数据安全推进计划
DATA SECURITY INITIATIVE

数据安全治理实践指南

（3.0）

数据安全推进计划

2023年12月

版 权 声 明

前　言

数据作为数字经济发展的核心资源，是驱动社会创新、经济高质量发展的源动能。近期，随着国家数据局的成立、财政部《企业数据资源相关会计处理暂行规定》等的发布，数据获得各方空前关注。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，探讨数据安全建设路线，解决数据安全实践难点问题，中国信息通信研究院数据安全推进计划发布《数据安全治理实践指南》（以下简称《指南》）系列，围绕数据安全治理目标、治理框架、治理实践路径展开论述。

相较于《指南（1.0）》《指南（2.0）》，本指南主要对数据安全治理总体视图及相关内容进行更新，主要体现在：

（1）针对数据安全治理体系，丰富了基于数据全生命周期视角、基于工作内容分工视角的体系解读，贴近组织实际工作。

（2）针对数据安全运营，丰富了从运营对象、管控流程两个角度的建设内容，为组织提供更多的选择。

（3）增加数据安全专项工作开展思路，围绕数据分类分级、数据安全风险评估及治理、个人信息保护、数据出境安全评估、合作方数据安全管理等重点话题，阐述工作思路与方法。

（4）删除数据安全治理实践案例的附录，各组织的优秀实践案例将另行汇聚出版。

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，分析数据安全治理原则。

（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）数据安全治理原则

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

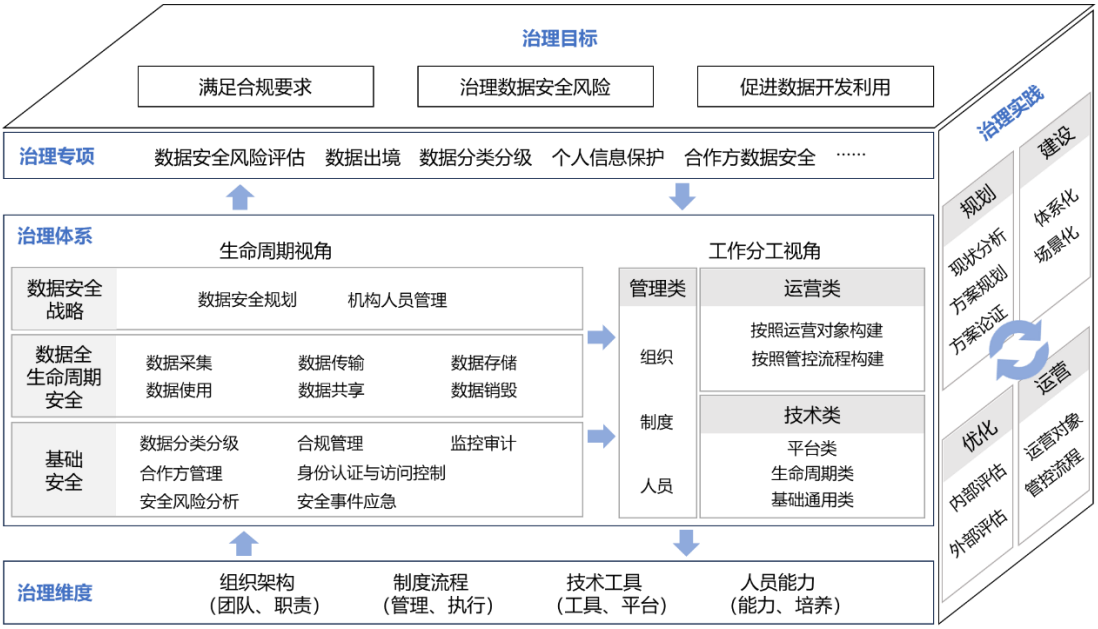
无论是从广义还是狭义的角度出发，数据安全治理不是仅仅依靠一方力量可以开展的工作。对国家和社会而言，面对数据安全领域的诸多挑战，政府、企业、行业组织、甚至个人都需要发挥各自优势，紧密配合，承担数据安全治理主体责任，共同营造适应数字经济时代要求的协同治理模式。这也与《中华人民共和国数据安全法》（以下简称《数据安全法》）中强调建立各方共同参与的工作机制相一致。对组织机构而言，数据安全治理需要从组织战略层面出发，协调管理层、执行层等相关方，打通不同部门之间的沟通障碍，统一内部数据安全共识，实现数据安全防护建设一盘棋。因此，数据安全治理必然是涉及多元化主体共同参与的工作。

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、治理数据安全风险、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。

治理数据安全风险。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治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，组织应该围绕该体系进行建设。本指南依据 BDC 91-2022《数据安全治理能力评估方法》，基于**数据全生命周期视角**提出了一个三层架构，同时基于该三层架构在实践中的**工作分工**，演化出管理、技术、运营三类工作内容。

1. 基于数据全生命周期视角

数据安全治理体系的三层框架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，其中：

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。

2. 基于工作内容分工视角

上述三层框架在组织内部落地实践过程，涉及到多方面的工作，根据组织内常见的工作划分，我们按照管理、技术、运营三类的工作内容进行演化，生成基于工作内容的数据安全治理体系视角，其中：

管理类工作涉及组织架构、制度流程、人员管理等三方面工作，是数据安全治理体系在组织内运作的基石，主要负责协调、整合及优化各种资源，最终实现数据安全治理目标。更详细的内容可以参考“（三）数据安全治理维度”。

