CAICT 中国信通院

数据安全治理实践指南（1.0）

中国信息通信研究院云计算与大数据研究所

2021 年 7 月

版权声明

编制说明

本指南的撰写得到了行业内许多专家的支持和帮助，他们分别来自：北京天融信网络安全技术有限公司、OPPO 广东移动通信有限公司、杭州美创科技有限公司、中国电信股份有限公司、联通数字科技有限公司、北京百度网讯科技有限公司、启明星辰信息技术集团股份有限公司、蚂蚁科技集团股份有限公司、天翼云科技有限公司、中国联合网络通信集团有限公司、杭州安恒信息技术股份有限公司、北京奇虎科技有限公司、奇安信科技集团股份有限公司、中国联通研究院、闪捷信息科技有限公司、恒安嘉新（北京）科技股份公司、京东数字科技集团、贝壳找房（北京）科技有限公司等。在此表示由衷的感谢。

前　言

2021 年 6 月《中华人民共和国数据安全法》（以下简称“《数据安全法》”）正式颁布，标志着我国数据安全进入有法可依、依法建设的新发展阶段。《数据安全法》明确提出在坚持总体国家安全观基础上，建立健全数据安全治理体系，提高数据安全保障能力。

由于数据本身具有流动性、多样性、可复制性等不同于传统生产要素的特性，数据安全风险在数字经济时代被不断放大，因此，对数据安全治理的要求也越来越高。如何协调政府、行业、企业、个人等多元主体，形成协同共治机制？如何平衡数据开发利用和数据安全保护，实现发展与安全的齐头并进？如何构建覆盖数据全生命周期安全的治理框架？如何在各组织中落实数据安全治理的具体要求？这些都是当前数据安全治理面临的重要问题。

本指南参考数据安全领域的相关标准，重点以中国互联网协会 T/ISC-0011-2021《数据安全治理能力评估方法》为基础，阐述了数据安全治理的内涵；从组织如何落实数据安全治理要求的角度出发，提出数据安全治理总体视图；按照数据安全治理目标、治理框架、治理实践路径分别提出落地建议，并对未来发展进行展望。此外，指南还收录了部分企业开展数据安全治理的实践经验。

目 录

图 目 录

表 目 录

一、数据安全治理概述

（一）数据安全治理概念内涵

随着数据作为生产要素的重要性凸显，数据安全的地位不断提升，尤其**随着《数据安全法》的正式颁布，数据安全在国家安全体系中的重要地位得到了进一步明确。**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。

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，中国互联网协会发布团体标准 T/ISC-0011-2021《数据安全治理能力评估方法》，为不断提升数据安全治理能力提供标准依据。本指南以上述标准为基础，梳理数据安全治理概念内涵，认为应该从广义和狭义两个角度进行理解。

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和促进发展的良好环境，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，建设与实施标准体系，研发并应用关键技术，培养专业人才等。

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，为确保数据处于有效保护和合法利用的状态，多个部门协作实施的一系列活动集合。包括建立组织数据安全治理团队，制定数据安全相关制度规范，构建数据安全技术体系，建设数据安全人才梯队等。它以保障数据安全、促进开发利用为原则，围绕数据全生命周期构建相应安

全体系，需要组织内部多利益相关方统一共识，协同工作，平衡数据安全与发展。

（二）数据安全治理要点阐释

无论是广义还是狭义的数据安全治理，都可以从以下三个要点进行阐释。

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，由于不同环节的特性不同，面临的数据安全威胁与风险也大相径庭。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

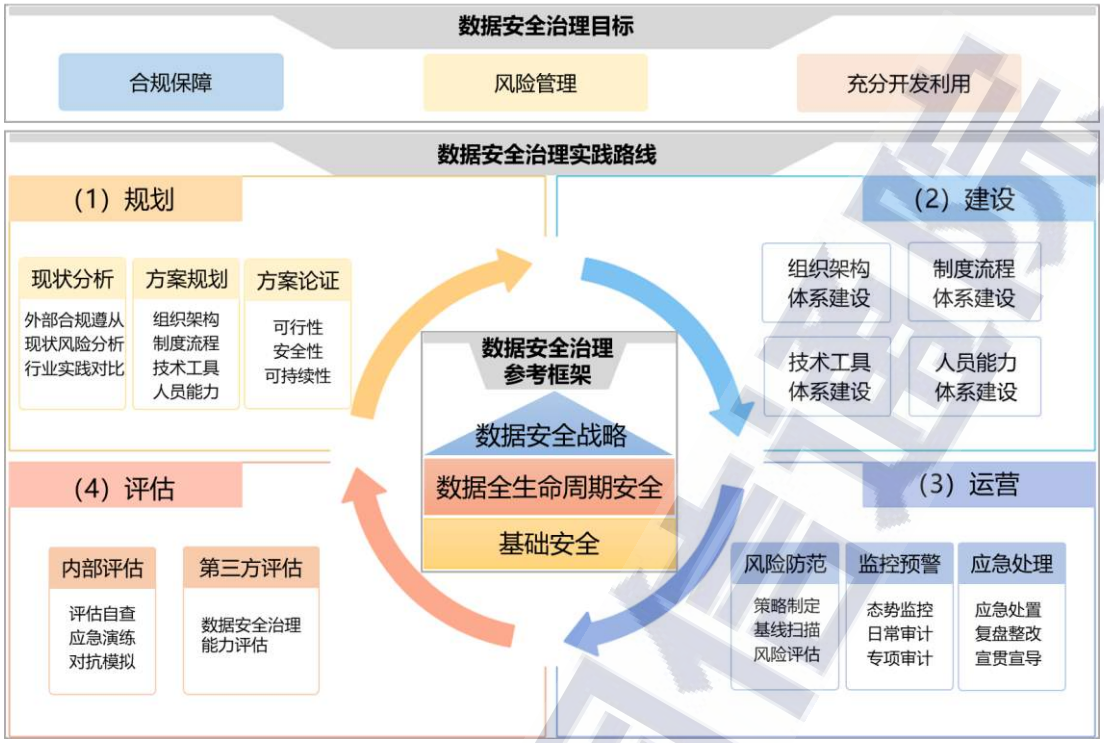
无论是从广义还是狭义的角度出发，数据安全治理不是仅仅依靠一方力量可以开展的工作。对国家和社会而言，面对数据安全领域的诸多挑战，政府、企业、行业组织、甚至个人都需要发挥各自优势，紧密配合，承担数据安全治理主体责任，共同营造适应数字经济时代要求的协同治理模式。这也与《数据安全法》中强调建立各方共同参与的工作机制相一致。对组织机构而言，数据安全治理需要从组织战略层面出发，协调管理层、执行层等各相关方，打通不同部门之间的沟通障碍，统一内部数据安全共识，实现数据安全防护建设一盘棋。因此，数据安全治理必然是涉及多元化主体共同参与的工作。

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，必须要辩证的看待数据安全治理。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，同时也要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

数据安全治理的概念一经提出，即受到全行业的广泛关注。作为推动组织数据安全合规建设、数据安全风险防范、数据业务健康发展的重要抓手，数据安全治理的内涵不再局限于技术层面或管理层面，而是围绕数据全生命周期安全，涉及组织内多部门协作、全流程制度制定、体系化技术实现、专业化人才培养等的一系列工作集合。基于本指南提出的狭义数据安全治理概念，本章将围绕组织数据安全治理参考框架，结合组织数据安全治理目标，给出组织数据安全治理实践路径，并提出如图 1 所示的数据安全治理总体视图。



来源：中国信息通信研究院

图 1 数据安全治理总体视图

数据安全治理目标：合规保障是组织数据安全治理的底线要求，风险管理是数据安全治理需要解决的重要问题。数字经济时代，数据的流通交易才能最大限度释放数据价值。因此，**数据安全治理的目标是在合规保障及风险管理的前提下，实现数据的开发利用，保障业务的持续健康发展，确保数据安全与业务发展的双向促进。**

