中国民生银行 CHINA MINSHENG BANK

CAICT 中国信通院

银行业业务安全体系建设白皮书

中国民生银行

中国信息通信研究院云计算与大数据研究所

2023年8月

版 权 声 明

参 编 单 位

中国民生银行股份有限公司、中国信息通信研究院云计算与大数据研究所

参 编 人 员

毛斌、吕晓强、李吉慧、魏巍、郭雪、卫斌、马铭洋、付佳、李振、袁阔、霍鑫怡、李博言、王天娇、杨易、李红旺、王绍源、蔡宁、张凯、付雨婷、张月等。

前　言

随着数字时代的飞速发展，银行业作为金融领域的重要组成部分，正面临着前所未有的改变。金融科技的迅猛发展，各种新型业务模式和技术手段不断涌现，为银行业带来了巨大的发展潜力。与此同时，大量业务风险也随之凸显。

数字化的浪潮下，银行业面临着诸多业务安全层面新挑战。一方面，随着在线支付、移动银行、在线金融等新型金融业务的普及，银行业正进行着交易流程的转型，同时会带来诸如数据泄露、身份盗用、电信诈骗等交易风险。另一方面，金融科技的快速发展也带来了新的合规挑战，随着云计算、大数据、区块链等新兴技术的出现，银行业需适应快速转型，积极应对可能产生的如数据隐私、信息安全等相关安全问题。

基于此，中国民生银行与中国信息通信研究院云计算与大数据研究所联合撰写《银行业业务安全体系建设白皮书》，旨在通过梳理银行业面临的业务安全核心问题，帮助银行业机构深入了解当前行业的业务安全挑战和趋势，加强安全管理和风险防范能力，保护客户的资产和信息安全，以促进业务创新和业务平稳安全进行。

目　录

一、业务安全概念逐渐清晰，重要性凸显

（一）业务安全定义与范围

近年来，提出和应用业务安全相关概念的机构与企业逐渐增多，该概念旨在保护企业业务系统免受安全威胁，保障业务平稳安全运行。工信部 2020 年正式发布的 YDT 3796-2020《基于云计算的业务安全风险解决方案技术要求》标准中对业务安全定义为保护业务系统正常逻辑免受被滥用或篡改，减少业务目的与业务结果产生不确定性的措施或手段。一般说来，**传统的业务安全**为在业务中综合考虑各种风险，保障整体业务逻辑的顺畅，最终帮助企业达成业务目标、从而降低经营成本、提升业务收益、增强企业竞争力。但近年来，随着业务线上化和数字化，业务越来越依赖于网络系统和互联网，**网络空间的业务安全应运而生，**指业务方防范在网络空间中所面临的特定风险和威胁，更多关注的是业务逻辑漏洞、欺诈风险、数据泄露、违规交易等业务层风险情况。

本白皮书关注的业务安全涵盖在网络空间的业务安全之下，更聚焦于利用数字化技术，防范业务逻辑漏洞、电信诈骗、内部欺诈、数据泄露、违规交易等风险，履行银行风险防控主体责任，满足监管要求，保障银行业务安全平稳运行，保护客户和银行的信息及资产安全。

（二）业务安全重要意义与价值

数字化浪潮下，企业上云不可避免，为提高云上业务稳定性、减少云上业务风险，业务安全受到了来自**用户侧**、**企业侧**和**社会侧**的广泛关注。

用户侧对于业务安全的关注重点包含以下三个方面。**一是保障**用户获得公平的金融决策、营销活动，避免出现高价黄牛交易。**二是**用户的信息安全、个人隐私安全可得到安全防护。**三是**降低用户被欺诈而受到的损失。

企业侧对于业务安全的关注重点包含以下四个方面。**一是**履行企业风险防控的主体责任，满足法律和监管要求，保障业务合规性。**二是**针对各种业务层面风险进行管理助力企业作出正确的决策。**三是**助力保护企业资产的安全和完整。**四是**助力实现企业的经营活动目标。

社会侧对于业务安全的关注重点包含以下三个方面。**一是**通过保证企业的健康业务发展保证国民经济的可持续发展。**二是**社会人员对业务风险以及业务安全认识的提升。**三是**保障社会群众的财产安全，保证社会稳定。

（三）业务安全监管清晰化

企业数字化进程加速，市场监管的清晰化对企业业务的稳定与安全起着重要的作用。随着金融业线上化业务深入发展，以黑灰产、电信网络欺诈、数据泄露、业务逻辑漏洞等为代表的新型犯罪持续高发，

严重影响了银行业业务安全。相关监管政策和规章制度逐渐清晰，国务院、人民银行等监管机构进行了全面深入的决策部署，相继出台多项法律法规和纲领性指导文件，涵盖涉赌涉诈资金链治理、反洗钱、非法集资、大额可疑交易报告、外部欺诈、内部管控等方面内容，给金融机构业务风险防范提出了严格要求，并给予了全面细致的指导。

1.2006 年 10 月，中国人民共和国第十届全国人民代表大会常务委员会第二十四次会议通过《中华人民共和国反洗钱法》

2007 年 1 月起施行的《反洗钱法》对客户身份识别、交易记录保存、可疑交易报告等相关反洗钱制度作了规定，这些制度是银行业业务安全的重要基础。

2.2022 年 1 月，人民银行印发《金融科技发展规划(2022-2025 年)》

2022 年 1 月印发的《金融科技发展规划（2022-2025 年）》提出八个方面的重点任务，重点包括要强化金融科技治理、全面加强数据能力建设、深化数字技术金融应用、构建安全高效的金融科技创新体系、深化金融业务智慧再造、加快监管科技的全方位应用、扎实做好金融科技人才培养，通过实现业务、数据、技术的联动来提升金融业务质效。

3.2022 年 9 月 2 日，中华人民共和国第十三届全国人民代表大会常务委员会第三十六次会议通过《中华人民共和国反电信网络诈骗法》

2022 年 12 月 1 日起施行的《反电信网络诈骗法》是一部针对数字化业务，提高社会治理体系和治理能力、加强预防性法律制度建设的法律法规，从根本上、制度上预防、遏制、打击电信网络诈骗，在银行业数字化浪潮下，成为数字业务安全领域立法的重要探索。