技术类工作涉及基础通用类、生命周期类、平台类技术的策略配置、技术实现等，主要为管理类工作的落地提供技术支撑，是数据安全的直接保障。具体的技术工作将在“（三）数据安全治理维度”进行描述。

运营类工作可以从运营对象、管控流程两个维度切入实现，主要承担优化数据安全工作流程，及时持续的为数据安全决策提供有价值

的信息和洞察。更详细的内容将在第三章进行阐述。

（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。

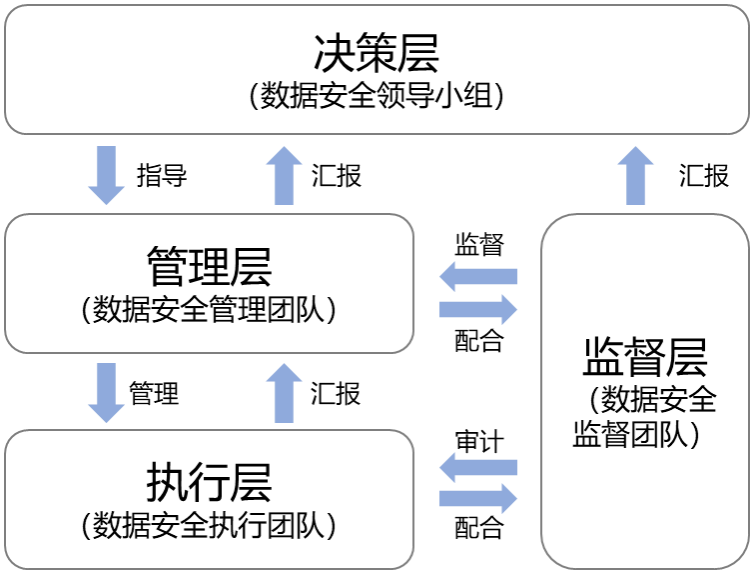
1. 组织架构

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，一般以虚拟组织的形式存在，如数据安全领导小组，该小组通常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，主要职责包括：



来源：数据安全推进计划

图 2 数据安全治理组织架构示例

- 制定数据安全整体目标和发展规划；
- 发布数据安全管理制度及规范；
- 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；
- 重大数据安全事件协调与决策。

管理层则对执行层提出数据安全管理要求，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，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，主要职责包括：

- 制定数据安全管理制度及规范；
- 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；

- 推进数据安全风险评估、数据出境安全评估等专项工作的开展；
- 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；
- 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。

执行层一般由业务部门、技术部门等构成，负责执行或支撑各项数据安全管理要求的贯彻落实，主要职责包括：

- 负责依据国家法律法规、政策文件、标准规范及企业相关数据安全管理要求，合理开展工作；
- 负责制定本部门相关业务场景下的数据安全实施细则；
- 负责按照要求构建数据安全建设的技术支撑能力，助力管理要求落地；
- 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；
- 积极参与数据安全意识培训、能力培养及考核工作。

监督层负责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，一般涉及合规、风控、内审等部门，主要职责包括：

- 对数据安全制度及规范的执行情况进行监督；
- 对数据安全技术工具的落地情况进行监督；
- 对数据安全风险评估过程进行监督审计。

各层的主要分工和构成如表 1 所示。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，不同机构还需结合现有组织

架构，进行适度的调整和补充。

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/技术部门/人力部门	合规部门/风控部门/内审部门
整体建设规划	牵头负责	遵照执行	遵照执行	执行并监督
组织架构调整	牵头负责	遵照执行	遵照执行	执行并监督
制度流程建设	意见审批	牵头负责	遵照执行	执行并监督
技术体系建设	意见审批	日常管理	牵头负责	日常监督
安全要求落实	意见审批	日常管理	牵头负责	日常监督
安全专项检查	意见审批	牵头负责	遵照执行	日常监督
安全教育培训	意见审批	牵头负责	遵照执行	日常监督

