DISE数智实审

构建合规与风险导向的数据安全审计体系——方法、实践与挑战

演讲人：李松　　日期：2025年8月27日

数字风险赋能中心

数实融合　智审未来!

1 数据安全动态

2 数据安全知识体系

3 数据安全审计实务

4 挑战与展望

01

数据安全动态

1.1 数据安全正式立法

DISE 数智实审

外部合规：“四法四例四规”驱动全行业数据保护

《网络安全法》

第二十一条 国家实行网络安全等级保护制度。其安全保护义务第4条明确采取数据分类、**重要数据备份和加密**等措施。

《密码法》

二十七条 法律、行政法规和国家有关规定要求**使用商用密码进行保护**的关键信息基础设施，其运营者应当使用商用密码进行保护。关键信息基础设施运营者，**应当自行或者委托商用密码检测机构开展商用密码应用安全性评估**。

《数据安全法》

第二十七条　开展数据处理活动应当依照法律、法规的规定，建立健全全流程数据安全管理制度，组织开展数据安全教育培训，**采取相应的技术措施和其他必要措施，保障数据安全。**利用互联网等信息网络开展数据处理活动，应当在网络安全等级保护制度的基础上，履行上述数据安全保护义务。

《个人信息保护法》

第五十一条第三款：采取相应的**加密、去标识化**等安全技术措施；

第六十六条：情节严重的，由省级以上履行个人信息保护职责的部门责令改正，没收违法所得，并处**五千万元以下或者上一年度营业额百分之五**以下罚款……

《网络安全等级保护条例》（征求意见稿）

国家密码管理部门根据网络的安全保护等级、涉密网络的密级和保护等级，**确定密码的配备、使用、管理和应用安全性评估要求**，制定网络安全等级保护密码标准规范。

《关键信息基础设施安全保护条例》

《关键信息基础设施安全保护条例》（国令第745号）规定履行**个人信息和数据安全保护责任**，建立健全**个人信息和数据安全保护制度**。关键信息基础设施中的**密码使用和管理**，应当遵守相关法律、行政法规。

《商用密码管理条例》

《商用密码管理条例》提出法律、行政法规和国家有关规定要求使用商用密码进行保护的**关键信息基础设施，其运营者应当使用商用密码进行保护**。

《网络数据安全管理条例》（征求意见稿）

国家对个人信息和重要数据进行重点保护，对核心数据实行严格保护。数据处理者**应当采取备份、加密、访问控制等必要措施**，保障数据免遭泄露、窃取、篡改、毁损、丢失、非法使用；数据处理者应当**使用密码对重要数据和核心数据进行保护**。

等保

等保2.0建设，结合HVV攻防演练

关保

对关键信息基础设施的增强保护

HVV

密评

政务、等保、关基等领域，落实“密码三同步”

数评

对网络运营者开展数据收集、存储、使用、加工、传输、提供、公开等处理活动进行认证

1.2 国家两会对数据安全持续关注度

DISE 数智实审

2024年3月5日，第十四届全国人民代表大会第二次会议在北京人民大会堂隆重召开，国务院总理李强作《政府工作报告》（以下简称《报告》）。《报告》提出“深入推进数字经济创新发展”“健全数据基础制度，大力推动数据开发开放和流通使用”“以高质量发展促进高水平安全，以高水平安全保障高质量发展”“推动解决数据跨境流动等问题”“提高网络、数据等安全保障能力”“维护国家安全和社会稳定。贯彻总体国家安全观，加强国家安全体系和能力建设”。**数据安全**已经连续四年被写入政府工作报告，不仅体现了国家对**数据安全**的高度重视，更彰显了**数据安全**在国家安全、经济安全以及社会稳定中的核心地位。这也向全社会传递了一个明确的信号：**数据安全**不仅仅是技术问题，更是关乎国家长远发展和人民福祉的重大问题。

关键词概览全国两会政府工作报告

关键词	2021	2022	2023	2024	趋势图
数字	11	12	6	21	
数据	2	5	1	5	
安全	25	15	25	29	
网络	7	5	2	5	

1.3 全国数据工作会议重要指示精神

DISE 数智实审

4月1日，2024年全国数据工作会议在北京召开。会议指出，2024年数据工作要坚持以习近平新时代中国特色社会主义思想为指导，全面贯彻落实党的二十大和二十届二中全会精神，按照中央经济工作会议部署，大力发展新质生产力，坚持稳中求进工作总基调，坚持“一条主线”，统筹“三个建设”，着力健全基础制度、释放要素潜能、加快转型赋能、促进科技创新、完善基础设施、强化安全保障、推进国际合作、抓好试点试验，更好发挥数字化在中国式现代化中的驱动引领作用，奋力开创国家数据工作新局面。

“八要”指示精神

一要健全数据基础制度。
二要提升数据资源开发利用水平。
三要以数字化赋能高质量发展。
四要促进数据科技创新发展。
五要优化数据基础设施布局。
六要强化数据安全保障能力。
七要提升数据领域国际合作水平。
八要发挥试点试验的引领作用。

1.5 数字化伴生数据风险

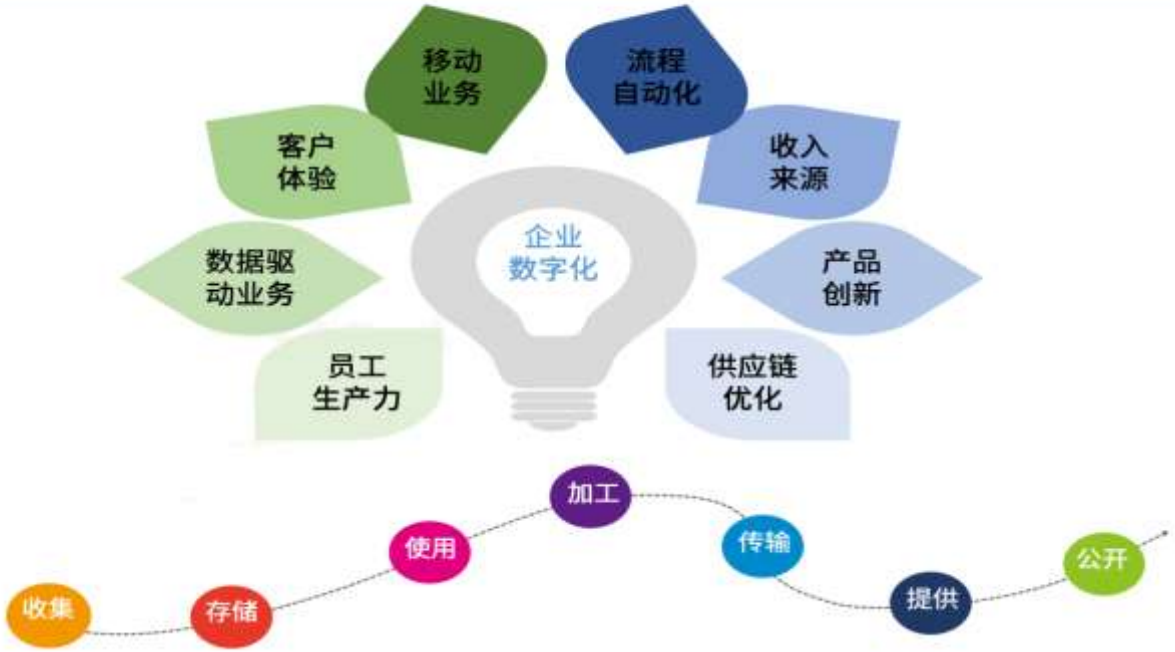
DISE数智实审

企业IT发展进入数字时代

二十大报告提出，“**加快发展数字经济，促进数字经济和实体经济深度融合，打造具有国际竞争力的数字产业集群。**

数据要素是数字经济深化发展的核心引擎。数据对提高生产效率具有乘数作用，数据的爆发增长海量集聚蕴藏巨大价值，用好数据要素将为经济社会数字化发展带来强劲动力。

数据风险：伴生数据处理如影随形



1.6 数据安全事件案例

DISE 数智实审

（一）南昌某高校因 3 万余条师生个人信息数据泄露被罚

案例描述

2023年8月，接到网友举报南昌某高校**3万余条师生个人信息数据**在境外互联网上被公开售卖的消息后，南昌公安网安机构立刻组织人员展开调查，最终成功抓获犯罪嫌疑人3名。同时，公安机关对涉案高校不履行数据安全保护义务违法行为开展执法检查。