数据安全治理参考框架：数据安全是数据安全治理的目标对象，参考框架是数据安全治理的参照对象。组织可以通过持续构建参照对象，实现对目标对象的有效管理。依据团体标准 T/ISC-0011-2021《数据安全治理能力评估方法》，本指南规定的参考框架包括数据安全战略、数据全生命周期安全、基础安全三部分主要内容。

数据安全治理实践路线：围绕上述数据安全治理参考框架，按照

治理规划、建设、运营、成效评估的实践路线，结合业务发展需要，从现状分析入手，结合组织架构、制度流程、技术工具、人员能力体系建设，构建相适应的数据安全治理能力，并针对风险防范、监控预警、应急处理等内容形成一套持续化运营机制，再根据成效评估进行改进，以保障整个实践过程的持续性建设。

三、数据安全治理参考框架

参考框架是组织数据安全治理所需的体系化结构，依据团体标准T/ISC-0011-2021《数据安全治理能力评估方法》，其包括数据安全战略、数据全生命周期安全、基础安全三部分，如图2所示。本章将对其具体内容进行详细介绍。

来源：中国信息通信研究院

图 2 数据安全治理参考框架

（一）数据安全战略

在组织启动数据安全治理工作前，必须制定相应的战略规划，明确治理目标和具体任务，匹配对应的资源，使得治理工作能够有条不

案的展开。数据安全战略可以从数据安全规划、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。

数据安全规划是指结合组织业务发展需要，对当前面临的数据安全风险现状进行梳理，并制定组织整体的发展规划。应从以下关键活动入手：

- 明确组织的数据安全决策团队及职责分工；
- 梳理组织面临的内外部数据安全风险；
- 根据业务发展制定年度及中长期发展规划，形成规划清单；
- 按照规划内容，落实各团队任务分工及考核；
- 建立任务分发及考核平台。

机构人员管理是指建立负责组织数据安全治理的团队及人员，并通过在人员入职、转岗、离职等环节设置安全控制措施，防范由人员本身带来的数据安全风险。应从以下关键活动入手：

- 明确组织负责数据安全管理、数据安全执行、数据安全监督等工作的团队及职责分工；
- 明确人员岗位及职责，按最小化原则开通各项权限；
- 与工作人员签订保密协议、数据安全责任协议等；
- 明确相应的数据安全追责机制；
- 制定并落实各项数据安全培训及考核计划；
- 针对岗位变动，落实人力资源部门与数据安全管理部门、IT部门、业务部门等在系统账号、访问权限等方面的联动机制；
- 建立人员统一管理平台。

（二）数据全生命周期安全

数据安全治理应围绕数据全生命周期展开，以采集、传输、存储、使用、共享、销毁各个环节为切入点，设置相应的管控点和管理流程，以便于在不同的业务场景中进行组合复用。数据全生命周期安全包括数据采集安全在内的九项内容，如图 2 所示。

数据采集安全是指为确保在组织系统中生成新数据，或者从外部收集数据过程的合法、合规及安全性，而采取的一系列措施。应从以下关键活动入手：

- 明确负责数据采集安全工作的团队及职责；
- 采集数据源的可信管理、身份鉴定、用户授权；
- 数据采集设备的管理，比如访问控制、安全加固等；
- 涉及个人信息和重要数据的业务场景，应在采集前进行合规性评估；
- 采集过程的日志记录及监控审计；
- 建立数据采集工具；
- 采集过程中，实现敏感数据识别及防泄漏。

数据传输安全是指为防止传输过程中的数据泄漏，而采取的一系列数据加密保护策略和安全防护措施。应从以下关键活动入手：

- 明确负责数据传输安全工作的团队及职责；
- 传输通道两端主体的身份鉴别；
- 在数据分类分级的基础上，根据业务场景，制定数据加密传输方案，以及传输通道加密方案；

- 梳理数据传输接口，形成接口管控清单；
- 开展接口调用日志记录及监控审计。

存储安全是指为确保存储介质上的数据安全性，而采取的一系列措施。应从以下关键活动入手：

- 明确负责存储安全工作的团队及职责；
- 在数据分类分级的基础上，结合业务场景，明确不同类别和级别数据的加密存储要求，包括对加密算法的要求和加密密钥的管理要求；
- 建立存储系统或平台，并实现对账号、权限、安全基线等的管理；
- 建立存储介质管理系统或平台，对购买、标记、审批、入库、出库等操作进行安全管理，保障存储介质本身的安全。

数据备份与恢复是指通过规范数据存储的冗余管理工作机制，保障数据的高可用性。应从以下关键活动入手：

- 明确负责数据备份与恢复工作的团队及职责；
- 制定数据备份与恢复的操作规程；
- 建立数据备份与恢复清单；
- 建立数据备份与恢复平台，按照上述清单定期执行备份，并对备份数据完整性和可用性进行验证。

使用安全是指为保障在组织内部对数据进行计算、分析、可视化等操作过程的安全性，而采取的一些列措施。应从以下关键活动入手：

- 明确负责使用安全工作的团队及职责；

- 基于数据分类分级情况，建立不同类别和级别的数据使用审批流程及安全评估机制；
- 部署数据脱敏工具，实现不同类别、不同级别的数据脱敏；
- 对各类数据处理活动进行日志记录和监控审计。

数据处理环境安全是指为确保组织的数据处理系统、终端、平台等环境的安全性，而采取的一系列措施。应从以下关键活动入手：

- 明确负责数据处理环境安全工作的团队及职责；
- 明确系统开发、上线、运维过程的安全控制措施；
- 对生产网、测试网等不同环境进行资源隔离；
- 对用户在数据处理环境上的各项加工操作进行日志记录和监控审计；
- 部署数据处理环境的数据防泄漏工具。

数据内部共享安全是指为确保组织内部之间的数据交互过程安全，而采取的一系列措施。应从以下关键活动入手：

- 明确负责数据内部共享安全工作的团队及职责；
- 对共享的数据内容进行评估、审批；
- 对共享过程进行日志记录及监控审计；
- 建立内部共享清单，明确共享链条；
- 建立数据共享工具或平台，并对其账号、权限等进行管控。
- 部署数据脱敏工具；
- 部署数据溯源工具。

数据外部共享安全是指为确保不同组织之间的数据交互过程安

全，而采取的一系列措施。应从以下关键活动入手：

- 明确负责数据外部共享安全工作的团队及职责；
- 针对数据脱敏、数据溯源、数据留存期限、监控审计、共享接收方的身份识别、共享平台或接口的访问控制等内容制定相应的安全管理策略；
- 明确共享双方的安全责任，尤其是接收方的安全责任。应在共享全过程中，对接收方的数据安全防护能力进行评估。

数据销毁安全是指通过对数据及其存储介质实施相应的操作手段，使得数据彻底消除且无法通过任何手段恢复。为确保销毁过程安全，应从以下关键活动入手：

- 明确负责数据销毁安全工作的团队及职责；
- 根据数据分类分级情况，结合业务场景需要，明确不同的销毁方法及销毁工具；
- 建立数据账期清单，确保过期数据按时销毁；
- 对数据销毁过程进行监督；
- 对数据销毁效果进行评估；
- 针对已外部共享的数据，明确销毁记录并验证。

（三）基础安全

基础安全能力作为数据全生命周期安全能力建设的基本支撑，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。基础安全能力包括数据分类分级在内的七项内容，如图 2 所示。

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。应从以下关键活动入手：

- 明确负责数据分类分级工作的团队及职责；
- 进行资产梳理；
- 结合数据特点和业务需求，明确数据分类分级原则、方法、安全管控措施；
- 定义数据识别规则；
- 建立分类分级工具，实现数据标识；
- 建立数据资产管理平台，实现数据的有效管理。

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。应从以下关键活动入手：

- 明确负责数据合规管理工作的团队及职责；
- 定期梳理国内外法律法规、行业监管等的合规要求，形成组织的合规清单；
- 针对合规要求落实情况，定期监控审计；
- 建立合规评审工具，定期开展合规评估评审。

