数据安全推进计划
DATA SECURITY INITIATIVE

数据安全治理实践指南（2.0）

数据安全推进计划
2022年12月

版权声明

特别鸣谢机构

中国信息通信研究院、中国移动通信集团有限公司、中国联合网络通信集团有限公司、中国电信集团有限公司、中移信息技术有限公司、中国联合网络通信有限公司广东省分公司、联通数字科技有限公司、联通（广东）产业互联网有限公司、天翼电子商务有限公司、北京百度网讯科技有限公司、深圳市腾讯计算机系统有限公司、中国工商银行股份有限公司、中国建设银行股份有限公司、中国光大银行股份有限公司、华泰证券股份有限公司、国信证券股份有限公司、吉利控股集团有限公司、上海汽车集团股份有限公司、国网四川信通公司、OPPO 广东移动通信有限公司、天道金科股份有限公司、上海淇毓信息科技有限公司、中国电子科技网络信息安全有限公司、天达共和律师事务所、北京中银（深圳）律师事务所、奇安信科技集团股份有限公司、北京天空卫士网络安全技术有限公司、北京天融信网络安全技术有限公司、杭州安恒信息科技有限公司、杭州美创科技股份有限公司、绿盟科技集团股份有限公司、北京数安行科技有限公司、IBM、北京奇虎科技有限公司、浪潮云信息技术股份公司、北京旷视科技有限公司、上海新炬网络信息技术股份有限公司、浙江零跑科技股份有限公司、江苏保旺达软件技术有限公司、上海爱数信息技术股份有限公司、郑州信大捷安信息技术股份有限公司、数安信（北京）科技有限公司、北京亿赛通科技发展有限公司、江西省信息中心、安徽辰图大数据科技有限公司

特别鸣谢专家

刘雪花、李雪妮、魏凯、姜春宇、闫树、龚诗然、李天阳、郝志婧、张越、张亚兰、温暖、赵晨斌、于文良、曹继文、鄂梅、宁相军、何晓倩、刘建国、谷陟军、吴剑锋、陈泽楠、许琛超、杜悦艺、吴芳琼、李克鹏、袁文生、吴凡、顾晓强、张坤、邵媛、刘巍、江旺、张炎、王君、周思佳、左银康、肖雪、孙雄涛、王一斌、刘坤灵、苏振波、王同新、张赣、崔新炜、柳伟杰、薛锋、申晓雨、叶鹏、潘良、王新华、杨勇涛、李洪亮、梁伟、杨明非、张文礼、谢雄、林鹭、王彦翔、金岳阳、刘玉红、孔祥慧、王雨薇、唐会芳、李传忠、李连伟、赵华涛、程永新、梁铭图、黄国标、陈昺润、刘险峰、卢伟、张震、刘为华、胡国华、李楷、张艺伟、何黎明、周剑涛、关中华

前 言

数据作为新型生产要素，已成为国家重要资产和我国数字经济发展的基础战略资源。2021 年以来，国家、行业、地方相继颁布了大量数据安全政策文件。作为数字经济健康发展的重要基石，数据安全的重要性愈发突出，数据安全治理需求愈加明显。

为了梳理数据安全治理的概念内涵，探讨企业数据安全建设路线，中国信息通信研究院云计算与大数据研究所于 2021 年 7 月发布《数据安全治理实践指南（1.0）》（以下简称《指南（1.0）》），围绕数据安全治理目标、治理框架、治理实践路径展开论述。经过一年多的发展，企业数据安全治理取得了有效进展，同时也面临新的挑战。比如，当前大部分企业的数据安全管理制度聚焦在原则、管理规定等较粗颗粒度的层面，对数据业务的下沉指导不充分，导致具体业务场景下的技术落地仍然缺乏实践指引，容易与管理要求脱节等。

本指南依据大量行业调研和企业实践，在《指南（1.0）》的基础上优化了数据安全治理总体视图，并针对数据分类分级难落地、管理与技术易脱钩等焦点问题的建设方案进行了初步探索，进一步细化了数据安全治理实践路线。

目 录

一、数据安全治理概述

发展数字经济、加快培育发展数据要素市场，必须把保障数据安全放在突出位置。这就要求我们着力解决数据安全领域的突出问题，有效提升数据安全治理能力。随着数据安全监管要求逐渐落地，组织数据安全治理动力明显攀升，数据安全技术及服务供给不断释放。整体来看，数据安全治理进入快速发展阶段。本章将解析数据安全治理概念内涵，分析数据安全治理要点。

（一）数据安全治理概念内涵

为指导行业数据安全治理能力建设，促进行业数据安全治理能力发展，依据中国通信标准化协会大数据技术标准推进委员会 BDC 91-2022《数据安全治理能力评估方法》，梳理数据安全治理概念内涵，本指南认为应该从广义和狭义两个角度进行理解。

狭义地说，数据安全治理是指在组织数据安全战略的指导下，为确保组织数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力，内外部相关方协作实施的一系列活动集合。包括建立数据安全治理组织架构，制定数据安全制度规范，构建数据安全技术体系，建设数据安全人才梯队等。

广义地说，数据安全治理是在国家数据安全战略的指导下，为形成全社会共同维护数据安全、促进开发利用和产业发展的良好环境，国家有关部门、行业组织、科研机构、企业、个人共同参与和实施的一系列活动集合。包括完善相关政策法规，推动政策法规落地，建设实施标准体系，研发应用关键技术，培养专业人才等。

（二）数据安全治理要点

（1）以数据为中心

数据的高效开发和利用，涵盖了数据的采集、传输、存储、使用、共享、销毁等全生命周期的各个环节，不同环节的特性不同，都面临丰富多样的数据安全威胁与风险。因此，必须构建以数据为中心的数据安全治理体系，根据具体的业务场景和各生

命周期环节，有针对性地识别并解决其中存在的数据安全问题，防范数据安全风险。

（2）多元化主体共同参与

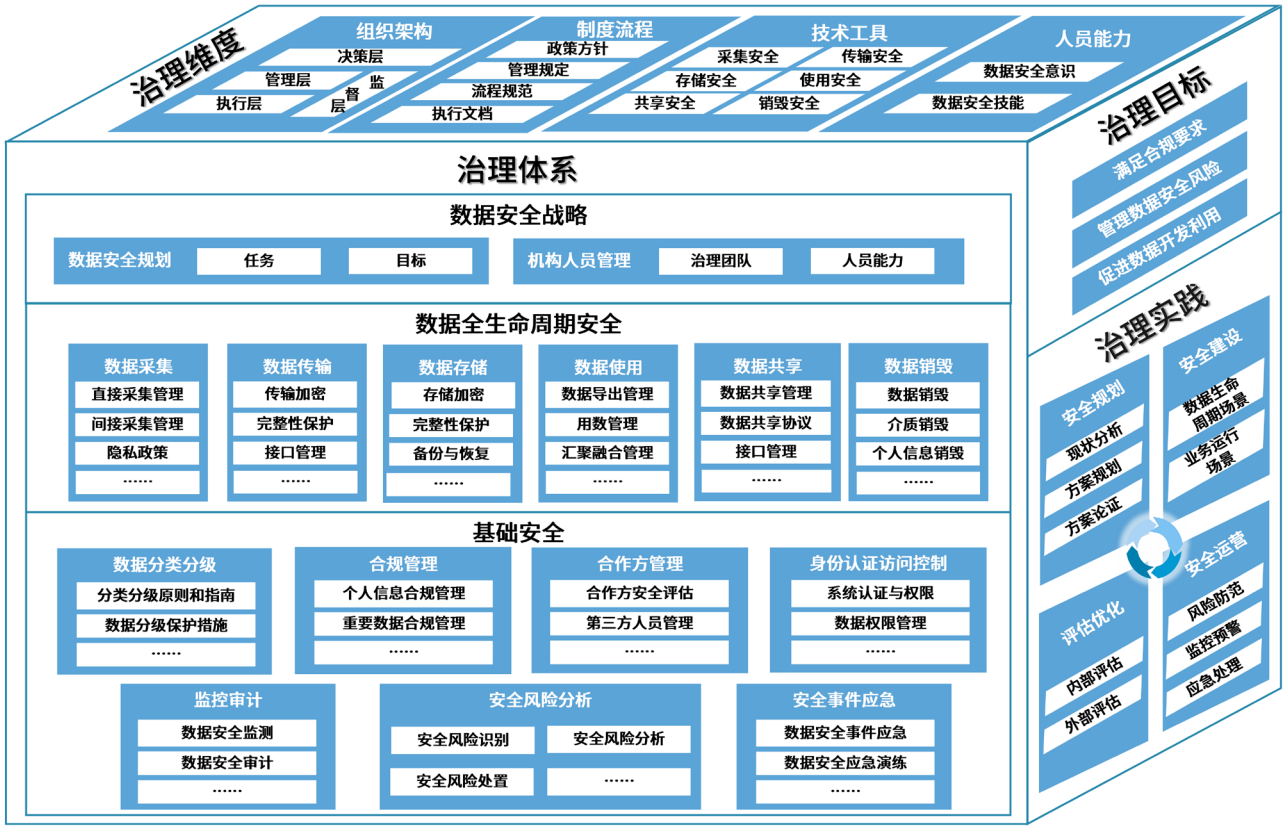
无论是从广义还是狭义的角度出发，数据安全治理不是仅仅依靠一方力量可以开展的工作。对国家和社会而言，面对数据安全领域的诸多挑战，政府、企业、行业组织、甚至个人都需要发挥各自优势，紧密配合，承担数据安全治理主体责任，共同营造适应数字经济时代要求的协同治理模式。这也与《中华人民共和国数据安全法》（以下简称《数据安全法》）中强调建立各方共同参与的工作机制相一致。对组织机构而言，数据安全治理需要从组织战略层面出发，协调管理层、执行层等相关方，打通不同部门之间的沟通障碍，统一内部数据安全共识，实现数据安全防护建设一盘棋。因此，数据安全治理必然是涉及多元化主体共同参与的工作。

（3）兼顾发展与安全

随着国内数字化建设的快速推进，无论是政府部门，还是其他组织均沉淀了大量的数据。数字经济时代的应用场景下，数据只有在流动中才能充分发挥其价值，而数据流动又必须以保障数据安全为前提，因此，必须要辩证看待数据安全治理。正如《数据安全法》提出的“坚持以数据开发利用和产业发展促进数据安全，以数据安全保障数据开发利用和产业发展。”数据安全治理不是强调数据的绝对安全，而是需要兼顾发展与安全的平衡。

二、数据安全治理总体视图

本指南结合前期大量调研和数据安全治理能力评估实践，依据中国通信标准化协会大数据技术标准推进委员会 BDC 91-2022《数据安全治理能力评估方法》，提炼出一套行之有效的数据安全治理总体视图，用以描绘数据安全治理的建设蓝图和实践路线，如图 1 所示。



来源：数据安全推进计划

图 1 数据安全治理总体视图

（一）数据安全治理目标

数据安全治理目标是组织数据安全治理工作开展的前进方向。本指南认为其主要包括满足合规要求、管理数据安全风险、促进数据开发利用三方面。

满足合规要求。逐渐细化的数据安全监管要求，为组织数据安全合规工作的推进提出了更高的要求。及时发现合规差距，协助组织履行数据安全责任义务，为业务的稳定运行和规范化开展筑牢根基是数据安全治理工作的首要目标。

管理数据安全风险。不断产出的海量数据在动态实时流转过程中，面临着较大的风险暴露面，数据安全威胁及带来的影响与日俱增。叠加数据安全边界较为模糊、数据安全基础不够强韧等问题，组织数据安全风险的有效管理必然是数据安全治理的重要使命。

促进数据开发利用。数字经济的高速发展离不开数据价值的充分释放，数据安全则是保障数据价值释放的重要基石。数据安全治理通过体系化的建设，完善组织的合规管理和风险管理工作机制，提升数据安全保护水平，促进数据的开发利用。

（二）数据安全治理体系

数据安全治理体系是组织达成数据安全治理目标需要具备的能力框架，组织应围绕该体系进行建设。本指南提出的数据安全治理体系是一个三层架构，分别包括数据安全战略层、数据全生命周期安全层和基础安全层。

数据安全战略层是推进数据安全治理工作开展的战略保障模块，要求组织在启动各项工作前，应制定相应的战略规划。数据安全战略从数据安全规划、机构人员管理两方面入手，前者确立目标任务，后者组建治理团队。

- 数据安全规划要求根据国家政策、组织业务发展需要以及数据安全需求等多方面因素明确组织整体数据安全规划。
- 机构人员管理要求建立负责组织内部数据安全工作的部门、岗位和人员，并与人力资源管理部门进行联动，防范机构人员管理过程中存在的数据安全风险。

数据全生命周期安全层是评估组织数据安全合规及风险管理等工作下沉至各业务场景能力水平的重要模块。要求组织以采集、传输、存储、使用、共享、销毁等环节为切入点，设置管控点和管理流程，保障数据安全。具体来说包括：

• 数据采集安全是指根据组织对数据采集的安全要求，建立数据采集安全管理措施和安全防护措施，规范数据采集相关流程，从而保证数据采集的合法、合规、正当和诚信。

• 数据传输安全是指根据组织对内和对外的数据传输需求，建立不同的数据加密保护策略和安全防护措施，防止传输过程中的数据泄露等风险。

• 数据存储安全是指根据组织内部数据存储安全要求，提供有效的技术和管理手段，防止对存储介质的不当使用而可能引发的数据泄露风险，并规范数据存储的冗余管理流程，保障数据可用性，实现数据存储安全。

• 数据使用安全是指根据数据使用过程面临的安全风险，建立有效的数据使用安全管控措施和数据处理环境的安全保护机制，防止数据处理过程的风险。

• 数据共享安全是指根据组织对外提供或交换数据的需求，建立有效的数据交换安全防护措施，降低数据共享场景下的安全风险。

• 数据销毁安全是指通过制定数据销毁机制，实现有效的数据销毁管控，防止因对存储介质中的数据进行恢复而导致的数据泄露风险。

基础安全层作为数据全生命周期安全能力建设的基本支撑模块，可以在多个生命周期环节内复用，是整个数据安全治理体系建设的通用要求，能够实现建设资源的有效整合。具体来说包括：

