数据安全推进计划
DATA SECURITY INITIATIVE

大数据技术标准推进委员会
Big Data Technology and Standard Committee

银行保险机构数据安全实践指南（2024）

数据安全推进计划

数据安全推进计划
中国通信标准化协会大数据技术标准推进委员会
2024年12月

目录

数据安全推进计划

数据安全产业推进计划

一、数据安全责任体系

（一）合规要点

《银行保险机构数据安全管理办法》“第二章 数据安全治理”要求企业建立数据安全责任机制，明确数据安全责任人，指定归口管理部门负责本机构的数据安全工作，明确各业务领域的数据安全管理职责。

（二）面临问题

1. 数据安全工作缺少高层关注和全员参与

数据安全工作具备来自监管要求和业务发展的双重驱动，一方面需要企业从整体管理层面进行合规的要点宣讲、要求内化、分工协作，另一方面需要从业务层面进行落地执行、效果反馈、优化纠偏。由于数据和业务的伴生关系，数据安全风险的防范与治理往往涉及企业所有业务部门及大多数职能部门。为了推动数据安全工作的高效协作与落实，企业高层领导的关注必不可少—数据安全工作也经常被称为“一把手”工程。这也意味着，提升企业高层对数据安全工作的关注度，提升企业员工参与度，确保数据安全管理与企业战略发展同步，已成为当下亟待解决的问题。

2. 数据安全责任划分成为焦点问题

据《2023 年数据安全行业调研报告》调查情况，45.3%的企业在数据安全工作开展过程中面临数据使用部门、数据属主部门、数据安全牵头部门的数据安全权责划分不清晰，数据安全工作开展拉通困难

数据安全发展计划

大的问题。因此，在企业内部，数据安全工作“谁牵头、谁辅助、谁执行、谁监督”成为热议话题，如何建立一套行之有效的数据安全责任划分体系备受关注。

（三）合规实践建议

1. 建立覆盖全员的数据安全组织架构，提升高层参与度[1]

数据安全组织架构是数据安全治理体系建设的前提条件。通过建立专门的数据安全组织，落实数据安全管理责任，确保数据安全相关工作能够持续稳定的贯彻执行。同时，因数据安全治理是一项多元化主体共同参与的复杂工作，明确的组织架构有助于划分各参与主体的数据安全权责边界，促进协同机制的建立，实现组织数据安全治理一盘棋。

在一个企业内部，安全部门、合规部门、风控部门、内审部门、业务部门、人力部门等都需要参与到数据安全治理的具体工作中，相互协同，共同保障组织的数据安全。一种较为典型的数据安全治理组织架构一般由决策层、管理层、执行层与监督层构成，如图 1 所示，各层之间通过定期会议沟通等工作机制实现紧密合作、相互协同。决策层指导管理层工作的开展，并听取管理层关于工作情况和重大事项等的汇报。管理层对执行层的数据安全提出管理要求，并听取执行层关于数据安全执行情况和重大事项的汇报，形成管理闭环。监督层对管理层和执行层各自职责范围内的数据安全工作情况进行监督，并听取各方汇报，形成最终监督结论后同步汇报至决策层。

[1] 来自：数据安全推进计划《数据安全治理实践指南（4.0）》

来源：数据安全推进计划

图 1 数据安全组织架构示例

各层的主要分工和构成如表 1 所示。决策层以虚拟组织的形式存在，如数据安全领导小组，该小组由企业的高层领导及相关部门负责人共同构成，主要负责对数据安全的重大事项进行统筹决策。管理层一般由数据安全归口管理部门与数据安全技术保护部门构成，通常是企业内部的安全部门或数据部门，负责数据安全的管理、建设、宣贯等工作。执行部门一般由业务部门或数据生产部门构成，负责在本部门内落实执行各项数据安全管理要求。监督层涉及到合规部门、风控部门、内审部门等，负责从不同的角度对数据安全治理工作的开展情况进行监督。

表 1 数据安全组织职责分工表

	决策层	管理层	执行层	监督层
数据安全责任	组织高层领导及相关部门负责人	安全部门/数据部门	业务部门/数据生产部门	合规、风控、内审等部门
安全策略规划	牵头负责	落实执行	遵照执行	落实监督
安全工作管理	/	牵头负责	遵照执行	落实监督

安全能力建设	/	牵头负责	遵照执行	落实监督
安全制度建设	/	牵头负责	遵照执行	落实监督
安全落地执行	/	日常监督	牵头负责	落实监督
安全运营管理	/	牵头负责	遵照执行	落实监督
安全教育培训	/	牵头负责	遵照执行	落实监督

来源：数据安全推进计划

因不同企业的部门设置都有较大不同，涉及到实际治理体系建设时，不同企业还需结合现有组织架构，进行适度的调整和补充。

2. 明确各部门工作内容与权责边界，建立协同工作机制

在传统“主体责任制”的责任划分基础上，企业应充分考虑监管“谁管业务，谁管业务数据，谁管数据安全”[2]的核心思想与数据自身的强业务属性，细化数据安全责任划分机制，将数据安全融入业务规划，从源头保障数据处理活动的安全合规。建议如下：

一是应由业务部门直接参与。业务部门作为数据的生产者和使用者，对数据价值与风险有着最直观的了解。可以遵循“谁创建，谁主管；谁使用、谁负责”的原则进行数据安全责任的划分，确保数据在采集、使用和流转的每一个环节得到有效保护。

