

ICS 03.060
CCS A 11

Q/CMBC

中国民生银行企业标准

Q/CMBC 008—2023

中国民生银行智慧金融服务标准

Enterprise standard of smart finance services of China Minsheng Bank

2023 - 11- 30 发布

2023 - 11- 30 实施

中国民生银行 发布

目 次

前 言	II
引 言	III
1 范围	1
2 规范性引用文件	1
3 术语与定义	1
4 网络系统安全	2
5 服务功能	9
6 数据治理能力	13
7 服务及技术创新	23
8 实施保障	27
参 考 文 献	29

前 言

本文件按照GB/T 1.1—2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》给出的规则起草。

本标准由中国民生银行股份有限公司提出。

本标准起草单位：中国民生银行股份有限公司。

本标准主要起草人：王海峰、郭婷婷、石菁菁、龚育民、李凡、齐少蕾、李洪伟、方应飞、石鑫俊、何鹏、郭晓波、丁妍、解朝辉、范瑞恒、杨岚。

本标准为首次发布。

引 言

智慧银行作为移动互联网、人工智能、大数据、云计算、区块链、物联网、虚拟现实等新兴技术与金融业深度融合的新业务，具有线上化、平台化、场景化、智能化和数字化等特点，是金融科技发展的高级形态，是金融业在数字化基础上的转型升级，代表金融业未来发展趋势，并成为其核心竞争力。发展智慧金融有利于推动金融机构提高效率、降低成本，有利于增强金融产品和服务的灵活性、适应性与普惠性，有利于提高风险防控能力，有利于促进金融科技的发展。

为提升中国民生银行智慧金融服务标准和服务水平，增加智慧金融服务领域的标准供给，促进智慧金融服务健康发展，中国民生银行发布《智慧金融服务企业标准》，对发挥企业标准引领质量提升、促进消费升级和推动金融业务转型升级等方面具有重要意义。

本文件参照国家、金融行业相关标准，根据业界当前的实践，采用半形式化的方式给出了智慧金融服务的主要服务功能及属性，主要涉及网络系统安全、服务功能、数据治理能力、服务及技术创新、实施保障五个方面，旨在明确中国民生银行智慧金融服务标准，促进智慧金融服务规范、健康发展。

中国民生银行智慧金融服务标准

1 范围

本文件规定了本行智慧金融服务要求，明确了智慧金融服务安全、功能、数据、创新及前瞻性标准，确立了智慧金融服务实施保障机制。

本文件适用于本行所有境内机构的智慧金融服务，包括运用移动互联网、人工智能、大数据、云计算、区块链、物联网、虚拟现实等新兴技术与银行业务深度融合的新服务。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 20988-2007 信息安全技术 信息系统灾难恢复规范

GB/T 35273—2020 信息安全技术 个人信息安全规范

GB/T 36073-2018 数据管理能力成熟度评估模型

GB/T 39786—2021 信息安全技术 信息系统密码应用基本要求

JR/T 0071—2020 金融行业网络安全等级保护实施指引 第1-4部分：基础和术语、基本要求、岗位能力要求和评价指引、培训指引

JR/T 0168—2020 云计算技术金融应用规范 容灾

JR/T 0171—2020 个人金融信息保护技术规范

JR/T 0197—2020 金融数据安全 数据安全分级指南

JR/T 0201—2020 金融科技发展指标

JR/T 0223—2021 金融数据安全 数据生命周期安全规范

3 术语与定义

下列术语和定义适用于本文件。

3.1 智慧金融 (smart finance)

移动互联网、人工智能、大数据、云计算、区块链、物联网、虚拟现实等新兴技术与金融业深度融合的新业态。

3.2 APP (application)

基于软件的提供部分或全部服务的机制。

3.3 API (application programming interface)

软件系统不同组成部分衔接的约定。

3.4 服务 service

至少有一项活动必需在组织和客户之间进行的组织的输出。

3.5 客户 customer

已经或要发生直接交易关系的对象。

3.6 产品 product

在组织和顾客之间未发生任何交易的情况下，组织能够产生的输出。

[GB/T 19000-2016，定义3.7.6]

3.7 远程银行 air bank

单独组建或由客户服务中心转型形成，具有组织和运营银行业务职能，借助现代化科技手段，通过远程方式开展客户服务、客户经营的综合金融服务中心。

[T/CBA 204-2019 (R[1]2022)，定义2.1]

4 网络系统安全

4.1 信息安全

4.1.1 安全技术通则

智慧金融服务信息安全应符合GB/T 35273—2020《信息安全技术 个人信息安全规范》、JR/T 0071—2020《金融行业网络安全等级保护实施指引》第1-4部分（包括基础和术语、岗位能力要求和评价指引、培训指引）、JR/T 0171—2020《个人金融信息保护技术规范》等相关标准的要求，应至少满足GB/T 39786—2021《信息安全技术 信息系统密码应用基本要求》中对信息系统第三级密码应用的基本要求，并在国家标准和行业标准的基础上，增加包含客户端、网络及个人信息保护在内的安全标准。

4.1.2 安全管理

我行已通过ISO27001认证。安全管理应包括以下内容：

- a) 应建立网络安全责任制，按照“谁主管谁负责，谁运行谁负责”的原则承担辖内网络安全风险防范的主体责任；
- b) 应加强网络安全工作检查考核，完善考核机制，明确考核内容，压实责任，确保网络安全责任层层落实；
- c) 应建立信息安全各领域活动的管理办法、制度规范、操作流程、实施细则、技术标准和表单模板等，用于指导日常信息安全管理行为。

4.1.3 信息资产管理

信息资产管理应包括以下内容：

- a) 应建立清晰的资产清单，明确各信息资产的所有者、使用人、保管人等相关责任人，制定各自的职责和权力；

- b) 应依照信息资产的类型、敏感程度等差异情况，对信息资产进行分类分级。对分类分级的信息资产采取不同的安全保护措施，制定完善的访问控制策略，防止未经授权的使用。

4.1.4 人员安全管理

人员安全管理应包括以下内容：

- a) 应加强人员身份管理，应在人员入岗、岗位调整和离岗时，按照流程及时进行用户身份创建、关联变更、挂起冻结等操作，用户身份信息应真实有效，不得出现冒用或交叉使用；
- b) 应通过正式的信息安全培训，以及网站、简报、会议、讲座等各种形式的信息安全宣贯活动，不断加强全员信息安全意识，提高信息安全技能。

4.1.5 系统安全管理

系统安全管理应包括以下内容：

- a) 应建立健全网络与信息系统安全管理制度，明确管理职责，严格管理网络接入、系统变更和远程访问控制，并建立相应的审批机制、安全保护和审计措施；
- b) 项目应在规划与立项阶段同步考虑安全需求，信息安全管理机构负责对项目的安全需求、技术方案进行安全评审并提出相应的建议，未通过安全评审的项目不得立项、上线；
- c) 开发和测试环境应受到严格控制，信息系统开发环境、测试环境和生产环境应采取严格的隔离措施；
- d) 应定期对网络和应用信息系统进行安全检测、漏洞扫描等安全检查。检测、扫描和评估结果属敏感信息，不得向外界提供，国家及行业主管部门另有规定的按照相关规定执行。

4.1.6 访问控制管理

访问控制管理应包括以下内容：

- a) 应制定用户授权管理流程，明确权限申请、权限分配、权限变更、权限回收、权限核查等活动，基于最小原则对用户进行授权，确保用户获得的权限与其岗位职责相一致，并定期对权限进行核查；
- b) 对应用系统及数据的访问应采用必要的认证手段，按照系统级别、用户权限等方面采用不同的认证方式。应妥善保管本人用户身份认证因素及安全设备或工具，只允许本人使用，严禁转借他人使用；
- c) 存储介质必须受到控制和物理保护。禁止将敏感数据泄露给未授权访问的人员，对于不再需要的介质应对其内容进行清除；
- d) 应对第三方访问和网络接入建立严格的审核及准入机制，并严格管控和审核第三方访问活动，限制非必要的访问以降低信息泄露的风险；
- e) 对应用系统和信息的访问应只限于已授权用户，控制措施包括但不限于：应用系统应制定符合其业务需求的访问控制策略；应具备监控重要信息系统安全现状的能力，以防止恶意软件、黑客攻击所造成的未授权访问；应定期检查网络、操作系统、应用系统等访问情况等。

4.1.7 信息安全事件管理

信息安全事件管理应包括以下内容：

- a) 应建立完备的信息安全事件管理体系，对信息安全事件进行分级，规范信息安全事件报告、处理、总结的过程，明确责任部门，建立问责机制；

- b) 应建立信息安全通报机制，通过对全行信息的及时预警、监控和通报，提升我行应对网络安全威胁的防控和应急响应处置能力；
- c) 信息安全事件应急处置后，应对信息安全事件应急措施、处置过程及控制结果进行复盘和总结，提升信息安全事件的应急处置能力。

4.1.8 客户信息安全管理

应对客户的账户信息、鉴别信息、金融交易信息、个人身份信息、财产信息、信贷信息和其他反映特定个人金融信息进行严格保护，制定相应的相关管理制度，在管理制度中对客户个人信息等进行明确分类分组定义。

客户信息生命周期包括从客户信息产生开始，历经采集、传输、存储、使用、删除、销毁的整个过程。

客户信息安全管理遵循以下原则：

- a) 目的明确原则，应明确客户信息活动的安全防护目标和要求，确保数据活动的合法性和正当性。
- b) 知情同意原则，在进行个人客户信息、单位客户的非公示信息采集和处理前征得个人和单位客户的合法有效授权同意。
- c) 最小够用原则，在保证业务功能完整实现的基础上应赋予不同安全等级客户信息最小的操作权限，客户信息使用单位应设立严格的权限管理要求，仅将工作所需最小范围的数据向指定人员开放权限，且处理的客户信息为业务所必需的最小数据类型和数量。
- d) 全程可控原则，应采取与客户信息级别相匹配的安全管控机制和技术措施，确保客户信息在全生命周期各环节的保密性、完整性和可用性，避免客户信息在全生命周期内被未经授权访问、破坏、篡改、泄漏或丢失等。
- e) 可审计原则，对于高等级安全域的数据活动，需要记录整个数据活动相应的操作记录，记录应可追溯可审查。

