施、数字资产等各要素实施科学管控，才能保障企业数字化转型的成功。

本报告第一章基于对企业数字化治理机制和实践的梳理，提出了包含治理目标、数字化治理战略、数字化治理机制、数字化治理应用、数字化治理对象等层面的企业数字化治理的体系。**在此体系框架的基础上，**根据各治理领域的成熟度和企业关注程度，有针对性的对企业数字化运营、新技术治理、智能安全与隐私合规、法律科技、数字化风控、数字化审计等企业数字化治理应用的关键领域展开研究。**第二章**分别从各关键领域产生背景、最新理念和最佳实践入手，以技管结合为主线总结归纳典型应用现状和典型特征。**第三章**详细分析了各关键领域发展过程中的关键问题、重难点问题，并针对性提出实施建议。**第四章**从多元共治的角度提出企业数字化治理应用发展建议。**附录中**针对各领域数字化治理行业优秀实践进行了筛选和归纳，提炼案例核心特色和价值，以期望对企业开展数字化治理提供有效参考。

目 录

图 目 录

表 目 录

一、数字化治理助力企业数字化转型

2021 年是“十四五”开局之年，也是数字化转型关键年。数字经济势不可挡，成为中国崛起、弯道超车的重大机遇，也是企业提升效率的必由之路。然而，企业在享受数字化带来红利的同时，挑战也随之而来，加强数字化治理迫在眉睫。

（一）企业数字化治理和数字化转型的关系

“十四五”期间是我国企业数字化转型的关键时期，转型期企业在进行组织赋能模式创新和业务突破的同时，也必然会在数字化战略规划、管控模式、业务融合、安全隐私等方面遇到新的挑战。企业需要进行有效的数字化治理来应对一系列数字化新风险。

数字化转型的核心是新基础设施的建设和新业务模式以及与之匹配新生态体系的建设。数字化治理是对数字化转型过程中的安全、隐私保护等核心风险的管控，以及整体组织形态、运营管理模式的优化调整，是对数字化转型过程中生产关系的重塑，兼顾风险防范和效能提升。

数字化转型和数字化治理协调一致，保障了企业数字化转型健康发展，驱动了企业数字化转型价值最大化。

（二）数字化治理概念内涵

中国信息通信研究院 2021 年 4 月发布的《中国数字经济发展白皮书》提出数字经济的“四化”框架，包括数字产业化、产业数字化、数字化治理、数据价值化。其中**数字化治理**包括但不限于多元治理，以**“数字技术+治理”为典型特征的技管结合**[1]，以及数字化公共服

务等。该观点从宏观视角阐述了数字化治理的典型特征和范围。

国务院国有资产监督管理委员会在其数字化转型知识方法系列专栏文章中对数字化治理进行了微观角度的阐释，文章认为**数字化治理指建立与数字化转型下的新型能力建设、运行和优化相匹配的数字化治理机制，应用架构方法，推动人、财、物，以及数据、技术、流程、组织等资源、要素和活动的统筹协调、协同创新和持续改进，强化安全可控技术应用以及安全可控、信息安全等管理机制的建设与持续改进等内容**[2]，主要包括：

- **数字化治理机制**，包括为实现四要素协同、创新管理和动态优化建立的标准规范和治理机制等内容；
- **数字化领导力**，包括高层领导者对数字化转型敏锐战略洞察和前瞻布局，以及由一把手、决策层成员、其他各级领导、生态合作伙伴领导等共同形成的协同领导和协调机制等；
- **数字化人才**，包括全员数字化理念和技能培养，数字化人才绩效考核和成长激励制度，以及跨组织（企业）人才共享和流动机制等；
- **数字化资金**，包括围绕新型能力建设等数字化资金投入的统筹协调利用、全局优化调整、动态协同管理和量化精准核算等机制；
- **安全可控**，包括自主可控技术研发、应用与平台化部署，网络安全、系统安全、数据安全等信息安全技术手段应用，以及安全可控、信息安全等相关管理机制的建立等。

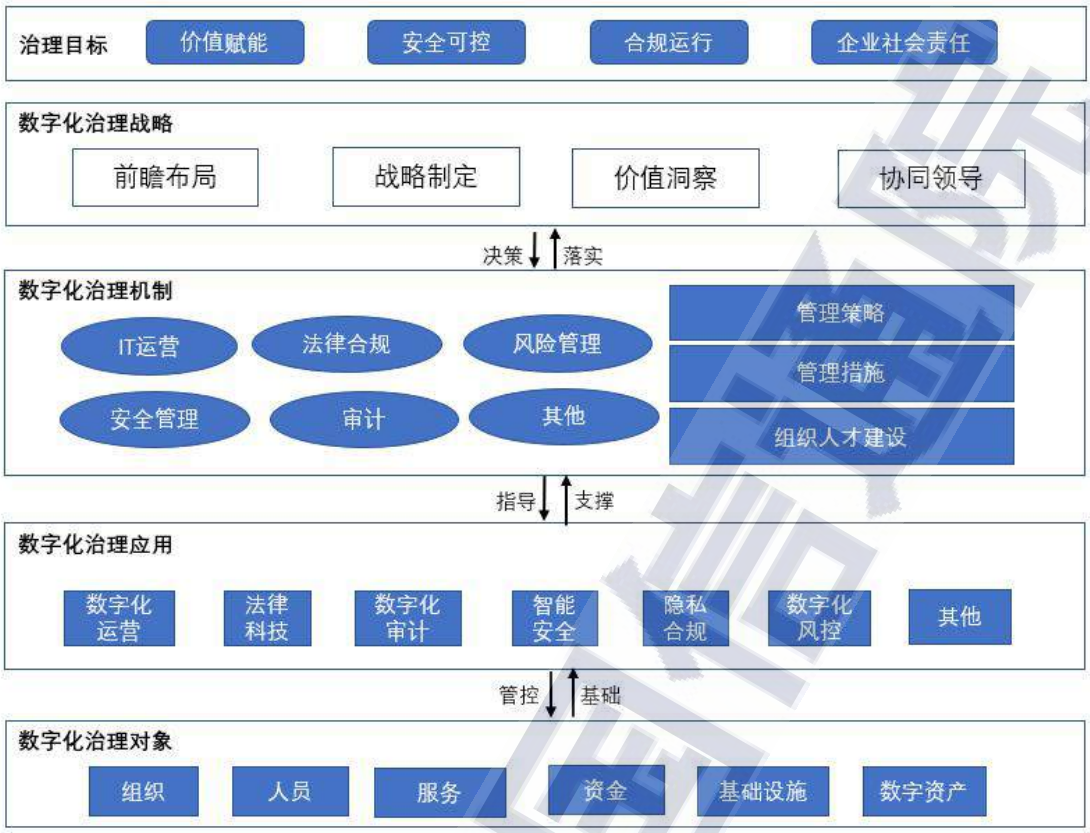
本报告以企业视角展开数字化治理应用发展研究，结合上述宏观和微观角度的数字化治理涵义，本报告认为**企业数字化治理的本质是企业治理活动的数字化和对数字化对象的治理。**

治理活动的数字化方面，数字化转型对企业传统治理体系进行了数字化重塑，各领域治理流程和活动均经历显著数字化转变，如 IT 运营、安全管理、风险管理、审计、法律合规等领域。

治理对象数字化方面，随着数据的生产要素属性增强以及人工智能、区块链、云计算等技术对生产力和生产关系的加速调整，全球对于数据和新技术的治理愈发密集。对于企业来说，不仅仅要治理技术本身，还需要治理技术产生的外部性，数据及新兴技术等数字资产已成为企业稳定持续经营不可忽视的治理对象。

（三）企业数字化治理体系

基于对企业数字化治理机制和实践的梳理研究以及与相关领域行业专家的大量讨论和交流，我们提出如下企业数字化治理框架供业界参考及共同完善。



来源：中国信息通信研究院

图 1 企业数字化治理框架

我们认为，企业数字化治理体系是以价值赋能、安全可控、合规运行、企业社会责任为**治理目标**，以人员、组织、业务、流程、基础设施、数字资产为**治理对象**，自上向下通过**数字化治理战略、数字化治理机制、数字化治理应用**来构建。具体为：**数字化治理战略，**企业数字化治理战略需要企业管理者对数字化转型中企业应具备的数字化治理能力进行敏锐洞察和前瞻布局，以及由一把手、决策层成员、其他各级领导、生态合作伙伴领导等共同形成协同领导和协调机制。**数字化治理机制，**是针对价值管理、IT 运营、合规管理、安全及风险管理、组织人员管理等核心领域建立的标准规范和管理措施。**数字化治理应用**是支撑数字化治理机制有效运行的数字化手段，关键应用

领域包括：数字化运营、法律科技、数字化审计、智能安全与隐私合规、数字化风控等。

习近平总书记指出“要运用大数据提升国家治理现代化水平”，“要建立健全大数据辅助科学决策和社会治理的机制，推进政府管理和社会治理模式创新”。这些重要论断为提高社会治理体系和治理能力现代化水平提供科学的技术赋能路径。同理，企业治理体系和能力现代化的实现离不开**数字化治理应用，数字化治理应用是实现企业数字化治理建设的重要保障**。本报告重点对企业数字化治理应用的关键领域进行研究，从关键领域的应用现状、应用痛点及实施建议三方面进行梳理、分析、归纳总结，为企业数字化治理应用的有效落地提供参考。

二、企业数字化治理应用关键领域现状分析

根据行业调研情况及案例研究过程中企业的关注程度和各数字化治理领域的成熟度，现阶段企业数字化治理应用的关键领域包括企业数字化运营、新技术治理、智能安全与隐私合规、法律科技、数字化风控、数字化审计。本章将从各关键领域产生背景、最新理念和最佳实践入手，以技管结合为主线总结归纳典型应用现状，希望对各行业企业开展数字化治理有所启发和帮助。

（一）数字化运营

企业在推进数字化转型的过程中，需要 IT 团队支撑业务系统、技术平台、基础设施的规划、设计、实施、运维和管理。企业数字化运营是数字经济时代企业研发运维管理的转型升级。它有两大核心特

点，一是研发、运维与业务的高度融合，二是价值赋能。企业数字化运营的主要模式有业务研发运营一体化（BizDevOps）、智能化运维（AIOps）和工作流自动化等。

1.BizDevOps 覆盖业务侧，实现端到端的价值闭环管理

随着用户需求的日益增长、对产品交付的快速响应、快速实现、高质量的要求，以及来自团队内部的压力和数字化转型的迫切需求，业务需求和技术创新并行驱动软件开发模式发生巨大变革，企业引入研发运营一体化（DevOps）打破了传统研发和运维之间的隔阂，缩短产品研发周期，加速产品交付效率，提升产品交付质量，以适应飞速发展的客户需求和市场变化。

在此基础上，BizDevOps 覆盖了业务、开发、测试、运维的业务全生命周期，与 DevOps 相比，更关注整体商业价值的实现，从业务部门原始需求到 IT 开发实现和持续运维，通过运营数据反馈到业务部门进行改进优化，从而形成针对业务商业价值的生命周期闭环管理，实现业务与 IT 的对齐。BizDevOps 能够弥补 DevOps 被动式响应及价值呈现单薄、业务关联度低等的不足，打通 IT 与业务端，并围绕业务商业价值驱动，构筑企业数字化治理的核心竞争力。

2.大数据、AI 等新技术驱动企业运维智能化（AIOps）

企业正在面临 IT 规模增长、系统复杂度提高、迭代速度加快等情况，传统运维难以支撑 IT 业务的快速发展。通过对海量数据的积累，结合云计算、人工智能、大数据等技术的成熟应用，AIOps **成为必然趋势**。根据 2021 年 Gartner 预测，从 2020 年到 2025 年 AIOps

市场规模的复合年增长率将达到 15%[3]。

当前，互联网、金融、通信等行业已积极探索 AIOps 应用场景实践，以解决在故障处理、变更管理、容量管理等过程中，由于按人员经验进行处理、决策而阻碍运维质量、效率的问题。通过对智能运维的探索应用，可以有效降低运维难度，使传统运维人员专注自身的业务逻辑，提高开发和迭代效率，并且充分发挥人工智能领域的技术成果，使得机器能够辅助/代替人作出决策，提高决策反应速度与质量。

3.工作流自动化创造数字化转型增量价值

数字化时代要求企业打破屏障，在信息化系统之间形成有机衔接。工作流自动化通过对各种 IT 能力的封装和串联，快速构建流程化业务的能力，并将业务进行自动化处理。工作流自动化能力主要从**价值链网络化、协同能力整合和技术能力维度**三方面构建。价值链网络化是指“价值链”开始向“价值网络”转变，它可以使企业更加灵活、动态地、自组织式的生产和提供服务，通过与合作伙伴和客户的协作实现价值共创。协同能力整合是指企业在面对市场的不确定性时，通过数字化业务流程平台快速整合后台资源，快速交付价值，并持续改进。技术能力维度主要围绕在线化、编排化、自动化以及智能化等能力的建设。通过自动化、智能化技术的引入，可以使员工从事更高价值的工作，显著提升工作效率。

（二）新技术治理

随着人工智能、区块链、大数据、云计算等技术在企业不断应用，

企业对于新技术的治理需求也越来越强烈。本报告选取当前发展较成熟的云治理以及企业广泛关注的人工智能模型管理作为研究对象，分析其代表应用和核心特点。

1.云治理确保企业云采用质效合一

国务院发展研究中心国际技术经济研究所《中国云计算产业发展与应用白皮书》预测到2023年中国云计算产业规模将超过3000亿元，政府和企业上云率将超过60%，云计算市场稳定增长[4]。企业上云过程中和上云后，为了确保整个云环境能够始终保持安全和稳定地运行，云治理同样不可或缺。

在支持企业向云上迁移及企业业务转型创新的过程中，云开创了全新的模式，而这些新模式也会改变治理方式。企业上云过程中需要解决上云策略、上云准备、持续治理等阶段的工作，完成传统IT治理向云治理的转变。当前，诸如阿里云、AWS、Azure等众多云服务提供商均提出各自的**云采用框架（Cloud Adoption Framework），辅以丰富的技术工具，指导企业快捷、安全、稳定、低成本成功上云并确保上云后整个云环境能够始终保持安全和稳定运行。**

企业在上云前，需要有**一整套顶层设计**和**一系列基础框架**，否则可能导致后续上云面临成本、网络、安全、效率等多方面问题。业界通常称这些基础框架为Landing Zone，企业实践中典型的Landing Zone包括商业关系、访问控制、成本管理、网络规划、资源结构、持续治理、自动化等模块。

表 1 典型 Landing Zone 模块

Landing Zone 模块	描述
商业关系管理	管理和云平台的合同、优惠、付款关系、账单，以及认证公司在云平台的实体、发票抬头等财务相关的属性。
网络规划	规划云上 VPC 的拓扑结构、混合云网络的互联、网络的流量走向、相关的安全措施，以及如何构建高可用和可扩展的网络架构。
资源规划	规划云上账号及其组织结构。根据公司的运维模式，定义所需要的管控关系。
身份权限	规划谁能够访问云，并通过单点登录 SSO 和细粒度授权实现人员按需访问。
安全防护	通过在云上构建基础的安全环境，帮助业务系统在云上快速的安全落地。
成本管理	通过标签、账单让公司在云上的成本做到可见、透明，并通过预算、规则等方式控制和优化云上成本。
持续治理框架	设计治理的目标和流程，并通过相应的工具来实现对于治理规则的监督。
自动化	定义自动化场景和目标，并通过相应的工具实现自动化。常见的场景如 Landing Zone 自身的搭建以及 CI/CD 流水线的自动化。

来源：阿里云

Landing Zone 以风险为导向，覆盖了企业在云采用过程中不同阶段面临的不同风险，也对应不同的治理要求，主要风险有：

● **安全风险：**由于云环境安全漏洞被威胁利用导致的风险，如 DDoS、不安全 API 接口、跨租户攻击、网络访问控制失效等。

● **业务风险：**一切可能对业务收益造成损失的潜在问题，比如数据泄露、服务中断、成本溢出、合同履约风险等。

● **合规风险：**因无法获得第三方合规机构的资质认证以及无法实现隐私保护、网络安全、数据跨境等方面的合规要求，导致企业无法与合作伙伴完成商务合同，或面临合规处罚的风险。

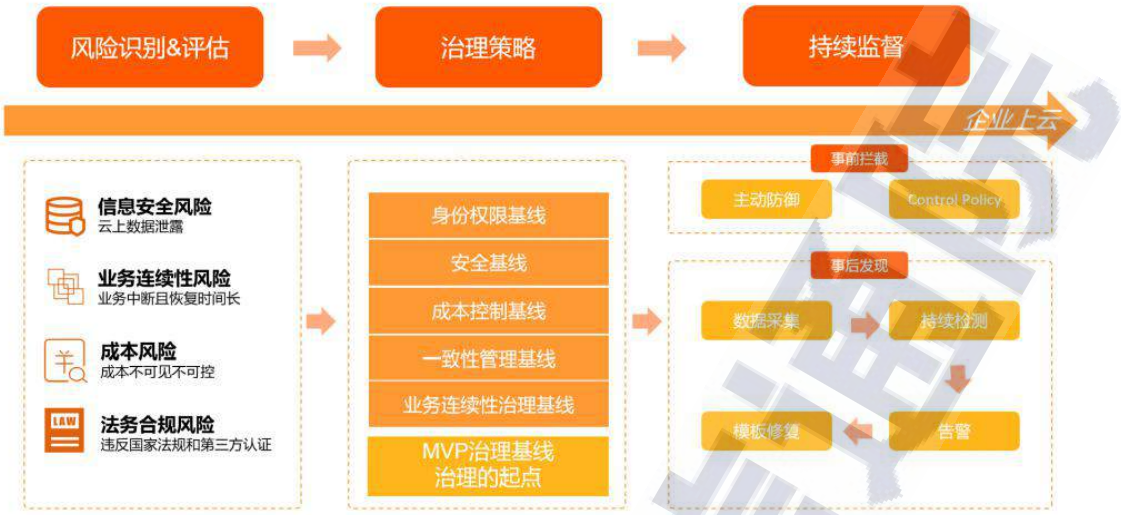
● **流程风险：**因企业内部管理流程的缺失，使管理决策和管理基线难以被强制执行和实时监督。

通过对比国内外领先云服务商提供的云采用框架中对于治理的内容和调研企业实际云采用过程中的实践，我们归纳出：对于各个阶段的风险，企业通过执行风险识别&评估、治理策略、持续监督等一系列治理活动实现云采用质效合一。

● **风险识别与评估：**充分考察企业在每个阶段面临的潜在风险，并通过量化风险可能造成的损失来评定风险等级，针对不同的风险等级制定不同程度的治理决策。

● **治理策略：**将治理决策转化为治理策略，治理策略是可被系统化实现的技术规则。

● **持续监督：**治理策略自动部署及实施后，需要使用技术手段持续对云上行为进行事前拦截、事中监测、事后审计的持续监督和改进。

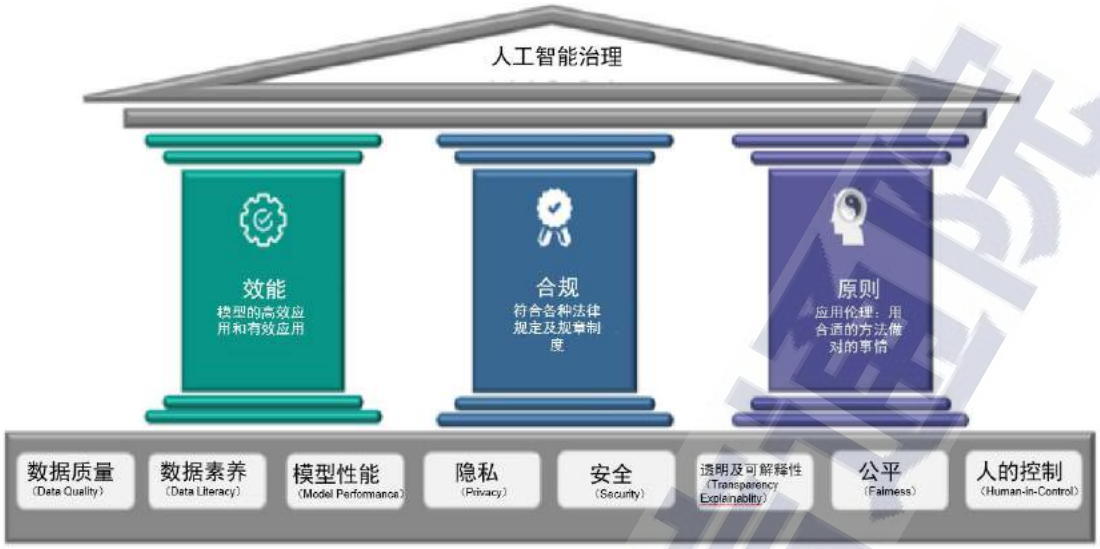


来源：阿里云&中国信息通信研究院

图 2 云治理路径

2.人工智能模型开发应用一体化盘活模型资产价值

随着人工智能技术的广泛应用，企业逐步在效能、安全、风险管理、审计等方面开始重视并逐步开展人工智能治理。2020 年 4 月 30 日，上海市科学研究所发布《全球人工智能治理年度观察 2019》英文版（AI GOVERNANCE IN 2019: A YEAR IN REVIEW OBSERVATIONS OF 50 GLOBAL EXPERTS）人工智能治理报告，报告基于 2019 年全球人工智能治理总体形势，从不同层面和角度提出全球人工智能治理的趋势观点。其中涉及企业视角对于人工治理的观点为：**人工智能治理手段逐渐市场化，企业成为越来越重要的治理主体。**