4.2023 年 1 月，银保监会提出《关于银行业保险业数字化转型的指导意见》

该意见中提出“加快建设与数字化转型相匹配的风险控制体系”，强调利用大数据、人工智能等技术优化各类风险管理系统，将数字化风控工具嵌入业务流程，提升风险监测预警智能化水平。要求银行保险机构董事会要加强顶层设计和统筹规划，围绕下务实体经济目标和国家重大战略部署，科学制定和实施数字化转型战略，将其纳入机构整体战略规划，明确分阶段实施目标，长期投入、持续推进。

5.近期，证监会发布《证券期货业科技发展“十四五”规划》

该规划明确“十四五”期间行业要以金融科技发展、数字化转型为目标，从治理体系、业务创新、技术和数据能力建设、风险防范等多维度提出重点任务，用以推动行业的数字化转型落地实施。

同时，中国人民银行、支付清算协会、公安部等监管机构就业务安全问题也发布了加强监管等内容文件。如《中国人民银行关于加强支付结算管理防范电信网络新型违法犯罪有关事项的通知》、《打击治理跨境赌博金融监管工作组关于印发<涉赌涉诈可疑资金特征及账户线索核查要点>的通知》、《中国人民银行办公厅、公安部办公厅关于印发《电信网络诈骗和跨境赌博"资金链"治理工作方案》的通知》、《中国人民银行关于做好小微企业银行账户优化下务和风险防控工作的指导意见》等文件的发布，进一步加强了对于例如账户分类管理、支付安全、涉赌涉诈核查、电信网络诈骗、账户优化下务等一系列业务安全风险的监管。

二、银行业务呈现数字新业态，业务安全与风险博弈发展

（一）新技术驱动数字新业态不断发展

1．新技术驱动数字新业态不断发展，银行业数字化转型大势所趋

数字新业态高速发展，逐渐由数字新业态发展为数字生存新常态。**云计算、大数据、人工智能等为代表的数字技术不断发展，已成为新业态新模式升级的关键驱动力。**云计算的快速发展，实现了对网络数据的便捷访问和计算资源的快速共享，大大的提高了不同组织和部门之间的协同合作能力，同时降低了企业或组织之间的数字资源管理技

术门槛。大数据技术的出现，使得企业可以实现对现有海量数据的深度挖掘和运用，推进企业现有的数据资产向着价值进行转换，大数据技术对企业的优化生产、降低能耗、精准营销等领域起着革命性的改变。人工智能技术的出现，通过个性化、自动化的方式给银行客户体验带来了全面的提升，为传统的用户交互带去了改变，帮助企业进行用户体验优化、个性化下务等行为。

技术的升级催生了互联网金融等新业务的兴起，银行纷纷开启数字化转型之路。一方面，通过互联网+，银行业可以实现线上开户、移动支付、智能投顾等一系列金融下务，极大地方便了客户的金融操作。另一方面，新业务的发展离不开金融科技创新，因此近年来，银行业注重以核心系统转型为主线，带动银行的总体架构升级，利用数字化技术，不断推动银行业务能力的提升和业务流程的变革。

2．客户体验要求不断升级，驱动银行数字化转型

随着技术的发展，消费者已经不再满足于标准化的产品和下务，更希望银行提供更精细化、个性化、场景化的下务。目前不同性质的银行、金融机构面临的同质化竞争较为严重。对这些机构和组织来说，生存的基础就是要增强本地客户的黏性，而最为重要的是打破传统、单一的下务模式。因此，以提升客户体验为驱动的数字化转型更显得尤为重要。

（二）银行业数字化发展呈现四大新态势

多方因素驱动引发数字新业态不断发展，银行业在这一转型过程中呈现出数据化、开放化、智能化和协同化的业务新态势。

1．数据化为银行积累海量高质量数据资产，提升业务创新能力

数据化为银行快速积累海量高质量数据资产，更准确高效理解用户需求。中国信通院《数据资产管理实践白皮书（5.0版）》对“数据资产”的定义为“由组织（政府机构、企事业单位等）合法拥有或控制的数据资源，以电子或其他方式记录，可进行计量或交易，能直接或间接带来经济效益和社会效益。”银行业的数据化趋势使银行能够积累大量的高价值数据资产，通过这些资产更好地理解客户需求和行为模式，从而提供更加个性化的产品和服务。通过大数据分析和机器学习算法，银行可以准确预测客户的需求、优化营销策略，进而提升客户满意度和忠诚度。

数据化成为银行开放融合、展开业务创新的重要基础。数字化转型将传统线下信息转变为线上数据，这使得银行可以通过开放API接口和与第三方合作，开发新的金融科技产品和服务，以寻求业务创新及更多的可能。同时，数据化提高了银行业务的效率和效益，银行可通过自动化处理、在线交易和数字化文件管理等方式，实现更快的交易处理速度、降低运营成本，并提供更加便捷的服务体验。

2．开放化促进银行业数据共享，带来行业新机遇

银行业与商业生态系统深度融合和数据共享，为银行业带来新的改变和机遇。通过与第三方合作伙伴、技术公司和创新企业建立合作关系，银行可以共享数据、算法、交易和流程，加速产品和服务的创新。这种合作模式推动了银行业务的数字化转型，使其能够更好地满足客户需求并提供个性化的金融解决方案。其次，开放化加强了客户体验和服务质量。通过开放 API，银行可与第三方应用程序和平台集成，提供更便捷、个性化的金融服务。客户可通过单一的应用程序或平台访问多个银行的产品和服务，实现无缝的金融体验。此外，开放化的态度使得银行积极与技术创新企业合作，引入大数据、人工智能、区块链、物联网等新技术，提升服务质量和效率。