二是强化组织内部协同工作机制。建立企业内部数据安全归口管理部门、数据安全技术保护部门、业务部门、风险合规与审计部门等之间的协同工作机制，是数据安全工作能够有效承接、完整落实监管合规要求，抵御相关风险的关键举措。

三是强化监督与考核奖惩机制。企业应建立并维护一个安全稳定

[2] 来自：国家金融监督管理总局《银行保险机构数据安全管理办法》

的数据活动工作环境，这种环境的建立及维护除了依靠技术手段之外，还需要通过管理手段来激励并约束。通过建立明确的数据安全考核标准和奖惩措施，将数据安全工作纳入考核体系，可以引导员工形成正确的行为模式，自觉遵守相关法律法规和企业规章制度，促进数据安全合规文化与企业氛围的建立。

二、数据分类分级

（一）合规要点

《银行保险机构数据安全管理办法》“第三章 数据分类分级”要求企业制定数据分类分级保护制度，建立数据目录和分类分级规范，动态管理和维护数据目录，并采取差异化的安全保护措施。

（二）面临问题

1. 数据分类分级跨部门协调待提效

数据分类分级旨在根据数据的重要性、敏感程度以及业务价值等，对数据进行合理的划分与保护，以确保数据的安全与合规使用。当前，企业通常具备数据量级大、结构多样化、分布范围广等特点，在开展数据分类分级工作时，必然要面临数据、技术、业务、安全等多个部门的协调沟通，协同推进。如何统筹安排各部门工作职责、统一分类定级标准是保障数据分类分级工作高效开展的重要内容。

2. 数据分类分级工作成效待评价

数据分类分级是一项持续、动态的工作，一方面需要花费大量的

人力、物力、财力去盘点存量及增量数据资源信息；另一方面需要根据级别制定安全保护策略，让技术可行，让业务可用，以确保精细化管控的目标达成。近年来，数据分类分级作为金融监管的重要事项之一，各企业也在快速响应，积极推进，如何评价数据分类分级建设成效也成为大家关心的问题。

（三）合规实践建议

1. 建立数据分类分级组织保障，推动跨部门协同

数据分类分级是业务知识、数据知识和安全知识的交叉领域，是一项复杂的长期性工作，需要相关部门协作开展。这就需要通过明确数据分类分级工作的组织架构，划分各部门职责分工，为数据分类分级工作的协同开展提供支撑。

在实际工作中，我们观察到数据分类分级工作多由数据管理部门牵头，主要职责包括统筹工作计划、牵头数据资源盘点、制定标准规范、分类定级结果复核等内容，安全部门负责明确分级安全管理策略和技术要求，技术部门负责建设技术工具或平台，业务等其他部门负责配合执行及问题反馈。

2. 依据数据分类分级成熟度评价模型，对标建设过程及成效

2023年中国信息通信研究院牵头制定BDC 155-2023《数据分类分级成熟度评价模型》，根据PDCA的闭环工作思路，按照“规划-实施-运营”三大模块内容评价数据分类分级工作成效。

（1）数据分类分级规划

金融机构在制定数据分类分级规划时，应至少包含数据分类分级战略规划、数据分类分级的资源保障以及数据分类分级的标准设计三部分内容：

- 数据分类分级的战略规划应具备帮助金融机构为其开展分类分级工作制定指导要求，进行资源规划的能力。
- 数据分类分级资源保障应确保金融机构提供的资源保障能力能够完整覆盖分类分级工作的开展。特别是金融机构数据量级庞大、分布广泛，分类分级工作需要较强的跨部门联动能力，所以足够的高层关注和资源保障是促进数据管理部门、科技部门、职能部门与业务部门携手推进分类分级的前提条件。
- 数据分类分级标准设计应考虑监管要求、行业标准，并结合企业实际情况，明确数据范围、概念定义、执行步骤、反馈优化等工作内容，迅速对齐参与方理解与认知。尤其针对一些平台级企业和关键信息基础设施企业，对于重要、核心数据的识别管理也应当纳入分类分级的考量范围。

（2）数据分类分级实施

数据分类需要充分考虑监管要求，根据数据属性、对象、使用场景、格式等，对数据基本信息进行识别分析。金融机构应根据已制定的数据分类原则，定义包含多个层级的数据类别清单，再对数据资源清单中的数据逐个进行分类。结合金融监管要求与业实际业务场景，本指南建议将数据类型划分为客户数据、业务数据、经营管理数据、

系统运行和安全管理数据一级分类[3]。

数据定级需要充分考虑数据的重要性、敏感程度、精度、规模等诸多因素。因此，金融机构在定级过程中，可以通过综合评估数据本身的重要程度和所面临的风险危害程度。具体的评估要素应至少包括影响对象和影响程度。若定级过程中出现多个影响对象，应按照影响程度的最高等级进行判定。

影响对象是指数据一旦遭到泄露、篡改、破坏或者非法获取、非法利用、非法共享，可能影响的对象。数据安全风险涉及的影响对象包括国家安全、公共利益、组织权益、个人权益。影响程度是指数据一旦遭到泄露、篡改、破坏或者非法获取、非法利用、非法共享，可能造成的影响程度。影响程度从高到低可分为特别严重危害、严重危害、一般危害。对不同影响对象进行影响程度判断时，采取的基准不同。如果影响对象是组织或个人权益，则以本单位或本人的总体利益作为判断影响程度的基准。如果影响对象是国家安全、经济运行、社会稳定或公共利益，则以国家、社会或行业领域的整体利益作为判断影响程度的基准。