来源：数据安全推进计划

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。

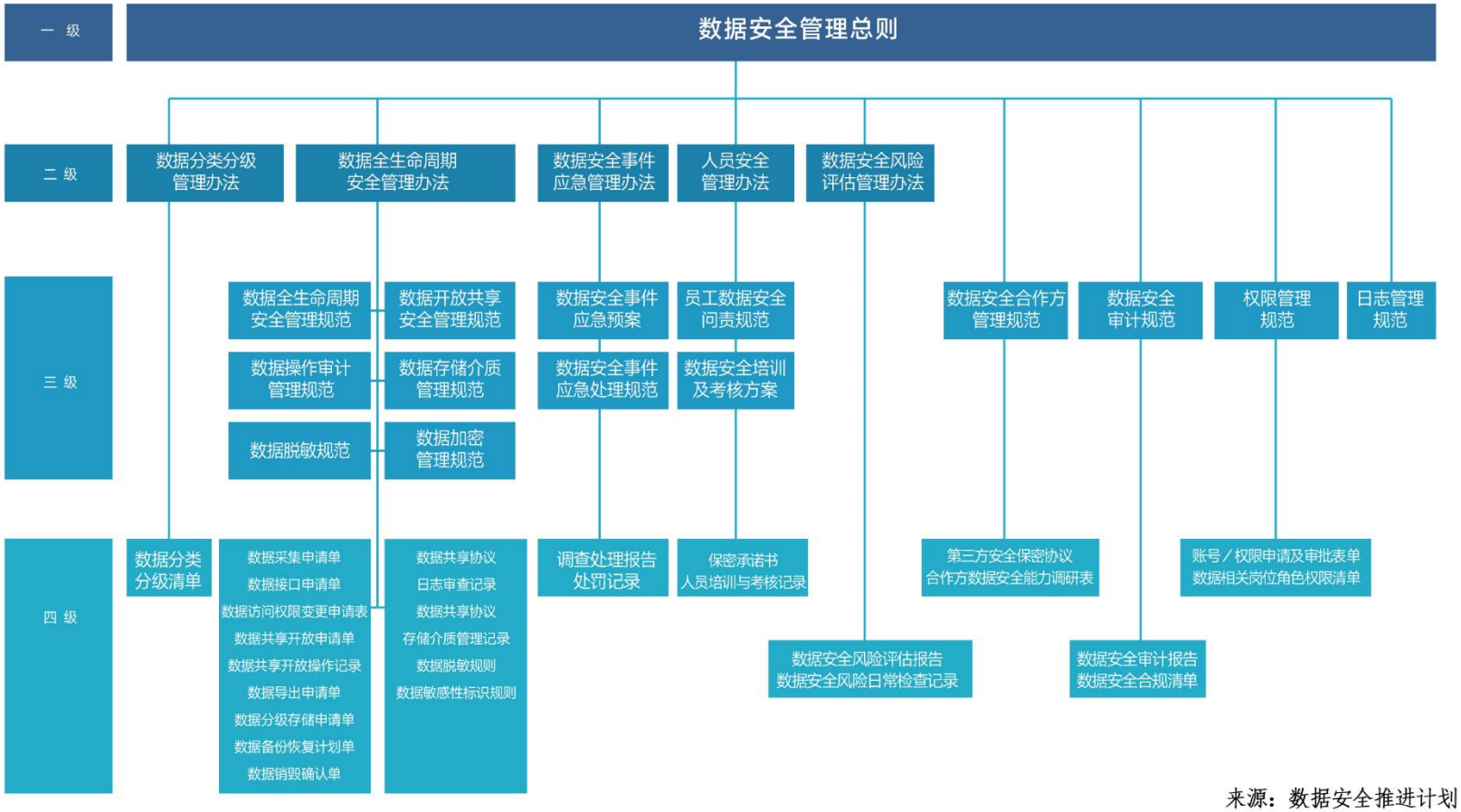
数据安全管理制度文件可分为四个层面，一、二级文件作为上层的管理要求，应具备科学性、合理性、完备性及普适性。三、四级文件则是对上层管理要求的细化解读，用于指导具体业务场景的具体工作。常见的制度体系如图 3 所示。

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. 技术工具

数据安全治理体系的技术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治理技术体系如图 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 数据安全治理技术体系

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：

• 数据安全运营管理平台通过数据资产梳理、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。

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、人员角色等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。

表 2 不同类型人员的数据安全能力要求和培养机制

人员角色	数据安全能力要求
决策层	了解数据安全法律法规、具备数据安全意识、知晓常见数据安全陷阱
管理层	熟知数据安全法律法规、知晓数据安全风险、熟悉数据安全合规评估工作流程、熟悉数据安全操作规范
执行层	了解数据安全法律法规、具备数据安全技术能力、熟悉业务流程的安全风险、熟悉数据安全操作规范
监督层	熟知数据安全法律法规、熟悉数据安全工作流程、具备数据安全意识

来源：数据安全推进计划

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，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）数据安全治理专项

如前所述，数据安全治理的要点之一是多元化主体的共同参与，其工作过程涉及数据、安全、合规、业务等诸多部门，因此协调落实复杂程度较高，为了保障各部门及各项管理要求的有效配合及落实，数据安全专项工作必不可少。结合监管要求及业务发展需要，数据分类分级、数据安全风险评估、数据出境安全评估、合作方数据安全管理等专项工作的开展需要提上日程。本指南结合相关要求及行业实践，将在第四章详细描述以上专项工作的开展思路。

（五）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。该实践路线将在第三章展开论述。

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，可以按照体系化和场景化相结合的思路推进实践过程。一方面，体系化思路，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蓝图。另一方面，场景化思路，针对各业务场景敏捷落地相关数据安全能力点，通过实际业务场景中数据安全的建设落地实践，反向总结输出相应管理规范，并由点及面应用至相似场景，以强化管理对业务的下沉指导。以上实践过程可以有效避免管理和技术的“两张皮”问题。