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。可以从以下关键活动入手：

- 明确负责合作方管理工作的团队及职责；
- 合作前对合作方的数据安全防护能力进行评估；

- 签订数据保护协议，明确双方合作过程中的权责边界、责任划分，约束合作双方行为；
- 明确合作过程中，对合作方人员账号、权限等的管理要求；
- 业务合作结束后，督促合作方依照合同约定及时关闭数据接口、删除数据；
- 建立合作方统一管理平台，对合作方的引入、安全评估等工作进行管理。

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、数据泄漏等安全风险。可以从以下关键活动入手：

- 明确负责监控审计工作的团队及职责；
- 组织可根据自身业务流程特性、安全目标及风险控制水平，梳理形成高风险、高敏感操作清单，并设置监测点；
- 明确各场景日志记录要求、监控要求、审计要求；
- 建立统一的监控审计平台，对高风险、高敏感操作日志进行监控分析；
- 定期开展数据安全监控审计。

鉴别与访问，顾名思义，即用户身份鉴别与访问控制管理，是组织实现数据安全保障的关键环节，可以从以下关键活动入手：

- 明确负责账号管理、权限管理的团队及职责；
- 对用户的账号进行管理及鉴别；
- 对系统、平台、数据等的权限进行管理及访问控制；

- 建立账号及权限管理平台；
- 定期开展账号及权限的审计。

风险和需求分析是指根据组织面临的具体数据安全风险和安全需求，提出有针对性的防护对策和改进措施，将风险控制在可接受的水平，最大限度的保障数据安全。可以从以下关键活动入手：

- 明确负责风险和需求分析管理的团队及职责；
- 定期梳理组织面临的数据安全风险；
- 从合规遵从、面临风险等方面，梳理业务的数据安全需求；
- 定期开展需求分析、风险分析。

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。可以从以下关键活动入手：

- 明确负责数据安全事件应急的组织架构及职责；
- 定义数据安全事件的分类和分级；
- 明确数据安全事件应急处置和上报流程；
- 制定应急预案；
- 定期开展应该演练；
- 建立数据安全事件管理平台，对已发生的数据安全事件进行统一记录、管理、宣导。

四、数据安全治理实践路线

如前所述，数据安全治理是一项体系化工程，需要以数据为中心，结合业务场景和风险分析情况，构建可持续运转的闭环数据安全防护

体系，实现组织数据安全治理能力建设。本章从实践角度出发，围绕参考框架，探讨数据安全治理规划、建设、运营、成效评估等方面的工作路线。

（一）第一步：治理规划

1.现状分析

如前所述，数据安全治理的目标是在合规保障和风险管理的前提下，实现数据的充分开发利用，确保安全和发展的双向促进。因此，在规划初期就需要充分考虑组织现状，分析差距，从而得出针对性的需求点，作为组织数据安全治理规划设计的依据。**一是外部合规遵从，**对业务适用的外部法律法规、监管要求进行梳理，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。**二是现状风险分析，**结合业务场景，基于数据全生命周期安全防护要求，梳理并形成组织风险问题清单，明确内外部风险形成原因，提炼数据安全建设需求点。**三是行业最佳实践对比，**将组织数据安全能力现状与国内外或行业先进实践进行横向对比，明确差距所在，找到突出问题。

2.方案规划

根据现状分析结果，结合上述参考框架，应从以下方面着手规划适用于本组织的数据安全治理体系，防范数据泄露、数据篡改、数据非法使用等风险，保障数据安全。**一是组织机构建设，**通过成立专门的数据安全治理团队，自上而下的建立从各个领导层面至基层执行层面的管理组织架构，以保障数据安全管理方针、策略、制度的统一制

定和有效实施。**二是制度流程建设，**应在遵循现有相关国家要求的基础上，结合自身业务场景，明确需要编制的相关一级、二级、三级、四级管理和技术文件，指导数据安全制度体系的总体建设。**三是技术工具建设，**应结合业务场景，通过建立围绕数据全生命周期的安全防护技术体系，实现各项数据安全制度要求的自动化落实，为实现数据安全防护总体目标提供技术支撑。**四是人员能力建设，**人员是数据安全工作开展的主要参与方，应根据人员角色、岗位职责，从安全意识培养、安全能力培训、安全能力考核三方面入手构建相适应的人才培养机制。

3.方案论证

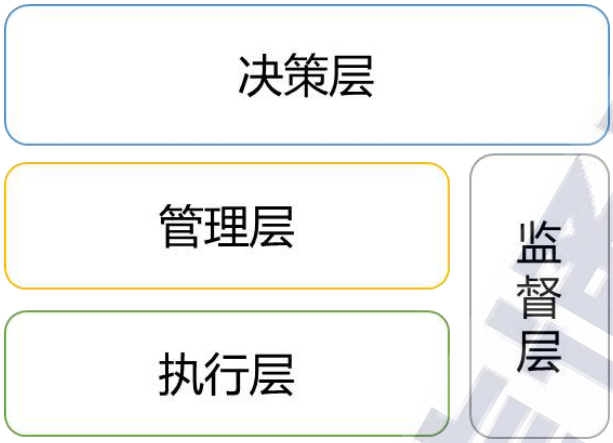
为保障规划方案在建设过程的顺利实施，应从以下方面进行论证分析。**一是可行性分析，**根据组织现状，明确人力、物力、资金的投入与产生的效益对比，确保在业务发展与安全保障之间达到平衡。**二是安全性分析，**通过对方案的各项实施内容进行安全性分析，确保方案的引入不会带来额外的安全风险。**三是可持续性分析，**数据安全治理是持续性过程，无法一蹴而就，随着业务拓展和技术进步，规划方案在保证与当前组织现有体系兼容的同时，也要考虑与后续的发展相适应。

(二)第二步：治理建设

1.组织架构体系

明晰的组织建设是保障数据安全治理工作顺利开展的首要条件。

一种典型的组织架构如图 3 所示。



来源：中国信息通信研究院

图 3 数据安全治理组织架构示意图

根据以上图 3 所示的典型数据安全组织架构，可以参考表 1 完善各组织层级职责及分工，确保数据安全责任层层落实。

表 1 数据安全组织架构角色及职责分工

组织层级	承担角色	角色描述	主要职责
决策层	数据安全领导小组	采取“一把手负责制”，由组织高层管理者、各业务部门及技术部门的直接领导共同组成。	（1）制定数据安全整体目标和发展规划； （2）发布数据安全管理制度及规范； （3）提供数据安全规划、设计、建设、实施、运营等全过程的资源保障； （4）负责重大数据安全事件协调与决策等。
管理层	数据安全管理团队	由数据安全领导小组指派中高层人员作为数据安全负责人，并组建数据安全管理团队。	（1）制定数据安全管理制度及规范； （2）制定数据安全工作在各层级的运行机制，保障数据安全工作的顺利运营； （3）推进数据安全意识培训、安全技能提升、安全技术考核等工作的开展； （4）负责与国家数据安全相关监管部门及行业组织的协调沟通； （5）负责数据安全的日常管理工作等。

执行层	数据安全执行团队	由各业务部门中与数据处理活动相关的人员，以及风控、技术、运营等团队的人员组成。	（1）负责数据安全制度及规范的具体执行； （2）负责数据安全事件的检测、处置、分析； （3）负责数据安全的风险评估； （4）负责反馈合理的数据安全需求，促进数据安全防护工作的改进； （5）积极参与数据安全意识培训、能力培养及考核工作等。
监督层	数据安全监督小组	由风控、审计、合规、等多部门组成的数据安全监督小组。	（1）对数据安全制度及规范的完整性及执行情况进行监督； （2）对数据安全技术工具的落地情况进行监督； （3）对数据安全风险评估过程进行监督审计等。

来源：中国信息通信研究院

决策层。为保证数据安全工作的顺利开展及持续保持，建议数据安全管理采取“一把手负责制”，由各业务、技术、法务等部门的直接领导共同组成“数据安全领导小组”，负责组织数据安全整体目标及发展规划等的制定。