问题分析

涉案高校在开展数据处理活动中，**未建立全流程数据安全管理制度，未采取技术措施以保障数据安全，未履行数据安全保护义务**，导致学校存储教职工信息、学生信息、缴费信息等 3000 余万条信息的数据库被黑客非法入侵，其中 3 万余条教职工、学生个人敏感信息被非法兜售。

1.6 数据安全事件案例

DISE 数智实审

（二）银行600余万条个人信息遭某微信代理商泄露

案例描述

某微信代理商为多家银行提供企业微信相关服务，将银行客户经理和客户的聊天会话存档在该服务商租用的公有云服务器上，会话存档数据包含部分**客户姓名、身份证号、 手机号、银行账号**等敏感个人信息。未经银行同意，该服务商私自使用数家银行**600余万条**会话存档数据用于该公司模型训练，并提供给关联公司。银行因未尽到对客户敏感数据保护责任，引发消费者维权投诉。

问题分析

一是银行机构对**数字生态场景合作情况底数不清，缺乏统筹管理**。开展数字生态合作时，风险部门、科技部门和数据管理部门均未参与，缺乏数据安全风险评估、数据安全风险监控等机制，存在突出风险隐患。

二是银行对合作中数据安全风险和责任识别划分不清，存在**数据收集使用不合规、安全责任交叉、数据保护存在盲区**等问题。

02

数据安全知识体系

2.1 什么是数据安全

DISE 数智实审

《数据安全法》第三条数据安全，是指通过采取必要措施，确保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。

《数据安全法》第四条维护数据安全，应当坚持总体国家安全观，建立健全数据安全治理体系，提高数据安全保障能力。

我国是数字经济大国，正在积极建设数字中国，推动数字经济高速发展，数字经济发展对数据安全提出新要求。当前，随着大数据、人工智能、区块链等技术应用，经济社会发生系统性变革，驱动我国加速迈入数字新时代。党的二十大报告中多次提及“数字”领域关键词，部署了加快发展数字经济、打造具有国际竞争力的数字产业集群、推进各领域数字化等一系列重大任务和重要举措，对建设数字中国提出了新的要求。同时，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首要位置。

2023年2月，中共中央、国务院印发《数字中国建设整体布局规划》(以下简称《规划》)。《规划》明确，数字中国建设需按照“2522”框架进行总体布局，即夯实“数字基础设施”和“数据资源体系“的两大基础体系，推进落实”数字技术与经济、政治、文化、社会、生态文明建设“五位一体重要举措，强化”数字技术创新体系“和”数字安全屏障“的两大技术能力，优化数字化发展“国内”、“国际”的两个环境，并对数据安全能力提出了“筑牢可信可控的数字安全屏障“全面要求。

同年，工业和信息化部等十六部门发布的《关于促进数据安全产业发展的指导意见》也提出了推动数据安全产业高质量发展，全面加强数据安全产业体系和能力，夯实数据安全治理基础，促进以数据为关键要素的数字经济健康快速发展的指导要求。

2.2 数据安全普遍“痛点”

DISE 数智实审

对数据安全重视不足

缺少数据安全顶层设计，缺少数据安全专职部门和人员。

尚未形成数据安全体系

数据安全不成体系，仅部署数据安全工具，缺少流程和工具。

数据安全的制度不落实

制度建设与实际落实脱节。

数据分类分级不明确

缺少有效的分类分级方法，部分方法冲突，结果不准确。

数据安全未形成生命周期机制

未从数据安全的全生命周期进行管控，部分管理缺位。

数据安全技术防护不到位

缺少技术防护手段，导致数据泄露、数据丢失事件频发。

2.3 数据安全的核心价值

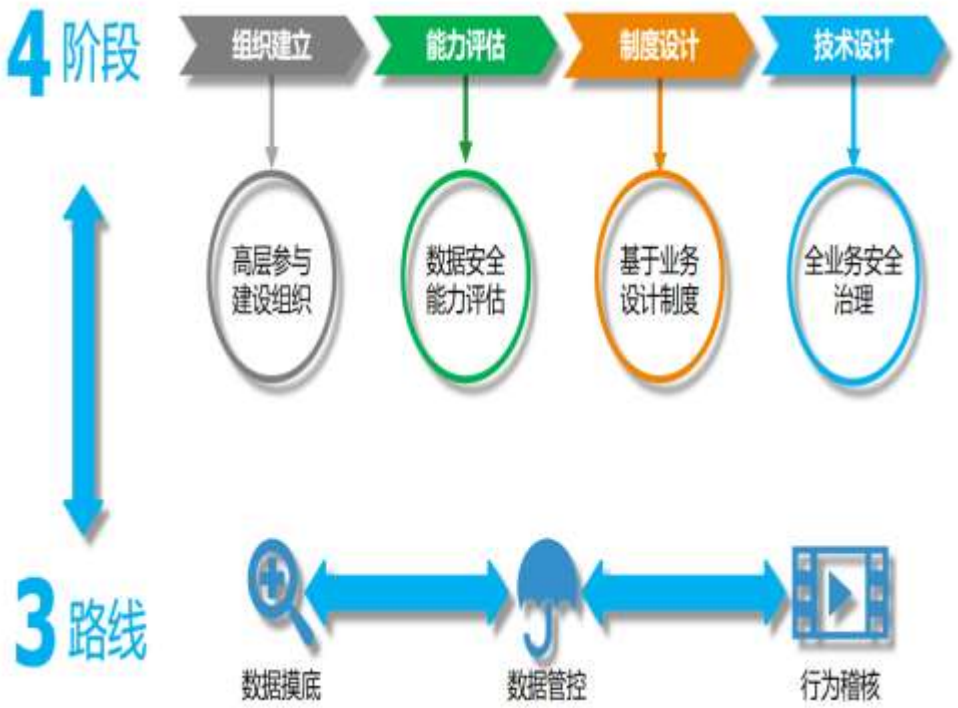
2.4 数据安全相关法律、规范、标准

DISE 数智实审

序号	政策或标准名称
1	中华人民共和国网络安全法
2	中华人民共和国数据安全法
3	中华人民共和国个人信息保护法
4	关键信息基础设施安全保护条例
5	网络安全审查办法
6	数据出境安全评估办法
7	关于促进数据安全产业发展的指导意见
8	信息安全技术 数据安全能力成熟度模型
9	信息安全技术 大数据安全管理指南
10	信息安全技术个人信息安全规范
11	信息安全技术 健康医疗数据安全指南
12	信息安全技术 网络数据处理安全要求
13	信息安全技术 电信领域数据安全指南
14	信息安全技术 网络数据分类分级要求
15	信息安全技术 政务信息共享 数据安全技术要求
16	信息安全技术 物联网数据传输安全技术要求
17	信息安全技术 个人信息安全影响评估指南
18	信息安全技术 个人信息去标识化指南
19	中国人民银行-个人金融信息保护技术规范
20	中国人民银行-金融数据安全 数据安全分级指南
21	中国人民银行-金融数据安全 数据生命周期安全规范
22	中国人民银行网络数据安全管理指南
23	中国人民银行-金融业数据能力建设指引
24	中国人民银行金融消费者权益保护实施办法