（一）全局数据安全体系规划

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。

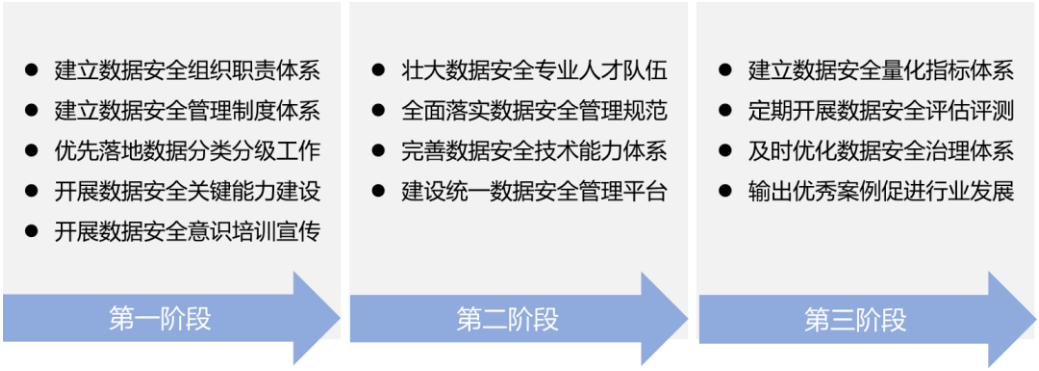
二是数据安全风险现状分析。有效的数据安全风险管理是组织推进业务发展的重要保障。不同组织需结合其业务场景，基于数据全生命周期安全防护要求，通过数据安全风险评估等专项工作的开展，识别数据面临的安全威胁及所在环境的脆弱性，形成风险问题清单，提炼数据安全建设需求点。

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指标体系，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

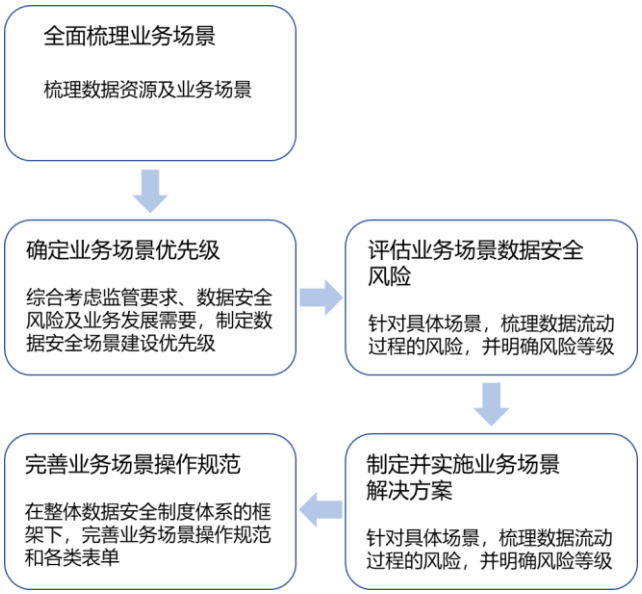
为保障规划方案在建设过程的顺利实施，应从以下方面进行论证分析。**一是可行性分析，**根据组织现状，明确人力、物力、资金的投入与产生的效益对比，协调数据安全管理机制和技术能力建设与业务系统之间的分歧，确保在业务发展与安全保障之间达到平衡。**二是安全性分析，**方案在正式实施前，要进行详细的方案论证分析，确保可以在业务稳定运行的前提下实施治理建设，同时要考虑治理过程中可能产生的新风险，避免未知风险的引入。**三是可持续性分析，**数据安全治理是持续性过程，随着业务拓展和技术进步，规划方案在保证与当前组织现有体系兼容的同时，也要考虑与后续的发展相适应。因此数据安全治理方案不仅要考虑当下，还要着眼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

（二）数据安全场景有序建设

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

1. 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之间以及外部机构之间的数据传输场景。

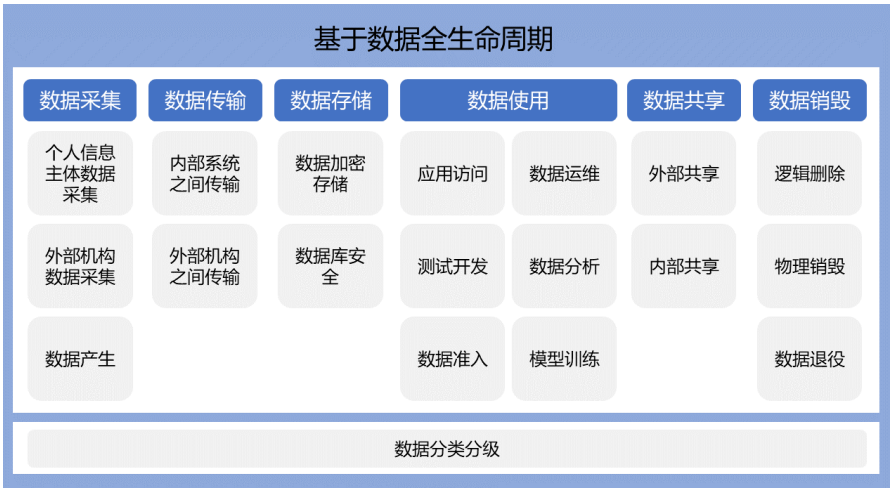
• 数据存储环节主要有数据加密存储、数据库安全等场景。

• 数据使用环节主要有应用访问、数据运维、测试和开发、终端安全、数据准入、数据分析、模型训练等场景。

• 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

在组织实际工作中，业务场景较为复杂，一般涉及多个全生命周期环节，两者更多是如表 3 所示的多对多的关系。当组织从全生命周

期环节出发划分业务场景难度较大时，也可以从业务的流转视图开始，分析其涉及到的全生命周期环节。其最终目的是建立业务场景与全生命周期环节的对应关系，便于形成基于数据全生命周期的统一安全管理。