3．智能化已成为银行数字化转型的核心策略

人工智能、大数据等智能化技术已成为银行业数字化转型策略制定核心考虑因素。随着数字化转型的不断深入，银行业呈现出一种以数据为基础，以智能科技为核心的转型策略，通过将数据转化为资产，重塑银行发展的驱动模式。毕马威指出未来银行是银行把握科技变革对商业社会重塑的奇点性机遇，通过智能化改造，从而实现对未来银行的全方位赋能。

智能化技术为银行实现了全方位的赋能，对客户洞察、产品与服务、渠道交互以及运营流程等方面进行智能化改造。**一是客户洞察方**

面，银行自动化获取和分析海量数据，提升数据处理能力，并智能化处理将这些洞察转化为产品、服务和客户体验。**二是在产品智能化方面**，银行通过数据自动发现业务规则，洞察客户需求，从而增强了产品的智能性。**三是在渠道智能化方面，**银行创造了与客户交流、交互的全新界面，为实现开放银行带来了新的交互体验。**四是在流程智能化方面，**银行实现了流程的智能化、自动化和无人化，提高效率的同时降低了成本。通过智能化改造，银行可更好地适应快速变化的市场环境，提供更优质、高效的金融服务。

4．协同化帮助银行构建金融生态，促进行业共同发展

银行积极构建协同化的金融生态，通过开放和共享实现信息价值的最大化。财资中国联合西湖财资金融科技研究院发布的《2021-2022年交易银行报告》中指出，银行需建立“数据+场景+生态”的数智化新范式，立足“开放与融合”，重构发展新逻辑与新框架，打造智能、无界、开放的服务新格局，赋能产业数智化发展。

其一，协同化已成为开放金融模式的重要组成部分。银行通过与第三方合作伙伴建立合作关系，共同创新并提供场景化的金融服务。例如，与电商平台合作开展供应链金融服务，与科技公司合作推出数字支付解决方案，与创业企业合作提供融资支持等。通过开放金融模式，银行能够扩大服务范围，满足不同客户群体的需求，促进金融创新和业务增长。

其二，协同化成为实现银行业价值共享的关键。银行与其他金融机构、技术提供商、创新企业等建立紧密的合作关系，共同开发和共享数字化服务和资源。通过数字化生态协同，银行能够获得更广泛的资源和专业知识，提高服务质量和创新能力。协同合作可涵盖跨行业的合作，如与保险公司合作开展综合金融服务，与科技公司合作推动数字身份验证解决方案等。通过数字化生态协同，银行可实现资源的共享和优势的互补，进一步提升交易银行的综合竞争力。

（三）银行业数字新业态下，风险与业务博弈发展

1.黑灰产业发展迅猛，规模逐渐壮大

（1）黑灰产活动隐蔽性增强且规模逐渐壮大

在银行业数字化转型的进程中，黑灰产业也有了新的改变，组织规模日益壮大、黑产行为更加隐秘、从业者犯罪手段不断升级，加剧了银行业业务风险防护的压力。

一是黑灰产行为变得更加隐蔽。黑灰产活动者不断创新手段，挖掘新型漏洞，银行业需与监管机构持续加强合作，加大对黑灰产的打击力度和技术防范手段。为应对黑灰产的威胁，银行业不断加强安全技术和风险管理措施，采取多层次的身份验证、加密通信、实时监测等措施，以减少黑灰产对银行业务的影响。监管机构也加强了对银行业的监管，提出了更加严格的反洗钱和反欺诈要求，加大对黑灰产活

动的打击力度。

二是黑灰产形成规模化、集团化的新运作模式。黑灰产所运用的攻击手段逐渐具备高迭代速度和强可复制性。数字化转型进程当中，很多企业在不断做着技术及业务的创新，希望能够获得更大的利益。然而，随着互联网用户红利增长趋缓，用户获客成本增高，平台方花费大量营销资源在客户获取等环节。黑灰产利用各种欺诈手段对平台上的营销活动进行套利变现，导致营销活动不能达到预期的活动效果，且造成正常用户不能享受应有的权益和活动体验。

三是黑灰产从业者变得更有组织性、传播性和信息感知度。黑灰产滥用平台的各种营销活动机制，如新人奖励、用户裂变拉新奖励、签到奖励、秒杀优惠、商户补贴等，利用批量账号和自动化软件，绕过平台设定的限制规则，以积少成多的方式，大量地获取营销活动礼包，然后将现金聚集到统一账号，或将红包、优惠券、电子券等以不同方式进行变现获利。随着各平台风险监控力度的加强，黑灰产也在逐步改变欺诈方式，由原来的机器批量操作，改为人肉众包的形式，给企业识别欺诈分子带来了一定困扰。

（2）黑灰产各环节集成化发展，形成完整产业链条

黑灰产从业者游走于法律监管的边缘地带，逐渐形成一条分工明确、合作紧密的黑灰产业链条。形成了围绕账号的上下游产业链。按照供给结构划分，可以分为上中下游，分别对应的是资源层、下务层、

变现层。

上游资源层阶段，作为黑灰产业链的源头，对于当今组织化规模化越来越清晰的犯罪团伙来说，各类账号已经成为了他们的首要核心资源。黑灰产会通过养号等方式进行物料积累，同时，黑灰产从暗网、QQ 群等渠道不断获取最新的营销活动、企业漏洞等信息，发现可薅羊毛的活动之后，即在内部核心群中传播，同时一些批发商会通过钓鱼网站和木马来批量获取用户信息。黑灰产从各种渠道获得 IP、账号、设备号等资源，为非法套利做好前期资源准备。

中游服务层阶段，黑灰产从业者并不做实际的攻击，依据资源层提供的基础资源，在营销活动前进行批量的账号注册、养号，或者直接盗号、再洗号等活动。中游会进行大量的账号生产与分销，积累大量的账号信息，并提供给变现层，同时通过组合资源和基础工具，来完成资源的串联，形成各种各样的欺诈工具，以支撑变现层，提升欺诈效率。

