19th Asian Games Hangzhou 2022

杭州2022年第19届亚运会官方合作伙伴

数字政府一体化安全保障体系建设

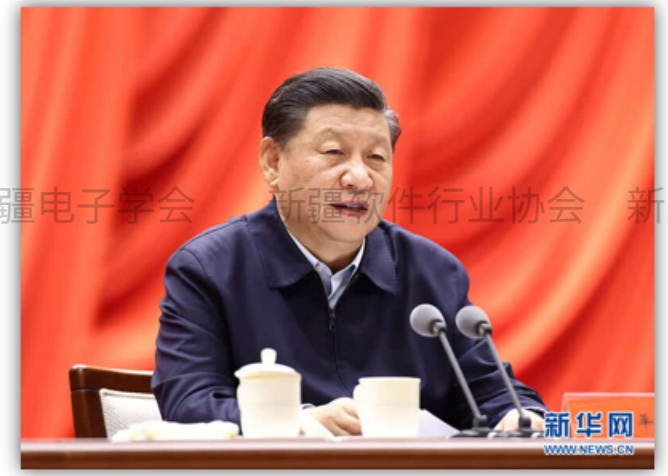
安恒信息 周俊

www.dbappsecurity.com.cn 400-6059-110

总书记有指示

2022年4月19日下午，中央全面深化改革委员会第二十五次会议。习近平总书记在主持会议时强调，要全面贯彻网络强国战略，把数字技术广泛应用于政府管理服务，推动政府数字化、智能化运行，为推进国家治理体系和治理能力现代化提供有力支撑。会议强调，**要始终绷紧数据安全这根弦**，加快构建数字政府全方位安全保障体系，全面强化数字政府安全管理责任。

2023年7月15日,习近平习近平对网络安全和信息化工作作出重要指示，强调，坚持党管互联网，坚持网信为民，坚持走中国特色治网之道，**坚持统筹发展和安全**，坚持正能量是总要求、管得住是硬道理、用得好是真本事，**坚持筑牢国家网络安全屏障。**



国家有要求

坚持安全可控是推进数字政府建设的先决条件

加快推进全国一体化政务大数据体系建设，加强数据治理，依法依规促进数据高效共享和有序开发利用，充分释放数据要素价值，确保各类数据和个人信息安全。

——国务院关于加强数字政府建设的指导意见（2022年6月23日）

形成制度规范、技术防护和运行管理三位一体安全保障体系

以“数据”为安全保障的核心要素，强化安全主体责任，健全保障机制，完善数据安全防护和监测手段，加强数据流转全流程管理，形成制度规范、技术防护和运行管理三位一体的全国一体化政务大数据安全保障体系。