4.1.9 安全检查和评估管理

安全检查和评估管理应包括以下内容：

- a) 应定期检查和评估信息系统的安全性，确保信息安全现状符合国家的法律法规、行业监管及相关标准的要求；
- b) 依据国家相关规范，每年对关键信息基础设施、网络安全等级保护系统开展安全检测、等级保护及安全风险评估工作，并通过测评、监督、检查，持续改进重要信息系统的安全保护措施；
- c) 应依据国家及监管机构要求，开展网络安全审查申报及配合工作；
- d) 依据国家相关法规，制定密码应用管理制度，使用国家密码管理部门认可的商用密码技术、产品和服务，对关键信息基础设施、网络安全等级保护三级以上等系统使用密码保护，并定期开展商用密码应用安全性评估。

4.2 数据安全

4.2.1 数据安全通则

智慧金融服务数据安全应符合JR/T 0197—2020《金融数据安全 数据安全分级指南》、JR/T 0223—2021《金融数据安全 数据生命周期安全规范》等相关标准的要求。

应依据法律法规和监管规范开展数据分类分级工作，具体要求如下：

- a) 制定数据分类分级和数据安全定级的相关管理制度，在管理制度中明确数据分类分级和数据安全定级的组织保障和职责分工；
- b) 明确数据分类分级原则、数据分类框架、数据分级框架，按照数据分类分级原则和框架开展数据安全分类分级工作，形成数据分类分级清单；
- c) 制定数据安全定级流程，开展数据安全定级工作。

4.2.2 数据生命周期安全

数据安全保护措施应覆盖包括采集、存储、传输、使用、删除、销毁完整的数据生命周期。

4.2.2.1 数据采集安全

- a) 从个人信息主体采集数据，安全要求如下：
 - 1) 应通过隐私政策等方式向用户明确告知智慧金融服务过程中收集用户个人信息的类别、目的、方式和范围等，以及收集、使用个人信息的规则，并获得个人信息主体的明示同意；
 - 2) 应仅采集与智慧金融服务相关的数据，不得超出隐私政策中约定的范围，并按照服务所需最低频率采集数据；
 - 3) 应对数据采集过程进行日志记录，并采取技术措施确保日志来源的可追溯性，以及日志内容的完整性；
 - 4) 通过客户端收集数据时，在智慧金融服务完成后应清除缓存中3级及以上个人信息，不得本地留存。
- b) 从外部机构采集数据，安全要求如下：
 - 1) 应与外部机构在合同或协议中明确双方的数据安全责任及义务，明确数据采集范围、频度、类型、用途等；
 - 2) 涉及个人信息时，外部机构应说明其个人信息的来源，并确认来源合法性，同时说明所获个人金融信息主体的授权内容，包括使用目的，是否授权同意转让、提供、共享、公开披露等情况。

4.2.2.2 数据存储安全

- a) 应依据最小够用原则存储数据，不应以任何形式存储非业务必需的数据；
- b) 数据存储时间应为实现信息主体授权使用目的所必需的最短时间，超出存储期限后，应对数据进行删除或匿名化处理；
- c) 存储3级及以上数据时，应采用加密、访问控制等安全技术措施保证数据存储的保密性；
- d) 应对生产数据定期备份，并进行恢复验证，保证备份数据的有效性和可用性。

4.2.2.3 数据传输安全

- a) 在数据传输过程中，应采取数字签名、身份认证、密码技术等措施保障数据传输的抗抵赖性、可信性和完整性；
- b) 应在数据传输完成后立即清除传输历史缓存数据，传输不完整时清除缓存数据。

4.2.2.4 数据使用安全

- a) 应根据数据使用人员的角色和业务职能，按“最小授权”“不相容”原则确定2级及以上数据的访问权限规则；

- b) 2级及以上的数据使用应留存相关日志，日志应至少包含明确的主体、客体、操作时间、具体操作类型、操作结果等；
- c) 展示3级数据时，应采取展示屏蔽等措施，防止数据在展示过程中泄露；
- d) 开发测试应使用虚构的或经过去标识化处理的数据，禁止使用真实数据。

4.2.2.5 数据删除和销毁安全

- a) 应依据国家及行业主管部门有关规定及与个人金融信息主体约定的时限等，针对不同类型的数据设定其数据保存期；
- b) 对于超过国家及行业主管部门、金融服务合作方有关规定及合同协议所述保存期限的数据，应执行数据删除操作并做好记录。

4.3 网络安全保障能力

4.3.1 分类分级

4.3.1.1 信息系统分级

根据面向客户的直接程度、账户处理的时效性、与其他应用关系密切程度等因素，将所有信息系统分为A、B、C、D四个等级。

- a) A类应用：主要包括面向客户、涉及账务处理且时效性要求极高的应用类产品，或者与其他多个应用有密切相关的应用类产品。
- b) B类应用：主要包括面向客户、涉及账户处理且时效性要求较高的业务处理类或业务管理类系统，或者与其他应用相关性较高的应用类产品。
- c) C类应用：主要包括经营分析类系统、不涉及账务处理的业务系统、非直接面向客户的业务系统。
- d) D类应用：主要指面向内部管理、时效性要求较低的业务系统。
- e) 对于支撑类系统，系统故障可能影响后台多个系统正常运行，在进行应用分类等级划分时，划分标准应与后台受影响系统中等级相对较高的系统一致。特别是与报价等相关的信息系统，重要性较高，在进行应用分类等级划分时应充分考虑其重要性和敏感性。
- f) 对于和多个系统紧密关联的信息系统，在进行应用分类等级划分时，应考虑该系统故障时受影响的其他系统，划分标准应与受影响系统中等级相对较高的系统一致。

4.3.1.2 信息系统灾备分级

信息系统灾备等级分为5、4、3、2、1、不适用，灾备等级划分原则：

- a) 信息系统灾备等级分为5、4、3、2、1、不适用共6种类型，5级属于高灾备等级，4级属于中灾备等级，3、2、1级属于低灾备等级，“不适用”表示该应用不需要实施灾备，通常为工具类应用、客户端类应用及平台框架类应用；
- b) 灾备等级与应用分类原则上有如下对应关系：A类对应灾备等级5级或4级，B类对应灾备等级4级或3级、C类对应灾备等级2级，D类对应灾备等级1级或不适用；
- c) 对于部分信息系统，如该系统被“高灾备等级”信息系统为实现核心业务服务所实时调用，则其灾备等级要保持和“高灾备等级”信息系统一致；
- d) 对于多个生产信息共用设备和架构的情况，应按照信息实施对应的灾备等级保障策略；
- e) 如果灾难情况下有应急措施可满足业务需求，或者因技术因素受限，相关灾备系统要求可适当降低。

4.3.1.3 信息系统安全保护分级

根据安全等级保护相关管理文件，总行信息系统安全保护等级分为一级、二级、三级、四级，等级划分原则：

- a) 第一级：自主保护级，信息系统受到破坏后，会对公民、法人和其它组织的合法权益造成损害，但不损害国家安全、社会秩序和公共利益。
- b) 第二级：指导保护级，信息系统受到破坏后，会对公民、法人和其它组织的合法权益产生严重损害，或者对社会秩序和公共利益造成损害，但不损害国家安全。
- c) 第三级：监督保护级，信息系统受到破坏后，会对社会秩序和公共利益造成严重损害，或者对国家安全造成损害。
- d) 第四级：强制保护级，信息系统受到破坏后，会对社会秩序和公共利益造成特别严重损害，或者对国家安全造成严重损害。
- e) 对于涉及客户身份、资产、交易记录等敏感信息的重要信息系统，原则上信息系统安全保护等级定为较高级别。
- f) 信息系统安全保护等级与应用分类原则上有如下对应关系：A类对应等级保护第四级和第三级，B类对应等级保护第三级、C类和D类对应等级保护第二级和第一级。

4.3.1.4 重要信息系统清单

应定期开展重要业务和渠道关联系统分析，分析其依赖的信息系统及资源需求，梳理重要信息系统清单。通过审议后，最终确认重要信息系统清单。重要信息系统清单可通过管理系统查看。

4.3.2 指导原则

4.3.2.1 灾备策略

不同灾备等级的信息系统，其应用的本地可用性、同城可用性及异地灾备策略不同。

- a) 灾备等级5应用可用性
 - 1) 本地可用性：
 - 应用服务器应实施负载均衡。
 - 数据库服务器应优先考虑 MySQL MHA、DB2 HADR 或 Oracle RAC 等方案，其次实施 HA 高可用；数据库服务器建议使用中高端 PC 服务器。
 - 存储数据实施本地定期（至少每天一次）磁带备份。
 - 2) 同城可用性：
 - 在同城站点应用服务器应实施负载均衡。
 - 在同城站点数据库服务器应实施高可用部署。
 - 应对主站点数据实施数据库级或存储级复制。
 - 3) 异地灾备：
 - 原则上在异地站点预先分配应用服务器和数据库服务器用于主站点的灾难切换。
 - 应对主站点数据库实施数据库级、存储级或备份级复制。
- b) 灾备等级4应用可用性
 - 1) 本地可用性：
 - 应用服务器应实施负载均衡。
 - 数据库服务器应实施 HA 高可用；数据库服务器优先使用中高端 PC 服务器。
 - 存储数据实施本地定期（至少每天一次）磁带备份。