• 数据分类分级是指根据法律法规以及业务需求，明确组织内部的数据分类分级原则及方法，并对数据进行分类分级标识，以实现差异化的数据安全管理。

• 合规管理是指根据组织内部的业务需求和业务开展场景，明确相关法律法规要求，通过制定管理措施降低组织面临的合规风险。

• 合作方管理是指通过建立组织的合作方管理机制，防范组织对外合作中的数据安全风险。

• 监控审计是指通过建立监控及审计的工作机制，有效防范不正当的数据访问和操作行为，降低数据全生命周期未授权访问、数据滥用、数据泄露等安全风险。

• 身份认证与访问控制是指根据组织的安全合规要求，建立用户身份认证和访问控制管理机制，防止对数据的未授权访问。

• 安全风险分析是指根据组织的业务场景建立数据安全风险分析体系，将风险控制在可接受的水平，最大限度的保障数据安全。

• 安全事件应急是指通过建立数据安全应急响应体系，确保在发生数据安全事件后能够及时止损，保障业务的安全和稳定运行，最大程度降低数据安全事件带来的影响。

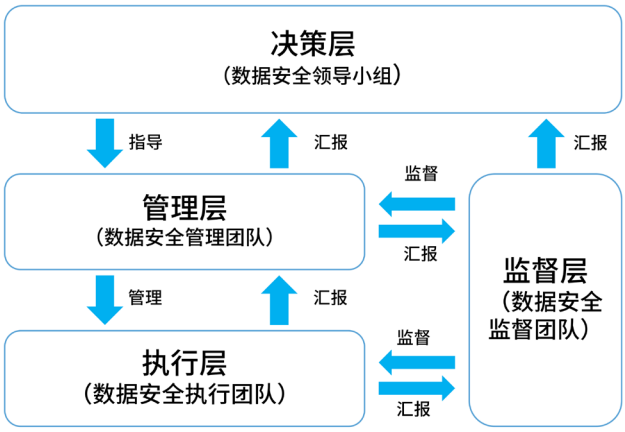
（三）数据安全治理维度

以数据安全治理目标为指引，围绕数据安全治理体系框架，可以从组织架构、制度体系、技术工具和人员能力四个维度开展治理能力建设工作，以解决“谁来干”、“怎么干”、“干的如何”、“有没有能力干”等关键问题。

1. 组织架构

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。

在一个组织内部，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 2 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。



来源：数据安全推进计划

图 2 数据安全治理组织架构示例

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，该小组一般由组织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。管理层一般由安全部门或数据部门牵头，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

数据安全责任	决策层	管理层	执行层	监督层
	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

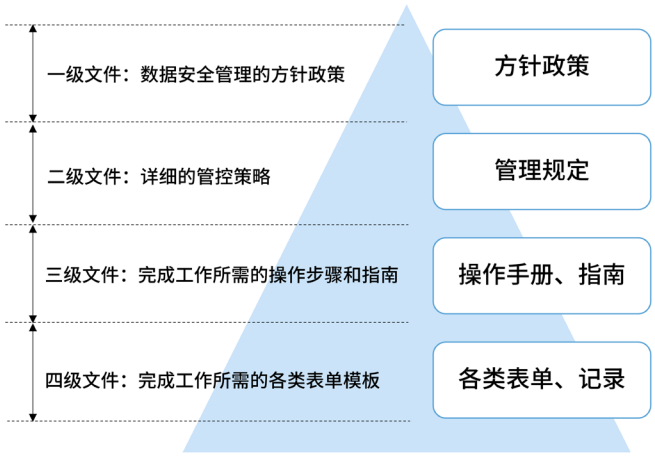
来源：数据安全推进计划

因不同组织的部门设置都有较大不同，涉及到实际组织体系建设时，不同单位还需结合现有组织架构，进行适度的调整和补充。

2. 制度流程

数据安全制度流程一般会从业务数据安全需求、数据安全风险控制需要，以及法律法规合规性要求等几个方面进行梳理，最终确定数据安全防护的目标、管理策略及具体的标准、规范、程序等。

数据安全管理制度文件可分为四个层面，一、二级文件作为上层的管理要求，应具备科学性、合理性、完备性及普适性。三、四级文件则是对上层管理要求的细化解读，用于指导具体业务场景的具体工作。常见的制度体系如图 3 所示。

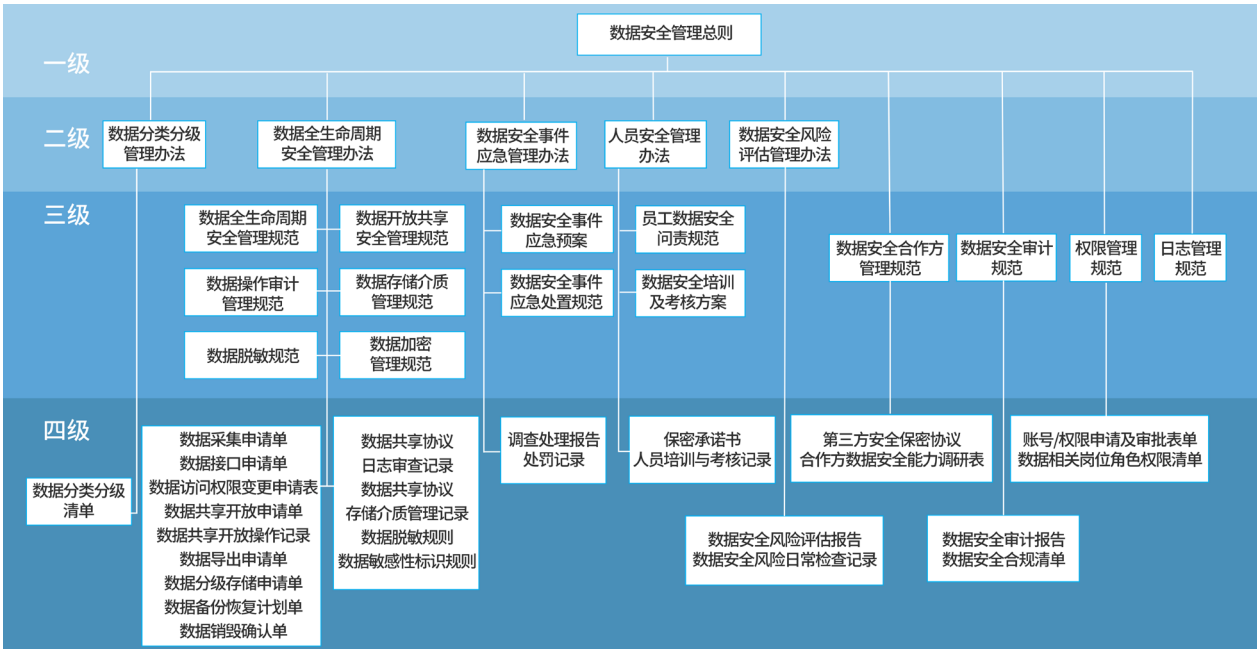


来源：数据安全推进计划

图 3 数据安全治理制度体系示例

一级文件是由决策层明确的面向组织的数据安全管理方针、政策、目标及基本原则。**二级文件**是由管理层根据一级文件制定的通用管理办法、制度及标准。**三级文件**一般由管理层、执行层根据二级管理办法确定各业务、各环节的具体操作指南、规范。**四级文件**属于辅助文件，是各项具体制度执行时产生的过程性文档，一般包括工作计划、申请表单、审核记录、日志文件、清单列表等内容。

根据图 3 所示的常见制度体系，围绕数据全生命周期安全要求，可以参考图 4 完善组织各级制度文件内容。

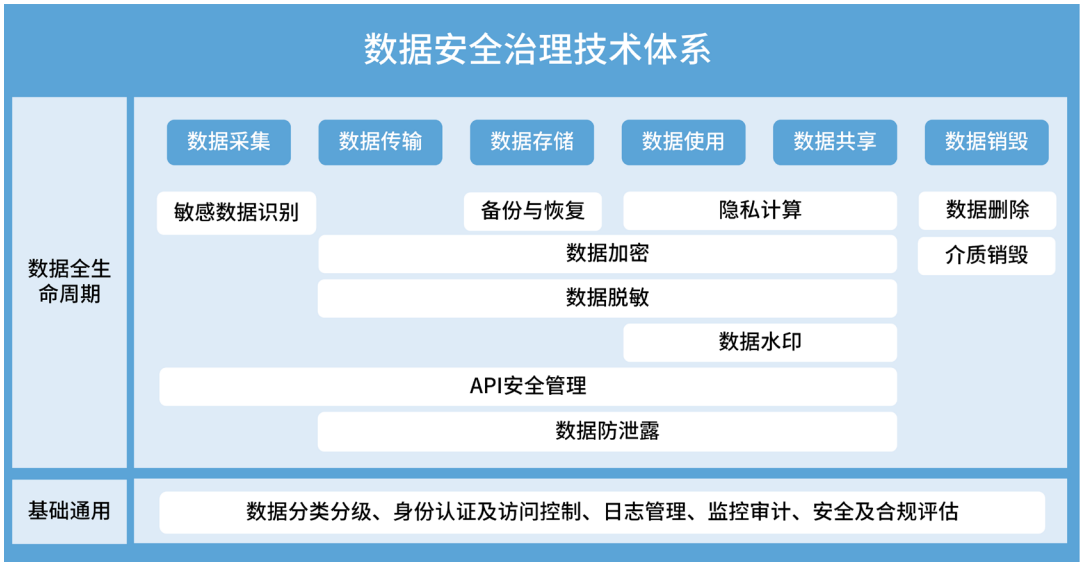


来源：数据安全推进计划

图 4 一套可参考的数据安全管理制度体系

3. 技术体系

数据安全技术体系并非单一产品或平台的构建，而是覆盖数据全生命周期，结合组织自身使用场景的体系建设。依照组织数据安全建设的方针总则，围绕数据全生命周期各阶段的安全要求，建立与制度流程相配套的技术和工具。一种数据安全治理技术体系如图 5 所示。



来源：数据安全推进计划

图 5 数据安全治理技术体系

其中基础通用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。
- 数据泄密防护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企业。
- API 安全管理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。
- 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。

4. 人员能力

数据安全治理离不开相应人员的具体执行，人员的技术能力、管理能力等都影响到数据安全策略的执行和效果。因此，加强对数据安全人才的培养是数据安全治理的应有之义。组织需要根据岗位职责、人员角色，明确相应的能力要求，并从意识和能力两方面着手建立适配的数据安全能力培养机制，如表 2 所示。

意识能力培养方式。可以结合业务开展的实际场景，以及数据安全事件实际案例，

表 2 不同类型人员的数据安全能力要求和培养机制

人员类型	数据安全能力要求	培养机制
全员	数据安全意识、员工安全操作规范	宣贯
领导层	数据安全意识、法律法规政策	宣贯
专业技术人员	数据安全技术、业务能力、合规能力	宣贯、能力认证结合

来源：数据安全推进计划

通过数据安全事件宣导、数据安全事件场景还原、数据安全宣传海报、数据安全月活动等方式，定期为员工开展数据安全意识培训，纠正工作中的不良习惯，降低因意识不足带来的数据安全风险。

技术能力培养方式。一方面，构建组织内部的数据安全学习专区，营造培训环境，通过线上视频、线下授课相结合的方式，按计划、有主题的定期开展数据安全技能培训，夯实理论知识。另一方面，通过开展数据安全攻防对抗等实战演练，将以教学为主的静态培训转为以实践为主的动态培训，提高人员参与积极性，有助于理论向实践转化，切实提高人员数据安全技能。

为保障培训效果，形成人员能力培养的管理闭环，还需要结合能力考核的管理机制。通过结合人员角色及岗位职责，构建数据安全能力考核试题库，通过考核平台分发日常测验及各项考核内容，评估人员数据安全理论基础。同时将人员在实战演练中的实际操作能力作为重要考核指标，以综合评估数据安全人员能力水平。

（四）数据安全治理实践

数据安全治理体系给出了组织数据安全治理的建设框架，如何将整套框架切实应用于建设过程，离不开实践路线的绘制。本指南基于行业发展现状，提炼出**“全局体系规划，场景有序落地，运营持续加强，评估助力优化”**的数据安全治理实践理念，并进一步丰富形成**“规划—建设—运营—优化”**的闭环路线，用以指导各行业组织数据安全治理工作的落地推进。该实践路线将在下一章展开论述。

三、数据安全治理实践路线

基于以上数据安全治理实践理念，可以按照自顶向下和自底向上相结合的思路推进实践过程。一方面，组织自顶向下，以数据安全战略规划为指导，以规划、建设、运营、优化为主线，围绕构建数据安全治理体系这一核心，从组织架构、制度流程、技术工具和人员能力四个维度构建全局建设思路。另一方面，组织自底向上，针对各业务场景敏捷落地相关数据安全能力点，以快速满足业务场景的数据安全需求，降低数据安全治理的长期性对业务开展的影响。通过各个场景的建设与完善，最终全面覆盖组织的所有数据处理活动。以上的实践过程可以有效避免管理和技术的“两张皮”问题。

（一）数据安全规划

数据安全规划阶段主要确定组织数据安全治理工作的总体定位和愿景，根据组织整体发展战略内容，结合实际情况进行现状分析，制定数据安全规划，并对规划进行充分论证。

1. 现状分析

组织应通过现状分析找到数据安全治理的核心诉求及差距项，以此作为规划设计的依据。可以从安全合规对标、风险现状分析、行业最佳实践对比入手。

一是数据安全合规对标。数据安全合规是组织履行数据安全相关责任义务的底线要求。不同组织应对组织适用的外部法律法规、监管要求、标准规范等进行梳理，将重要条款与现有情况进行对比，分析其差距，确定合规需求。

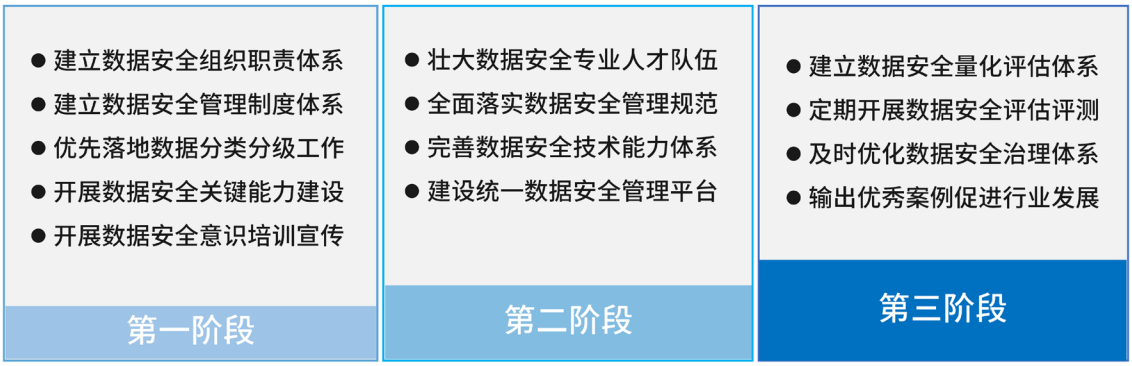
二是数据安全风险现状分析。有效的数据安全风险管理是组织推进业务发展的重要保障。不同组织需结合其业务场景，基于数据全生命周期安全防护要求，通过数据安全风险评估等方式识别数据面临的安全威胁及所在环境的脆弱性，形成风险问题清单，提炼数据安全建设需求点。

三是行业最佳实践对比。行业对比是组织经营决策的主要参考。通过分析同行业的数据安全建设先进案例，并与组织现状进行横向对比，有助于提炼出更加适宜的数据安全建设方向和建设思路。