根据上述内容，通过判断数据一旦被泄露、篡改、破坏或者非法获取、非法利用、非法共享，对国家安全、经济运行、社会秩序、公共利益、组织权益与个体合法权益的影响程度，本指南建议金融机构将数据等级分为核心、重要、一般（敏感）、一般（其他）四个安全级别，分级方法如表 2 所示。

[3]来自：国家金融监督管理总局《银行保险机构数据安全管理办法》

表 2 数据分级方法

影响对象/影响等级	特别严重危害	严重危害	一般危害
国家安全	核心数据	核心数据	重要数据
经济运行	核心数据	重要数据	一般数据（其他）
社会秩序	核心数据	重要数据	一般数据（其他）
公共利益	核心数据	重要数据	一般数据（其他）
组织权益、个人权益	一般数据（敏感）	一般数据（敏感）	一般数据（其他）
注：如果影响大规模的个人或组织权益，影响对象可能不只包括个人权益或组织权益，也可能对国 家安全、经济运行、社会秩序或公共利益造成影响。			

来源：数据安全推进计划

（3）数据分类分级运营

金融机构在开展数据分类分级运营工作时，应至少包含数据分类分级的常态化运营机制、检查优化以及对分类分级的结果应用三部分内容：

- 金融机构在建立常态化运营机制和开展检查优化工作方面重点关注其建立分类分级的 PDCA 循环体系的能力，包括常态化运营机制、人员问责机制、分类分级结果纠错机制、级别动态调整机制、定期检查机制等运营机制的建立和运行能力。
- 数据分类分级结果应用方面应重点关注分类分级结果是否能被业务系统进行调用，并应用于后续的数据管理、数据安全策略制定中。

数据安全推进计划

三、数据安全管理体系建设

（一）合规要点

《银行保险机构数据安全管理办法》“第四章 数据安全管理”要求企业强化数据安全管理，按照国家数据安全与发展政策要求，根据自身发展战略，制定数据安全保护策略，建立数据安全管理制度和数据处理管控机制。

（二）面临问题

1. 数据安全管理体系建设框架如何设计

企业在建立数据安全管理体系时，首先要明确数据安全管理边界，厘清管理体系工作内容及建设要求。从法律法规和监管要求来看，一方面，数据安全的保护主体是数据本身，保护能力要贯穿数据收集、存储、使用、加工、传输、提供、公开等数据全生命周期处理活动。另一方面，数据安全要在制度流程、组织建设、管控机制等方面明确管理要求，开展管理工作。

2. 数据与业务紧耦合增加管理策略制定难度

数据与业务的强关联关系导致数据安全管理策略需要更加精细化和动态化。不同业务场景下的数据使用需求和风险等级各异，传统的静态、一刀切的安全管理策略已难以适应。企业需要制定更加灵活、高弹性的数据安全管理措施，以确保在保障数据安全的同时，不阻碍业务的正常开展。

数据治理计划

（三）合规实践建议

1. 梳理数据全生命周期安全要求，明确管理框架及管理办法

数据安全管理体系是企业开展数据安全工作需要具备的能力框架。针对该项工作，国家、行业均有相关标准供金融机构参考。如图2所示，GB/T 37988-2019《数据安全能力成熟度模型》从宏观数据管理的角度出发，定义了数据安全管理体系建设的过程维度、能力维度、等级维度等内容。如图3所示，JR/T 0223-2021《金融数据安全 数据生命周期安全规范》定义了围绕数据全生命周期的安全框架及防护要求。如图4所示，YD/T 4558-2023《数据安全治理能力通用评估方法》从数据安全管理工作开展的视角，明确了数据安全管理体系基本框架及总体要求。

各企业可以根据现有标准及监管要求，结合已经开展的数据安全工作，梳理形成适用于自身的数据安全管理体系，并制定数据安全管理制度，通过将各项要求落实在制度文件中，形成对内的统一管理，确保数据安全管理工作“有章可依”。