- 2) 同城可用性：
在同城站点应用服务器原则上应实施负载均衡。
在同城站点预分配数据库服务器单机部署。
应对主站点数据实施数据库级或存储级复制。
- 3) 异地灾备：
应对主站点数据实施不低于备份级复制级别容灾。
- c) 灾备等级3应用可用性
 - 1) 本地可用性：
应用服务器应优先实施负载均衡，其次实施 N+1 备份。
数据库服务器应实施 HA 高可用；数据库服务器优先使用中高端 PC 服务器。
存储数据实施本地定期（至少每天一次）磁带备份。
 - 2) 同城可用性：
应对主站点数据实施存储级或备份级复制。
 - 3) 异地灾备：无。
- d) 灾备等级2和灾备等级1应用可用性
 - 1) 本地可用性：
应用服务器应优先实施负载均衡，其次实施 N+1 备份。
数据库服务器应优先实施 HA 高可用，其次实施冷备或者单机；数据库服务器应使用中高端 PC 服务器。
存储数据实施本地定期（至少每周一次）磁带备份。
 - 2) 同城可用性：无。
 - 3) 异地灾备：无。
- e) 原则上应用服务器要求优先使用容器或者虚拟机部署；非MySQL/DB2/Oracle数据库应结合其产品技术特点参照以上标准采用类似技术实施本地高可用保障，并在总体方案中明确说明；对于应用内部提供不同功能的物理节点，可以依据可用性要求不同，进行有差异的可用性设计及部署，但这种情况应说明原因并提供详细的可用性方案。

4.3.2.2 灾备建设

原则上重要业务依赖的信息系统应优先考虑灾备建设，或者灾备4级及以上的信息系统应优先考虑灾备建设。

4.3.2.3 应急预案更新与评审

原则上A、B、C、D类信息系统每年应至少进行一次应急预案更新和评审工作，并保留重检记录。

4.3.2.4 灾备切换演练

原则上灾备等级为5、4的信息系统应在三年内至少实施一次灾备切换演练，演练应以真实业务接管为目标，验证灾备系统有效接管信息系统及安全回切的能力。

4.3.2.5 性能和容量评估

原则上A、B、C、D类信息系统每年应至少进行一次性能和容量管理评估工作，并保留评估记录。

4.3.2.6 基础安全保护能力

不同安全保护等级的信息系统，应具备的基础安全保护能力不同。

- a) 第一级：应能够防护系统免受来自个人的、拥有很少资源的威胁源发起的恶意攻击、一般的自然灾害、以及其他相当危害程度的威胁所造成的关键资源损害，在系统遭到损害后，能够恢复部分功能。
- b) 第二级：应能够防护系统免受来自外部小型组织的、拥有少量资源的威胁源发起的恶意攻击、一般的自然灾害、以及其他相当危害程度的威胁所造成的重要资源损害，能够发现重要的安全漏洞和安全事件，在系统遭到损害后，能够在一段时间内恢复部分功能。
- c) 第三级：应能够在统一安全策略下防护系统免受来自外部有组织的团体、拥有较为丰富资源的威胁源发起的恶意攻击、较为严重的自然灾害、以及其他相当危害程度的威胁所造成的主要资源损害，能够发现安全漏洞和安全事件，在系统遭到损害后，能够较快恢复绝大部分功能。
- d) 第四级：应能够在统一安全策略下防护系统免受来自国家级别的、敌对组织的、拥有丰富资源的威胁源发起的恶意攻击、严重的自然灾害、以及其他相当危害程度的威胁所造成的资源损害，能够发现安全漏洞和安全事件，在系统遭到损害后，能够迅速恢复所有功能。

4.3.3 应用实践

民生银行已建设“两地三中心”灾备体系，北京马坡机房为主中心，北京鹏博士机房为同城灾备中心，郑州的河南电信机房为异地灾备中心。重要信息系统灾备覆盖率为100%。2022年网络安全等级保护测评中均获得“优级”。关键信息基础设施的安全性得到有效保障，完成4次真实带载的关基切换演练，实现遇到灾难性突发事件时“令下即切，切即可用，用可持续”，业务连续性保障水平大幅提升。

5 服务功能

5.1 线上化服务

5.1.1 线上服务渠道

5.1.1.1 网上银行渠道

网上银行服务功能包括个人客户服务功能、对公客户服务功能、公共安全服务功能。

- a) 个人客户服务功能包括：账户管理、转账汇款、支付服务、存款服务、贷款服务、银行理财服务、银行代销产品服务、投资交易类服务、综合金融服务、客群专属服务、网点联动服务、线上客服类服务、消息类服务、API输出业务、信用卡类服务。
- b) 对公客户服务功能包括：账户管理、转账汇款、票据服务、现金管理服务、对公存款服务、银行理财服务、投资交易类服务、商户服务、贸易金融服务、网络融资服务、客户专属服务、功能设置类服务、银企直联服务。
- c) 公共安全服务功能包括：身份认证、安全工具、交易安全、个人信息保护。

5.1.1.2 手机银行服务渠道

手机银行服务渠道指以移动电话等智能设备为载体，用户通过使用特定手机银行客户端程序自助使用的综合金融服务。手机银行服务渠道用户范围包括个人客户、企业客户，对特定客户群体提供个性化服务的专属服务，包括私人银行客户、老年客户、小微客户等；服务功能包括基础平台和安全体系类功能、线上金融服务类功能、综合金融服务类功能。

- a) 基础平台和安全体系类功能包括：平台基础服务、安全认证服务、专属服务、营销工具、证书更新、权限及限额管理等；

- b) 线上金融服务类功能包括：账户查询管理、转账汇款、电子支付、投资理财、跨境金融、贷款、信用卡等；
- c) 综合金融服务类功能包括：围绕日常生活提供的衣、食、住、行、游、购、娱等增值服务。

5.1.1.3 微信银行渠道

微信银行服务渠道指通过微信公众号、小程序提供银行服务的渠道。

- a) 微信银行服务功能包括账户服务和其他服务。
 - 1) 账户服务包括：账户查询、账户信息即时通、信用卡服务、理财服务等；
 - 2) 其他服务包括：在线开户、贷款申请、网点服务、智能客服等。
- b) 小程序服务功能包括账户管理、转账汇款、电子支付、信用卡等服务以及围绕日常生活的增值权益。

5.1.1.4 电话银行渠道

电话银行服务渠道指通过客户服务热线，采用电话自助语音和人工服务方式提供金融服务的渠道。服务功能包括交易功能、公共服务功能。

- a) 交易功能包括：账户查询、挂失、同名转账、代缴费等服务；
- b) 公共服务包括：开户行查询、基金净值查询等服务。

5.1.1.5 远程银行渠道

远程银行服务渠道指客户发起与远程柜员的音视频交互服务。服务功能包括个人客户服务、对公客户服务。服务范围包括但不限于：

- a) 业务咨询；
- b) 业务查询；
- c) 交易办理；
- d) 投诉受理；
- e) 风险排查；
- f) 增值服务。

[T/CBA 204-2019 (R[1]2022)，4.2]

5.1.2 线上服务渠道应用

线上服务渠道应建立全面的服务指标管理体系。通过用户数、活跃度、粘性等指标的制定、考核评估、指标结果反馈、分析提升等一系列流程，实现数据化闭环管理，促进线上化服务渠道的应用范围、应用效果和服务能力逐步提升。

5.2 智能化服务

5.2.1 智能终端设备

5.2.1.1 智能终端设备功能

智能终端设备指具备银行业务服务功能，采取客户自助操作模式或银行人员辅助客户操作模式受理，并完成客户个人、对公业务受理及业务单据等物料交付的银行设备。智能终端设备包括现金智能柜、非现金智能柜、对公智能柜、便携式移动终端、自动柜员机、单功能机具等。

- a) 现金智能柜：服务于个人客户，主要功能包括现金存取款、账户签约管理、远程银行服务等。

- b) 非现金智能柜：服务于个人客户，功能包括个人开卡、综合签约、回单打印、实物领取、远程银行等。
- c) 对公智能柜：服务于对公客户，功能包括票据业务、远程银行等。
- d) 便携式移动终端：服务于对个人客户、对公客户，功能包括开卡、开户、综合签约、理财管理、面签管理、产品签约等。
- e) 自助柜员机：服务于个人客户，功能包括现金存取款。
- f) 单功能机具：服务于个人客户、对公客户，功能包括回单管理、票据业务办理、远程银行等。

5.2.1.2 智能终端设备布放

智能终端设备布设于银行营业场所，包括营业厅堂、24小时服务区域。布放安装应符合安全环境要求和当地公安部门相关要求。

5.2.2 远程银行服务

远程银行服务于个人客户、对公客户。

- a) 个人客户服务包括：账户管理、个人信息管理、交易权限管理、转账汇款、安全工具管理、存款产品、凭证管理、预约服务、公共信息查询、业务咨询等服务；
- b) 对公客户服务包括：账户管理、转账汇款、客户专属服务、功能设置类服务、公共信息查询、业务咨询等服务。

5.2.3 智能客服

智能客服服务方式包括但不限于：

a) 语音服务：通过电话渠道接入，以自助语音和人工应答的形式为客户提供业务咨询、业务办理、产品营销等银行服务。自助语音菜单或语音机器人系统应便捷友好、易于使用，能满足客户多样化服务需求。人工服务应有较明显的提示，在线响应及时，能为客户提供有效的解决方案。

b) 文本服务：通过微信、手机 APP、网站、短信等多渠道接入，以机器人或人工文本应答的形式为客户提供业务咨询、业务办理、产品营销等银行服务。各渠道应有明确的客户服务菜单，机器人和人工能快速准确识别客户需求，提供的解决方案易于理解。

c) 视频服务：通过 VTM、手机 APP 等渠道接入，以视频形式为客户提供业务咨询、业务办理、产品营销等银行服务。视频服务应充分运用人机交互协助、远程智能控制、电子化信息采集、图像识别等技术，能为客户提供安全高效、便捷灵活的解决方案。

[T/CBA 204-2019 (R[1]2022)，4.3.2]

5.2.4 智慧银行（网点）服务

智慧银行（网点）应用5G、人工智能、生物识别、区块链、物联网、VR、AR等前沿技术，将基础金融服务、综合金融服务融合，对客户精准识别，为客户提供智能化金融服务体验。

我行智慧银行已建成网点的运行，应关注客户服务体验、技术迭代更新、产品适配优化、智能应用改进。推广建设应本着“流程合规、设计合理、技术复用、充分利旧”的原则，既保留“智慧”风格、展现“智能”体验，又融入城市特色元素和客户需求。