序号	政策或标准名称
25	中国银保监会监管数据安全管理办法(试行)
26	银行保险机构消费者权益保护管理办法
27	证券期货业数据分类分级指引
28	证券期货业数据安全管理与保护指引
29	证券期货业数据安全风险防控　数据分类分级指引
30	证券期货业网络和信息安全管理办法
31	生成式人工智能服务管理暂行办法
32	基础电信企业数据分类分级方法
33	电信和互联网用户个人信息保护规定
34	工业和信息化领域数据安全管理办法（试行）
35	工业数据分类分级指南（试行）
36	个人信息跨境处理活动安全认证规范
37	民用航空空中交通管理管理信息系统技术规范 第7部分：数据安全
38	医疗卫生机构网络安全管理办法
39	汽车数据安全管理若干规定(试行)
40	车联网信息服务数据安全技术要求
41	移动互联网应用程序信息服务管理规定
42	App违法违规收集使用个人信息行为认定方法
43	常见类型移动互联网应用程序必要个人信息范围规定
44	中国人民银行业务领域数据安全管理办法（征求意见稿）
45	银行保险机构数据安全管理办法-征求意见稿
46	网络数据安全管理条例（征求意见稿）
47	移动互联网应用程序个人信息保护管理暂行规定（征求意见稿）
48	个人信息保护合规审计管理办法（征求意见稿）

2.5 数据安全治理现状评价

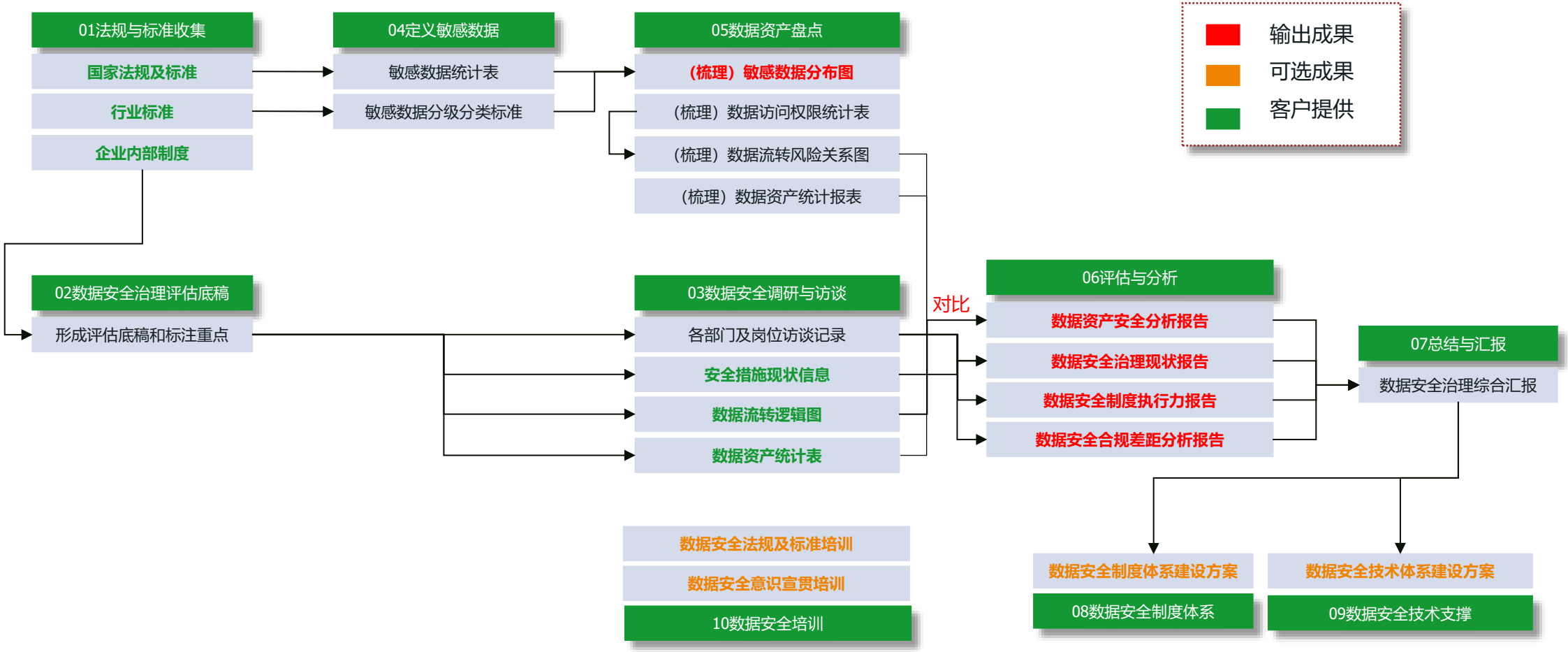


序号	评分项	标准分	权重	评估得分	综合得分
1	数据安全治理组织架构	100	0.05		
2	数据安全管理职责	100	0.05		
3	数据安全管理制度体系	100	0.08		
4	数据采集管理	100	0.08		
5	数据传输管理	100	0.08		
6	数据存储管理	100	0.08		
7	数据使用管理	100	0.08		
8	数据删除管理	100	0.08		
9	数据销毁管理	100	0.08		
10	数据安全运行管理	100	0.05		
11	数据安全策略	100	0.03		
12	数据安全访问控制	100	0.05		
13	数据监控与审计	100	0.05		
14	数据安全检查和评估	100	0.05		
15	数据安全事件处置	100	0.03		
16	数据安全治理工具	100	0.08		
总计			1		

主要关注风险或不足：

1）数据安全缺少成熟度级别　2）数据安全管理与技术脱钩

2.5 数据安全治理现状评价



2.6 数据安全组织建设

数据安全组织架构可按照决策层、管理层、执行层、监督层的组织架构设计。在具体执行过程中，组织也可赋予已有安全团队与其它相关部门数据安全的工作职能。

主要关注风险或不足：

1）未以正式文件明确数据安全负责人、管理机构及管理职责

2）未建立数据安全组织架构

3）数据安全委员会履职不充分

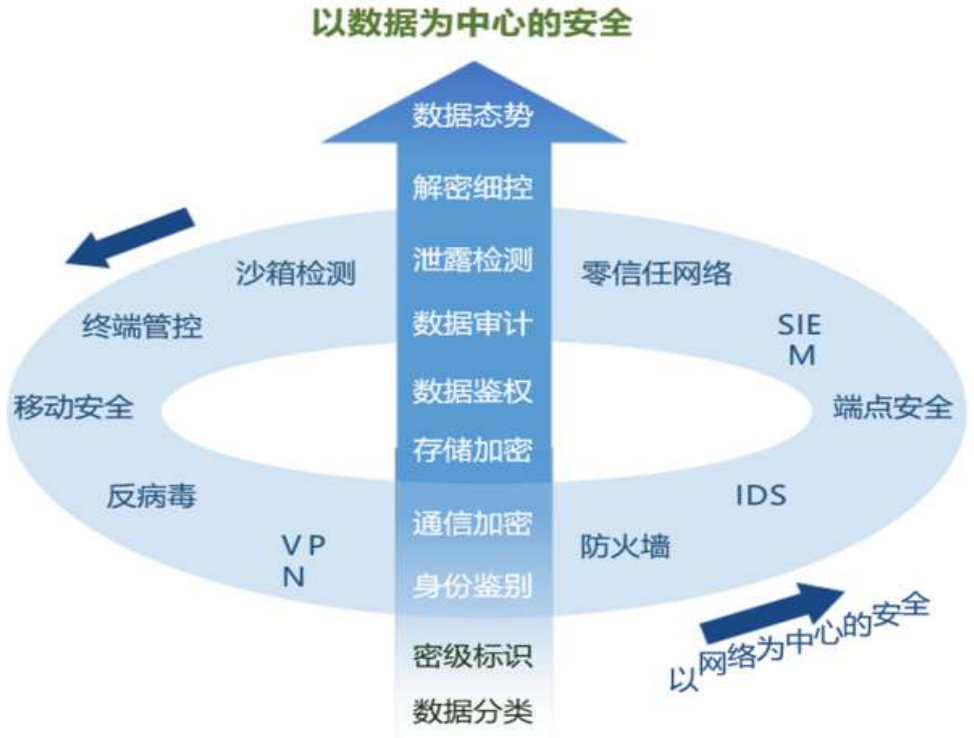
4）高管层对数据安全重视程度不足

5）数据安全缺少高管层有效推动

6）数据安全主管部门工作落实不到位

7） 未开展数据安全教育培训，或培训缺少过程记录

2.7 数据安全规划



网络与数据并重的新安全建设理念

基于网络安全与数据安全并重的建设理念，结合业务应用场景，聚焦“以数据为中心”、“以网络为中心”的双线安全建设思路，企事业单位可结合自身组织使命和业务价值，进行与组织特色匹配的数据安全治理顶层设计，构建有效的数据安全防线。

