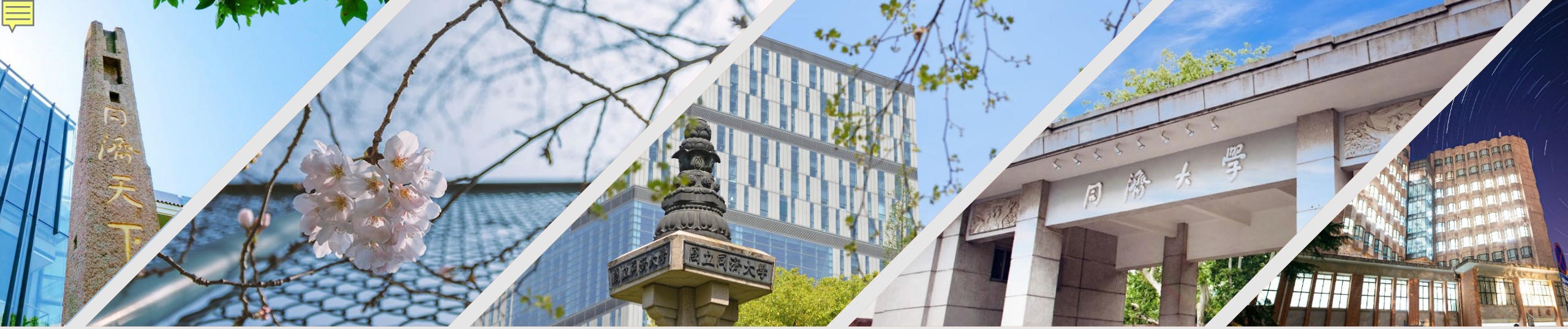


推进高校数据安全治理的实践与思考

同济大学 信息化办公室

邵炜晖

2023.11.30

汇报要点

1 背景和挑战

2 具体探索实践

3 推进工作思考

背景和挑战

01

为什么

- 国家有战略
- 法律有规定
- 行业有要求
- 学校有需求

1.1 国家有战略

2022年10月16日，习近平在中国共产党第二十次全国代表大会上作报告

十一、推进国家安全体系和能力现代化，坚决维护国家安全和社会稳定

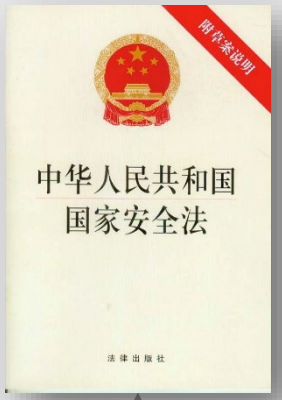
（一）健全**国家安全**体系。坚持党中央对国家安全工作的集中统一领导，完善高效权威的国家安全领导体制。强化国家安全工作协调机制，完善国家安全法治体系、战略体系、政策体系、风险监测预警体系、国家应急管理体系，完善重点领域安全保障体系和重要专项协调指挥体系，强化经济、重大基础设施、金融、**网络**、**数据**、生物、资源、核、太空、海洋等安全保障体系建设。

2023年3月27日，中共中央、国务院印发《数字中国建设整体布局规划》

“2522”整体框架：强化两大能力——数字技术创新体系和数字安全屏障

筑牢**可信可控**的**数字安全屏障**。切实维护网络安全，完善网络安全法律法规和政策体系。增强数据安全保障能力，建立数据分类分级保护基础制度，健全网络数据监测预警和应急处置工作体系。