智慧银行内已成熟运行的一站式服务场景，应在常规网点全面推广应用，包括一站式开户、一站式签约、远程面签、智能交付等。

5.2.5 智能适老化服务

智能适老化服务应坚持传统服务与智能创新相结合，在各类日常生活场景中，必须保留老年人熟悉的传统服务方式，充分保障在运用智能技术方面遇到困难的老年人的基本需求，提供更多智能化适老产品和服务；坚持普遍适用与分类推进相结合，针对老年人在运用智能技术方面遇到的突出共性问题，采取普遍适用的政策措施；坚持线上服务与线下渠道相结合，充分考虑老年人习惯，便利老年人使用；坚持解决突出问题与形成长效机制相结合，切实保障老年人基本服务需要。

5.2.6 智能精准营销服务

智能精准营销服务应满足客户个人信息保护要求，借助大数据、人工智能技术提高触达和成功率。应建立“需求洞察－策略匹配－评估反馈”细分客群营销闭环，打造数智化营销大脑，数据驱动客户需求洞察，总分行共建零售用户标签联盟，完善用户标签模型体系，精准构建用户画像体系。

5.2.7 政企合作服务

政企合作服务应通过系统对接、客户导流、信息共享，优化企业营商环境，提升企业金融服务便利度，为个人客户提供综合全面的综合金融服务。

5.3 场景化服务

5.3.1 接口类型

我行应用程序接口按照应用集成方式，分为服务端对服务端集成方式与移动终端对服务端集成方式两种。

对于服务端对服务端集成方式，主要包含两种实现形式：

- a) 应用方服务端直接调用我行应用程序接口（如REST、SOAP协议）；
- b) 应用方服务端使用我行提供的服务端SDK，间接访问我行应用程序接口。

对于移动终端对服务端集成方式，主要包含两种实现形式：

- a) 应用方移动终端应用软件直接调用我行应用程序接口；
- b) 应用方移动终端应用软件使用我行提供的移动终端应用SDK，间接访问我行应用程序接口。

5.3.2 合作方式

合作方式包含直连型、第三方合作和接口聚合。

- a) 直连型：将银行指定产品和服务能力嵌入其运营管理的应用系统，供其自用；
- b) 第三方合作：将银行指定产品和服务能力嵌入自身行业应用场景中，供其用户使用；
- c) 接口聚合：聚合商业银行应用程序接口，制定统一的接口和安全规范，直接输出给直连型合作方式第三方平台。

5.3.3 应用场景

采用自主研发的“云原生”技术架构，构建场景化解决方案和多级线上授权体系。2022年发布开放银行“民生云”品牌，输出一体化综合服务。升级“民生云·钱包”产品，支持财富类产品输出合作；新增“民生云·易付”产品，满足企业客户的多场景结算需求。

- a) “民生云·代账”助力小微企业突破“数字鸿沟”，实现财税数字化。聚焦提升金融服务普惠性，助力中小微企业数字化转型，打造“民生云·代账”服务，依托开放银行API接口，将金融服务与第三方财税SaaS平台无缝连接，帮助中小微企业及代理记账行业提升财务记账效率，跨越“数字鸿沟”。

- b) “民生云·货运”助力网络货运行业降本增效。“在全面提升实体经济运转效率的大背景下，充分调研物流运输行业的痛点问题，打造“民生云·货运”服务，为网络货运交易中的参与各方提供分账服务，提高货运平台资金管理效率，助力货运物流降本增效。

5.3.4 供应链金融

有序推进金融创新与实体经济需要、人民群众需求对接，围绕“企业供应链生态、个人生活旅程、机构平台生态、金融同业资金交易”四大场景创新生态银行商业模式，依托“技术+数据”双引擎提升智慧银行服务质效。

5.4 平台化服务

5.4.1 平台建设

建设以“分布式、云原生”为基座，以“业务中台、数据中台、AI中台”为核心的企业级架构，形成“渠道接入层、场景中台层、技术平台层”三层体系。

5.4.2 敏捷研发机制

敏捷研发产品模式过程管理包括：团队组建、需求分解、需求澄清与论证、需求决策、实施交付、定期审视与改进、验收、后评估。

- a) 团队组建：由业务主管部门、项目实施部门选定业务牵头人，与科技牵头人共同组建双人牵头负责的实施团队，包括但不限于各相关模块开发人员、测试人员、数据人员等；
- b) 需求分解：业务牵头人分解阶段性价值目标，科技牵头人根据阶段性价值目标分解本阶段业务需求条目；
- c) 需求澄清与论证：科技牵头人制定需求方案，分析、论证业务可行性、技术可行性；
- d) 需求决策：由业务牵头人进行业务可行性评估，由科技牵头人进行技术可行性评估，决策通过后共同带领团队进行交付实施；
- e) 实施交付：业务牵头人与科技牵头人共同对交付时效性和价值目标实现承担主体责任；
- f) 定期审视与改进：定期组织召开价值审视会议，依据会议决议更新下一阶段任务需求；
- g) 验收：验收内容包括但不限于任务需求完成情况、是否符合阶段性价值目标等；
- h) 后评估：跟踪投产运行成效，后评估发现未成达到价值目标的，采取熔断。

5.4.3 研发运营一体化

依托DevOps高效能研发体系和业务中台标准化、模块化开发能力，产品研发和客户对接效能提高不低于30%，提升高效系统平台对接能力和敏捷研发交付能力，丰富B端C端G端F端综合金融服务场景。

6 数据治理能力

6.1 数据管理能力成熟度

6.1.1 数据战略

围绕数据战略规划、数据战略实施、数据战略评估，开展数据战略相关工作。以数据管理能力成熟度稳健级为发展目标，争取达到量化管理级水平。

- a) 制定符合业务发展需要的数据战略；
- b) 制定数据战略实施路线图，并按计划推进落实数据战略；

- c) 明确数据战略落地实施的战略保障，如组织分工、制度保障、资源配置、文化培养等；
- d) 应用标准流程及工作方法，定期检视评估数据战略。

6.1.2 数据治理

开展数据治理组织建设、制度建设和流程规范建设，提升数据治理技术支撑能力，加强数据沟通。以数据管理能力成熟度量化管理级为发展目标，争取达到优化级水平。

- a) 明确统一的数据治理归口部门，构建数据、科技、业务各部门紧密联动的数据治理组织架构，推动全行数据治理工作的高效开展和实施；
- b) 建立数据治理制度体系，不断补充完善各类制度和规范，主要包括主数据管理制度、元数据管理制度、数据管家管理办法等；
- c) 建立数据治理相关考核制度，明确数据治理考核的目标、范围和方法；
- d) 建立健全数据认责体系，明确各方在数据治理过程中的职责，促进数据治理各项工作高效沟通；
- e) 定期进行培训和经验分享，开展数据制度相关培训和宣传，不断提高数据治理能力，在全行范围内开展数据治理文化宣贯、数据管家培训。

6.1.3 数据架构

开展元数据管理、数据模型、数据分布、数据集成与共享等方面，加强数据架构管理。以数据管理能力成熟度稳健级为发展目标，争取达到量化管理级水平。

- a) 明确主数据领域定义、业务分类、信息分类、数据项清单、数据关系等；
- b) 明确主数据系统的主责与协同管理责任；
- c) 明确主数据创建、维护、分发、删除、新增发布等管理流程；以及流程的管理机制和提升方案；
- d) 推进解决与主数据相关的重点数据质量问题；
- e) 扩展优化元数据采集范围；与数据模型管理工具等结合，规范提升库表元数据质量；
- f) 与指标管理系统结合，规范指标元数据信息；
- g) 制定统一的元数据管理规范，优化开发，持续提升元数据服务能力。

6.1.3.1 企业级数据架构

企业级数据架构与业务架构、应用架构、技术架构共同组成了企业架构体系。数据架构是业务战略和技术实现之间的桥梁，是数据管理的基础。企业级数据架构的重点目标是从企业级视角看待数据资产，重点规划全行企业级信息模型，信息实体在架构层次上的分布，以及数据有效流转、共享、整合及存储，解决数据如何定义、如何布局、如何使用等问题，核心内容包括数据模型、数据布局（数据分布、数据集成、数据流转）等。

6.1.3.2 企业级数据架构建设原则

- a) 数据模型
 - 1) 科学性：模型体系框架参考和借鉴业界成熟经验，划分合理。
 - 2) 规范性：有数据模型规范，保证模型设计和实施过程中的命名、格式的规范性。
 - 3) 继承性：数据模型和业务模型，应用级模型和企业级模型，物理模型和逻辑模型有继承性。
 - 4) 鲜活性：模型要持续改进、维护和优化，反应业务规则的变化。

- 5) 松耦合性：通过灵活的实体和关系设计，保证模型是灵活的，可扩展的。
- b) 数据分布
 - 1) 主数据。全行所有数据按数据分类进行管理，每类数据都有一个合理的唯一管理主体、信息采集和存储系统。
 - 2) 数据一致性。数据的冗余使用中，有可靠的机制确保数据同步，对冗余数据有清晰的使用约束。
 - 3) 分布规范与管理。统一了数据分布管理规范，建立了数据分布关系应用和维护机制，明确了管理职责。
- c) 数据流转
 - 1) 数据安全性。遵从数据安全原则、按照数据安全级别采取相应的安全措施进行数据传输、数据交换。
 - 2) 数据准确性。数据传输中准确、一致、完整，有质量保证措施。
 - 3) 数据及时性。数据及时传输、交换，满足应用对数据的时效性要求。
 - 4) 流转支撑平台。建立了统一的数据流转支撑系统，对数据交换实行统一管理。
 - 5) 流转规范与管理。数据的传输、交换中进行数据准确性验证。
- d) 数据集成
 - 1) 数据完整性。实现全行多种类型数据的集成，覆盖内外部数据、总分行数据、境外机构数据、集团成员数据。
 - 2) 数据关联性。建立内部数据的关联、内外部数据的关联，形成数据的业务单一全视图。
 - 3) 集成支撑平台。建设分区的数据集成共享环境，实现实时数据、批量数据的统一采集，集中共享。
 - 4) 集成规范与管理。建立了数据集成规范及管理制度，明确数据集成管理的原则、方式和方法，实现内部数据规范整合与有序流转。
 - 5) 数据服务。提供规范、灵活、复用性强、易用性好的数据服务。
- e) 数据服务业务
 - 1) 业务支撑度。数据可以支持业务的分析和需求。
 - 2) 业务依赖度。数据以及数据服务能被业务广泛的使用。
 - 3) 迭代优化。数据应用和业务场景能形成闭环，迭代优化。