2.7 数据安全规划

数据安全规划发展蓝图

主要关注风险或不足：

1）数据安全顶层规划不明确

2）数据安全规划内容不全面，如缺少愿景、蓝图和具体任务。

3）数据安全规划未发文（未有效传达）

4）数据安全规划缺少任务分解及落地分工

2.8 数据安全制度体系建设

主要关注风险或不足：

1）数据安全制度体系不完善或不健全，如缺少数据分类分级管理办法、数据生命周期管理制度、数据访问管理制度等

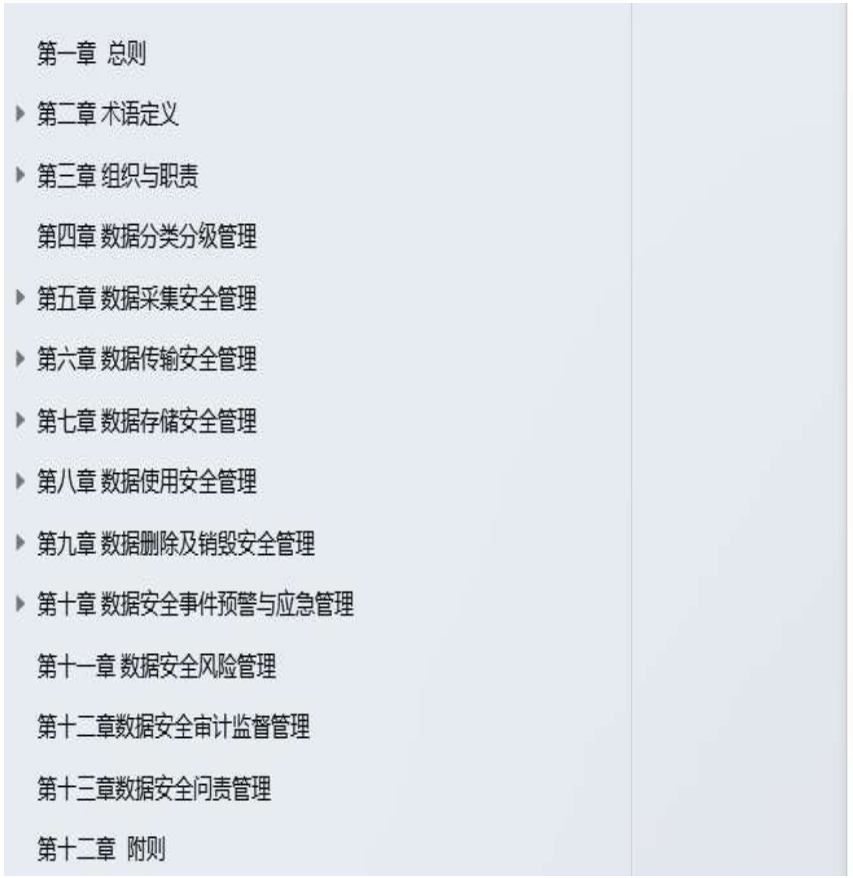
2）XXX制度与XXX制度存在冲突矛盾

3）XX制度、XX制度落实不到位

4）XX制度内容与实际情况不匹配

2.8 数据安全制度体系建设

DISE 数智实审



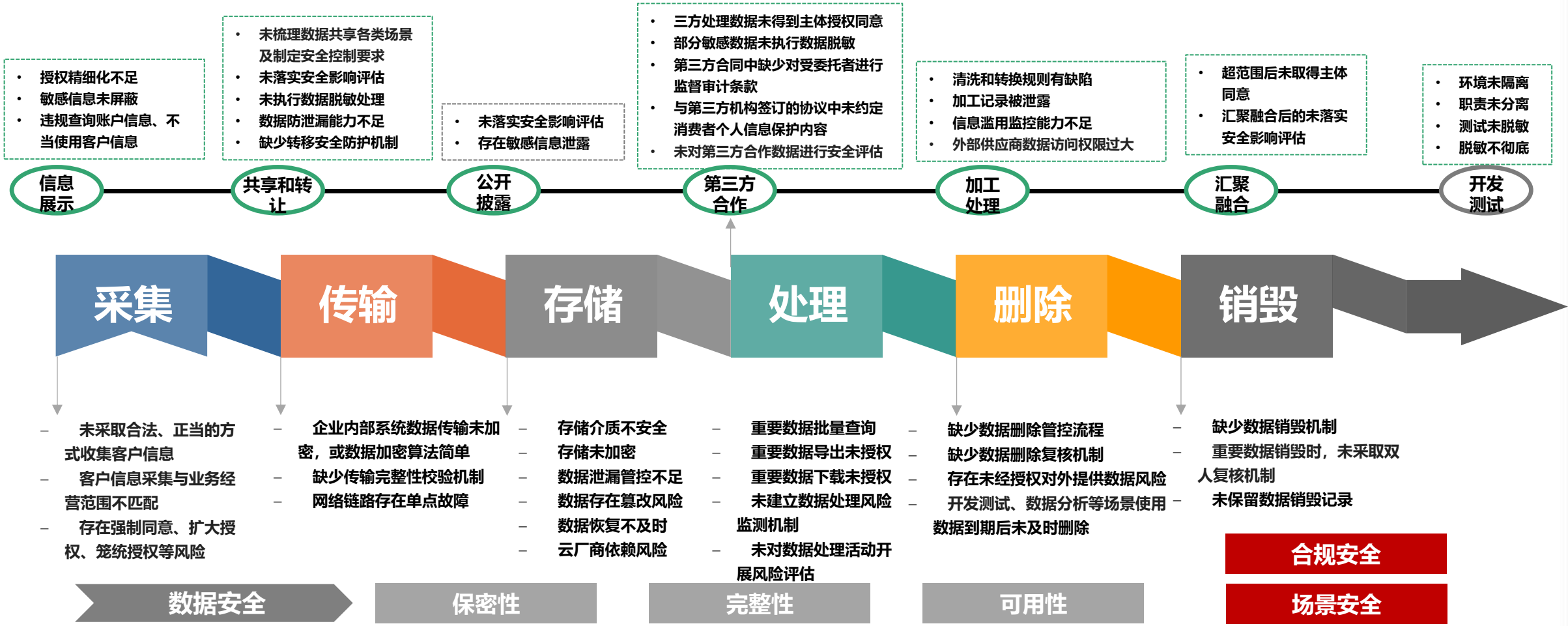
XX 企业

数 据安全管理办法

数据管理部

2.9 数据生命周期安全建设

DISE 数智实审



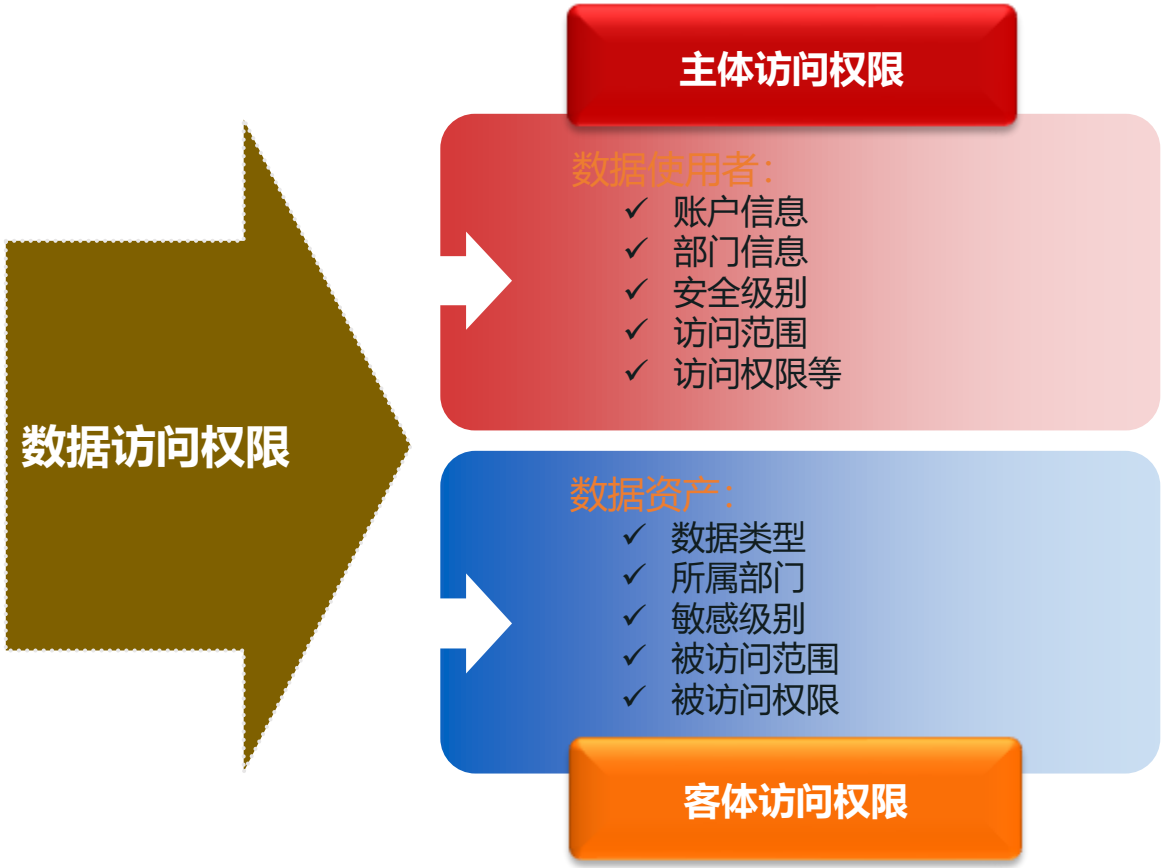
2.10 数据访问管理

DISE数智实审

凡是有处理数据的业务场景
就会存在风险，也就有了数据安全

分类	关注异常行为	影响分析
异常的查询频率	一段时间内重复查询客户信息几百次	高
	一个号码一天内被查询10次以上，或一个月内被查询100次以上	中
	某些特殊号码被多次查询，例如吉祥号	中
帐号异常	长时间不登陆的帐号登陆使用，查询敏感信息	低
	同一个帐号被多个人员使用，同时登陆或登陆IP地址经常变化。	中
异常的修改频率	一段时间内修改客户信息几百次	高
	单号码信息一天内被修改10次以上，或一个月被修改100次以上	中

