数据安全治理框架及实践探讨

中国信息通信研究院云计算与大数据研究所　刘雪花

2021.09.25

目录

Contents

数据安全法落地实施

◆ **《中华人民共和国数据安全法》**已于2021年9月1日正式实施，数据安全成为全行业的关注焦点。

兼顾数据安全与发展

- 支持数据开发利用和数据安全技术研究，培育、发展相关产品和产业体系
- 推进数据开发利用技术和数据安全标准体系建设
- 促进数据安全检测评估、认证等服务的发展，支持检测评估和认证工作

国家建立数据安全制度

- 建立数据分级分类保护制度
- 建立集中统一、高效权威的数据安全风险评估、报告、信息共享、监测预警机制
- 建立数据安全应急处置机制
- 建立数据安全审查制度

明确数据安全保护义务

- 要求企业建立健全全流程数据安全管理制度、技术措施，组织开展数据安全教育培训
- 要求企业加强风险监测，发生安全事件时，应告知用户并上报主管部门
- 要求企业定期开展风险评估，并报送报告
- 要求企业和个人合法正当收集数据
- 数据交易中介应当核验数据来源，审核交易双方身份，留存审核、交易记录

个人信息保护法正式公布

◆ **《中华人民共和国个人信息保护法》**已于2021年8月20日全文公布，全行业数据安全合规再次加码。

构建以“告知同意”为核心的处理规则

- 告知个人信息处理者的名称或者姓名和联系方式
- 告知个人信息的处理目的、处理方式，个人信息种类、保存期限
- 告知个人行使权利的方式和程序
- 告知法律、行政法规规定应当告知的其他事项。
- 严格限制不需要告知的情形；
- 发生变更的，应当重新取得个人同意。
- 个人有权撤回其同意。

明确个人在个人信息处理活动中的权利

- 知情权
- 处理决定权
- 查阅复制权
- 转移权
- 更正补充权
- 删除权
- 要求解释权
- 代行使权

明确个人信息处理者的义务

- 制度规程制定
- 信息分类管理
- 安全技术措施
- 人员管理规范
- 应急预案制定
- 法定其他措施
- 指定安全负责人
- 设立机构/代表
- 定期合规审计
- 事前影响评估
- 事后告知

明确监管部门的职责

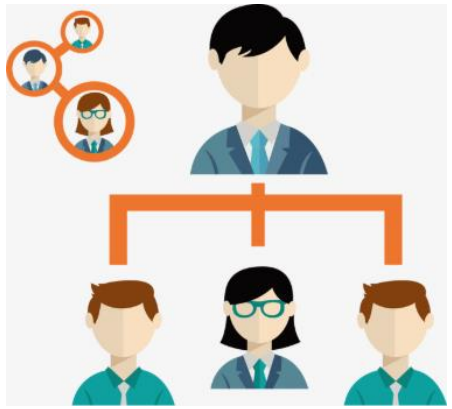
- 明确责任架构
- 规定职责范围：
  - 开展宣传教育
  - 处理投诉举报
  - 测评相关应用
  - 违法调查处理
  - 法定其他职责
- 推进相关工作：
  - 规则标准制定
  - 认证技术支持
  - 服务体系建设
  - 投诉举报机制

法律体系衔接

	网络安全法	数据安全法	个人信息保护法
立法目的	关注安全和信息化发展	平衡数据安全与发展	促进个人信息合理利用
	保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和组织的合法权益，促进经济社会信息化健康发展	规范数据处理活动，保障数据安全，促进数据开发利用，保护个人、组织的合法权益，维护国家主权、安全和发展利益	为了保护个人信息权益，规范个人信息处理活动，促进个人信息合理利用
适用范围	在中华人民共和国境内建设、运营、维护和使用网络，以及网络安全的监督管理	在中华人民共和国境内开展数据处理活动及其安全监管	处理自然人个人信息的活动
主要内容	➢ 关键信息基础设施 ➢ 网络安全支持与促进 ➢ 网络运行安全 ➢ 网络信息安全 ➢ 监测预警与应急处置	➢ 数据安全与发展 ➢ 数据安全制度 ➢ 数据安全保护义务 ➢ 政务数据安全与开放	➢ 个人信息处理规则 ➢ 个人信息跨境提供的规则 ➢ 个人在个人信息处理活动中的权利 ➢ 个人信息处理者的义务 ➢ 履行个人信息保护职责的部门

落实数据安全保护和个人信息保护义务，需要建设数据安全治理体系

- 《数据安全法》明确提出要**建立健全数据安全治理体系**。
- 通过数据安全治理提升企业数据安全水平已成为行业共识。



明确的组织架构作保障

体系的制度流程作依据

完备的技术工具是能力底座

合格的人员能力是有效支撑

需要体系化，建立机制，形成闭环

何为数据安全治理

◆ 数据安全治理**不仅局限于**组织内部，而是一个需要国家、行业组织、科研机构、企业和个人**共同**努力完成的课题。因此，应该分别从**国家层面**和**组织内部**角度来看待数据安全治理。

Gartner 数据安全治理是风暴之眼

Microsoft 隐私、保密、合规性（DGPC）

CAICT 中国信通院

从组织内部来看

- 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。

数据安全治理要点

◆ “以数据为中心”、“多元化主体共同参与”、“兼顾发展与安全”是数据安全治理的三个要点。

“以数据为中心”

- 围绕数据全生命周期
- 针对具体业务场景
- 识别数据安全威胁与风险

“多元化主体共同参与”

- 构建多方参与治理框架
- 明确各方职责
- 统一各方数据安全共识

“兼顾安全与发展”

- 坚持以数据开发利用和产业发展促进数据安全
- 坚持以数据安全保障数据开发利用和产业发展

目录

Contents

国外数据安全治理现状

◆ 依托**市场化机制**，国外已经形成了较为完备的数据安全**第三方评估**测试体系，在助力法律法规落地、提升企业数据安全管理水平、推动行业健康有序发展方面发挥了重要的作用。

美国 TRUSTe 安全认证

- 吸收借鉴了CCPA、GDPR等各国法律法规和OECD、APEC等国际组织的隐私保护框架。
- 对企业隐私与数据治理实践进行认证，聚焦数据隐私保护。

欧盟 GDPR 数据保护机制

- 对企业和组织的数据行为进行评估认证。

英国个人信息管理系统认证

- 基于BS10012:2009《数据保护——个人信息管理系统规范:实施方法》。
- 侧重于信息管理过程，并有针对中小企业设置的特别准则。

美国iKeepSafe COPPA认证

- 由特定非营利性组织依据美国儿童在线隐私保护法(COPPA)的原则和要求对APP、云解决方案和网络服务等针对儿童个人信息的行为进行评估。

法国CNIL电子保险箱认证

- 由CNIL依据法国数据保护法案对数据存储的安全性进行评估认证。

国内数据安全治理现状

国家高度重视标准化工作

- GB/T 35274-2017《信息安全技术 大数据服务安全能力要求》
- GB/T 37973-2019《信息安全技术 大数据安全管理指南》
- GB/T 37988-2019《信息安全技术 数据安全能力成熟度模型》（DSMM）
- GB/T 35273-2020《信息安全技术 个人信息安全规范》
- **T/ISC-0011-2021《数据安全治理能力评估方法》**