1.2 法律有规定



2015.7

第二十五条

国家建设网络与信息安全保障体系，提升网络与信息安全保护能力，……实现网络和信息核心技术、关键基础设施和重要领域信息系统及数据的安全可控……

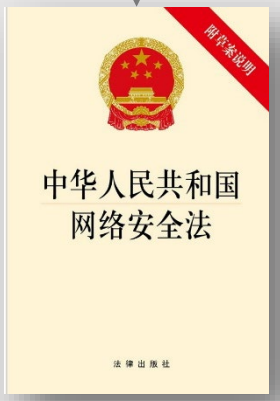
第十八条

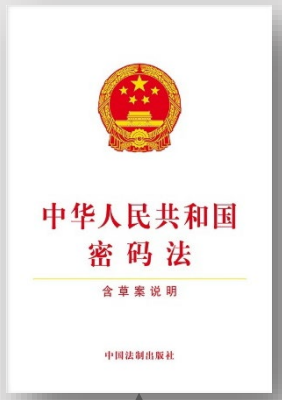
国家鼓励开发网络数据安全保护和利用技术，促进公共数据资源开放

第二十一条

（四）采取数据分类、重要数据备份和加密等措施

2017.6





2020.1

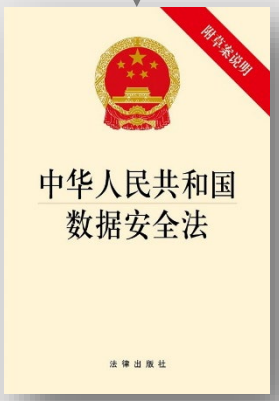
第二条

……密码，是指采用特定变换的方法对信息等进行加密保护、安全认证的技术、产品和服务

第八条

公民、法人和其他组织可以依法使用商用密码保护网络与信息安全

2021.9



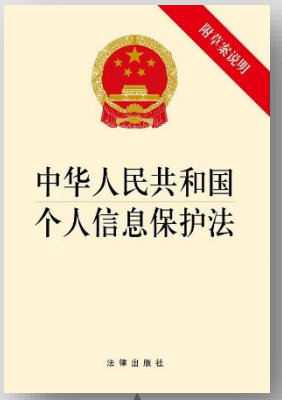
第三章数据安全制度

第二十一条　数据分类分级保护制度

第二十二条　数据安全风险评估、报告、信息共享、监测预警机制

第二十三条　数据安全应急处置机制

第二十四条　数据安全审查制度



2021.11

第一章 总则

目的明确原则、选择同意原则、最少够用原则、公开透明原则、确保安全原则、权责一致原则

第二章 个人信息处理规则

一般规定、敏感个人信息的处理规则、国家机关处理个人信息的特别规定

其他

行政法规

- 《关键信息基础设施安全保护条例》
- 《网络数据安全管理条例（征求意见稿）
- ……

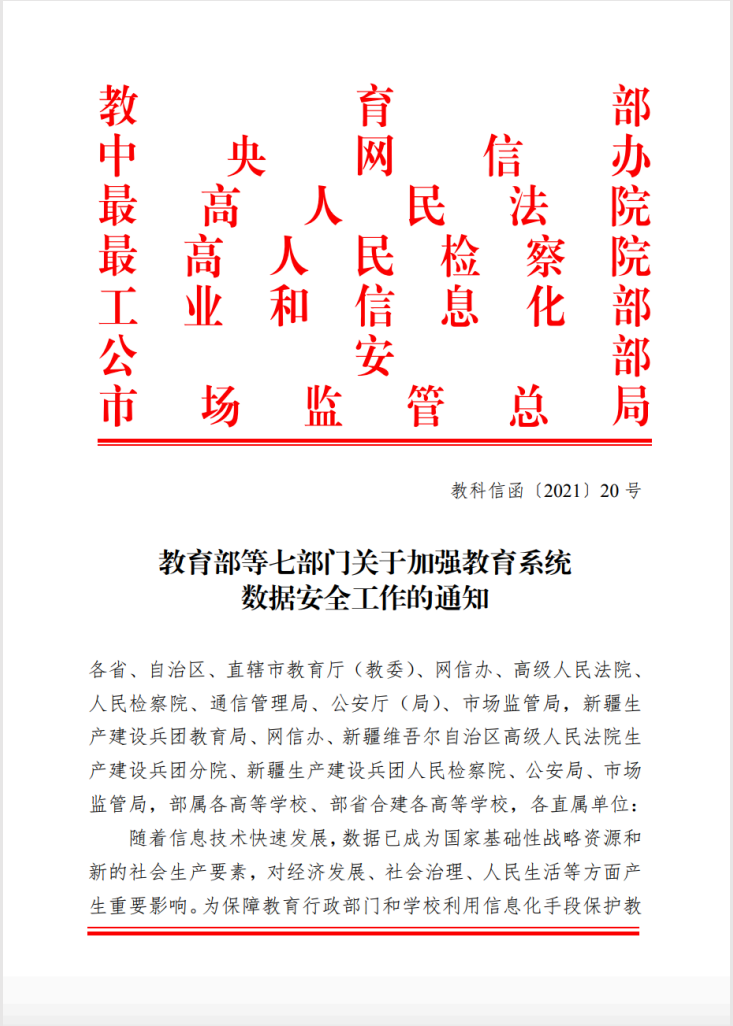
部门规章

- 《个人信息出境标准合同办法》
- 《数据出境安全评估办法》
- 《网络安全审查办法》
- ……

国家标准

- GB/T35273-2020《信息安全技术 个人信息安全规范》
- GB/T41479-2022《信息安全技术 网络数据处理安全要求》
- ……

1.3 行业有要求



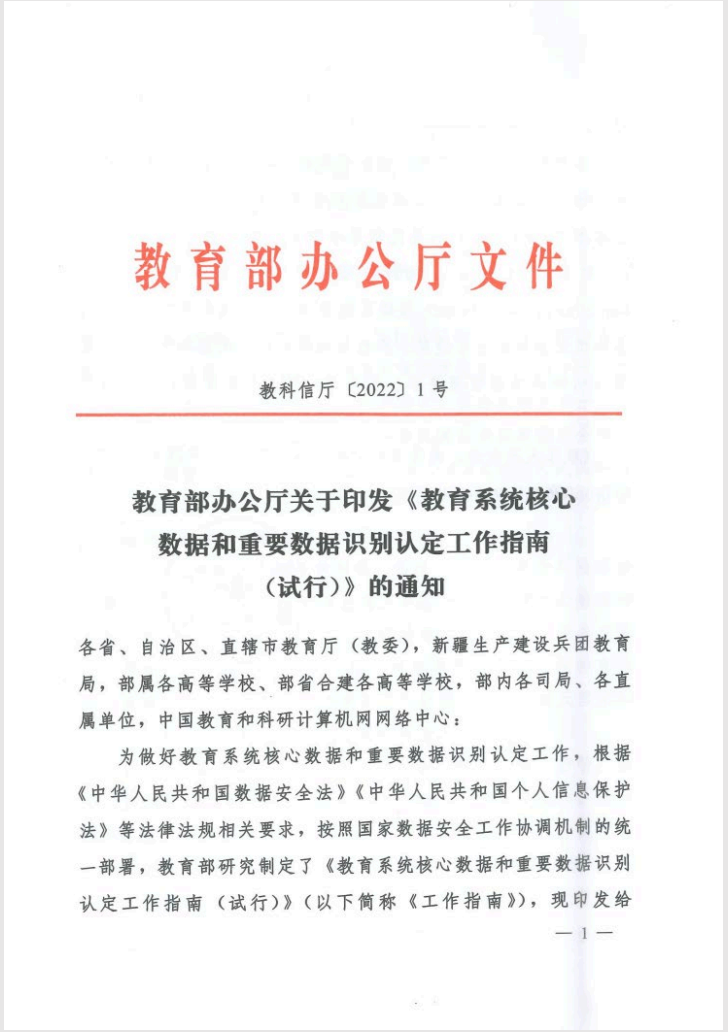
教育部办公厅 中央网信办 最高人民法院 最高人民检察院 最高人民信息化和业安全 工公市场监管总局 部院部部局

教科信函〔2021〕20号

教育部等七部门关于加强教育系统数据安全工作的通知

各省、自治区、直辖市教育厅（教委）、网信办、高级人民法院、人民检察院、通信管理局、公安厅（局）、市场监管局，新疆生产建设兵团教育局、网信办、新疆维吾尔自治区高级人民法院生产建设兵团分院、新疆生产建设兵团人民检察院、公安局、市场监管局，部属各高等学校、部省合建各高等学校，各直属单位：

随着信息技术快速发展，数据已成为国家基础性战略资源和新的社会生产要素，对经济发展、社会治理、人民生活等方面产生重要影响。为保障教育行政部门和学校利用信息化手段保护教



教育部办公厅文件

教科信厅〔2022〕1号

教育部办公厅关于印发《教育系统核心数据和重要数据识别认定工作指南（试行）》的通知

各省、自治区、直辖市教育厅（教委），新疆生产建设兵团教育局，部属各高等学校、部省合建各高等学校，部内各司局、各直属单位，中国教育和科研计算机网网络中心：

为做好教育系统核心数据和重要数据识别认定工作，根据《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等法律法规相关要求，按照国家数据安全工作协调机制的统一部署，教育部研究制定了《教育系统核心数据和重要数据识别认定工作指南（试行）》（以下简称《工作指南》），现印发给

— 1 —

《教育部等七部门关于加强教育系统数据安全工作的通知》

要建立教育系统数据安全责任体系和数据分类分级制度，形成教育系统数据资源目录。健全覆盖数据收集、传输存储、使用处理、开放共享等全生命周期的数据安全保障制度，开展常态化的数据安全监测预警通报。

《教育系统核心数据和重要数据识别认定工作指南（试行）》

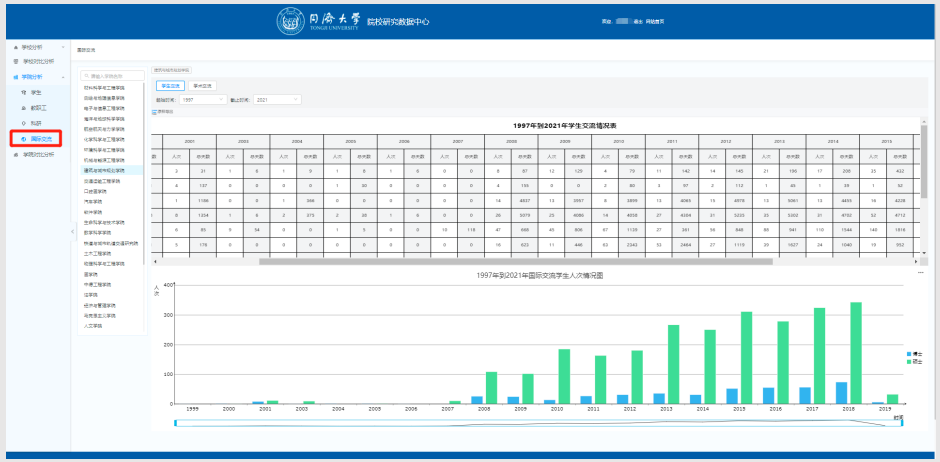
《教育系统数据分类分级工作指南》（征求意见稿）

1.4 学校有需求

■ 院校研究系统

归集人才培养、科学研究、社会服务、文化传承与创新、国际合作与交流指标，整合校内外数据，**基于海量数据为校、院两级提供管理和决策支持。**

- 学校分析（人才、科研、教学、声誉）
- 学校对比分析
- 学院分析（学生、教职工、科研、国际交流）
- 学院对比分析



1.4 学校有需求

■ 一网统管

利用AI、大数据、物联网、数字孪生技术，构建与物理校园孪生共融的虚拟智慧校园，**采集能源、安防、门禁、电梯、楼宇等物联终端海量数据，实现校园运行“观”“管”“防”**，以数字化＋智能化支撑校园治理现代化。

- 对接6个部门、10家公司、14个业务域
- 数字孪生2个校区、170栋楼宇、教学南楼室内、建设4000+设备模型
- 对校园运行业务域进行数据治理，整理了50+开放接口，集成50000万+条数据