下游变现层阶段，黑灰产会实际攻击各大企业，包括营销薅羊毛、恶意引流、刷量作弊、盗号洗号、网络诈骗等行为。欺诈行为后会有专门人员将资金转到不属于黑产人员的名下银行账户中，再迅速将资金进行转移、提现和变现。此时，企业会感知到异常，便开始加强风控策略，黑灰产攻击成功率随之降低，发现成功率降低的黑产，也会再次研究企业的策略变化，并修改自己的攻击逻辑，一来一回间，黑

灰产和企业陷入了攻防拉锯战。

2.欺诈手段不断升级，呈现多趋势变化

第一，欺诈手段呈现场景化趋势，攻击手段随着场景变化不断优化，利用不同手段攻击。欺诈从业者通过场景化伪造、编造信息以获取客户信任，最终达到欺诈的效果。**一是在线银行和移动支付应用的场景。**欺诈者会伪造虚假的银行网站或移动应用界面，诱使用户输入个人敏感信息，如账号和密码；通过电子邮件、短信和社交媒体等渠道发送欺诈性信息，骗取用户点击恶意链接或下载恶意软件，从而获取用户的财务信息。**二是在网络借贷场景，**账户注册阶段，欺诈者经常采用伪造身份注册、冒用他人身份注册、自动化垃圾注册等手段完成欺诈行为。在登录阶段，欺诈者可使用盗用、冒用、异常共享的手段。在贷款申请阶段，欺诈者通过提供虚假信息进行超大额度的贷款申请。在还款阶段，欺诈者通过恶意拖欠等手段进行破坏。**三是在消费金融场景下，**欺诈者可通过账户注册、激活、登录、交易、信息修改等各个环节进行诈骗，实现资金套现。**四是在供应链金融场景，**欺诈者可伪造企业的虚假交易数据、虚构经营数据，进行虚假的供应链授信。

第二，群体年轻化已成为银行业欺诈的新现象。年轻群体已成为银行业欺诈的主要群体之一。年轻群体通常更加依赖移动支付和在线银行业务，对于新技术也更加熟悉和接受。欺诈者利用年轻群体对科

技的热情和信任，设计出更加精巧的骗局。例如，可通过社交媒体上的假活动或竞赛吸引年轻用户参与，并要求提供个人银行信息或支付一定费用，最终骗取钱财。此外，欺诈者还利用社交工程技术，通过在线社交平台获取个人信息，进而实施针对特定个体的欺诈行为。可伪装成熟悉的朋友、家人或者银行工作人员，通过发送虚假信息或进行电话诈骗，诱使受害者透露个人敏感信息或进行资金转账。

3.银行业务数字转型，多样风险苗头渐露

在银行业数字化转型的浪潮中，除黑灰产业、欺诈等场景，多样化的业务安全风险也逐渐暴露出来，这些风险的存在对银行机构、客户和整个金融生态系统将造成严重影响。

一是业务逻辑漏洞风险，数字化业务复杂的业务逻辑交织在各种应用和系统中，可能存在漏洞和不完整的逻辑判断。黑客或恶意用户可利用漏洞来绕过安全控制，执行未经授权的操作，从而导致资金损失、客户隐私泄露等安全事件。

二是电信诈骗风险，数字化转型为银行业带来便利的同时，也使银行客户更容易受到电信诈骗的威胁。不法分子可冒充银行人员，通过虚假通知、欺诈性短信或电话，引诱客户提供个人信息、账户凭证或执行非法转账，从而导致客户财产损失。

三是数据泄露风险，大量敏感客户数据被存储和传输。数据泄露可能因网络攻击、员工失误或供应商漏洞而发生，导致客户隐私曝露、

身份盗窃，甚至被用于其他犯罪活动。

四是非法洗钱风险，数字化业务为洗钱行为也带来了更多的机会和挑战。数字化银行业务使得资金转移变得更加快捷、方便，同时跨境交易也更为迅速和隐蔽。犯罪分子可通过虚假交易、匿名账户以及跨境转移等手段来掩盖其非法资金来源，从而逃避监测和追踪。此外，自动化技术和人工智能的应用也为洗钱行为提供了更多的遮蔽和隐匿手段，例如通过分散的小额交易来规避监测系统的关注，或是利用算法来模糊资金流向的真实目的。

为减轻上述风险，银行业需要采取一系列综合性的安全措施，建立全面的业务安全治理体系，更好地平衡数字化转型的机遇与风险，确保机构与用户的资产和信息得到充分保护。

三、银行业务安全发展仍处初期，体系建设面临诸多问题

（一）业务安全建设技术手段有效性面临挑战

银行业业务安全体系建设中，如何保证所选技术的有效性、时效性、适配性，仍是实际落地建设当中面临的重大挑战。

1.数据来源有效性难以保证

在银行的业务安全体系建设中，如何确保数据来源的有效性，利用数据进行更高效的风险评估和决策制定成为新的挑战。

一是用户申请时提交的数据信息有效性难以保证，这些数据往往

是用户自行填写，可能存在虚假信息或出现错误填写的情况。**二是用户行为数据的有效性难以保证，**用户行为数据的使用需要进行大规模的数据清洗、整理和分析，这是一个复杂的过程，有效性同样难以保证。**三是来自协同方的数据有效性难以保证，**协同方包括政府、公用事业、银行等机构，他们可以提供用户在多场景下的留存数据，提供多角度展示用户特征的信息，在使用第三方数据时需要慎重考虑数据来源的合规性和有效性。

2.技术应用有效性难以保证

在银行业务中，如何确保所选的技术应用能够有效的强化银行业务安全建设，成为了银行业业务安全的一大挑战。

一方面，如何保证技术应用的迭代优化成为了银行业业务安全面临的新挑战，技术应用的迭代优化需要大量的历史数据来进行支撑，基于大数据进行模型构建和效果验证，从而更准确地评估技术应用的性能和效果。这意味着需要足够的历史数据，才能够支持模型的验证和优化。因此，对于银行业来说，如何收集、整理和清洗大量历史数据，保证技术应用的迭代和优化成为了一个难点。