偏重信息安全认证

- 中国信息安全认证中心：开展企业信息安全认证工作
- 中国信息安全测评中心：开展信息安全漏洞分析与风险评估、信息技术产品、系统和工程建设的安全性测试与评估等工作

◆ 我国数据安全标准化工作迈入了新阶段，针对企业数据安全能力和产品数据安全能力的评估评测标准需求较大。

◆ 当前我国安全评估工作的重点在于信息安全，而面向数据安全的市场化评测评估尚处于起步阶段。

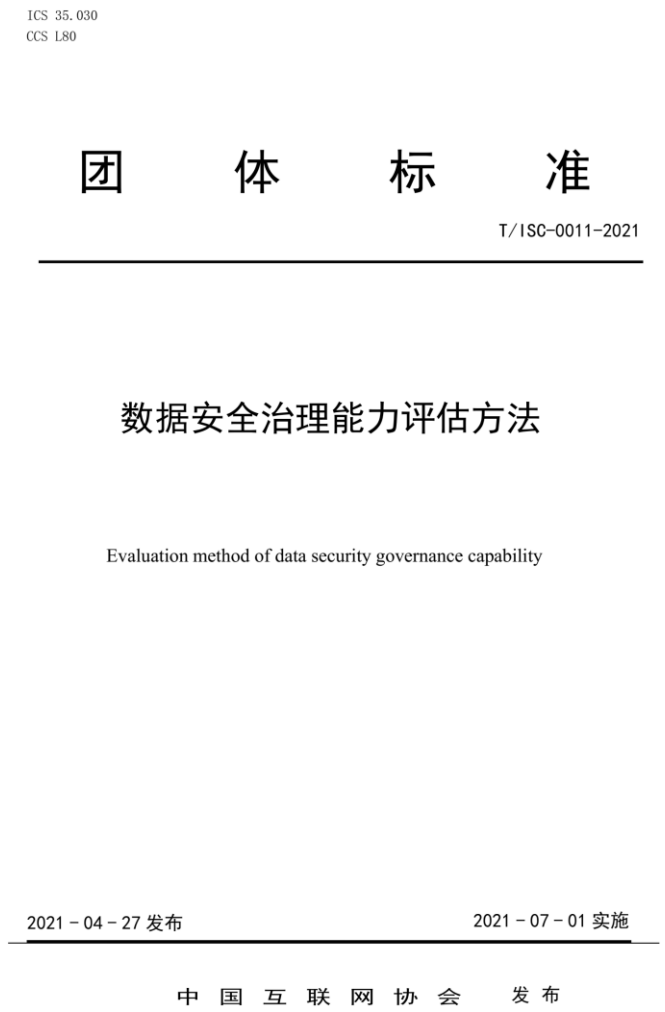
◆ **中国信息通信研究院：数据安全治理能力评估**

推动数据安全治理能力评估标准建设

◆ 2020年10月初在中国互联网协会**启动标准**编制，由来自百度、联通大数据、奇安信、蚂蚁等**20余**家电信和互联网企业的**近30位专家参与**。

中国互联网协会 Internet Society of China

CAICT 中国信通院 | China unicom 中国联通 | Baidu 百度 | 奇安信 | 蚂蚁集团 ANT GROUP
京东数科 | iQIYI 爱奇艺 | mi | EVERSEC 恒安嘉新 | 美团 | 中国移动 China Mobile
天翼云 e Cloud | 闪捷信息 SECSMART | 快手 | 同盾科技 www.tongdun.cn | 天融信 TOPSEC
ByteDance 字节跳动 | 贝壳找房 | oppo | 安恒信息 DAS-SECURITY | 启明星辰