2.10 数据访问管理



数据访问权限也是数据安全关注重点内容之一，需根据角色不同进行数据合理授权访问和使用。

主要关注风险或不足：

1）业务人员合理授权

2）客服人员合理授权

3）开发测试人员合理授权

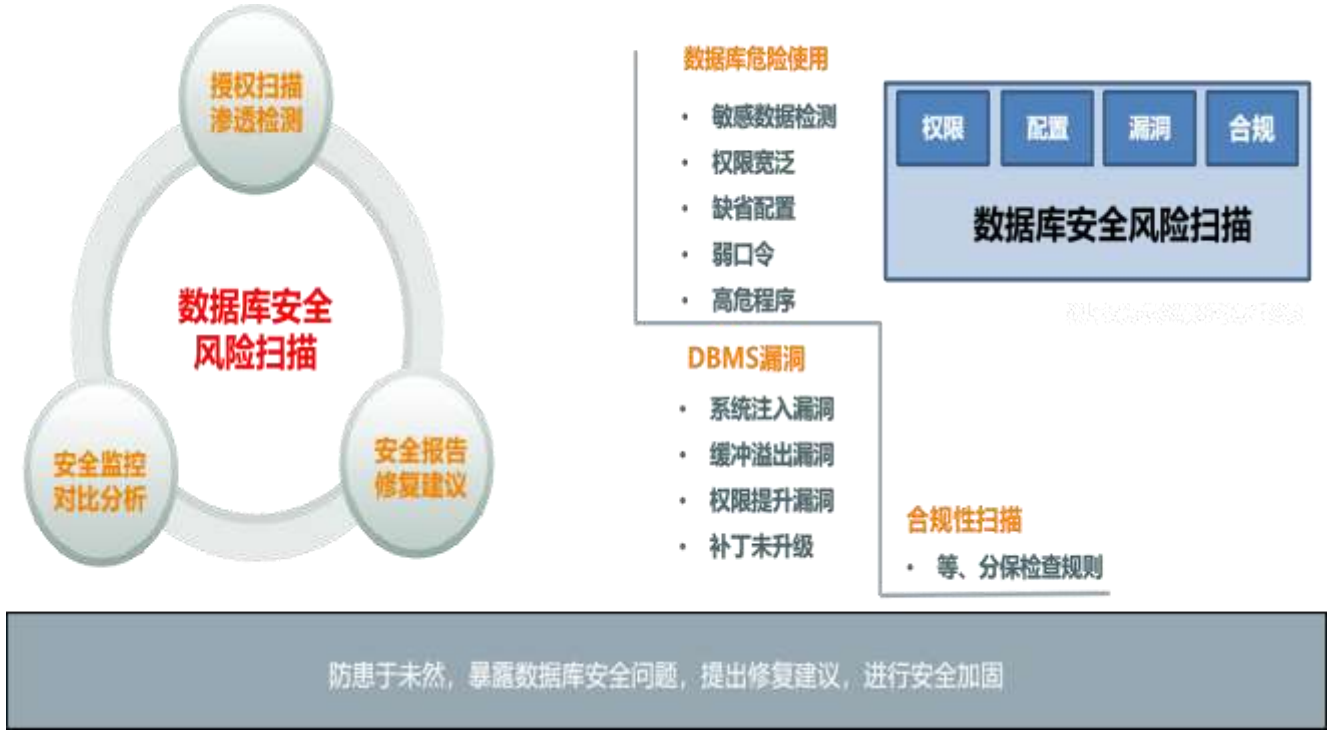
4）外包人员合理授权

5）运维人员合理授权

6）数据分析人员合理授权

7）集中存储数据的系统合理授权

2.11 数据安全技术测试



通过对数据库进行扫描和渗透测试，以发现其中存在的数据安全漏洞和风险隐患。

主要关注风险或不足：

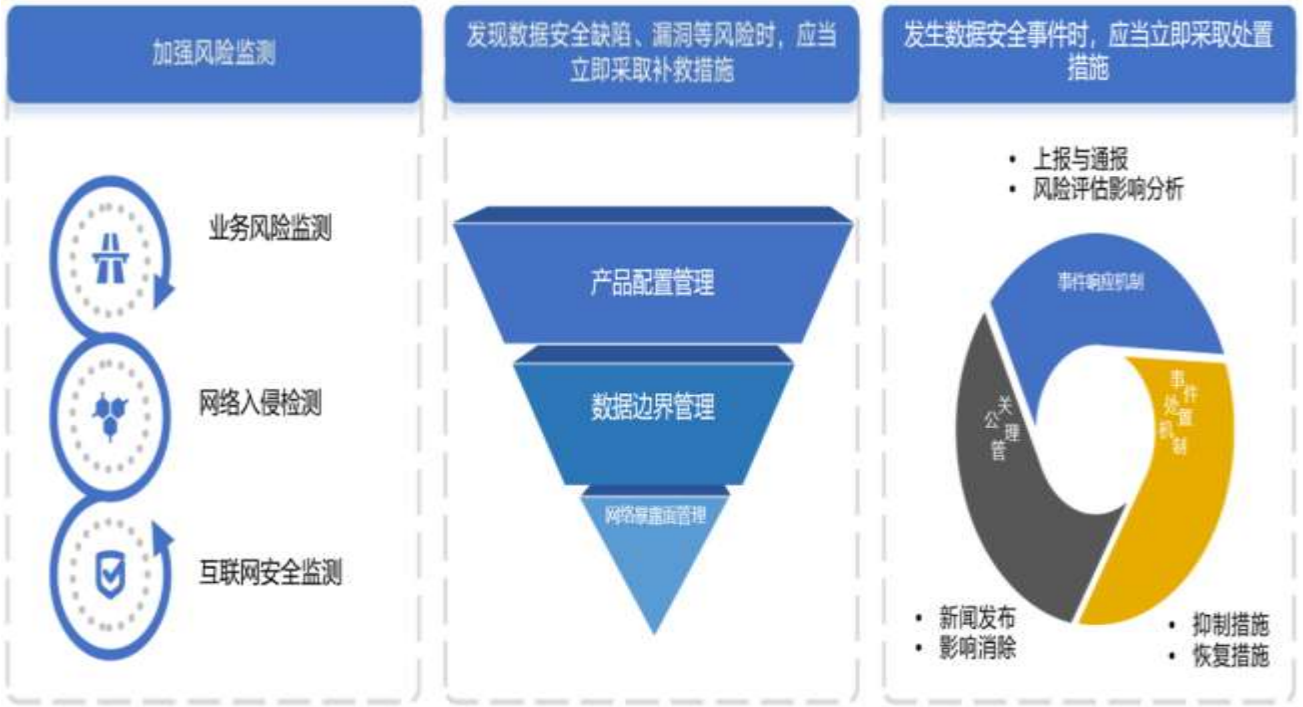
1）数据库未定期执行安全漏洞扫描

2）发现问题未及时进行加固

3）加固后的数据库未及时进行复测

4）缺少数据库安全测试报告

2.12 数据应急管理



数据安全风险监测、数据安全缺陷及漏洞修复、数据安全事件处置等对于数据安全应急管理至关重要。

主要关注风险或不足：

1）未形成数据安全风险监测机制

2）数据安全风险监测指标不完善

3）缺少数据安全风险监测或科技风险监测报告

4）未制定数据应急预案

5）数据应急预案场景不完善

6）未实施数据应急演练

7）数据应急演练缺少记录及总结报告

2.13 数据安全技术

DISE数智实审

（1）数据脱敏

数据掩码

1.基本解释：它通过替换或掩盖真实数据来提供一种安全层，使原始数据即使在非安全环境中也能保持机密性。

2.典型应用：在开发和测试环境中，为了模拟真实环境而需要用到生产数据时，可以通过数据掩码技术对诸如信用卡号、身份证号、电话号码等敏感字段进行遮蔽处理，例如：

1）**信用卡号**：中间部分替换为固定字符或随机数字
6225760083037090 ➡ 6225**********7090

2）**手机号**：显示前 1/3 和后 1/3（向下取整），其他用*号代替
13789709050 ➡ 137****9050

3）**身份证号**：使用缺省信息隐藏规则，如隐藏出生日期或身份证号码屏蔽后 6 位
230104198609261915 ➡ 230104198509******或 230104******1915

4）**电子邮箱**：@前面的字符显示前 3 位，3 位后显示 3 个*，@后面完整显示
zhichao@163.com ➡ zhi***@163.com

2.13 数据安全技术

DISE 数智实审

（1）数据脱敏

数据伪装

1.基本解释：数据伪装与数据掩码相似，但更加注重混淆数据的外观以增加破解难度，而不是简单的替换或屏蔽。

2.典型应用：