另一方面，新技术高昂的使用和维护成本也成为了银行业业务安全的一大挑战，新技术的使用需要对银行业从业者进行专业培训、购入较多技术设备，人员和财力上的投入对银行业来说是一个不小的成本。技术手段的引入需要与现有系统相兼容、进行全面测试和验证，

以保证其在生产环境中的兼容性，这给银行的新技术使用带来了很高的使用成本。除此之外，当银行应用新技术之后，随着技术革新、业务变动、市场变革等影响，后续技术应用的维护、更新也会给银行带来更多资源上的支出。

（二）银行业务安全建设管理制度仍需加强

在银行业的数字化转型过程中，除了外部黑灰产业带来的欺诈等风险，内部业务管理手段也随着更加高效、迅速的新业务形态引发了新的问题。

1.业务安全专业人才缺失、业内管理制度仍需加强

银行业因新技术发展、业务形态转变、市场变化等影响正积极进行转型，快速转型的业务引发了专业型人才的缺失。在既有科技人才中，既懂银行业务又懂安全技术的复合型人才相对较少，直接影响了银行业业务安全的的发展进程。另一方面，受限于自身的科技开发能力、专业科技人员储备等因素，银行业在产品研发创新中多依赖于科技合作机构，这种长期依赖外部合作方的发展模式，不仅造成成本费用过高，也存在信息安全等问题，不利于银行业长远发展。

银行业业务安全工作的展开需要进行多部门联动和深度合作，银行业需要进行制度上的升级来更好的支撑业务安全的工作开展。业务安全的工作展开往往需要跨部门合作和全面数据收集与分析，以便获

得准确的数据来支持决策和管理层的判断。部分银行技术线与业务线缺乏敏捷联动机制，后台技术研发部门与前台业务营销部门相对割裂，彼此间信息不对称，引进研发的相关技术或系统不能有效匹配一线的关键需求，只有建立有效的管理制度，银行才能更好地应对业务安全所面临的挑战，并不断提升数据安全治理的效果。

2.业务安全重视程度仍需加强，亟需达成统一共识

银行业界对业务安全的关注度仍需加强，企业多在出现安全事件后才开始关注业务安全。企业在出现业务安全导致的损失之前，防范意识不高，业务安全也不会作为行业重点考量因素。目前，发展完备业务安全部门的企业仍在少数，绝大多数企业仍依靠传统安全部门解决业务安全的问题，最终通过基础安全团队解决问题，处理效果达不到预期。因为很难计算通过业务安全为企业减少的损失以及投入产出比，很多企业在意识到业务风险点之前不会设立单独的业务安全部门，在意识到风险点之后可能也仅仅设立简单的开发或运维部门下面的业务安全负责人。

银行业界的业务安全建设亟需达成统一的方法论与共识。经过前期调研，业务安全、智能风控等名词均尚无明确统一的概念和定义。行业对使用何种算法、采用哪些方案才能最大限度体现出数字化业务安全的优势并无明确共识。行业内亟需输出符合业务发展特点的数字化业务安全方法论。

四、银行业业务安全防御体系建设及应用

（一）新技术在银行业业务安全应用

1.云计算技术保驾护航，为银行业务安全提供安全底座

云计算技术作为新型技术底座，为银行的业务安全建设提供强有力的支撑。一是保障业务稳定性，通过弹性和可伸缩资源，银行能够根据需求快速调整其资源和基础设施，银行根据业务需求来分配和管理计算和存储资源，有助于应对交易量的波动和突发事件。**二是加强数据可靠性，**银行处理的数据量庞大，云计算提供了弹性和可扩展性的存储和计算资源，银行能高效地管理和处理大数据，从中提取有价值的信息。**三是提供灾备功能，**银行可将数据和应用程序备份到云端，确保即使在硬件故障、自然灾害或其他灾难性事件发生时，数据不会丢失，并且可快速恢复业务正常运作。**四是提供安全隔离能力，**云计算可提供更先进的安全措施和更严格的访问控制，确保敏感数据的保密性和完整性、防止恶意攻击和数据泄露。**五是提升业务系统容错性，**云计算使得银行能够构建分布式防御系统，将安全功能和防护机制部署在多个地理位置和数据中心，提高银行业务的容错性和抗攻击能力，同时减少单点故障的风险。

2.大数据提升银行风险分析能力，助力银行欺诈检测

大数据技术应用广泛，助力银行风险评估、欺诈检测等多方面应

用场景。通过大数据的应用，银行能够更加精准地评估风险、识别欺诈行为，并采取相应的措施保护自身和客户的利益。**一是助力实时风险评估和欺诈检测，**传统的违约风险评估主要基于过去的静态数据，易忽略实时的信贷欺诈风险，通过大数据，银行可以利用实时数据平台和智能规则引擎进行实时交易业务安全分析，提高对违约风险的识别和预防能力，并建立预测模型，通过自动分析对事件快速进行分类处理，有效识别和应对滥用和欺诈行为。**二是助力银行识别虚假代理，**银行业面临虚假网络代理维权等不法行为风险，通过大数据的应用，可以利用用户画像和精准分析，准确识别虚假网络代理维权行为。**三是助力实时交易监控和高并发数据处理，**银行拥有海量历史数据，通过大数据技术可以进行实时业务安全交易监控，并且可以分布式实时进行数据采集和决策，可帮助银行高效整合多系统业务数据，处理海量高并发线上行为数据，识别恶意用户和欺诈行为，并实时预警和处置。

大数据技术在银行和金融领域的工作中得到了普遍推广和应用，但目前还存在着几点挑战。一是数据样本数量影响建模分析精准度。商业银行报送金融统计表数据的数量少，粒度大，难以对数据信息之间的内在逻辑关联进行解析，进而挖掘数据信息的内在应用价值。**二是专业人才数量不足，开展相关工作推进困难，**商业银行缺乏相关方面的专业人才，导致大数据技术在其金融统计工作中难以有效开展，