管理层。由数据安全领导小组指派中高层管理人员作为数据安全负责人，并组建数据安全管理团队。为保证数据安全管理的独立性、客观性，建议数据安全负责人应为专职人员。管理团队应结合行业监管及组织业务发展需要，制定与组织整体目标相适应的数据安全管理策略，形成规范化管理体系等。

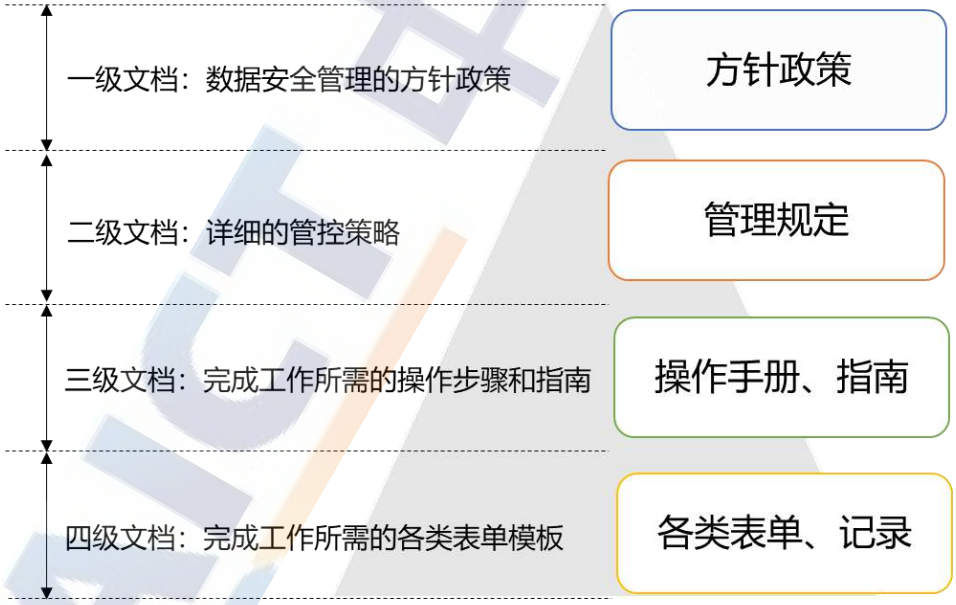
执行层。由各业务部门中与数据处理活动相关的人员，以及风控、技术、运营等团队的人员组成数据安全执行团队，需要与管理团队紧密配合。针对各数据安全场景，负责按照既定的数据安全管理策略、管理要求，在不同的业务流程中进行落地及运营维护。

监督层。由风控、合规、审计等多部门组成数据安全监督小组，负责对管理层、执行层的工作进行定期审核监督，并将发现的问题及时反馈给决策层，对违规行为予以纠正。

2.制度流程体系

数据安全相关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 4 所示。



来源：中国信息通信研究院

图 4 数据安全管理制度体系示意图

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。

根据以上图 4 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 5 完善组织各级制度文件内容。

来源：中国信息通信研究院

图 5 一套可参考的数据安全管理制度体系

为保证数据安全管理制度的落实，基于数据安全管理制度体系各级文件要求，应制定相应的执行流程规范及审核规范，保障数据安全管理的高效运行。图 6 是可参考的管控流程示意图，实际建设过程包括但不限于图中所示内容。

来源：中国信息通信研究院

图 6 数据安全管控流程参考示意图

3.技术工具体系

技术工具是落实各项安全管理要求的有效手段，也是支撑数据安全治理体系建设的能力底座。围绕参考框架，结合实际场景，构建完善的技术工具，可以体系化的解决数据全生命周期各阶段安全隐患。数据安全技术工具的部署可参考图 7 内容进行展开。

来源：中国信息通信研究院

图 7 数据安全技术工具部署示意图

根据以上图 7 所示的示意图，可以参考但不限于表 2 内容，完善各项技术工具以及产品平台的功能项，确保数据安全技术能力的具体落实。

表 2 技术工具对应功能描述

参考框架	技术工具/产品平台	功能诉求
数据安全战略	公文/制度管理平台	（1）公文审批、上传、下发、更新、废止； （2）制度审批、上传、下发、更新、废止等。
	人员管理/考核平台	（1）内部员工新增、转岗、离职管理； （2）实习/第三方人员新增、离职管理； （3）员工数据安全责任承诺书等管理； （4）员工数据安全违规管理； （5）员工绩效分发、考核记录等。
数据全生命周期安全	数据采集安全技术	（1）采集数据源身份鉴别； （2）敏感数据识别； （3）采集工具及防泄漏工具部署； （4）采集过程监控及日志记录； （5）采集合规性评估等。
	数据传输安全技术	（1）传输主体两端身份鉴别； （2）数据加密/脱敏算法管理及实现； （3）密钥管理； （4）传输通道加密管理； （5）传输接口管理、认证及监控等。
	存储安全技术	（1）存储加密算法管理及实现； （2）密钥管理； （3）存储系统部署及安全配置管理； （4）存储介质审批、购买、上架等的管理等。
	数据备份与恢复技术	（1）数据备份； （2）数据恢复； （3）备份数据可用性及完整性验证等。
	使用安全技术	（1）数据静态/动态脱敏算法管理及实现； （2）使用授权审批； （3）数据流转及人员操作监控及审计等。

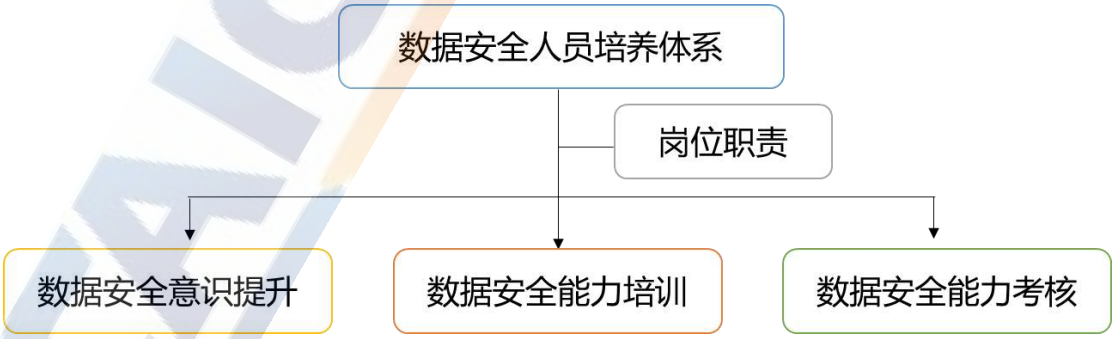
	数据处理环境安全技术	（1）测试环境、开发环境等的资源隔离； （2）数据处理系统等的身份鉴别及访问控制； （3）数据处理系统等的数据操作日志记录及监控审计； （4）部署数据防泄漏工具等。
	数据内部共享安全技术、数据外部共享安全技术	（1）共享双方身份鉴别； （2）数据脱敏算法管理及实现； （3）数据流转溯源实现，如数字水印； （4）共享审批及授权； （5）共享过程日志记录及监控审计； （6）数据共享平台建设等。
	数据销毁安全技术	（1）逻辑删除、硬盘格式化、文件粉碎等内容销毁； （2）消磁、捣碎、焚毁等介质销毁； （3）销毁结果验证等；
基础安全	数据分类分级技术	（1）敏感数据识别； （2）分类分级规则定义及管理； （3）分类分级结果打标等。
	数据资产管理平台	（1）数据资产的识别、录入、管理； （2）数据资产分类分级标识。
	工单审批管理平台	（1）覆盖数据全生命周期和业务场景的各类工单的申请、审批、流转跟踪等； （2）根据申请内容，与其他平台形成联动管理机制等。
	合规管理平台	（1）法律法规、行业监管规范、组织合规要求等的文件管理； （2）合规风险库管理； （3）覆盖数据全生命周期和各业务场景的合规评审计划、记录、报告、整改的管理等。
	合作方管理平台	（1）合作方录入、删除、更新等； （2）合作商机评审管理； （3）合作方安全评估计划、记录、报告等的管理。
	监控审计平台	（1）覆盖全部业务场景、系统、平台等的数据流动及人员操作监控及审计； （2）监控点及监控阈值管理； （3）风险告警策略的配置管理等。