1）攻击路径不存在：若攻击者试探某个网站的数据库路径，可以通过“错误重定向”方法把详细错误信息用某些固定的代码替换掉，这样攻击者就无法知道详细错误信息和数据库结构和路径。

2）大数据研究：医疗研究机构在分享临床试验数据时，可以通过数据伪装技术改变患者的年龄、性别、地理位置等细节，但仍保留疾病分布和治疗效果的相关性，保障数据可用的同时保护了参与者的隐私

姓名	身份证号	手机号
贺辉	432503198706225063	13101752976
吴燕梅	369020199204247828	13200532663
蒲孝容	511023198608131861	18500185539
陈双清	430381199003102623	13202927715

部分替换

脱敏

姓名	身份证号	手机号
韩沿	432503196508127267	13101278126
傅彤	369020197810245325	13200192263
高翔	51102319810630196X	18500534718
贾华	430381196905086129	13202725549

2.13 数据安全技术

DISE 数智实审

（1）数据脱敏

数字水印

1.基本解释：是一种将信息（如标识符、作者信息、版权声明等）以几乎不可察觉的方式嵌入到数字媒体（如图像、音频、视频或文档）的技术。

2.典型应用：

1）**在企业环境中：**对内部文档、屏幕显示等数据进行动态数字水印处理，可以有效防止员工泄密，并在发生泄密时通过水印快速定位信息来源。

2）**在影视行业中：**好莱坞电影公司常常在影院上映前预先发送给院线的影片中嵌入不可见的数字水印，一旦在网络上出现非法泄露的副本，通过分析水印就能追踪到最初的泄露源头，进而采取法律行动打击盗版行为。

动态水印溯源

1、**水印生成与嵌入：**动态水印首先需要在数据分发或使用过程中实时生成。这通常涉及到根据特定的策略（如用户身份、访问时间、地理位置等）生成唯一的、不可预测的水印信息。将此水印信息以某种方式隐秘地嵌入到原始数据中，原始数据包括：图像、音频、视频、文本、表格等。

2、**数据传播与监测：**数据一旦嵌入了动态水印后，随着数据在网络中流通、下载、复制或分享，水印也会随之传递。安全管理系统会对数据的流转情况进行监控，比如通过网络爬虫、内网审计、日志记录等方式收集可能泄漏的数据样本。

3、**水印提取与分析：**当疑似泄露的数据被发现时，通过专门的水印检测算法或工具，可以从数据中提取出隐藏的水印信息。分析提取出的水印内容，可以揭示出诸如使用者的身份标识、访问时间戳、授权级别等相关信息。

4、**追溯与定位：**根据水印中携带的信息，可以准确追溯到数据泄露发生的环节，如哪个用户在何时通过何种途径获取了这份数据。如果水印设计得足够安全可靠，还能帮助确定数据是否被篡改，以及泄露路径的细节。