ICS 35.030
CCS L80

团　体　标　准

T/ISC-0011-2021

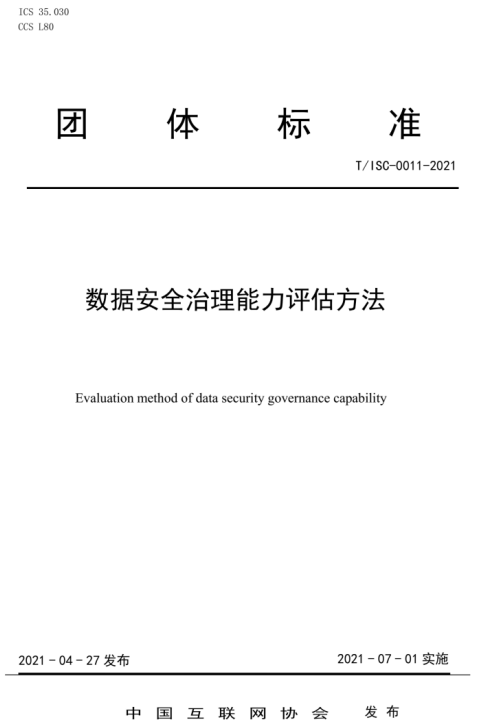
数据安全治理能力评估方法

Evaluation method of data security governance capability

2021－04－27 发布　　2021－07－01 实施

中 国 互 联 网 协 会　发布

标准概览



ICS 35.030
CCS L80

团　　体　　标　　准

T/ISC-0011-2021

数据安全治理能力评估方法

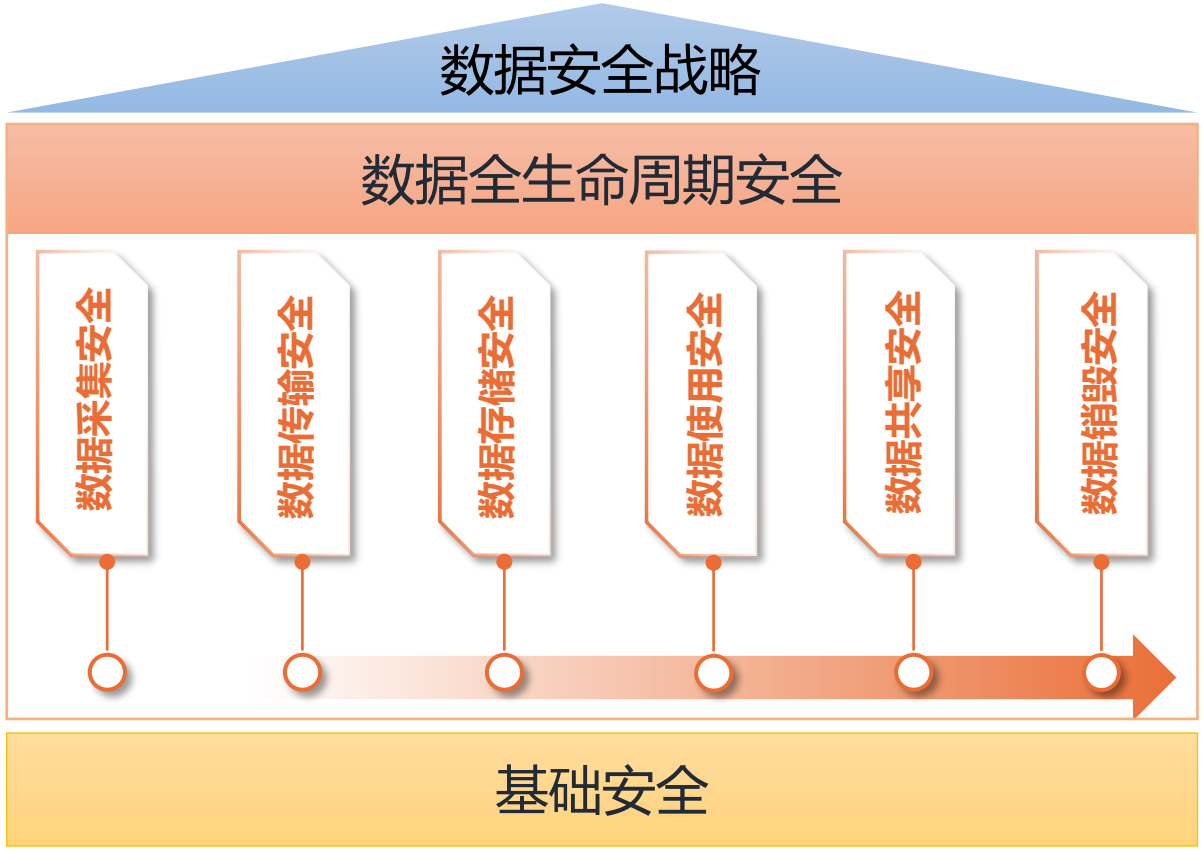
Evaluation method of data security governance capability

2021－04－27 发布　　2021－07－01 实施

中 国 互 联 网 协 会　发布

明确数据安全治理框架

◆ 明确包括**数据安全战略**、**数据全生命周期安全**、**基础安全**的治理框架。



治理框架具体能力项

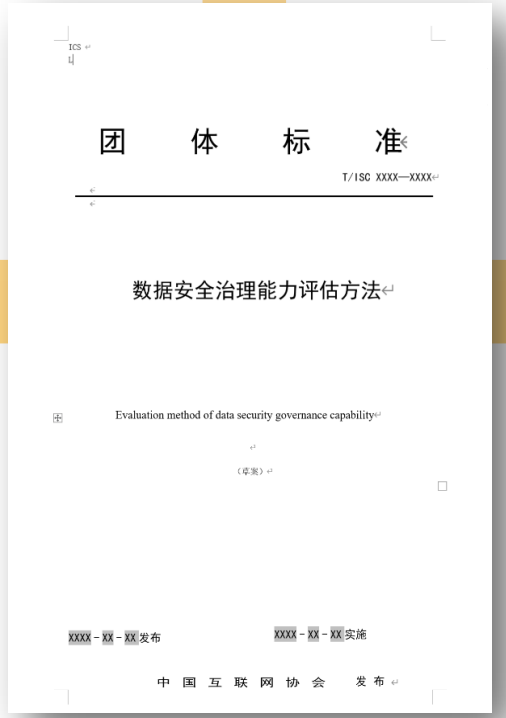
- 共包括**18个**能力项。

数据安全战略

- 数据安全规划
- 机构人员管理

基础安全

- 数据分类分级
- 合规管理
- 合作方管理
- 监控审计
- 鉴别与访问
- 风险和需求分析
- 安全事件应急


团 体 标 准

T/ISC XXXX—XXXX

数据安全治理能力评估方法

Evaluation method of data security governance capability

（草案）

XXXX-XX-XX发布

XXXX-XX-XX实施

中 国 互 联 网 协 会 发布

数据全生命周期安全

- 采集：数据采集安全
- 传输：数据传输安全
- 存储：存储安全、数据备份与恢复
- 使用：使用安全、数据处理环境安全
- 共享：数据内部共享安全、数据外部共享安全
- 销毁：数据销毁安全

治理框架解读——数据安全战略

◆ 从企业的顶层规划方面提出要求，为数据安全治理体系的建设**定目标**、**建团队。**

数据安全规划

- 关注企业在数据安全治理方面的发展规划情况。

目标及任务

团队分工及考核

机构人员管理

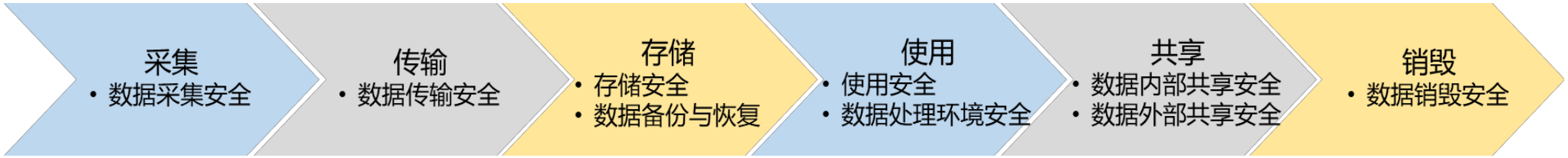
- 关注企业数据安全治理的团队建设，以及从业人员的安全管理规范。

团队及人员构成

人员安全管理

治理框架解读——数据全生命周期安全

◆ 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，对数据全流转过程进行规范和约束。



• 关注**直接**、**间接采集**过程的各项安全保护**措施**、采集**原则**以及采集的**合规性评估**等工作。	• 关注数据在传输过程中的安全性保障。 • 数据及传输通道**加密**。	• 关注存储介质、存储系统或平台的**安全**建设内容。 • 关注数据的**高可用性**建设。	• 关注数据使用方对数据相关**操作**的安全管理。 • 关注**不同处理场景、平台**的安全策略的实施。	• 关注组织**内部**数据流通安全保障建设。 • 关注**不同主体之间**的数据流通安全建设。	• 关注**数据及介质**的销毁管理。

治理框架解读——基础安全

◆ 基础安全能力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**。

数据分类分级	• 关注分类和分级的**原则、方法、结果清单**，以及不同的安全保护**策略**等内容。
合规管理	• 关注企业数据安全建设**是否符合**国家法律法规、行业监管指引等的要求。
合作方管理	• 关注企业对**合作伙伴**、**合作驻场人员**的各项安全管理要求。
监控审计	• 一方面关注数据全生命周期的**流动**行为，另一方面关注人员对数据的**操作**行为。
鉴别访问	• 关注企业人员的**账号**管理、访问**权限**控制的建设情况。
风险和需求分析	• 关注企业发展过程中面临的数据安全**需求分析**及**风险控制**问题。
安全事件应急	• 关注数据安全事件的**定义、分级、响应处置、上报**等工作的开展。