来源：公开资料整理

图 3 企业人工智能治理参考框架

企业在进行人工智能治理时可以从数据质量、数据素养、模型性能、隐私、安全、透明及可解释性、公平、人的控制等方面入手，实现效能、合规、应用原则等三个治理目标。**人工智能的治理是需要逐步实施的工程。**当前，**在效能方面，部分企业已使用数字化、一体化解决方案实现 AI 模型的全生命周期管理，达成对模型的高效构建和有效应用。**

模型的全生命周期管理通过平台集成一系列的工具、接口，实现对**建模数据探索**（多数据源和数据格式）、**模型构建**（包括自动化构建、交互式构建、图形化构建等）、**模型部署**（包括云部署、大数据环境中的部署、批量部署、一键部署等）、**模型监控**（包括模型性能、模型业务价值的实时监控）、**模型更新**（包括自动化更新、自动化重建等）的统一管理，其中**模型监控是企业当前模型平台建设的重点。**自动化的模型数据探索、模型构建、模型部署提高了模型质量、建模

效率，**有效降低了模型的开发成本**。此外，通过一体化管理，**模型构建的知识体系化地沉淀于平台**，实现知识积累和传递。更重要的是，**模型投入应用后**，通过对**模型性能和业务使用价值的监控**，实现**模型的价值可视化**，有效赋能业务发展。

（三）智能安全与隐私合规

1.新一代安全运营中心(Security Operations Center)促进网络安全走向主动式和智能化

传统的网络安全架构仅限于被动式防御，根据安全管理人员配置的安全规则进行被动式防御，但是安全事件是动态的，攻击技术及手段总是在不断的更新和变化，新的攻击手段、漏洞信息等层出不尽，企业安全体系必须切换到主动式、智能化模式。

当前，越来越多的企业正在解构其被动式的传统网络安全防御体系，通过调整资源、技术、管理、运营等手段向主动式的网络安全治理体系转变。**从传统根据紧急安全事件、监管要求、业务需求等进行被动防御的模式转向主动式 SOC 建设。**企业新一代 SOC 呈现**安全与业务目标融合、安全一体化运营、智能化海量数据分析、实战检验**等特征，**实现了技术、流程和人的有机结合。**随着安全态势感知平台的兴起，安全运营中心以态势感知平台作为智能安全运营的载体，融入终端监测响应、机器学习、东西向流量采集技术、大数据技术等，在风险监测、分析研判、通知协作、响应处置、溯源取证等各方面进行增强。

新一代 SOC 智能化方面，物联网的普及和联网设备的数量不断

增加、网络威胁实例不断增的网络安全现状下，新的攻击面和攻击矢量往往超出传统安全防御体系的感知范围、处理能力和响应速度。运用 AI 技术，特别是深度学习技术智能化解决安全问题成为业界热门的研究方向，在学术界也沉淀了不少研究成果。

新一代 SOC 建设可从安全架构设计、安全运营、安全专家团队、安全大数据平台、安全基础设施等方面入手逐步完善，大致包括如下几个部分：

- **自适应安全架构：**新一代 SOC 应以持续监控和分析为核心，覆盖防御、检测、响应、预测四个维度，可自适应于不同基础架构和业务变化，并能形成统一安全策略应对未来更加隐蔽、专业的高级攻击。

- **安全运营：**安全运营除注重安全系统工程的规划与落地，以及微观基础设施的攻防理念策略、管理制度流程、安全技能使用、事件响应预案外，还应通过实战机制来检验域内安全能力体系是否依然健壮可靠。在已有系统常规运转过程中，新系统上线、重大安保事件之前，利用实网攻防、众包众测手段、安全监理等手段进行常态化安全检验机制。通过实战检验机制动态发现已建成安全体系的脆弱性，持续提升自身的安全能力成熟度。

- **构建立体安全治理团队：**安全治理团队由安全攻防人员、算法开发、大数据开发人员组成，组成集安全业务理解、数据角度洞悉问题、算法角度摸索探查的人员矩阵。

- **完善的切面数据体系：**能够在系统、应用的各个位置、节点、

通道以及动作行为环节获取充分的业务、运行甚至供应链链路关键信息，且可以和已知的资产、情报、风险信息形成有效关联。

● **支持大数据规模的计算平台：**应对安全相关的大规模数据量，需要有相应的计算平台进行稳定支撑。

● **机器智能和专家智能的有效结合：**企业网络安全治理涉及到的因素繁多，包括安全与业务的关系、成本与效率的考量等等，因此在整个体系中既需要有机器智能提升效率，又需要专家智能深度分析、综合决策。

2.隐私合规一站式平台实现隐私保护融入研发运营(DevPrivacyOps)治理闭环

为了保障公民的个人信息与隐私安全，全球掀起了个人信息和隐私法规的立法热潮。联合国贸易和发展会议官网(UNCTD)调查显示，截至 2020 年 12 月，全球受调查的 194 个国家中已有 128 个国家立法保护数据安全和个人隐私[5]。实践中，数据安全和个人隐私保护存在本质区别，**数据安全合规侧重数据种类的管理**，而**个人隐私保护由于数据主体（用户）一系列特殊的权利，如可携带权、被遗忘权等**，工作重心在于对每一位个人用户的个人数据进行管理。企业要在海量个人数据中为每一位用户提供“定制化”的隐私相关的服务，则必须**依赖自动化的解决方案才能有效完成隐私保护工作**。

Gartner 发布的 2020 年九大安全和风险趋势提出隐私正在成为一门独立的学科[6]，其不再仅是 IT、法务或者审计的一部分，需要各部门紧密合作才能将隐私保护整合到企业治理体系中。

企业隐私合规一站式管理平台成为企业在数字时代探索隐私合规的有效路径之一，其将技术部门与法律团队集合在一起，可以显著提高企业隐私合规的能力。一站式管理平台使用 AI 技术、机器人和可视化工具，在一个平台上提供了隐私合规相关各个环节的实时展示，包括个人信息风险、用户权利请求履行状态、法规合规性、供应商风险、用户同意等，实现了自动化和复杂任务的调度，如用户权利请求履行、个人信息映射、同意全生命周期管理等，助力企业有效保护用户个人信息。平台通过标准化隐私合规要求和风险控制点，使法律遵从类的治理活动与产品研发类的技术项目产生关联，**结合研发运营的 DevOps 机制，帮助组织低成本的实现将隐私保护设计至产品**（Privacy by Design）**目标，**甚至进一步实现**隐私保护融入研发运营**（DevPrivacyOps）**的治理闭环目标。**

实现隐私合规一站式管理带给企业众多价值，如实时查看所有数据隐私风险、高效地实现并保持业务隐私合规性、确保整个组织内隐私合规性可靠性、增加团队专业知识和隐私理解、实现各个团队之间的有效协作。

（四）法律科技

法律科技（Legal Tech）主要指利用云计算、大数据、人工智能、区块链等前沿技术和各类科技手段创新改进传统法律行业提供的产品和服务，为法治社会治理提供支撑。

目前，法律科技在国家司法普法、商业交易活动、企业法务管理、及个人法律服务等方面都有着不同程度的应用实践。其中在司法领域

的应用相对更为成熟广泛，特别是推进司法公开、建设智慧司法与法治中国建设方面，我国法院在智慧审判、智慧执行、智慧服务、智慧管理、智能研判等方面，都借助于法律科技手段取得了巨大成绩。

企业应用法律科技方面，近年来多数央企、国企、及各行业领先企业都加快部署建设企业法务合规管理信息化、智能化应用平台，将法务与业务相结合，通过系统化方式进行规范与融合，在规范法务工作业务流程、提高内部工作协同效率的同时，提升企业法律风险管理水平，进一步保障企业稳健经营发展。**法律科技在企业法务管理中的应用特点和趋势如下：**

1.前沿技术成为法律科技发展重要推手

人工智能、大数据、区块链等前沿技术与法律科技的深度结合，促进法律科技不断发展。

企业经过信息化及数字化历程，积累大量的合同数据、纠纷案件数据、知识产权、公司治理等相关法律数据。大数据技术在法律领域的应用日趋成熟，已经出现了针对案例、法规、律师、企业等信息进行检索、分析和评估的技术与服务，以及利用大数据技术进行法律数据的提取、存储、检索、共享、分析和处理的技术。当前，**企业法务大数据已成为企业法务管理的核心且呈现管理价值。**以企业合同数据、纠纷案件数据、知识产权数据等为例，合同数据作为企业最重要、最全面的交易数据，在协助领导者掌握企业的交易量、交易分布并对未来交易进行预测中，起到最为关键的作用。纠纷案件数据在帮助企业决策者了解案件信息、发案原因、涉案主体等，并通过数据分析找出

避免此类案件再次发生的流程、制度或监管的缺陷，降低企业法律风险的过程中，发挥着不可替代的作用；知识产权、公司治理等相关数据，同样为企业的战略规划、目标制定等，提供非常重要的价值。

人工智能技术的进步和法律大数据的丰富极大促进了法律科技的发展。人工智能与法律结合方面，深度学习在法律文本分类、法律文本自动生成、自然语言案例检索上都有较大突破。目前**已经在法律检索、文件审阅、案件预测、咨询服务等四大领域有了较大的应用**。

区块链在法律科技的应用主要表现为区块链存证和智能合约。其中，**企业初步应用区块链存证赋能法务管理**。《最高人民法院关于互联网法院审理案件若干问题的规定》正式承认了区块链证据在法律纠纷中的效力。当前，部分法律科技提供商及企业法律部门已将区块链技术应用于电子文件的数据存证场景，链上保存流转电子文件的签署时间、签署主体、文件哈希值等数字指纹信息，信息一经存储，任何一方无法篡改，满足电子证据的司法存证需求。

企业法务管理加速与新一代信息技术紧密结合、与业务协同，帮助企业解决法务管理中的难点，防范风险，提升效率。

2.多场景深度应用，降本增效成果明显

在企业交易活动和法律服务领域，法律科技在**合同智能审查、电子合同签署、电子存证保护、纠纷案件管理、知识产权管理、普法宣传教育、企业合规治理、法律大数据应用、法律服务机器人、企业尽调及法律风险评估**等方面都已经有大量应用。这些成果与实践，助力企业提高服务效率、加强风险控制、提升服务体验，为广大企业营造

更加可靠、可信、可持续的法律环境和营商环境赋予了更加丰富的技术手段支持。

随着数字化法务管理平台、合同智能审查工具、电子合同签、电子存证、机器人法律服务等法律科技应用在企业的深度落地，**法律科技为企业带来降本增效、风险防控等核心价值**。

（五）数字化风控

企业风险管理是指企业在实现未来战略目标的过程中，试图将各类不确定因素产生的结果控制在预期可接受范围内方法和过程，以确保和促进实现组织整体利益。企业风险管理领域最权威和被广泛接受的概念和理论框架（Enterprise Risk Management）是由美国科索委员会（COSO，反虚假财务报告委员会发起组织）于 2004 年 9 月在其企业内部控制框架上提出的，并于 2017 年 9 月发布新版。2006 年国务院国资委发布《中央企业全面风险管理指引》，中国企业率先从中央企业层面启动了全面风险管理体系建设工作。随后，各行业监管机构陆续发布针对不同类型企业的全面风险管理体系建设指引，如 2008 年财政部会同证监会、审计署、银监会、保监会制定了主要针对上市公司企业风险管理的《企业内部控制基本规范》；银监会于 2016 年发布针对银行业金融机构全面风险管理的《银行业金融机构全面风险管理指引》等。当前，企业风险管理实践已从体系建设走向数字化、智能化发展。

1.企业风险管理从“合规遵从型”走向“价值创新型”

中国企业风险管理实践逐渐从“合规遵从型”走向基于智能化风

险洞察的“价值创新型”。从企业实践来看，中国企业在针对监管指引进行企业风险管理的过程中经历了三个阶段，分别为：第一阶段 1.0 合规导向风险管理，第二阶段 2.0 以风险导向的企业全面风险管理体系建设，第三阶段以赋能企业价值为导向的智能化风控体系建设。数字经济时代的来临，加速了企业的技术创新。在数字化转型的过程中，企业需要统筹规划、确保业务与数字化方案的深度融合，以及不同数字化平台间的互联互通等问题。与此同时，**企业也应关注数字化转型中可能存在的风险以及如何管治**，例如风险防范意识不强、合规管理不到位、存在网络安全隐患等，并应用大数据分析以及人工智能、区块链等技术，对可能存在的潜在风险做好监测预警、识别评估和研判处置，**打造“数据+模型+场景+流程”的数字化风控体系。**

2.数字化风控助力企业实现风险控制要求嵌入业务流程

2019 年，国务院国资委出台了《关于加强中央企业内部控制体系建设与监督工作的实施意见》，在其第三章“加强信息化管控，强化内控体系刚性约束”中提出了风控数字化建设要求，可归纳为三个层次，一是要实现与业务系统的信息互联互通，二是风控标准要嵌入业务信息系统的流程，三是要探索导入智能工具。

企业实践方面，不同行业、不同规模的企业所面临的风险类型均有较大差异。因此，**不同企业在进行企业风险管理时，均根据行业和规模有所侧重**，如金融机构风险管理主要侧重风险领域有信用风险、市场风险、流动性风险、操作风险、国别风险、银行账户利率风险、声誉风险、战略风险、信息科技风险等；互联网企业进行风险管理时

主要侧重业务安全风险、合规风险、舞弊风险、反垄断风险等。

不管对于什么行业什么规模的企业，实现数字化风控均有助于将风险控制要求嵌入企业业务流程，实现风险的动态、主动治理。如**在金融机构的反洗钱风险管理过程中，**企业根据不断丰富的业务数据基础、欺诈样本数据和案件特征库的积累，通过应用自适应学习算法的能力自动调整模型以适应外部欺诈环境变化而引发的风险规则的调整，解决普通模型和专家规则需要过多人工训练和调优的问题。此外，风控规则还作为业务规则的一部分嵌入业务系统中，实现诸如自动拦截交易异常、禁止注册异常账号等风控功能。又如**在传统企业内部消费合规风险控制过程中，**数字化风控解决方案解决了财务、业务系统整合程度低、数据不统一导致的费用管控成本高昂、效率低的问题，通过业务系统、财务系统、企业内部管理系统以及外部合作平台间风险管控规则的联动，企业费用控制逐步实现“事后算账”向“事前预算、事中管控、事后分析”的全流程风险管理发展。

数字化风控使得企业风险管理流程标准化、自动化，减少了人工运营和风险报告等领域所需资源。风险控制要求端对端嵌入业务流程和业务系统中，集中的风控系统后台通过自动化和实时处理实现高度无纸化和去人工化。风险管理人员的重点转向风险管理的全局设计，即充分考虑组织风险管理目标、风险偏好、设计关键风险指标、设计风险数据目录、设置风控节点、建立风险事件管理程序等，风险管理人员的专业价值得到最大化体现。

（六）数字化审计

作为一种重要的国家和社会治理手段，审计对于保障国家经济安全、政策执行和企业合规稳健经营具有显著的支持保障作用。近年来，党和国家高度重视审计监督工作，对推进审计管理体制改革，强化审计监督提出新的要求出台了一系列重大决策部署。如国务院国资委 2020 年 9 月 28 日正式印发《关于深化中央企业内部审计监督工作的实施意见》（国资发监督规〔2020〕60 号），其中关于内部审计信息化方面，《实施意见》明确指出国有企业应构建与**‘三重一大’决策、投资、财务、资金、运营、内控等业务信息系统相融合的‘业审一体’信息化平台；信息化基础较好的企业要积极运用大数据、云计算、人工智能等方式，探索建立审计实时监督平台，对重要子企业实施联网审计。**《实施意见》要求明确指出了内部审计信息系统应与前端业务系统集成连接，获取业务数据开展实时监督工作，为国有资产审计监督工作从传统手工模式向现代数字化动态智能监测方式的转变指明了建设方向。

在我国，审计主要采用政府审计、注册会计师审计、内部审计三位一体的审计监督体系。**本报告专注于对企业内部审计数字化的研究总结。**

从审计的发展历程分析可知，审计经历了三个关键阶段，三个阶段的审计特征分别为现场审计、非现场审计和数字化审计。

（1）第一阶段：现场审计为主

现场审计是由审计机构派出审计小组和专职人员到被审计单位

现场进行的审计。

现场审计特点主要有人工为主、工作方式简单、直观性观察等特点。现场审计不足是审计方式单一、工作效率低、审计的广度和深度有限、审计成本高等，容易出现审计监督盲区，审计风险较大。

（2）第二阶段：现场审计和非现场审计结合

非现场审计是借助信息化技术，帮助审计对象收集、整理和分析信息，查找经营管理中存在的问题、疑点和异常，评价经营管理状况、内部控制状况和风险程度，为现场审计提供线索和资料，是现场审计的一种辅助。

非现场审计特点是信息化技术与审计融合形成的一种审计监督方式，与现场审计相比具有效率高、信息比较全面、审计范围较大等特点。非现场审计不足是受制于信息化水平，审计内容、范围、深度等存在一定不足。

（3）第三阶段：数字化审计

数字化审计是借助移动互联网、大数据、人工智能、5G 等先进数字技术，通过审计数字化、在线化、自动化、智能化、可视化，助力审计全面性、真实性和可靠性等目标。数字化审计是审计的一场体系化变革，目前逐渐成为审计应用的发展趋势。

1.数字化审计促进审计职能转向咨询型审计

根据国际内审协会(IIA)定义:“内部审计是一种独立、客观的确认和咨询活动，旨在增加价值和改善组织的运营。它通过应用系统的、规范的方法，评价并改善风险管理、控制和治理过程的效果，帮助组

织实现其目标。[7]”

内部审计活动从作业方式上分为现场审计和非现场审计。针对**现场审计的数字化主要为通过数字化的手段对审计流程和审计作业管理的线上化、自动化**；针对**非现场审计的数字化主要为借助更全面、更真实、更准确、更实时的大数据，形成新的审计模型，使审计更加科学、准确、客观、统一、公正，提高审计发现问题的广度和深度，提升审计能力和审计价值**。

数字化审计促使审计职能由遵循型审计向咨询型审计转变。企业数字化转型过程中，数字化审计充分运用海量数据及 RPA、大数据分析、区块链、云计算等新一代信息技术，不断扩大审计覆盖面，实现审计活动从事后向事中、事前延展，审计范围覆盖从会计向业务、管理和治理延伸，**审计工作重点从传统的监督和评价转向实时确认与咨询**。通过对海量数据的全面深入分析，深入挖掘组织存在的风险和机会，为组织创造更大价值。

2.审计对象数字化驱动数字化审计体系化建设

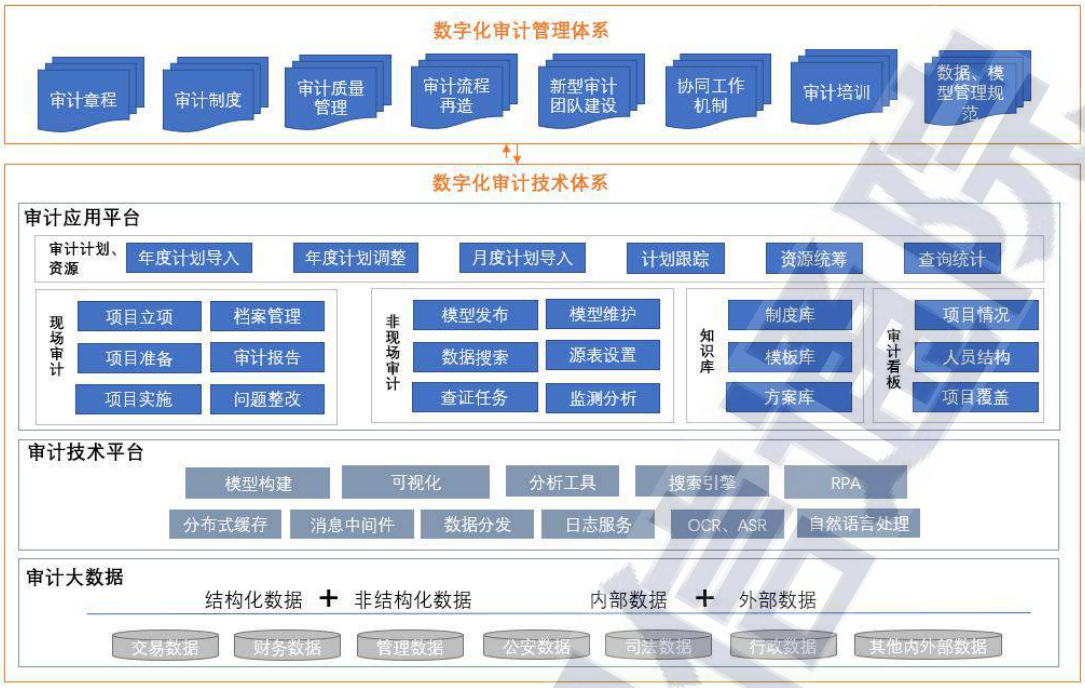
近年来产业数字化和数字产业化深度融合，各类生产生活活动高度依赖数据及数字技术。企业前中后台诸如营销、运营、风控、财务、法律等经营管理活动都在逐步数字化，**审计对象的数字化促使企业内部审计需通过数字化审计进行体系化建设相适应**，实现与审计对象的同步，减少审计成本、提高审计效率、最大限度发挥审计在企业管理中的最后一道防线的价值。