6.1.4 数据应用

以数据驱动决策为目标，结合数据战略、科技规划相关要求，加强数据共享、数据分析、数据服务水平。以数据管理能力成熟度稳健级为发展目标，争取达到量化管理级水平。

- a) 搭建统一的数据分析支撑平台，支持数据级综合分析和结果共享、支持报表级统一发布及资源整合，支持部门内部及跨部门的数据及报表分析；
- b) 建立健全数据分析应用管理办法，明确数据分析应用的常用方法、分析加工路径和管控要求；
- c) 筹建专业的数据分析团队，并形成快速响应、灵活分派的数据分析师协调机制，支撑各类数据分析需求；
- d) 建立全数据分析模型库，促进数据价值发掘和数据应用交流推广，以点带面加速推动全行数字化转型；
- e) 建立数据对外服务平台，在满足数据安全管控、数据质量管理要求的前提下，通过平台能力，整合内外部数据资源，进行数据产品共研共产，提供跨领域及行业的数据服务。

6.1.5 数据安全

围绕数据安全策略与数据安全要求，以数据管理能力成熟度稳健级为发展目标，争取达到量化管理级水平。

- a) 明确数据安全管控机制和分级保护策略，落实数据安全管控措施与管控技术，将数据安全分级保护措施嵌入业务管理与数据使用全流程；
- b) 建立数据分类分级基础制度和分类分级规则，持续推动开展关键系统信息要素的数据分类分级。

6.1.6 数据质量

围绕数据质量需求、数据质量检查与分析，全面推进数据质量提升。以数据管理能力成熟度量化管理级为发展目标，争取达到优化级水平。

- a) 制定统一的基础数据质量规则管理框架及管理流程；
- b) 持续优化数据质量规则库，扩大数据质量检核范围；
- c) 建立统一问题管理流程，支持多途径多渠道、主动全面开展问题收集和登记；
- d) 基于数据质量问题开展根本原因、影响范围分析，明确数据质量问题原因和影响；
- e) 建立数据质量问题跟踪机制，开展数据质量问题整改并制定和实施提升数据质量的长效机制；
- f) 基于数据质量检核结果、问题整改验收情况，定期发布数据质量分析报告；
- g) 建立数据质量分析知识库，提升人员对数据质量的关注度和理解，持续优化数据质量知识库。

6.1.7 数据标准

加强基础数据标准和指标标准建设。以数据管理能力成熟度量化管理级为发展目标，争取达到优化级水平。

- a) 基础数据标准：
 - 1) 对全行基础数据标准实现统一管理，提高标准制定效率，提供标准查询、在线管理和下发等功能；
 - 2) 与DDM对接实现数据标准及数据字典引用，加强开发过程的引标和落标管控；
 - 3) 持续推进数据标准落标实施，形成较为完善的标准新增和存量管控机制实施；
 - 4) 建立对基础数据标准符合度的检测和评价机制，定期发布基础数据标准符合程度的评价报告。
- b) 指标标准：
 - 1) 建立较为完善的指标标准化管控流程，采集并不断规范完善指标元数据信息，有效满足指标标准全流程管理要求；
 - 2) 满足业务和技术用户存量指标查询检索等基本需求，支持提升指标管理和指标标准制定效率；
 - 3) 梳理存量指标资源，建立统一的指标数据资源目录，加强指标资源的统一和共享；
 - 4) 参考国家、行业标准，建立业务术语字典，建立维护检查机制并提供查询渠道，提升业务术语管理和应用，加强业务术语宣贯和推广；
 - 5) 建立对指标标准符合度的监测和评价机制，定期发布指标标准符合程度的评价报告。
- c) 主数据管理：
 - 1) 明确主数据领域定义、业务分类、信息分类、数据项清单、数据关系等；
 - 2) 明确主数据系统的主责与协同管理责任；
 - 3) 明确主数据创建、维护、分发、删除、新增发布等管理流程；以及流程的管理机制和提升方案；

- 4) 推进解决与主数据相关的重点数据质量问题。

6.1.8 数据生存周期

围绕数据需求管理、数据设计和开发、数据运维管理和历史数据管理。以数据管理能力成熟度稳健级为发展目标，争取达到量化管理级水平。

- a) 建立统一的数据需求管理机制，建立数据需求收集、评审和整合的规范流程，提升数据需求管理与开发项目管理流程的一致性；
- b) 健全完善数据开发流程，建立数据开发规范，强化数据权限管控，量化评价数据开发过程的有效性；
- c) 建立数据运营维护管理，量化评价数据运营维护管理工作的有效性。持续改善数据运营维护管理方案和流程；
- d) 明确历史数据定义规范和处置规范，并制定相应的管理策略和处置流程，执行历史数据的归档、迁移和销毁工作。

6.2 企业级数据湖仓能力

围绕数据基础能力建设，依托大数据技术框架构建的融合型湖仓平台是我行数据体系的基座，实现全行数据资源统一管理。

6.2.1 湖仓建设总原则

数据湖仓采取“统筹规划、以用促建、分步实施”的建设策略，整体上遵从以下原则：

- a) 数据安全原则：数据湖仓内所有数据的采集、存储、处理、传输、使用等过程均应满足数据安全要求，具备权限控制、数据加密、数据脱敏等管理能力；
- b) 数据共享原则：推动数据湖仓内数据全面共享，在满足数据分类分级、数据授权等管理要求的条件下，建立适配不同场景的数据使用通道，满足各类使用需求；
- c) 信息架构遵从原则：数据湖仓数据资产应遵从全行的信息架构。

6.2.2 数据模型管理

明确数据湖仓平台内数据模型层次和主题划分，确定各部分数据模型的管控模式及技术规范。

6.2.3 数据分区管理

为有效管理数据，实现集约化管理，建立分区管理能力

- a) 原始数据区：规划不同来源数据的存储结构，具备按原始格式进行数据存储的能力，接入结构化数据、非结构化数据，实现数据资源“应入尽入”；
- b) 标准数据区：建立银行核心数据管理区域，按照分层分域方式管理集团化数据，可划分贴源模型层、整合模型层、共性加工层及应用集市层等，建立统一的模型管理规范；
- c) 实时数据区：具备实时数据接入能力，实现流批融合数据加工能力，支持实时类数据应用；
- d) 历史数据区：提供历史数据存储，具备长周期历史数据的在线查询能力。

6.2.4 数据生命周期管理

6.2.4.1 数据采集：

数据采集入湖仓需要严格满足数据准入的 6 项标准，确保入湖仓的数据都有明确的业务责任人，各项数据都可理解，同时都能在相应的信息安全保障下进行共享消费。

- a) 明确数据OWNER：数据OWNER由数据产生对应的流程OWNER担任，是所辖数据端到端管理的责任人，负责对入湖的数据定义数据标准和密级，承接数据消费中的数据质量问题，并制定数据管理工作路标，持续提升数据质量。
- b) 发布数据标准：入湖仓数据要有相应的业务数据标准，业务数据标准描述全行需共同遵守的“属性层”数据的含义和业务规则，是全行层面对某个数据的共同理解，这些理解一旦明确并发布，就需要作为标准在全行内被共同遵守。
- c) 认证数据源：通过认证数据源，能够确保数据从正确的数据源头入湖。认证数据源应遵循全行数据源管理的要求，一般数据源是指业务上首次发布某项数据的应用系统，并经过数据管理专业组织认证。认证过的数据源作为唯一数据源头被数据湖仓采集接入，当承载数据源的应用系统出现合并、分拆、下线情况时，应及时对数据源进行失效处理，并启动新数据源认证。
- d) 定义数据密级：定义数据密级是数据采集接入湖仓的必要条件，为了确保数据湖仓中的数据能充分地共享，同时又不发生信息安全问题，采集接入湖仓的数据必须要定密级。数据定密的责任主体是数据OWNER，数据OWNER有责任审视这些数据密级的完整性，并推动、协调数据定密工作。数据定级密度在属性层级，根据资产的重要程度，定义不同等级。不同密级的灵敏数据有相应的数据消费要求，为了促进全行的数据消费，数据湖仓中的数据应该有响应的降密机制，到降密期或满足降密条件的数据应及时降密，并更新密级信息。
- e) 数据质量评估：数据质量是数据消费结果的保证，数据采集接入湖仓不需要对数据进行清洗，但需要对数据持有量进行评估，让数据的消费人员了解数据的质量情况，并了解消费该数据的质量风险。同时数据OWNER和数据管家可以根据数据质量评估的情况，推动源头数据质量的提升，满足数据质量的消费要求。
- f) 元数据注册。元数据注册是指将采集接入湖仓的数据的业务元数据和技主元数据进行关联，包括逻辑实体与物理表的对应关系，以及业务属性和表字段的对应关系。通过联接业务元数据和技术元数据的关系，能够支撑数据消费人员通过业务语义快速地搜索到数据湖仓中的数据，降低数据湖仓中数据消费的门槛，能让更多的业务分析人员理解和消费数据。

6.2.4.2 数据加工：

数据采集入湖仓后，根据场景需求进行数据加工，消除数据中的杂质，使数据更清洁易用；进行数据主题联接，将数据转换为信息，以更方便的为业务分析人员使用和消费数据。数据湖仓系统采用企业级数据架构分层模式按照近源模型层、整合模型层、共性加工层、应用集市层，采用分层分域的方式进行数据加工。将数据由“原材料”加工成“半成品”或“成品”，支撑不同场景的数据消费需求。

- a) 近源模型层：源模型层数据是对原始数据区中的结构化数据以及非结构化数据做过结构化提取后形成的新的结构化数据，通常根据表的不同性质而采用拉链表或快照表进行历史存储，在近源模型层内按照数据来源的源系统不同，采用不同的前缀编码分域管理数据；
- b) 整合模型层：整合模型层是主题模型层，统一按主题模型进行设计，数据标准化处理后，多以拉链表形式以最小存储保留最全的历史，尽可能保留数据全貌，在整合模型层内，按照业务主题采用不同的前缀编码分域管理数据；
- c) 共性加工层：共性加工层是为了应用方便而进行数据预加工和数据预处理，以数据快照的形式存储数据，保留周期相对短一些，同时共性加工层以共性加工为主；
- d) 应用集市层：应用集市层也是为了应用方便进行数据预加工和数据预处理，以数据快照的形式存储数据，与共性加工层不同的是应用集市层是个应用领域的个性化数据加工。