	日志管理平台	（1）覆盖数据全生命周期和各业务场景的数据处理日志收集、记录等； （2）全部数据访问者的操作日志收集、记录； （3）日志监控与分析等。
	账号及权限管理平台	（1）账号申请、分配、回收等的管理； （2）权限申请、分配、变更、回收等的管理； （3）涉敏/超级账号的统一管理； （4）涉敏/超级账号权限的统一管理等。
	需求管理平台	（1）业务数据安全需求的申请、分析及安全方案管理等。
	风险管理平台	（1）覆盖数据全生命周期和各业务场景的数据安全风险的登记、评估、更新； （2）与以上风险相对应的防控措施记录及更新等。
	数据安全事件管理平台	（1）数据安全事件的登记、应急处置记录； （2）数据安全事件的宣贯宣导管理等。

来源：中国信息通信研究院

4.人员能力体系

数据安全治理离不开相应人员的具体执行，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，并建立适配的数据安全人员能力培养机制，如图 8 所示。



来源：中国信息通信研究院

图 8 数据安全人员能力培养体系

数据安全意识提升。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，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。

数据安全能力培训。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。

数据安全能力考核。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，实现人员培养的闭环建设。

（三）第三步：治理运营

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。在业务需求阶段开展数据安全风险评估，并将评估结果与安全基线进行对标检查。针对不满足基线要求的评估项，可以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，降低类似数据安全事件风险。

（四）第四步：治理成效评估

数据安全治理是一个持续性过程，成效评估是考核组织数据安全治理能力的重要环节，其结果也是新一轮数据安全治理的改进依据。如何评价数据安全治理成效，并实现治理体系的优化改进是组织在数据安全治理能力建设过程中面临的重要问题。

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，确保评估开展的有效执行，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。

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，帮助组织面对数据安全攻击时实现以攻促防，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，有针对性的完善数据安全治理技术能力。

2.第三方评估

除了内部评估外，组织应引入第三方评估。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。结合业务场景和数据全生命周期数据流，可以从组织架构、制度流程、技术工具、人员能力体系的建设情况入手，考察组织数据安全治理能力的持续运转及自我改进能力。

依托市场化机制，国外已经形成了较为完备的数据安全治理能力第三方评估评测体系，例如美国 TRUSTe 认证、欧盟 GDPR 相关认证等，在助力法律法规落地，提升组织数据安全治理水平，推动行业健康有序发展方面发挥了重要的作用。

目前，我国第三方数据安全治理能力评估处于起步阶段。2020 年 12 月，中国信息通信研究院依据团体标准 T/ISC-0011-2021《数据安全治理能力评估方法》**推出了国内首个数据安全治理能力评估服务，**为实践提供操作指南和度量准则。

《数据安全法》中也明确提出支持专业机构开展数据安全相关评估认证服务工作。

五、数据安全治理未来展望

数据应用场景和参与主体的日益多样化，使得数据安全的外延不断扩展。对国家而言，数据是国家基础性战略资源，加强数据安全治理已成为维护国家安全的战略需要，对组织而言，数据是重要的商业资源，加强数据安全治理已成为其重构竞争力的必要手段。未来数据安全治理将走向何方？有以下几点方向。

国家层面，《数据安全法》作为数据安全领域的上位法，将数据安全上升到了国家安全层面。作为纲领性法规，《数据安全法》明确了数据、数据权力、数据安全的范畴，厘清了数据安全防护主体责任，规范了国家行政主管部门、企业、个人的职责与权力。后续各部门、各行业、各领域将推进《数据安全法》配套制度、措施、规范和标准的构建，推动《数据安全法》的全面落地。

行业层面，通过持续跟进技术及行业应用研究，加速构建更加完善的数据安全治理标准体系；并依据相关标准，面向企业推出权威、专业的第三方咨询及评估评测服务，大力推广数据安全治理最佳实践，提升行业数据安全治理水平。同时，推动建立健全数据安全人才培养机制，储备人才资源。

企业层面，积极探索数据溯源、隐私计算等技术的发展动态，夯实数据安全治理能力底座，推动数据安全治理落地实践。同时，积极参与标准编写，贡献优秀实践，并结合第三方咨询与评估评测工作，完善企业内部数据安全治理体系建设。

考虑到数据安全治理在以上三个层面的发展，未来一段时间内，

数据安全治理将围绕以下两个核心展开。

一是促进数据安全治理实践的“行业化”和“场景化”。由于不同行业、不同场景面临的数据安全风险与潜在威胁不尽相同，因此需要有针对性的开展数据安全治理。行业、企业需着眼于此，大力推进数据安全治理的“行业化”和“场景化”。

二是探索数据安全治理从“离散”到“体系”的演进路线。数据安全问题由来已久，且愈演愈烈，“离散”的补丁式解决方法已不能完全适应企业当前的发展需要。如何整合有效资源，平衡数据保护与业务发展，推动“体系化”数据安全治理建设，是行业与企业需要考虑的问题。

“天不言而四时行，地不语而百物生。”数据安全治理的深入发展，正是立足国情、紧跟时代步伐、顺应历史规律的必然结果，我们相信，在以数据为核心生产要素的大前提下，数据安全治理将为数字化转型的国家战略方针保驾护航，对于全面建设社会主义现代化国家，起到核心推进作用。

六、附录：数据安全治理企业实践

（一）中国联通集团数据安全治理实践

1.数据安全治理建设思路及方案

按照《网络安全法》、《电信和互联网用户个人信息保护规定》等国家法律法规以及行业的数据安全要求，依据公司的“数据安全是生命线、安全事件零容忍、敏感数据不出门”的安全原则，结合多年数据安全管理、技术防护与运营的实际经验，从数据安全管理体系、数

据安全技术体系、数据安全运营体系三个方面构建了数据安全防护体系，涵盖数据采集、传输、存储、使用、交互等数据全生命周期，实现了职责清晰化、管理规范化、防护智能化、运营精细化，切实保障联通用户个人信息安全。

本方案以防止数据泄漏与数据滥用为目标，以零信任安全为理念，将自主研发的数据追踪溯源系统、数据安全网关系统等数据安全产品实际应用到具体的数据生产场景中，以解决数据安全问题，保障公司大数据业务的快速发展，保护用户个人隐私，维护社会稳定，保障国家安全。总体框架如图 9 所示。

来源：中国联通集团

图 9 中国联通数据安全体系总体框架

2.数据安全治理实践

（1）建立规范化数据安全管理体系

公司设立数据安全管理部门，并建立了横跨多个部门的大数据生产、服务、安全管控组织架构，将数据安全防护责任落实到每个部门、

每个业务、每个系统和每个员工。公司高度重视大数据安全人才的培养和培训，重视大数据产学研的结合，建立起一支具备数据安全评估、数据安全产品开发、数据安全咨询等专业安全能力的自有人才队伍。并深入研究国家关于网络安全、数据安全与个人隐私保护相关的法律法规和标准。结合公司的实际现状，建立了公司的安全制度体系，包括基础安全管理、业务安全管理和数据安全管理。在数据安全管理策略之下，构建数据安全技术体系，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）建设智能化数据安全技术体系

围绕数据全生命周期，通过开发建设数据安全技术产品与工具，形成了覆盖事前、事中、事后的数据安全技术能力。

一是建设数据资产地图，动态跟踪并管理数据资产信息。从安全角度自动化构建细粒度数据资产信息，对内部数据资产进行安全保护。并通过提供对数据资产体系化、结构化的管控视图，为数据资产的管理提供完整统一的视角。

二是建设数据脱敏系统，实现敏感数据使用安全。依据数据分类分级规范，从业务、安全、法规多角度对表字段进行安全分级，基于数据分类分级情况，对敏感的数据字段进行加密与脱敏。

三是建设统一账号认证授权审计系统，实现数据入口访问安全。对大数据平台及系统的所有服务器、数据库等 IT 资产进行集中管理，通过建设统一账号认证授权审计系统实现用户的统一认证、授权。