审计对象数字化最主要特征为丰富、实时的审计数据。企业内部

审计团队基于丰富的审计数据，借以人工智能、大数据、区块链、云计算等为代表的新一代信息技术，实现内部审计的数字化。

以商业银行审计大数据构建为例，其主要经历三个阶段，第一阶段将主要的账务数据、交易数据进行 T+1 日采集、转换和加载，实现了线上分析疑点数据，解决了传统审计人海战术的弊端；第二阶段改善系统可拓展性及可用性，增强数据加载和处理能力，接入包括对公信贷、零售信贷、国际业务在内的更多业务数据，并向审计分支机构进行推广；第三阶段是借以 A（人工智能）、B(大数据)、C（云计算）为代表的信息技术，统筹行内外一切可用的数据资源，充分挖掘数据的内在价值。

审计数字化是对于企业内部审计是一场体系化的变革。**企业不仅需要从数据、新技术应用、技术平台等方面建立新的审计生产力，也需要同步推进制度、流程、团队、人员能力结构、文化等管理因素对生产关系的重构，成体系构建企业数字化审计，**实现内部审计的“风险警示、监督评价、管理增值”三大职能。



来源：中国信息通信研究院

图 4 数字化审计体系

数字化审计体系建设需要经历**规划、实施、运行、完善等路径**，持续推进。**在规划阶段**，企业应展开广泛调研，了解业界最佳实践，并根据组织现状，明确数字化审计目标，识别主要的工作任务并成立由审计专家、业务专家、技术专家等不同视角的项目团队，对目标和任务进行详细的规划设计，形成行动方案和蓝图；**实施阶段，管理体系构建方面**主要任务为梳理重构传统审计流程、构建新型审计团队，建立由审计部门统筹、各部门配合的多部门协作工作机制；**技术体系构建**应首先构建完善的审计大数据，在数据基础上构建技术平台向下处理审计大数据，向上支撑审计应用平台的构建；**运行阶段，**推广数字化审计体系，通过技术平台和机制的运转，以宣传、培训、考核、反馈、改善为手段，确保数字化审计体系顺畅运转，为组织创造价值。**完善阶段，**需要根据组织内新的审计需求，运用新技术，不断优化体

系，修补漏洞，保持数字化审计体系的先进性。

三、企业数字化治理应用关键领域痛点分析及应对

（一）数字化运营

1.数字化运营典型痛点分析

（1）技术准入门槛、团队协同机制等方面问题阻碍 BizDevOps 落地

BizDevOps 强调覆盖业务价值管理，形成业务、研发、运维、运营的闭环流程，因此业务人员需要参与到全过程中。然而，由于业务人员的工作技能与经验更偏向业务分析、需求设计、业务建模等内容，掌握的技术能力无法实际参与到研发、运维、运营的工作中，因此在实施 BizDevOps 过程时难以进行全流程拉通。此外，由于工作流程标准化、自动化、数字化、透明度等能力的不足，业务与技术各角色间高效率、高质量的协同存在困难。

（2）海量运维数据的接入与管理以及算法模型维护成为 AIOps 实践瓶颈

由于在进行信息化能力建设初期对信息系统（生产运营、企业管理、协同办公）的互联互通和信息共享能力考虑不足，当前很多企业难以实现针对各系统间多数据源的海量运维数据的统一采集和纳管，进而无法支撑 AIOps 应用场景落地的数据分析、机器学习建模等能力要求。

当算法落地在不同的 AIOps 应用场景时，通常会采用不同的模型编排组合，从而造成模型的维护成本高、效率低，难以达到降本增

效的实践目的。

（3）工作流自动化实践中面临组织、技术和架构变动等多方面挑战

由于工作流自动化涉及到协同能力整合以及一体化、平台化能力建设，企业内各组织间系统的打通是不可避免的。组织层面上，打通组织间的信息系统对于企业的组织架构存在变革要求，在此过程中具有转型驱动力不足的情况；技术层面上，在进行平台资源整合时，会通过 API、JDBC、Agent 等多种方式实现各系统间的串联，但存在使用多年的老旧系统无法提供标准接口等功能的情况，影响平台整合效果。此外，企业在数字化转型过程中，常涉及到对应用架构的调整与重构，因此已建成的工作流自动化平台存在与现有架构不匹配的风险。

2.数字化运营实施建议

在 BizDevOps 方面，通过微服务、低代码/无代码、RPA 以及 AI 等技术的融入，实现行业生态的全面融合，持续降低业务人员参与研发、运维、运营过程的技术准入门槛。同时规范工作流程，借助一体化工具平台拉通不同部门、团队，提高各角色间的协同能力。在此基础上，通过全局的信息透明和数字化洞察能力，有效促进团队协同，并为团队持续改进优化路线提供方向。

在 AIOps 方面，通过发展数字化运营基础平台，能够实现海量数据资源的融合、共享与开放，推动大数据挖掘、分析和服务，并实现 AIOps 各关键应用场景的实施落地。同时，形成数据资产，更好的服务于数字化运营转型。此外，针对模型维护成本高的问题，可以

考虑通过在线学习等模型训练方法，根据线上数据反馈情况，实时快速地进行模型调整，提高 AIOps 应用场景落地的效率与准确率。

在工作流自动化方面，针对组织层面挑战，可以通过试点方式先布局小范围内的组织变革与转型实践，助力工作流程自动化能力的实现，获得一定成效后再向组织更大范围推广。针对技术层面挑战，可以通过 RPA 等技术模拟用户行为，帮助老旧系统创造 API，从而完成系统的串联整合，形成一体化、平台化能力。同时企业需要识别是否针对陈旧、过时系统进行更新换代，在考虑成本等因素的同时从根本上解决问题。针对应用架构变动带来的问题，可以通过 API 生命周期管理和元数据管理等手段，第一时间发现异常，避免因为变动而产生的影响，自动化实现工作流搭建与应用架构的协作联动。

（二）新技术治理

1.云治理典型痛点分析

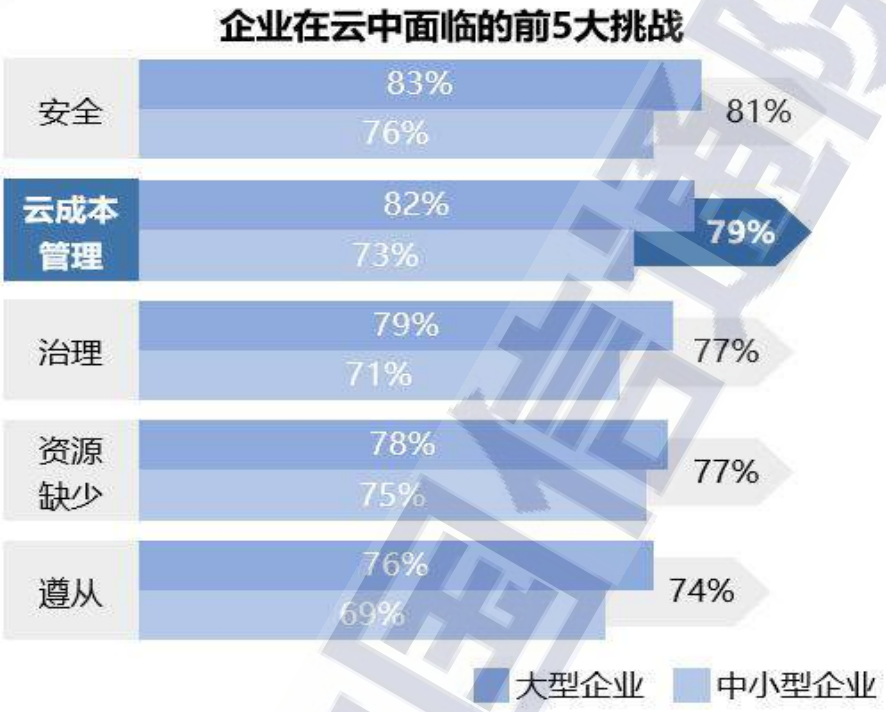
（1）安全合规问题成为企业云采用潜在的重要风险因素

不管是私有云、公有云还是混合云，企业在云采用过程中面临着业务、网络、数据等一系列内外部合规要求。同时，云安全联盟 CAS 公布的 2020《云计算 11 大威胁报告》中指出身份、凭证、访问和密钥管理不善为 11 大威胁之一[8]，大量企业实践也出现各种相关问题和事件，对业务和声誉造成了很大影响。

（2）云成本管理问题阻碍云采用价值最大化

伴随着云资源投入的不断增加，云资源成本超支、成本可见性差、闲置资源浪费等问题困扰着上云企业。IT 管理解决方案提供商

Flexera 在其 2020 年关于全球 750 家企业云计算使用现状的调查报告显示云成本管理是受调查企业在云中面临的前 5 大挑战[9]。



来源：Flexera, 2020

图 5 企业在云中面临的前 5 大挑战

企业在云成本管理过程中如何衡量云资源投入有效性，平衡发展效率、质量与成本之间的问题日益凸显，而云资源投入的利益相关方——使用者、建设者及管理者的视角间存在较大差异，消弭部门间视角差异，有效融合业务、IT 及财务需求已成为发展需要。

来源：中国信息通信研究院

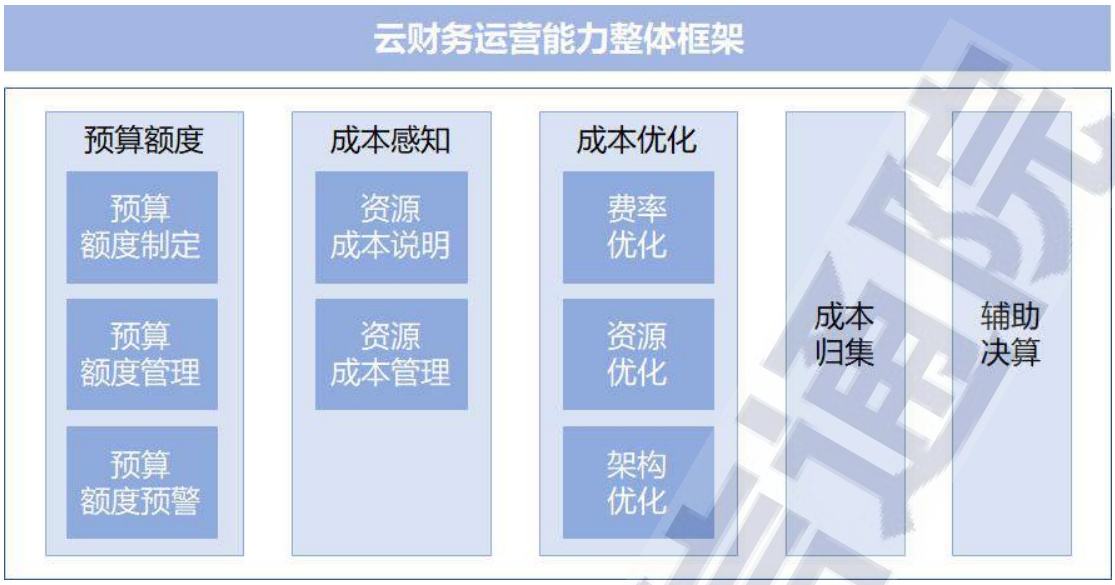
图 6 云成本管理不同视角

2.云治理实施建议

云采用安全合规方面，企业首先明晰云租户和云供应商责任共担模型中责任与业务，共同承担合规性责任，各自实现合规目标，保证云上运行的安全合规。企业自身可从上云的架构设计、解决方案选择、运维环境以及数据和隐私保护等多方面入手，将合规性融入管理、技术、流程与操作中，符合广泛且不断变化的合规清单，使合规成为企业云上运营与发展的基石。

企业在**云治理过程中，需要首先对云上账号、角色、权限的风险治理制定章程、制定并实施治理基线，**由此可避免在规模壮大后可能出现的人员冗杂、权限难以梳理、账号无法清退的困境，避免因低效混乱的账号管理遭受恶意访问和攻击。

云成本管理方面，组织迫切需要从财务角度进行云服务的预算制定、成本感知、成本优化、成本归集和辅助决算，以期实现对云服务的精细化管理、经济型运营。



来源：中国信息通信研究院

图 7 云财务运营能力整体框架

企业在云上稳定发展后，最重要的是持续治理。规划好身份、安全、成本、业务连续性、合规等方面的治理策略并部署后，利用云上具备监控和持续检测能力的治理工具，确保企业在云上持续满足安全性和合规性，并实现成本优化。

3.AI 模型治理典型痛点分析

（1）模型治理未形成技术+管理的有效治理体系

当前，已经部署模型管理平台的企业针对 AI 模型的治理实践中存在部署技术平台后**未形成相匹配的模型治理组织结构和配套制度体系**，导致技术平台无法发挥最大作用，制约企业最大化实现模型价值和对模型的治理。

（2）模型应用过程中缺乏模型业务价值监测评估

目前，开始尝试进行模型治理的企业通过技术手段对**模型开发**的全生命周期进行管理，并初步建立了模型资产管理平台。但在**模型投**

入使用后缺乏对于模型产生业务价值的监测和评估，无法对于模型进行有效优化，导致模型的开发应用未形成有效闭环，模型资产的价值未进行有效运营。

4.AI 模型治理实施建议

企业应积极了解业界 AI 模型治理动向，结合企业实际，制定本企业人工智能模型应用原则、治理原则，并形成从上到下，从管理到技术全方位的人工智能模型应用和治理体系。**组织形式上**形成由业务人员、模型开发人员、安全人员、审计人员等构成的多职能协调的结构。**制度流程上**形成覆盖模型全生命周期的管理流程并完善模型清单、模型开发报告、模型实施报告、模型验证报告、模型监控报告、模型年审报告等一系列文档。**技术上**以 AI 模型管理平台为技术手段，实现模型的集中化、流程化管理。

模型投入应用后，还需加强模型对于**模型性能和业务效果的监控与评估**，形成监控评估机制，最大化发挥模型业务价值，以及通过可视化模型价值辅助业务决策。

（三）智能安全与隐私合规

1.智能安全典型痛点分析

（1）海量安全数据计算的准确性、及时性无法保障

企业智能化网络安全体系建设过程中存在无法有效解决海量大数据计算、分析、研判的及时性和准确性问题，导致对业务安全风险的判定存在偏差或疏漏；

（2）机器智能与专家智能结合学习曲线陡峭

企业推进智能安全治理体系时需要结合机器智能和专家智能，当前存在技术人才对工具依赖性强、安全专家经验无法适配智能安全需求、以及机器学习相关获取曲线陡峭等问题，导致技术人才的专业性与智能安全体系发展的要求存在较大缺口。

2.智能安全实施建议

海量异构数据源是利用大数据技术得出精确结果的关键前提，包括 IT 基础设备的性能数据、网络流量数据、安全监测数据、状态数据、告警数据、系统登陆数据、操作日志、操作审计数据等。企业应采用大数据底层架构，**实现海量异构数据采集、存储、计算**。对大数据组件进行深度整合，在确保基础设施性能的同时，通过**场景化的安全建模，打磨关联分析规则**，确保及时准确发现安全风险，建立威胁图谱，同时开展定向的威胁狩猎，挖掘隐藏更深的安全威胁。大数据分析应**清晰划分逻辑结构，详细定义数据采集层、数据消费层、数据存储层、分析引擎层、安全应用层**等几个主要部分。

企业在建设智能安全治理体系时应整合资源，制定规划，并将人员培养与建设规划上升为战略层级，通过管理、流程、运营、演练等机制，打造**“大安全”团队模式：**

● 专业技术团队的建设和人才的培养需要过程，不可能一蹴而就，一方面要结合当前发展现状，制定完整的规划蓝图，确定各阶段关键里程碑，同时根据不同场景，融入技能培训，实战演练，攻防比赛等多种形式，激发团队兴趣，发挥团队擅长；另一方面必须着眼未来、

立足长远，对未来行业新风险、新技术应用、新发展态势有充足预判和应对措施，适应不断快速变化的内外部环境。

● 建立“大安全团队”的目的是让企业树立新的安全技术理念，对传统的信息安全管理运营模式进行改革，解决分散化、碎片化、低效能的问题。通过“大安全”团队模式，串联不同技术擅长、不同技术部门，以及不同技术职责的人员所有工作成果，做到网络信息安全工作全流程闭环运营，无死角全覆盖。

3.隐私合规典型痛点分析

（1）隐私合规管理未形成统一“大脑”

面对日益严峻的隐私合规监管态势，**大多数企业未建立统一的“隐私合规大脑”**，仍使用传统的邮件、群组等方式来处理隐私相关的合规事务，然而其合规工作通常涉及法务、数据、IT 和信息安全等多个业务团队的合作，通过**传统方式进行沟通、审查或审批，实施过程较为冗长，费时费力，较难应对数字时代处理海量个人信息的合规需求**。

（2）关键隐私合规环节需要提升自动化能力

自 2019 年以来工信部、网信办等开展的 App 专项治理行动，对 App 运营者及时应对监管行动提出了很高的要求。企业落地隐私保护监管要求时，存在隐私保护**相关法律法规要求未能很好映射到企业 APP 收集使用个人信息相关行为**上的问题以及**普遍未实现自动化自查 APP 隐私合规风险**。

4.隐私合规实施建议

隐私合规治理过程中首先**应对流程和要求进行梳理**，协调内部已有的系统和相关方，**实现聚合统一管理**。此外，通过隐私合规一站式平台承载隐私合规治理统一流程，优化已有流程，提高应用效率，实现自动化动态监控企业隐私合规风险状态，全方位一体化把握风险。

此外，企业还可通过数字化手段，实现管理和维护法律法规原文要求，也可将内部针对隐私相关法律法规的解读，映射到 APP 的具体采集个人信息行为要求，并录入隐私合规一站式平台。

APP 隐私合规自动化监测方面，**可通过配置 APP 行为要求基线至监测评估工具中，并将检测评估工具嵌入 App 开发研发流水线，**帮助 App 在上架前进行隐私合规自测并进行整改，从而降低 App 收集使用个人信息的违规风险。

（四）法律科技

1.法律科技典型痛点分析

（1）企业法务数字化与法务管理制度流程相脱节

企业法务数字化建设是一项庞大而复杂的系统工程，需要管理和技术双螺旋推进。**企业在法务数字化建设的实践中往往存在未对企业法务管理制度规范体系进行系统梳理，导致法务数字化建设与法务管理步调不一致，数字化不能很好的实现法务管理的目标。**

（2）法务系统“信息孤岛”制约法律科技效能发挥

企业法务数字化过程中存在未系统考虑公司全面风险管控的需

求，导致**法务系统与其他业财系统之间缺乏互联互通，成为“信息孤岛”**，无法有效支撑合同履行监控、纠纷案件预警、法律风险决策等目标，是制约企业法律科技发挥效能的“瓶颈”。

（3）合同智能化水平及电子签章使用率低

当前，对于占据企业法务工作大量工作时间的合同管理流程，普遍存在合同智能化水平低、电子签章使用率低的情况。

当前，由于合同条款的复杂性和合同审核的标准化程度低，导致企业**无法推广使用合同模板，难以实现合同智能化管理和有效控制合同条款风险**。企业同时面对庞大的合同量，有限的法务人力资源每天为审查合同应接不暇，且很难不出现疏漏，合同审查耗时费力。电子签章由于企业内部系统复杂、集成难、个性化需求多等因素导致的**电子签章平台交付时间长以及安全考虑**，导致普及率有待提高。合同签章流程中盖章申请流程慢、异地合作盖章周期长、印章签署需求大等问题严重影响合同签约效率。

2.法律科技实施建议

企业在推进法务数字化的过程中，应首先理清当前法律工作中的难点，从管理流程的角度审视如何解决法务数字化与法务管理制度流程相脱节这一难点问题。**明晰管理难点后，才能更好的匹配数字化的需求，才能更好的选择法律数字化的解决方案和产品工具**。以合同管理为例，企业需首先梳理当前企业在合同签订前、签订中、履行中、履行后整个合同生命周期存在的问题和难点，区分可通过管理流程解决的问题，如流程不清晰、不同部门职责划分、经办人员责任心、总

部和分支机构管理界限等，以及需要数字化手段解决的问题，如审核效率低、过程没有记录、过程不透明、查询统计不便、信息共享、信息传递等问题，通过管理和技术的有效结合才能更好实现法务数字化管理的目标。

构建高质量的法务大数据方面，内部数据集成方面，企业应重点以合同为中心串联企业经营数据，实现与财务、项目、销售、采购、风险、审计等各个领域的数据贯通，实现数据协同共享，构建高质量的企业法务大数据。外部数据方面，应充分集成法律法规库、司法案例库、企业工商信息库等公共数据。

智能合同及电子签章促进法务管理流程的自动化、智能化，提高管理效率。合同智能化方面，使用合同智能管理工具提高合同审核效率，通过对各类合同文本的多维度分析，结构化，逻辑化，将合同文本分解成多维度相关联的知识体系，结合合同审核工具，高效快捷完成合同的起草与审查工作。此外，通过 Web 应用程序集成、APP 集成等多种手段缩短电子签章与现有系统集成的交付周期并通过安全加固签章 API 以及保留电子签章所有操作日志等组合方式保证签章安全，降低电子签章使用的风险，提高其使用率，释放法律人员的专业价值。