对大数据技术的应用价值功能的发挥具有严重的制约后果。

3.人工智能技术增强银行信息洞察，助力业务风险防范

人工智能技术能够帮助银行进行数据资产的深度挖掘、客户关系网络分析以及欺诈等风险防范。**一是在数据挖掘与用户画像建立方面，**人工智能技术可以深度挖掘银行内部数据的内在关系，建立用户联系，通过对零售贷款、信用卡等多类零售产品的用户、设备等数据进行深度分析和关联分析，助力银行进行客户关系画像的建立。**二是在可视化关系网络与关联分析方面，**通过建立可视化的关系网络，审批人员可以直观、快速地分析客户关联关系和团伙关系。这种基于动态关系网络的可视化呈现方式，能够帮助银行工作人员更好地理解关联关系，进行交互式探索。**三是在助力欺诈识别与风险防范方面，**借助人工智能技术，金融机构能够快速发现欺诈团伙，并有效挖掘新型欺诈手段，提升对未知风险的防范能力。通过使用社会关系网络分析工具，可以分析关系网络图中是否存在大量共用设备等拓扑结构，从而识别潜在的欺诈行为和风险。

人工智能的应用仍处初期阶段，普遍应用仍存挑战。一是构建门槛过高，业内缺乏快速、高效、低成本的相对通用的人工智能模型应用。**二是行业资源不足，**缺少开源、易用、高性能、易拓展的人工智能模型、应用以及训练数据，人工智能技术的巨大潜力仍有待发掘。

4.隐私计算技术解决数据孤岛及多方不信任问题

数据孤岛和多方不信任的问题，一直是阻挠银行业界各组织进行数据协同的因素之一，隐私计算技术通过实现数据的可用不可见，在保护数据隐私、满足政策法规的要求下实现了数据共享与协同。**一方面，针对数据孤岛问题，**传统风控下的数据孤岛问题包含数据互通难以及法律监管严的问题，训练 AI 所需要的大数据很难获得，数据的控制权分散在不同机构、不同部门；政策法规对数据隐私和数据安全的要求严格。通过隐私计算技术，金融机构间可以合规地构建计算网络，使用本地数据对模型进行训练、迭代。**另一方面，针对互不信任问题，**传统风控下的互不信任问题包含数据维度匮乏等问题，传统信贷管理体系由于客户数据维度匮乏，数据量有限，造成客户信息收集困难、信息准确性难以验证的问题；金融机构和企业（数据提供方）间，由于担心隐私数据泄露，造成数据难以互通。通过隐私计算技术，三方机构提供用户的交易数据、消费能力、行为习惯；银行提供用户基于银行自有数据的用户特征；双方在数据不出库的情况下进行联合建模，有效降低信息不对称性与不透明性，提升信贷风控能力。

隐私计算解决数据孤岛和互不信任问题的同时，也引发了新的挑战。一是其性能瓶颈阻碍其大规模商业化落地，隐私计算目前在业务安全场景下的应用逐渐丰富化，已在金融信贷风控、反洗钱、业务安全、营销、保险定价与理赔等场景落地应用，在金融行业的实践应用

大多仍处于单点实验阶段，距离规模化商用仍需时日。**二是算法协议难以达成统一，**隐私计算产品的算法协议差异化较大，难以形成统一的安全基础；**三是数据样本数量影响建模分析，**金融机构出于隐私保护顾虑，所提供的数据维度单一，影响建模效果；**四是设备环境可能存在安全风险，**多方数据的共享、使用过程中所处硬件环境的安全可信程度存在安全风险。

5.大模型（AIGC）技术提供智能客户支持，应用场景广泛

大模型技术在银行业务安全领域有多种应用，大模型（AIGC）技术是指基于人工智能技术的大规模语言模型，如 OpenAI 的 GPT-3 模型，这种利用深度学习算法和海量数据训练而成的模型，具有强大的自然语言处理能力和智能问答能力，在银行业业务安全领域有着诸多应用。**一是在欺诈检测方面，**银行可以利用大模型技术对交易数据进行分析，以识别潜在的欺诈行为。**二是在身份验证方面，**大模型技术可以应用于银行的身份验证过程中，以提高准确性和安全性。通过分析客户提供的个人信息、账户活动和历史数据，大模型可以评估身份真实性并检测任何异常或可疑行为。**三是在智能客服和虚假信息识别方面，**银行可以利用大模型技术来构建智能客服系统，以回答客户的安全相关问题并提供相应建议。此外，大模型还可以帮助银行识别虚假信息，例如在在线申请过程中检测伪造的身份证件或虚假的财务信息。**四是在反洗钱（AML）和反恐怖融资（CFT）方面，**大模型也可以

起到很好的预防效果，通过分析大量的交易数据，以帮助银行识别可疑的洗钱和恐怖融资活动。通过对交易模式、金额和相关方的关联进行分析，大模型可以提供潜在风险的提示，并支持银行进行调查和报告。**五是在威胁情报和网络安全方面，**大模型技术可以分析大量的网络日志和安全事件数据，以帮助银行监测和应对潜在的网络威胁。它可以识别异常的网络活动、恶意软件和网络攻击行为，并及时发出警报，以保护银行的网络和系统安全。

大模型技术在解决银行业务安全问题时，仍面临部分挑战，一是在数据隐私保护方面，银行处理的数据包含大量敏感信息，如个人身份信息、财务数据等。在应用大模型技术时，确保数据的隐私和安全是一项重要的挑战。**二是对于大模型的数据质量和准确性方面，**大模型的准确性和效果受到数据质量的影响，如有面临数据缺失、错误或不完整的情况，可能导致模型的输出结果不准确。**三是大模型具有低解释性和低透明性，**大模型通常是复杂的，其中的内部逻辑和决策过程可能难以解释。**四是在面临新的欺诈模式时，大模型的学习成本相对较高，**当银行遇到新型的欺诈手段或者新的欺诈模式时，现有的大模型需要大量成本来识别和捕捉到这些新型欺诈行为。