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。

表 3　业务场景与数据生命周期关系示例

场景\生命周期	采集	传输	存储	使用	共享	销毁
业务场景 1	√	√	√	√		
业务场景 2				√	√	
业务场景 3		√	√		√	

来源：数据安全推进计划

（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。

2. 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。

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，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，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《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。

（三）数据安全运营持续加强

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。运营体系的构建可以从运营对象、管控流程两个方向进行切入建设。

1. 从运营对象的角度

（1）数据的运营

数据作为数据安全的主要管理对象，必然是数据安全运营的关键内容。通过对数据的运营，可以全面掌握数据的分布及流转情况，为数据安全的策略制定、风险排查等提供有效输入。一般来说，数据运营可以从数据资源目录、数据分布地图、数据流转视图等几个方面开展工作。

数据资源目录。将梳理的数据资源情况进行统一的纳管，明确数据来源、数据属主、数据类型等情况，形成数据资源的统一目录视图。一方面有助于解决数据重复、不一致等数据质量问题，另一方面可以作为数据分类分级工作的范围参照和数据输入。

数据分布地图。数据作为业务的共生体，存在于组织的不同部门、不同系统、不同存储资源中。当发生数据泄露、篡改等安全事件时，清晰的数据分布地图有助于快速定位受影响的系统和数据，提高数据安全措施的针对性，提升事件的应急响应效率。同时也能够快速为业务指明目标数据资源所在，加快数据协同。

数据流转视图。流动是发挥数据价值的重要环节，也是数据安全风险的源头之一。数据流转视图一方面呈现了业务流过程，有助于业务流程优化，另一方面有助于呈现数据使用情况，为数据流动过程的

风险防范提供视角。

（2）合规的运营

合规工作是组织数据安全治理的底线要求，如何将法律条文、监管要求内化为组织可落地的管理指标，并定期开展检查及整改工作是合规运营的主要内容。因此，可以从合规库管理、合规检查、合规监管处置三方面开展工作。

合规库管理。明确的合规要求以及清晰的合规理解，是合规实践工作的重要前提，因此各机构需要依据国家法律法规、行业监管要求等建立合规知识库，并动态更新管理。与此同时，数据安全部门、合规部门等需要将以上要求分解为业务可用的数据安全指标，为数据安全运营活动提供输入与参照。

合规检查。合规检查主要基于合规库，面向组织数据处理活动的安全合规情况进行定期检查，包括对数据脱敏、数据采集、访问控制等活动的合规性检查，判断数据安全合规现状与检查指标的符合程度。

合规监管处置。合规整改是合规运营的重要一环，主要实现对合规检查结果的公布与处理，也可兼顾给上级监管机构的合规数据报送等工作。

（3）安全的运营

安全是发展的保障，发展是安全的目的。对数据安全的有效运营才能促进业务更健康的持续发展。通过分析产业界数据安全运营相关工作，安全策略运营、安全能力管理、协同管理关联分析都是安全运

营的重要工作。

安全策略运营。风险的防范离不开相应策略的制定与实施，因此构建一套安全策略的运营机制是实现风险治理的前提。针对不同的数据安全风险，需要具备成熟的安全管理策略，同时能从数据安全事件中吸取经验教训，反哺安全策略的升级。

安全能力管理。据《2022 年数据安全行业调研报告》显示，44%的组织已应用了 5~8 项的数据安全技术产品，产品的堆叠与管理不仅为组织带来困扰，不同产品之间的壁垒也为安全作用的发挥带来了阻碍。因此针对多个数据安全产品的接入与集成管理成为运营工作的关键。集成的安全能力管理有助于实现不同安全策略的编排、下发，实现联动防御。

协同关联分析。安全运营通过采集各安全设备和第三方厂商安全事件信息进行关联分析，建立资产画像、身份画像等威胁模块，提升风险感知效率，加快风险处置进程。

2. 从管控流程的角度

（1）事前风险防范

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）事中监控预警

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 4 所示内容。

表 4 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、个人信息保护合规审计等工作。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、个人信息保护合规性等多方面内容，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）事后应急处理

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）数据安全评估助力优化

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，在组织内部开展专项评估，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。