1.4 学校有需求

■ 智慧教学分析和督导评价系统

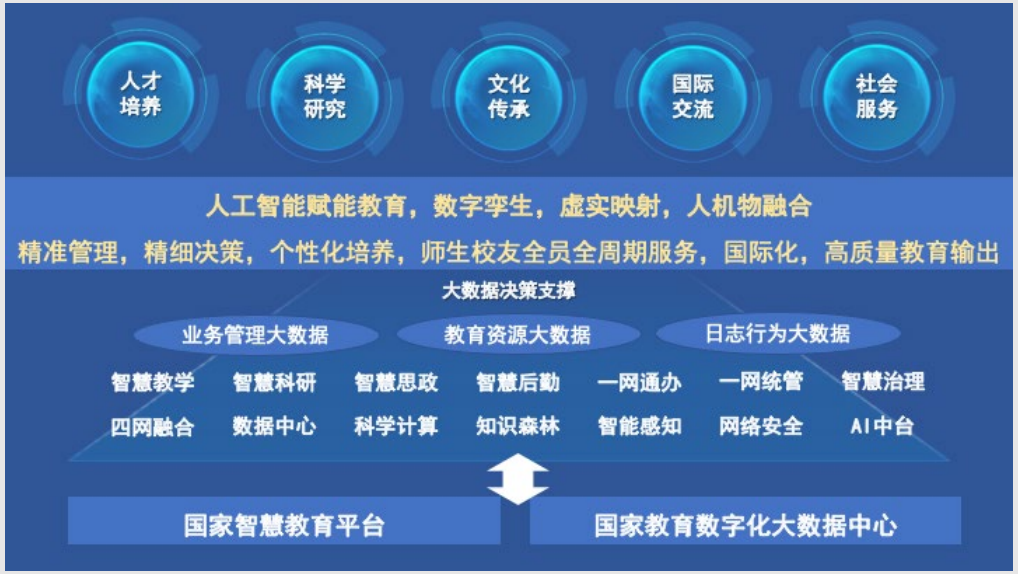
充分利用智慧教室各类设备采集音视频数据，基于AI分析能力，**对老师教、学生学的多模态数据进行行为分析**，结合人工督导评价指标等专家系统数据，实现常态化的教学行为智慧督导，即AI分析报告(课程、教师、学科等多维度)与实时预警相结合。

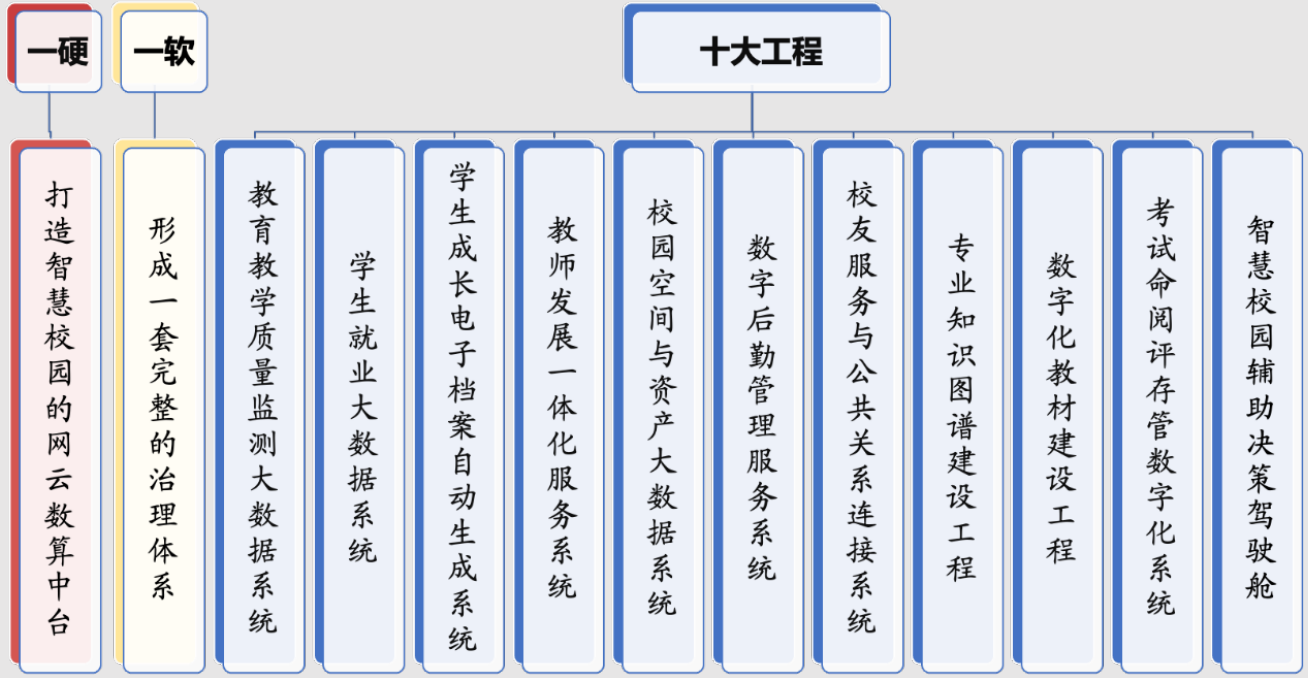
类型	多模态数据	核心能力	隐性指标	显性指标
数字空间	教学内容（文本、测验、录像…）	结构化数据 日志数据	线上教学资源	灵活处理教学内容，创造性使用教材，反映学科专业前沿
	教学延伸		学生线上教学参与度	把握新时代教学特点，充分利用线上教学平台开展课前、课后教学活动
物理空间	教师表情	面部表情识别	教师状态	教学状态投入，教学重点突出，富有情感，课堂气氛融洽
	教师语速	语音识别	教师表达能力	
	教师音量	语音识别		
	教师语言	语音转文字	师生互动	注重教学互动，启发学生思考，引导学生主动学习
	学生抬头率（当前、平均）	动态人脸识别	学生反馈	课堂富有吸引力，学生积极参与
	学生出勤率	动态人脸识别	教学吸引力	
定性测量空间	督导巡课指标、教学大赛获奖课程、教育大赛评分标准	量化评价指标依据与验证		

1.4 学校有需求

■ 数字化转型新任务

- 6月4日，信息化工作推进会。郑庆华校长作报告《AI赋能教育：赋什么怎么赋》，人工智能全面赋能教育创新发展的新认识，推动教育范式、场景、技术系统性创新，实现学科专业转型升级、教学评管创新应用、智慧校园科学决策。
- 9月20日，数字化转型工作推进会。
- 11月5日，数字化转型十大工程需求评审会。