（五）数字化风控

1.数字化风控典型痛点分析

（1）顶层设计及部门间配合机制不足致使数字化风控难推进

风险管理的数字化转型不仅仅是技术层面的转型，更需要有配套

的机制加以保障，才能更顺利地推动转型。目前企业风险管理数字化转型实践中存在顶层设计以及部门间配合机制不健全，导致执行力欠佳，影响内部管理效率的问题，如风险管理数字化转型计划及其详细的实施路径拆解不够明晰，各部门配合机制不顺畅，落地执行力不足等。

（2）风险管理应用场景设计不完善限制风控效果

企业在推进数字化风控过程中，存在由于**对业务缺乏深刻理解，导致风险管理应用场景规则设计不能很好贴合实际业务场景风险控制需求**，无法实现风险控制效果的问题。例如业务反舞弊风险管理场景中，若未针对反舞弊场景进行详细分析，识别风险点和场景特征，就无法设计有效的风险防控规则，从而使风险防控沦为简单的权限管理。

（3）风险分析数据匮乏、质量低成为数字化风控瓶颈

数据贯穿于数字化风控的每一个环节，其全面性、完整性很大程度上决定了风险管理工作的主动性、精准性和预见性。企业风险管理数字化过程中，往往存在**风险分析所需的内外部数据匮乏、数据质量不高的问题。**

一方面是企业虽已建立大数据平台并进行数据治理，但由于历史遗留问题较多，导致风险管理活动需要的数据质量仍需不断改进提高。其二，内部数据有限，外部数据可用性较差。以反欺诈风险管理为例，企业在实施反欺诈模型过程中存在用于模型训练的欺诈数据样本少、欺诈数据样本与正常数据样本比例严重失衡的问题。欺诈数据样本一

般标注成本相对较高、样本获取渠道相对有限，使得模型策略对于用户欺诈特征无法全部准确学习、模型策略的效果提升空间受到限制。

2.数字化风控实施建议

风险管理数字化转型是一个持续的系统性工程，需要在决策、管理、协作和执行等方面建立稳定的机制，保障转型工作的有序可控。具体来看，企业应当从风险战略、治理架构、风险文化、流程机制、考核激励、工具技术和人才等方面构建完整的全面数字化风险管理体系，破解碎片化的风险管理局面，以企业治理角度，整合企业前中后台各职能，促成同一语言、同一方向，使风险管理融入企业治理的方方面面。

企业在每一个风险场景智能化改造的功能设计上，都应**坚持紧贴真实业务场景，持续迭代，在合理完善的风控规则基础上，利用多维度、多特征的数据进行分析**。此外，在模型算法选择时，需要考虑数据基础以及模型和应用场景的匹配度。

为应对风险分析数据质量问题，一方面企业应注重数字化转型过程中**各流程、各应用、各数据流标准统一规划，提高数据生成的质量。风险管理部门可以在现有大数据平台的基础上，基于风险管理的需求提出数据源、数据采集、数据处理等标准要求**。此外，对于数据缺乏问题，企业**积极探索应用隐私计算技术、多方安全计算等方法等加强行业间、企业间数据共享**。加强内外部数据治理，统一数据来源，丰富数据类别，持续加强有效风险数据加总、报告、分析、运用能力建设。

（六）数字化审计

1.数字化审计典型痛点分析

（1）难以建立跨组织联动、敏捷、高效的组织架构

数字化审计要实现“全面性、时效性、成本低、效率高和规范性强”，需要一个具有跨职能联动、敏捷、高效的组织架构，并按需设置相应的管理岗位，按照统分结合的管理办法要求，共同落实数字化审计的建设、管理、运营、服务等目标。目前，很多**企业对于建立新型审计组织的认识和实践不足，导致企业数字化审计的全面落实受阻。**

（2）数据管理困难制约数字化审计实施效果和发展

在数字化审计中，数据是关键要素，但目前企业的业态通常比较复杂、业务分布散、数据特性异常复杂。受业务源数据质量参差不齐、业务领域数字化转型成熟度不一的影响，导致企业数据汇集难、数据共享难、数据管理难，大大降低了数字化审计结果的精准性和效用性。

（3）审计模型构建和发挥效果成为数字化审计难点

模型是审计数字化转型的难点，也是提升审计数据分析能力的关键因素。一方面，企业审计数字化的过程中审计模型构建依赖于审计人员对审计流程、业务流程、数据分析的充分了解，实践中企业存在审计师不具备数据思维、模型思维，缺乏数据分析意识和敏感性的问题，导致审计模型构建成为难点，审计模型构建慢、数量少，不能满足数字化审计建设需求；**另一方面，**审计模型构建后缺乏有效的反馈调优机制，导致审计模型不能很好地随着业务变化和审计规则的变化

进行调整，导致模型使用效果差强人意。

（4）数字化审计专业人才不足阻碍数字化审计发展

数字化审计所需的复合型审计人员，需要具备一定的专业审计能力、业务经验、信息系统 IT 技能、甚至新技术应用等多方面知识。但是，目前企业的审计人员多为财税、法律等专业相关，具有信息技术能力的人才往往在审计专业知识方面又有所欠缺。审计人员知识、能力参差不齐，同样的审计任务，报告千人千面，呈现出专业局限，企业亟需加强数字化审计文化建设、互动、交流、培训等，为数字化审计培养更多专业人才，支撑数字化审计建设。

2.数字化审计实施建议

数字化审计不是数字化平台和技术工具的简单堆积，企业需要发挥**协同思维**，融合各相关方视角推动企业在审计组织、人员数字化能力、审计规程、审计质量等方面进行适配性变革，才能建立起联动、敏捷、高效的数字化审计组织架构。

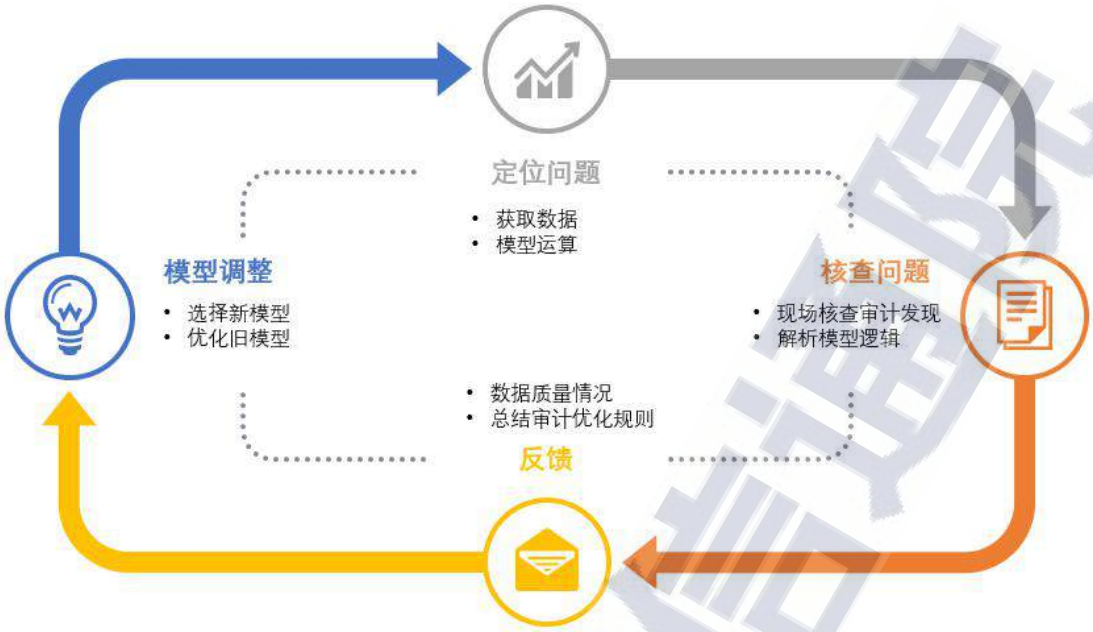
数字化审计队伍建设方面，企业应积极探索数字化审计工作模式、建立起数字化审计专业团队的选拔和培训机制，采取分批选拔、定期考核、动态管理、优胜劣汰的方式，建立起优胜劣汰的选人用人机制。通过增量调整存量，逐步加大具有数据分析能力和业务背景的复合型人才的占比，通过加强培训、管理、考核等措施，逐步提升全体审计人员的专业能力。

企业要建立高质量的审计大数据体系，需要在管理层面提出数字化**审计大数据建设与治理的统一要求，**为大数据管理、大数据平台组

件研发、大数据建设等提供管理能力。**审计数据质量控制方面，企业应制定并优化审计数据质量体系，提供数据标准和接口规范，**有效管理审计数据的来源、采集、清洗、存储、备份、销毁等全生命周期流程，保证审计数据质量的准确性、完整性、一致性、唯一性、适时性和有效性，实现数字化审计数据资源的 **“逻辑统一、互联互通、共建共享”**。

审计模型是提升审计数据分析能力的关键因素。企业应在充分的内外部调研的基础上，立足组织现有模型资产并结合市场领先机构的经验，构建包括规则类、统计类和机器学习类模型体系，通过模型来开展各类数据分析，并在此基础上建立以审计数据全覆盖的审计作业体系，降低审计抽样风险。**分阶段搭建审计模型，实现“审计规则—审计模型—审计框架”**的模型构建路径，满足多种审计业务，扩展审计的深度和覆盖面。

审计模型优化方面，模型构建后非现场运算得到模型结果，并通过现场审计核查模型结果以及解析模型逻辑，依靠审计现场反馈优化审计思路，并转化成审计规则以便对审计模型进行调整。根据该循环迭代的交互方式不断提升审计模型的效用。



来源：中国信息通信研究院

图 8 数字化审计模型优化循环

在丰富完善的审计大数据和有效的审计模型之上，企业在建设**审计应用系统时**，应考虑组织内控三道线在数据、模型、工具、流程和成果方面的共享，构建**三道线联防联控**的企业级审计平台。

四、企业数字化治理应用发展建议

要实现完善的企业数字化治理机制，**需要打造多元主体参与、多措并举、协同治理的机制**，依赖于政府、行业组织、研究机构、企业、公众等各方参与合作，需要各方各司其职、各尽所能，以适当的角色、多样的治理手段协同共治。

作为企业数字化治理的主体，企业应将数字化治理与数字化转型同步考虑，形成数字化转型与数字化治理的发展共生双螺旋。一方面，通过数字化治理，保障数字化转型的有效、可持续。另一方面，通过数字化转型与数字化治理的资源共建共享，实现 IT 投入价值最大化，

企业整体战略目标的胜利达成。

作为数字化治理的**产业侧**，应积极投入数字化治理各领域产品和解决方案的研发和创新，并加强与需求侧的交流合作，打造良性的发展生态。

行业协会、联盟、科研机构等组织应充分发挥行业协调作用，展开广泛调研，通过制定指南、标准以及协同行业共享经验、解决方案、产品等方式降低企业探索、试错成本以及合规成本，促进企业数字化治理发展。

政府部门一方面可发挥对企业技术与服务的监督管理职责，制定发展方针、建设原则，为企业数字化治理营造良好的发展环境。另一方面，加大力度支持在企业治理相关法律法规、制度标准、合规案例、合规实务、合规产业信息等相关公共资讯服务平台建设。通过该类公共服务基础设施帮助不同性质、不同业务的企业全面地、清晰地、快速地了解需要满足的合规要求与注意事项，协助企业健康、有效开展数字化治理。

附录：数字化治理典型案例

（一）数字化运营

1.中国联通一站式研发管理平台提升企业研发质效

（1）案例背景

为贯彻十四五规划，在企业数字化转型过程中，IT 作为支撑企业转型发展的底座，不仅要持续提升 IT 研发效能和吞吐率，更重要的是企业 IT 需要从交付价值进阶为基于业务场景的价值交付和数字运营。“更快、更好、更有效”的为业务创新赋能是研发交付的新要求，从上往下的规模化工程能力提升是急需解决的问题。

（2）解决方案

从软件研发管理平台、研发管理流程、量化体系、工程能力成熟度模型 4 个角度进行数字化治理，主要体现在：

集团统一的研发过程管理流程，包括项目管理、需求管理、任务管理，统一定义、统一工作属性/状态流程，并作为项目管理要求进行落地，体现在工具平台。目前软件研究院已经实现全量项目的研发过程统一。

来源：中国联通软件研究院

图 9 一站式研发管理体系架构

制定统一的项目管理量化体系，结合软研院“提高业务价值、实现快速交付、提高自主研发掌控率”的管理导向、以 DevOps/SAFe 等先进思想为价值导向，提取可横向比较、多维度的指标，形成能横向比较的研发效能评价体系，并在组织内进行月度公开；建立完整的研发效能指标体系，区分项目级、组织级的项目画像、个人画像展示项目和个人的研发效能，实现软件研发全生命周期可控、可视、可评价。

支撑敏捷、瀑布双模灵活管理项目，满足项目集协同项目管理过程要求；持续完善过程管理、持续集成等能力，提升性能完善功能，增加项目集流程专项支撑；依托天宫云 IaaS 平台能力打造流水线云服务能力，为项目提供统一流水线编排、配置及调度能力；度量管理满足项目度量数据统计采集需要。

整合软研院的专家资源，结合软研院的组织结果等自主性特点和业内主流项目管理理论，形成**中国联通软件工程能力成熟度模型**（The Chinaunicom Capability Maturity Model of DevOps，缩写为 CCMD）从需求、开发、构建与持续集成、部署与发布、测试、反馈与改进 6 大能力域、4 个能力级别来描述 24 个能力子域的工程能力水平及方法，为项目提升效能提升理论指导和工程实践方法。

（3）应用场景及治理效果

2021 年 1 月正式在联通软研院内进行推广标准研发管理流程，

共涉及 300+项目，为研发效能量化体系可量化提供最基本的土壤环境。项目管理从需求管理、任务管理、测试管理、发布管理更加标准化、规范化。

建立研发效能量化体系，工具具备从组织>项目>个人的度量体系，可客观、实时、准确地展示研发能力水平，项目组可根据界面化展示的量化结果，在线分析效能评价，持续性进行效能改进。

经过 5 个月内的研发效能量化监督和监管，整体效能水平提升 77%，研发过程的补录现象有所收敛，过程质量提升，如代码违规质量提升 80%。

（4）创新性和示范性

- 全集团对内统一研发管理平台、流程，对外产品化

经过 4 年多的产品发展，研发管理发展经历了工具化、平台化、产品化的演进与沉淀，现以“研发数字化”为关键技术和特征，为中国联通全域 IT 系统研发管理能力与质效提升提供一体化解决方案和工具支撑，对标中国信通院发起的《研运数字化流程整合成熟度模型》，已达行业领先水平。天梯项目在平台规模上，20 年已实现集团内大范围推广，省分、软件研究院均已全部入驻天梯。

- 建立健全的量化体系，提升研发管理的实时性和客观性

从质量、效率、价值三方面提取过程性、结果性指标，形成能横向比较、多维度的立体式研发效能评价体系，为后续 AI 一体化运营奠定基础。

- 形成联通式的工程能力成熟度模型

整合软研院的专家资源，结合软研院的组织结果等自主性特点和业内主流项目管理理论，形成中国联通软件工程能力成熟度模型，为工具发展和效能管理提供方法论。

- 建立组织内企标项目，共享工程能力优秀实践

企业内树立标杆，助力项目组通过 DevOps 能力成熟度三级评级，达到行业领先水平行业领先。构建研发工程能力提升组织保障体系，以“PMO-天梯运营支撑团队-QA 群”的三角模式，高效运营，支撑研发效能提升。

2.中国移动江苏公司基于运维研发化的运维数智化

（1）案例背景

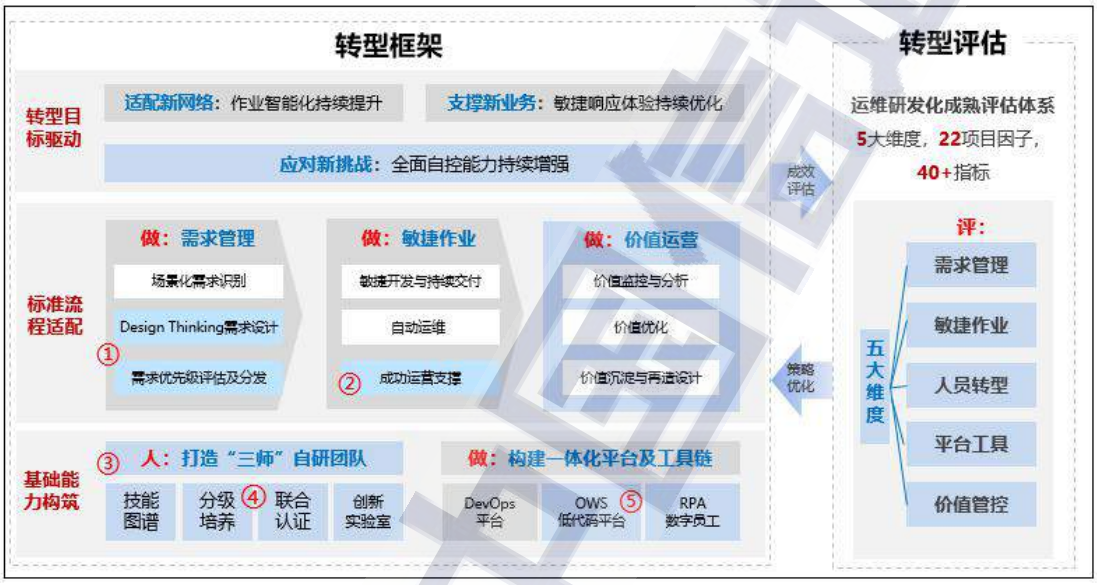
随着新网络、新业务的不断发展，运营商的传统网络运维模式无法满足敏捷响应和降本增效要求，面临诸多挑战。同时当前 5G、云网新技术大规模应用推进网络向虚拟化、智能化、软件化快速演进，运营商需要借助各类应用改造工作环节，提升运维自动化智能化水平。而传统网络运维中系统应用开发主要依靠外部合作方完成，存在开发周期长、无法敏捷迭代、缺少标准化流程等问题。

（2）解决方案

为加快推进传统网络运维模式向运维研发化体系转型，通过自研工作流程、工作机制和支撑工具链的建设，牵引网络各类应用转向自研开发，并支撑应用敏捷迭代和高效运维。

运维研发化改变了应用开发外包的传统模式，将 IT 自开发与网络运维紧密融合。针对可自动化、智能化的运维工作，设计网络策略

制定、数据分析建模、应用编排开发的“三师”新角色，组建三师自研团队；基于 DevOps 流水线建设具备高/低/无代码开发工具的一体化全栈开发工具链；参照 SCRUM 开发流程，制定从需求管理、敏捷作业到价值运营的标准化工作流程与管理机制。向运营商员工提供自研基础能力支撑，实现各类应用的敏捷开发和高效运维。



来源：中国移动江苏公司

图 10 运维研发化转型框架

（3）应用场景及治理效果

基于运维研发化体系，开展了 2B 方向的云专线自动开通、云资源池自动巡检 2 个案例和 2C 方向的 5G 故障管理机器人、自动值守机器人、网络投诉机器人 3 个案例的自研实践。

云专线自动开通：组建 3 人三师自研团队，根据专线开通规范设计自动开通业务流程流图和相关角色活动，参照 scrum 模式列出 sprint 目标和开发任务，利用工具链中业务编排中心对自助下单、局数据设置、资源调度、施工验收等原子能力自主编排配置，实现云专线端到

端开通流程自动化，实现全网首条跨域云专线自动开通，端到端开通时长由 2 周缩短至 5 个工作日，累计开通专线 100+，节省工作量 8400 人天/年，创造收入 2000+万元。

云资源池自动巡检：组建 7 人三师自研团队，根据巡检工作流程分步骤完成场景流图和高保真页面设计；参照 scrum 模式明确 10 个 sprint 目标与开发周期；利用工具链中 OWS 低代码开发工具对巡检规则、指令下发、结果分析等功能编排开发，与现网云资源池控制节点对接实现自动巡检。每日全量自动巡检 11 地市资源池服务器 600+、虚拟机 1200+，人工每日参与时间从 4h 减少为 10min，巡检准确率从 60%提升至 98%以上。

5G 故障管理机器人：组建 7 人三师自研团队，根据现网规范完成告警处理流图设计和专家规则梳理；参照 scrum 模式编写项目 backlog 和 sprint 目标，利用工具链 OWS 低代码开发工具编排告警处理流程，注入故障专家规则和容灾应对策略，实现异常检测、根因自动诊断和应急容灾恢复。日均处理云化网络全量告警 9000 张，告警压缩率提升 5%，5 分钟故障事件定位，时长下降 80%，3 人日常监控值班减少为 1 人。

网络割接值守机器人：组建 4 人三师自研团队，根据割接值守场景需求设计机器人工作流图和高保真页面，参照 scrum 模式设定 sprint 目标与开发计划，基于工具链 OWS 低代码开发工具编排设备数据自动对接、自动核查指令及健康度评估模型，实现自动化值守巡检和快速预警提醒，已完成割接后自动值守巡检 250+次，单次割接时长节

省 3 小时，节省工作量 240 人天/年。

网络投诉机器人：组建 5 人三师自研团队，根据手机上网和语音投诉两类业务场景设计处理流程和高保真交互页面，并梳理专家定界规则；参照 scrum 模式设定项目 sprint 目标与开发计划，基于工具链 DevOps 平台采用 Python 编写投诉处理功能模块和专家定界规则，并与现网投诉生产系统对接，实现投问题智能诊断。投诉处理流程 60%工作自动化，日均自动处理 600+全量投诉工单，定界时长缩短至 15 分钟，效率提升 75%，工单平均处理时长下降 5.5%。