2. 方案规划

组织应根据现状分析结果，结合数据安全治理目标，给出可落地实施的数据安全治理规划方案，并提炼重点目标和任务，分阶段落实到工程实施中。方案规划可以从前文所述的四个数据安全治理维度入手，通过对组织架构、制度流程、技术工具、人员能力的不断建设与完善达成建设目标。

以一个数据安全治理建设刚起步的企业为例，一般来说，可以将数据安全规划分为三个阶段，如图 6 所示。



来源：数据安全推进计划

图 6 数据安全治理规划示例

第一阶段，组织尚处于数据安全治理建设初期，急需在内部明确数据安全治理职责分工和管理要求，因而建议主要完成初步的数据安全治理体系建设工作，包括数据安全组织机构的建立、数据安全制度体系的编制、数据安全基础能力建设以及数据安全意识培训宣贯。同时数据分类分级作为实施数据安全管理措施和技术措施的前提，是一个需要提前布局且长期推进的工作。

第二阶段，组织有了一定的数据安全治理基础，可以在这一阶段着重完善数据安全技术能力体系，通过建设统一的管理平台，全面落实数据安全管理规范及策略要求，并通过常态化数据安全运营，实现持续的数据安全保障能力。同时，应加强数据安全能力培训体系的构建，培养复合型数据安全专业人才，壮大数据安全人才队伍。

第三阶段，组织已经初步建成数据安全治理体系，这一阶段以持续优化为主要目标，重在建立数据安全治理的量化评估体系，定期开展数据安全评估评测，监测各项指标的达标情况。再根据评估评测结果及时优化建设内容，最终达到较高的数据安全治理水平。同时，通过提炼并输出成功经验，促进行业共同进步。

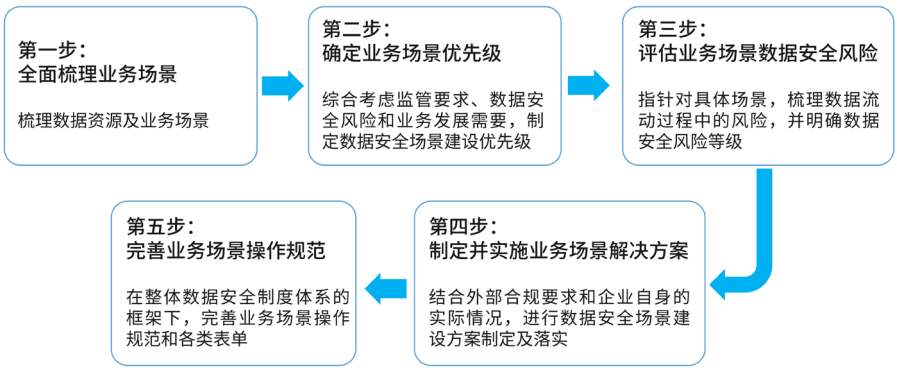
3. 方案论证

为保障规划方案在建设过程的顺利实施，应从以下方面进行论证分析。**一是可行性分析，**根据组织现状，明确人力、物力、资金的投入与产生的效益对比，协调数据安全管理机制和技术能力建设与业务系统之间的分歧，确保在业务发展与安全保障之间达到平衡。**二是安全性分析，**方案在正式实施前，要进行详细的方案论证分析，确保可以在业务稳定运行的前提下实施治理建设，同时要考虑治理过程中可能产生的新风险，避免未知风险的引入。**三是可持续性分析，**数据安全治理是持续性过程，随着业务拓展和技术进步，规划方案在保证与当前组织现有体系兼容的同时，也要考虑与后续的发展相适应。因此数据安全治理方案不仅要考虑当下，还要着眼于未来。在满足当前数据安全需求的同时，还要适应后续的持续发展。

（二）数据安全建设

数据安全建设阶段主要对数据安全规划进行落地实施，建成与组织相适应的数据安全治理能力，包括组织架构的建设、制度体系的完善、技术工具的建立和人员能力的培养等。

通过数据安全规划，组织对如何从零开始建设数据安全治理体系有了一定认知，同时也应意识到数据安全治理的建设是一项需要长期开展和持续投入的工作，无法一蹴而就。为了快速响应不同业务场景下不同的数据安全策略要求，应基于场景需要选择性部署技术工具，编制三级操作指南文件，形成四级记录模板。通过逐个场景的数据安全建设，最终推动数据安全治理体系在组织内的全面落地。本指南梳理了场景化数据安全治理建设的总体路线，如图 7 所示。



来源：数据安全推进计划

图 7 场景化数据安全建设五步走

第一步：全面梳理业务场景

梳理数据资产和业务场景是组织进行场景化数据安全治理建设的前提，可以帮助组织了解数据安全治理对象全貌，为组织场景化数据安全治理提供行动地图。

目前，对业务场景的划分尚未有统一的标准，本指南根据对数据安全供应侧及需求侧的调研，将场景划分方法归类为基于数据全生命周期和基于业务运行环境两种划分方式。

（1）基于数据全生命周期的场景划分

基于数据全生命周期的场景划分是分别在采集、传输、存储、使用、共享、销毁各环节抽象出典型应用场景，如图 8 所示。

- 数据采集环节主要有个人信息主体数据采集、外部机构数据采集、数据产生等场景。
- 数据传输环节主要有内部系统数据传输、外部机构数据传输等场景。
- 数据存储环节主要有数据加密存储、数据库安全等场景。
- 数据使用环节主要有应用访问、数据运维、测试和开发、网络和终端安全、数据准入、数据分析与挖掘等场景。
- 数据共享环节主要有内部共享和外部共享等场景。
- 数据销毁环节有逻辑删除、物理销毁和数据退役等场景。
- 此外还有一些基础性的工作，如数据分类分级应该作为单独的场景纳入到整体的场景视图中。

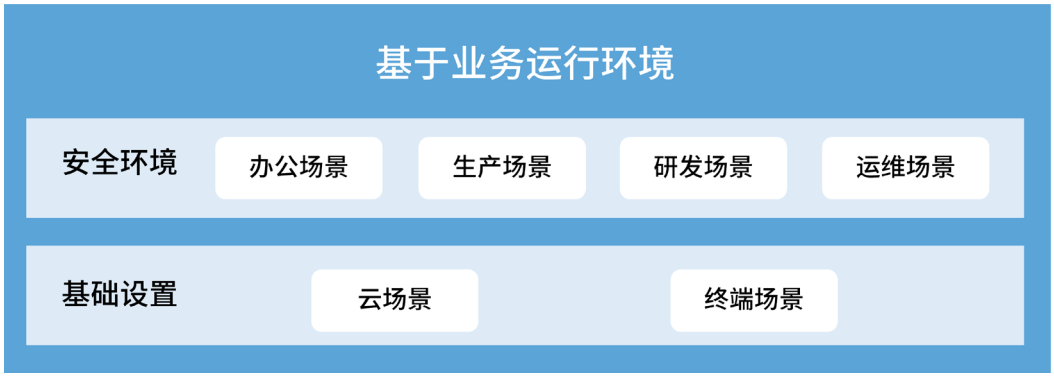
来源：数据安全推进计划

图 8 基于数据全生命周期的场景划分

基于数据全生命周期的场景划分方式，一方面能更好地契合当前法律法规中关于数据全生命周期的安全要求，一方面更加匹配当前主流的数据安全治理体系框架。

（2）基于业务运行环境的场景划分

组织的业务虽然各有不同，但是其业务运行环境的划分基本相同，据此可以将业务场景划分为：办公场景、生产场景、研发场景、运维场景等。还可以基于支撑业务运行的基础设置进一步细分为云、终端等场景，如图 9 所示。



来源：数据安全推进计划

图 9 基于业务运行环境的场景划分

基于业务运行环境的场景划分方式，一方面与业务的研发上线紧密关联，有利于场景的识别，另一方面兼容组织安全域的划分，有利于充分利用原有的网络安全能力。

第二步：确定业务场景治理优先级

在业务场景梳理完成后，组织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。

以上文提到的基于数据全生命周期的场景划分方式为例，数据分类分级是数据安全的基础性工作基本已经成为行业共识，随着行业数据分类分级指南的不断建立和完善，组织应跟紧行业发展步伐，前置数据分类分级工作的优先级。其次，数据采集环节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，容易影响组织品牌形象，因而需要优先治理。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。

第三步：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。

第四步：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，组织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，组织需要根据实际情况通过自研解决方案或者甄选适宜的供应侧解决方案。

第五步：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，组织应督促业务部门在实施具体的技术措施后，及时完善组织整体数据安全制度体系中关于三级与四级的制度文件，如《远程访问操作规范》、《数据备份操作规范》、《数据防泄露操作规范》、《堡垒机操作规范》等，以保持制度流程和技术落地的一致性。

（三）数据安全运营

数据安全运营阶段通过不断适配业务环境和风险管理需求，持续优化安全策略措施，强化整个数据安全治理体系的有效运转。

1. 风险防范

数据安全治理的目标之一是降低数据安全风险，因此建立有效的风险防范手段，对于预防数据安全事件发生有重要作用，可以从数据安全策略制定、数据安全基线扫描、数据安全风险评估三方面入手。

数据安全策略制定。一方面，根据数据全生命周期各项管理要求，制定通用安全

策略，另一方面，结合各业务场景安全需要，制定针对性的安全策略。通过将通用策略和针对性策略结合部署，实现对数据流转过程的安全防护。

数据安全基线扫描。基于面临的风险形势，定期梳理、更新相关安全规范及安全策略，并转化为安全基线，同时直接落实到监控审计平台进行定期扫描。安全基线是组织数据安全防护的最低要求，各业务的开展必须满足。

数据安全风险评估。通过将日常化定期开展的数据安全风险评估结果与安全基线进行对标，发现不满足基线要求的评估项，再通过改进业务方案或强化安全技术手段的方式实现风险防范。

2. 监控预警

数据安全保护以知晓数据在组织内的安全状态为前提，需要组织在数据全生命周期各阶段开展安全监控和审计，以实现对数据安全风险的防控。可以通过态势监控、日常审计、专项审计等方式对相关风险点进行防控，从而降低数据安全风险。

态势监控。根据数据全生命周期的各项安全管理要求，建立组织内部统一的数据安全监控审计平台，对风险点的安全态势进行实时监测。一旦出现安全威胁，能够实现及时告警及初步阻断。

日常审计。针对账号使用、权限分配、密码管理、漏洞修复等日常工作的安全管理要求，利用监控审计平台开展审计工作，从而发现问题并及时处置。审计内容包括但不限于表 3 所示内容。

表 3 日常审计项目示例

审计项目	活跃度异常账号、弱口令、异常登录
	敏感数据是否加密存储
	敏感数据是否加密传输
	个人信息采集是否得到授权
	异常 / 高风险操作行为
	敏感数据是否脱敏使用
	漏洞是否定期修复
	分类分级策略是否正确落实
	接口安全策略的落实情况
	销毁过程的日常监督

来源：中国信息通信研究院

专项审计。以业务线为审计对象，定期开展专项数据安全审计工作。审计内容包括数据全生命周期安全、隐私合规、合作方管理、鉴别访问、风险分析、数据安全事件应急等多方面内容，从而全面评价数据安全工作执行情况，发现执行问题并统筹改进。

3. 应急处理

一旦风险防范及监控预警措施失效，导致发生数据安全事件，组织应立即进行应急处置、复盘整改，并在内部进行宣贯宣导，防范安全事件的再次发生。

数据安全事件应急处置。根据数据安全事件应急预案对正在发生的各类数据安全攻击警告、数据安全威胁警报等进行紧急处置，确保第一时间阻断数据安全威胁。

数据安全事件复盘整改。应急处置完成后，应尽快在业务侧组织复盘分析，明确事件发生的根本原因，做好应急总结，沉淀应急手段，跟进落实整改，并完善相应应急预案。

数据安全应急预案宣贯宣导。根据数据安全事件的类别和级别，在相关业务部门或全线业务部门定期开展应急预案的宣贯宣导，降低发生类似数据安全事件的风险。

（四）数据安全评估优化

数据安全评估优化阶段主要是通过内部评估与第三方评估相结合的方式，对组织的数据安全治理能力进行评估分析，总结不足并动态纠偏，实现数据安全治理的持续优化及闭环工作机制的建立。

1. 内部评估

组织应形成周期性的内部评估工作机制，内部评估应由管理层牵头，执行层和监督层配合执行，确保评估工作的有效执行，并应将评估结果与组织的绩效考核挂钩，避免评估流于形式。常见的内部评估手段包括评估自查、应急演练、对抗模拟等。

评估自查通过设计评估问卷、调研表、定期执行检查工具等形式，在组织内部开展评估，主要评估内容至少应包括数据全生命周期的安全控制策略、风险需求分析、监控审计执行、应急处置措施、安全合规要求等内容。

应急演练通过构建内部人员泄露、外部黑客攻击等场景，验证组织数据安全治理措施的有效性和及时止损的能力，并通过在应急演练后开展复盘总结，不断改进应急

预案及数据安全防护能力。应急演练可采用实战、桌面推演等方式，旨在验证数据安全事件应急的流程机制是否顺畅、技术工具是否实用、安全处置是否及时等，进一步完善应急预案，补足能力短板。

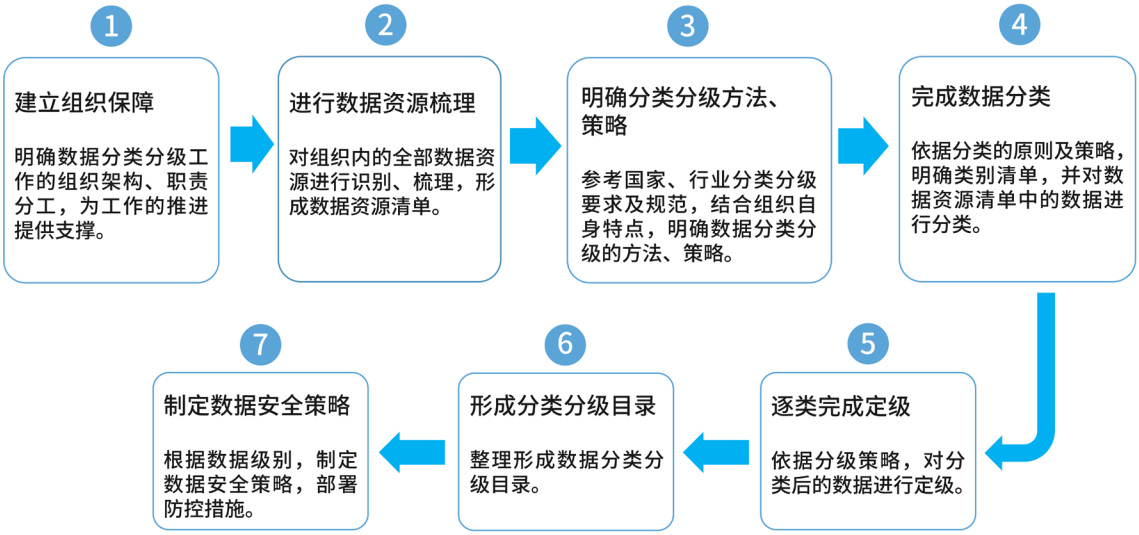
对抗模拟通过搭建仿真环境开展红蓝对抗，或模拟黑产对抗，帮助组织面对内外部数据安全风险时实现以攻促防，沉着应对，并在这个过程中不断挖掘组织数据安全可能存在的攻击面和渗透点，尤其是面对组织内部数据泄露风险，可以有针对性的完善数据安全治理工作机制和技术能力。