1.4 学校有需求

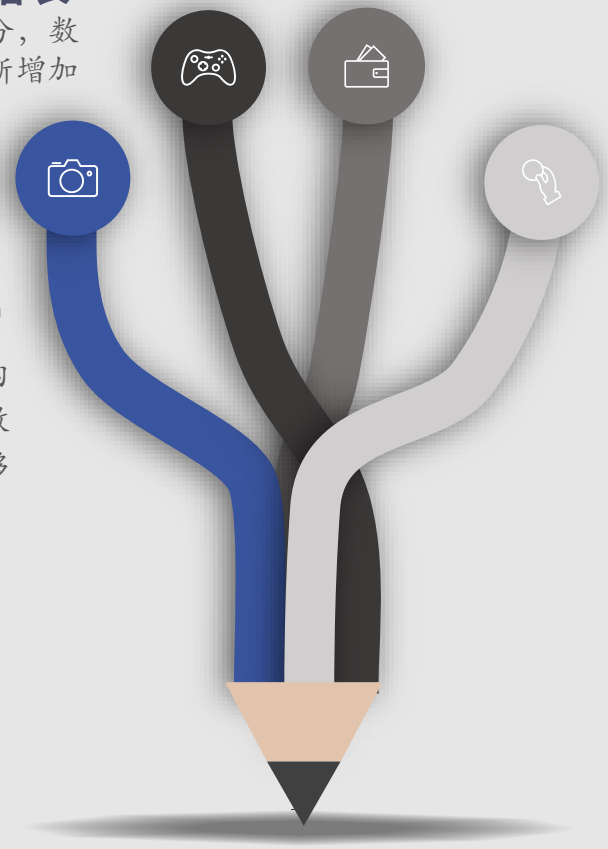
内因驱动数据安全治理

数据总量不断增长

对数据作为核心生产要素的重要性认知更加充分，数据大量积累、总量不断增加

数据类型不断丰富

物联网和AI应用的不断涌现，数据结构从单纯的结构化数据为主，向包含结构化、半结构化和非结构化数据在内的混合模式转移



数据的共享与开放的需求发生变化

数字化转型驱动下，建设重点已由事务业务管理型系统向数据分析决策型系统转变，且多教学、科研业务自身的生产数据

IT环境越来越复杂，数据泄露真的发生

安全重点已经从网页内容安全、系统应用安全转变为数据安全和个人信息保护

具体探索实践

02

做了啥

- 数据安全风险评估
- 核心业务数据分类分级
- 完善数据安全防护能力
- 可信密码服务体系支撑
- 人脸数据安全防护实践

2.1 数据安全风险评估

评估对象

电信学院协同育人平台——二级学院基于低代码平台构建的一站式事务平台，通过API获取数据中台中本学院各类数据。

评估目标

以点及面，摸清学校典型数据业务的安全现状，为制定整体数据安全规划、确立数据安全策略、补齐数据安全能力提供依据。

参考标准

《信息安全技术 网络数据处理安全要求》（GB/T 41479-2022）
《信息安全技术 数据安全风险评估实施方法》（征求意见稿）
《信息安全技术 信息安全风险评估规范》（GB/T 20984-2022）
《信息安全技术 信息安全风险评估方法》（GB/T 20984-2022）
《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）

评估方法

文档审阅、人员访谈、现场调研、工具扫描、渗透测试、综合分析、评估报告

2.1 数据安全风险评估

数据处理活动风险评估

覆盖采集、存储、传输、使用、加工、提供、公开、删除33个检查点

- 是否在法律、行政法规规定的目的和范围内收集、使用数据；
- 是否明确数据备份与恢复的策略和操作规程；
- 数据公开过程是否开展日志记录；
- 是否建立用户数据删除需求的响应机制；
- ……

数据安全管理风险评估

覆盖数据安全组织管理、数据安全制度流程、数据安全分类分级管理、人员安全管理、数据合作方安全管理、数据安全应急管理46个检查点

- 是否设立由高级管理层组成的数据安全领导小组；
- 是否对数据处理关键岗位人员数据安全意识或专业能力考核；
- 是否制定数据安全事件应急预案，定义数据安全事件类型，明确不同类别事件的处置流程和方法；
- ……

数据安全技术风险评估

覆盖数据访问控制、安全监测预警、数据脱敏、数据防泄漏、接口安全、备份恢复、安全审计42个检查点

- 是否建立与数据类别级别相适应的访问控制机制情况，并限定用户可访问数据范围；
- 开发测试、人员信息公示等应用场景的数据脱敏效果验证情况；
- 对网络、终端数据防泄漏技术手段部署情况；
- ……

个人信息保护

覆盖保护基本原则、保护措施、告知同意、主体权力、个人信息处理37个检查点

- 个人信息保护内部管理制度和操作规程的建设落实情况；
- 在处理个人信息前，是否以显著方式、清晰易懂的语言真实、准确、完整地公开个人信息处理规则；
- 是否将个人生物识别信息与个人身份信息分开存储；
- ……

■ 评估结果

序号	风险类别	涉及数据处理活动	风险等级
1	数据篡改风险	数据采集	中
2	数据存储过程泄露风险	数据存储	中
3	数据存储过程恶意攻击风险	数据存储	高
4	数据存储过程抵赖风险	数据存储	中
5	数据存储过程泄露风险	数据存储	中
6	数据传输过程泄露风险	数据传输	中
7	越权或滥用风险	数据使用	中
8	恶意攻击风险	数据安全管理	中
9	接口安全管控能力不足	数据接口管理	高
10	数据安全执行记录缺失	数据安全管理执行	高
11	接口安全管控能力不足	数据接口管理	高
12	数据防泄露能力不足	数据安全审计	高
13	数据防泄露能力不足	数据防泄露	中
14	安全监测预警能力不充足	数据安全监测预警	中

2.1 数据安全风险评估

- 根据评估结果确定工作思路和当前重点

数据标准

数据治理

2.2 核心业务数据分类分级

■ 参考标准

1. 《中华人民共和国网络安全法》
2. 《中华人民共和国数据络安全法》
3. 《中华人民共和国个人信息保护法》
4. GB/T 10113-2003 分类与编码通用术语
5. GB/T 25069-2010 信息安全技术术语
6. GB/T 35295-2017 信息技术 大数据 术语
7. GB/T 37964-2019 信息安全技术 个人信息去标识化指南
8. GB/T 38667-2020 信息技术 大数据 数据分类指南
9. GB/T 39335-2020 信息安全技术 个人信息安全影响评估指南
10. GB/T 35273-2020 信息安全技术 个人信息安全规范
11. GB/T 41817-2022 信息安全技术 个人信息安全工程指南
12. GB/T 41479-2022 信息安全技术 网络数据处理安全要求
13. GB/T 41817-2022 信息安全技术 个人信息安全工程指南
14. JY/T 1002-2012 教育管理信息 教育管理基础信息
15. JY/T 1006-2012 教育管理信息 高等学校管理信息
16. TC260-PG-20212A 网络安全标准实践指南—网络数据分类分级指引
17. 信息安全技术 网络数据分类分级要求（征求意见稿）
18. 信息安全技术 重要数据识别规则（征求意见稿）
19. 信息安全技术 重要数据识别指南(征求意见稿)
20. 教育系统核心数据和重要数据识别认定工作指南（试行）
21. 上海教育数据安全管理规范（试行）

2.2 核心业务数据分类分级

同济大学 TONGJI UNIVERSITY

■ 分级方法

- 影响对象

  数据遭到篡改、破坏、泄露或者非法获取、非法利用、非法共享后，受到危害的对象，包括政治安全、国家安全、经济运行、社会稳定、公共利益、组织权益、个人权益。

- 影响程度

  数据遭到篡改、破坏、泄露或者非法获取、非法利用、非法共享后所造成的危害影响的大小，包括无影响、一般影响、严重影响、特别严重影响。

- 数据价值
- 数据规模
- 数据可用性
- 数据可共享性
- 数据可开放性

敏感等级		判定标准
核心数据		影响政治安全 (一)高精度、未公开的覆盖全国范围的教育机构数据; (二)1亿人及以上个人信息或1000万人及以上敏感个人信息; (三)1000万条及以上经过计算加工生成的，对数据描述对象有较深刻画程度，且影响国家安全的衍生数据; (四)经评估的其他数据。
重要数据		影响国家安全、经济运行、社会稳定、公共健康和安全。 (一)覆盖全国范围的教育机构数据; (二)1000万人及以上个人信息或100万人及以上敏感个人信息; (三)全国性的业务数据; (四)在生成国家秘密的过程中所使用分析的原始非秘密数据; (五)经评估的其他数据
一般数据	三级	组织和个人权益造成特别严重影响。 （一）可能导致组织遭到监管部门严重处罚（包括取消经营资格、长期暂停相关业务等），或者影响重要/关键业务无法正常开展的情况，造成重大经济或技术损失，严重破坏学校声誉，带来严重负面影响和群体事件。 （二）个人信息主体可能会遭受重大的、不可消除的、可能无法克服的影响，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害。如遭受无法承担的债务、失去工作能力、导致长期的心理或生理疾病、导致死亡等。
	二级	组织和个人权益造成严重影响。 （一）可能导致组织遭到监管部门处罚（包括一段时间内暂停经营资格或业务等），或者影响部分业务无法正常开展的情况，造成较大经济或技术损失，破坏学校声誉，带来负面影响。 （二）个人信息主体可能遭受较大影响，个人信息主体克服难度高，消除影响代价较大。如遭受诈骗、资金被盗用、被银行列入黑名单、信用评分受损、名誉受损、造成歧视、被解雇、被法院传唤、健康状况恶化等。
	一级	组织和个人权益造成一般影响或无影响。 （一）可能导致个别诉讼事件，或在某一时间造成部分业务中断，使组织的经济利益、声誉、技术等轻微受损。 （二）个人信息主体可能会遭受困扰，但尚可以克服。如付出额外成本、无法使用应提供的服务、造成误解、产生害怕和紧张的情绪、导致较小的生理疾病等。