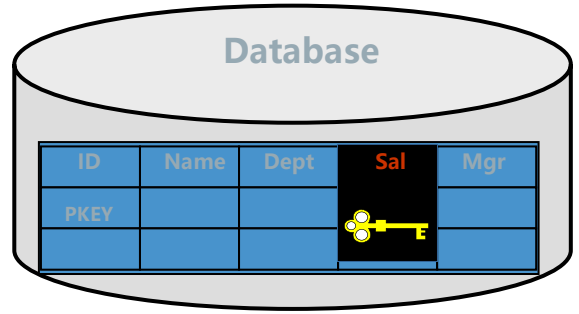
2.13 数据安全技术

DISE数智实审

（2）存储加密

存储加密

- 以列为单位有选择的进行加密
- 支持各种常用数据类型
- 每个加密列拥有唯一的密钥
- 随机盐进行密文扰乱
- 国家自主加密设备和加密算法



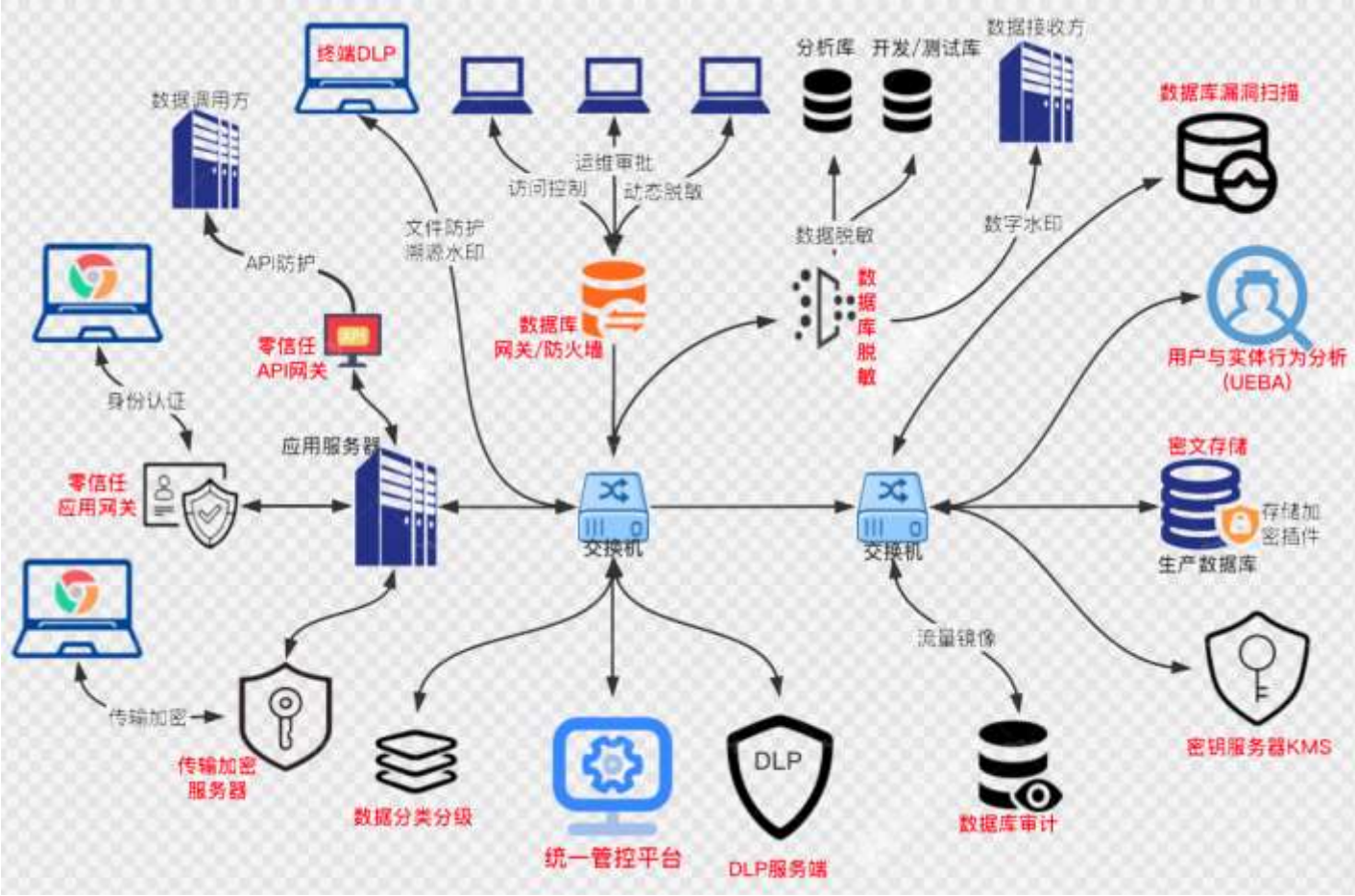
	PID	PERSIONID	DATEFIELD	NAME
1	979	43092719811026091[illegible]	1982/5/9 4:52:52	李其淑
2	980	430972197810265958	2005/4/4 3:15:15	徐秀娥
3	981	430769197411151741	2008/3/15 14:38:38	刘利霞
4	982	430958198908083955	1978/1/17 0:48:48	王爱萍
5	983	430106198211152077	1987/10/14 9:57:57	张莉
6	984	430312199310029294	1970/5/13 16:40:40	邢宪梅
7	985	430164198309130146	1994/1/21 0:24:24	孙青
8	986	430010197508206985	1998/1/17 12:48:48	韩爱玲
9	987	430331198705251303	2009/4/28 15:39:39	王洪爱
10	988	430326197009172306	1990/1/1 12:00:00	方庆莲
11	989	430281200412120254	1993/4/8 15:03:03	方荣

加密前

	PID	PERSIONID	DATEFIELD	NAME
1	979	bNGDR2[illegible]X6Pq9He+8wR4CYFGuQw3jdpxbd+frXL5mVQvbhHrg	1982/5/9 4:52:52	du207Tq8Wb4Z4OBeT33nFrdGuBFJg
2	980	UzBMWADxufOE27qgJgDoY+8vfJLuK9mlltbCDNwMz5FQvbgPC	2005/4/4 3:15:15	pqQC68yH3DUmmlUtdtORZ7dGuHQWg
3	981	awBPS8t+OJzKqsVOcVFMMBXD6TyMRpkqRL4rkh7TWI1QvbjA	2008/3/15 14:38:38	Pxu0LQks6gtD1/SqTVeZC7dGuBC5g
4	982	ju6HZtb0j+WKwVOgBOmUR6ll6XwO8cseHgS9eVHLIFRQvbjFk	1978/1/17 0:48:48	JPb1/69ARMVwO3HRuP2MRbdGuCIEg
5	983	iQ9KLrdW8l7urHyWzZfiT8+DVyGoZxUGflV28bNCL3JQvbj+qQ==	1987/10/14 9:57:57	KwP3LFC33wxX9ZSmlxsq9bdGuMclg
6	984	5p5FSqwsfKkeHkBPqF7sM/1ASdDRrz2v6HaXdn8+/mVQvbgBr	1970/5/13 16:40:40	Pwh+yZ25F9DEUQQKgyxSNLdGuJlVg
7	985	8zACepVK90WQC+5GzylJQFrolnvVd+y2fdv7iZ3omRRQvbhpvQ	1994/1/21 0:24:24	iZiixOUf+dG/JT4SWES7grdGuOW/g
8	986	nlqsHKK08qdL2yvQuAdl3DGGzGY5tuM8Ebmbn9b8RSlQvbiFVg	1998/1/17 12:48:48	4+KHx430YqJyB4V/DrhLZbdGuBVwg
9	987	m0j3MqbO92DiZlXnumxB4BezsNzsFYDekn4sH3jBE3lQvbiwAQ=	2009/4/28 15:39:39	HeoyXhnhHq9pyL0Pk3O8SLdGuERcg
10	988	DxrkUrw/RdfgQC6Gc7tuAE5ysXiPxXRGMMjgnE/0ushQvbiJzA==	1990/1/1 12:00:00	khEamlg1cwLe9C5W3S11ybdGuG4Zg
11	989	gEJaTOH/yXG9SjwwT8Vv/e95CqawXwvbXmOlypDoGdQvbj4M	1993/4/8 15:03:03	XQG5g4V/C9biFwrtetpW1bdGuBJ8g

加密后

2.14 数据安全工具



1、堡垒机
2、桌面管控系统
3、统一备份系统
4、分布式数据保护系统
5、数据库加密系统
6、数据库防火墙
7、数据水印系统
8、数据管控平台
9、数据脱敏系统
10、数据防泄露系统（终端、邮件）
11、数据库审计系统
12、用户行为分析系统
13、隐私计算平台
14、安全运营平台（SOC）
15、漏洞安全扫描系统
16、企业数据库系统
17、企业APP（个人信息保护）
18、相关业务系统
19、……

审计定义角色

审计定义

审计是系统化评估组织数据安全措施的过程。

内部审计与外部审计

内部审计侧重于组织内部的自我评估，外部审计则由第三方进行。

数据安全审计目标与原则

目标是确保数据安全，原则包括合规性、保密性、完整性和可用性。

DISE数智实审

数据安全审计实务

数字风险赋能中心

数实融合　智审未来!