6.2.4.3 数据服务：

数据服务是基于数据分发、发布的架构，将数据作为一种服务产品提供，满足客户的数据需求，既能复用并符合服务标准，又兼顾数据共享和安全。

- a) 数据服务的识别与定义：针对数据需求，规范数据服务识别过程，列出数据服务识别过程需要了解的关键内容，明确数据服务的实现方式和准入条件，提高数据服务的客复用性，减少重复建设；
- b) 数据服务的设计与实现：在服务设计与实现阶段，要定义服务契约和数据契约，重点明确服务契约所涉及的服务责任主体、处理逻辑，并以数据契约规范服务的数据个数与数据安全要求；
- c) 服务运营：随着业务需求的不断变化，服务需要随之进行调整，因此在建设中也应做好数据服务的变更管理与下架管理。

6.2.4.4 数据质量：

数据质量是一个系统性工程，但可以从以下几点描述数据质量，即数据的完整性、及时性、准确性、一致性、唯一性、有效性。数据质量管理以数据清洁为目标，以业务需求为驱动，制定政策、规范来构建数据管理机制，并通过技术工具实现自动融入日常业务。

6.3 企业级数据中台能力

6.3.1 数据中台功能架构

6.3.1.1 数据采集接入

根据业务系统的架构特性和数据应用需求，构建采集链路，开发采集工具和系统，实现对数据的全面、准确的采集，并且不断提升数据的时效性。

- a) 提供批量与实时数据采集能力。通过批量数据采集的方式，确保每日凌晨目标模块所获取到的源模块数据为真实反映源模块 T-1 日日终业务状态的数据内容，不会因变更、主动维护、切换演练、计息、计提等原因导致数据采集时点的变化而引起数据内容的差异或错误。通过实时数据采集能力，可以及时、准确地获取源模块最新的数据内容，更快的捕捉到客户的业务信息变化。
- b) 构建多种采集工具，满足异构系统、不同时效采集的需求。数据源方面，支持对关系型数据库、NOSQL数据库、流式处理系统、消息中间件系统、文本文件和文件系统等数据源的采集；采集方式方面，提供基于文件采集、基于数据库同步采集、基于消息采集等多种采集方式，并提供HTTP/HTTPS等标准协议的数据接收能力。同时，对于非结构化数据或者半结构化数据，在采集之后需强化相关的数据解析能力，使之转为结构化数据。
- c) 完善的采集调度与监控能力。支持多样化的任务管理方式，可实现多种场景的任务调度机制，对数据接入的任务支持多角度的任务监控功能，支持异常处理、重新调度等功能；支持多样化的任务调度机制，批量定时调度支持按年、月、周、日、小时、分钟定时调度，可选指定有效时间内调度，同时支持批量信号依赖调度，实时场景使用流计算引擎进行实时数据的采集和接入；支持推（push）、拉（pull）的数据使用方式，数据增量捕捉支持按时间戳、数据快照、日志等方式。

6.3.1.2 数据集中处理

根据数据内容建设规划与业务需求，对已采集的数据进行清洗、整合、加工计算，形成面向分析和面向交易的数据支持。

- a) 推进数据清洗和标准化，对缺失、错误、重复的数据进行标准化处理，并补充结构化字段，提升数据质量。
- b) 推进数据整合，根据金融主题构建维度库，对源数据根据应用场景和业务需求进行整合和维度扩充，提升数据场景化赋能能力。
- c) 完善离线与实时计算能力，建设包括SQL、Spark在内的批量、微批计算工具，以及事件感知、实时计算等实时计算工具平台，完善一体化的数据加工和分析能力。
- d) 实现湖仓一体化存储，完善离线及实时数据区，推进实时数据入湖，基于Hudi实现面向分析与交易的企业级数据基座支持。

6.3.1.3 数据共享服务

- a) 根据数据战略要求，提供数据服务的设计、研发、共享、评估的完整能力，实现数据易连接可共享；
- b) 根据数据服务特点，完善数据开放服务能力，实现数据易连接可共享。
 - 1) 制定符合业务发展需要的服务分级分类标准，建立数据服务管理体系，不断提高数据服务管理能力，使得数据更方便快捷的赋能业务；
 - 2) 明确数据服务收口，统一数据服务开发规范。具体包含服务注册、审批、发布、鉴权、分级分类、入参出参、负责人等管理功能；
 - 3) 不断提升数据服务容灾、告警及分析统计能力。具体包含服务状态监控、限流、熔断、告警管理、调用统计分析等。

6.4 数据运用于客户服务的能力

6.4.1 客户数据查询能力

企业级数据中台应具备客户数据查询能力，可通过整合客户信息数据、客户资产数据、客户持有数据、客户交易数据、客户行为数据等多种数据来源，全面覆盖企业客户的各类信息，为企业提供全方位、多维度的客户数据查询能力，支撑企业级客户类应用的各个场景。企业级数据中台应提供包括但不限于以下类型的客户数据查询能力：

- a) 支持客户信息数据查询，包括客户基础信息、联系信息、关系信息、身份信息、层级信息、账户信息等以客户为中心的各类基础数据；
- b) 支持客户资产及负债数据查询，包括客户各类资产数据、资产变动、贷款负债等数据，并提供实时数据和历史数据的查询；
- c) 支持客户持有数据查询，包括客户各类产品的签约数据、持有数据等，提供客户级、产品级、协议级等各维度的持有数据查询；
- d) 支持客户收益数据查询，包括客户投资的基金、理财、保险、储蓄等各类产品的收益数据，提供各维度总收益、区间收益以及收益趋势等数据的查询；
- e) 支持客户交易数据查询，包括客户历史交易明细、来往明细等数据的查询，以及对客户收支数据进行分类打标；
- f) 支持客户行为数据查询，包括客户的签约行为、购买行为、交易行为、操作行为、浏览行为等数据，提供全方位的客户行为分析。

6.4.2 客户标签能力

以客户标签敏捷加工为目标，以构建面向营销场景的标签体系为指引，通过平台功能建设，打造企业级数据应用工具能力，同时进行线上化的客户标签生命周期管理和价值运营。

6.4.2.1 客户建模

- a) 支持基本模型，依据客户金融资产/消费倾向/行为习惯/地区等基本属性维度进行的客户细分；
- b) 支持客户价值RFM模型：依据最近一次消费（Recency）、消费频率（Frequency）和消费金额（Monetary）三个消费特征进行的用户细分（通常最近有消费、消费频次高且消费金额高的客户意味着对企业有高价值）；
- c) 支持生命周期模型：依据引导期/成长期/成熟期/衰退期（类比产品的生命周期）等时间维度进行用户细分。

6.4.2.2 标签体系

- a) 支持规则类标签体系，包括支持行为/明细/属性数据的规则圈选，基于行为路径灵活创建标签；
- b) 支持洞察类标签体系，支持生命周期标签与分析，以及基于RFM模型划分用户价值；
- c) 支持拓展类标签体系，支持自定义模型标签，基于用户关键行为进行预测；
- d) 支持实时标签体系，满足实时运营&营销场景个性化需求。

6.4.3 客户分群能力

利用专家规则，结合机器学习算法，实现营销客群的灵活、快速圈选，结合营销自动化，支持以客户为中心的个性化营销。

6.4.3.1 客户圈选

- a) 支持提供多种自助式用户分群方式，可以精准、快捷地圈出人群包，满足多样化的分析与运营需求；
- b) 相似人群扩展，基于用户画像，通过群体的特征相似度，寻找更多类似的用户；
- c) 支持以人群为中心展示人群应用全流程。支持展示人群包从生成，到流转，最后到应用的全流程，展示人群包与之相关的营销增长平台的所有任务，支持跳转查看任务详情。

6.4.3.2 营销自动化

- a) 支持通过多渠道/平台联合对具体用户或者细分人群进行个性化营销；
- b) 支持由规则引擎来实现营销自动化的实施，同时支持运营管理后台与基础服务底层的配合实施。

6.4.4 客户洞察分析能力

为提高营销成功率，可以结合客群的特征分布画像洞察和营销效果评估，找到增长机会点并进行策略迭代，争取达成优化级水平。

6.4.4.1 可视化洞察分析

- a) 支持画像分析，展示用户画像，展示客户所处的阶段和特点，查看用户的行为路径；
- b) 支持标签透视，圈选目标群体生成洞察报告，剖析分群显著特征，通过柱状图/条形图/环状图/表格等图表形式展现每个洞察维度的群体画像表现。支持交叉分析、下钻分析等，深度挖掘客户特征；
- c) 支持多维特征分析，支持正负样本输入，辅助模型训练，基于模型精准预测，推荐最佳标签，按显著度、覆盖率、人群数量导出人群包；

- d) 支持生命周期分析，通过多种归因方式将各渠道的数据打通，并通过图表化能力展现。支持查看用户资产信息，展示各阶段关键指标，支持进行各阶段用户流转分析；
- e) 支持数据看板分析，可查看数据资产看板，支持查看用户总量/每日新增&减少用户数等，支持查看标签&分群的使用情况及热门标签。

6.4.4.2 营销效果评估

- a) 支持营销任务效果分析，展示人群包整体推送转化漏斗，点击人群和未点击人群的差异对比等。支持展示标签表现明细；不同渠道表现效果，任务整体转化情况。
- b) 支持标签透视，圈选目标群体生成洞察报告，剖析分群显著特征，通过柱状图/条形图/环状图/表格等图表形式展现每个洞察维度的群。

6.4.5 风险管理

利用"大数据+AI"构建智能实时的风险管理体系，实现风险智能感知，提升预警准确率，增强风险自动处置能力。结合线上、线下的业务场景全面应用智能模型，提升风险的全流程管理能力，提高资产质量。