2.2 核心业务数据分类分级

分类框架

- 充分调研业务部门，了解主管单位数据安全保护需求、未来业务规划下可能涉及的数据项等关键信息；
- 形成学校概况数据、学生数据、教职工数据、教学数据、科研数据、校务数据、其他数据7个大类，22个二级子类、70三级子类、287个四级子类的数据分类框架（征求意见中）；
- 基于数据安全综合治理平台，对19个系统、563个表、12602个字段的进行分类分级标注（非19个系统的全部数据）；

一级分类	二级分类	三级分类	四级分类	详细内容	影响对象	影响程度	最终定级
概况数据	学校基本数据	领导干部	学校委员会（领导小组）数据	组织与领导干部信息	组织权益	一般危害	L1
		行政部门	院系所单位数据	部门名称、部门领导、部门层级、部门代码、上级主管部门、行政级别等	组织权益	一般危害	L1
			院系所单位变更				
			院系所单位概况				
		学校概况数据	学校基本数据	学校名称、简介、地址、代码、邮政编码、学校性质、办学类型、主管部门、联系方式等基本数据	组织权益	一般危害	L1
			校区基本数据	校区名称、校区地址、校区邮政编码、校区联系电话、校区负责人等	组织权益	一般危害	L1
	学科点数据		学科点基本数据	学科点简介、学科目录、学科门类、课程信息等学科点基本数据	组织权益	一般危害	L1
			学科点统计数据	学科点统计相关的数据	组织权益	严重危害	L2
	学生基本数据		学生基础数据	姓名、学生ID、学号、身份证号、护照号码、居留许可号码、性别、出生日期、出生地点、婚姻状况、职业、联系地址、国籍等	个人权益	特别严重危害	L3
			学习简历数据	最后学历、生源地等	个人权益	严重危害	L2
			工作简历数据	工作或学习单位、工作经历等	个人权益	严重危害	L2
			个人通讯	邮箱、电话号码、邮编、QQ号、微信号等	个人权益	严重危害	L2
			学生金融账户信息	银行卡相关数据、保险购买数据、一卡通号码、	个人权益	特别严重危害	L3
			学生实体标识	人像照片、证书照片/影印件	个人权益	特别严重危害	L3
			学生私密资料	宗教信仰、家庭情况、血型、民族、病史等揭示个人种族、家属信息、居住地址、宗教信仰、基因、个人健康、私人生活等有关的用户私密信息：法律、行政法规规定禁止公开的用户其他信息	个人权益	特别严重危害	L3
			政治面貌	政治面貌相关信息	个人权益	严重危害	L2
			家庭通讯方式	家长手机号、邮箱、地址等联系方式	个人权益	严重危害	L2
			家庭成员	姓名、身份证号码、性别、出生日期、家庭关系、婚姻状况、工作单位相关信息、职务、政治面貌等	个人权益	特别严重危害	L3
			家庭经济情况				
			学生来源数据				
			住宿				
			户口状况				
		本专科新生数据	本专科生考生				
			本专科生考生总分				
			本专科生考生科目成绩				
			本专科生录取				
			本专科生新生测验成绩				
		研究生招生数据	研究生考生				
			研究生入学考试成绩				
			研究生录取				
			研究生调剂录取				
		研究生招生辅助数据	研究生招生计划辅助				
			研究生报名点辅助				
			研究生入学考试科目辅助				
			研究生入学考试考场辅助				

教学数据	教学管理数据	专业班级数据	专业信息数据	开设专业的专业号、专业名称、专业简称、专业英文名称、学科门类码、专业码等	组织权益	一般危害	L1
			班级数据	班级名称/代码、专业、单位、学生类别、年级、集体荣誉称号相关信息等	组织权益	一般危害	L1
		课程数据	课程基本信息	课程名称、课程号、学时、课程简介等基础信息	组织权益	一般危害	L1
			教学计划数据	开课信息、排课信息、课表、考试信息、教学班信息、培养方案、总体计划、教学进度、学分等	组织权益	一般危害	L1
			排课数据				
			选课数据				
			研究生专业培养方案数据				
			考试安排数据				
		教学配套支撑数据	教室管理数据	教室基本数据、教室使用数据	组织权益	一般危害	L1
			教材数据	教材基本数据、获奖教材、教材编者	组织权益	一般危害	L1
		教学质量评估数据	教学成果数据	教学成果获奖、教学成果完成人	组织权益	一般危害	L1
			评教数据				
	教学生产数据			视频、音频、上课录像、作业、考试等			
科研数据	科研管理数据	科研机构数据	科研机构基本数据				
			科研机构人员				
		科技项目数据	科技项目基本数据	项目编号、项目名称、项目负责人、项目来源、课题信息、学科门类等	组织权益	特别严重危害	L3
			项目协作单位	协作单位名称、协作单位类型、合作方式等	组织权益	严重危害	L2
			项目经费	计划经费总额、项目经费来源、项目凭证等	组织权益	特别严重危害	L3
			项目人员	参与项目人员号（工号、学号）、姓名、性别、职称、单位、工作量等	个人权益	特别严重危害	L3
			项目合同信息	合同编号、合同名称等合同相关内容	组织权益	严重危害	L2
		科技成果数据	科技成果人员	人员号、角色、排名/总人数、贡献率、姓名、所在单位、人员类型	组织权益	严重危害	L2
			科技著作	著作编号、著作名称、学科领域、项目来源、论著类别、语种、出版信息等	组织权益	一般危害	L1
			科技论文基本数据	论文编号、论文名称、论文类型、所属技术领域、收录情况等	组织权益	一般危害	L1
			科技论文发表数据	刊物名称、刊物级别、发表时间、刊发相关信息	组织权益	一般危害	L1
			科技论文报告	会议编号、论文报告形式、论文集名称	组织权益	一般危害	L1
			鉴定成果	鉴定成果编号、鉴定成果名称、鉴定批文号、学科领域、完成形式、成果类型、鉴定单位、鉴定结论等	组织权益	严重危害	L2
			专利成果基本数据	专利成果编号、专利成果名称、申请编号、专利类型、学科领域、专利证书编号、专利费用、专利代理相关信息等	组织权益	一般危害	L1
			专利出售	出售日期、出售金额、受售单位等	组织权益	一般危害	L1
			技术转让基本数据	合同编号、合同名称、成交金额、学科领域、负责人、受让方信息等	组织权益	一般危害	L1
			获奖成果基本数据	获奖成果名称、科技奖类别、获奖级别、颁奖单位等	组织权益	一般危害	L1
			计算机软件著作权	软著证书编号、软件名称、证书颁发机构等	组织权益	一般危害	L1
		学术交流数据	学术会议				
			派出人员				
			接受人员				
	科研生产数据			数据集、数据模型、算法等			