（4）创新性和示范性

通过运维研发化探索实践，形成一套从需求管理、敏捷开发、价值运营的运维研发化标准工作流程，从而实现全过程的标准化、规范化、可视化。组建自有三师团队形成“一个”可迭代、增量式、高效协作的研发工作机制，推动业务人员从应用的使用者向设计开发者转变，营造良好转型氛围，提升员工认同感、激发组织转型活力。建设开放、安全、可信的“一体化”支撑工具链的“3 个 1”运维研发化体系，支撑各类应用的敏捷开发和高效运维，实现网络运维降本增效、提质优服、价值变现的目标。

3.超级自动化驱动的 JKSTACK Workflow 工作流治理

（1）案例背景

某金融证券客户数字化转型过程中出现了组织变革下融合团队的诞生，即应用运维团队。其起到了承上启下的作用，承上包含两大服务内容：（1）服务于分支机构的营业厅人员，来支持围绕业务应用

的技术问题咨询服务。（2）服务于企业内部的业务团队、运营团队、管理团队提供业务运营的服务，如业务账户属性变更，业务数据报表查询等。启下主要负责所有业务应用的 SLA 保障。这种模式下主要面临的问题是没有很好的工具对现有工作进行支撑，主要存在的问题如下：

- 目前只是作为一线服务台，遇到具体问题与故障需要转派升级至其他技术与业务部门解决，部门价值低；
- 无工具支撑留痕，工作不可量化，不可评价，不可精进；
- 百项服务内容为线下操作，无流程管控，对服务质量与 SLA 无法跟踪；
- 知识无法积累，一线问题拦截率低；
- 服务内容重复工作量大，服务流程执行效率低；
- 信息化系统众多，无法统一编排管理；
- 各分支机构的服务支持通过技术论坛问答的方式，客户响应时效低，服务体验较差。

（2）解决方案

通过导入“企业级工作流”的业务流程自动化能够实现企业的数字化运营和 CIO 角色的转换。JKSTACK 企业级工作流套件是超级自动化的各种能力的封装和串联，产品形态上符合 Gartner“超级自动化”定义，关联机器学习、低代码、RPA、iPaaS、iBPMS 等多种技术能力形成编排和自动化业务应用的能力，同时借助 RPA/iBPMS/iPaaS 的自动化能力和数据观测的辅助实现完整的业务

流程自动化和智能化。在产品形态上，JKSTACK 工作流更像是一个枢纽，连接聚合各种技术能力并调度到需要的场景中实现自动化能力，而不是一个直接集成其它能力和应用的平台。通过连接多种技术、工具或平台进行编排，业务驱动的超级自动化可以最大化的快速识别各类业务和 IT 流程并使其自动化。超级自动化可关联机器学习、RPA（机器人流程自动化）、LCAP（低代码应用平台）、iBPMS（智能化业务流程管理套件）等创新性技术，充分利用其组件能力在企业整体层面进行业务流程自动化、低代码开发、流程挖掘、数据建模与数据分析、业务规则与决策管理、任务管理与协作、情景理解与行为历史等一系列数字化运营实践。

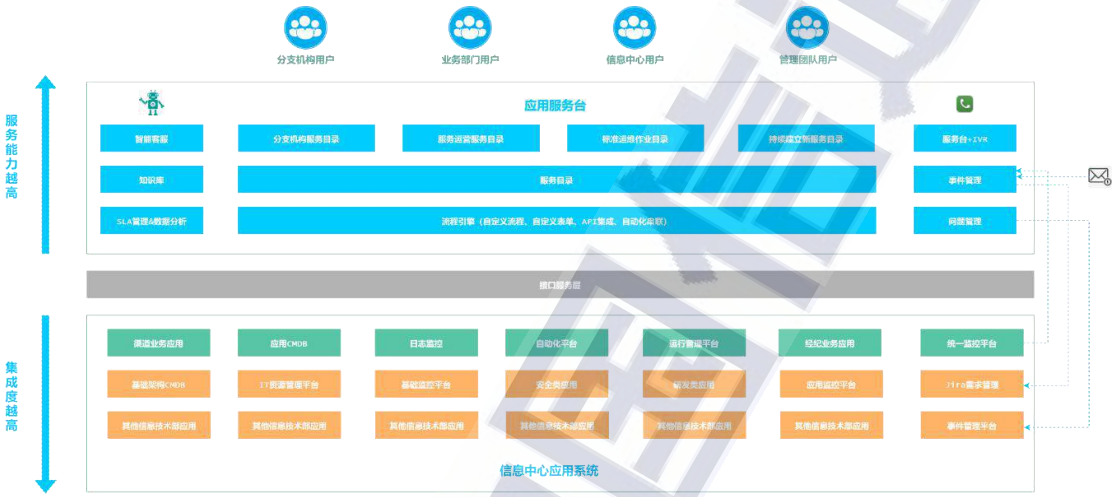
“工作流”是精鲲产品方案中实现数字化运营的基本单位，工作流套件把不同业务场景下的工作和系统操作按照逻辑顺序进行编排，并且以自动化的方式执行整条流程，而且还能按照业务逻辑在必要环节加上负责人审批机制保证合规与安全性。

（3）应用场景及治理效果

部署精鲲数字工作流平台，建设了统一服务台。针对不同服务对象建立不同的服务目录，将百项服务内容和分支机构的服务支持进行服务目录梳理与整合。并通过低代码、自动化技术，打通后端部门各类运维/运营/业务系统，通过服务运营团队将后端 IT 能力整合统一对外提供服务。

针对分支机构的技术问题咨询，提供了智能客服（关联知识库）和自助式的服务目录来支撑服务，提升了客户体验和一线拦截率。针

对业务运营服务，通过服务目录自动化和智能化，释放大量重复人力，有更多时间关注业务创新。针对业务应用的 SLA 保障，建立事件、问题、变更的闭环流程，对故障进行追溯持续精进应用可用性，并使用流程自动化编排完成了自动巡检、监控运营分析、告警工单自动派发等场景。



来源：精鲲

图 11 基于工作流的企业统一服务台

服务对象决定服务目录高度，可以统一整合其他 IT 和业务部门的信息化系统的能力，面对业务服务需求变化具体快速构建一个新的业务流程的能力，团队价值得到提升。

通过连接第三方 ITOM 工具集和业务应用，将服务目录背后一系列的动作和跨平台的操作自动化的手段来赋能企业，提供顺畅、标准化的 IT 服务体验，并从 IT 运营视角得到的数据为业务提供指导。使用流程挖掘技术，对现有流程进行分析，对流程进行优化与再造。

对于组织管理而言，当没有统一服务平台的时候，各个部门重复造轮子。现在统一服务台可以把各部门的信息化能力整合，各部门只

要关注自己领域的建设即可。

（4）创新性和示范性

组织变革下，会出现越来越多的融合团队，而融合团队需要融合工具的支撑，数字化工作流是一个很好的平台支撑。

数字化工作流和超级自动化的理念在案例里得到印证与实践，以服务目录作为服务和价值输出的媒介，通过低代码、自动化、iPaas 等技术对人员、信息化系统、数据进行混合编排，快速交付服务与价值，并通过流程挖掘分析和精进，对于服务对象提供智能客服进行自助式服务，提升用户体验。

针对组织面临不确定性和新需求时，组织用于敏捷力使用数字化工作流能力快速构建新的业务流程和服务提供价值。

随着组织数字化转型的不断深入，数字化工作流会因为衔接组织越多，整合信息化系统越多，平台价值也会越来越大，因为组合的可能变多了，增量价值的场景也随之变多。

4.紫羚云一体化科技运营助力研运提质、增效、控风险

（1）案例背景

某网络银行在 IT 运营管理和研发方面存在问题：研发一体化平台与研发生产环境相互独立，无法实现项目的透明化管理，无法实时了解项目的进度、风险、成本等要素；对人的依赖，尤其对外包的依赖较为严重，无法有效沉淀知识；从需求收集到投产，平台审批流程环节较多，拉长了产品的交付周期；未将质量管理环节化整为零的渗透到日常开发工作内，质量风控仍在软件生产全流程的偏后阶段；开

发、测试、预发、生产等各类环境归属于不同部门或团队，无法设定标准化基线，环境部署充斥着大量的、非标的手工操作；代码分支管理较混乱，项目组各自为政，代码基线与投产介质货不对版。

（2）解决方案

● 通过引入咨询服务，建立 DevOps 规范和度量体系

为保证交付流水线可实施，该行建立了一系列技术规范、应用模型和实施指南，为应用产品快速实现 DevOps 应用提供技术指导。建立了成熟度模型，形成 DevOps 评价体系，为 IT 工艺提升提供改进机会。规范敏捷开发、持续集成、持续交付等过程，形成组织级的规范要求。通过建立应用模型，实现敏捷需求分析、迭代活动、版本控制、构建实践、自动化测试、代码质量控制、部署发布、运营监控等关键活动的自动化和工具化。

建立 DevOps 应用平台管理实践过程，实现信息的可视化，从而促进开发、测试、运维过程向标准化、一致化、自动化和智能化的方向发展。

建立该行 DevOps 评价体系，以评价应用产品在敏捷开发、持续集成、持续交付、应用运营等环节具备的过程能力，持续改进。

● 建立“端到端”交付流水线

依托现有的一体化管理平台，对研发管理模块进行升级，并在研发管理和其持续集成/发布工具之间新建一层控制软件，将一体化平台与 CI/CD 工具链进行打通“端到端” 交付流水线，形成以交付为核心的开发、测试、运维一体化流程，使产品交付更加快捷可靠。

完成该行核心应用系统产品在“端到端”交付流水线上的应用，实现全过程一体化技术的突破。每条交付流水线，贯穿从需求到运维的 IT 实施过程，包括敏捷需求分析、迭代、版本控制、构建、自动化测试、代码质量控制、部署发布、运 营监控等工程活动。

通过提升交付流水线上各工程活动自动化能力，提升整体工艺水平 ；通过交付流水线，促进部门间协作融合，实现应用产品“端到端”的交付 ； 同时依托流水线，搭建该行开发中心和运行中心之间协作的桥梁，实现信息透明共享，变更可追溯。围绕任务管理、开发管理、配置管理、测试管理、环境管理、运维管理等领域，通过引入自动化工具应用，建立该行“端到端”交付流水线上的工具链。

（3）应用场景及治理效果

推进科技管理能力提升，提高项目发布速度，缩短开发周期，不会产生直接的经济收益，但在如下领域可取得显著的管理收益：

● 提质

将针对持续集成规范建设、信息安全相关重点领域进行制度流程精细化深度咨询梳理，并将咨询成果比如开发管理一体化、持续集成、开发安全等举措固化落地在软件平台中，通过系统化、标准化的运作，确保管理举措执行的有效性。

● 增效

通过一体化平台的管理下沉以及 DevOps 应用，提升了协作能力，降低了流程审批、人工操作、低效率沟通等成本，可以投入更多成本在真正的交付价值中。二是可实现版本的持续快速发布。通过

DevOps 应用，由以前的大变更、按批次交付版本，调整为小变更、按业务需求随时交付。 三是对业务发展的促进作用。在 IT 具备了快速交付上线能力后，业务部门可随时将新的业务推向市场。

● 控风险

加强数据安全和客户隐私保护机制建设、以及开发过程的安全控制，通过引入安全运营补强科技部内部科技风险三道防线建设的人力缺口，能更好地应对监管要求，提升监管评级。

（4）创新性和示范性

企业科研运维一体化平台覆盖 ITSM、安全管理、业务连续性管理、投产指挥管理、DevOps、研发项目管理、CMDB 自动化及数据治理等领域。目前已在金融、互联网、物流、智能制造等行业进行应用，服务各行业的大型灯塔客户。随着平台的智能化水平，对于降低客户的管理成本，提高管理效率，降低人机耦合度，具有重要意义。而将行业经验与知识利用通过系统平台进行数字化沉淀，将大幅提高对客户服务水平，对于整个行业都起到了重要的示范意义。

5.中冶宝钢智能化运维提升企业“智造”水平

（1）案例背景

在中国“智造”大背景下，中冶宝钢提出智能化运维是公司提高核心竞争力的重要途径。通过推进智能化运维，优化生产组织模式，提高作业效率；同时通过信息化的手段将每天上万条的施工信息数据通过收集、归纳、总结、运用，使数据自动转化为信息、信息自动转化为知识，知识自动转化为智慧。通过知识的持续沉淀、固化、迭代、

提升和传承，进而实现将现场的经验优势、施工技术优势转化为核心竞争优势，提升企业核心竞争力，推动企业高质量发展。

（2）解决方案

为了满足智能化运维业务需求，也为未来的系统扩展和集成创造一个可持续利用的 IT 架构，根据目前业界先进的、成熟的系统架构设计理论、规范和标准，采用由接入平台、云平台、多云智能管理平台、数据中台、技术中台、统一门户、业务应用系统共七个部分组成的系统技术架构体系，同时将信息化整体规划贯穿于系统架构的各层面中，从而保障整个系统安全、平稳、有效地运行。总体构架设计如下图所示：

来源：中冶宝钢

图 12 智能化运维整体架构

（3）应用场景及治理效果

智能运营平台是实现数字化业务运行落地的载体，包括敏捷的业务应用、中台化的基础平台支撑，以及集成了包括物联网 IoT、人工

智能、BIM、区块链、大数据、边缘计算、移动 5G 计算在内的新兴 ICT 技术在内的信息网络。

通过构建以人、财、物、业务数字化管理为核心的公司级智能运营平台，并对接现有各系统，实现“业财一体化“的信息互联互通。从而，以整合的数字化能力，支撑公司业务的高效率运行，促进公司业务的持续创新与长期演进。

基于**检修业务**实现全流程的信息化，全面渗透检修项目各系统、单位、人员的业务应用场景，形成标准化、数字化和智能化为一体的检修平台。实现全流程标准化、数字化管理，提升效率；施工信息、检修项目状态、物料消耗和人员评价实现可视化；实现关键设备检修项目三维施工模拟，设备状态实时监测。

支持整合中冶宝钢现有信息系统的数据资源，覆盖运**维常态监测监管、远程指挥**等多个业务领域，凭借先进的人机交互方式，实现数据融合、数据显示、数据分析、数据监测等多种功能，可广泛应用于监测指挥、分析研判、展示汇报等场景。支持集成视频会议、远程监控、图像传输等应用系统或功能接口，可实现一键直呼、协同调度多方警力资源，强化指挥管理部门扁平化指挥调度的能力，提升处置突发事件的效率。

（4）创新性和示范性

● 打造基于全流程信息化的智能检修新模式

实现项目智能分配、方案智能推送、可视化交底、现场视频监控、过程管控移动化、验收结果自动记录等功能，同时应用 BIM、AR/VR

等先进技术，辅助检修作业、员工培训、远程指导，助推检修管理模式发生根本变革；通过设备运维数据的积累和知识的沉淀，形成一个知识可共享、数据可复制、功能可推广的智能化检修新模式。

● 研究智能诊断技术，形成技术储备

把长期的设备运维过程中积累的大量设备故障案例进行信息化、知识化处理，并设置一定的逻辑关系规则，形成故障诊断系统，辅助点检人员进行设备故障诊断。

● 建设公司级的智能化运维示范项目

建设一个涵盖“智能检修、智能诊断、远程视频监控、BIM 应用、数字孪生、智能巡检、环境监测、备件资材、生产运营”等全场景的智能化运维示范项目，形成可复制、可推广的经验，并开展示范交流活动，进行复制推广。

（二）智能安全与隐私合规

1.蚂蚁集团 AEYE 智能安全分析对抗系统保障业务安全

（1）案例背景

安全领域充满着跟黑灰产、黑客、不法安全研究者的对抗过程，传统的做法主要依赖于专家经验构建，通过一系列规则和策略，生成相应的告警，并进行运营处置。在此过程中，为了保证召回率，部分规则的范围设置地比较宽，命中率比较高，从而带来大量误报。AEYE 智能对抗系统构建了超大数据规模的分析挖掘能力、训练相关模型进行告警降噪，提升运营效率，降低人工成本和处置时长。

（2）解决方案

智能对抗平台采用阿里集团开源 Python 项目 MARS（基于分布式的 CPU/GPU 计算引擎）作为底层数据计算引擎，集成 GRAPE 图关系挖掘分析平台作为图计算平台，开发了涵盖离线及实时对抗的模型算法工具，构建了一套数字可视化交互分析和对抗平台 AEYE。平台实现的核心技术包括 python 分布式计算能力、GPU 加速能力、大规模图计算能力、交互式分析能力、情报能力等。

来源：蚂蚁集团

图 13 智能安全分析对抗系统架构

（3）应用场景及治理效果

AEYE 智能安全对抗系统在安全检测场景中实现综合告警降噪效果达到了 85%+。一方面节省了安全运营团队的运营成本，另一方面系统突出有效告警，降低了有效告警被忽略的风险。此外，系统通过融合情报能力及大数据挖掘算法，探查出一系列专家经验暂时无法覆盖的未知风险，实现安全预警，有效降低企业的安全风险。

在网络攻防、生物核身风控、移动黑产挖掘及溯源等多个业务场

景保驾护航，做到 7*24 小时全时全源多任务并行运行，保障业务安全。

（4）创新性和示范性

AEYE 系统在安全智能领域，针对 AI 在安全场景落地难的几大问题给出了相应的解决方案，并在实际应用场景中实现了很好的效果，具有很好的示范意义，具体为：

● 系统通过构建 python 生态的大规模分布式计算平台，实现 AI 能力赋能安全场景；

● 通过 GPU 等加速引擎，提升算法开发和运行速度，实现提能增效；

● 交互式的前端分析工具，提升开发及运营效率；

● 情报能力结合大规模的图计算及无监督算法助力未知风险的挖掘。

2.字节隐私合规一站式平台助力企业隐私合规治理

（1）案例背景

隐私合规治理涉及多个领域和相关方，且隐私合规和业务的发展一般是互相制约的，在实际执行中面临诸多问题，如：

- 缺乏标准且唯一的数据仓库来管理与隐私合规有关的信息；
- 缺乏易用且覆盖多个相关方的隐私合规评估工具；
- 法规要求、内部政策、技术实施、度量指标之间缺乏可见的联系；
- 缺少有关产品隐私合规性状态的全貌信息；

- 与隐私合规治理相关的执行成本高昂；

字节隐私合规一站式平台通过自动化技术、聚合的数据集以及标准化的合规流程提供一站式隐私合规项目管理和风险治理，对组织内的数据资产、产品技术、合规流程等相关治理活动实施数字化管控。

（2）解决方案

字节隐私合规中心通过数据发现能力、核心产品功能、有针对性的解决方案、通用性和可集成性、以及赋能生态的合作模式为用户提供从底层技术到上层隐私合规风险治理的一体来源：字节跳动

图 14 隐私合规一站式平台应用架构

平台实现的核心技术点有：数据发现、打标和溯源；数据资产扫描和归类；合规风险评估、度量和可视化；隐私合规要求和风险控制点的标准化记录和引用；结合业务 DevOps 机制的合规预判和冲突校验；PIA/DPIA、Privacy by Design 流程承载；合规审计案例归档和查阅；合规状态指标监控；数据主体权益保障相关的合规管理工具等。

（3）应用场景及治理效果

APP 个人信息合规场景，在《网络安全法》、《工业和信息化部关于开展纵深推进 APP 侵害用户权益专项整治行动的通知》等要求下，监管部门要求 App 提供者强化 APP 个人信息保护，及时整改消除违规收集、使用用户个人信息和骚扰用户等落等突出问题。在上述场景中，平台可以承载线上化政策解读内容、转化法规要求为可执行的治理评估点、通过流程下发整改任务、业务定位问题数据资产（比如

SDK、服务等）、治理结果反馈和校验、以及生成半成品治理报告的工作。通过平台的治理活动，相关项目可实现风险治理的 PDCA 闭环和提高执行效率，同时，风险治理活动的结果可沉淀、可分析和可追溯，为业务不断优化隐私合规和数据安全保护相关的治理活动提供基础数据。

个人信息的数据流地图场景，DataMapping 工作往往是通过采访和审计的方式完成，并且每次梳理都仅能完成对存量信息的整理，而对于增量信息，组织往往缺乏流程和技术手段去实现真正的自动化监控和统计。

在上述场景中，平台通过制度、流程、自动化技术以及与 QA 团队的密切配合，不仅可以协助用户快速完成对存量信息的梳理，也能通过自动化监控技术，以分钟级获取业务在关键数据生命周期中的合规变化，比如在新需求中，业务是否在数据收集阶段过度收集了个人信息；同时，增量管控流程完全与产研的 DevOps 机制结合，平台可以协助业务“左移”发现合规问题的时机，最大化降低风险暴露的可能性。除此之外，平台也可以结合监控结果自动地发现与合规预期相悖的冲突结果，再与业务 QA 团队密切配合，协助业务、合规等合规相关方完成隐私合规风险治理的 PDCA 闭环。

（4）创新性和示范性

平台作打破了知识边界，在一个产品上实现了法律、安全、技术等多个领域的信息交汇，为数字化隐私合规领域治理工作提供了标杆价值。另外，平台通过标准化隐私合规要求和控制点，**使法律遵从类**

的治理活动产品同研发类的技术项目强关联，同时，结合业务侧的 DevOps 机制，平台帮助组织低成本的实现 Privacy by Design 目标，进一步实现 DevPrivacyOps 的治理闭环目标，帮助组织实现对数据主体权益保障请求的快速响应。