建设风控中心，提供公共的、用于风险领域的策略计算服务，为各具体应用场景提供"计算器"。目前我行重点建设的几个风控策略服务如下：

6.4.5.1 风险反欺诈

目标是建立全面的反欺诈体系，包括申请反欺诈及交易反欺诈。充分运用行内外数据，包括实时与非实时数据，通过可适配的欺诈识别规则模块、关联分析模块和欺诈评分模型，对可疑的申请或交易欺诈进行识别，并根据风险等级采取相应处理，包括阻断等。其中交易反欺诈主要通过对客户账户交易流水信息的分析，识别出资金归集、商户刷单等可疑欺诈行为。我行目前建立了零售信贷申请反欺诈，在产品模块中增加了卡盗刷反欺诈；但是功能建设欠合理，并且不完善，后续的重心是将分散的反欺诈功能进行整合，打通业务条线，补充欠缺的反欺诈功能，如安全攻击等识别，真正建设全面的反欺诈体系。

6.4.5.2 风险预警

通过对商业银行授信客户所处经济周期、所处行业、所处区域的风险分级管理，结合客户关联关系、客户银企关系、客户在他行贷款表现、客户在外部不良名单、客户在外部负面舆情等多角度分析、归纳，设置动态、有效的风险预警指标和指标参数，建立灵活、可扩展的风险预警管理功能。通过对商业银行对公授信客户所处经济周期、所处行业、所处区域的风险分级管理，结合客户关联关系、客户银企关系、客户在他行贷款表现、客户在外部不良名单、客户在外部负面舆情等多角度分析、归纳，设置动态、有效的风险预警指标和指标参数，建立灵活、可扩展的风险预警管理功能。风险预警产生的预警事件结合风险流程，做到风险预警的恰当应用。

6.4.5.3 在线风评

依托大数据技术，为互联客户提供线上的风险测评服务，是线上贷款的基础服务。

6.4.5.4 数字化授信

依托大数据技术，为互联客户提供线上的授信服务，是线上贷款的基础服务。风险领域的主要目标实现全场景风险服务，共享风险结果，统一风险管控。包括风险决策引擎、风险预警、风险反欺诈、额

度管理等功能，形成公私统筹联动机制。同时面对监管或管理审计要求提供的联机风险管控系统，包括客户资产监管、监管查控、警方布控等功能，后续将利用大数据提高风险管控水平。

6.4.5.5 整合多方资源，夯实数据底座

拓展数据渠道，加强外部数据引入。构建统一风险数据集市、反欺诈数据集市等，完善基础数据模型，接入各类外部数据，与行内数据进行充分融合，形成统一、共享的数据基础。

构建指标、标签、特征体系。完善风险指标体系，提升指标体系的规范化与完备性，推进风险指标标准管理，加强风险数据加总能力建设；结合内外部数据和行为数据加强特征建设，为各类风险模型的构建提供统一风险特征集市，实现特征的共享、共用、共建。

建设关联图谱，深度识别潜在风险。构建丰富、准确、高效的客户关联关系图谱，并结合内外部数据持续完善、丰富图谱内涵，提升图谱数据的可用性、易用性。

提升数据时效，打造实时风控能力。构建实时风控的数据采集和应用体系，加强风险事件感知能力和处置能力建设，满足高时效的风险感知、风险预警、风险处置要求。

6.4.6 数据资产

通过规范化、制度化的数据资产管理流程，提高数据资产使用效率，加强数据共享，充分发挥我行数据资产价值。

- a) 制定数据资产管理制度，明确资产管理的组织架构与职责，规范数据资产管理要求及相关流程；
- b) 形成数据资产分类框架及数据资产目录卡片；
- c) 支持用户对各类数据资产快速查询、智能检索，通过资产卡片展示多视角、多维度的数据资产；
- d) 明确数据资产盘点的优先级，开展存量、增量数据资产盘点；
- e) 发布数据资产盘点成果，以供全行查询使用；
- f) 建立数据资产申报、变更、处置及审批运营管理机制；
- g) 从不同角度分析数据资产使用与共享情况；
- h) 对数据资产分析结果进行逐级汇总与细分维度展示，设计数据资产评估报告。

7 服务及技术创新

7.1 重点项目

7.1.1 智慧政务

高效联通政务信息流，搭建立体式公共服务体系。率先完成中央财政一体化项目财政部验收，积极响应财政预算一体化部署建设。建设医保、教培、行业资金监管、总行国库、非税、社保、公积金等场景化数字项目，开展“预付通”业务，升级“招标通”“银法通”“房管通”“银医”“银关税”等产品。

7.1.2 智慧营销

实现“全渠道”协同营销，连接策略库与“民生小微”APP、智能外呼等各类客户触点，精准匹配产品与客户需求；引入事件类标签，支持复杂营销策略分析；升级及时雨、营销云等数字化营销系统，

支持综合客群营销和实时活动管理。优化“全场景”增值服务，打造权益体系，快速接入多类综合金融权益产品，丰富个性化服务内容。提供“全旅程”客户陪伴，上线客户旅程全节点可视化看板，支持实时分析断点，优化客群经营链路，提供全旅程智能化客户陪伴。

7.1.3 智慧风控

用数赋智“事前防+事中管+事后控”，打造全行“人智+数智+机智”风控体系。

- a) 建设智能风控体系，升级“贷前”全面监测能力。建设人机协同的智能贷前评审体系，构建“数据+模型+场景”的辅助授信审查作业模式，提升授信审查质效；建设小微主动授信智能决策体系，利用遗传算法优化智能风控策略；引入数字化评审模型，实现银票贴现授信额度全自动核定；优化“掌中眼”营销行为管理系统，实时展示现场真实场景，预防欺诈风险。
- b) 强化“贷中”资金管控能力。打造新一代反洗钱系统，结合AI平台构建反洗钱智能模型，基于知识图谱平台提供实时反欺诈能力；打造与司法机构联通的区块链电子存证平台，确保授信业务全流程留痕可追溯、不可篡改；应用OCR、电子签名等技术，融资风险精准识别和管控效率显著提高。
- c) 提升“贷后”主动预警能力。“AI+BI”打造统一风险全景视图，持续优化中长期监测预警模型和策略，主动退出高风险贷款，贷后风险有效识别率提升近一倍。报告期内，本行应收账款融资线上签约占比达96%，业务处理时间平均节省2-4小时。

建成企业级统一资金链治理平台，以交易阻断、延迟支付、加强验证等手段拦截高风险交易，实现客户识别、风险决策、预警处置、风险倒查的全流程一体化管控，具备事前、事中、事后全生命周期风险管控能力，保护客户资金安全。

7.1.4 智慧管理

打造智慧数字化管理工具。在人力资源、财务管理、资产负债管理、办公综合等领域，建设标准化、规范化管理体系，提升协同管理效率。

建立从发现到收集数据问题，再到分析、解决问题的闭环处理机制，持续推进重点数据问题治理，进一步强化数据标准管理，制定并发布全行统一数据标准，基础数据质量明显提升。推进重点领域数据资产化，构建数据资产管理能力，完善数据治理重点工作方案并加紧推进落实。

7.1.5 智慧运营

集中运营发挥强支撑作用，通过完善操作标准、优化操作流程、简化作业岗位，集约化运营效率显著提高，以产品服务、客户支持和集中放款审核实现信融e、票融e等产品专属集中运营服务，全行线上化、智能化、精细化运营能力不断增强。

远程银行智能服务升级，扩大“智能远程柜员”、“智能坐席助手”等智能应用，“一键接入”功能为老年客户提供便捷体验。本行远程银行及电话客服接通率及客户满意度保持业内领先水平。

智慧网点转型加速，“账户机器人”优化开户体验，显著提升账户服务质效，释放一线和后台人员产能；深化大数据、RPA、OCR等新技术在运营领域的应用，持续将智能技术嵌入运营业务场景及流程，以技术应用替代标准作业；建立全场景服务断点监测优化体系，有效降低客户投诉数量；打造“对公综合服务”等新服务模式。

7.1.6 数字人民币

拓展数字人民币应用场景，成立“数字人民币应用创新实验室”，推出“对公账户直发数币薪资”等8项首发应用。

7.1.7 数字化转型应用实践

2022年，民生银行全面深化数字化转型，积极打造“敏捷开放的银行”，在体制机制、队伍建设、智慧转型、生态建设等方面统筹推进，数字化经营管理能力明显提升。

- a) 开展端到端客户旅程重塑：从重要性和可行性出发选取十余个高价值客户旅程，用数字化手段进行端到端重塑，客户体验和内部流程效率明显提升。
- b) 供应链金融生态方面：持续创新数据增信类产品，构建全链条数字服务能力。新增服务下游分销商融资的采购e-数据增信系列产品，服务上游供应商的订单e系列产品，升级票融e、信融e产品，新增采购e强增信、全棉通等产品。
- c) 金融生态方面：跨界融合共建生态，提供一站式多元场景服务。构建“民生财资云”，以资金流数字化和信息流互联互通为核心，提升企业资金管理效率。与头部平台建立生态合作，持续创新线上融资、消费贷款等生态金融产品，推出小微快贷、互联网生态贷系列产品。打造融资、账户、财富、结算、薪资代发、人事管理等综合金融服务体系，上线“企薪通”“彩银通”等生态服务产品。

7.2 服务创新性

7.2.1 产品创新

数字化产品流程更优，开开户、账户、票据、保理、电子保函、电子信用证、资金监管、财资管理、现金管理等产品操作流程显著简化。

交易银行“资金e收付”产品推出大消费、汽车销售、基金/保险销售、经营性物业、灵活用工平台等行业领先解决方案。个人养老金推出全流程产品和服务，成为首批拥有个人养老金业务开办资格的银行。上线汽车消费金融等消贷产品，创新推出纯线上信用类个人微贷产品。搭建定制化支付产品货架，支付产品和账簿体系联动，提供支付结算和资金管理综合服务，创新打造资金优先清算产品。