2. 第三方评估

除了内部评估外，组织还应引入第三方评估。第三方评估以国家、行业及团体标准等为执行准则，能客观、公正、真实地反映组织数据安全治理水平，实现对标差距分析。如中国信息通信研究院 2020 年底推出的**国内首个数据安全治理能力评估服务，**结合业务场景和全生命周期数据流，从组织架构、制度流程、技术工具、人员能力的建设情况入手，综合考察组织数据安全治理能力的持续运转及自我改进能力。目前该评估服务已在金融、电信、互联网、汽车等多个行业领域获得广泛认可，是组织进行全面摸排、横向对比的重要抓手。

四、数据分类分级场景建设思路

数据分类分级是数据安全治理实践过程中的关键场景，是数据安全工作的桥头堡和必选题。本指南结合行业实践，提出如图 10 所示的七步走建设思路，可供刚开展数据分类分级工作的组织参考。



来源：中国信息通信研究院

图 10 数据分类分级“七步走”建设思路

（一）第一步：建立组织保障

对组织而言，数据分类分级工作是一项复杂的长期性工作，是业务知识、数据知识和安全知识的交叉领域，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，我们看到各组织一般有数据安全管理的牵头部门或团队统筹数据分类分级工作的开展，而在职责分工上，则体现出一定的差异性。

- 以某电信运营商为例，在职责划分方面，明确了由数据安全的管理部门负责制定数据分类分级的方法及策略，规范数据资产梳理工作，并监督数据分类分级工作的落实。而各数据生产运营和使用的责任部门则需要维护本部门的数据资源清单、梳理部门的重要

数据目录、并按照数据安全管理部门制定的标准执行数据分类分级规定动作，制定并落实差异化管控措施等。

- 以某金融机构为例，在职责划分方面，明确了由数据安全的管理部门牵头开展数据分类分级工作，制定相关制度流程，并建设数据分类分级技术能力。由于建设了数据中台对数据进行统一管理，其他部门仅需配合数据分类分级评估工作，对数据分类分级结果进行复核。
- 以某互联网公司为例，在职责划分方面，明确了由数据安全管理部门负责各类数据的分类、汇总和管理等工作。其他部门主要负责识别本部门的各类敏感数据并同步至数据安全管理部门，同时负责本部门敏感数据相关数据安全管控措施的制定。

（二）第二步：进行数据资源梳理

在进行数据分类分级之前，需要对组织内的全部数据资源进行识别、梳理，明确当前组织内部存储了哪些数据、数据存储的格式、数据范围、数据流转形式、数据访问控制方式、数据价值高低等问题，并形成数据资源清单。

在实际工作中，数据资源的梳理有两种常见的工作思路。一种是站在数据治理的角度，为了达到对数据质量进行管理的首要目标而进行全量数据的盘点梳理，与此同时，梳理的结果可以复用于数据分类分级工作。一种是站在数据安全的角度，先对敏感数据进行识别梳理，以快速响应相关安全管理要求，再逐渐扩展至全域数据范围。

（三）第三步：明确分类分级方法、策略

数据分类分级的方法、策略是指导此项工作开展的重要依据。组织需要参考国家及行业相关数据分类分级要求及规范，并结合自身业务属性与管理特点，明确数据分类分级的方法、策略，如明确数据分类与定级的基本原则、基本方法等。

当前，为指导数据分类分级工作的推进落实，各行业、各领域纷纷制定相关标准规范，如表 4 所示。通过明确数据分类分级工作的原则、方法、定义，并在此基础上给出部分示例，进一步细化国家关于数据分类分级工作的要求，推动该项工作在不同行业企业及组织机构的落地实施。

表 4 近几年数据分类分级相关规范

发布时间	名称	发布方
2020 年 2 月	《工业数据分类分级指南（试行）》	工业和信息化部办公厅
2020 年 4 月	GB/T 38667-2020《信息技术 大数据 数据分类指南》	国家市场监督管理总局、国家标准化管理委员会
2020 年 9 月	JRT 0197-2020《金融数据安全 数据安全分级指南》	中国人民银行
2020 年 12 月	YD/T 3813-2020《基础电信企业数据分类分级方法》	工业和信息化部
2021 年 5 月	YD/T 3867-2021《基础电信企业重要数据识别指南》	工业和信息化部
2021 年 7 月	DB33/T 2351-2021《数字化改革 公共数据分类分级指南》	浙江省市场监督管理局
2021 年 10 月	《重庆市公共数据分类分级指南（试行）》	重庆市大数据应用发展管理局
2021 年 12 月	《网络安全标准实践指引——网络数据分类分级指引》	全国信息安全标准化技术委员会秘书处
2022 年 3 月	GB/T XXXXX/XXXX《信息安全技术 重要数据识别规则》（征求意见稿）	国家市场监督管理总局、国家标准化管理委员会
2022 年 9 月	GB/T XXXXX/XXXX《信息安全技术 网络数据分类分级要求》（征求意见稿）	国家市场监督管理总局、国家标准化管理委员会

来源：中国信息通信研究院

（四）第四步：完成数据分类

组织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。

在实际工作中，如表 5 所示，基础电信、证券期货、工业行业等领域制定了较为明确的分类方法和示例，有利于行业组织参考。对于暂未形成分类模板的行业，组织

可以从经营维度按照通用分类模板进行分类[1]。另外，针对个人信息的分类方式，组织也可以结合 GB/T 35273-2020《信息安全技术 个人信息安全规范》给出的规范进行完善。总体来说，类别定义一般会根据行业领域的不同而产生不同的子类划分方式，需要注意的是不同类别之间不能重复和交叉。

表 5 各行业数据分类示例

行业领域	一级分类示例	二级分类示例
基础电信	用户相关数据	用户身份相关数据、用户服务内容数据、 用户服务衍生数据、用户统计分析类数据
	企业自身数据	网络与系统的建设与运行维护类数据、 业务运营类数据、企业管理数据、其他数据
证券期货行业	交易	交易管理、结算管理、行情、资讯、投资者管理、产品管理
	监管	监管报送、合规风控、稽核
	信息披露	信息披露管理、研究报告
	其他	营销服务、业务管理、技术管理、综合管理
工业数据（工业企业）	研发数据域	研发设计数据、开发测试数据等
	生产数据域	控制信息、工况状态、工艺参数、系统日志等
	运维数据域	物流数据、产品售后服务数据等
	管理数据域	系统设备资产信息、客户与产品信息、 产品供应链数据、业务统计数据等
	外部数据域	与其他主体共享的数据等
工业数据（平台企业）	平台运营数据域	物联采集数据、知识库模型库数据、研发数据等
	企业管理数据域	客户数据、业务合作数据、人事财务数据等
通用	用户数据	/
	业务数据	/
	经营管理数据	/
	系统运行	/
	安全数据	/

来源：数据安全推进计划

1 《网络安全标准实践指南—网络数据分类分级指引》（TC260-PG-20212A）

（五）第五步：逐类完成定级

数据分级主要从数据安全保护的角度，考虑影响对象、影响程度两个要素对数据所在的安全级别进行判定。不同行业分级标准在影响对象和影响程度的划分上有所不同，从而也导致了分级结果的差异性。组织应根据实际情况完成定级工作，常见的数据定级示例如表 6 所示。

表 6 各行业数据分级示例

行业领域	影响对象	影响程度	分级示例（从高到低）
基础电信企业	国家安全、社会秩序、企业经营管理和公众利益	严重、高、中、低	第四级、第三级、第二级和第一级
金融行业	国家安全、公众权益、个人隐私、企业合法权益等	严重损害、一般损害、轻微损害、无损害	5 级、4 级、3 级、2 级、1 级
证券期货行业	行业、机构、客户	严重、中等、轻微、无	4（极高）、3（高）、2（中）、1（低）
工业数据	工业生产、经济效益	/	三级数据、二级数据和一级数据

来源：数据安全推进计划

（六）第六步：形成分类分级目录

基于上述工作，组织还需形成整体的数据分类分级目录，明确数据类别和级别的对应关系，为各部门落实数据分类分级工作提供依据。金融机构典型数据分类分级目录如图 11 所示。

（七）第七步：制定数据安全策略

在完成数据分类定级的基础上，还需要依据国家及行业领域给出的安全保护要求，建立数据分类分级保护策略，对数据实施全流程分类分级管理和保护。如某电信运营商建立了如表 7 所示的数据分类分级保护要求映射表。

数据归类和细分							安全级别	备注
一级子类	二级子类	定义说明	三级子类	定义说明	四级子类	内容	最低安全级别参考	
	合约协议	指合同或协议所包含的所有属性数据，如合同法以及商业银行法所规定的基本属性信息，以及各种特定业务合同所包含的特定属性信息。	合同通用信息	指合同法以及商业银行法所规定的、各种特定业务通用的基本属性数据。	基本信息	指合同法以及商业银行法所规定的、各种特定业务通用的基本属性数据，如合同编号、合同名称、合同种类、合同状态、生效日期、到期日期、终止日期、期限、金额、币种、利率相关属性信息等。	2	
			存款业务信息	指存款业务所涵盖的相关属性数据，如存款业务种类、期限类型等。	基本信息	指存款业务的基本属性数据，如存款业务种类、期限类型等。	2	
					计息信息	指账户的计息相关信息数据，如起息日期、到期日期、结息方式、计息基准、计息期限等。	2	
			贷款业务信息	银行贷款业务所涵盖的相关属性信息，包括指贷款业务所涵盖的相关属性信息，包括放款、还款、逾期、展期等相关业务属性信息。	基本信息	指贷款业务的基本属性信息数据，如贷款类型、贷款用途、贷款投向、贷款金额、贷款余额、保证金等。	2	
					授信信息	指贷款业务涉及授信的相关数据信息，如授信种类、授信用途、授信币种、授信期限、开始日期、终止日期等。	2	
					担保信息	指贷款业务涉及担保的相关数据信息，如担保人、担保方式、保证种类、担保金额、担保比例等。	2	
					放还款信息	指贷款业务放还款的相关数据信息，如放款日期、放款金额、还款方式、还款金额、还款日期等。	2	
					逾期信息	指贷款业务涉及逾期的相关数据信息，如逾期日期、逾期金额、逾期天数、罚息利率、罚息金额、欠息金额等。	2	
					展期信息	指贷款业务涉及展期的相关数据信息，如展期期限、展期利率、展期金额、展期次数、展期原因等。	2	
					垫款信息	指贷款业务涉及垫款的相关数据信息，如垫款种类、垫款金额、垫款日期、垫款利率等。	2	

来源：中国人民银行

图 11 金融业机构典型数据定级规则示例

表 7 数据分类分级保护要求映射表示例

数据全生命周期环节	安全管控要求	级别				
		1	2	3	4	5
数据收集环节	安全管控要求 1	√	√	√	√	√
	安全管控要求 2		√	√	√	√
	安全管控要求 3				√	√

来源：数据安全推进计划

五、数据安全治理总结与展望

根据数据安全推进计划发布的《2022 年数据安全行业调研报告》，六成以上参与调研的需求侧企业在制度文件编制、合规工作开展、技术工具部署等方面推进了相关工作。由此看出，随着数据安全合规要求的逐步完善，数据安全治理工作正在高速发展、有力推进。未来：

政策引领与战略自驱齐头并进，推进数据安全治理不断深入。根据调研，“合规需求”、“防范数据安全风险”、“企业自身发展需要”是组织开展数据安全能力建设的主要驱动因素。这说明，一方面，政策驱动的合规需求对组织数据安全建设具有强推进作用；另一方面，保障数据安全在推动业务健康运营方面的重要作用愈加明显。因此，政策引领的外部驱动与发展战略的内部驱动将成为数据安全治理工作不断深入的助推剂。

数据驱动的业务发展，激励数据安全治理组织从“有型”到“有效”。根据数据安全推进计划发布的《2022 年数据安全行业调研报告》，98.2% 的受访者建立了专门的数据安全牵头管理团队，数据安全治理组织架构逐渐明晰。但由于数据与业务密切相关，其在实时产生及流动过程中涉及的主体很多，导致数据安全主体责任边界的实际划分及管理仍然存在较大挑战，如何在不同部门之间建立有效沟通机制，保障业务的安全合规开展是下一步关注重点。

数据安全风险治理能力的建设与提升，成为数据安全治理的重要组成。由于数据本身具备流动性、泛在性等特点，过长的流转链条、过大的威胁暴露面、过多的数据处理活动等，都为数据安全风险管控带来挑战，并进一步影响到数据安全治理的整体成效。为了进一步防范数据泄露、数据篡改等安全事件的发生，落实数据安全风险的源头管控，常态化数据安全风险评估提上日程，基于风险的治理能力建设与提升也成为数据安全治理工作的重要组成部分。

第三方数据安全评估认证作为提升数据安全治理能力的主要抓手，将被更多行业组织引入。在国家层面的支持下，第三方数据安全评估、认证服务市场正在蓬勃发展。中国信息通信研究院推出的首款市场化数据安全治理能力评估服务，自 2020 年进入市场以来，共完成了 4 批次 43 家组织机构的评估，广受好评。同时，国家市场监督管理总局与国家互联网信息办公室推出的数据安全管理认证、个人信息保护认证等工作也在稳步推进。越来越多的行业组织将通过引入第三方评估认证工作，持续优化自身数据安全治理能力。

附录：数据安全治理实践案例

（一）华泰证券股份有限公司

1. 建设思路

（1）厘清数据安全风险，明确安全治理方向

证券行业是产生和积累数据量最大、数据类型最丰富的领域之一，随着证券行业数字化转型、深化，证券业数据有着更加广泛的应用场景、应用范围，有着更高的应用价值。随着证券业数据的价值日益凸显，数据非法采集、数据贩卖、数据篡改、数据攻击、数据权限滥用等安全问题也层出不穷。如何更加安全地保障企业的数字化转型，降低数据安全风险，释放数据价值，成为了诸多转型企业中的重点工作。

面对新形势带来的安全挑战，华泰证券积极应对，从外部攻击风险、内部数据滥用风险、外部渠道数据泄露风险三个方面，厘清当前面临的数据安全风险，梳理的风险点覆盖管理体系、制度流程、技术手段、运营机制四个层面。

面对上述的数据安全风险，华泰证券开展了新一轮的数据安全治理工作。从完善数据安全制度管理体系、建立数据安全风险评估机制、建设分层分级的数据权限管控体系、提升数据安全风险监测和响应能力、强化外部渠道数据泄露跟踪调查能力五个方面着手，全方位保护公司重要数据资产以及客户信息，为公司数字化转型保驾护航。