2.2 核心业务数据分类分级

■ 分类管理、分级管控策略

高等级所列安全保护措施是在低等级安全保护措施上增加和增强的部分，重复的不再列入

数据级别 数据活动	一般数据一级	一般数据二级	一般数据三级	重要数据与核心数据
数据收集	1.明确数据收集目的、用途和范围规范数据收集的流程和方法； 2.在有可参照原始数据的情况下，采取管理和技术措施保障数据收集前后的完整性； 3.对采集的工具、系统、设备采用准入控制，采集设备需要具体用户认证和权限访问控制，确保只有合法用户能访问。	1.通过外部数据提供方收集的数据，要求外部数据提供方说明数据来源，审核外部数据提供方的身份，并对信息来源的合法性进行确认，留存审核、交易记录，确保数据收集渠道的合法性和正当性； 2.在数据收集过程中采取管理和技术措施防止数据泄漏； 3.对数据收集的工具、系统、设备应符合安全检测或认证，并提供安全防护； 4.收集异常、传输量超过设定阀值情况可告警。	1.数据收集的工具、系统、设备账号应采用双因素认证； 2.采取一定程度的加密方式对数据进行保护。	1.使用溯源技术，对数据泄露风险进行分析，对行为进行追踪。
数据存储	1.建立数据存储管理规范和制度； 2.应对数据存储系统、设备（如数据库系统、数据库主机等）提供安全防护； 3.对有明确约定存储期限的数据应按约定期限进行存储； 4.建立本地数据备份和恢复机制。	1.建立存储数据系统账户权限统一管控规范和制度； 2.对不同安全等级数据设置访问控制规则； 3.应对数据存储环境（如机房环境、网络环境等）提供安全防护。	1.建立存储系统的身份认证和鉴权机制； 2.应提供对数据泄漏、篡改、破坏的监测和告警； 3.应在经授权和通过安全检测的环境下访问存储系统； 4.敏感度较高的数据，应采用文件加密或数据加密方式存储。	1.建立本地备份及异地备份保护和恢复措施，应设置合理的恢复点和恢复时间； 2.应采取技术手段防止数据的泄漏、篡改。
数据使用加工	1.建立数据使用加工管理流程，明确加工目的、范围及使用属性； 2.应提供数据使用加工测试环境，在测试环境开展数据使用加工过程的设计和开发，验证通过后再置入生产环境运行； 3.建立访问权限管理及身份认证机制。	1.应对数据使用加工系统的用户采用身份鉴别手段； 2.建立数据使用加工系统的账户权限统一管控规范和制度； 3.应采用措施保障访问数据使用加工系统的安全。	1.应周期性的检查数据使用加工系统用户操作数据的情况； 2.应对超出范围和超出规模的数据使用加工行为开展监测和告警。	1.应对数据使用加工的内容、行为、方式进行溯源； 2.应采取技术手段实现数据可用不可见。

2.2 核心业务数据分类分级

■ 分级管理、分级管控策略

高等级所列安全保护措施是在低等级安全保护措施上增加和增强的部分，重复的不再列入

数据级别 数据活动	一般数据一级	一般数据二级	一般数据三级	重要数据与核心数据
数据传输	1.应采用校验技术保证传输过程中数据的完整性。	1.建立传输两端的身份认证机制； 2.应采用加密通道进行数据传输。	1.在身份认证机制和数据传输通道上应采用符合国家法律法规要求的密码技术。	1.应采用不可篡改技术实现传输过程记录。
数据提供	1.建立数据提供管理流程，明确提供目的和范围及使用属性。	1.建立数据提供的工具、系统，对提供过程进行审批授权，并采用不可篡改技术实现提供过程审批授权的记录。	1.应采取技术措施对提供审批的业务过程和数据提供的技术过程开展风险监测和预警，对违规行为及时报警或阻断。	1.应采用可用不可见方式进行提供，如有特殊情况应采取“一事一议”进行审批。
数据公开	1.建立数据公开管理流程，明确开放目的和范围及使用属性。	1.应对提供公开的API或其他方式进行安全管理； 2.应采取技术措施对公开审批的业务过程和数据公开的技术过程开展风险监测和预警，对违规行为及时报警或阻断； 3.建立数据敏感度监测识别，防止敏感度较高数据被有意或无意公开。	1.应建立专用存储区域存储公开数据，并采用必要的访问控制措施； 2.应采用实名制方式申请并采取公开过程管控措施。	1.应建立公开数据二次校验机制； 2.仅在数据主体授权条件下允许公开。
数据删除 (销毁)	1.建立数据删除管理流程，明确删除的目的、范围、操作方式和删除记录，并建立定期检查机制。	1.建立数据删除的监督机制； 2.应使用规范的工具或产品执行数据删除工作。	1.在不影响业务的前提下或业务下线后，应以不可逆方式删除数据。	

2.3 完善数据安全防护能力

■ 数据仓库（2014年）

累计入仓56个业务系统、1566张数据表、数据总量270G，数据服务250余次

■ 数据交换（2015年）

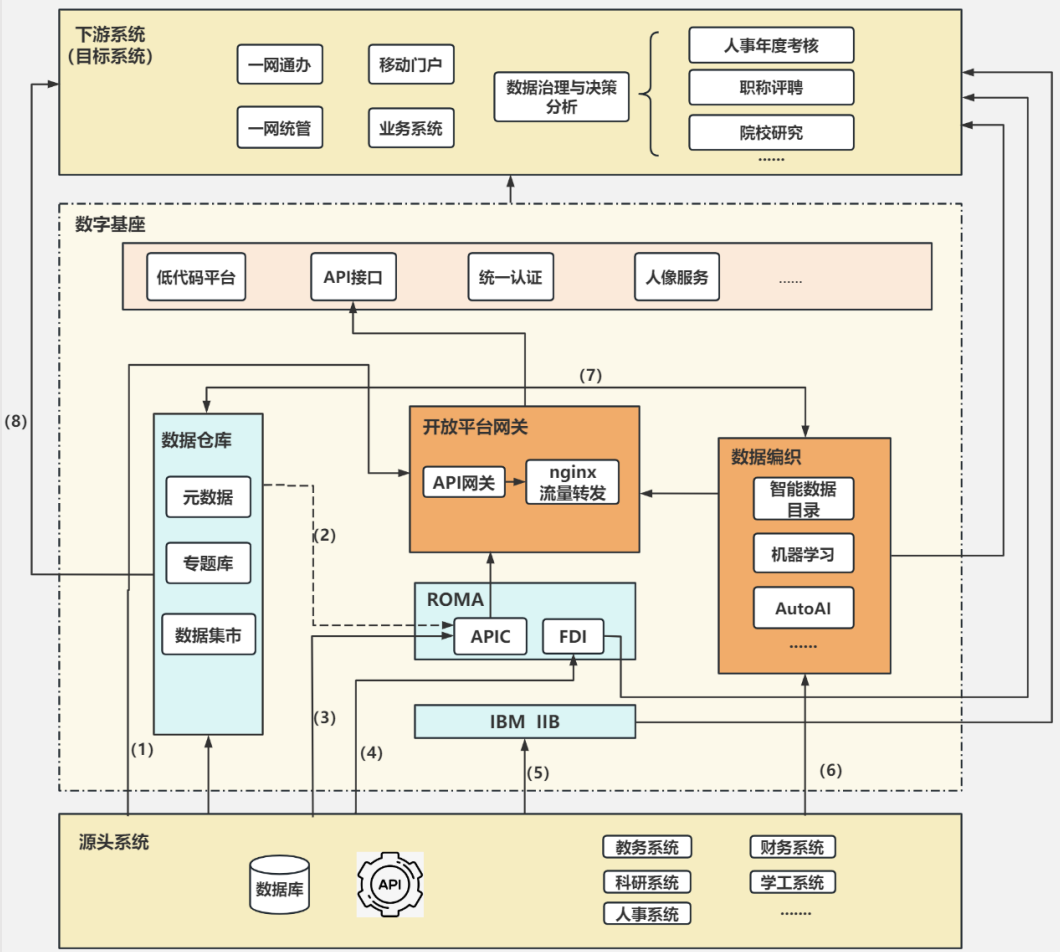
基于ESB高可用，梳理592个表、6462个字段的映射和转换关系，开发实时交换151个、批量交换477个

■ 数据集成（2018年）

基于Roma平台高效率实现百万级数据集成同步

■ 数据开放（2022年）

自主研发数据接口90多个，其中22个实时业务接口，支撑17个业务系统建设，已提供4.31亿次接口调用，接口响应时间毫秒级



分析需求制定数据共享方案：

数据交换场景：用于批量处理大量数据。当需要从多个来源收集数据，并对其进行处理、转换和加载到目标系统时，可以使用数据交换，过程涉及从源系统提取数据，对数据进行清洗、转换和整理，然后将其加载到目标系统中。这个过程通常是定期执行的，可以按计划自动运行。

提供API接口调用的场景：主要用于实时获取数据。当需要从外部系统或服务获取最新数据时，可以使用API。API允许下游通过编程方式与其他应用程序或服务进行交互，从中提取所需数据。可以通过调用API来请求特定数据，并以结构化的格式（如JSON）接收响应。