数据安全产业推进计划

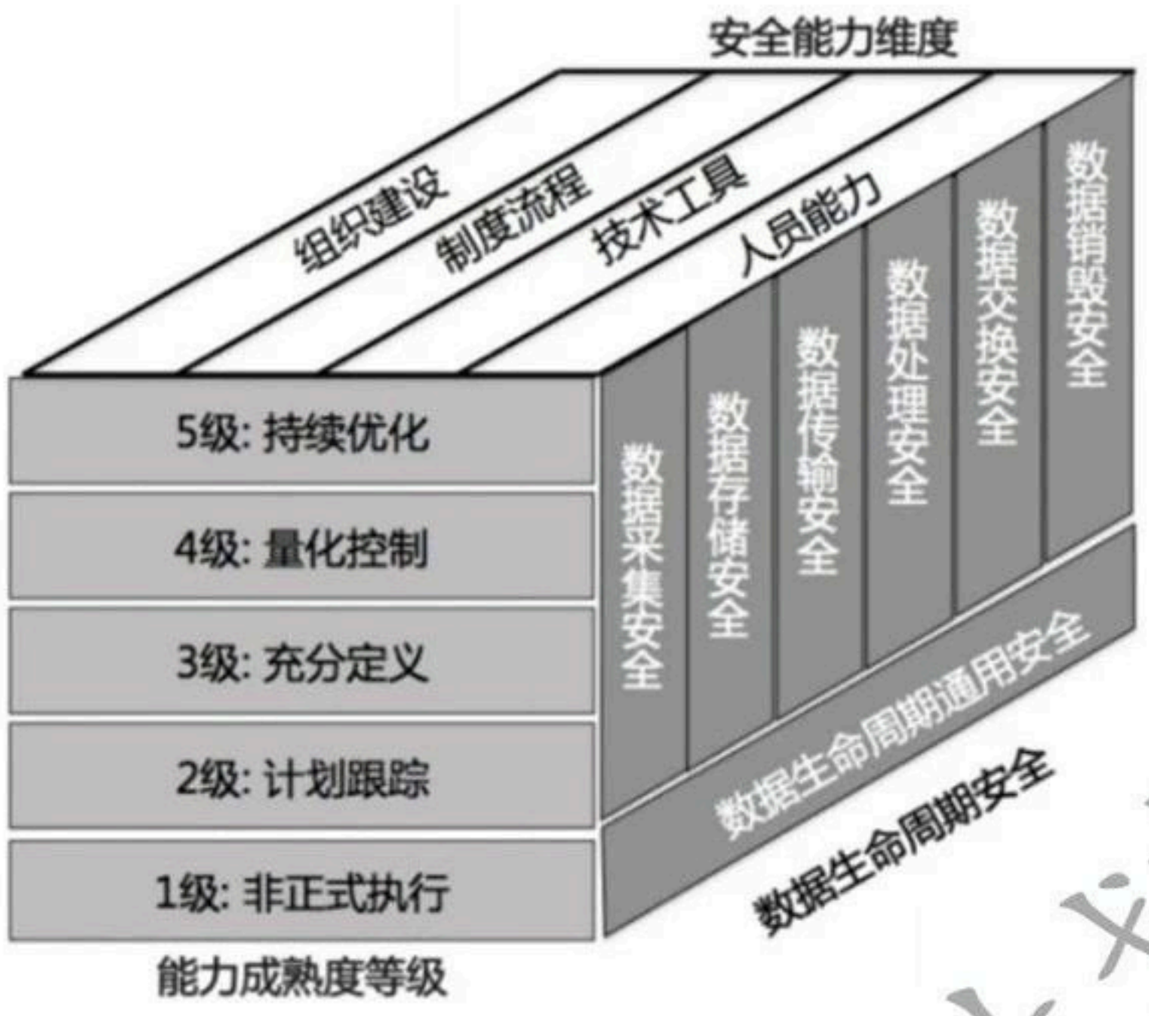


图 2 数据安全能力成熟度模型

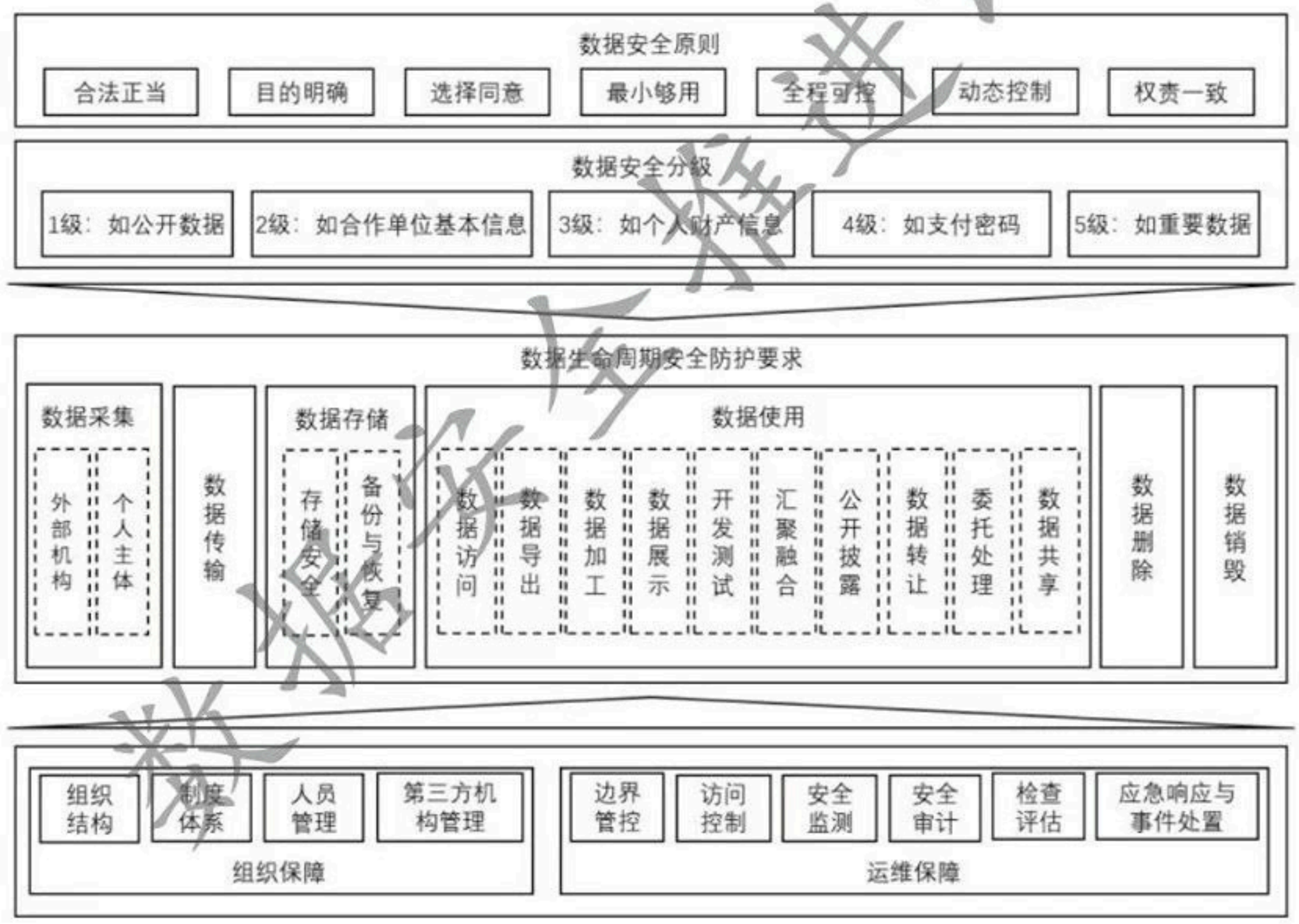
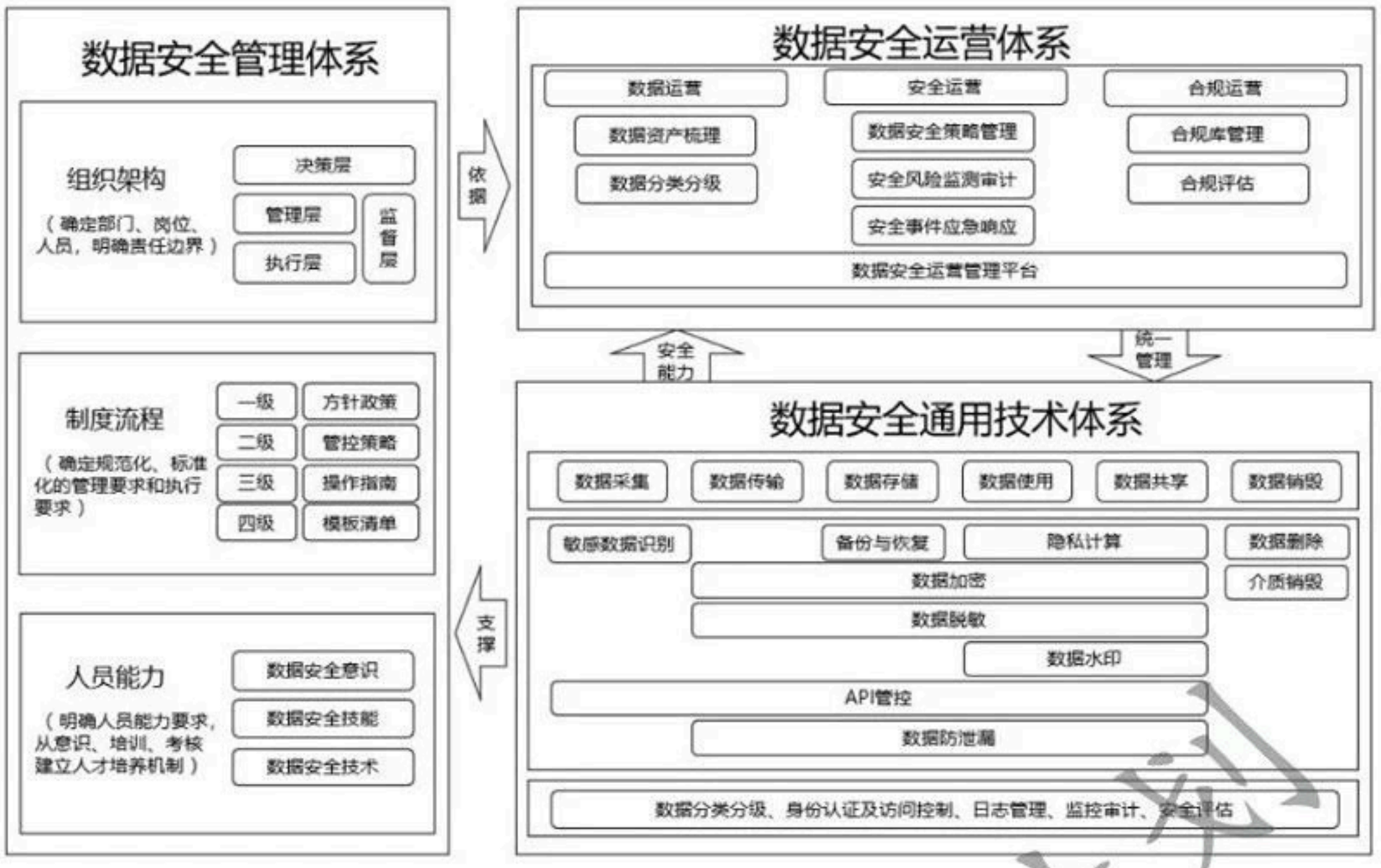


图 3 数据全生命周期安全框架

数据安全计划



来源：数据安全推进计划

图 4 数据安全体系建设示例

2. 分析业务场景安全风险，梳理个性化管控方案[4]

数据存在于业务中，离业务越近越能发现数据安全建设需求，深入业务场景和数据视图是制定有效管理策略的必经之路，具体工作内容如下。

（1）全面梳理业务场景

梳理数据资产和业务场景是企业进行场景化数据安全建设的前提，可以帮助组织了解数据安全管理对象全貌，为企业场景化数据安全管理提供行动地图。

（2）确定业务场景安全管理优先级

在业务场景梳理完成后，企业需要综合考虑监管要求、数据安全风险和业务发展需要，明确业务场景治理的开展优先级。例如，数据采集过程中个人信息主体数据采集、外部机构数据采集等场景均涉及