此外，字节内部建立了用户个人数据全生命周期保护的成熟度模型及度量标准，来体现隐私合规风险治理的效果，具体来说，相关要求覆盖了从用户选择同意到数据销毁全数据生命周期的合规治理能力。字节隐私合规中心结合上述模型和度量标准，不断完善关键合规监控指标，可以为业务人员提供直观的隐私合规水位看板和明确的能力演进方向。

3.中移杭州智慧家庭用户隐私保护实践

（1）案例背景

当前，智能家庭进入快速成长时期，并进一步延伸到家庭安防、社交、教育、娱乐、健康、养老、办公等场景。然而由于智慧家庭网络环境复杂等原因，智慧家庭领域个人隐私信息面临着严峻挑战。目前智能家庭数据安全主要存在以下安全问题和痛点：

● 数据全面、高频采集过程中，存在违规收集、过度收集、未知情收集等问题。

● 智能设备提供服务过程中，也存在数据过度采集、个人信息泄露等问题。

● 智能终端 APP 存在安全隐患。

● 系统存在未授权访问或非法入侵造成数据泄露风险。

为解决上述问题或管理痛点，中移（杭州）信息技术有限公司设计并实现智慧家庭数据安全解决方案。

（2）解决方案

智慧家庭数据安全解决方案，基于内生安全理念搭建端云协同的数据安全运营系统，立足于智慧家庭个人隐私信息保护需求，在智慧家庭终端、APP、网关、网络等软硬件上部署安全能力，并深入融合网络、设备、应用、内容、服务、数据、行为等多层次防护和分析，同时协同云端家庭安全大脑智能分析、业务控制器自动化管控以及家庭安全运营中心的可视化态势感知和运营管理，实现事前检测防护、事中实时监测、事后审计追踪的智慧家庭个人隐私信息全面安全保障。

系统实现终端、网络、云端的安全防护，其中终端侧主要在家庭环境以安全模组、安全插件等方式提供智能终端设备加固安全组件，以 SDK 等方式提供 app 加固安全组件。在后端业务侧通过集成安全设备，如防火墙、NDR 探针、DLP、漏洞扫描等产品，实现管理平台、业务平台、内容平台隐私数据安全风险检测和风险联动处置。在网络侧主要实现智能网关数据隐私保护，数据传送通道数据机密性、完整性保护等。在云端主要实现智慧家庭隐私数据资产识别、数据流转监控、数据风险检测、安全事件处置和集中化数据安全运营能力。

系统基于运营商家庭网络风险数据创新性打造家庭安全大脑分析引擎，针对智能家庭场景下个人信息和数据常见安全风险，利用**动态行为分析、人工智能算法、安全行为基线建模、全网风险情报**等技术实现实时监测和预警。

（3）应用场景及治理效果

通过智慧家庭数据安全解决方案的项目实践，解决智慧家庭场景下由于设备安全设计缺乏、网络场景复杂等导致的个人隐私信息泄露等安全风险，为家庭用户提供隐私信息保护等服务，保障家庭用户财产和隐私安全，全面提升了智慧家庭数据安全防护水平。

（4）创新性和示范性

● 终端设备实现个人信息防护处置

研发轻量级终端设备个人信息检测和防护能力，实现数据采集源头的数据资产有力保护，实现终端上采集的数据在外送和访问过程中提供隐私数据保护，数据违规访问和外送风险检测，实现终端数据向

外移动时隐私数据泄露风险处置。

● 终端设备个人信息访问控制技术

实现终端设备个人信息的安全访问控制机制，实现不同安全等级的数据隔离，采用 Bell-lapadula 模型实现个人隐私信息安全访问控制保护。

● 安全网关数据泄露防护

研究安全接入网关数据泄露防护安全组件，实现家庭出口网络流量高速报文解析和个人信息识别，全网流量个人信息和隐私数据识别准确率达到 95%。

● 云端个人信息切片存储

以家庭为单位实现个人信息“切片”存储，家庭间的数据其物理存储空间、数据访问权限相互隔离，数据访问需要属主用户明确知情和授权。

4.百度隐私合规检测系统助力 APP 个人信息保护

（1）案例背景

个人信息安全是国家数据安全体系的重要组成部分。随着移动 App 完全融入到每个人的生活之中，App 滥用敏感权限、未经用户同意收集个人信息、超范围收集用户个人信息等问题也日益严峻，这导致大量用户个人信息数据被窃取或滥用等恶意行为，给用户个人信息与财产安全带来了严重隐患。这些信息一旦泄漏或者遭到破坏必将造成重大损失和严重影响。因此，加强个人信息安全防护，提高 App 信息安全保障能力，实现 App 安全、稳定、高效运行，是个人信息

保护工作的迫切要求。

（2）解决方案

为高效、低成本地实现 App 隐私合规，百度安全开发了史宾格安全及隐私合规平台（以下简称“史宾格”）。史宾格是业界首款对外提供服务的 App 个人信息安全及隐私合规检测检测系统，依据《App 违法违规收集使用个人信息行为认定方法》、工信部 337 号文及 164 号文、《信息安全技术 个人信息安全规范》（GB/T 35273-2020）等规范性文件、国家标准，并基于 AI 检测技术，深度挖掘 App 个人信息安全及合规风险产生的源头，发现可能存在的收集使用个人信息方面的问题，生成可视化的隐私合规情况检测报告。史宾格检测内容覆盖隐私政策、个人信息收集与使用、用户权利保障等多重维度，可精准识别 App 违规风险点，助力企业高效低成本地完成 App 隐私合规自查，发现隐私违规风险。史宾格目前主要有四大功能点：App 静态扫描检测、隐私合规检测、法规专项检测、专家模式检测。

- App 静态扫描检测

用户在平台上传 APK \ SDK 可即时检测敏感权限的申请和使用情况，可精准识别过度申请权限、冗余权限与代码使用位置等权限调用风险，判断敏感权限使用的合理性。此外，平台还能够检测出 App 内集成的第三方 SDK 及其申请使用权限等情况，轻松解决第三方 SDK 合规难题。

- 隐私合规检测

史宾格梳理了各监管机构发布的 App 违规收集使用评估办法，

如《App 违法违规收集使用个人信息行为认定方法》、工信部 337 号文及 164 号文等，隐私合规检测分为三大维度：隐私政策、个人信息收集与使用、用户权利保障。企业使用 App 隐私合规检测，能够一目了然发现违规情况，输出风险评估报告，助力企业全方位监控违规风险。

- 法规专项检测

在隐私合规检测的基础上，企业可根据实际情况选择《App 违法违规收集使用个人信息行为认定方法》、工信部 164 号文进行专项检测。法规专项检测通过 AI 云端手机模拟 App 在不同环境运行的真实场景，实时监控 App 运行过程中存在的风险行为，并生成专项检测报告，使问题更聚焦，有侧重点地进行整改。

- 专家模式检测

史宾格提供隐私政策、个人信息收集类型、第三方 SDK、产品隐私设计、权限使用行为、数据安全等多重维度的合规性检测能力，以及在不同运行环境下自动化识别产生的违规收集行为，深入发现 App 隐私风险行为，并基于 VPNService 技术的应用流量监控方案，自动分析出 App 在网络数据传输过程中是否上传了个人敏感信息，并实现定位到具体的服务。

（3）应用场景及治理效果

史宾格经过长期的实践与技术积累，凭借发现 App 违规收集使用个人信息的自动化检测能力，具有广泛应用场景，并取得良好的治理效果：

公司内部应用：百度 App 上线前需要通过史宾格的隐私合规检测，史宾格作为检测工具嵌入研发流水线，以便开发人员在发版前能够发现问题，定位问题并及时解决问题。

应用市场：提供拥有高效并行处理任务集群的定制化接口，在不破坏原有运营框架和平台体量的情况下精准定位风险。对平台内上架的 App 落实管理责任，严格上架审核流程，发现违法违规 App 并及时处理。

App 开发企业：结合企业特色及监管要求，以 SAAS 服务方式为其他 App 开发企业提供商业化服务，一站式解决企业 App 矩阵隐私风险治理问题，帮助这些企业建立全面高效的隐私合规监控和管理体系。

App 开发者：自动化检测出 App 及第三方 SDK 的敏感权限申请和使用宏观现状，多维度测评隐私数据收集、使用、存储、传输的个人信息保护完备性，帮助中小 App 开发者快速发现、定位并解决 App 隐私合规问题。

（4）创新性和示范性

史宾格的检测覆盖隐私政策、个人信息收集与使用、用户权利保障等多重维度，可精准识别 App 违规风险点。史宾格的使命是用科技让隐私保护和合规更简单，其创新和先进性体现在如下方面：

- 业界首个全自动化 App 合规评估技术；
- 将个人信息保护相关法律法规智能映射到 APP 收集使用个人信息的相关行为检测上；

- 基于 NLP 技术构建的隐私政策文本理解能力，智能判定隐私政策文本合规性；
- 业界首个满足不同类型隐私数据识别能力，全面支持设备型、用户输入型和云态隐私数据识别；
- 业界首个基于 ARM 云手机集群的大规模可扩展的全自动化合规检测平台；
- 提交相关发明专利申请 12 篇。

（三）新技术治理

1.阿里云 Landing Zone 实现高效云治理

（1）案例背景

企业云上存在很多治理风险，如身份风险、成本失控、管理挑战、合规风险等。身份风险有共享使用账号、AK 被传 Github、离职员工恶意操作；成本失控风险有成本可见性差、闲置资源浪费、预算难以管理；管理挑战风险有账号和资源管理混乱、网络冲突混乱、人肉运维效率低等；合规风险有符合法律法规要求、内部合规要求等。

（2）解决方案

阿里云企业上云框架中 Landing Zone 源于大量客户的最佳实践。它可以体系化的管理与治理框架并缩短企业上云准备周期。方案包含 8 个模块的最佳实践和可快速搭建的开源代码工具。

- 财务管理：统一付款、费用预警、成本分析、成本优化
- 资源规划：账号架构、资源标识、账号工厂
- 身份权限：身份管理、授权管理、访问安全

● 审计合规：事前预防、事中发现、事后审计

● 网络规划：云上组网、网络互联、公网出入、网络安全

● 安全防护：主机安全、网络安全、数据安全

● 运维管理：配置管理、监控管理、日志管理

● 自动化：部署自动化、管理自动化、治理自动化

（3）应用场景及治理效果

阿里云 Landing Zone 企业适用以下场景。

● 可扩展的多账号架构：基于企业组织和业务需求，规划云上的账号架构，满足企业未来业务扩展的需要。

● 企业及网络架构规划：帮助企业以长期视角规划网络构架，保障其灵活性、安全性、易维护性可满足业务长期发展需要。

● 满足安全合规要求：定制化设计云上安全体系，帮助企业满足访问安全、网络安全、数据安全、操作审计等安全合规要求。

● 企业云成本管理：设计云上成本管理方案，可持续对企业的云上开支进行系统分析和降本优化。

（4）创新性和示范性

阿里云 Landing Zone 是企业可参考及实施的上云体系化框架，为企业提供包含身份管理、资源管理、网络规划、财务管理、合规审计、安全防护的云上 IT 顶层架构设计。帮助企业构建安全、可管理、可扩展的云上环境，为业务规模化上云打下良好的基础，确保上云后业务高效敏捷、安全可控。

2.恩耐博慧见 AI 模型全生命周期管理发挥模型价值

（1）案例背景

模型平台又称之为数据科学平台（Data Science Platform），是完成机器学习及相关高级分析的软件，其功能包括对多种数据源和数据格式进行数据探索；提供各种建模工具进行机器学习的模型构建、验证、测试、部署、监控等功能。模型平台的主要作用是提供完善的工具包，可以使数据分析者通过机器学习将数据的价值挖掘出来、并能够让不同业务场景使用和监控结果。

（2）解决方案

模型全生命周期的管理，提供完善的模型能力（包括自动化构建、交互式构建、图形化构建等）、部署（包括云部署、大数据环境中的部署、批量部署、一键部署等）、监控（包括模型性能、模型业务价值的实时监控）、更新（包括自动化更新、自动化重建等）。其特点包括：

● 开放的、可生长的生态

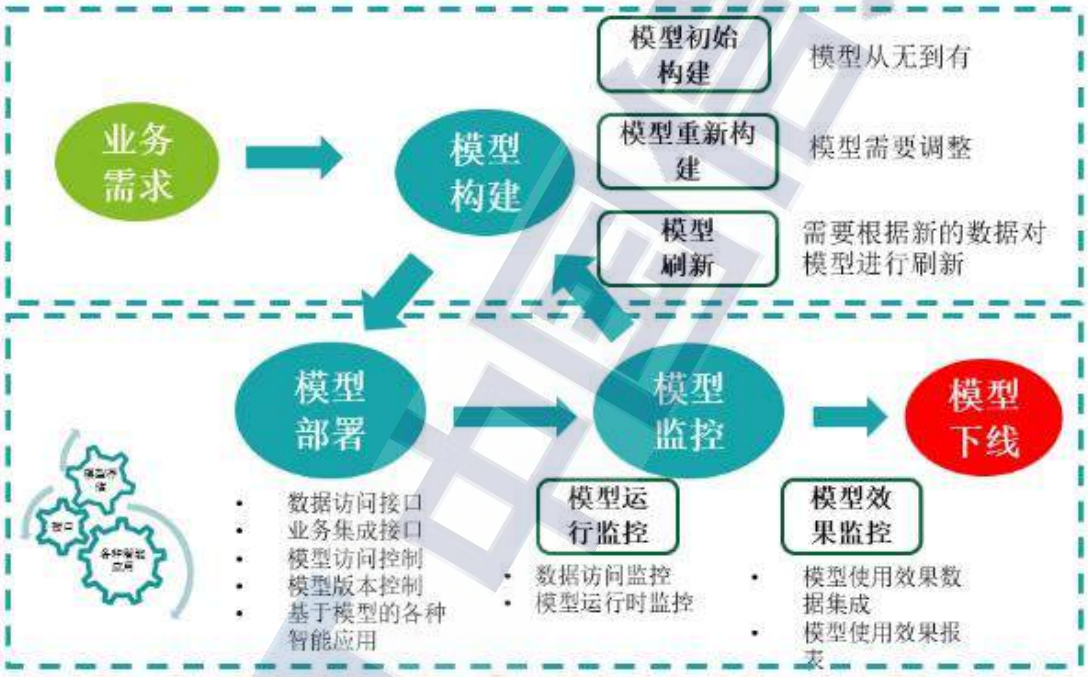
恩耐博在设计模型平台时，瞄准如何解决实际问题，提出“开放的、可生长”的理念，可以随时更新最新的算法工具、将最领先的技术引入到实际业务中。

● 全用户类型支持

建模分析人员由于角色、水平、偏好等不同，所使用的的工具也是不同的。恩耐博的模型平台通过提供自动化建模工具，支持业务人员建模；提供图形化建模工具，让初学者也能快速建模；提供交互式建模工具，让自身的建模人员可以随心所欲地建模。

● 全生命周期管理

模型构建、模型部署、模型部署的模型全生命管理，是恩耐博模型平台的核心特点。模型构建功能以“开放的、可生长”的形式提供最新最全的建模算法库和工具库；模型部署提供领先的基于最新云计算技术的“一键式”部署功能；模型监控提供 IT 监控、模型性能监控、模型业务效果监控三种全面的监控。



来源：恩耐博

图 15 模型全生命周期管理

● 高度自动化

恩耐博模型平台提供完善的自动化功能，包括建模自动化、部署自动化、监控自动化、更新自动化。建模自动化采用最领先的技术，只需要提供数据集即可完成模型构建；部署自动化提供领先的基于最新云计算技术的“一键式”部署功能，自动生成 API 供使用；监控自

动化是可以实现数据自动收集、模型效果自动监控、模型报表自动生成；更新自动化是指能够完成模型自动化刷新、自动化重建。

● 超强稳定性

由于采用最先进的云计算技术实现模型全生命管理，特别是模型一旦部署，由于云计算的特点模型部署后的服务几乎不会掉线。这种特点提供了超强的稳定性，适合企业级应用。

● 自更新、自学习

恩耐博模型平台实现了基于模型监控的模型自动更新、自学习的核心技术，并在多个场景检验有效。

（3）应用场景及治理效果

● 模型线上化

机器学习模型、人工智能模型、各种统计模型都可以借助于“慧见. AI 模型管理平台”的模型部署模块以线上服务的方式发布。模型线上化的益处是大幅降低模型应用的开发成本、并且将模型构建的知识能够体系化标准化地存储。

● 模型白盒化

模型结果在发布给业务部门时，业务部门往往期望知道模型输出结果的业务依据，并据此可以提高业务决策水平。通过“慧见. AI 模型管理平台”除了能够输出模型的结果，也能输出相关的业务数据，能够明显增强业务人员使用模型结果的信心。

● 模型自动化

模型的构建、部署、监控、更新在“慧见. AI 模型管理平台”都

提供了相应的自动化能力。“慧见.AI 模型管理平台”在客户现场实施时发现，基于其自动化建模的工具在模型质量、建模效率方面都大幅提高。最近的案例都表明，预测类的基于自动化建模技术构建的模型，其性能指标明显优于企业的数据科学家的模型，且模型构建过程只需在“慧见.AI 模型管理平台”点击数下鼠标即可完成。模型构建的时间由数周缩短为 1 小时之内。

● 模型可审计

“慧见.AI 模型管理平台”支持全面的模型审计需求，包括模型构建的人员投入、数据使用情况、模型被使用的情况、模型的准确性、模型产生的业务成效，以及构建模型的知识积累、模型源码、模型文档、模型的不同版本等。模型的全生命周期所有过程在模型平台上都留有各种数据。

● 模型管理流程规范化

模型的全生命周期管理在企业内部实施过程中需要配套相应的管理机制，比较常见的管理机制是模型构建、上线申请及批准、模型发布是不同的人员。模型构建需要数据科学家、业务人员共同参与；上线申请和批准是部门管理人员，在对模型结果和测试了解的基础上同意模型上线；模型发布主要依赖于 IT 人员通过模型平台的配置实现模型服务的发布。

（4）创新性和示范性

模型平台的亮点包括：

● 开放而不是封闭；

- 模型的真正全生命周期管理；
- 模型管理流程完善且可定制；
- 模型可审计；
- 自动化技术。

（四）法律科技

1.东华软件法务合规系统赋能企业法务数字化转型升级

（1）案例背景

BS 公司作为一家大型国有企业，长期以来高度重视企业法律风险管理与合规治理工作，组建了相对**完善的法务合规管理组织体系，**制订建立了一系列相关管理制度与流程规范。但随着监管要求的提高以及内部管理需求的激增，传统的管理模式已经在效率、质量、成本、及价值提升等方面都显得日趋艰难。为进一步提升法律服务效率、加强企业法律风险控制、提升企业合规治理水平，实现企业法务管理向信息化、数字化、智能化方向转型，BS 公司与东华软件深度合作，推出的新一代企业法务合规管理数字化平台，实施建设了符合 BS 公司管理实际的法务合规数字化平台，覆盖**法律审核、授权、案件、普法、法律队伍、工商事务、知识产权、合规管理**等八大模块，并结合第三方法律大数据平台，**无缝集成法律法规库、司法案例库、企业工商信息库等**，使法律科技赋能于企业法治建设与合规治理细分领域，实现企业法务管理数字化转型升级。

（2）解决方案

- 技术构架

法务合规系统针对不同的应用场景，围绕连接、数据、智能应用要素，构建了多层次、多维度、组件化的体系架构，系统架构的逻辑分层架构分为：数据存储层、数据服务层、抽象业务组件层、具体业务层、多态客户端。

● 主要功能模块

法务合规信息管理系统的主要内容是建设“**一个统一系统、八大业务模块、三大工具模块**”。

“一个统一系统”是指建设集法律管理、决策监控和学习交流三大功能于一体、贯通集团公司及各级企业的统一法律事务管理信息系统。**“八个业务模块”**是指法律审核、授权管理、案件管理、普法宣传与法治文化管理、法律队伍管理、合规管理、工商管理、知识产权管理。**“三大工具模块”**是指法律法规库、案例库、工商信息查询辅助模块。

● 核心技术点

通过一体化平台达到纵向到底、横向协同。纵向到底实现公司总部层面对全公司二级企业的法律事务进行统一监控；横向协同实现与企业门户、合同管理系统、企业微信的集成融合，实现数据互联、功能互补。

连接涉及的技术范围非常广泛，包括人与设备、人与计算机、计算机与计算机、设备与计算机中间的连接。通过泛连接，保证了用户在线协同的广泛性，业务响应的效率和广度得到了保证。

通过混合使用大数据技术和传统关系型数据库、文件型数据库，满足实际的业务要求。传统业务数据入库时，数据采集引擎将业务数

据再度加工，存储到大数据仓库，建立传统业务数据与大数据仓库数据集关系。前端业务数据检索混合使用大数据查询技术及传统关系数据库进行多线程的二次检索，形成有效的结果集。

采用智能推送技术，分析具体业务过程，形成有共识规则，将规则按照特定的逻辑存储。发生新业务时，对新业务进行针对性的分析提取，自动查询检索与警示，推送到业务操作界面。