（1）：API接口，源头系统提供业务接口，通过API网关转包接口并控制权限对外提供；

（2）：API接口，数据仓库提供分析处理后的业务数据库表，通过ROMA开发接口到API网关层转包接口并控制权限对外提供；

（3）：API接口，源头系统提供业务数据库表，通过ROMA开发接口到网关层转包接口并控制权限对外提供；

（4）：数据交换，通过ROMA的FDI执行批量同步作业，同步数据给下游；

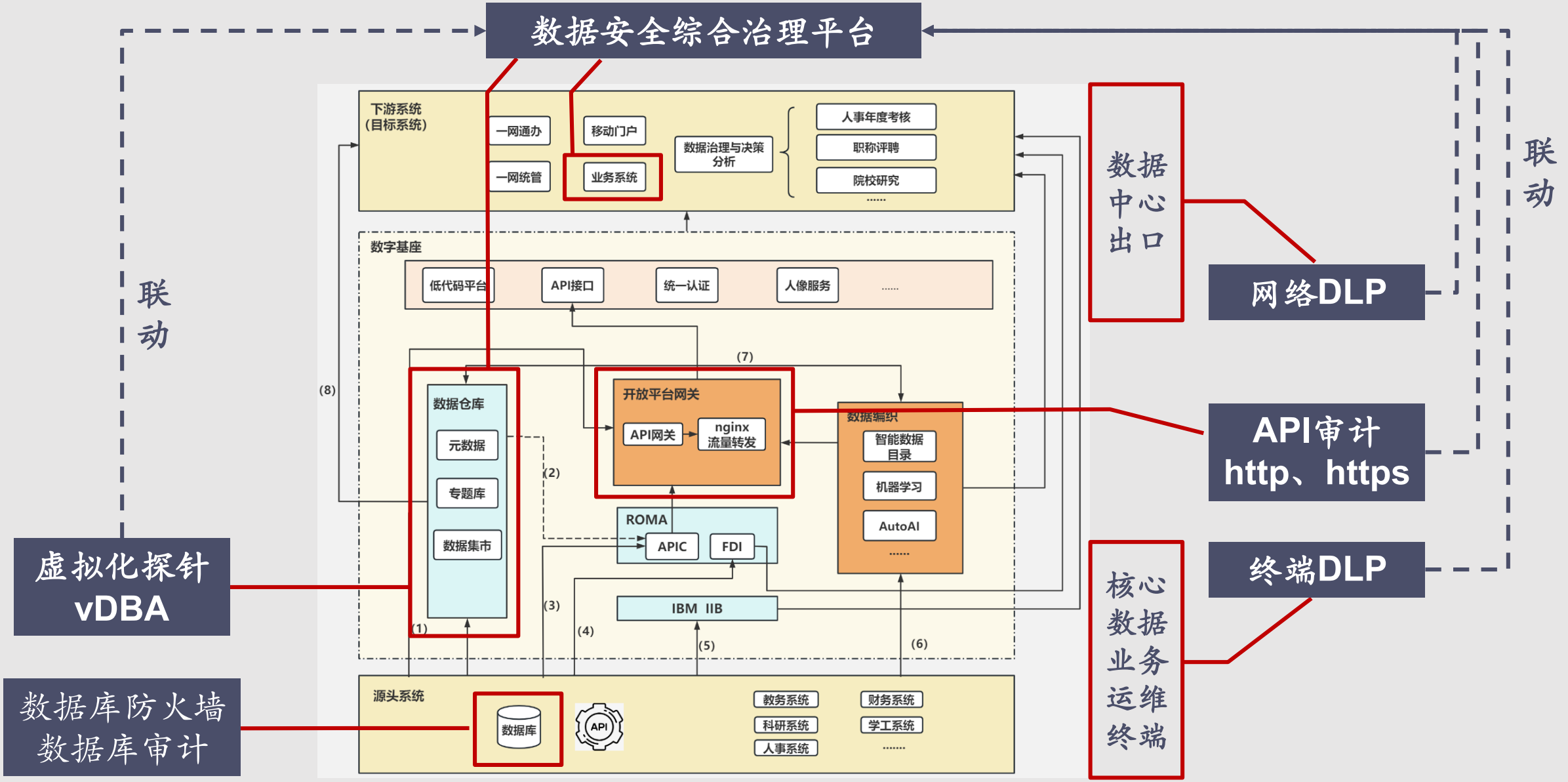
（5）：数据交换，通过IBM IIB执行批量或实时同步作业，同步数据给下游；

（6）：数据编织，源头系统提供业务数据库表供数据编制分析，生成智能数据目录等；

（7）：数据编织，数据仓库提供分析好的数据库表给数据编制分析，生成智能数据目录等，数据编制分析处理后的数据可存入数据仓库供下游业务系统使用，也可以通过API网关转包接口对外提供；