治理框架研制过程

◆ 标准编制工作于2020年10月初**启动**，并于2021年4月27日正式**获批**。

标准起草小组组建阶段：依托中国互联网协会，中国信通院牵头联合20余家企业组建标准起草小组，并成功立项。

2020年10月初

起草阶段：经过五次讨论形成草案，交由中国互联网协会组织专家函审，根据专家函审意见再次组织修订，形成征求意见稿。

征求意见稿阶段：通过中国互联网协会对外公开征求意见。汇总修订后形成送审稿，顺利通过送审稿评审会。

2020年10月-2021年1月

标准报批发布：顺利通过协会报批稿评审，并正式获批：T/ISC-0011-2021《数据安全治理能力评估方法》。

2021年1月-2021年3月

2021年4月27日

治理框架编制依据

法律法规和监管政策依据

- 《中华人民共和国网络安全法》
- 《中华人民共和国数据安全法（草案二次审议稿）》
- 《中华人民共和国个人信息保护法（草案二次审议稿）》

标准依据

- GB/T 35274-2017《信息安全技术 大数据服务安全能力要求》
- GB/T 37973-2019《信息安全技术 大数据安全管理指南》
- GB/T 37988-2019《信息安全技术 数据安全能力成熟度模型》

实践依据

- 以线上线下相结合的方式，开展数据安全治理交流

目录

Contents

推出国内数据安全治理能力评估工作

现状

- 行业水平参差不齐
- 度量方法缺失
- 与监管要求、公众期待尚有差距，缺乏贴近产业现状的指南。

问题

如何让监管放心

如何使用户满意

如何保数据安全

数据安全治理能力评估（DSG评估）

组织　制度　技术　人员

01规划 → 02建设 → 03审查 → 04优化

目标

通过准确**度量**企业的数据安全治理能力现状，合理规划数据安全治理能力**提升**路径。

用途

一套**构建方法**
一套**度量准则**
一套**改进指南**

效果

通过**以评促建**的方式，实现企业数据安全治理在**组织、制度、技术、人员**方面的闭环、循环提升

DSG评估等级

◆ 根据数据安全治理能力的**覆盖范围**、**支撑力度**等方面明确评估等级要求。

组织：没有正式的数据安全团队，由业务团队承担职责。
制度：应能保障核心业务的安全执行及故障恢复，基本满足监管要求。
技术：应能落实核心业务数据全生命周期安全要求。
人员：应关注人员的数据安全意识，进行定期培训。

组织：专门的安全团队。
制度：应能保障全部业务的安全执行及故障恢复，完全满足监管要求。
技术：积累大量的技术工具以支撑全业务、全生命周期的安全要求。
人员：制定考核机制，注重数据安全人才培养。

制度：建立量化的评估指标体系，能够有效应对监管变化。
技术：统一，不断优化的技术工具。

DSG评估：企业数据安全治理的自运转能力

组织建设

由谁来做

多方协同的团队架构

- 决策者
- 管理者
- 协作者
- 执行者

制度流程

应该怎么做

层次化的制度文件

- 方针总则
- 管理办法
- 操作指南
- 记录模板

技术工具

实际怎么做

体系化的技术能力

- 事后审计
- 事前预防
- 事中监控

人员能力

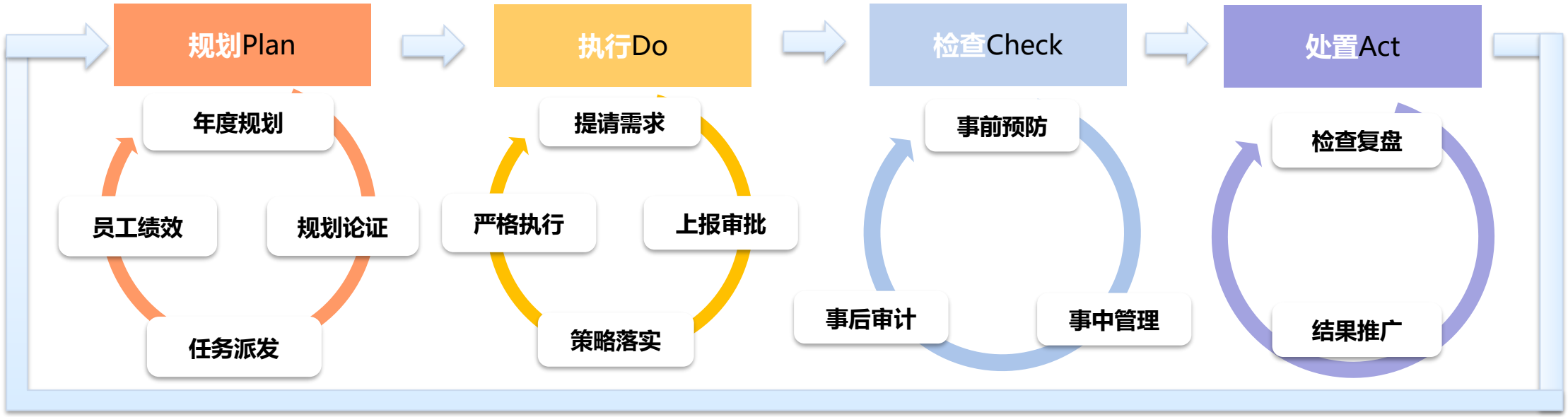
有没有能力做

自建人才培养体系

- 意识培养
- 能力提升
- 定期考核

DSG评估助推企业形成数据安全治理的双闭环

◆ 规划、执行、检查、处置4个环节流通的**大闭环**，以及各环节内的**小闭环**。



数据安全规划
机构人员管理 ＋ 数据全生命周期能力项 ＋ 合规管理、监控审计、鉴别与访问等基础能力项 ＋ 安全事件应急 ＝ **DSG评估**

DSG评估意义——对行业

◆ 准确评估行业数据安全治理能力发展现状

DSG评估

等级分布

行业内企业数据安全治理能力等级分布情况，逐年的改进和提升效果，以**评价行业数据安全治理能力发展情况。**

共性问题分析

准确把握数据安全建设过程中**普遍存在的问题**，为下一步的数据安全治理能力的提升奠定基础。

发现企业标杆

发现行业内数据安全治理能力建设的**标杆企业**，总结最佳实践，开展推广，提升行业整体水平。

DSG评估意义——对企业

◆ 发现存在问题，指明发展方向，提升治理能力

现状总结

通过问卷、访谈等形式对现状进行了解，发现**存在的问题**及**人员能力缺陷**，分析和行业水平的差距，并总结提炼**关键发现**。企业亦可依据标准进行**自评估**，初步发现企业自身问题。