——《全国一体化政务大数据体系建设指南的通知》（2022年10月28日）

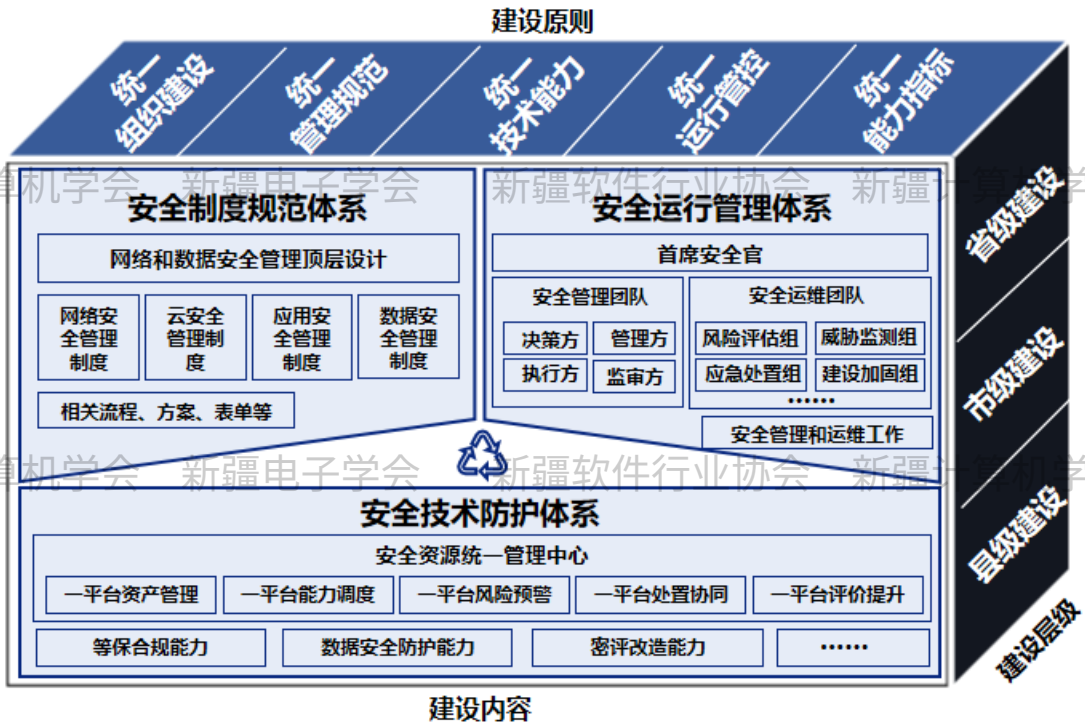
筑牢可信可控的数字安全屏障

《规划》明确，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。

——《数字中国建设整体布局规划》（2023年）

地方需落实：建设数字政府一体化安全保障体系

以习近平总书记总体国家安全观为指导，深入贯彻网络和数据法律法规，以安全保障一体化为建设总纲，持续迭代升级**三大体系**，省市县**分层级**推进安全建设工作，建成数字政府一体化安全保障体系，统筹平衡**安全与发展**的关系。



以“五个统一”为建设原则，

统筹规划全域安全体系建设；

以“三大体系”为建设内容，

提升网络和数据安全核心能力；

以“三个层级”为建设路径，

有序推进各层级安全建设工作。

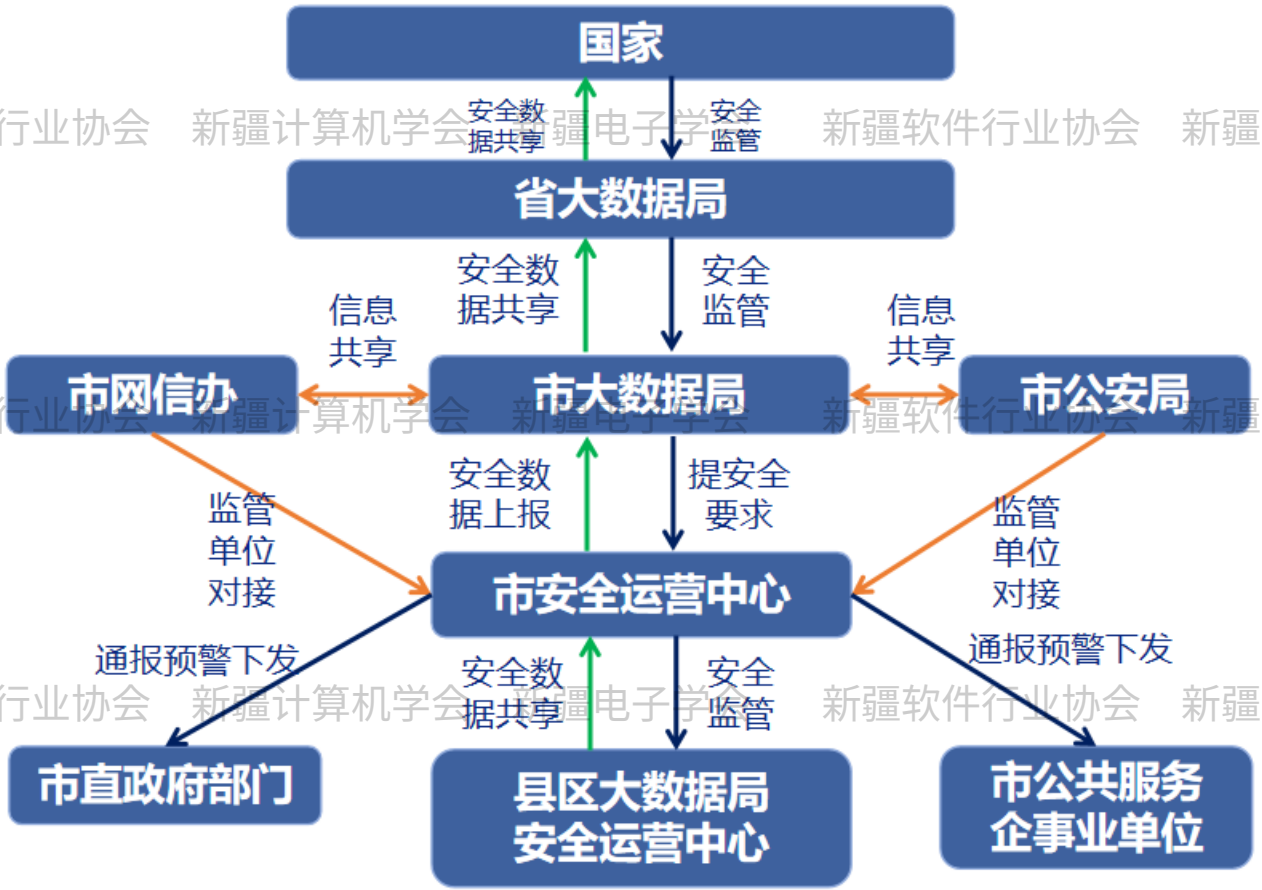
统一组织建设：构建安全管理和运维组织

各单位需明确安全管理组织，科学分配安全决策、管理、执行、监审等分工协作机制，建立专业化安全运维团队，明确各岗位职责要求，共同保障本单位安全建设、运维等工作有序开展。