[4] 来自：数据安全推进计划《数据安全治理实践指南（4.0）》

到个人信息权益保护，是当前数据安全合规出现问题的高危场景，容易影响企业形象，因而可以优先治理。此外，数字经济的繁荣发展离不开数据的流通共享，随之而来的风险也在不断显现，对数据流通的安全保护势在必行，因而也应着重进行相关场景的安全建设。

（3）评估业务场景数据安全风险

评估业务场景的数据安全风险是指针对具体场景，综合考虑合规要求、数据资源重要程度、面临的数据安全威胁等因素，将数据流动过程的风险点梳理出来，并明确数据安全风险等级。业务方应根据此项评估结果，确定要进行整改的风险点，并将其作为数据安全治理建设需求的输入，为制定场景化数据安全解决方案提供依据。

（4）制定并实施业务场景解决方案

结合业务场景的数据安全风险评估结果，企业可以根据相关政策及标准要求，申请充分的资源保障，并制定可落地的解决方案。目前，对于部分场景，业界已经形成了一些公认的典型解决方案，例如在数据加密存储场景中使用加解密系统，并在算法的选择上避开不安全的 MD5、AES-ECB、SHA1 等算法；在终端场景下部署终端 DLP 等。但更多情况下，企业需要根据实际情况自研解决方案或者甄选适宜的供应侧解决方案。

（5）完善业务场景操作规范

为规范业务场景日常的数据安全管理和运营工作，企业应督促业务部门在实施具体的技术措施后，及时完善整体数据安全制度体系中关于三级与四级的制度文件，如《数据导出申请单》《数据脱敏规则》

《数据安全合规清单》等，以保持制度流程和技术落地一致性。

四、数据安全技术保护

（一）合规要点

《银行保险机构数据安全管理办法》“第五章数据安全技术保护”要求企业健全数据安全技术保护体系，建立数据安全技术架构，明确数据保护策略方法，采取技术手段保障数据安全。

（二）面临问题

1. 产品工具孤岛现象阻碍安全作用发挥

据《2022 年数据安全行业调研报告》显示，44%的企业已应用了五到八项相关的技术产品，19.3%的企业甚至应用了超过八项以上的技术产品。然而，由于企业在引入这些工具时，往往缺乏统一的规划和标准，导致后续的技术栈和产品集较为杂乱，各项产品的堆叠与管理不仅为企业带来困扰，不同产品之间的壁垒也为安全作用的发挥带来了阻碍。

2. 多种技术产品如何体系化呈现

数据安全技术作为数据安全各项要求及管理策略落地的重要支撑，主要围绕数据在全生命周期中的安全需求，通过对数据进行识别、标记、变形、计算等操作，实现对数据的持续保护。据调研，敏感数据识别、数据脱敏、数据加密等多项安全技术产品在企业内应用广泛。因此，如何编排已有的技术工具，使得其对数据安全的支撑更加有效，

数据安全度计划

或者如何针对技术应用现状进行差缺补漏，都需要一个体系化的技术呈现。

（三）合规实践建议

1. 建立数据安全技术体系，有效落实安全管理要求[5]

数据安全技术体系的技术架构并非单一产品或平台的构建，而是结合组织自身使用场景，围绕数据全生命周期各阶段的安全要求，建立起来的与制度流程相配套的技术和工具。一种典型的数据安全技术体系如图 5 所示，由基础通用类技术、生命周期类技术、平台类技术构成。

来源：数据安全推进计划

图 5 数据安全技术体系示例

基础通用类技术工具为数据全生命周期的安全提供支撑：

- 数据分类分级相关工具平台主要实现数据资产扫描梳理、数据分类分级打标和数据分类分级管理等功能。
- 身份认证及访问控制相关工具平台，主要实现在数据全生命周

[5] 来自：数据安全推进计划《数据安全治理实践指南（4.0）》

期各环节中涉及的所有业务系统和管理平台的身份认证和权限管理。

- 监控审计相关工具平台接入业务系统和管理平台，实现对数据安全风险的实时监控，并能进行统一审计。

- 日志管理平台收集并分析所有业务系统和管理平台的日志，并统一日志规范以支持后续的风险分析和审计等工作。

- 安全及合规评估相关工具平台主要用于综合评估数据安全现状和合规风险。

数据全生命周期安全类技术为生命周期中特定环节面临的风险提供管控技术保障。整个数据全生命周期可以通过组合或复用以下多种技术实现数据安全:

- 敏感数据识别通过对采集的数据进行识别和梳理，发现其中的敏感数据，以便进行安全管理。

- 备份与恢复技术是防止数据破坏、丢失的的有效手段，用于保证数据可用性和完整性。

- 数据加密相关工具平台通过提供常见的加密模块及密钥管理能力，落地数据的加密需求。

- 数据脱敏是通过一定的规则对特定数据对象进行变形的一类技术，用于防止数据泄露和违规使用等。

- 数据安全网关通过建立统一的数据访问、分发的出入口，基于协议访问数据源，发现敏感数据，对访问数据的行为进行分析、处理，提供持续的数据安全保障及监测能力。

- 数据水印技术通过对数据进行处理使其承载特定信息，使得数

据具备追溯数据所有者与分发对象等信息的能力。在数据处理过程中起到威慑及追责的作用。

• 数据防泄露技术通过终端防泄露技术、邮件防泄露技术、网络防泄露技术，防止敏感数据在违反安全策略规定的情况下流出组织。

• 隐私计算通过实现数据的可用不可见，从而满足隐私安全保护、价值转化及释放。

• API 管控相关工具平台提供内部接口和外部接口的安全管控和监控审计能力，保障数据传输接口安全。

• 数据删除是一种逻辑删除技术，为保证删除数据的不可恢复，一般会采取数据多次的覆写、清除等操作。

• 介质销毁一般通过消磁机或者物理捣毁等方式对数据所在的介质进行物理销毁。

平台类技术是打破“孤岛”的关键。通过接入各技术工具的能力点，打破其之间的协作壁垒，实现对不同技术工具的能力编排与调度，进而提供统一的管理入口与操作方式，为组织的各项安全决策提供全局视角。

2. 构建数据安全运营管理平台，集中化调度安全能力

数据安全运营管理平台能够为用户提供统一的运营管理入口、全局一致的操作方式，实现对各安全工具的能力编排、调度，通过聚焦“人-业务-应用-数据”链路，打破单点能力边界，主要关注对外态势感知与对内业务免打扰，实现组织内部一体化的数据安全运营。这意味着数据安全运营管理平台实际接入的是组织的数据安全能力，而

非简单的工具集成。因此，数据安全运营管理平台需要基于“持续运营”的设计理念，通过数据资产梳理、数据合规管理、安全能力管理等核心功能，建立“协同管理”的能力，规避产品在实际应用过程中的粗防护、弱联动、单视角等问题。

五、个人信息保护

（一）合规要点

《银行保险机构数据安全管理办法》第五章“个人信息保护”章节要求企业加强个人信息保护，按照“明确告知、授权同意”原则处理个人信息，收集个人信息应限于实现金融业务处理目的的最小范围，不得过度收集。

（二）面临问题

1. 个人信息保护的监管压力大

针对个人信息泄露产生的垃圾短信、电信诈骗、骚扰电话等负面社会现象，国家层面，2021 年发布的《中华人民共和国个人信息保护法》，为个人信息权益保护提供法律依据。行业层面，金融监督管理总局、人民银行等部门通过一系列专项行动，严格治理企业个人信息泄露、滥用等问题。

2. 用户对其主体权益保护的要求高

随着法律普及和个人维权意识提升，用户对金融产品违规收集使用个人信息、过度索取、频繁骚扰等侵害用户主体权益的行为感受强

烈。个人信息作为多数企业的主要数据类型，是安全保护的重点领域，一旦发生用户个人信息泄露事件，企业将面临巨大的社会舆论压力和监管处罚。

（三）合规实践建议

1. 全面排查，重点聚焦，提升 APP 个人信息保障能力建设

结合监管要求，建议从以下几方面开展移动应用软件个人信息安全保护机制建立。

权限管理：权限申请方面首先应循序合理正当必要原则，只申请与业务功能相关的权限，不应过度申请无关权限，同时应满足事前告知原则，即在用户作出明确的确认行为之后再向操作系统进行权限申请，不得默认授权；其次，软件实际申请权限不应超出告知同意的范畴，且不得以捆绑方式强制要求用户一次性同意开启多个可收集个人信息的权限；APP 不得存在“不给权限不让用”的情况。

告知同意：当移动应用软件出于提供产品或服务的目的收集使用个人信息时，应当在使用其实质功能前，告知收集个人信息的目的、方式和范围，以及拒绝提供将带来的影响，并获取用户的主动授权同意（如主动勾选）。告知的时机应满足事前告知原则，在用户做出明确的确认行为之后应用软件再进行处理个人信息的相关操作。告知方式宜满足多样性原则，采取多种形式，这样更易于用户感知与理解。

定向推送：APP 使用个人信息时，除目的所必须外，应消除明确身份指向性，避免精确定位到特定个人。目前常见的定向推送有电话、

短信、通知、业务内容、广告定推等。在向用户提供业务功能中使用定向推送的，应显著区分定向推送展示内容，如在板块或页面显著位置，进行标识，并提供退出或关闭此类定向推送内容及广告的功能。存在通过通知、短信、电话等方式向用户提供定向推送功能的，影响用户提供通知关闭、短信退订、电话退订的相关功能。

用户主体权利实现：一是 APP 应建立个人信息查询、更正、删除、撤回授权同意和获取用户个人信息副本等个人信息保护机制，提供访问途径，保证用户个人权利。而是应建立询问、投诉的渠道与机制，并告知用户申诉处理的方式、流程以及响应时间，以及外部纠纷解决机构及联系方式。

2. 生物识别类信息应谨慎收集

生物识别类数据通常指代通过生物识别技术对自然人的物理、生理或行为特征进行特殊技术处理而得到的信息，并对获得的数据信息进行处理的活动[6]。通常用于与金融客户相关的身份鉴别与认证等场景，如门禁、金融支付、语音识别、活体验证等。

依据 JR/T 0171-2020《个人金融信息保护技术规范》等监管要求，生物识别属于 C3 类个人信息，安全保护要求更加严格。因此，企业应当在业务规则设计阶段评估采用生物识别技术的必要性，并依据国家标准 GB/T 35273-2020《信息安全技术 个人信息安全规范》、GB/T 39335-2020《信息安全技术 个人信息安全影响评估指南》等开展个人信息安全影响评估。同时，应严格遵循“告知-同意”规则，