（8）：数据仓库，提供数据治理与决策分析能力。

2.3 完善数据安全防护能力



2.4 可信密码服务体系支撑

■ 数字签名、电子签章

提供可信行为与电文服务，保障核心业务流程的有效性和可追溯性，确保用户业务行为的不可抵赖。

■ 时间戳服务器

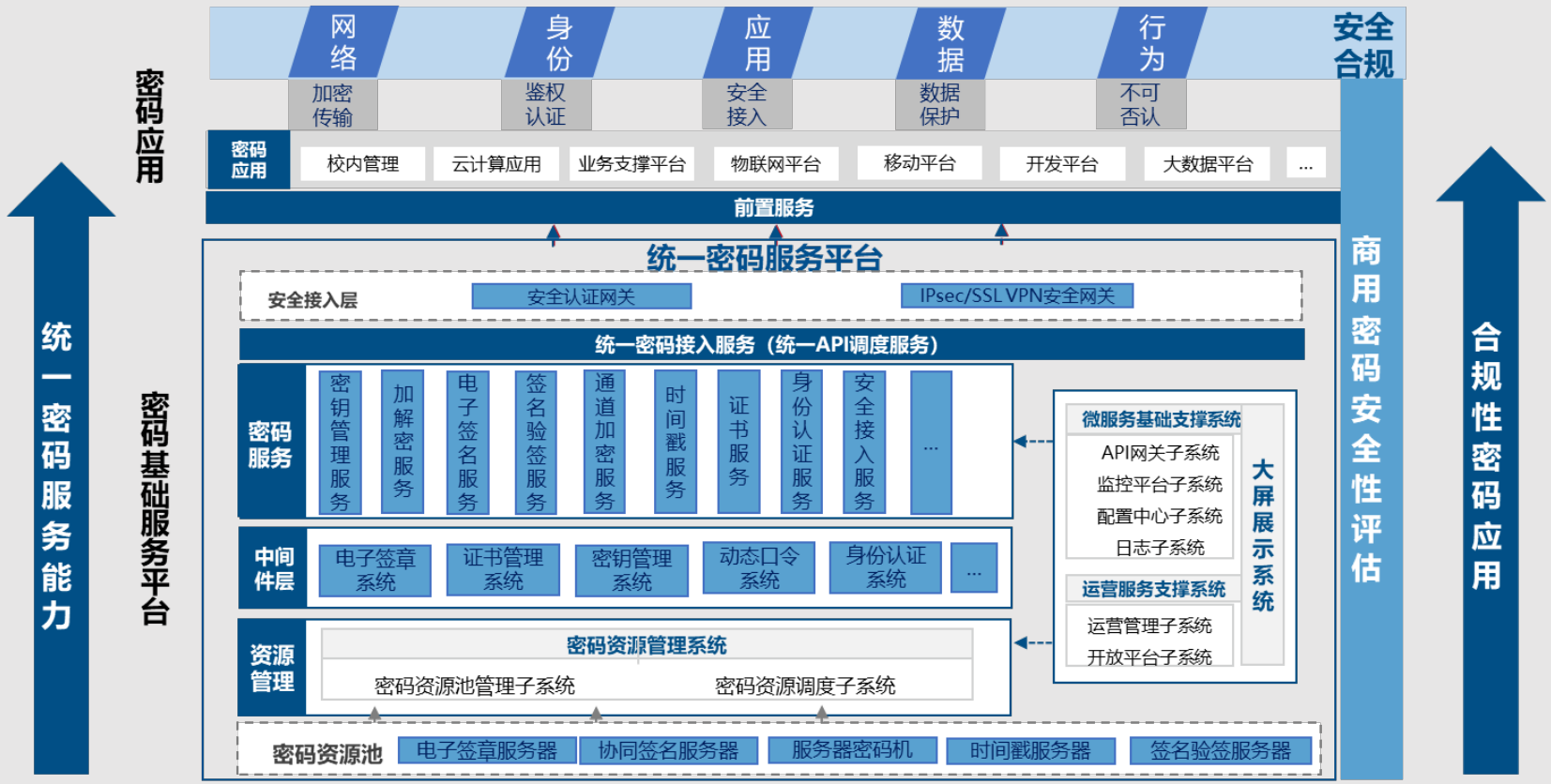
提供可信权威标准时间获取、同步、留存与认证功能，确保关键业务环节可信时间应用。

■ 安全认证网关

验证真实身份与宣称身份是否相符，保障业务主体合法身份和权限不被盗用，保证业务主体身份真实性、合法性。

■ 数据安全网关、IPSec/SSL VPN、服务器密码机

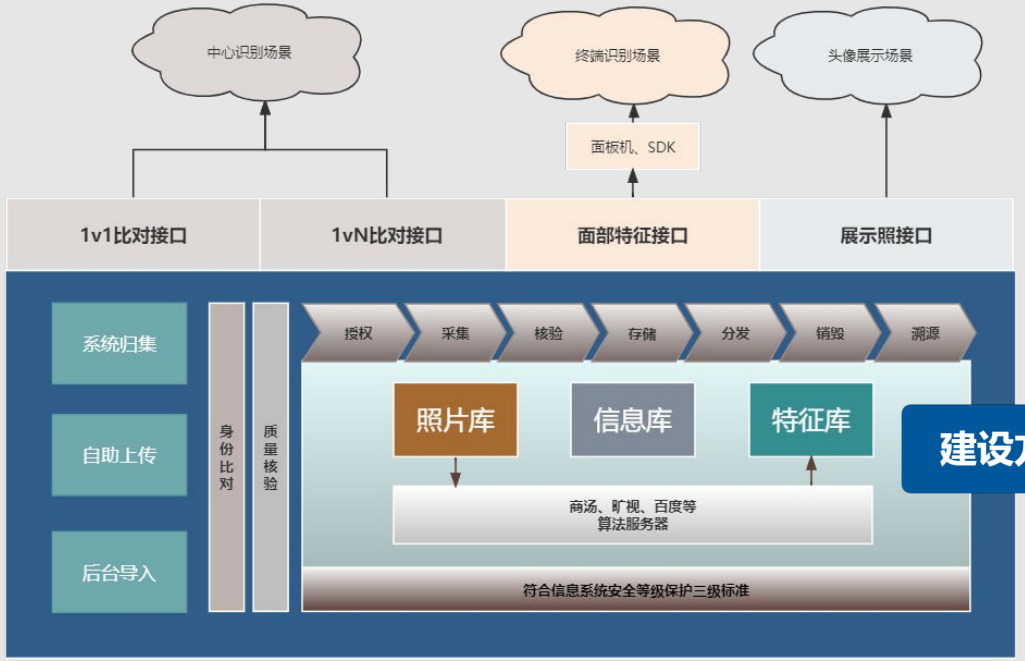
遵循国家密码管理局相关规范，采用国家密码管理局公布国产密码算法，确保数据传输安全性、机密性，数据使用过程中的动态脱敏、访问控制，以及数据存储过程的机密性、完整性等等确保数据全生命周期安全。



2.5 人脸数据安全防护实践

同济大学 TONGJI UNIVERSITY

■ 基于面部特征值、面向隐私保护的多引擎人脸管理和应用支撑平台



建设方案

识别

- **不知是谁，需自动识别**
  - 场地网络条件优秀：调用1vN接口进行中心识别，获取学工号等身份信息 → 如：新生报到、以图搜人
  - 场地网络难保证，要求及时响应：选取面板机或SDK安装包作为识别终端，获取对应的面部特征值，经本地计算得到识别结果。 → 如：讲堂签到、宿舍楼门禁
- **知道是谁，需验证身份**
  - 场地网络条件优秀：调用1vl接口进行中心识别，获取是否匹配。 → 如：移动端刷脸登录
  - 场地网络难保证，要求及时响应：选取面板机或SDK安装包作为识别终端，获取对应的面部特征值，经本地计算得到验证结果。 → 如：刷脸+刷卡双因子签到

展示

- **仅做头像展示**：调用展示照接口，实时获取照片 → 如：师生信息查询
- **展示照片更新**：调用展示照接口，自助上传展示类照片 → 如：人事系统、学工应用

2.5 人脸数据安全防护实践

同济大学 TONGJI UNIVERSITY

9万

注册用户数9万+

对8万多校内用户及1万多校外用户的人脸底片进行归集，统一管理。

6万

已授权用户6万+

对用户人脸数据进行分发和使用，需征得个人的单独授权同意。用户取消授权，业务端需同步关停人脸识别的使用，并删除人脸特征数据。

7套

已接入算法模型7套

涵盖旷视、商汤、百度等主流是脸识别厂商的算法模型，为业务端建设提供更丰富的适配资源。

...

场景陆续改造

已改造多栋宿舍楼、图书馆20+个闸机通道、正在接入高等讲堂人像签到、新生报到等更多场景。

荣誉证书

同济大学：

贵单位申报的“基于面部特征值、面向隐私保护的多引擎人脸管理和应用支撑平台”在2023年度上海高校信息化建设与应用优秀案例评选中荣获**银奖**。

特发此证，以资鼓励！

推进工作思考

03

有啥坑

3 推进数据安全治理工作的思考

1 组织机制：

谁负责？谁牵头？谁参与？

- 谁管业务谁管数据，谁管数据谁管数据安全；
- 信息办/信息中心外部与业务部门协同，信息办/信息中心内部数据条线与安全条线协同，业务+数据+安全协同；

2 目标认识：

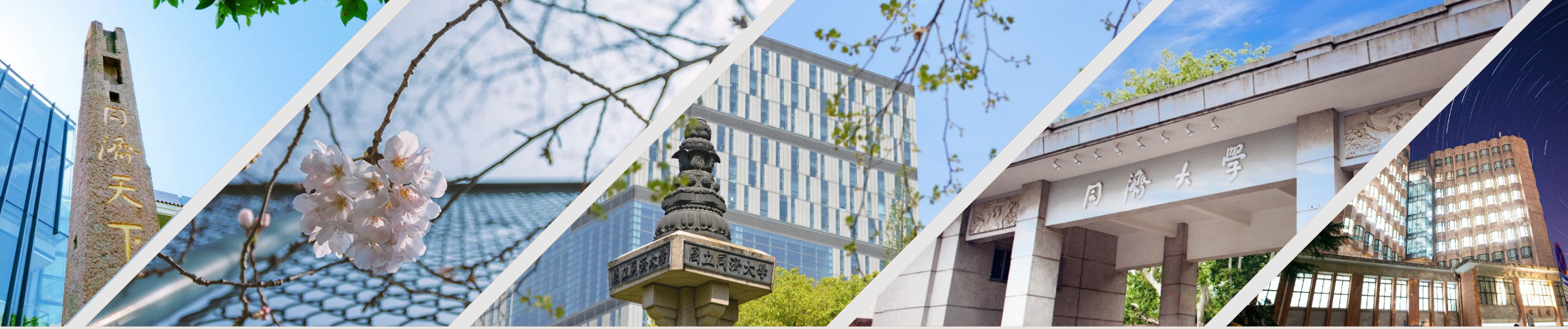
安全与发展？

- 促进数据有序共享，以共享为常态、不共享为例外；
- 安全不能因不合理的需求妥协；

3 方式方法：

全覆盖与全周期？一劳永逸？

- 结合自身数据业务特点，分阶段有序推进，形成方法论并建立机制；
- 业务和数据是动态变化的，因此数据安全也需动态跟随；
- 选择合适的工具可以提高效率，但大量人力、服务无法替代；



感谢倾听！

同济大学 信息化办公室

邵炜晖

2023.11.30