岗位职责		岗位描述
安全管理团队		负责安全运营整体战略和安全运营重大决策的制定，指导并监督安全运维团队。
安全运维团队管理小组		负责安全整体工作的指挥、调度、协调工作，参与安全运营重大决策，保障安全运营工作顺利开展。
各运维组	风险评估组	负责探查全网资并评估安全现状并指导加固
	威胁监测组	负责威胁分析研判，给出处置建议并指导
	应急处置组	负责应急演练；发生事件时快速应急取证
	安全情报组	负责收集威胁情报，根据实际情况推演判定
	建设加固组	负责安全建设、维护、策略优化、加固等

建立横纵协同的安全协同机制

从实战出发，建立跨层级、跨部门安全协同工作机制，支撑安全工作长效进行。



● 业务清　● 流程清　● 责任清

统一管理规范：形成一套体系化的安全制度规范

根据国家网络和数据安全法律法规为准绳，以数字政府相关国家标准和地方法规要求为依据，建立健全地方网络和数据安全制度规范体系，指导安全工作有效落实。

建立出台地方数字政府网络和数据安全管理办法

网络和数据安全管理办法是为落实相关法律法规，规范本区域网络和数据安全建设而制定，主要从“谁来干、怎么干、干的好不好”三方面来设计。

01 权责分工 **02 建设原则** **03 建设要求** **04 考核机制**

某市数字政府网络安全与数据安全管理办法

建设原则：坚持总体国家安全观，坚持安全和发展并重，按照“**谁建设谁负责，谁主管谁负责，谁运营谁负责，谁使用谁负责**”原则；

职责分工：明确数字政府主管部门的**监管责任**，建设单位的**主体责任**；建立市区**安全协调小组**，建立协同保障机制，确定小组成员单位职责分工……

一般规定：提出制定统一的**安全管理制度**，建立安全运营机制，配备**安全运营组织**；完善建设单位遴选机制；规定安全建设保障经费。

安全建设：针对规划建设、运行维护、监测预警等过程中的**网络和数据安全提出具体安全要求**，包括人员操作要求、账号管理要求、技术能力要求等……

监督保障：提出建设数字政府网络安全与数据**安全评估机制，建立评估指标**；明确风险或违法行为及其处理方式。

制定落实各项安全管理制度

数据分类分级管理办法示例

角色分工

数据安全管理员

1.制定规范策略即要求；
2.召集分类分级评审会议；
3.开展分类分级教育培训。

数据分类分级操作员

1.分类分级的具体执行、变更和记录工作。

安全审计管理员

1.负责分类分级工作的审计、跟踪和监督检查，提出改进意见。

数据分类

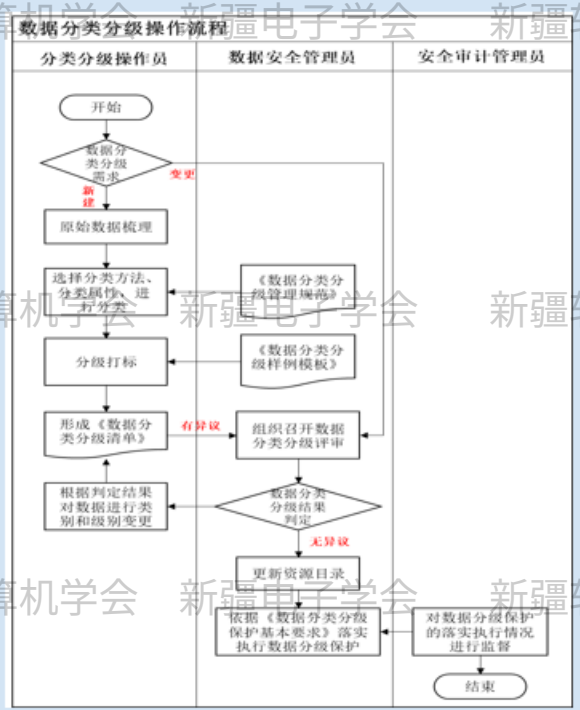
数据分级

	L1不敏感	L2低敏感	L3较敏感	L4敏感
分级评判标准	对社会秩序、公共利益、行业发展、信息主体均无影响。	对全社会、多个行业、行业内多个组织造成严重影响；对单个组织的正常运作造成极其严重影响；对人身和财产安全、个人名誉造成轻微损害。	对全社会、多个行业、行业内多个组织造成中等程度的影响；对单个组织的正常运作造成严重影响；对个人名誉造成中等程度的损害。	对全社会、多个行业、行业内多个组织造成严重影响；对单个组织的正常运作造成极其严重影响；对人身和财产安全、个人名誉造成严重损害。