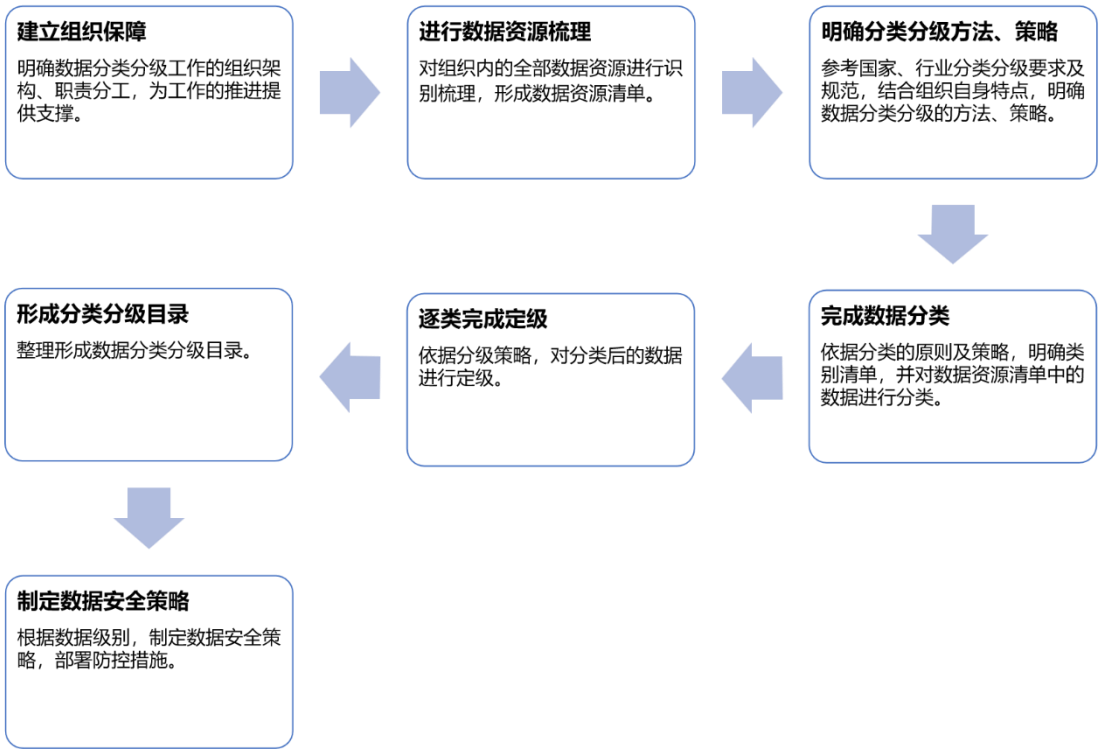
2. 第三方评估

除了内部评估外，组织还应引入第三方评估。第三方评估以法律法规、监管要求、标准文件等为执行准则，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、数据安全治理专项开展思路

（一）数据分类分级专项

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

1. 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由数据安全或数据管理部门牵头或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。

2. 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。

3. 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。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。

4. 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。

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

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]。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。

5. 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	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	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、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

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

6. 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。

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

7. 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。

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

（二）数据安全风险评估及治理专项

数据安全风险形势持续严峻，传统业务的数字化转型推进以及数据价值化加速推进，数据安全风险的识别、评估与综合治理已成为广大数据处理者面临的最紧迫、也同样是最根本的问题。

1. 数据安全风险评估

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。

（1）评估准备

组织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。组织可以采取

“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，组织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。以金融行业为例，组织可以参考的评估依据包括但不限于国家法律法规、国家网信、工信及金融等监管、主管部门的数据安全规章以及相关标准。涉及到组织相对特殊的业务和数据处理活动的，组织还可以将内部的数据安全管理制度纳入评估依据的参考范围。

（2）评估实施

组织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，组织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，识别、分析是否存在合作方安全能力水平低、合作安全责任不明确、外包访问权限过大等典型的风险问题，结合风险的影响程度与发生的可能性，

定性或定量判断具体风险的等级，结合组织资源分配等实际情况，输出问题清单、整改建议、风险分析等评估结果。

（3）评估总结

在完成数据安全风险问题的识别、评估分析后，组织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，但组织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，组织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. 数据安全风险治理

数据在流动中体现并创造价值，而流动必然伴随风险。业内相关研究多次提到数据安全风险的治理应与组织风险战略保持一致，不应是点对点的扑救与应对。这意味着组织不仅要在风险评估，更要在风险治理上紧密结合业务及数据处理活动，以实现风险可控的安全防护总体目标。然而，大量组织将注意力集中在对风险的评估与分析，整体上缺乏全局视角与调优参考，对风险评估的结果应用也不甚充分，未能形成一条可联动、可协同的治理链条。

针对这一问题，2022 年中国信通院基于对互联网、金融、电信运营商等行业企业的实地调研，牵头编制 BDC 136-2022《数据安全风险治理成熟度评价模型》，提出了数据安全风险治理的基本框架。数据

安全风险治理以风险为核心，强调了面向风险的控制与治理，关注对风险的识别、评估、处置以及监控改进的全生命周期管理，从“以建设防范风险”走向“主动认知风险”。

数据安全风险治理体系在面对协同管控及复杂数据生态上具有优势：其在风险准则确立、风险要素识别、风险评估分析、风险处置解决、风险治理改进五个能力领域明确了治理工作要求与对应的能力水平，提出了“预防为主、主动发现、积极防范”的工作原则，充分考虑了组织内部的多方多维协同、技术与管理措施配合，在推动组织的数据安全风险评估与后续风险处置、监控、改进的有效串联上具有重大的价值。

（三）个人信息保护专项

面对垃圾短信、电信诈骗、骚扰电话、财产损失等由于个人信息泄露带来的负面影响，国家重拳出击发布《中华人民共和国个人信息保护法》，为个人信息保护工作的开展落实提出了法律要求。当前，个人信息保护作为数据安全的一项重要内容，个人信息保护认证、个人信息保护影响性评估等工作备受关注，组织可以根据需要选择适用的专项开展。本小节只对个人信息常见的风险项[2]进行阐述，不针对某一项具体评估展开。