推荐最佳实践

通过评估，实现企业与行业水平的**横向对比**，找出差距所在，有助于后续水平拉齐。

资讯获取

针对现状总结，结合最佳实践以及企业发展需要，给出**针对性的优化建议**。

优化建议

《数据安全法》发布实施，强调提升企业数据安全治理能力。通过评估，在应对监管时做到**心中有数**。

业内交流

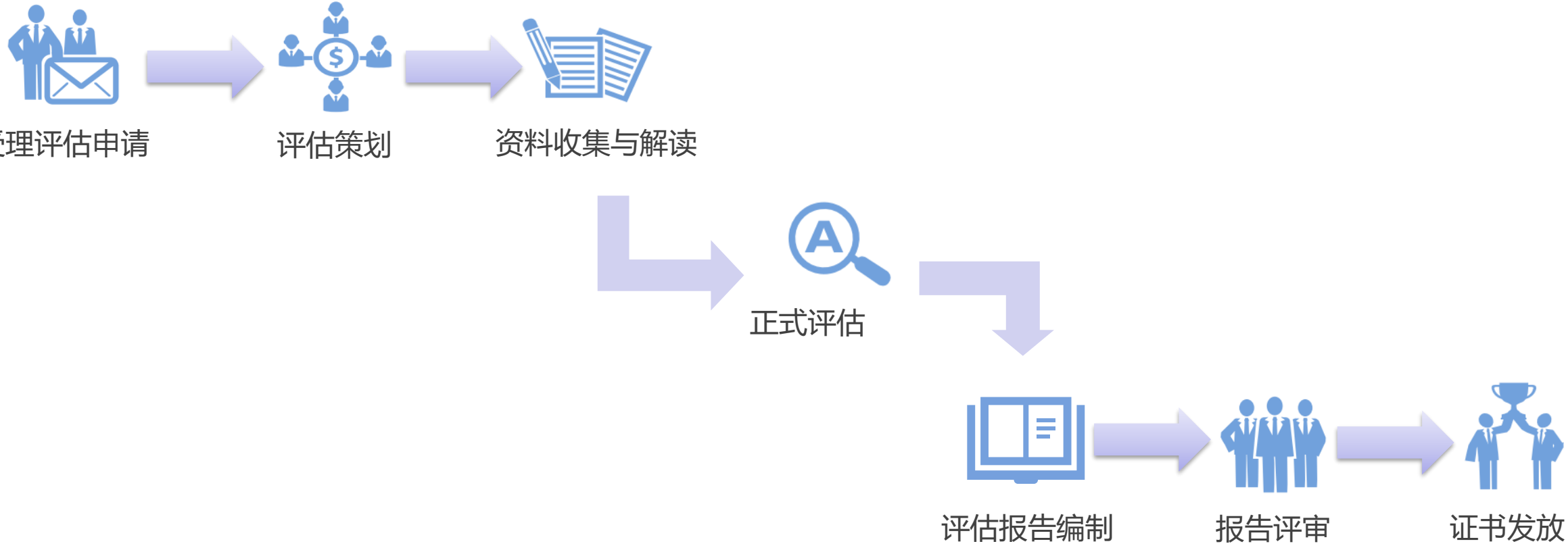
参与数据安全治理相关沙龙、论坛、大会等的交流中，了解行业发展情况，借鉴学习，提升治理经验。