四是建设数据安全监测与审计系统，保障数据操作行为安全。基

于零信任模型，采用大数据技术，以用户操作行为为核心，采集、存储日志类数据。通过分析用户操作行为，结合行为基线，全程追踪审计各项操作行为，确保人员行为合规、数据操作行为可控、可审计、可追溯。

五是建设云桌面系统，实现数据操作安全。建设云桌面系统，所有人员对大数据平台系统的所有操作都必须登录云桌面后方可执行。在云桌面内，数据可读可操作，但无法下载在本地终端中，防止了数据泄漏，保障数据安全。

六是建设数据追踪溯源系统，保护数据分发与传播安全。基于数字水印技术，针对大数据特性，对大数据内容进行标识。一旦发生数据泄漏，能够通过该系统的追踪溯源技术追溯到泄漏者。

七是建设数据安全网关系统，确保数据输出内容安全合规。数据安全网关为公司对外数据输出的唯一出口，解决数据分发途径混乱，缺乏统一管理和安全控制等问题。

（3）实施精细化安全运营体系

一是系统安全运营。通过定期评估大数据平台系统的安全风险，并及时对系统加固，有效降低系统被黑客攻击的风险，保障平台系统的安全性。同时，公司建立数据安全事件应急响应体系，建立应急组织机构，明确应急人员及职责，编制系统应急预案，开展系统应急演练，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。

二是数据运营管控。在数据业务中通过数据评估、模型算法评估、

代码评估、接口上线安全评估和数据出口审核等措施进行数据运营管控。在数据合作前，评估合作的数据内容、数据范围，数据使用场景是否合规，要求的数据合作方式是否安全。在数据合作中，严格对合作方数据模型的代码、算法、输入数据、输出数据进行审核，确保数据模型合作的合法合规、安全可信。严格对数据接口进行安全管控，所有接口均通过账号口令鉴权，接口上线前均经过安全检测，接口调用过程要进行日志记录。严格对数据系统进行质量审核，杜绝安全漏洞、控制逻辑错误、配置错误等问题。

三是业务运营管控。在业务运营中严格落实事前、事中、事后全闭环审核，管控数据合规风险。业务安全事前审核的内容包括服务对象的数据内容、数据用户和使用范围是否明确、要求的数据提供方式是否安全。业务安全事中审核主要进行合同审核，审核合作伙伴的资质，在与对外合作方签订的合作协议中，规定数据使用范围、用途、期限和违约责任，要求合作方提供技术手段对数据安全进行保护等。业务安全事后审核主要对合同执行过程进行审核和审计，包括话术审核、系统行为的监控和审计等。

3.数据安全治理效果

公司数据安全体系自开始运营以来，通过管理策略和技术措施的深入融合，监测和审计大量数据安全风险操作，发现和整改多个高风险漏洞，保障大数据平台超过 100P 的数据存储以及每天新增超过 200T 压缩数据量的安全，多次预防和阻止数据合作方违规使用数据，避免了数据的滥用和泄露，为公司业务保驾护航。同时，公司在公安

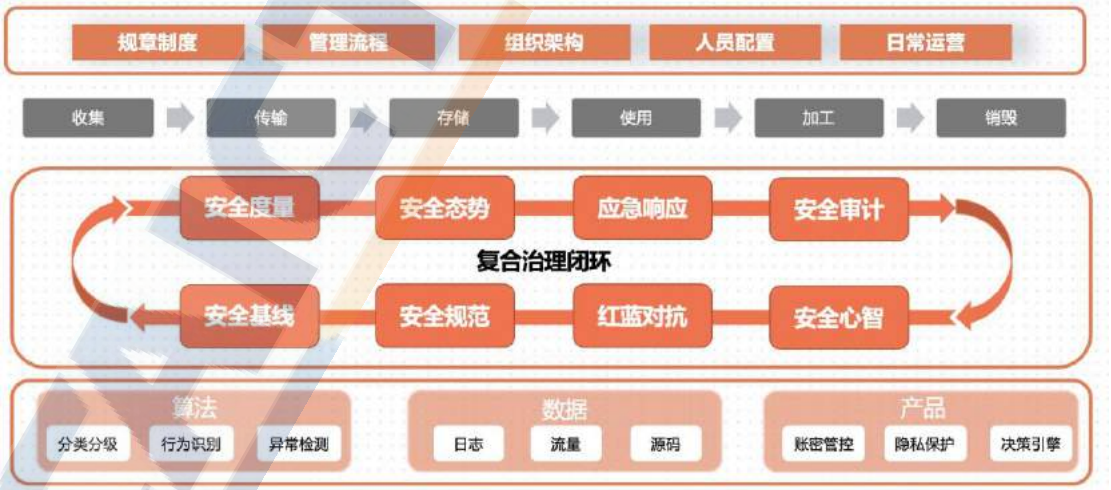
部、工信部、网信办历次的安全检查以及护网行动中均未发现重大安全问题，安全防护效果良好。

目前，该方案已在浙江省大数据发展管理局、广东省政务服务数据管理局等多个政府部门落地实施，运行效果良好，降低了政务信息共享交换环节数据泄露、数据篡改、数据滥用等问题的风险，实现实时掌握数据库动态，有效预防和避免安全事件的发生和扩散，为数据资源开放共享保驾护航。

（二）蚂蚁集团数据安全治理实践

1.数据安全治理建设思路

蚂蚁集团在过去几年的数据安全实践中，持续加大对数据、算法、产品的建设力度，不断强化流程规范的制定和实际落地，同时大幅提升数据安全基线、度量、审计、心智等重要环节工作，总结出一套行之有效、覆盖数据处理全生命周期的数据安全复合治理管理模式。蚂蚁数据安全复合治理管理模式如图 10 所示。



来源：蚂蚁集团

图 10 蚂蚁数据安全复合治理管理模式

数据安全复合治理管理模式主要包含以下几方面的内容：

一是基于合规要求、安全战略、安全需求、安全形势等进行系统分析梳理、提炼要求，从合规管理、资产管理、人员管理、数据处理生命周期管理、流程管理、教育培训管理等多个维度出发，制定清晰明确、具有较强指导性的安全规范。同时，对安全规范的落地实施效果进行监督与评价，根据结果反馈，对规章制度、流程规范、管理与技术措施等进行针对性的更新与优化。

二是从安全规范出发，将安全规范的具体要求提炼成可规则化表达的数据安全基线，使用指标化的方式对基线要求进行清晰明确的阐述，确保基线易于理解，具有很强的落地性。同时，通过对安全基线进行分析、评审、度量，保证安全基线的持续优化更新，确保安全基线与安全规范的要求始终保持一致。

三是安全规范和安全基线的实施效果可以通过自动化方式进行度量和感知。安全度量和感知体系的设计基于合规要求、安全规范、安全基线等，可以针对人员、数据资产、业务应用等进行实时立体地度量、刻画和感知。同时，针对不同对象制定了差异化的度量感知策略和机制，通过结果的清晰刻画，更好地辅助安全决策，持续提升安全防护能力与意识。

四是强化安全审计与应急响应。根据安全基线、安全度量、安全态势等的反馈，围绕数据处理生命周期，加大对各类违规行为的事前、事中、事后审计和处罚力度。此外，强化应急响应工作，制定完善的事前、事中、事后响应处置机制，形成事件发现、止血、恢复、溯源

的闭环机制。

五是加大数据安全工作的日常培训宣导，强化安全心智建设。通过法规政策和制度体系的解读宣传、应知应会的教育考核、流程规范的引导说明等全流程建设，将被动的知识灌输转变为安全意识和能力的主动提升，帮助员工形成良好的安全心智。

六是加强数据安全红蓝攻防，开展以数据为主体、以风险为依据的贯穿整个数据生命周期的对抗，提升未知风险发现能力，不断提升数据安全认知水平。

最后，强化闭环治理和治理成效持续提升。数据安全复合治理管理模式各环节形成有效了的治理闭环，环节间相辅相成、互相促进。在运营过程中，可以根据安全形势、安全战略、安全需求等进行持续优化，不断提升数据安全治理的适用性与成效。