（2）构建数据安全治理体系，夯实数字化转型基础

华泰证券从顶层明确公司数据安全管理战略，强化公司数据安全管理体系，以贯彻国家网络空间安全战略、满足政策合规要求、统筹全体系数据安全为目标，推进公司整体安全管控水平不断提升，为业务发展保驾护航。

华泰证券以数字化转型战略为指引，以数据安全管理为保障，以技术体系为支撑，建立了覆盖数据全生命周期的企业级数据安全治理体系，如图 12 所示。

华泰证券对标国家行业标准，并结合自身数据安全战略、数据安全管理体系，建立了基于数据全生命周期的数据安全管理三层框架体系，从管控层、技术支撑层、运营层三个维度开展数据全生命周期安全管理工作。

（3）共享行业经验，共建数据安全生态

华泰证券作为数据安全推进计划成员单位，积极参与行业数据安全交流，分享数据安全治理经验，参加业界数据安全相关标准建设工作，如参与编写《证券期货业数据安全风险防控 数据分类分级指引》，共同推进行业数据安全生态建设。

来源：华泰证券

图 12 华泰证券数据安全治理体系

2. 治理实践及亮点

华泰证券严格按照国家《数据安全法》《个人信息保护法》等法律法规、行业规范和监管规定，落实数据安全相关工作，通过建立健全数据安全管理机制，基于“制度、组织、人员、技术”为核心的管理框架，规范数据处理活动，强化公司经营活动中相关数据处理的合法合规性，从数据安全管理体系、数据安全技术体系、数据安全运营体系等方面推进数据安全治理实践，打造证券行业数据安全治理标杆。

（1）建立规范化的数据安全管理体系

华泰证券从数据安全组织架构、数据安全制度体系两个方面开展数据安全治理工作，以满足监管要求以及风险管理需要。

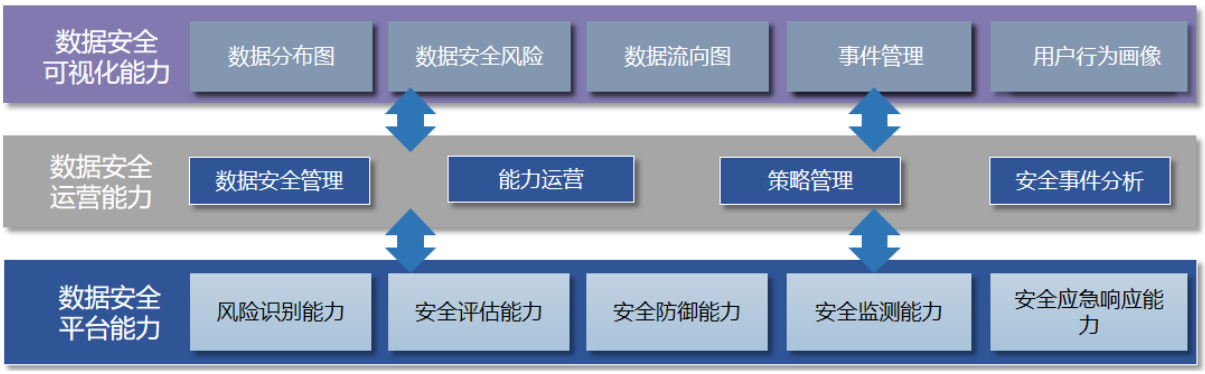
组织架构方面，华泰证券建立了完备的数据安全组织架构体系，设立公司数据治理委员会，在经营管理层的领导下，负责统筹和领导数据安全工作；数据治理委员会下辖数据安全与个人信息保护工作小组，由信息技术部门、业务部门、合规风控部门派员参与，多部门协同推进数据安全工作，将数据安全责任落实到每个部门、每个业务、

每个系统和每个员工。加强数据安全人才培养，建立起一支具备数据安全管理、数据安全建设、数据安全运营等专业安全能力的自有人才队伍。

制度体系方面，华泰证券深入研究国家关于数据安全、个人信息保护相关的法律法规和标准，结合公司实际情况，建立了公司的数据安全三层制度体系，包括：顶层的公司级数据安全管理办法、围绕数据全生命周期的安全管理规范、以及细化的各类数据安全细则，对数据安全管理职责分工、数据全生命周期安全保护要求、个人信息保护要求、数据安全实施细则等进行了明确，实现对数据全生命周期安全防护保障以及对数据安全管理和运营的支撑。

（2）建设覆盖数据全生命周期的数据安全技术体系

华泰证券以防范外部数据窃取、防范内部数据滥用和防范外部渠道泄露为抓手，依托数据安全可视化能力、数据安全运营能力、数据安全平台能力，构建如图 13 所示的公司数据安全三层技术体系，进一步加强数据安全保护能力，防范信息泄露。



来源：华泰证券

图 13 华泰证券数据安全技术体系

数据安全平台能力，基于IPDR框架，部署各类数据安全技术手段，覆盖网络、平台、应用、终端，形成事前、事中、事后的数据安全技术能力，并通过各技术能力组合形成风险识别、安全评估、安全防御、安全监测、安全响应五大服务能力。

数据安全运营能力，包括数据安全管理、能力运营、策略管理、安全事件分析四个方面。数据安全管理方面，通过深度分析各类法律法规和标准，形成数据安全基线和风险矩阵，为能力运营、策略管理和安全事件分析提供指引。能力运营方面，基于数据安全平台能力，开展安全评估、安全监测、安全检测和应急处置。策略管理方面，根据公司数据安全态势，动态调整数据安全管控策略，保障数据安全高效流转。安全事件分析方面，对数据安全告警、数据流转记录、用户行为日志等进行分析溯源，发

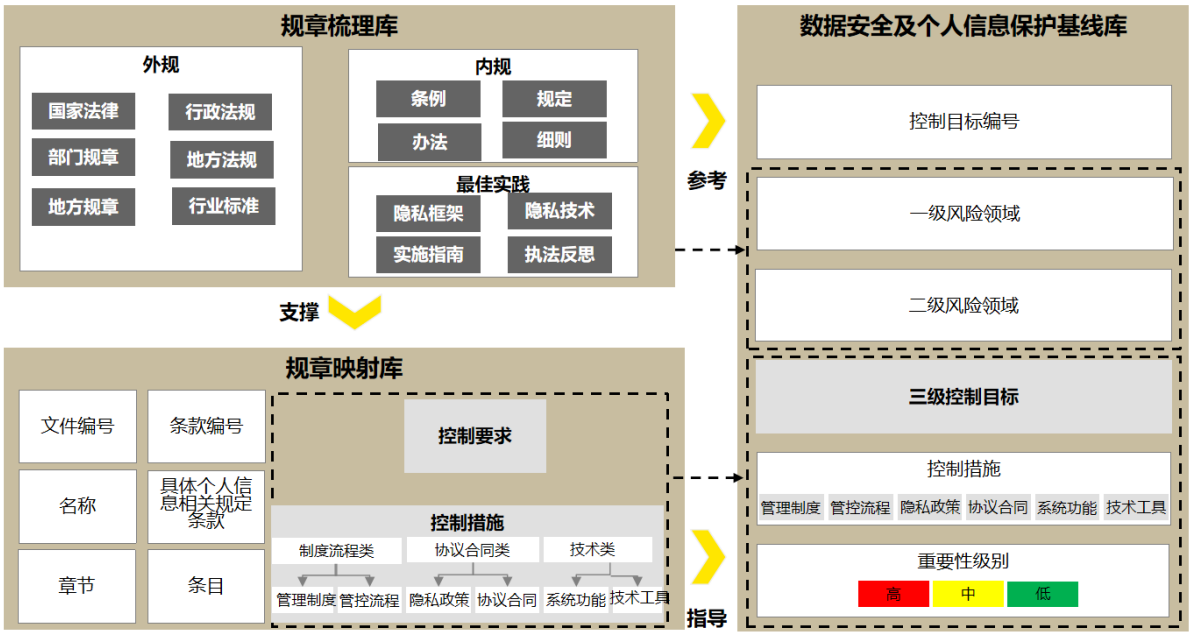
现数据安全风险。

数据安全可视化能力，基于数据安全平台能力和运营能力，绘制展示公司数据地图、数据流向图，依托态势感知能力展现数据安全风险态势、用户行为画像。

（3）实施精细化的数据安全运营体系

华泰证券从风险防范、监控预警、应急处置三个方面，构建“感知风险、看见威胁、抵御攻击”的数据安全运营体系，为公司数字化转型保驾护航。

风险防范，采用“基线化”+“工程化”+“技术化”理念，以法律法规、行业标准、实践指南为切入点，将数据安全评估过程嵌入业务原有生产流程并在早期介入风险管理，降低业务数据安全风险，如图 14 所示。



来源：华泰证券

图 14 数据安全评估基线化方案

监控预警，依托数据安全技术体系，动态监控公司内部跨网、跨域、跨实体流转的数据，实时发现数据安全威胁并预警，快速溯源处置安全事件。

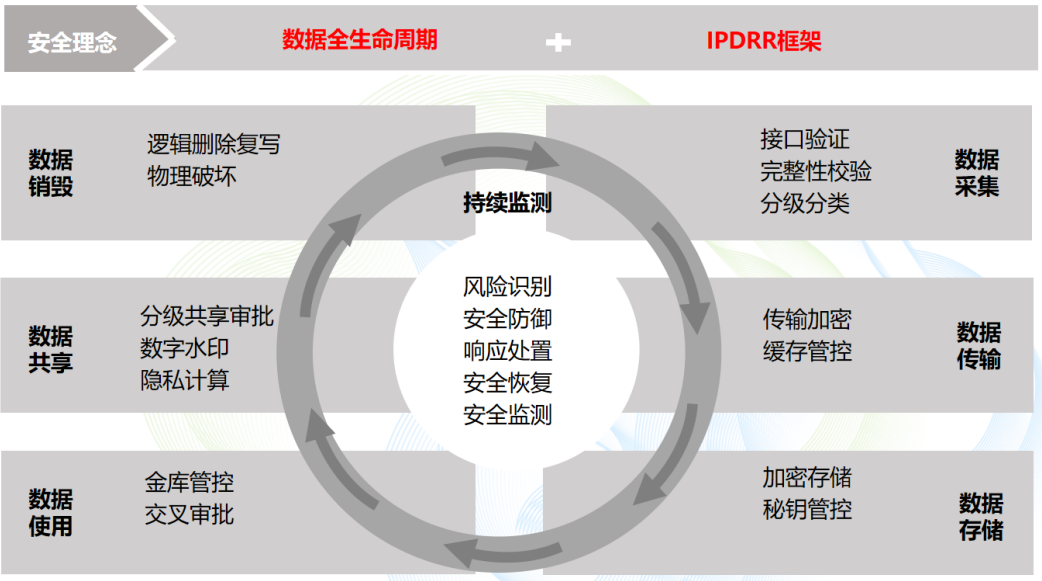
应急处置，建立数据安全事件应急响应机制，编制应急预案，开展应急演练，确保事件发生后可以快速响应，及时恢复，最大程度上减少损失，并降低事件造成的消极影响。

（二）中移信息技术有限公司

1. 建设思路

为落实国家、上级单位“十四五”规划要求，坚持营造良好数字生态，中移信息技术有限公司启动“十四五”IT 领域数据安全发展规划制定工作。主要包含 7 大能力，1 个党建引领保障，31 项关键任务，以加强基础保障能力建设、安全系统建设。并且梳理总结了 9 个发力点，分别是构建网络安全态势监测与感知体系、加强关键信息基础设施安全防护、增强统一调度指挥能力、强化安全融合保障、遵从网络安全法规、提升新型数字基础设施安全管理水平、完善技术手段建设、强化数据安全保护、加大核心技术安全可控。

如图 15 所示，公司通过结合 IPDRR 的安全框架和数据全生命周期的治理理念，来贯彻十四五规划，并且通过整合 IT 安全能力，全面构建了数据安全全生命周期的能力体系，实现数据安全的可管可控。在数据采集、传输、存储、使用、共享、销毁各个环节部署相应的安全技术，并对全流程进行持续监测、违规分析及告警处置。



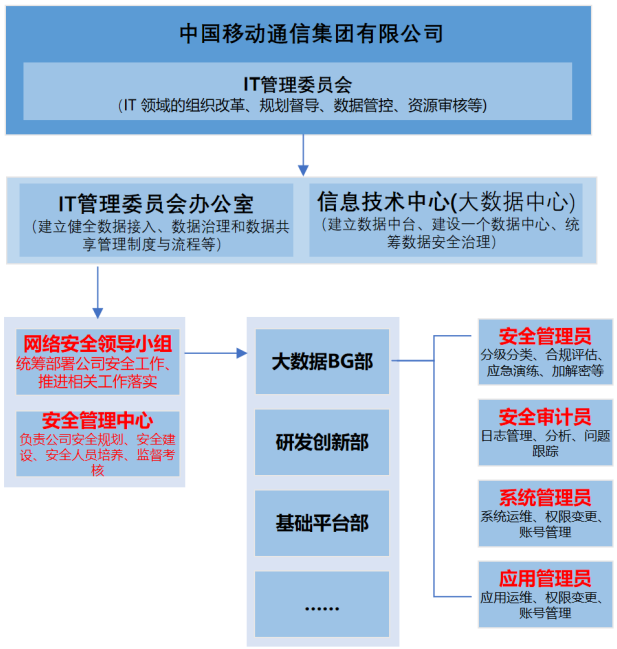
来源：中移信息技术有限公司

图 15 中移信息数据安全全生命周期能力体系

2. 治理实践

公司通过组织架构、制度流程、技术体系等方面作为抓手，落实“十四五”安全战略规划。

在组织架构方面，公司设立安全管理中心，负责统筹安全规划、建设安全平台、监督安全工作、考核执行情况，如图 16 所示。各个业务部门依据安全管理中心的要求，设立专人专岗负责数据安全管理、安全审计、系统管理及应用管理。2018 年，为了推进安全工作部署和落实，中移信息技术有限公司成立网络安全领导小组，领导小组包括公司高层领导，办公室设在安全管理中心。根据《数据安全管理办法》，网络安全领导小组兼顾数据安全领导职责。



网络安全领导小组：
公司网络安全领导小组在集团公司网络安全领导小组的统一领导下，负责贯彻执行政府相关主管部门有关数据安全法律法规、方针政策及各项工作要求，审定公司数据安全的发展战略、中长期规划和重大决策。

安全管理中心：
第八条安全管理中心是公司数据安全归口管理部门，其主要职责有：（一）负责组织制订数据安全管理规定和实施细则,明确数据安全整体要求；（二）负责制定年度数据安全保护计划；（三）负责监督和检查各部门数据安全相关政策要求落实情况；（四）负责组织开展数据安全管理审核与数据安全评估；（五）牵头组织开展数据安全培训；……

各数据安全支撑部门：
第九条数据安全支撑部门，除承担本部门数据安全管理职责外，还需承担职责包括：（一）协助开展数据安全技术保障措施的试点；（二）协助开展数据共享复评工作；（三）协助查处公司内部数据安全事件；（四）协助组织进行公司内部数据安全应急处置；（五）支撑建立数据安全技术保障措施，包括但不限于敏感日志上报等工作。