提供完整的二次开发能力支持，便于系统使用过程中能进行系统功能调整和修改，平台支持低代码开发平台、自由开发平台。

（3）应用场景及治理效果

一方面，结合企业实际性质，对事项类型进行全面梳理划分，基于事项类型梳理定义“送审材料规范”与“法律审核要点”，并**嵌入到系统的审核流程之中，实现操作指引提示及要素识别控制**，为数据规范管理和法律审核质量提供了保障；另一方面，通过**采用自动分词检索技术**，对事项关键要素进行智能解析后，智能识别推荐相关法律法规、规章制度、及历史类案。

通过梳理分析全公司各类业务的合同类型，及定义各种类型的审核要点，结合**智能审查工具**和相关法律法规、历史类似合同智能推荐等方法，为**合同法律审核提供智能辅助手段**，大大提升了合同审核工作效率与质量。

采用“业务主线”管理思维设计案件管理产品，构建从案发登记、方案策划、庭审准备、进展跟踪、审判、执行、到结案归档的“全景式”案件数字化管理体系，为案件承办人和企业管理者提供**全景可视**

化的案件管理方案，提升了办案效率和质量，降低了诉讼风险。

一方面，通过结合企业各类型案件特点，平台采用**智能问答机制**，引导承办人对案件诉讼方案做出更加全面的响应与深入的分析思考；另一方面，借助分词检索技术，结合第三方社会化大数据平台，智能推荐相关法律法规、类似案例、及办案知识等，为诉讼方案准备及案件办理提供辅导，降低了办案难度。

通过系统平台将合规义务、合规知识、风险控制规则、风险提示等内容与业务过程活动相融合，在业务处理过程中，精准进行关联控制、预警提醒、和知识指引，真正**实现业务、合规、风险一体化管理**，为整体提升企业内部管理水平提供技术支撑手段。

通过平台支持在线普法课堂学习、在线法律考核、专题普法宣传、法治文化宣传、法律知识推送、以及在线法律咨询，并在移动端与企业微信等产品进行连接集成，可实现员工普法全员覆盖，为企业员工法律学习和法律意识培养搭建了便利的桥梁。

（4）创新性和示范性

通过法务管理的模块化、表单化、流程化、集成化和智能化，将依法合规管理要求固化到业务流程和审核审批环节中，动态、全景式地展现每一项法律业务的流程进度，增强管理的透明度，提高工作效率。

通过设立法律法规库、案例库等辅助工具，为功能模块提供知识库指引，为法律业务人员提供专业知识支撑，提升法律人员专业知识水平。

通过对法律各业务板块全面的数据共享、分析及过程管控，辅助公司降低和规避经营管理和决策环节存在的风险，将现有分散的信息孤岛通过系统集成对接，实现数据大融合，为领导层决策及职能部室提供管理及数据支撑。

通过所属企业业务跨级审核、重要事项及时上报及数据报备的方式，实现公司总部对所属企业法律风险的监督管控管理，实现自主可控+集中管理，建立全方位、全过程、全层次的法律风险防范体系和合规管理规范体系。

2.智慧法务管理平台助力 360 集团一体化法务管理体系建设

（1）案例背景

为解决法务工作如下难点，360 采用技术手段实施开展法务相关领域的治理工作，研发上线 360 法务管理系统，助力一体化法务管理体系建设。

法律风险防范难。企业法律事务工作依靠手工管理，数据不准确、处理不规范、审批效率低，无法有效防控法律风险；

工作落实、跟踪难。集团各单位法务管理职责不一致，又缺乏统一协同的平台，没有一个部门可以掌握法务管理的全过程，工作执行过程难以跟踪，容易引发企业管理风险；

工作协同难。跨总部部门间、总部与所属企业间，缺乏统一协同工作的窗口，导致各部门工作相互孤立、协同困难；

知识共享效果差。企业缺乏统一的法务知识共享平台，法务管理

经验、成果等内部知识分享机制较差，不利于法务管理工作的提升；

企业法务管理数据很大程度上依靠人工上报和汇总，**缺乏统一的法务数据汇总平台**，无法有效支持管理者和领导者的科学决策。

（2）解决方案

● 建立智慧法务 PAAS 平台

360 智慧法务是基于自主开发统一的 PAAS 平台结合内部业务以及外部客户的实际需求研发的应用系统，系统融合和了先进的低代码开发技术，实现用户的全天候的多终端办公的应用场景，并且提供独立的移动法务管理门户，把法务管理数据的展示业务的办理有机结合起来，通过专业的数据仓库工具为领导以及用户提供法务业务个性化的数据统计分析展示。

● 建立一体化法务管理体系

提供包括合同、证照资质、案件、知产、投资并购、印控等各种法务管理业务，形成一体化的法务管理体系。提取各类管理报表，能更快速、准确地对法务管理业务信息进行采集、核对及分析，为公司管理决策提供服务。通过构建基于集团/企业的一体化法务管理系统（支持集中式及分布式部署），实现法务管理业务动态的实时化掌控，实现工作效率的跨越式发展。借助此平台达到各级部门之间数据共享、降低法务工作劳动强度、提高工作效率。

（3）应用场景及治理效果

通过智慧法务管理平台建设，构建一体化的法务管理体系，建设适应各类企业发展所需的“技术先进、功能强大、性能安全、高度集成”

的综合法务管理平台， 加强和规范企业的合同管理审批业务流程，实时监控合同履约情况，构建完整的企业证照管理库，实现业务审批与静态数据库的高效业务协同，并提供简捷、高效的移动化办公场景。主要实现系统的建设目标如下：

法律风险防范。360 法务管理系统以法律风险防范为主线，将法律风险防范机制落实到法务管理的各个环节中，提高法律风险过程控制能力，实现法律风险的闭环管理。

集团管控和应用。360 法务管理系统利用信息化手段实现法务数据的收集、查询、阅览、台账建立和汇总统计等工作，提高法务管理工作的效率和质量。

信息共享。360 法务管理系统利用信息化系统全面反映集团公司法治工作、诉讼案件、授权管理、知识产权等法务工作的管理情况，实现动态跟踪、自动提醒、汇总统计、查询阅览等工作。

跨领域集成。因为法务管理系统的业务过程与其他业务系统关联度较高，系统需要具有较好的集成性和拓展性，能够与其他系统进行数据和流程交换，实现全价值链。

（4）创新性与示范性

360 法务管理系统是在通过与各行业大中型企业用户进行访谈、交流与探讨、深入细致地对企业法务管理相关业务进行研究分析的基础之上建立起来的，其具有多元化、集团化、全面化、个性化的优势和特色，即：基于企业多业态经验沉淀，融入不同行业法务管理的特点；基于最新平台，发挥流程能力和权限管控的能力，加速和保障集

团化的实施；提供企业法务管理总体解决方案，覆盖集团企业法务管理；在总体方案下，灵活可扩展的平台架构支持，支持相应企业的个性化要求。

（五）数字化风控

1.度小满数字化治理下的反洗钱管理体系建设

（1）案例背景

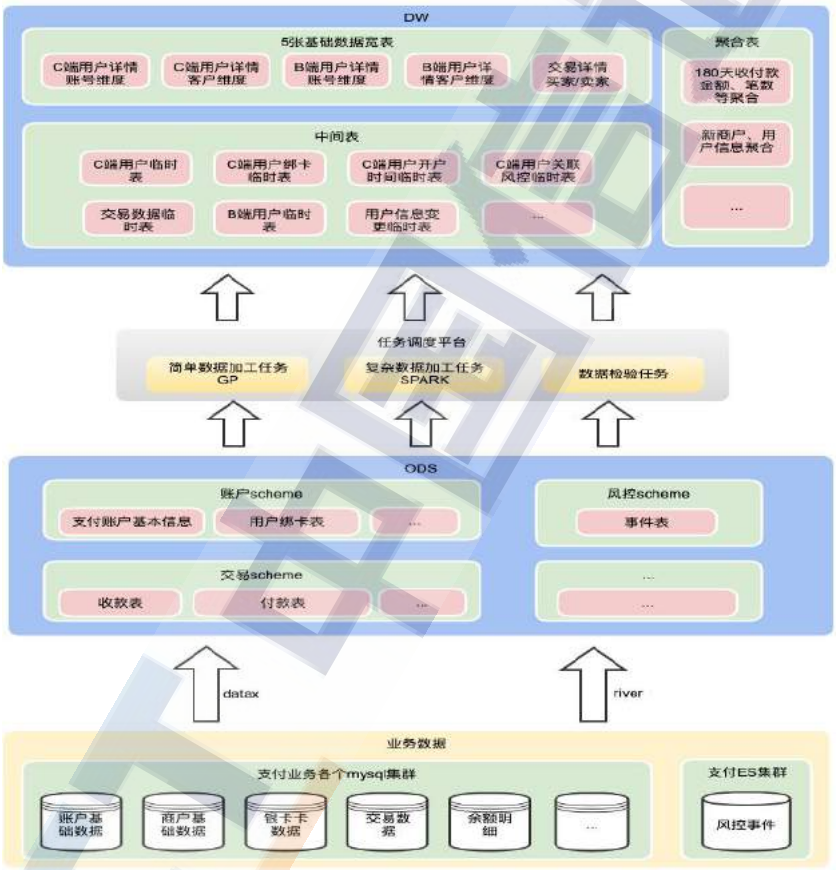
当前，金融机构反洗钱工作资源投入在不断进化的洗钱手段、庞大的业务量与日益复杂的业务模式面前呈现短板，规则系统的迭代速度和可疑案例抓取准确率亦受到了极大的挑战。北京度小满支付科技有限公司（以下简称“度小满支付”）基于监管要求及围绕业务风险，以风险为导向，综合利用大数据、人工智能等技术对可疑交易监测工作进行“微创新”，主要**解决因数据不完整、提取效率低，进而影响高风险客户以及可疑交易识别的准确性问题**；以及**解决因可疑案例准率率低、预警量大，进而影响报送可疑交易报告比例较低的问题**。度小满支付专注于智能决策和分析，不断完善反洗钱交易监测系统，力促践行以“风险为本”的理念开展反洗钱工作。

（2）解决方案

底层数据质量是金融机构可疑交易监测的生命线，为有效解决数据质量问题，运用大数据思维及人工智能等技术构建可疑交易监测系统，实现“全方位”监测和分析，提高可疑交易监测模型的预警精准度。度小满支付在以下两方面建设反洗钱管理体系：

- 反洗钱数据仓库

度小满支付通过整合各类交易信息、客户属性，建立反洗钱数据仓库。数仓使用大规模并行分析数据库 Greenplum（以下简称“GP”）存储数据，通过增加节点提高系统的存储容量和处理能力。各业务数据同步到同一 GP 集群后，通过 SQL 快速抽取、加工、校验数据，对于较复杂任务通过 Spark(分布式计算引擎)处理后可快速导入 GP。



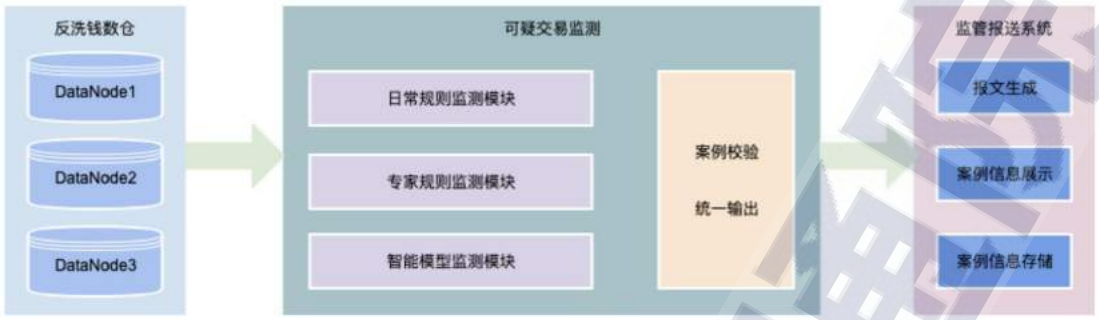
来源：度小满支付

图 16 反洗钱数据仓库架构图

● 反洗钱智能模型

度小满支付结合公司现有的业务场景、拟拓展的业务场景对反洗钱智能模型不断完善，在现有专家规则及日常规则的基础上，增加了机器学习模型，从多维度提升规则及模型覆盖度与识别效率，降低漏

报的机率。



来源：度小满支付

图 17 反洗钱可疑交易监测

度小满支付智能模型的构建根据数据分布的特点选择适合该场景的算法构建模型。可疑交易监测的数据场景最大的特点就是正负样本不均衡，因此度小满支付针对这种场景结合小样本学习、样本不均衡等机器学习研究方向的前沿成果，包括 Borderline-SMOTE（边界合成少数过采样技术）采样、ENN（最近邻采样）采样、代价敏感学习、损失函数重构等技术，分别使用孤立森林算法、LGBM（轻量级梯度提升树）构建了反洗钱可疑交易智能监测有监督模型与无监督模型。

度小满支付通过用户之间的全量交易构建出交易关系图谱，结合 GCN（图卷积神经网络）输出的特征，利用社区挖掘相关算法进行洗钱团伙挖掘。同时，利用交易关系图谱通过算法划分联通子图，对于孤岛类的子图进行过滤。对于每张子图利用 Louvain（基于模块度的社区挖掘算法）算法进行社区发现，从中找出明显具有团伙性质的交易结构并进行指标量化，如链式结构、环状结构等。

（3）应用场景及治理效果

反洗钱大数据构建方面，反洗钱业务开展初期，度小满支付业务数据主要存储在 MySQL 数据库中，为了支持业务高并发、稳定性等需求，客户及交易的数据存储在多个集群的多张库表中，数据存储较为分散，同时交易类型存储也极其复杂，使得交易数据和数据库记录是多对多的关系。从而导致数据提取不全且效率低下，进一步影响高风险客户以及可疑交易识别的准确性及效率。反洗钱数据仓库构建完成后，**数据完整度，数据获取效率、以及规则模型的运行迭代效率均有大幅度的提升**。首先，交易数据完整度从 99.98%提升至 100%，且一系列加密、校验等功能，有效保证了数据的质量。其次，客户风险评级全量客户评级时间从 5 天降低至 2 天；规则系统运行时间从 2 小时降低至 0.5 小时；新增或优化单条规则开发时间从 4 天降低至 0.5 天。

最后，反洗钱数据仓库集数据集成、处理、报警、校验、加密等服务于一体，作为整个反洗钱系统的基石，高效、稳定的支持反洗钱规则系统、评级系统、模型系统、后台审核系统。

搭建反洗钱智能模型方面，度小满支付反洗钱系统主要是利用专家规则识别可疑交易，依赖业务专家对通过不同业务场景分析、风险指标提取、风险指标量化、模型构建等步骤完成规则设计，系统规则的更新、优化成本较高；且规则系统，主要以单主体规则、单主体模型为主，多主体模型预警量少，准确率极低。

度小满支付通过机器学习、深度学习、社区挖掘等前沿 AI 技术在反洗钱风控领域的应用。增强反洗钱监测系统的稳定性和包容性，

以更强的识别能力应对日益严峻的洗钱风险。

（4）创新性和示范性

度小满支付在反洗钱可疑交易监测智能模型的训练中创新的使用了机器学习、深度学习等技术，并将其应用于可疑监测。同时在应对正负样本的占比相差悬殊的棘手问题中，度小满支付采用小样本学习的理论，通过迁移学习、元学习等方法构建深度神经网络。在传统机器学习技术的应用中采用样本比例不均衡问题的相关处理方案，结合相关论文的最新研究成果，综合数据采样、模型融合、自监督训练框架、优化模型损失函数、代价敏感学习等方法，有效提高模型的准确率和召回率，实现了正负样本和难易样本不均衡场景下的有监督模型的训练并投入实际使用。

经调研，由于要满足业务的高并发、稳定性等需求，目前支付机构的数据存储均是分散的。度小满支付反洗钱数据仓库的构建方案可供同业参考，现行构建数据仓库的工具多数为开源服务，依赖的内部服务也可通过其他开源组件替代。数据同步流程可复制性极高，只要理解各数据存储结构，按照前述流程即可构建一套完整反洗钱数据仓库。

2.小米集团数字化风控“灯塔体系”赋能业务促经营

（1）案例背景

小米集团业务遍布全球 100 多个国家和地区，随着业务发展和外部环境的变化，小米面临更加复杂的监管环境，现有风险管控模式和能力已经难以实现风险的有效管控。在此形势下，企业内控面临着前

所未有的挑战：

● 业务发展迅速，业务变化快，业务整体运营趋向于数字化、自动化；

● 业务数据量巨大，从效率效果角度考虑，均需要从传统的抽样方法过渡到全量数据持续监控方式；

● 全方位持续提升管理质量的管理诉求。

小米迫切需要自动、实时、智能的数字化解决方案，通过提升风险管控能力赋能业务，以满足日益增长的业务需求以及复杂多变的内外部监管环境。在此情况下，小米数字化风控合规体系应运而生。

（2）解决方案

小米集团基于内控、内审、合规、监察“四位一体”的建设思路，组建了内控内审监察部。在“赋能业务促经营”的核心目标指引下，以业务风险为导向，结合流程挖掘、大数据分析、NLP（Natural Language Processing）、RPA（Robotic Process Automation）等多种技术能力，开展“风险监控平台”、“持续审计平台”、“合作商合规管理平台”及“数字监察平台”建设，形成小米的数字化“灯塔”体系。在建设上述 4 个平台的同时，也同步考虑到业务管理的诉求，为业务方提供轻量化的数字风控产品，在有效管控风险的同时赋能业务管理。

以数字化、产品化为核心思路，在风险管控的不同环节，开发并应用多样化的数字化风险管控产品，即时识别和响应风险，准确揭示风险隐患和内控缺陷。小米风险监控平台建设，采用模块化的思想，结合行业最佳业务实践，以“搭积木”的方式，不断予以更新迭代，

可灵活适应不同国家、地区的外部监管合规要求及内部快速更新的业务模式与业务管理诉求，从而实现小米全球化、数字化的灵活风险管控。

在风险识别环节，主要通过流程挖掘技术与基于用户行为的大数据分析技术的运用，针对不同的业务场景，建立业务风险分析模型。在风险应对与风险监控环节，通过权限管控与流程管控工具，实时分析监控潜在的异常行为与业务安全风险，并对业务及内控人员进行预警，同时提供风险整改、跟进等管理功能。除以上方面外，风险监控平台还提供了风险事件库、审计发现库等多项工具，用于知识沉淀。

来源：小米

图 18 数字化风控“灯塔体系”

（3）应用场景及治理效果

通过数字化风险监控平台的运用，可有效监控各业务领域的风险情况。以下为该平台的应用与治理效果的简要介绍：

● 流程挖掘工具

流程挖掘工具，是以系统实际数据为基础，提供了业务流程可视化展现能力，从而帮助业务人员及内控团队快速复核业务流程的合规遵从程度，定位出不合理的业务场景及流程，同时还可以快速发现业务流程中的效率瓶颈。例如，针对单据审批的场景，通过各审批流程的可视化展现，**快速解决“审批量大、审批环节长、审批易出错、审批管理混乱”等问题**。

来源：小米

图 19 数字化风控业务流程挖掘和分析

● 持续风险监控

基于在流程挖掘过程中扫描到的业务风险，将控制点/监控点嵌入至业务流程过程中，从而实现对与潜在的异常行为与业务风险的的实施监控与分析，并提供预警、风险整改与跟进等管理功能。例如，在风险识别环节，发现了“早于发票账期的提前付款”场景，则在采

购到付款流程中嵌入监控点，即可实时监控是否存在提前付款的事件，并将发现通知相关人员进行后续的调查、整改与跟踪。

来源：小米

图 20 持续风险监控平台

（4）创新性与示范性

赋能业务为先。在风险防控的目标层面，确保一道防线与二道防线是一致的，都要为业务创造价值，为业务保驾护航。在此基础上，通过内控体系建设，不断提升和改善全公司的风险防控意识，从而将内控规则有效落地。

以信息化为基础，以数据为导向。通过以大数据分析为代表的先进 IT 技术，实现跨业务流程、跨信息系统的海量数据分析，从中挖掘业务风险，并予以数字化监控，可以极大的提升企业内控体系的运作效率，为企业的全球一体化运营提供有力支撑。

3.美团商企通助力企业消费合规管理数字化

（1）案例背景

移动互联网技术改变了人们生活的方方面面，企业员工的日常消费行为与习惯同以往也有了本质上的不同。随着供给侧改革的大势所趋，“企业消费的数字化变革”迎来了更佳的时期。

企业因公消费场景一般由“餐、机、酒、车”四大板图组成。报销繁琐、发票难题、综合管理成本较高、数据不闭环导致内控合规漏洞等现象，是企业消费及管理中最为常见的难题。美团商企通基于对内（美团内部六万名以上员工的用餐、用车、差旅场景）服务经验的沉淀及产品技术的打磨，于 2017 年正式展开对外部企业进行企业级 SAAS 服务的业务模式探索，满足市场需求，助力反腐倡廉。

（2）解决方案

美团商企通企业消费及管理解决方案，基于美团全场景本地生活供应链，为企业提供 SAAS 级费控管理能力。“供给服务、技术服务”一站式供应的模式下，美团商企通为企业客户配套了健全的“供给侧履约质量保障体系”为每一位员工在企业消费场景下的“安全性及稳定性”保驾护航。

与此同时，基于美团商企通 SAAS 管理系统，企业管理者可在事前审批、事中管控、事后报销三个维度进行基于标准能力的管理及控制，实现事前供给资源可配置、事中合规消费规则可定义、事后订单数据可留存于企业内部系统，最终实现全场景企业消费提效降本，廉洁透明。