宣传推广

对内加强宣讲，提升安全意识，对外加强推广，**扩大企业知名度**，推动行业发展。

DSG评估实施流程

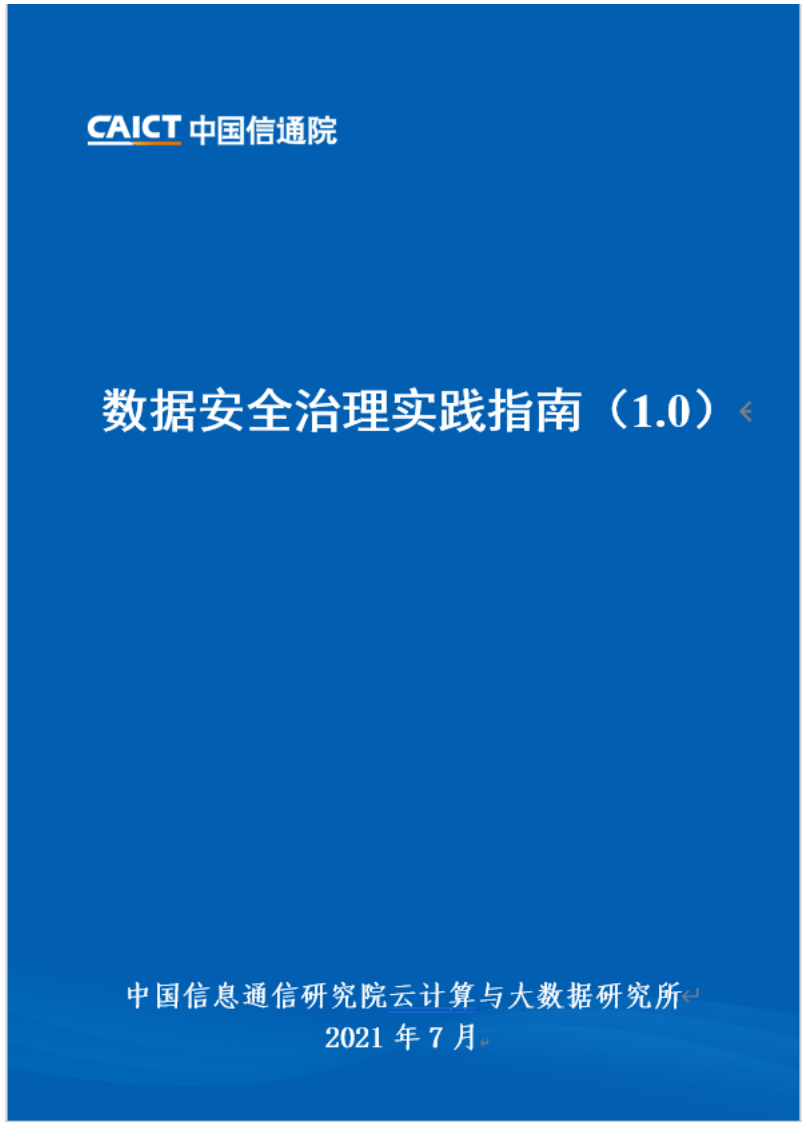
◆ 评估实施阶段主要分为前期准备、中期实施、后期审核三个阶段。



目录

Contents

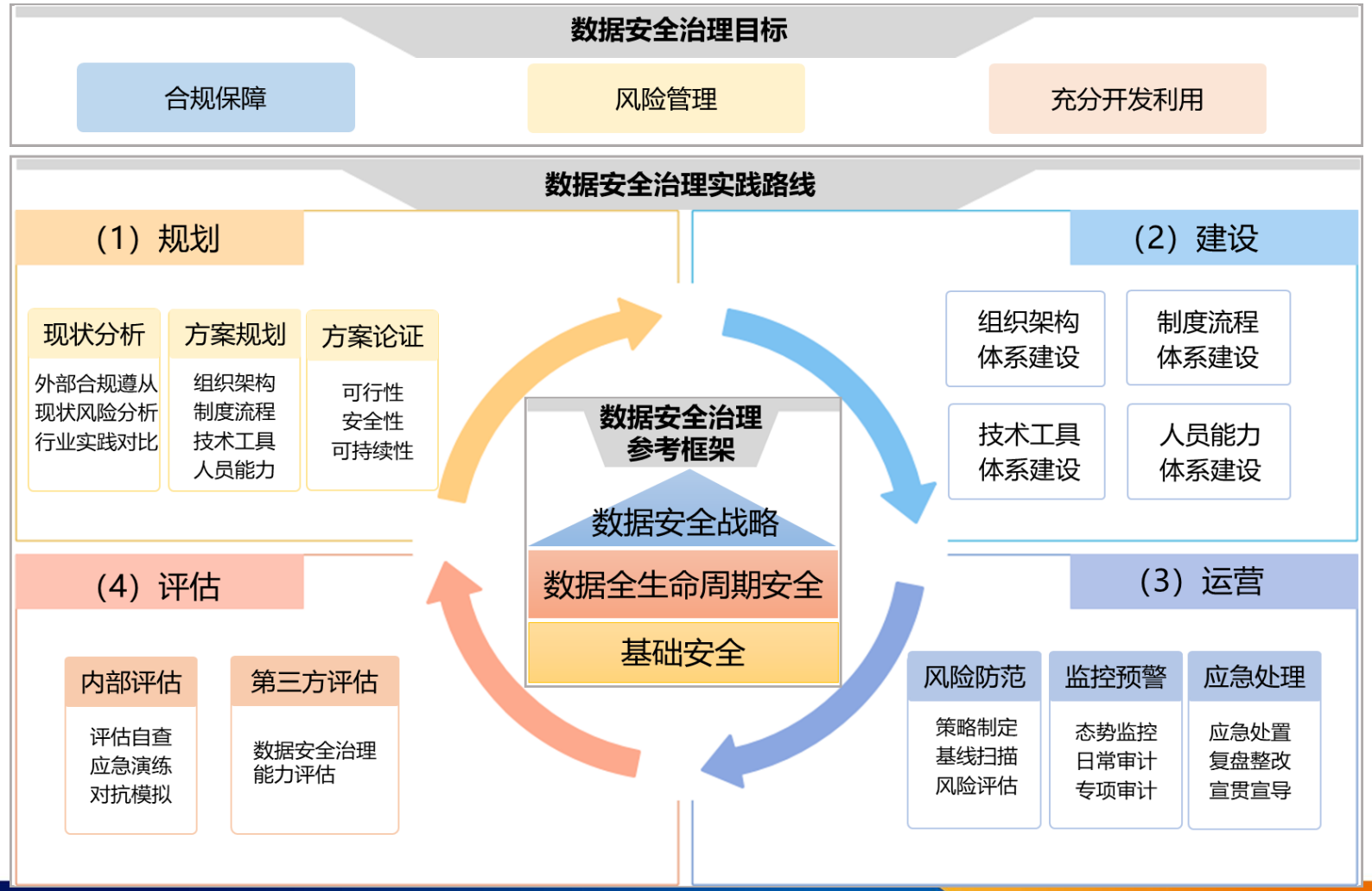
《数据安全治理实践指南（1.0）》发布



- **首次**从**广义、狭义**角度对数据安全治理进行定义
- **首次**系统的提出**数据安全治理总体视图**
- **创新性**的给出**可落地的实践路径**
- 从**三个层面、两个核心**，提出**发展建议**

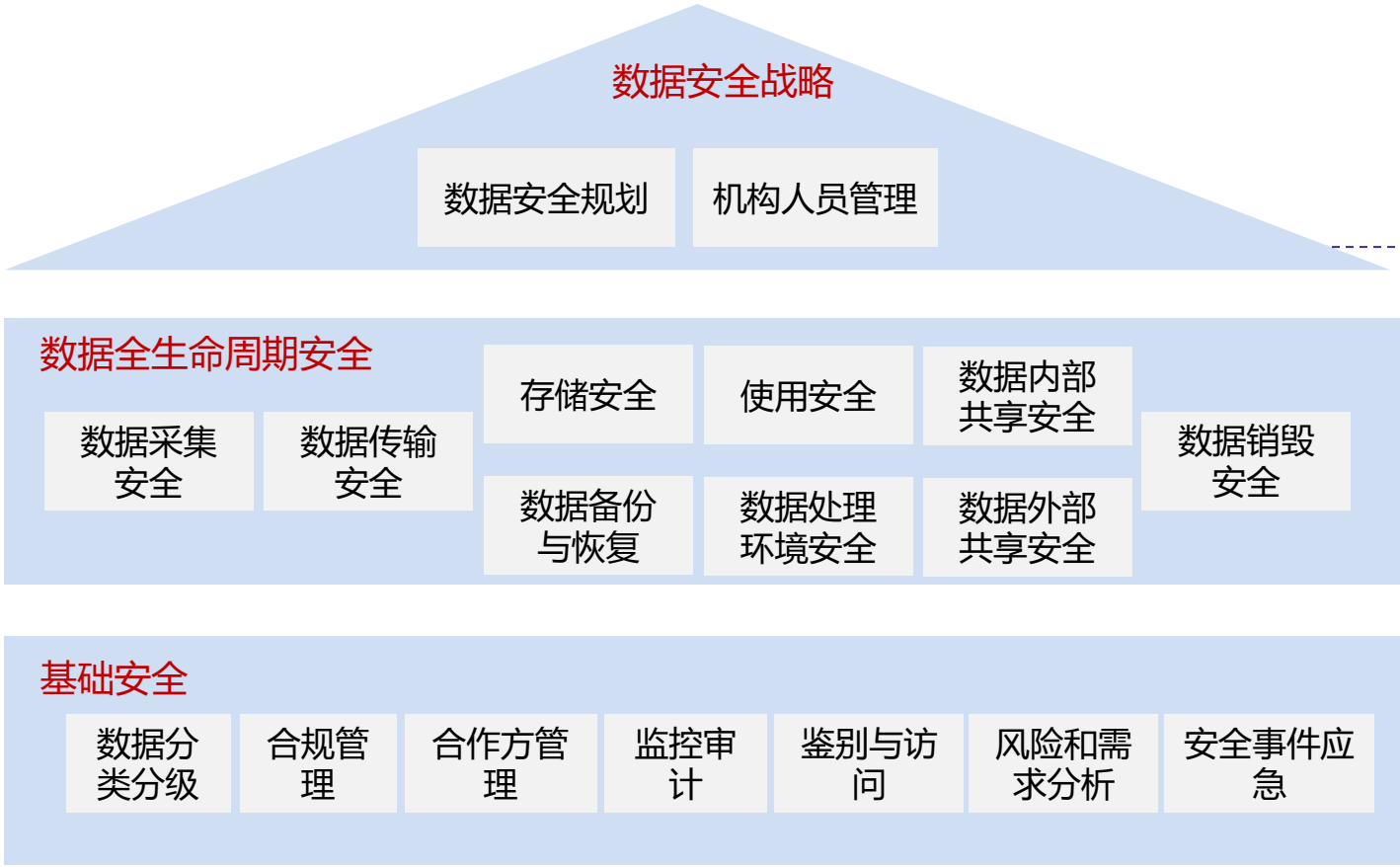
数据安全治理总体视图

◆ 围绕**参考框架**，开展数据安全治理**实践**，在**合规保障和风险管理**的前提下，实现数据的**开发利用**，保障业务的持续健康发展，确保安全与发展的双向促进。