来源：中移信息技术有限公司

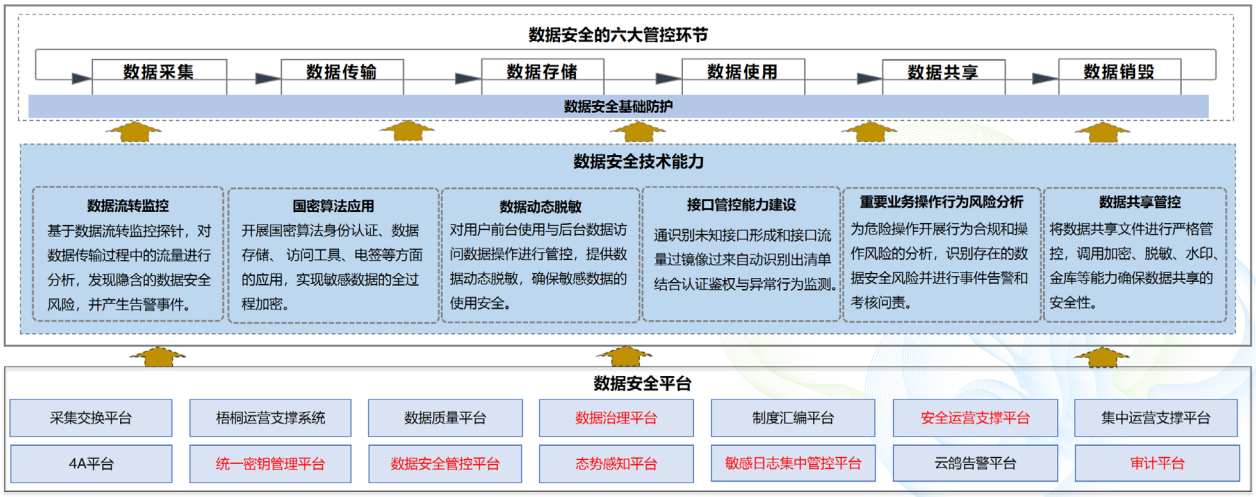
图 16 中移信息数据安全组织架构

在制度流程方面，公司依据法律法规、监管要求、行业要求、业务数据安全需求和数据安全风险控制需要等几个方面进行梳理，确定数据安全防护的目标、管理策略及具体的标准、规范、制度等，实现定责到人的管理机制。针对各个领域的安全管控制定了安全制度和流程规范，并建立了制度汇编模块展示公司的总体制度建设，全体人员可查阅，如图 17 所示。

来源：中移信息技术有限公司

图 17 中移信息数据安全制度体系

在技术体系方面，公司参照数据全生命周期安全管控的理念建设安全能力平台，构建数据安全技术支撑体系，如图 18 所示。遵循对不同级别的数据进行分级管控的原则，将安全技术体系贯穿数据全生命周期的 6 个阶段，实现数据安全保护目标。



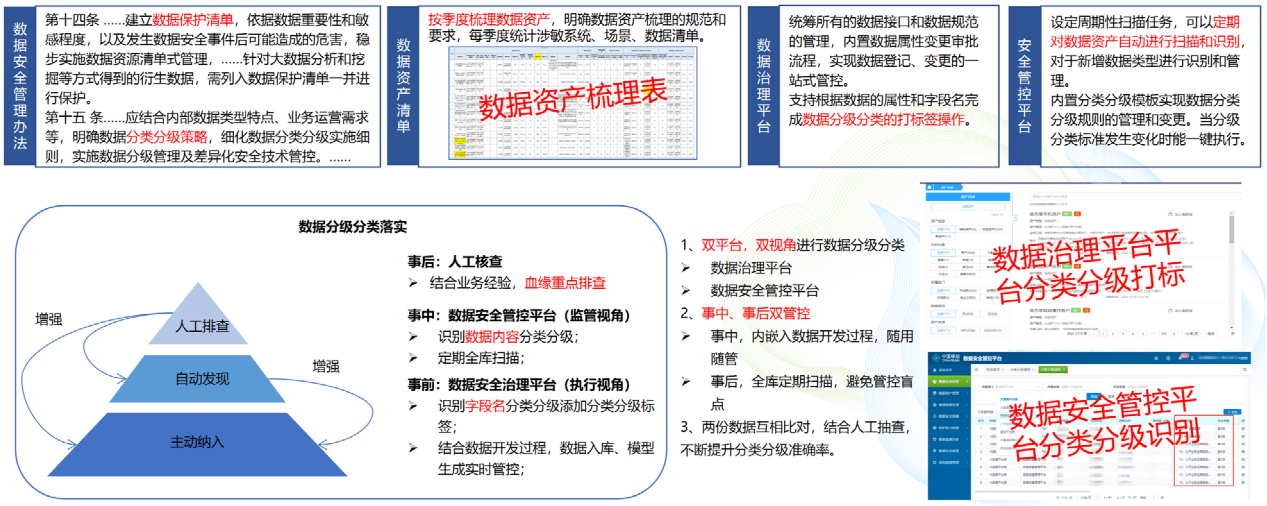
来源：中移信息技术有限公司

图 18 中移信息数据安全技术体系

3. 实践亮点

亮点一：如图 19 所示，为了打造安全的数据环境，保证数据在流动过程中时刻可以被管控，公司以数据分类分级作为治理基础，建立了事前主动纳入、事中自动发现、事后人工核查的闭环管理机制，实现数据在使用过程中自动化完成分级分类及敏感数据的流转监控。同时，建立了基于数据分类分级机制和数据流转流量分析的数据治理

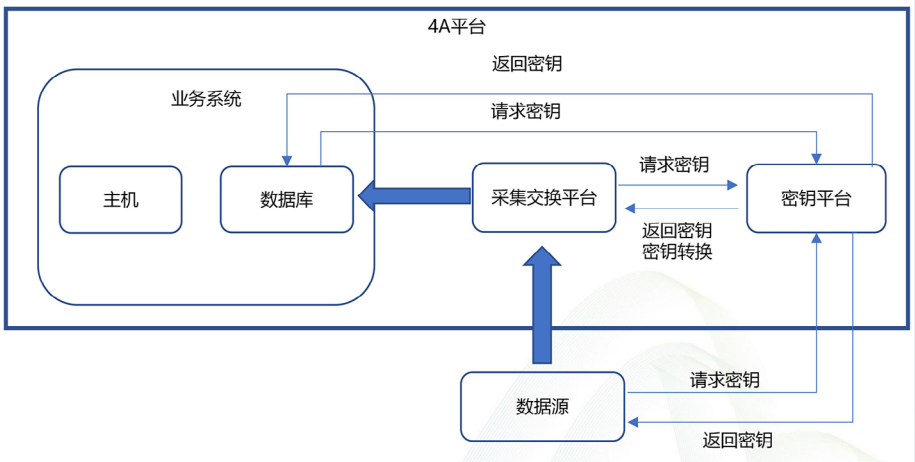
平台和数据安全管控平台，达到数据标签明确化，数据使用可控化的目标。



来源：中移信息技术有限公司

图 19 中移信息数据流动安全闭环管理机制

亮点二：如图 20 所示，为了保证数据静态安全，公司对存储的全量数据敏感字段进行加密处理，采用国密 SM4 等算法实现静态加密，全部四级敏感表以及个人信息字段均完成加密存储。在密钥管控工作中，遵循隐私保密原则，按需实时请求、不落地，进一步提升系统安全。 数据在存储使用及对外共享使用过程中也严格遵循以下原则：①保证数据需求通过严格的审批流程后，脱敏处理提供；②为了保证数据安全，大数据存储按分类分级标准，依据不同数据敏感等级进行差异化加密处理。

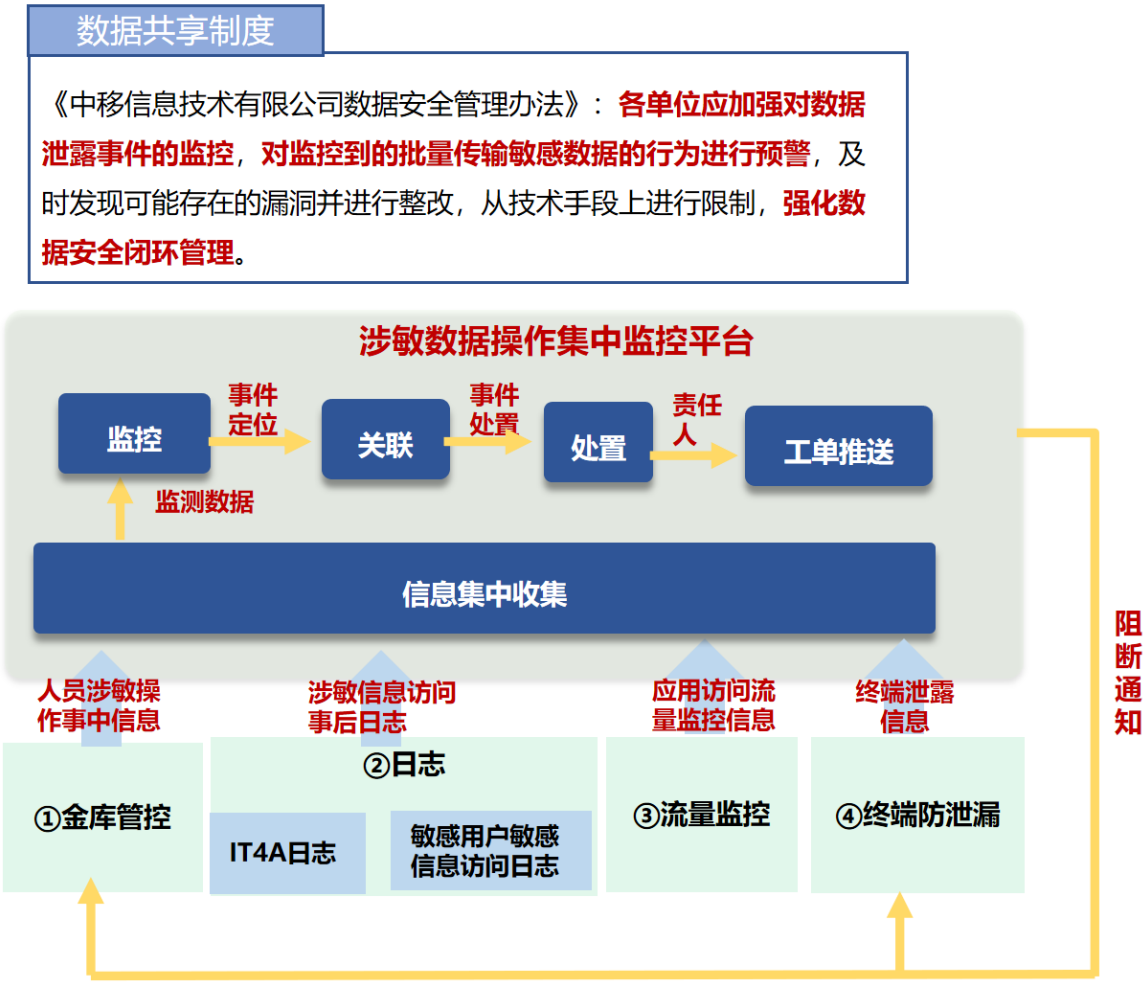


- 密钥平台功能包括：密钥生成、存储、分发、使用监控、鉴权、密钥转换等管理。

来源：中移信息技术有限公司

图 20 中移信息数据静态安全管理机制

亮点三：公司建设了如图 21 所示的共享操作实时管控体系，使用实时监控技术手段，建立数据下载行为分析引擎，实现对涉敏数据下载实时监控、高风险操作实时告警能力。同时，规范监控运营机制，组建涉敏数据下载监控运营团队，实现告警、确认、处置全流程的闭环运营模式，确保高风险操作得到及时排查和处置，提升数据下载（共享）环节的数据安全治理能力。



来源：中移信息技术有限公司

图 21 中移信息数据共享实时管控平台

（三）中国联通广东省分公司

1. 建设思路

广东联通以合法合规、安全使用为驱动，强化对内对外数据安全管控，分阶段规划构建“组织、管理、技术、运营”数据安全体系并不断完善。通过对数据全生命周期的防护，实现端到端的数据安全治理。总体分三个阶段建设数据安全体系：

- 第一阶段为“基础建设”，通过规划数据安全治理体系，组建数据安全组织，建设基础数据安全能力，夯实防护体系底座基础；
- 第二阶段为“能力升级”，通过升级数据安全一体化运营平台能力，逐步加强数据安全能力覆盖，实现基本完整的运营闭环；
- 第三阶段为“优化运营”，通过完善数据安全运营体系，实现数据安全指标精细化运营。

在治理过程中，对内专注于规范数据使用处理全流程，落实看数用数过程中数据分类分级管控各项安全措施；以及对数据要素赋能生产，数据服务过程构建安全防护体系。对外专注于数据对外合作的安全管控以及个人隐私保护。

广东联通的数据安全治理，在组织层面，嵌入广东联通数据治理组织架构，构建了自上而下的数据安全治理组织，明确部门职责分工、对人员定责定岗；在管理方面，承接集团数据安全要求，形成四级管理制度体系；在技术体系方面，广东联通使用集团集约化数安能力，结合省分自建数安能力，搭建对内对外的数据安全防护体系；在安全运营层面，通过“作业本”方式跟踪数据安全任务，结合考核与激励的管理措施，逐步实现数据安全精细化运营。

2. 治理实践

（1）构建数据安全治理框架

广东联通综合业界最佳的数据安全框架，依据集团公司战略与数据战略目标，制定数据安全治理战略。在战略指导下，建立如图 22 所示的一体化数据安全治理体系，即从数据安全组织、管理体系、技术体系到安全运营，提高广东联通数据安全管理及防护能力，使数据安全风险可感、可视、可控，保障数据安全有序流动，如图 22 所示。

来源：广东联通

图 22 广东联通数据安全体系框架

（2）建立健全数据安全治理体系

以组织架构为保障，通过建立健全数据安全管理体系、数据安全技术体系和数据安全运营体系，推动数据安全治理。

建立数据安全组织体系。广东联通设置了数据治理指导委员会（办公室），统筹推进数据安全工作，下设数据安全专项组，由管理组、业务组、对外合作组、技术组、隐私保护安全合规组、监督组 6 个小组构成，合力推动数据安全全面落地。

完善数据安全管理体系。广东联通依据国家、行业主管部门的数据安全相关法律法规与标准规范及联通集团相关数据安全要求，逐步构建四级数据安全制度体系，覆盖了数据全生命周期及数据分类分级、基础安全等各方面要求。

健全数据安全技术体系。广东联通数据安全技术体系以数据识别、数据加密、数据脱敏、接口安全、数据防泄露、操作审计、数据销毁、数据溯源八个安全能力为基础，围绕数据全生命周期安全需求，在集团能力基础上构建省分集约化数据安全能力，实现数据安全立体化防护。同时，积极研究并逐步推动建立隐私计算平台，探索个人隐私数据对外协同数据处理时合规防护，确保用户隐私数据安全。