2.数据安全治理实践

（1）APP 个人信息保护

在数据安全治理实践中，仅仅强化安全规范、心智等还不足以保障风险可控，还需要一系列的能力从技术层面防范相关风险。APP 是直面用户的窗口和数据入口，蚂蚁集团内部高度重视 APP 个人信息保护，在 APP 个人信息保护实践中，搭建了涵盖事前、事中、事后的四重保障体系。

首先内部制定了严格的 APP 个人信息保护安全管理制度和开发规范，并设置了严格的管控流程确保落地实施。

在 APP 需求阶段，需求方案必须开展隐私保护和数据安全专项

评估，评估通过后才能开展研发。APP 上线前，需要经过静态代码检测、动态沙箱及真机模拟检测，确保各场景的数据采集合法、正当、必要。APP 上线后，通过覆盖全场景的安全切面技术对 APP 进行保护，及时发现针对 APP 的异常攻击行为，并进行细粒度的动态安全管控。蚂蚁集团数据安全四重保障如图 11 所示。

来源：蚂蚁集团

图 11 蚂蚁集团数据安全四重保障图

（2）账密治理

除了 APP 个人信息保护广受关注外，数据安全保障的另一个重要场景是账密管理。当前，账密口令凭证及应用身份的管理已成为数据安全保障的重要基础，账密风险已成为整个行业面临的共同挑战。

在账密治理方面，账密的明文泄露、共用账密、弱密码、硬编码等各类风险是要、关注的重点。面对这些挑战，蚂蚁集团建立了专门的账密管控安全规范，并在产品设计、研发流程中进行强卡点，确保规范的有效落地和执行。同时，依托于自动化、智能化的扫描检测、

访问控制、安全存储等核心保障能力，持续强化账密治理能力。此外，通过对算法模型深入优化、建设账密保管产品能力、搭建自动化定期无损轮换管控能力等，可以进一步提升账密治理工作的准确率和覆盖率，更好地降低账密安全相关的风险敞口。

（三）百度数据安全治理实践

1.数据安全治理体系建设实践及创新

（1）治理路线实践与创新

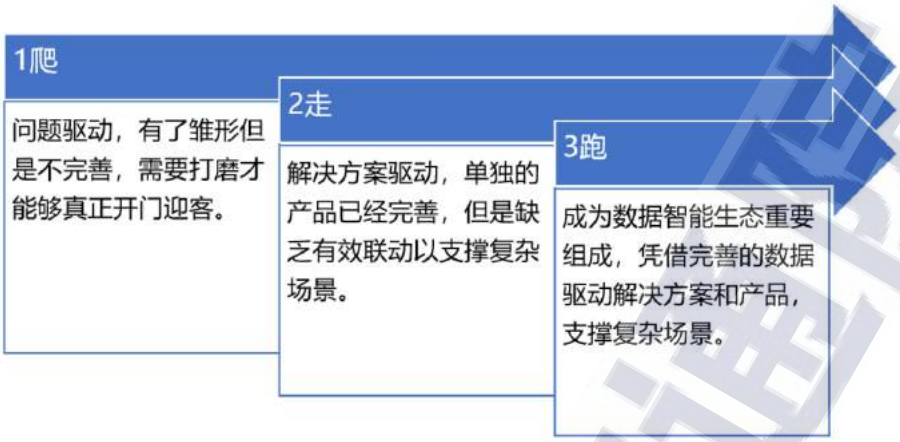
在数据安全合规性评估实践过程中，百度总结了自身特点，归纳成功治理的先决条件，并制定了清晰的工作路线，如图 12 所示。

来源：百度

图 12 百度数据安全治理工作路线

（2）数据安全保障工具与能力建设实践及创新

为支撑数据安全的治理目标、建设目标、防护目标顺利实现，百度定义了数据安全技术能力三步走的产品建设路径，从工具化向产品化过渡，实现管理能力提升，完成产品化后，通过**产品的整合形成成熟的安全方案，向平台化转型，实现数据安全治理效能提升**。三步走策略如图 13 所示。



来源：百度

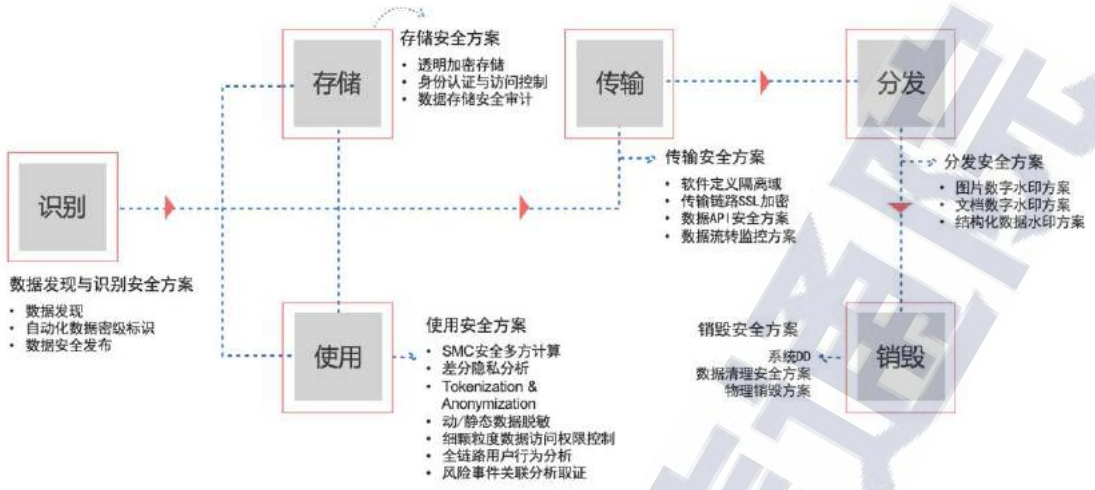
图 13 百度数据安全治理三步走

（3）数据安全风险运营实践与创新

采取降维打击思路，针对数据跨越安全信任边界的行为及关键节点布控，实行风险闭环运营。

2.数据安全合规性评估与场景化解决方案建设实践

百度在 AI 创新过程中，对于数据安全、隐私保护等问题有着切身的体会和深入的理解。百度业务与数据紧密结合，基础数据的标识、模型算法的优化都离不开数据的共享、应用、流通场景。百度现有的大规模数据需要一套高效、便捷的解决方案以完成数据安全合规评估与安全保障工作，为此百度基于现有的数据安全策略及相关规范要求，集成多维安全检测和防护能力，建立了覆盖数据全生命周期的数据安全与隐私保护解决方案，可实现“事前主动识别，事中灵活控制，事后全维追踪”的目标。百度数据安全治理实践路线如图 14 所示。



来源：百度

图 14 百度数据安全治理实践

数据作为 AI 时代重要的生产要素，数据的存在形式、使用方式、流转共享模式都产生了巨大变化，数据价值与数据使用场景及形式紧耦合，数据只有流动和使用才能产生价值，同时也必然产生风险。

因此，数据安全保护的理念也需要从传统信息安全的静态防护，向动态的风险防护转化。需要确保数据流经之地必须具有同等的风险抵御能力，这需要健全完善覆盖数据生命周期的数据安全技术保障手段。此外，数据安全是量体裁衣的过程，须从数据出发，以威胁入手，围绕数据流进行动态评估，并制定有针对性的场景化方案。

（1）典型场景一：高价值数据资产安全评估与保障

人工智能已经成为新一轮科技革命和产业变革的核心驱动力量，而人工智能技术的高速发展，依托于算法、算力和数据的快速发展。AI 数据作为其中的基础要素，具有数据价值高、数据规模小、时效长、低频更新的特点。因此区别于传统数据安全评估及保障，需要对

高价值属性数据进行更加集中严格的管控，使用数据安全域、信任边界异常检测、泄露检测、数据水印等数据安全能力，实现在正常数据分析及模型训练高效开展的情况下，对敏感数据操作及使用行为进行规范及监控；