1. 个人信息采集风险

- 采集过程不满足最小必要、合法性、授权同意等要求。

[2] GB/T 35273-2020 《信息安全技术　个人信息安全规范》

• 采集内容与采集声明不符。

• 隐私政策方面，没有相关隐私政策或者展示形式不够明显，没有在隐私政策中突出标识或以显著方式告知用户采集相关信息的目的、方式、存储时间、地点等。

2. 个人信息存储风险

• 保存时间不满足相关要求，未对到期的个人信息进行处理。

• 技术手段缺失，未对需要存储的信息施展加密、脱敏或去标识化等安全措施。

• 未按照个人信息主体的要求对其信息进行处理操作。

3. 个人信息使用风险

• 未设置审批流程或者未执行审批过程。

• 未按照最小授权原则分配访问权限。

• 使用目的与采集声明不一致。

• 展示过程未进行去标识化等技术处理。

• 委托处理、共享、转让、公开披露等处理过程不满足合规要求。

4. 组织管理风险

• 未明确个人信息保护的责任部门和人员。

• 未定期开展个人信息保护相关评估测试工作。

• 缺少个人信息保护的员工培训及合规审计工作。

（四）合作方数据安全管理专项

我国数据要素市场正处于蓬勃发展阶段，在政策、业务、技术等

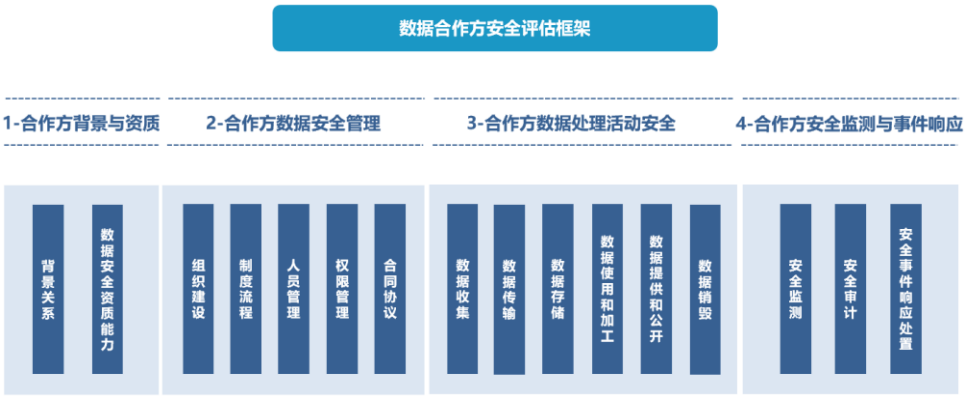
多方因素的驱动下，数据合作需求激增，数据合作场景愈发多样化。然而数据合作方的安全保护能力参差不齐，数据合作过程中，数据泄露、数据滥用等安全事件频发，严重危及国家、公众及个人安全。国家战略要求统筹好安全和发展，保障数据合作安全已成为重要议题。

1. 数据合作方识别

落实数据合作方安全管理要求的首要任务是识别数据合作方，需要明确数据合作的形式、触发条件、对象。数据合作形式多样，主要可以概括为业务合作、技术支撑、数据服务和监管要求四大类。参照上位法和行业标准，可以明确将“参与组织的数据处理活动过程”作为数据合作的触发条件。数据合作的对象包括外包服务机构和外部合作机构。综上，数据合作方定义为因业务合作、技术支撑、数据服务、监管要求等参与本组织数据处理活动的外包服务机构与外部合作机构。

2. 数据合作方安全评估

数据合作安全事件频发，落实数据安全保护和个人信息保护义务，组织需要建立数据合作安全保护机制，开展数据合作方的数据安全保障能力动态评估，对数据合作方的安全保护能力进行核验，采取必要的安全保护措施。本指南结合前期大量调研和数据安全评估实践，依据 BDC 163-2023《数据合作方安全评估要求》，提出数据合作方安全评估框架，从背景资质、数据安全管理、数据处理活动安全、安全监测响应四方面评价合作方的数据安全保护能力，如图 12 所示。