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。
- 直接采用T/ISC-0011-2021《数据安全治理能力评估方法》的治理框架。



从顶层规划方面，**定目标、建团队**

以采集、传输、存储、使用、共享、销毁各个环节为**切入点**，设置**管控点**

是整个治理体系的**通用**要求，能够实现建设资源的**有效整合**

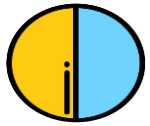
数据安全治理实践路线：治理规划

- 在组织启动数据安全治理工作前，必须制定相应的规划，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紊的展开。

现状分析

外部合规遵从

现状风险分析



行业最佳实践对比

方案规划

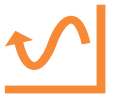
组织机构建设

制度流程建设

技术工具建设

人员能力建设

方案论证



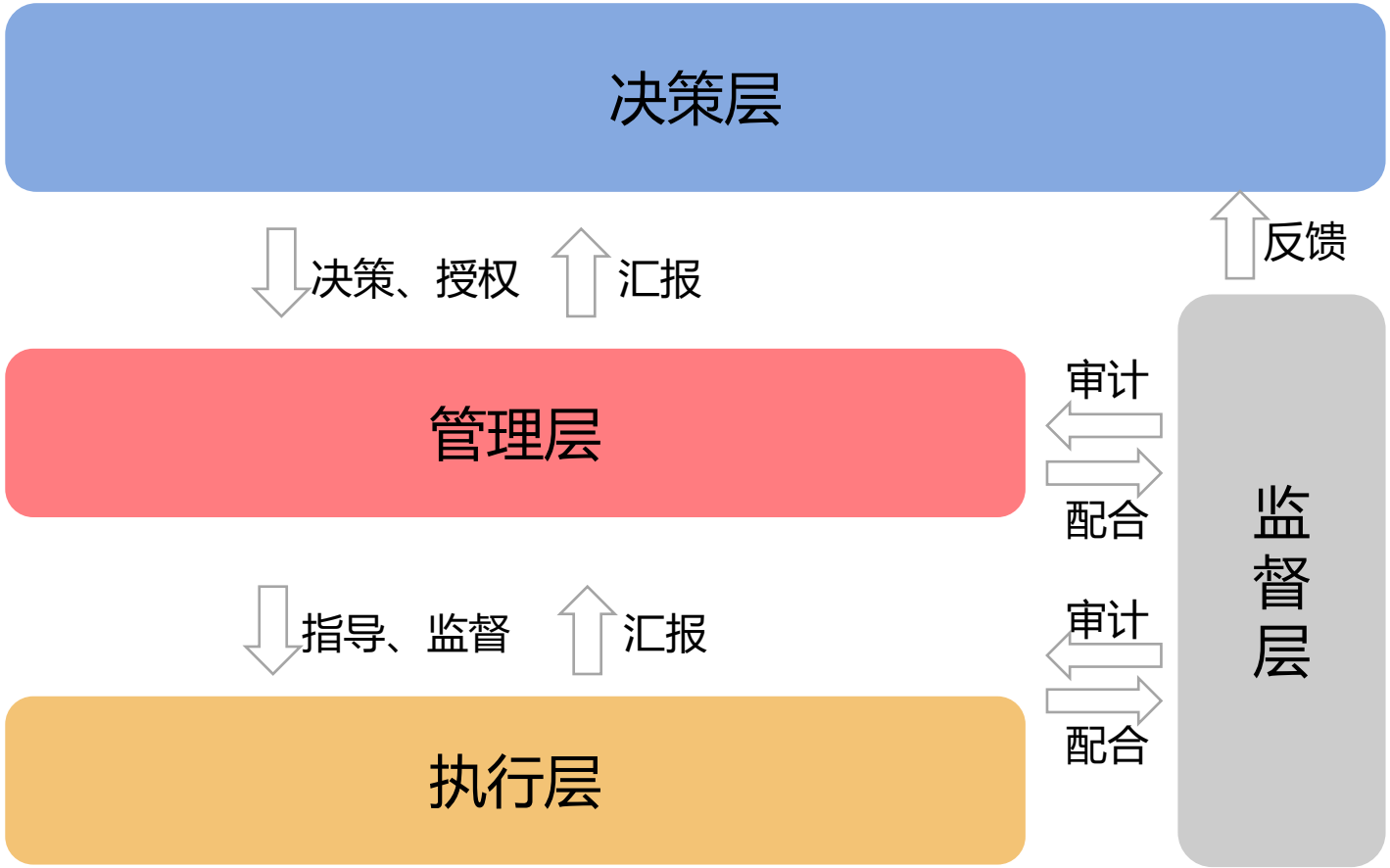
可行性分析

安全性分析

可持续性分析

数据安全治理实践路线：治理建设——组织架构体系

◆ 明晰的组织建设是保障数据安全工作顺利开展的**首要条件**。



数据安全治理实践路线：治理建设——制度流程体系

◆ 制度流程是数据安全**防护要求**、**管理策略**、**操作规程**等的集合。

制度层级	层级作用	制度示例
一级：方针政策	面向组织层面的的方针和总则	《数据安全管理总则》
二级：管理规定	对一级制度的落实	《对外数据输出管理办法》
三级：操作手册	以操作流程或执行指南方式落实二级制度	《传输接口管理细则》
四级：各类表单	三级制度执行中产生的报表、记录、报告等文件	《数据接口清单》

数据安全治理实践路线：治理建设——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**。

数据安全战略

规划管理　　人员管理/考核

数据全生命周期安全

数据采集	数据传输	数据存储	数据使用	数据共享	数据销毁
采集源鉴别 ……	身份鉴别 数据加密 ……	数据加密 备份恢复 ……	数据脱敏 使用授权 ……	共享审批 数据溯源 ……	内容销毁 介质销毁 ……