完善数据安全运营体系。广东联通以安全合规需求为驱动，组建 SOC，构建了围绕数据感知、风险感知、安全合规、事件管理四个方面的运营体系，制定了安全实施、安全意识、数据保护、安全事件、敏感数据扩散五项运营指标，运用恰当的安全技术和管理手段，整合人、技术、流程，持续降低数据安全风险。依据运营指标结果，广东联通不断优化总结运营内容，提升数据安全运营能力，为数据持续性提供安全防护。

3. 实践亮点

亮点一：全面梳理和重塑工号实名管理的规范流程，打造基于身份证唯一标识的“实名认证、分级授权、日志溯源”，实现人脸识别、操作留痕、审计追溯，消除工号借用、盗用、越权等隐患。

广东联通 2022 年实施了工号实名制项目，该项目以“1 身份证：1 活体认证：N 工号”为底层逻辑，以八步法开展工号实名实人、高权限管控，实现核心系统 100% 实名，100% 实人登录，对异常工号行为进行监控，逐步实现工号数字化规范化管理。目前已纳管 199 套系统进行工号持续安全运营，清理不合规工号 28 万多个，回收高权限工号 1000 多个，4 套系统启动“活体 + 账号口令”登录，33 套系统启动“短信验证码 + 账号口令”登录，已设计 42 项安全指标周期性运营，有效保障了工号权限数据安全。

亮点二：针对 IT 系统多，且对用户基础数据调用服务需求大，以及业务发展、数据分析、运营等访问敏感数据的频繁需求，启动数据服务安全项目，确保数据服务涉及的数据调用、数据使用安全。

如图 23，依托集团数据中台和天擎能力商店，构建省分数据能力开放平台，统一提供基础数据调用服务。通过应用系统注册审批、账号身份校验、账号稽查稽核，并进行接口实时监控审计，确保数据调用安全；2022 年累计提供数据能力调用 6 千万次。同时，建设自助工具平台，并建立 OA 审批、DLP 加解密及溯源联动机制对内部提供批量数据分析需求，批量敏感数据限制特定云终端访问并限制向外传输，以此确保数据使用安全；目前已累计提供批量数据使用需求 17 万次。通过项目实施，确保了数据服务 100% 合规、安全。

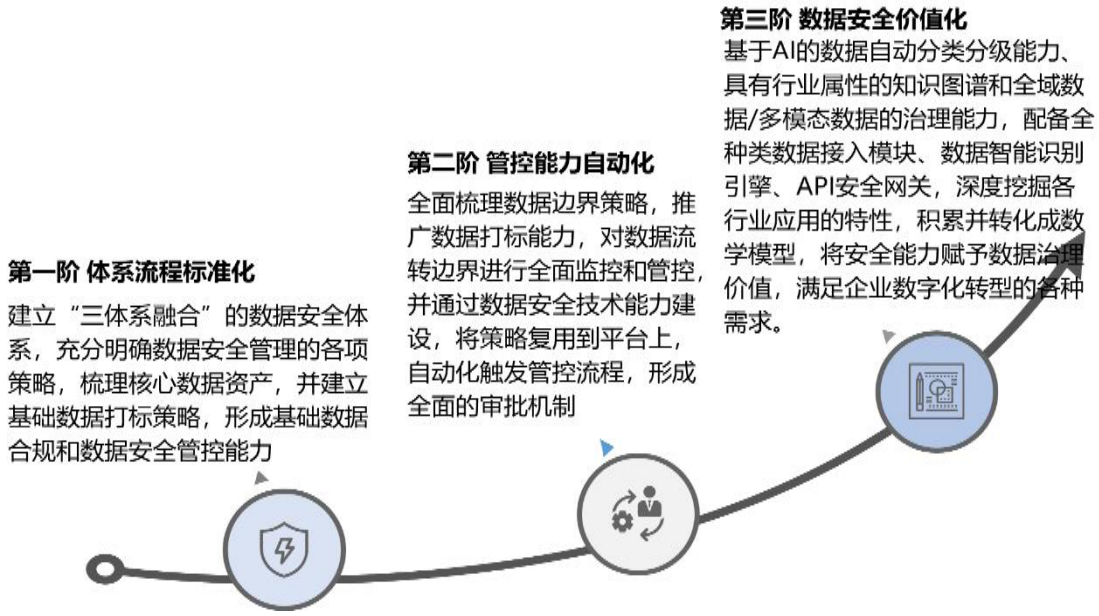
来源：广东联通

图 23 广东联通数据服务安全体系

（四）吉利汽车集团有限公司

1. 建设思路

吉利汽车对企业内部数据进行了全面划分，以经营数据、业务数据、个人数据、汽车数据等基础分类，对结构化数据、非结构化数据等进行了类型定义，制定以数据为中心的全生命周期的管控策略，企业数据安全治理的框架。以业务风险场景为导向，将吉利汽车的数据安全现状进行了细致梳理，从组织人员、制度流程、文化意识、安全管理活动、技术管控措施 5 个方面进行全局规划，制定了 “体系流程标准化、管控能力自动化、数据安全价值化”三步走的数据安全目标和实施路径，如图 24 所示。



来源：吉利汽车

图 24 吉利汽车集团数据安全三步走战略

2. 治理实践

近年来，各类数据安全风险逐步上升，吉利汽车数据安全治理方案以法律法规、行业标准规范为依据，通过“人、管、技”三个方面来推动完善，建立一个完善的组织机构，形成常态化的宣传、培训的模式，并辅以制度标准规范，引入适宜的工具、平台，并开展螺旋式上升的运营机制，从而构建“事前防范、事中监测、事后响应”全面的安全能力，如图 25 所示。

来源：吉利汽车

图 25 吉利汽车集团数据安全治理框架

在组织人员管理上，上层组织层面吉利在原有信息安全委员会下设了数据安全专业委员会，获得领导层的支持和资源保障，并专门成立了企业数据安全合规与产品数据安全合规团队，各业务单位配备专兼职的数据安全接口人，设置品牌安全负责人，来推动汽车的数据安全治理能力，并持续推广运营，保证各业务单位的形成良性的运转机制。

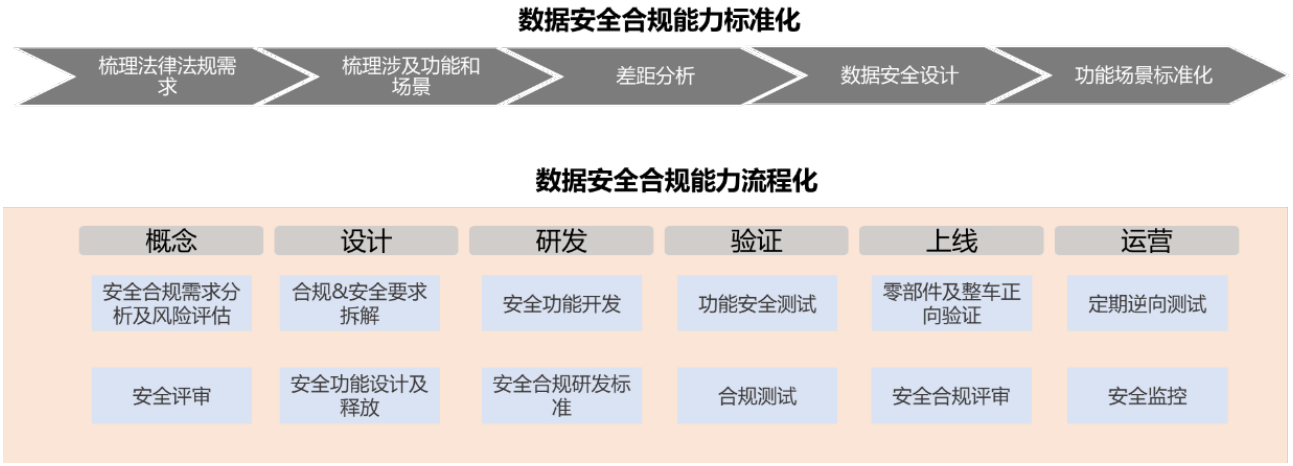
在流程制度建设上，吉利对 ISMS、DSMS、PSMS 三套体系进行充分融合、求同存异，制定了三套体系一套执行标准的“三体一式”管理机制，并通过制定数据安全管控基线，对基线进行持续优化改善，来适应不同安全环境，从而构建全面的安全体系管理策略。在体系章程、组织人员、事件管理等通用数据安全制度上充分沿用已有的信息安全管理制度，在数据分类分级、数据安全评估、数据共享使用、数据跨境合规等方面将要求进行细化，并结合技术能力建设，形成标准化的流程。针对汽车数据方面，在总体的制度框架下，结合《汽车数据安全管理若干规定（试行）》、《汽车数据处理安全要求》中要求，形成落地实践的细则或指引，如汽车数据分类分级指引、汽车数据分类分级目录、汽车数据安全设计指南等。

在技术能力落实上，从数据采集、数据传输、数据交换、数据处理、数据存储、数据销毁等数据全生命周期进行技术能力建设，结合业务场景风险和成本的考量，确

定在各业务形态下的技术能力需求。数据分类分级工具对数据字段进行识别打标，实现数据资产的识别，推动数据全面接入大数据平台，回收应用导出功能，实现数据流转通道的统一化，结合数据加密、数据脱敏工具实现数据安全合规的流转。

3. 实践亮点

软件定义汽车是大势所趋，汽车数据安全保护落地，需要通过安全开发能力嵌入，形成一整套 SDL（Security Development Lifecycle，软件安全开发周期）管理流程，来有效提高安全开发能力，抵御威胁，提高防范能力。吉利汽车集团依托数据安全治理体系，强化包括在概念规划、开发验证等活动中的数据安全开发嵌入能力，如图 26 所示。



来源：吉利汽车

图 26 吉利汽车集团 SDL 流程

概念规划阶段：全面梳理车辆的数据相关功能和场景，根据相关法律法规要求，对汽车的数据处理要求进行需求分析及风险评估，明确数据安全目标及其可行性。

设计阶段：对涉及到的数据相关功能和场景，进行数据安全合规及管理要求拆分，对安全功能进行设计并释放。

研发阶段：根据各数据场景和功能的设计要求，进行数据安全要求开发。

测试验证阶段：根据设计阶段的数据安全功能需求，进行安全功能测试及合规性测试，对数据安全需求设计过程的问题进行纠偏。整个测试过程应对各零部件测试和组装测试。

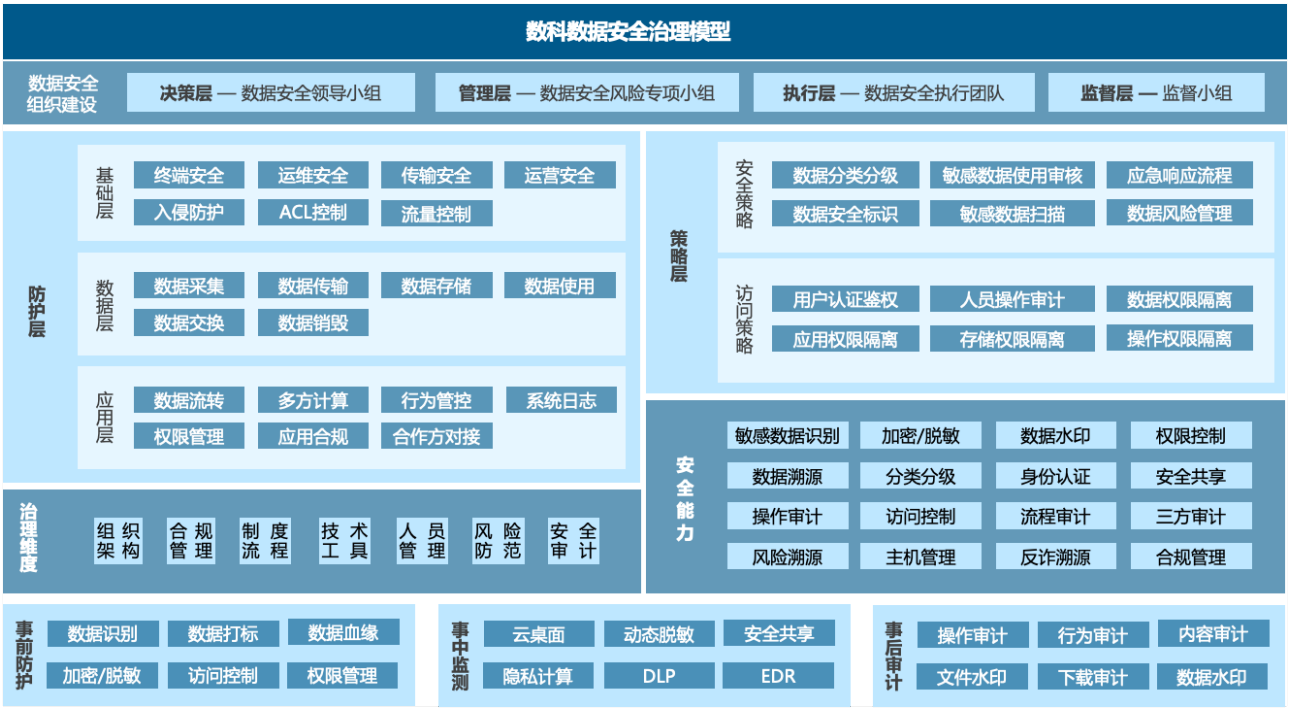
上线阶段：进行整车正向测试，确保各零部件和整车的数据安全要求，并整体进行安全合规评审，全部合格后进行上线。

运行阶段：应定期进行逆向测试和安全监控，及时发现其他安全风险，并及时修复；同时也可以从用户处收集反馈，协助改进数据安全需求。

（五）360 数科

1. 建设思路

360 数科结合数据安全治理能力 DSG 的总体框架要求，制定数据安全总体战略规划，巩固安全保障。并围绕数据全生命周期，从数据分类分级、数据合规管理、监控审计、风险分析、安全事件应急等多维度进行全面建设，将“事前防护，事中监测，事后审计”的核心原则贯穿数据安全治理全过程，形成如图 27 所示的数据安全治理模型。