[6] GDPR《通用数据保护条例》

与其他个人信息分开告知，并单独征得用户自愿、主动地授权同意。在这个过程中，原则上来讲，企业不应直接存储原始生物识别信息，选择“即采即用”的方式，或仅将数据存储在用户终端，使用后及时进行删除。

六、数据安全风险监测与处置

（一）合规要点

《银行保险机构数据安全管理办法》“第六章数据安全风险监测与处置”要求企业完善数据安全风险监测与处置机制，将数据安全风险纳入全面风险管理体系，明确风险监测评估、应急响应报告、事件处置的管理流程。

（二）面临问题

1. 监管侧及业务方对金融机构的风险防范能力提出了新要求

政策方面，《中华人民共和国数据安全法》明确规定重要数据处理者应当按照规定对其数据处理活动定期开展风险评估，并向有关主管部门报送风险评估报告。《网络数据安全管理条例》要求定期开展本领域风险评估。《银行保险机构数据安全管理办法》进一步明确了银行保险领域的风险评估要求。业务方面，随着业务数字化、数字业务化的转型不断深入，业务方对基于数据的业务分析需求增加，对数据安全风险的防范需求也同步增长。

数据安全推进计划

2. 新技术应用衍生新的安全风险

5G、人工智能、云计算、移动互联网、大数据分析等新兴技术应用极大地推动了各行业领域的组织发展与创新，为广大用户提供了更为智能、便利的服务，但同时也带来了大量的安全漏洞、风险。以人工智能为例，为了提高智能化输出的准确率，提升用户体验，往往在模型训练过程需要用到个性化的敏感、隐私数据，但训练数据集的生成、训练环境的部署、模型的分发等过程都会存在数据泄露、篡改等风险。

（三）合规实践建议

1. 定期开展数据安全风险评估，加快风险处置[7]

数据安全风险评估工作得到了国家、行业主管部门以及产业多方的高度重视与关注，业内相继发布了多项风险评估标准、实施指引，现已形成一套完整、清晰的实施流程，具体如下[8]。

（1）评估准备

企业内部在评估准备阶段首先需要明确数据安全风险评估的目标，与相关方建立基本共识。基于自身需求和已制定的评估目标，组织能够进一步确定数据安全风险评估的对象、范围和边界。通常来说，评估范围可以覆盖组织全部的数据和数据处理活动，也可以仅针对某个单独的业务、信息系统涉及的数据和数据处理活动。企业可以采取“全面摸排、重点评估”的原则，结合数据分类分级工作成果，识别

[7] 来自：数据安全推进计划《数据安全风险评估实务：问题剖析与解决思路》

[8] 来自《数据安全治理实践指南（4.0）》

出重点评估对象，例如个人敏感信息、重要数据、核心数据及其相关的数据处理活动。

针对已选定的评估对象和范围，企业需要选取并参照自身适用的评估依据，规划数据安全风险评估工作，确定风险评估依据。

（2）评估实施

企业在实施数据安全风险评估的过程中，主要围绕数据处理者、业务、信息系统、数据处理活动、安全措施的基本情况进行信息调研，重点识别组织在数据安全管理、数据安全技术、个人信息保护、数据处理活动安全等方面是否存在潜在的风险问题。例如 2023 年金融领域《关于印发银行保险机构信息科技外包风险监管办法的通知》，提示了银行保险机构需要有效控制由于外包而引发的风险，加强重点外包安全管理，对敏感信息采取严格管控措施、风险持续监测。针对这一问题，企业可以从合作方管理机制、合作协议约束、外包人员访问权限、第三方接入与数据回收等常见风险点入手进行评估分析。

（3）评估总结

在完成数据安全风险问题的识别、评估分析后，企业需要总结在评估实施过程中获取的信息以及发现的风险问题，提出风险处置建议，形成数据安全风险评估报告。至此，数据安全风险评估工作已基本完成，但企业的相关方还需要制定整改计划，限期完成整改，无法及时完成整改的，应采取临时安全措施，防止数据安全事件发生。风险整改结束后，企业可以开展数据安全风险复评工作，重点分析风险处置后的残余风险或者衍生风险。

2. 开展大模型数据安全风险评估

金融作为数据密集型行业，大模型对于提高企业金融业务的智能化服务水平、风控能力和决策效率具有重要意义，在关键决策辅助、文本生成、提升客户陪伴质量等应用场景中潜力巨大。

与此同时，大模型训练和运营过程中面临的数据安全风险多种多样，需要定期及在上线和更新等重要节点开展全面的风险评估和短板提升，金融机构可参照图 6 中大模型数据安全通用评估框架开展大模型数据安全风险评估工作。

来源：数据安全推进计划

图 6 大模型数据安全

海量数据集是大模型开发和应用的基础，数据集准备过程应重点评估用于大模型训练的数据安全性，包括数据来源的合法合规性、训练数据是否经过有效脱敏、数据标注和清洗流程是否安全完备等。

模型开发及应用阶段应重点评估数据处理过程中的安全性，覆盖模型文件数据、训练和微调数据集、测试数据等，包括数据传输、存储加密、数据使用的权限与技术控制以及数据的及时删除销毁等。。

数据安全推进计划

通用安全部分应重点评估大模型在企业整体安全保障体系中的通用安全能力，包括针对新技术引入等场景的制度规范建立、鉴别与访问控制要求与落实、安全测试能力、定期开展安全评估、合作方安全管理以及是否具备专项应急预案等。

数据安全产业推进计划