7.2.2 服务模式创新

数字化服务质效更高，升级手机银行、企业网银、远程银行，新增企业微信、e点通小程序等，打造“线上+线下”多维服务矩阵；数字化客户体验更佳，构建客户权益体系，引入增值服务，打造“法人+个人”一体化产品交付与服务模式。

7.2.3 平台建设创新

升级零售线上服务平台，发布手机银行7.0，打造智能账簿，新增手机银行个人养老金专区，客户体验大幅提升。全面建成小微版、私银版、长辈版、未成年版、乡村振兴版手机银行多元化、定制化专属服务体系。

升级对公线上服务平台，企业网银扩充小微客户服务场景，登录流程更简化，权限管理更灵活，客户端操作更流畅，用户体验极大提升。企业手机银行4.0提供企业管理服务能力，银企直联API对接场景持续增多。

7.2.4 科技赋能创新

数据湖仓等基础设施建设大幅提速，数据集成体系进一步优化，数据资源集成与供给质量明显提高。推进重点数据能力的中台化，为共性业务应用场景提供赋能。完善AI研发平台和AI服务平台，初步运用隐私计算、机器学习、OCR、NLP等技术创新数据应用，赋能重点业务领域。

7.2.5 社会责任实践创新

着力服务国家发展大局，积极融入国家发展战略，积极履行社会责任，深入落实ESG理念，坚持将公司金融作为助力实体经济高质量发展的重要手段，持续强化对绿色金融、乡村振兴、高端制造等实体经济重要领域的金融支持，努力践行“民生担当”。

2022年，中国民生银行入选福布斯中国ESG50。

7.3 技术创新性

7.3.1 技术创新内容

- a) 人工智能：采用机器学习、深度学习、知识图谱等人工智能技术，在虚拟仿真客服、AIoT、风控、反洗钱、信用证审单、操作流程自动化等方面进行应用探索，实现高并发自动化标准化业务场景降本增效、实时监测与多路决策提高管理效能、探索打造居家金融服务新体验。
- b) 区块链：依托于我行构建的区块链基础能力平台实现多应用场景，包括司法存证、区块链股票质押、多地域区块链发票、企业电子身份认证等。
- c) 5G：应用于手机银行、智慧银行（网点）等项目，引入5G基础网络，实现更高的响应速度和更好的实时交互体验，植入更多的动态视频，结合点播和直播，引导客户体验金融功能学习金融知识；降低移动多端适配开发成本，减少终端手机空间压力。
- d) 大数据：应用于智慧银行（网点）、风险与欺诈分析、运营优化、市场洞察、舆情分析、智能获客、智能调度等方面。
- e) 生物识别：可使用指纹、人脸、虹膜、声纹等生物识别技术认证方式，增加身份认证安全性和认证手段多样性；
- f) 云计算：宜实施基础设计IaaS云化改造和容器云PaaS建设；

7.3.2 技术创新实践

民生银行以企业级架构规划管理和企业级平台能力建设提升科技和数据能力，从全集团视角整体规划打造数字化科技底座，统筹全行科技资源布局，提升资源整合能力和组合式业务创新能力，加速技术创新成果向业务价值转化。

建设“总行云、分行云、集团生态云”，分行特色业务全面上云，数据驱动智能化运维升级；实现“全分布式”技术架构转型；建设人工智能、区块链、物联网等创新研究实验室；加固集团信息安全风险防线；分批制定并发布全行统一数据标准，基础数据质量不断提高；全行统一大数据平台促进数据资源共享。

云服务能力支撑高效研发和运维。构建支持多地多中心、一云多芯、满足金融级安全防护要求的全栈云服务底座，容器、虚拟机等敏捷资源比例达75%，基础设施资源交付效率有效提升。打造技术栈统一、组件丰富、平台健壮、弹性扩展的云原生技术平台和能力体系，2022年新建应用超35%采用云原生架构，上线部署速度明显提升。通过信通院DevOps能力成熟度模型技术运营2级（优秀级）标准认证。

7.3.3 绿色金融创新技术应用

民生银行从战略调度推进绿色金融，建立绿色金融管理体系，加大对绿色、低碳、循环经济的支持，防范环境、社会和治理风险，提升自身的环境、社会和治理表现，促进经济社会发展全面绿色转型。

运用大数据、机器学习和区块链等金融科技增强绿色信息采集、共享、分析和绿色评价，以及绿色金融业务识别和风险预警的智慧金融服务标准。通过大数据、机器学习和区块链等金融科技的应用增强绿色信息采集、共享、分析和绿色评价，以及绿色金融业务识别和风险预警能力。帮助商业银行更好地把握绿色金融市场机遇，同时提高其风险控制能力和服务水平。具体包括：

- a) 采集和共享绿色信息：通过大数据技术，收集和整合来自不同来源的绿色信息，包括环境数据、企业社会责任报告等。通过机器学习和人工智能技术对这些信息进行处理和共享，以提高信息质量和可用性。
- b) 分析绿色信息：通过机器学习和人工智能技术帮助商业银行对绿色信息进行分析，包含评估企业的环保表现、预测未来环境风险等。分析结果用于为银行提供更准确和可靠的决策支持。
- c) 绿色评价：通过运用大数据和机器学习技术，对借款企业或项目进行更全面和准确的绿色评价。这种评价包括环境风险评估、可持续发展评估等，帮助银行更好地了解借款方的环保表现和潜在风险。
- d) 绿色金融业务识别：利用大数据和机器学习技术来识别潜在的绿色金融业务机会。包括但不限于通过对环境数据和企业社会责任报告的分析，发现具有良好环保表现的企业，为金融机构提供更多潜在的合作机会。
- e) 风险预警：通过运用大数据和机器学习技术，可以对潜在的绿色金融风险进行预警。包括但不限于通过对历史数据的分析和预测模型的应用，及时发现可能出现的环境风险，为银行提供及时的风险预警和应对措施建议。

8 实施保障

8.1 组织保障

8.1.1 智慧金融领导机构设置

“一把手”挂帅的数字化金融工作领导小组负责对数字金融重大项目和资源投入进行决策，总行发展规划部作为领导小组秘书处承担全行数字化转型工作的组织推动职责。从政策导向和全行战略出发，启动《信息科技发展规划（2023-2025年）》编制工作，为提升科技能力、加快数字化转型制定发展蓝图和实施路径。

数字化金融工作领导小组是数字化金融转型工作的最高议事和决策机构。职能包括：

- a) 审定数字化金融实施方案、实施任务，统一部署整体及年度实施工作；
- b) 审定重大生态金融项目名单，指定项目负责人；
- c) 决策配置数字化金融实施方案和重大生态金融项目落地所需的财务、人力等资源；
- d) 督导数字化金融实施策略和重大生态金融项目整体推进；
- e) 协调解决数字化金融实施和重大生态金融项目推进过程中的重大争议事项；
- f) 验收数字化金融和重大生态金融项目实施成效，决策部署后续工作安排；
- g) 审定数字化金融实施和重大生态金融项目考核结果。

8.1.2 智慧金融实施推动

数字化金融工作领导小组下设数字化金融秘书处，职能包括：

- a) 编制数字化金融转型实施方案，并根据执行情况提出方案调整的建议，上报领导小组；
- b) 分解数字化金融转型实施任务，督导各项任务进展，协调及督办领导小组决策事项，并向领导小组成员通报执行情况；
- c) 定期组织召开数字化金融实施推进情况检视会议，向领导小组汇报重大事项，统筹保障会议会务，起草并提交会议决议，保管审议事项的相关档案资料；
- d) 配合开展数字化金融转型相关宣导、培训和内外部宣传。

8.1.3 智慧金融体制机制保障

应借鉴互联网金融企业运行模式，完善组织架构与机制。优化调整组织架构和职能，促进业务、风险、科技深度融合；建立大项目敏捷推进、快速迭代等机制，快速响应市场需求；建立以长期回报为导向的考核机制、试错容错的大数据风控机制，培育全行数字化经营文化与理念，让数字化转型根植每个员工心底。

由业务、风险、科技、数据等部门组成的跨职能敏捷团队深化融合，创新产品研发和迭代效率大幅提升。依托建立的常态化敏捷协同机制，小微主动授信智能决策、消贷生态合作、数字化协同办公等一系列重大转型项目均取得突破性进展。

8.2 管理制度

8.2.1 政策指导类制度

应制定政策指导类制度，可纳入年度发展规划及数字化转型实施方案中，以明确智慧金融的战略导向和发展方向，具体包括发展环境分析、战略愿景目标、业务发展策略、重点发展领域、体制机制保障、落地实施安排等。

8.2.2 场景搭建类制度

应制定场景搭建类制度，以明确智慧金融相关的场景搭建管理规范及实施标准，具体包括：搭建规范、场景选择原则、实施路径、应急方案、效果评估等。

8.2.3 产品研发类制度

应制定产品研发类制度，以确保智慧金融相关的产品研发资源合理安排，规范研发项目的管理流程，提高研发效率，具体包括：产品创新制度、项目评审制度，项目开发规范、设计规范、后评机制等。

8.2.4 测试投产类制度

应制定测试投产类制度，以确保智慧金融服务相关的项目安全、高效、顺利实施，具体包括：测试过程管理规范、测试质量管理规范、系统投产规范等。

8.2.5 生产运营类制度

应制定生产运营类制度，以确保智慧金融服务相关的生产安全与运营规范，具体包括：生产运营规范、配置规范、变更规范，以及系统、网络、数字、安全、资源等配套管理规定。

8.2.6 业务管理类制度

智慧金融服务相关服务渠道应制定渠道业务管理制度，以规范其部门职责、业务范围、经营模式、风险管理等。智慧金融服务相关业务应遵循相关产品负责部门制定的产品管理制度，包括产品主管部门职责、产品主要功能、产品运营模式、产品管理要求等。

8.2.7 服务响应类制度

应制定服务响应类制度，以确保智慧金融相关服务具备应急响应措施，妥善处理各类突发事件，保证服务的连续性，具体包括：信息系统、反洗钱、流动性、消费者权益保护等突发事件应急预案、业务连续性应急预案、生产系统事件管理办法等。

参 考 文 献

- [1] T/CBA 204-2019 远程银行客户服务与经营规范
 - [2] GB/T 19000-2016 质量管理体系
-