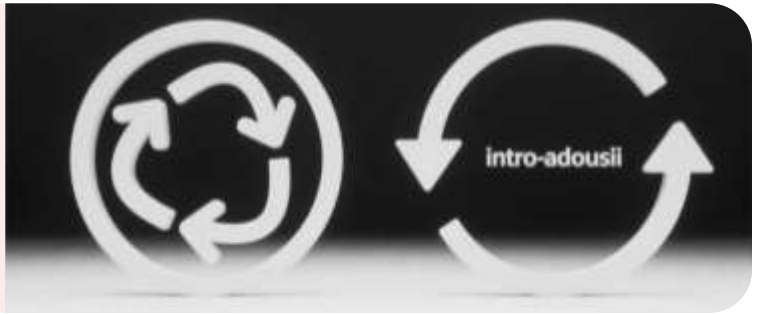
审计定义角色

审计定义

审计是系统化评估组织数据安全措施的过程。

内部审计与外部审计

内部审计侧重于组织内部的自我评估，外部审计则由第三方进行。



数据安全审计目标与原则

目标是确保数据安全，原则包括合规性、保密性、完整性和可用性。

关键概念解析

“三横三纵”审计框架

框架包括治理层面的组织与职责、制度与流程、合规与审计，以及技术与操作层面的数据生命周期、技术控制、操作执行。

PDCA循环应用

PDCA循环是审计中用于持续改进的模型，包括计划、执行、检查和行动四个阶段。

治理角度的三横

组织与职责

责任体系建立，确保高层管理支持。

制度与流程

政策制定与执行，管理数据生命周期。

合规与审计

遵循法律法规，建立持续改进机制。

管理和实施层面的三纵

数据生命周期

涵盖数据采集、存储、使用、共享、销毁。

技术控制

实施访问控制、加密技术、日志审计。

操作执行

包括日常运维、应急响应、第三方管理。

Plan阶段

目标

确立数据安全的领导机构与责任体系。

核心任务

成立数据安全领导小组（由法定代表人或高管牵头）。
任命数据安全官（DSO）或数据保护官（DPO）。
明确各部门（IT、法务、业务、人力）的数据安全职责。

Do阶段

控制措施部署

实施阶段，部署必要的数据安全控制措施。

培训与意识提升

通过培训提高团队对数据安全的认识和技能。

Check阶段

内部监控与外部审计

监控阶段，执行内部监控和外部审计活动。

问题发现与记录

检查阶段，发现并记录审计过程中遇到的问题。

Act阶段

整改计划制定

根据检查结果，制定并执行整改计划。

持续改进与反馈

实施改进措施，并建立持续改进与反馈机制。

云环境泄露审计

事件还原与根本原因分析

通过详细回顾云环境数据泄露事件，分析导致泄露的根本原因。

整改建议与成效评估

提出针对性的整改建议，并对实施后的效果进行评估。

API接口滥用审计

行为分析与权限审查

分析API接口被滥用的行为模式，审查相关权限设置。

技术加固与流程优化

通过技术手段加固API安全，并优化相关操作流程。

04

挑战和展望

主要挑战

数据安全审计中遇到的主要挑战

在数据安全审计过程中，企业会面临各种挑战，如数据量巨大、审计资源有限、技术更新迅速等。

新兴技术影响

新兴技术对数据安全审计的影响

新兴技术如AI、区块链等对数据安全审计产生了深远影响，它们改变了数据处理方式，也对审计工具和方法提出了新的要求。

未来发展趋势

对数据安全审计发展趋势的预测

随着技术的发展和数据安全威胁的增加，数据安全审计将更加注重自动化、智能化，同时，对审计人员的专业能力要求也将更高。

结语

强调重要性

数据安全审计的重要性

数据安全审计对于组织的保护至关重要，能够帮助组织应对数据泄露事件，满足法规遵从性要求。

数据安全审计的必要性

数据安全审计是提升组织数据安全保障能力，构建系统化审计框架的必要手段。

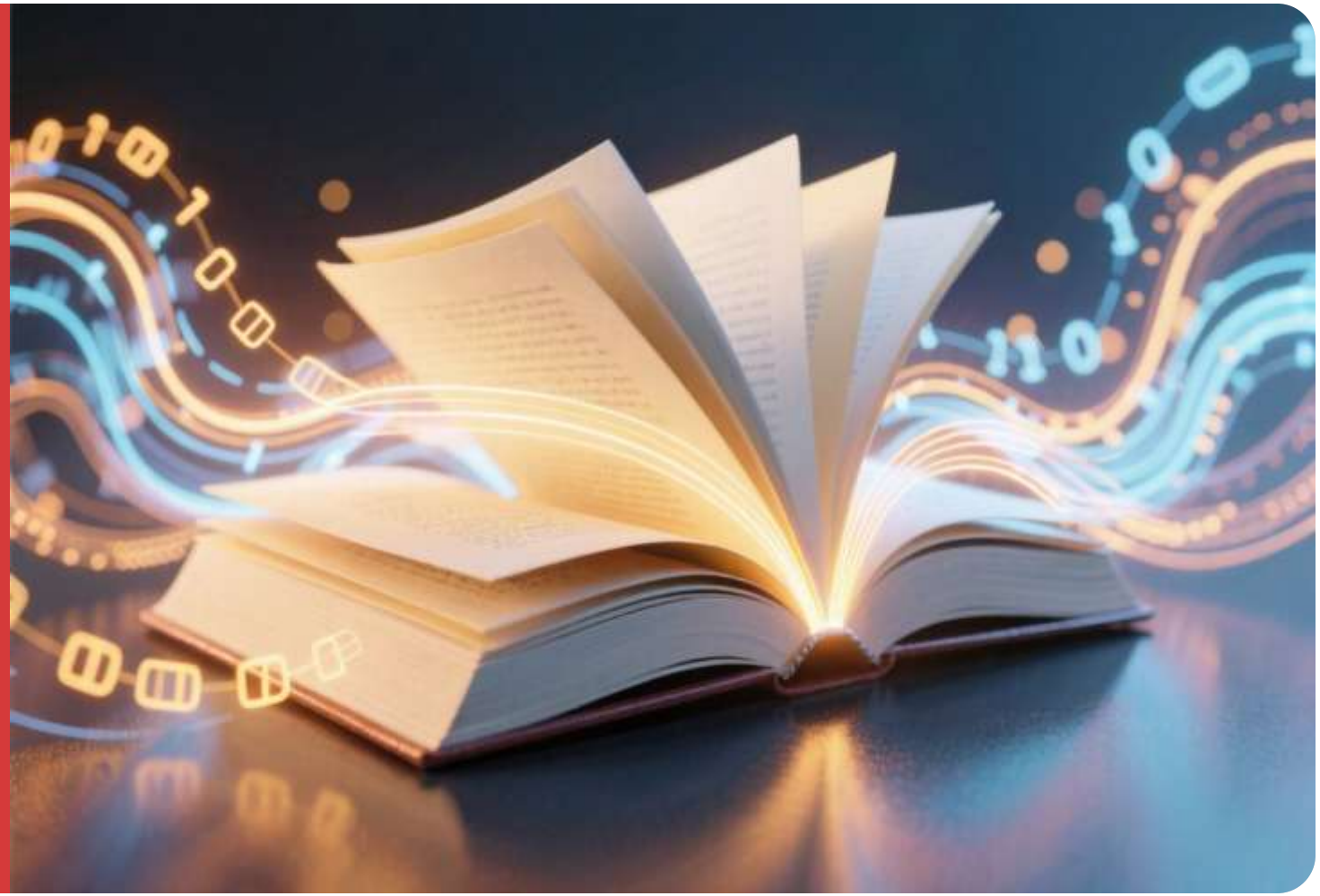
学习创新

持续学习的重要性

鼓励持续学习，以适应数据安全审计领域的新挑战和新解决方案。

实践创新的鼓励

鼓励实践创新，以推动数据安全审计领域的发展和进步。



DISE数智实审后续直播方向预告

后续陆续直播方向如下，感兴趣的朋友可以持续关注“数智实审”视频号！

群聊： 数智实审生态群

1、国家重要法规解读
2、主要行业标准解读
3、关键审计领域底稿讲解
4、典型领域共性问题分享
5、审计实战化案例解析
6、行业热点技术漏洞分析
7、重点行业痛点及难点剖析
8、数智化审计经验分享

大家可以关注视频号，私信回复‘进群’，获取微信生态群入口，获取直播 PPT、标准汇编、标准解读报告、热点领域文章、安全牛行业分析报告等众多福利。

DISE数智实审

感谢观看