（二）银行业务安全防御体系建设关键点

1.业务安全防御体系建设目标

银行业业务安全防御体系建设目标是通过数字化技术、支撑平台、

防御策略和管理机制的建设及应用，履行银行风险防控主体责任，满足监管要求，保障银行业务能安全平稳运行，保障客户和银行的信息及资产安全。

2.业务安全防御体系建设思路与路径

围绕上述目标，与传统网络安全防御体系建设相比，有效的业务安全防御体系更需要银行的各业务经营部门、中后台风险合规管理部门及科技部门的紧密配合。数字化技术和科技支撑平台能赋能业务安全防御体系各项工作高效运营，但防御策略需要嵌入到各业务开展过程中才能有效落地，因此，银行业的业务安全防御体系需支撑平台、防御策略和管理机制三个方面有机结合，同步建设。

（1）银行业业务安全体系支撑平台建设关键点

业务安全防御体系支撑平台建设的主要目标为支撑全行业务安全防御体系各项工作线上化、高效化运转。如图 1 所示，从事前、事中、事后三个阶段细化，业务安全防御体系的各项工作及支撑平台相应的关键功能如下。

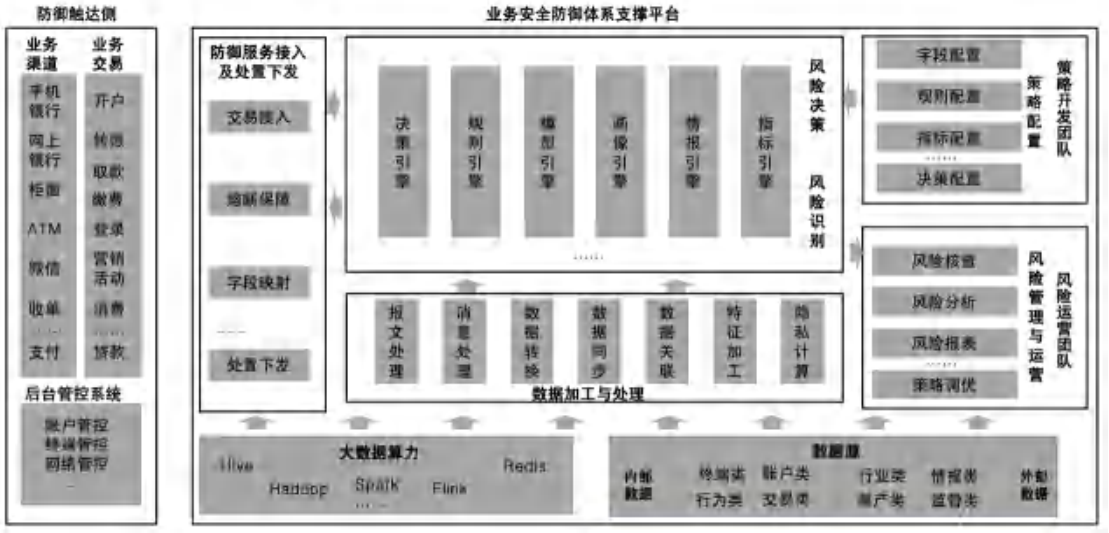

图 1 业务安全防御体系关键点

事前阶段：在风险未发生前采取相应的应对措施，如制定开发风险识别、处置策略，引入黑产情报服务等提升风险感知能力。为此，支撑平台应具备策略配置功能，能灵活支撑策略开发团队开发上线风险识别及处置策略。通常风险识别策略可分为规则评分类和算法模型识别类，策略配置中心应能支持字段、指标、规则、评分及算法模型参数的页面化配置，无需开发即可上线风险识别和处置策略，提升策略上线的敏捷性，能及时应对不断变化的外部攻击手段。此外，为了提升风险防御策略的覆盖度和准确度，支撑平台应至少建立以下 6 类引擎并整合各类引擎输出结果，持续丰富风险识别因子和手段。规则引擎负责规则评分类策略的落地和执行；规则中所需的指标由指标引擎采用大数据算力进行加工和实时计算；模型引擎应能支持机器学习、关联图谱等算法模型的开发和运行；画像引擎能支持对客户、账户、设备等实体打标签，丰富风险识别因子和差异化风险识别手段；情报

引擎负责引入、加工外部数据源（如监管类、行业类、黑产情报类等）并输送给其它引擎使用；决策引擎负责整合各类引擎输出结果，执行决策方案，输出最终决策。在引入外部数据过程中，支撑平台可利用隐私计算技术实现安全引入并可进一步与第三方进行联合建模，丰富风险识别策略。

事中阶段：在风险发生时能及时识别并处置风险，是业务安全防御的重点工作。银行各类业务的开展依托渠道，如手机银行、网上银行、线下柜台、ATM 等，并在系统中落地成各类交易执行，如开户、登录、转账、贷款、取款、缴费等。为了在事中阶段能及时识别风险，业务安全风险识别及处置策略应嵌入到各类交易环节。因此，支撑平台应具备防御下务接入功能，接收业务渠道推送的交易信息，运行风险识别策略和处置策略，并将识别结果和处置指令返回给渠道端或后台管控系统。为了保障业务连续性，支撑平台应具备自熔断能力，在风险策略运行发生故障时也能给渠道系统返回熔断指令，使交易能继续执行而不中断。支撑平台还应能支持银行至少每秒万级的并发交易的风险识别，为此事中阶段的的各类风险识别和处置策略的执行必须做到高并发、低延迟。当前业内均采用流式计算、内存缓存等大数据组件保证高并发和低响应延迟（最高不能超过 100ms）。在处置策略方面，支撑平台应能支持根据风险等级下发不同级别处置指令，如拦截、增强认证、远程见证、延迟支付、弹窗提醒等交互式防护措施，

提升客户体验。

事后阶段：围绕风险管理和运营工作展开，采取风险分析、风险核查、风险报表和策略调优等措施，感知安全防御效果，查漏补缺，进一步防范风险，形成闭环。支撑平台应具备可视化风险分析功能，支持对风险交易、账户、客户等开展多维度分析，可快速发现问题；支撑平台应具备风险核查功能，能支持总分支不同层级核查任务下发和流转，并通过风险分析工具，提升核查效率；支撑平台应具备风险报表功能，包含风险大盘和可视化报表，及时感知安全防御效果；支撑平台应具备策略调优功能，根据安全防御效果能快速调整或新增策略，并通过规则实验室、模型实验室等功能测试策略调整后的效果，保障策略的有效性。