（2）典型场景二：敏感数据安全评估与保障

在隐私数据的合规性评估与保障中，百度将前沿的联邦学习、联邦计算平台在实际应用中部署，高效融合多方安全计算、可信执行环境、差分隐私和数据脱敏等多种领先数据安全和隐私保护技术，在各方数据不出域的基础上进行联合计算，获取各方所需的计算结果，全力打造跨组织数据合作“可用不可见，相逢不相识”的安全服务，在保障用户权益的前提下，提供了安全合规的高效数据合作模式。

（3）典型场景三：私有化部署下数据安全评估与保障

私有化部署是人工智能服务交付的重要形式之一。针对私有化部署产品的安全合规性评估，均需要在方案设计和实施阶段，从数据角度考虑基础环境、操作系统、硬件加密环境、应用层、运维等方面的安全要素。

为了在非可控环境的私有化部署项目中，有效保护核心文件、模型、代码等敏感数据，百度在各类不同交付场景的安全评估及建设中，逐步积累了一套有针对性的防护方案，实现灵活的鉴权安全、应用安全防护及 AI 模型安全防护能力，从而解决私有化部署项目中常见的安全风险，如无鉴权或鉴权失效、核心代码和算法被逆向分析和破解等，以助力业务合规、安全交付私有化项目。

百度将牢记初衷，把安全合规、伦理以及广泛的社会关怀，融入到公司的血液当中。伴随社会经济与科技产业的进一步融合，持续用科技创新回应社会需求的社会价值创造，为 AI 新基建发展注入新动能，加速中国产业智能化升级步伐。

（四）天翼云数据安全治理实践

1.数据安全治理建设思路

天翼云对数据安全的重视由来已久，早在 2014 年，天翼云便提出了数据全生命周期安全防护体系方案，并在实践中不断探索落实。建设初期，面临数据资产不清晰、数据分类分级难、管理体系不健全、技术工具不完善等诸多问题和困难，经过多年探索实践，逐一攻克，已实现可管可控可信化的数据安全运营体系。回顾建设路标，从明确数据安全治理目标、建立健全管理制度、探索完善技术工具到建立常态运营指标，形成了一套完整的数据安全保障体系。数据安全治理实践路标如图 15 所示。

来源：天翼云

图 15 天翼云数据安全治理实践路标图

天翼云数据安全治理的总体思路，是以“管理 + 技术 + 运营”为闭环运转，螺旋式不断推进提升。以国家法律法规、行业标准为主线，结合业务场景和领域经验，构建完备的管理体系；以自研技术工具为依托，落实各项管控要求，实现全方位监控审计；建立统一运营指标，落实常态化运营工作，真正做到数据安全解决方案可落地与可实施。

2.数据安全治理实践

天翼云参与中国互联网协会《数据安全治理能力评估方法》团体标准的制定工作，并作为首批参评企业获得了数据安全治理能力优秀级证书。该标准以数据全生命周期的安全治理能力建设为切入点，定义了 18 个能力项，以评估企业在数据安全战略、数据全生命周期安全和基础安全方面的治理能力。

天翼云也是数据安全技术实践的先行者。经过不断实践探索，天翼云率先研发出国内首款大数据环境下的数据脱敏系统，支撑日均 300T 规模数据加密和脱敏，总保障数据 PB 级；自主研发的出口审计系统，可基于内容和行为进行检测，达到实时监控千量级规模接口审计，及时发现出口数据的泄露风险；用户操作管控方面，通过关联分析 10+类日志全面监控用户操作数据行为，形成了数据安全事前加密脱敏、事中监控检测、事后审计追踪的保障机制。此外，天翼云也率先研发、部署敏感数据发现能力，实现敏感数据扫描、自动分类分级、敏感数据地图，打造数据全息可视化。天翼云数据安全治理能力如图 16 所示。

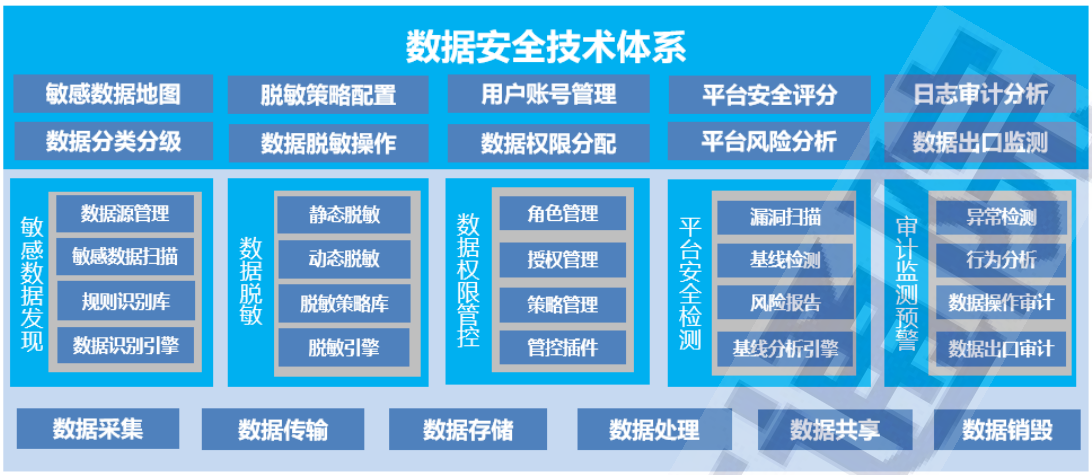
来源：天翼云

图 16 天翼云数据安全治理能力

3.数据安全治理场景化解决方案

天翼云以多款自主研发的数据安全产品为支撑，保障数据全生命周期安全，形成统一的数据安全管控平台，可满足不同场景下数据安全治理的各类需求。

天翼云数据安全产品之一的数据安全平台采用先进的机器学习、自然语言处理技术，围绕数据全生命周期构建一套从数据采集、数据访问、数据使用、数据传输、数据共享、数据销毁的全生命周期大数据安全技术体系，具备敏感数据识别、数据脱敏、权限管控、智能异常检测、审计监测预警等数据安全能力，实现对企业核心数据的保护和管理。天翼云数据安全技术体系如图 17 所示。



来源：天翼云

图 17 天翼云数据安全技术体系

在不同场景下，基于不同用户身份的数据访问请求，数据安全平台基于角色或策略进行 HDFS、Hive、Hbase、Yarn、Strom、Kafka 的访问控制，并根据细颗粒度授权实现数据访问的权限管控。同时，平台从接口日志、输出文件拉取数据到审计服务引擎，引擎依据审计管理平台配置的检测规则和审计策略，对日志、文件进行审计，有效监测数据出口并且防止数据泄露。数据安全平台具备用户操作审计功能，以数据操作行为为核心，根据业务模式、场景、对象的不同，利用智能分析引擎、用户行为分析等手段，分析用户访问敏感数据的情况，及时发现数据访问的异常行为，保障业务运营全流程可追溯、可审计。

目前，天翼云已在智慧政务、智慧城市、智慧工业等不同领域推出满足不同业务类型的专属解决方案，数据安全治理能力也融入到天翼云诸葛 AI 平台，在为企业提供一站式 AI 解决方案的同时，捍卫企业用户隐私，为企业数字化转型夯实安全基石、为合规经营保驾护航。

参考文献

[1] T/ISC-0011-2021 《数据安全治理能力评估方法》.

[2] 郑云文.《数据安全架构设计与实战》. 机械工业出版社.

[3] 数据资产实践管理白皮书（4.0 版）. 中国信息通信研究院云计算与大数据研究所 CCSA TC601 大数据技术标准推进委员会.

[4] 全球数字治理白皮书. 中国信息通信研究院.

[5] 数据价值化与数据要素市场发展报告. 中国信息通信研究院政策与经济研究所.

中国信息通信研究院 云计算与大数据研究所

地址：北京市海淀区花园北路 52 号

邮编：100191

电话：13581661287

传真：010-62304980

网址：www.caict.ac.cn