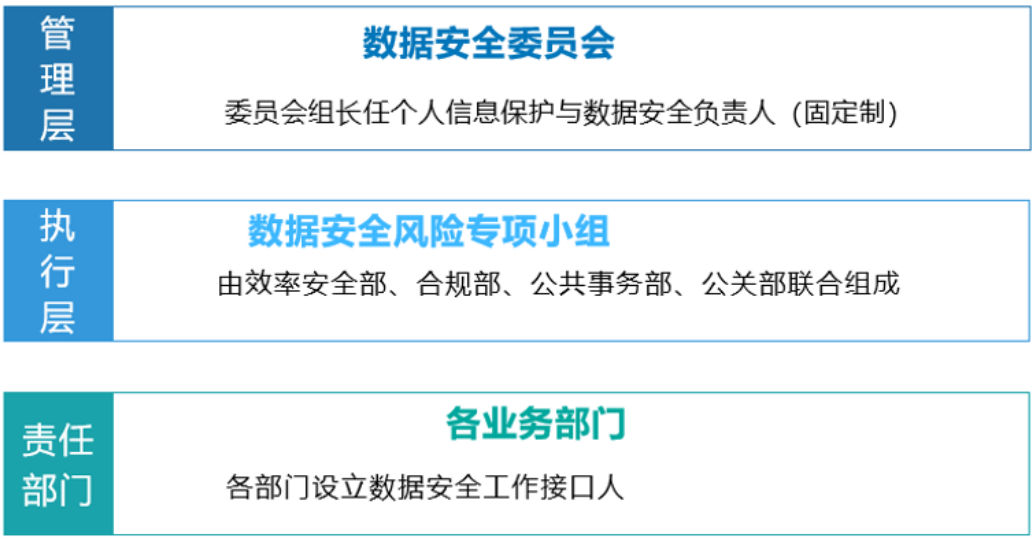


来源：360 数科

图 27 360 数科数据安全治理模型

2. 治理实践

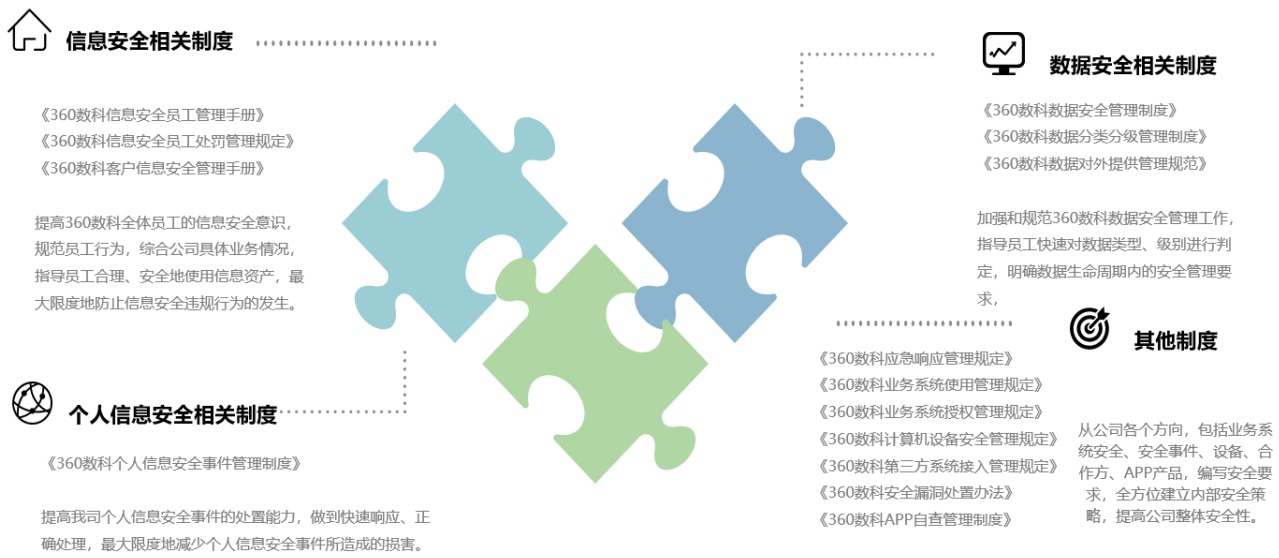
如图 28 所示，在数据安全组织架构建设方面，360 数科建立了数据安全管理机构，主要由管理层、执行层、相关责任部门组成。同时，内部也配有监督部门，主要风险中心、内审部门负责。



来源：360 数科

图 28 360 数科数据安全治理组织架构

如图 29 所示，在制度流程建设方面，360 数科建立了数据安全、信息安全、个人信息安全制度 30 余份，全面覆盖数据安全治理体系内容。主要包括《数据分类分级管理制度》、《360 数科个人信息保护与数据治理基本政策》、《360 数科信息安全员工管理手册》等等。

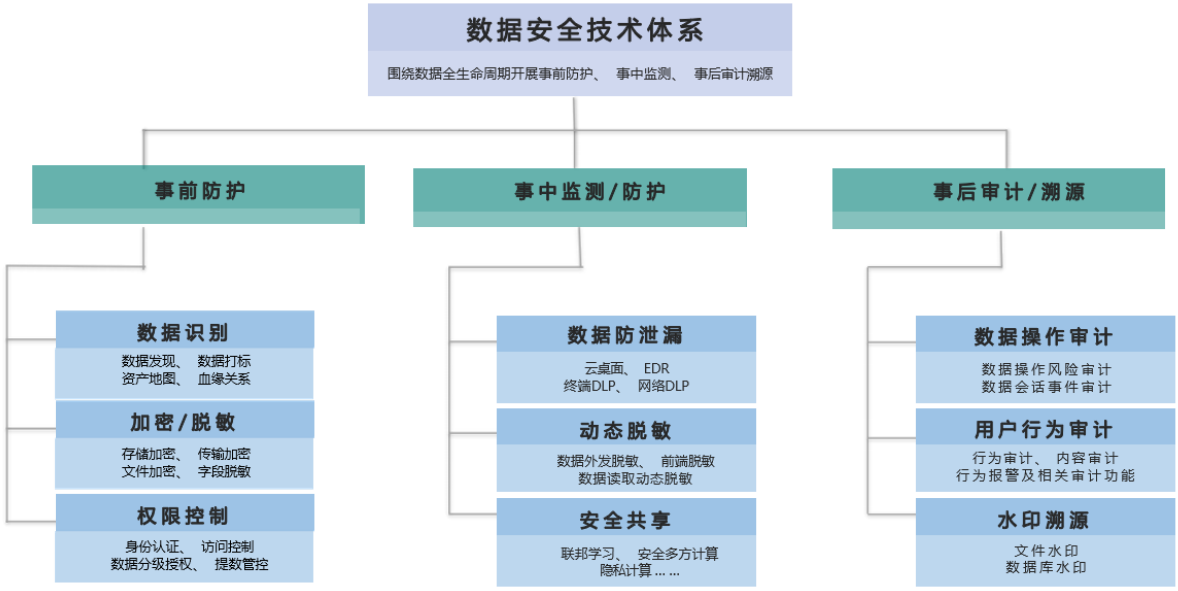


来源：360 数科

图 29 360 数科数据安全治理制度体系

在人员能力建设方面，360 数科全方位培养内部数据安全人员能力，各方向均设有专职安全人员管理，组织相关安全人员通过线上线下相结合的形式，参加中国信通院等权威机构开展的安全讲座、沙龙、会议等多种安全活动，提升安全人员专业水准。

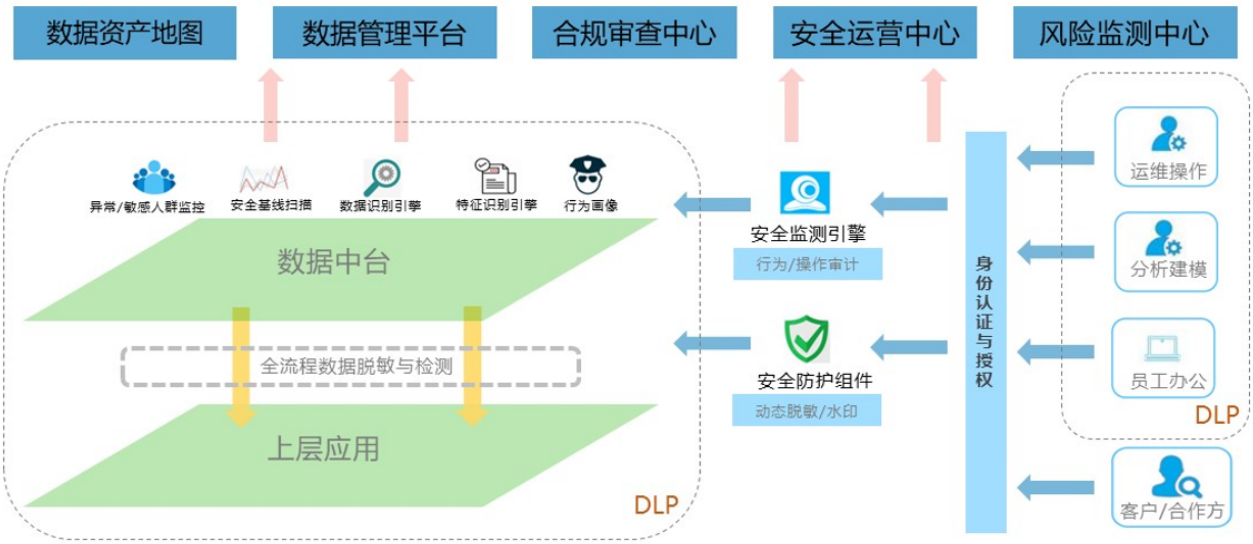
如图 30 所示，在技术防护体系建设方面，360 数科结合自身业务模式，在确保数据安全合规落地的前提下，以“事前防护、事中监测、事后审计”为核心原则，全面开展数据安全技术体系建设，并建成数据安全一体化防护解决方案。结合风险隐患排查、专项审计、安全评审等多种机制，持续优化完善数据安全技术手段，确保公司内部自动化决策、外部业务合作等一系列数据处理活动的合规落地有效性。



来源：360 数科

图 30 360 数科数据安全治理技术体系

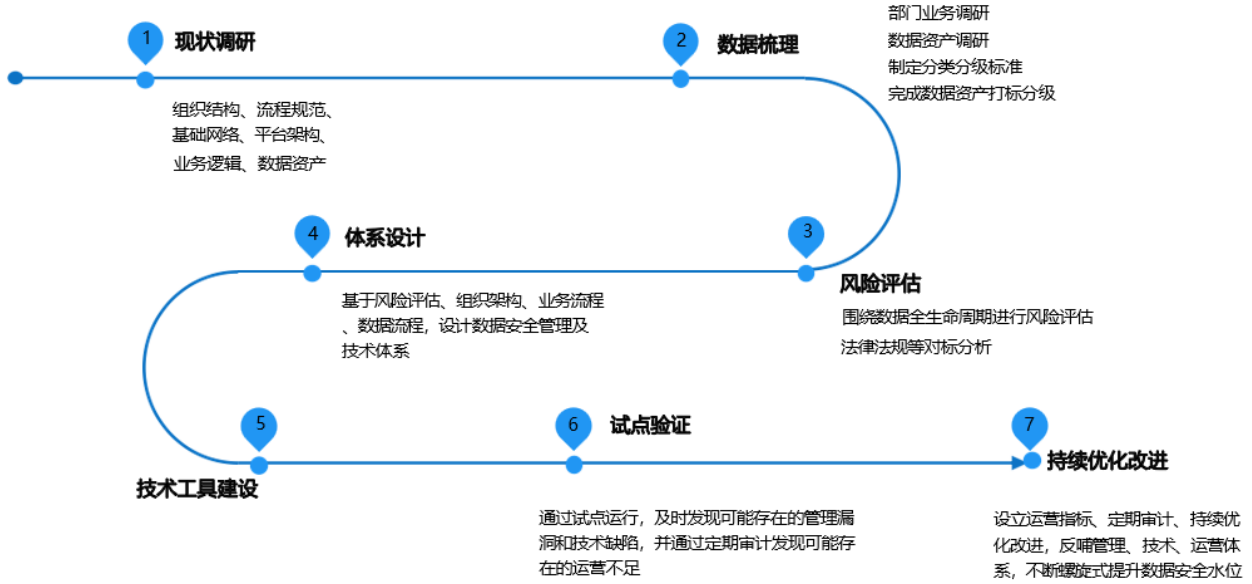
如图 31 所示，360 数科通过建设数据资产地图，梳理内部数据资产，严格把控数据权限，上线数据加密脱敏公用安全组件，构建统一的数据安全开发环境，落实数据安全管理要求，防范风险的发生；通过建设安全共享平台、合规自查平台、安全答题系统，提升全员数据安全意识的同时，实时感知潜在的安全合规风险，并借助数据防泄漏平台实时阻断违规数据流转；通过建设安全运营中心，借助监测预警、应急响应、用户行为审计、数据操作审计等手段及时捕获已发生的风险并跟进处置。最终，形成了独有的数据安全一体化防护解决方案。



来源：360 数科

图 31 360 数科数据安全一体化防护解决方案

如图 32 所示，360 数科基于互联网信贷业务，依据现状调研、数据梳理、风险评估、体系设计、技术工具建设、试点验证、持续优化改进的实践思路，将一整套数据安全治理方案，包含制度管理要求、安全技术手段、监督审计机制等运用至实际业务中，最大化解决公司、行业内相关数据安全问题。



来源：360 数科

图 32 360 数科数据安全治理实践路线

3. 实践亮点

亮点一：落地内部治理体系，设立数安风险专项小组。为全面搭建内部数据安全治理体系，360 数科内部专门成立了“数据安全风险专项工作小组”，更好地落实公司个人信息保护与数据安全治理体系建设，实现对个人信息及数据的全流程、全生命周期的保护。

亮点二：紧随新法新规，推出全覆盖式安全制度体系。公司内部对数据安全相关新法出台开展同步解读，并落实执行，编制内部相关制度文件，例如《360 数科数据安全管理制度》、《360 数科分类分级管理制度》、《360 数科个人信息保护与数据治理基本政策》、《360 数科用户个人信息权利响应规范》、《360 数科数据安全影响评估规范》等。通过全员宣贯讲解，提高全员数据安全意识，搭建全套数据安全制度体系。

亮点三：建设全面技术体系，强化业务安全保障。公司除了落实了以上体系化的建设外，还结合自身金融业务特点，在数据委托处理、数据共享的业务场景下，创新性的实现了安全共享平台，在业务数据脱离公司内部一系列安全防护前，为用户隐私数据再增一层防护屏障。该系统在安全技术上，可为业务系统再增一层防护屏障，用户数据在企业的平台，已经具备了基本的数据安全防护能力，如若需要进行下载或导出，均须经过该安全下载系统的全方面监测，含数字水印、隐私数据识别、动态脱敏、分级审核等多种安全策略，实现了用户信息的多重防护，为用户数据保驾护航！

数据安全推进计划
DATA SECURITY INITIATIVE

简介

数据安全推进计划（Data Security Initiatives，DSI）是2021年9月1日成立的公益性项目，主要围绕数据安全政策学习、数据安全标准建设、数据安全评估评测、数据安全咨询服务、数据安全人员培训等内容搭建交流平台，构建专业社群。致力于推动法律法规及监管要求的贯彻落实，促进数据安全技术交流，推广数据安全最佳实践，提升数据安全治理水平。

成立至今，DSI成员单位已达300余家，涵盖金融、汽车、互联网、电信、安全厂商等不同行业。并在专家智库、行业工作组、公开课等方面构建专业品牌，输出丰富研究成果。

联系人：姜铎

电　话：13521786562

邮　箱：jiangduo@caict.ac.cn

数据安全推进计划公众号