除上述关键功能模块建设以外，支撑平台在建设过程中还需注重数据安全保护，在采集、加工处理、展示、存储、访问等各阶段采取有效的安全机制保护银行和客户数据。

（2）银行业业务安全体系防御策略建设关键点

如第二章所述，当前黑灰产已形成产业化作业，生物识别、大数据、云计算等新型技术也可被其利用，使黑灰产在业务交易层面的攻击手段更加隐蔽，往往隐匿于大量正常客户交易行为中；同时银行侧的交易环节通常处在黑灰产整体作案过程的最后一环，银行难以全面感知攻击链路，建立有效的业务安全防御策略更具挑战性。

为了应对挑战，银行也必须在事前、事中和事后各阶段形成全行级体系化、主动化的业务安全防御策略。在事前阶段，业务安全防御策略应与业务交易同步设计、同步建设、同步上线，使业务交易具备自生风险防御能力，可大幅提升防御效果。在事中阶段，应围绕业务交易层面常见的安全风险（如欺诈、信息窃取、薅羊毛、洗钱、赌博等违规交易）和黑灰产常用的作案手段，不断丰富风险识别策略和不断提升交易覆盖面。为了保障风险防御策略的精准性，可重点从丰富风险识别手段、风险识别要素、差异化风险识别特征、弹性化风险处置等方面提升。如风险识别手段可包含规则评分、机器学习模型、关联图谱模型或 AIGC 大模型；风险识别要素可包含当笔交易的异常要素（如 IP、终端、账号、客户等）、客户交易行为（如频次、金额、时间）、客户历史交易行为比对等；差异化风险识别特征指建立“一客一策”或“一户一策”；弹性化风险处置指可根据风险等级、交易场景、客户诉求等维度执行层层递进的处置策略，如直接拦截、增强认证、远程外呼、延迟支付、弹窗提醒等。在事后阶段，应建立敏捷的防御效果感知机制，能根据防御效果及时调整风险防御策略。此外，在各阶段应建立黑灰产情报动态跟踪和应用机制，通过外部情报数据引入与合理应用，实现知己知彼、主动式精准防护。

（3）银行业业务安全防御体系管理机制建设关键点

如前所述，业务安全防御体系需各业务经营部门、中后台风险合

规管理部门及科技部门的紧密配合。为此，可建立全行级的管理办法和指引方针，明确各部门的职责和工作内容。此外，围绕防御策略在各阶段的落地应建立配套的管理机制和流程，如业务安全评估机制、风险策略开发及上线机制、客户投诉机制、工作信息交流机制、风险数据共享机制、检查及考核机制等。

五、银行业业务安全发展趋势与展望

（一）业务安全建设不断夯实，体系标准更加完善

银行业务安全领域发展逐渐成熟，持续推进标准化建设，银行业业务安全是一个持续发展的领域，未来充满着挑战和机遇。随着技术的不断发展和安全威胁的日益增加，银行业在保护客户资产和数据安全方面面临着巨大的压力。为了应对这些挑战并保障业务的可持续发展，标准化建设可帮助银行业业务安全规范相应的制度和策略，为银行业提供一套统一的准则和指导方针，确保安全防护措施得到一致性的应用和执行。2022 年，中国信息通信研究院联合多家企业撰写了《面向云计算的零信任体系 第 5 部分：业务安全能力要求》，从内容安全、交易安全、信贷安全、营销安全、钓鱼安全、防伪溯源、私域安全、风控中台等方面进行能力要求规范，旨在为企业在进行功能设计、产品研制、能力评估，以及对自身业务安全体系建设时提供参照。

（二）聚焦关键技术创新，集合产学研力量加强攻关

银行业对于创新技术的资源投入将持续增加，银行业未来在数字化转型上的资源投入会持续、稳定、高速增长，而在其整体资源投入中，业务安全体系建设的投入会成为侧重点，越来越多的银行开始重视业务安全，并将“科技创新”作为自身的发展战略，以保证全面数字化转型下的业务安全。

产、研、学力量的集合将加快业务安全体系的搭建进程，加速攻破业界痛点。多方力量的融合可以帮助业界更好地把握产业最新发展趋势，助力业务安全产业健康发展。中国信息通信研究院云大所业务安全团队也将持续助力银行业业务安全平台建设，加强企业间沟通交流，对标国际优秀实践，开展技术研究、供需对接、产业交流。结合各方技术优势互补，助力用户构建可靠安全的业务安全体系，推动银行业数字化进程不断升级。

（三）业务安全重视程度不断增加，业界内外均展开意识理念培养

在银行业务安全的发展中，强化业务安全教育理念将成为趋势，银行业界内外都会加强业务安全理念建设。

一是会加强全民业务安全意识的培养，未来社会各界会加强面向大众宣传的业务安全理念知识，培育业务安全文化建设，提高民众的安全意识，减少诸如薅羊毛、欺诈等业务风险发生的可能性。

二是会加强对从业人员的业务安全理念教育，银行业信息安全的理念建设是银行安全文化的核心，关系到员工对安全重要性的认识、行为准则以及整个组织对安全工作的态度。银行业需加强对员工的安全意识培养，深刻认识到安全对于银行业务的重要性，并确立银行的安全价值观，将安全作为银行文化的重要组成部分，并将其融入到各项业务和决策中，最后通过加强危机意识的培养，让员工知道如何在面临安全事件时快速反应和有效处理。

三是会更加重视业务安全从业者的人才培养，未来银行业更趋向于为员工提供定期的安全培训和学习机会，包括最新的网络安全威胁和攻防技术，提升有效的安全应对能力，并通过各种手段吸引优秀的安全专业人才加入银行，打造懂业务、懂技术的复合型人才，进一步强化银行业界的业务安全体系建设。

若您对本白皮书有任何建议，请联系：

95568server@cmbc.com.cn
welcome@caict.ac.cn