（3）应用场景及治理效果

基于平台级供给覆盖，可有效帮助企业进行因公消费管理。在插件化、开放性的产品架构设计下，系统可与企业原生系统进行自由耦合。

来源：美团

图 21 企业因公消费数字化管控

在充足的供给资源、完善敏捷的产品能力、全流程数据闭环的优势支撑之下，企业级消费的合规风险识别能力、服务品控能力、综合管理效率，将得到质的提升。

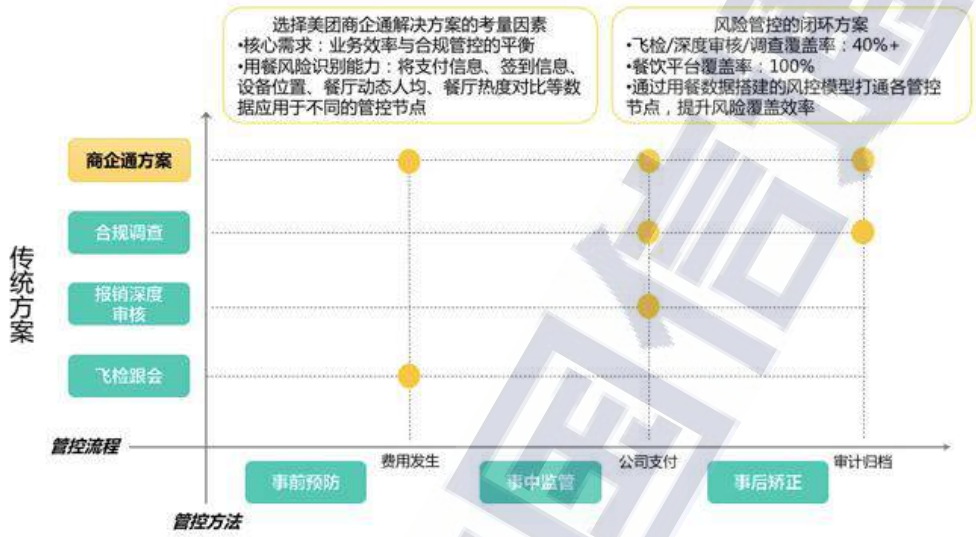
相较于传统的“风控稽核”手段，商企通方案存在明显可见的全闭环全流程覆盖及更低成本更高效率的优势，部分企业治理效果如下：

● 某通信服务商使用美团商企通 TMC 解决方案半年，每笔报销单的综合成本降低 23%；

● 某事业单位使用美团商企通福利发放解决方案，员工福利津贴消费数据每单可于系统中留存，内审外审更合规更透明，支持的消费

场景相较原来的“米面粮油、电影票”，数量增加 500%；

● 美团商企通为美团六万名员工提供了「机酒餐车：一站式服务」，达到员工免贴票（报销只需系统点击确认），财务免审票，报销总成本降低 54%的效果。



来源：美团

图 22 系统级全闭环费用风险合规管控

（4）创新性和示范性

科技向善，反腐倡廉。用技术让企业因公消费管理提效降本，廉洁透明；

高价值低成本。整合本地生活全场景数据，一站式解决企业消费及合规管理痛点。全流程 SAAS 服务，降低企业综合成本。

(六)数字化审计

1.中国宝武穿透式监督之大数据审计

（1）案例背景

为了贯彻落实习近平总书记关于“坚持科技强审，加强审计信息

化建设”的指示精神，践行中办、国办实行审计全覆盖的要求，中国宝武高度重视，及时布置组织研究落实。内部审计是集团对下属公司进行风险管控的重要方式，但是**集团审计存在数据分散、关联查账不方便、审计质量不高、大部分事后人工审计等问题和不足**，导致不能及时监控并发现问题，从而无法及时发现企业日常运营中的缺陷和问题，不利于中国宝武的良好发展。

（2）解决方案

中国宝武针对当前审计的发展需要和存在的问题，提出了**穿透式监督的数字化审计方案**，如下：

● 建立数字化审计“一套运营治理体系”

“一套运营治理体系”解决数字化审计的组织如何建设、数据语言如何统一、数据如何可持续运营治理等问题，从管理层面为中国宝武数字化审计的大数据建设与治理提出统一标准规范要求，为大数据管理、大数据平台组件研发、大数据中心建设等提供体系能力支撑，包括组织体系和运营治理体系。

● 建立数字化审计“一个技术平台”

落实“科技强审”，充分利用数字化技术，研发建设中国宝武新一代审计技术系统。“一个技术平台”是按照集团“构建高质量钢铁生态圈和打造工业互联网平台”战略要求，宝武大数据中心规划并逐步构建了新一代大数据技术解决方案，生态技术平台 ePlat，ePlat 上则体现为 5S 组件，包含“数存(DataStore)”、“数成(DataSucceed)”、“数智(DataSmart)”、“数现(DataShow)”和“数典(DataStandard)”，

简称 5S 组件。

ePlat 技术体系融合了 AI 智能算法框架，引入 OCR 识别、NLP 自然语言处理、ES 搜索引擎等 AI 服务，满足集团数字化、智能化审计要求，提高审计计划、审计方案针对性，提升审计效率。

● 建立数字化审计“一个大数据中心”

基于数字化审计“一套运营治理体系”和“一个技术平台”，按照“1+N”统分结合的大数据中心建设模式、“云+边”协同共建的大数据中心物理架构以及构建大数据中心能力中枢的三层逻辑架构，建设形成逻辑上统一的中国宝武数字化审计“一个大数据中心”，从而**实现数据互融互通和数据能力的共建共享，为穿透式在线提供技术保障**。

依托中国宝武数字化审计“一个大数据中心”，汇聚来自各专业系统与审计相关的所有数据，通过构建横向到边、纵向到底全体系审计数据模型，运用总体分析、发现疑点、分散核实、系统研究的数字化审计模式，对重要内控合规风险进行在线穿透式监督。

（3）应用场景及治理效果

中国宝武的穿透式监督审计系统目前完成**大数据审计框架的搭建以及法人审计画像、损失预警、投资后评价、内控合规审计**等 4 大应用场景。

● **法人审计画像：**从画像总览、法人画像、风险监测、健康检查四个维度全面分析并帮助审计人员快速、全面地掌握公司情况，更加及时、有效地挖掘公司的潜在风险，提升审计效率；

● **损失预警：**聚焦资产减值损失（存货、坏账、长期股权投资、商誉等）、营业外支出（赔偿、罚款、盘亏等）、汇兑损益、公允价值变动损益四大类非主营业务损益，针对 500 万元以上损失账务处理实时预警，及时揭示风险；

● **内控合规审计：**应用 OCR 识别、NLP 自然语言处理、ES 搜索引擎等技术将非结构化数据结构化，整合形成统一的多源数据集合，通过统计分析、勾稽比对、规则预警、历史经验等模型自动化挖掘审计疑点和线索，实现业务招待费等的穿透式在线监督，提高审计的实时性和全面性；

● **投资后评价：**聚焦长投项目后评价总投资、股权交割日期偏差等 7 项指标以及固投项目后评价产量、月达产时间偏差等 17 项指标。

治理效果方面，基于“一套运营治理体系”显著的**提升了数字化审计的数据标准和数据质量，形成内部审计相关的高质量数据资产，**为审计画像、损失预警、投资后评价、内控合规审计应用提供了有效的支撑。通过“一套运营治理体系”，有效的支撑“一个大数据中心”建设，目前 ePlat 已在集团内部启动了 6 个**大数据中心节点建设，并实现了互通互联**。数字化审计应用初见成效，如通过对集团公司 2018 年-2020 年主要非经常性损益开展**穿透式、全覆盖在线审计调查**，揭示了五类需重点关注的问题；业务招待费审计调查，对集团标准财务系统已覆盖的子公司及下属单位 2020 年业务招待费进行了穿透式、全覆盖在线审计调查，发现 3,638 个线索，通过进一步核查，揭示了五类主要问题，提出了相关针对性建议。

（4）创新性和示范性

中国宝武内部审计按照数字化审计的发展目标，建立**适配数字化审计组织架构以及数字化审计的“一套运营治理体系”、“一个技术平台”和“一个大数据中心”，形成数字化审计体系，通过汇聚来自各专业系统与审计相关的所有数据以及过构建横向到边、纵向到底全体系审计数据模型，实现审计全覆盖；**并探索**“总体分析、发现疑点、分散核实、系统研究”的数字化审计模式；**通过内控合规风险监督，及时发现管理薄弱环节，发挥常态化“经济体检”作用，从而实现企业现代化治理。

2.中国移动内蒙古公司基于智慧审计系统提升内部审计数智化

（1）案例背景

中国移动近年来加速智慧审计建设，成为推动内部审计高质量发展、助力公司战略目标达成的重要着力点。传统审计呈现出差常态化、人员聚集、密闭空间的特点，随着数字化的深入，传统审计模式与审计数据大、频率高、地域广的矛盾凸显，因此必须推动审计从现场审计为主向“现场+远程”的审计模式发展，实现审计数字化、智能化。

随着大数据技术的发展，企业内部数字化生态已成熟，形成企业运营数字化化闭环，经过多年的积累，已具备智慧审计的数据和能力基础。

（2）解决方案

- 基于“大数据+微服务”构建智慧审计系统

以“微服务+平台”的方式，建立 IT 审计、数字审计、持续审计能力，通过大数据分析、非结构化数据识别和分析能力，逐步构建智慧审计能力，有效促进审计效率和效能提升。

来源：中国移动通信集团内蒙古有限公司

图 23 智慧审计系统架构图

大数据是智慧审计的基础，首先通过大数据平台收集数据，获取真实、完整的审计数据。模型计算基于内蒙古移动的大数据平台 GBase 组件，进行数据清洗、转换、分析，并将分析结果存入审计数据集市。

采用微服务架构模式使智慧审计系统具备开放性、轻量级、松耦合、可扩展的特性，使之更快地满足企业快速响应服务扩张、业务开放、服务整合等需求,动态扩展审计模型。

● 布局智慧审计工作体系

基于智慧审计系统，形成较为完善的智慧审计布局，从团队、数据、工具、场景、模型和系统六方面分别推进智慧审计工作建设，全

方位达成智慧审计的业务目标，打造出适合企业发展的审计体系，及时发现运营管理缺陷和风险，实现企业健康、稳健运营发展。

来源：中国移动通信集团内蒙古有限公司

图 24 智慧审计工作体系

● 固化审计模型、调整工作组织

通过梳理审计模型，分条细化，固化审计点规则，实现“审计规则—审计模型—审计点—审计框架”的全程配置，快速满足多种审计业务，扩展审计的深度和覆盖面。审计模型的动态调整需深入理解业务，分析异常行为特征，基于相关数据开展数据探索，设计模型运算逻辑、参数阈值、审计结果形式等相关内容。

在新的审计体系下，审计组织架构、工作机制与流程相较于以往产生新的变革：审计团队不再是单一固定的现场审计团队，而是划分为远程数据审计团队、现场审计团队。

（3）应用场景及治理效果

促进公司打造“低成本、高效率”的运营环境，公司内审部自

2021 年 1 月组织开展网络费用专项审计，通过智慧审计系统覆盖网络费用管理高风险领域和关键环节识别审计代维费、网络优化整治费、技术支持服务费相关领域存在的违规情况及风险问题。对成本费用的实时或准实时数据审计监控，助力提升网络成本费用管理水平，落实公司“降本增效”举措。

经过本次数字化治理的具体应用，实现了网络费用管理审计的降本增效，具体分析如下：

● 审计模型运行 6 个月，根据系统分析，各地市问题环比呈收敛趋势，证明智慧审计对实际审计工作的精准度至少提升 40%，效率提升 70%。

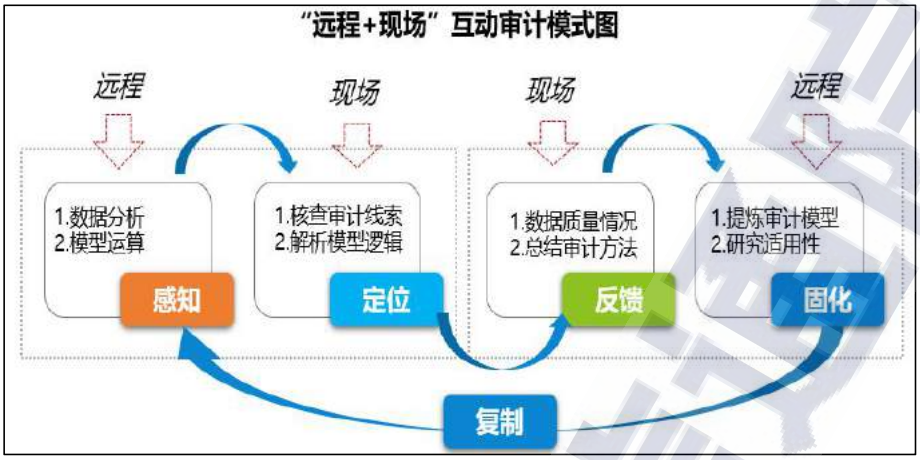
● 在审计计划、准备、实施等全过程实现“远程”审计，节约至少 6 个人力成本，120 人天，审计范围更全面、审计工作更高效、审计过程更安全，快速发现风险点。

（4）创新性和示范性

● 形成“远程”+“现场”一体化互动审计模式

改变传统审计工作模式，全面提升审计成效。线上发现定位问题，现场核实问题，实现线上+线下的一体化互动模式，最大程度的提高内审工作的效率。**通过现场审计总结审计模型，以远程方式固化模型，并在更多审计现场应用，依靠已固化模型对现场线索进行“探针式”定位，依靠审计现场反馈实现审计思路学习、优化。**根据该循环迭代的交互方式不断提升数据审计的效用。同时在审计过程中，贯穿审计人员与审计系统的人机交互环节， 最终**形成“远程+现场” 、“闭环**

+协同”的互动审计模式。



来源：中国移动通信集团内蒙古有限公司

图 25 “远程+现场”、“闭环+协同”互动审计模式

● 突破审计应用方法，构建审计风险新框架

新技术的应用，改变传统审计识别方法采取抽样方法单点揭示风险的局限性，通过对数据审计方法、智能审计技术的深入应用，轻松实现全量数据分析、非结构化数据，迅速找出业务规律，揭示隐蔽性风险。按照组件化原则，固化审计点规则，实现“审计规则—审计模型—审计点—审计框架”的全程配置，快速满足多种审计业务，扩展审计的深度和覆盖面。

3.大家衞助力大家保险集团审计工作数字化转型

（1）案例背景

“大家衞”审计信息系统作为大家保险集团坚持科技强审的重要举措，由审计中心和大家信科有限责任公司共同建设。大家衞定位为集团审计中心开展工作的基础工具，实现审计科技信息化的主要平台，充分发挥审计的风险防控第三道防线功能、为集团公司持续健康发展

和战略目标的顺利实现保驾护航的重要抓手。

大家衛以**“统筹规划、全面覆盖、互联共享、便捷应用”**为设计理念，建立**以审计知识集市为支撑，集审计管理、信息管理、数据监测预警及数据分析挖掘为一体的审计工作平台，搭建从宏观到微观的非现场监测预警体系**，持续提升审计监督的精准性和及时性，实现高度融合的数据审计模式，实现审计监督的智能化和审计管理的自动化，为数字化审计转型奠定基础。

（2）解决方案

● 搭建数据审计组织架构

结合大家衛建设，建立一支**独立的数据审计团队**，在总部设立独立的数据审计团队（处室），该团队应与部门各处室平级，并与总部各处室与各区域中心之间进行合理分工、有效交互，确保高效协同完成各项工作，各区域中心可设立相应岗位，根据实际情况配备 1-2 人专岗或兼岗，在数据审计团队指导下，支持区域中心开展数据审计工作。

● 明确数据审计职能

风险预警。监控风险预警指标，处理并应对指标报警；设计并优化风险预警指标及其预警值；根据风险预警运行结果，定期统计分析预警规则的准确性和有效性；为审计风险评估、年度计划提供数据分析结果。

远程常规。根据审计计划，执行常规的数据审计数据分析，及时发现审计线索；通过现场验证或远程影像验证，查实常规审计发现，

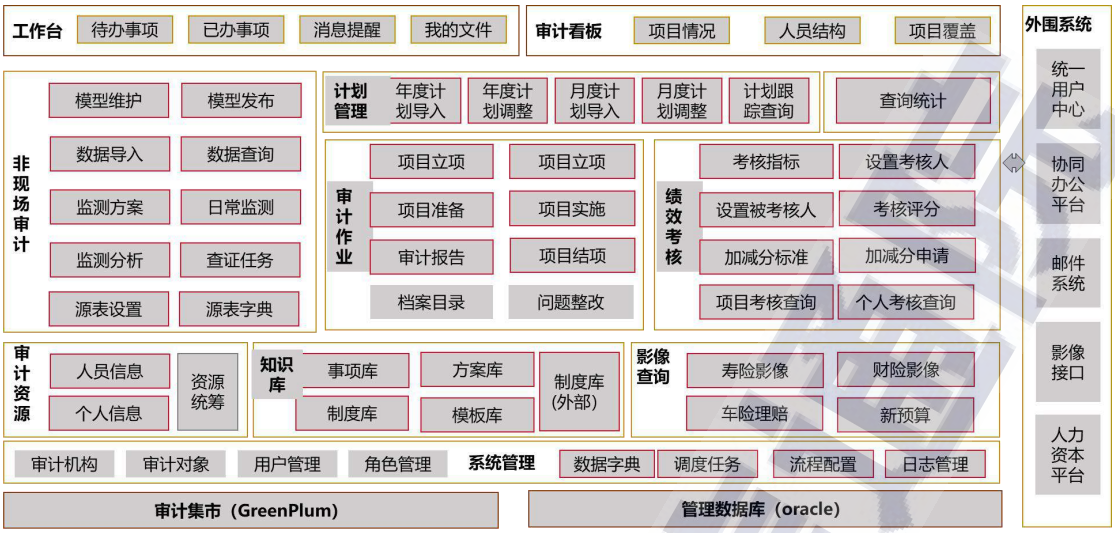
编制审计报告；设计并优化远程常规审计相关的数据审计分析规则；根据模型运行结果，定期统计分析规则的准确性和有效性。

现场支持。提供现场审计审前支持—分析风险分布，计量风险程度，并推送审计线索；提供现场审计审中支持—接受现场审计需求，缩小抽样范围，并进一步推送审计线索；提供现场审计审后支持—量化分析审计发现的影响程度；设计并优化现场审计支持相关的数据审计分析规则。

模型研发。提供模型的全生命周期管理；优化及维护模型、参数、阈值等；确认的新模型的开发需求，评估可行性和实现难度；实施新增需求的开发、测试、验证、上线工作；定期收集模型运行结果，评估模型是否有效、是否要调整或下线。

规则设计。定期收集应用功能区的新增需求，总结业务特征，识别风险事件和异常场景，设计规则；根据现场支持和数据审计的反馈，对规则进行完善和调整；不断完善规则库，拓展对业务领域的覆盖。

数据管理。提供数据的全生命周期管理；管理数据审计数据的来源、采集、清洗、存储、备份、销毁等流程；制定并优化审计数据质量体系，提供数据结构化标准、规范和模板；构建并优化数据安全体系。



来源：大家保险集团

图 26 数字化审计平台功能架构

（3）应用场景及治理效果

根据数据审计与现场审计的特点，建立多样化协作审计模式，组合形成三类审计模式：独立数据审计、联合审计、辅助审计。**独立数据审计**是利用数据技术独立承担审计项目，作为一个新兴的审计手段，大幅压缩审计成本。**联合审计**是采取数据审计与现场审计相结合的方式，两者分工作业，优势互补。**辅助审计**是将数据审计放到审计支持的地位，为现场审计提供支持。

大家衛实现了**审计对象提供数据和报表取数向系统供数转变，手工作业向系统作业转变，实物取证向电子取证转变，项目审计向数据审计转变。**

（4）创新性和示范性

大家衛完善了集团现有的审计方式、审计抽样技术、审计证据搜集等技术和方法。审计人员可采用搜集和分析被审单位所有数据的总

体审计模式，而不再拘泥于对数据的随机抽样，将“样本=总体”植入审计人员的思维中，帮助审计人员进一步接近真相，创新了全方位大数据审计工作模式，打破取数范围的限制，实现数据共享和交换。整合各类业财数据，实现大数据集中存储的同时，构建了一套科学的、成体系的大数据挖掘方法。

参考文献

[1] 中国信息通信研究院，中国数字经济发展白皮书，2021.
[2] 国务院国有资产监督管理委员会，数字化转型知识方法系列之十一：治理体系，2021.
[3] Gartner, Market Guide for AIOps Platforms. 2021.
[4] 国务院发展研究中心国际技术经济研究所，中国云计算产业发展与应用白皮书，2019.
[5] UNCTAD, Data Protection and Privacy Legislation Worldwide. 2020.
[6] Gartner, Gartner Top 9 Security and Risk Trends for 2020. 2020.
[7] IIA, International Professional Practices Framework(IPPF). 2017.
[8] Gartner, Top Threats to Cloud Computing: Egregious Eleven Deep Dive. 2020.
[9] Flexera, State Of The Cloud Report. 2020.

中国信息通信研究院 云计算与大数据研究所

地址：北京市海淀区花园北路 52 号

邮编：100191

电话：010-62304342

传真：010-62304364

网址：www.caict.ac.cn