来源：数据安全推进计划

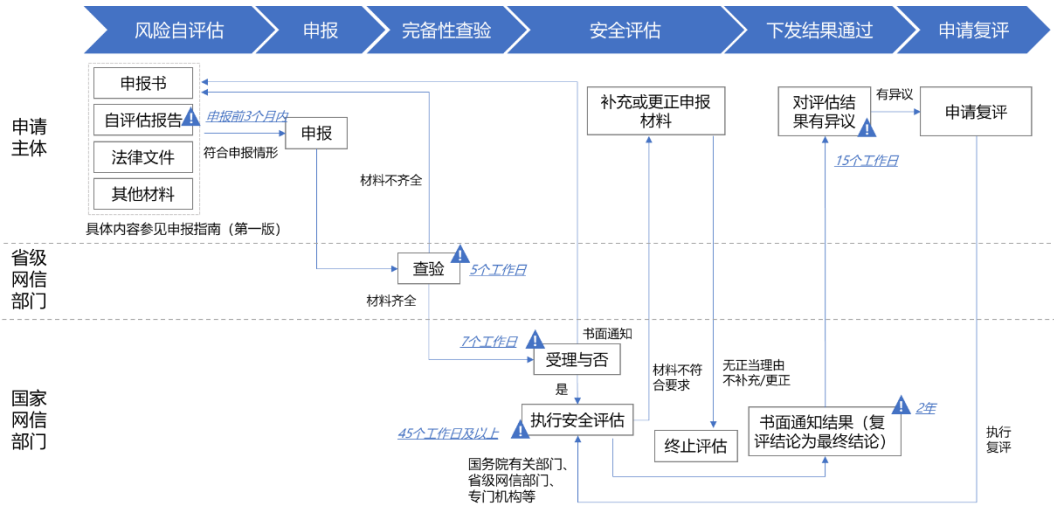
图 12 数据合作方安全评估框架

数据合作业务场景复杂，可以按照数据合作方在数据流转中的角色实施差异化评估内容。按数据流转参与的角色及其功能，可以将数据合作方划分为数据提供方、数据接收方、数据中间商、重点相关方。针对数据提供方，应重点评估数据的真实性、准确性、合法合规情况以及数据保护措施等安全能力。针对数据接收方，应重点评估接收方组织架构和制度流程等安全管理的合规性，安全保护措施和安全事件应急预案的充分性和有效性。针对数据中间方，应重点评估中间方服务、基础设施的安全性，所采取数据安全保护措施的充分性和有效性。针对重点相关方，即数据上报到监管部门的情况不在评估范围内。

（五）数据出境安全评估专项

数据出境安全评估是由国家网信部门为落实国家上位法而实施的数据安全专项工作。通过数据出境安全评估能够划定可能影响国家安全的数据出境行为，强化数据处理者的数据出境风险自评估义务。本指南根据国家互联网信息办公室公布《数据出境安全评估办法》，

梳理了数据出境评估工作角色与流程，如图 13 所示。此处我们仅讨论申请主体在出境评估中的工作内容。



来源：数据安全推进计划

图 13 数据出境安全评估流程及执行主体

1. 判断是否适用数据出境安全评估

当前数据出境有数据出境安全评估、个人信息保护认证、个人信息出境标准合同三条路径，各组织机构需要根据业务场景，结合监管规定，选择适合的路径开展出境工作。

2. 明确需要数据出境安全评估的场景

出境安全评估的适用范围在《数据出境安全评估办法》第二条有明确规定，主要涉及重要数据和个人信息。2023 年 9 月 28 日，国家网信办针对《规范和促进数据跨境流动规定（征求意见稿）》公开征求意见，明确了无需申报数据出境安全评估的场景。因此各组织在判断适用情形时，可以参考以上两个文件。

3. 准备各项申报材料

依据《数据出境安全评估申报指南（第一版）》（简称《申报指南（第一版）》），出境安全评估需要准备申报书、自评估报告、法律文件等材料。

申报书：申报书由《承诺书》和《数据出境安全评估申报表》组成，可以参见《申报指南（第一版）》。

自评估报告:《申报指南（第一版）》中给出了自评估报告的模板，主要由自评估工作简述、出境活动整体情况、拟出境活动的风险评估情况、出境活动自评估结论组成。相较风险自评估，由国家网信部门执行的安全评估，还关注接收方所在地的法律政策环境、数据安全保障能力、数据处理者历史合规情况等内容，各组织需要在自评估报告中对以上问题详细阐述。

关于数据安全保障能力，主要关注管理组织体系及制度流程、数据分类分级、应急处置、风险评估、全生命周期技术能力等内容。

法律文件：与境外接收方拟订立的数据出境相关合同或者其他具有法律效力的文件影印件。

具体的材料准备内容，可以参考国家网信办或者地方网信办的申报指南及相关规定。各组织机构作为申报主体完成申报工作后，需要及时关注申报进展，对需要补充说明的内容进行准备，并在申请通过后，根据需要开展重新评估工作。

五、数据安全治理总结与展望

随着国家数据局的成立，数据要素市场化进度加快，数据流通交易力度加强，数据安全的重要性愈发突出。同时，由人工智能等新技术发展带来的数据安全风险愈加严峻，未来：

数据要素市场化进程加快，数据安全进入流通安全深水区。国家数据局于 2023 年 10 月 25 日正式揭牌，标志着数据资源整合共享与开发利用进程加快，各组织机构的数据将逐渐由组织“内”流通转向组织“外”流通，数据安全问题随之而来。一方面，流通环节涉及的责任主体增多，如何有效划分各方数据安全责任，成为数据高效流通的基本保障；另一方面，多频次、广范围的数据流转将带来更大的风险暴露面，如何保障流通环节的安全合规是现实问题。因此随着数据要素市场化的发展，数据安全风险在流通场景下会不断放大，数据安全工作难度也随之加深。

人工智能浪潮席卷全球，数据安全面临新发展与新挑战。人工智能技术可以通过对海量数据的收集分析与实时学习建立大模型文件，以驱动数据分类分级、数据安全风险监测等数据安全治理工作向智能化、高效化、精准化方向演进。同时，数据作为人工智能技术的主要输入之一，在训练、调优等过程面临数据窃取、数据泄露、数据篡改等安全风险，训练生成的模型文件也有可能遭到安全攻击，因此，大模型数据安全风险管理必将成为行业新议题。

数据生态日益复杂，数据安全能力运营愈发关键。一方面，面对数据流通交易场景下愈加复杂多样的数据生态，数据安全的常态化实践与持续运营成为各机构提升流通效率，降低流通风险的关键手段。另一方面，数据安全运营能力的构建能够打破各组织既有数据安全产品之间的壁垒，实现策略的有效整合，提升数据安全工作成效。

数据安全推进计划
DATA SECURITY INITIATIVE

简 介

数据安全推进计划（Data Security Initiative，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、电信、互联网、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：李老师

联系方式：13581661287

数据安全推进计划公众号