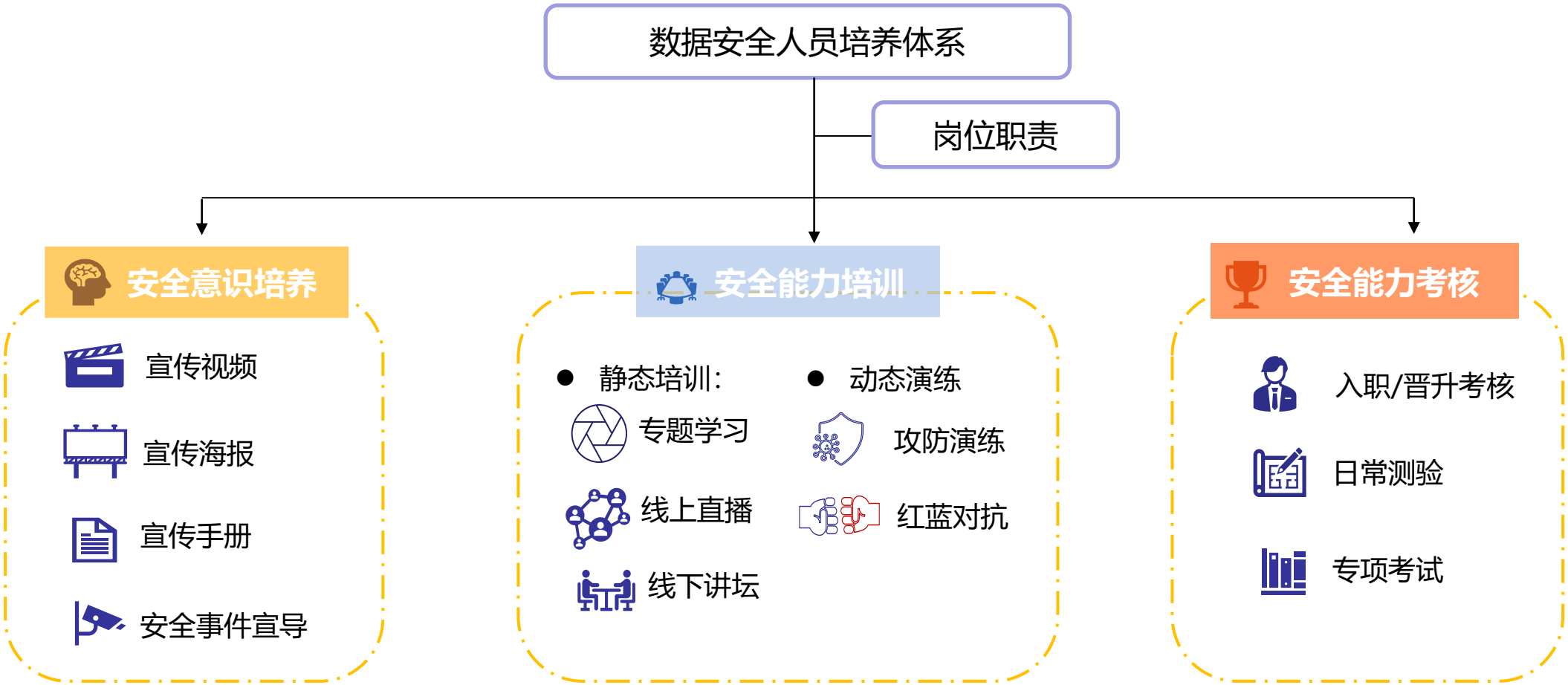
基础安全

数据分类分级　　合规管理　　监控审计　　身份鉴别与访问控制

……

数据安全治理实践路线：治理建设——人员能力体系

◆ 数据安全治理**离不开**相应人员的具体执行，加强对数据安全人才的培养是数据安全治理的应有之义。



数据安全治理实践路线：治理运营

◆ 数据安全治理的持续运营，能够打通各环节的建设内容，促进整个体系的**良性发展**。

风险防范

- **数据安全策略制定**

通用场景 + 个性化场景

- **数据安全基线扫描**

基线梳理及落实

定期扫描

- **数据安全风险评估**

风险评估 → 基线对标 → 方案改进

监控预警

- **态势监控**

通过监控审计平台，及时告警并初步阻断

- **日常审计**

针对账号使用、权限分配、漏洞修复等日常管理进行审计

- **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

应急处理

- **数据安全事件应急处置**

- **数据安全事件复盘整改**

事件分析 → 应急总结 → 预案完善

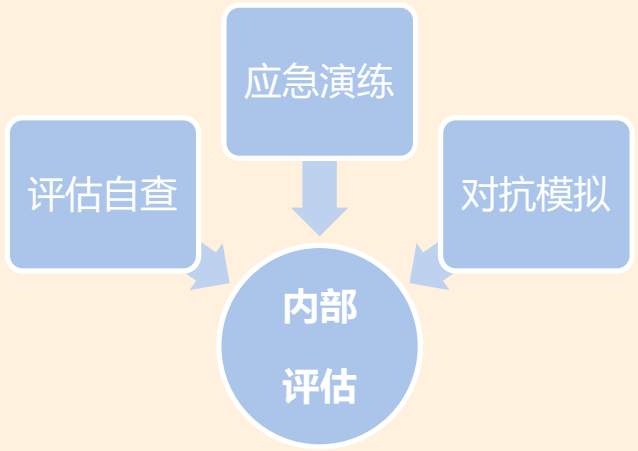
- **数据安全应急预案宣贯宣导**

数据安全治理实践路线：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**。

内部评估

- 应由组织管理层**牵头**，执行层和监督层**配合执行**
- 应将评估结果与组织的绩效考核**挂钩**，避免评估流于形式



第三方评估

- **《数据安全法》**：**支持**专业机构开展数据安全相关**评估认证服务**工作

现状	问题
行业水平参差不齐 度量方法缺失 与监管要求、公众期待尚有差距，缺乏贴近产业现状的指南。	如何让监管放心？ 如何使用户满意？ 如何保数据安全？

数据安全治理能力评估
Data security governance capability evaluation

- **首批参与**企业：百度、蚂蚁、联通数科、电信云、度小满

目录

Contents

数据安全落地存在诸多挑战

◆ 《网络安全法》、《数据安全法》和《个人信息保护法》为行业主管部门的**数据安全监管要求**提供了法律依据，指明了方向，企业侧也将在**数据安全监管应对**上面临**前所未有的挑战**。

法律法规 → **监管实施** → **企业落地实践**

主管部门**监管要求**？

数据安全**审查**制度如何推行？怎样合规？

数据**分类分级**怎么做？

数据安全**治理能力**如何建设、提升、评估？

数据安全**风险监测**如何推进？

数据安全相关**监管应对**？

相关安全**技术**怎样提升？

个人信息保护**影响评估**怎么做？

数据安全**应急**处置如何达标？

数据安全**制度体系**如何建？

数据安全**风险评估**怎么开展？

数据安全整体**解决方案**如何实现？

数据安全，正在形成产业

加解密	密钥管理
数据脱敏	数据审计
数据水印	行为分析
行为画像	内容识别
身份认证	权限管理
数据目录	资产可视化
……	
血缘分析	隐私计算

数据安全技术

各项能力的实现技术

数据安全中心	数据管理工具 数据服务工具
身份管理平台	
数据审计平台	日志审计工具 行为分析
数据加密	
终端防泄漏	堡垒机 数据防泄漏(DLP)
……	
运维服务	

运维服务 + 平台or工具

解决方案的能力

数据安全通用解决方案

解决方案的供给

解决方案

场景 + 需求 → 用户

谢谢！