数据共享要求	审批要求：数据主管部门审批后无条件共享。	审批要求：数据主管部门审批后无条件共享。	审批要求：数据主管部门审批和数据提供单位授权后受限共享。 技术要求：视情况脱敏；对数据共享全链路各环节的权限最小化控制，比如白名单控制并对异常进程监控；对数据共享全链路各环节风险进行监控。	不共享
数据开放要求	审批要求：数据主管部门审批后无条件共享。	审批要求：数据主管部门审批后无条件共享。	审批要求：数据主管部门审批和数据提供单位授权后受限共享。 技术要求：视情况脱敏；对数据共享全链路各环节的权限最小化控制，比如白名单控制并对异常进程监控；对数据共享全链路各环节风险进行监控。	不开放

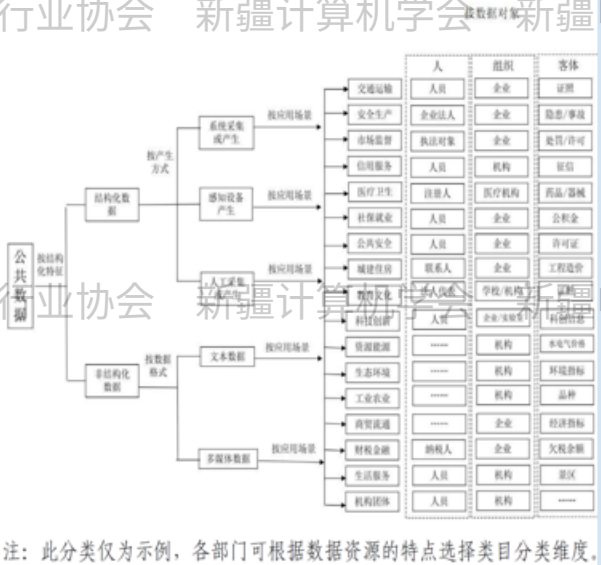
细化落实各项制度的操作流程和规范

➢ 数据分类分级实施细则示例

分类分级操作流程



分类方法示例



分级防护示例

数据级别	数据采集	数据传输	数据存储	数据访问	部门内部共享	部门外部共享	数据开放	数据销毁
3 级	公共数据采集设备应符合安全认证，采集环境安全，采集流程和方式符合相应要求。	应在可信可控环境中传输；通过互联网和无线方式传输时应加密。	分布式存储；应保存在可信或可控的信息系统或物理环境中，非可信或离线环境应进行加密存储。	需设置粗颗粒度的身份标识与鉴别机制；应建立访问控制矩阵，明确可访问用户和可访问内容；宜采用口令、密码、生物识别等鉴别技术对用户进行身份鉴别。	审批要求：根据单位内部数据管理要求确定。 技术要求：参照有关法律法规和标准执行。	审批要求：数据主管部门审批和数源部门授权后受限共享。 技术要求：视情况脱敏。	审批要求：数据主管部门审批和信息主体授权后受限开放。 技术要求：视情况脱敏。	业务终止时需以不可逆的方式销毁有关数据或脱敏存储，有数据存档要求的从其规定。
2 级	公共数据采集流程和方式符合相应要求。	通过互联网和无线方式传输时应进行加密。	应保存在可信或可控的信息系统或物理环境中。非可信或离线环境应进行加密存储。	需设置粗颗粒度的身份标识与鉴别机制。应建立访问控制矩阵，明确可访问用户和可访问内容。宜采用口令、密码、生物识别等鉴别技术对用户进行身份鉴别。	审批要求：根据单位内部数据管理要求确定。 技术要求：参照有关法律法规和标准执行。	审批要求：数据主管部门审批后无条件共享。 技术要求：视情况脱敏。	审批要求：数据主管部门审批后受限开放或无条件开放。 技术要求：视情况脱敏。	业务终止时需脱敏存储，有数据存档要求的从其规定。
1 级	公共数据采集流程和方式符合相应要求。	不需要进行传输加密。	有存储在经过安全认证的公有云上。	可不设置身份标识与鉴别机制。	审批要求：无。 技术要求：无。	审批要求：无。 技术要求：无。	审批要求：无。 技术要求：无。	自行决定数据处理方法。

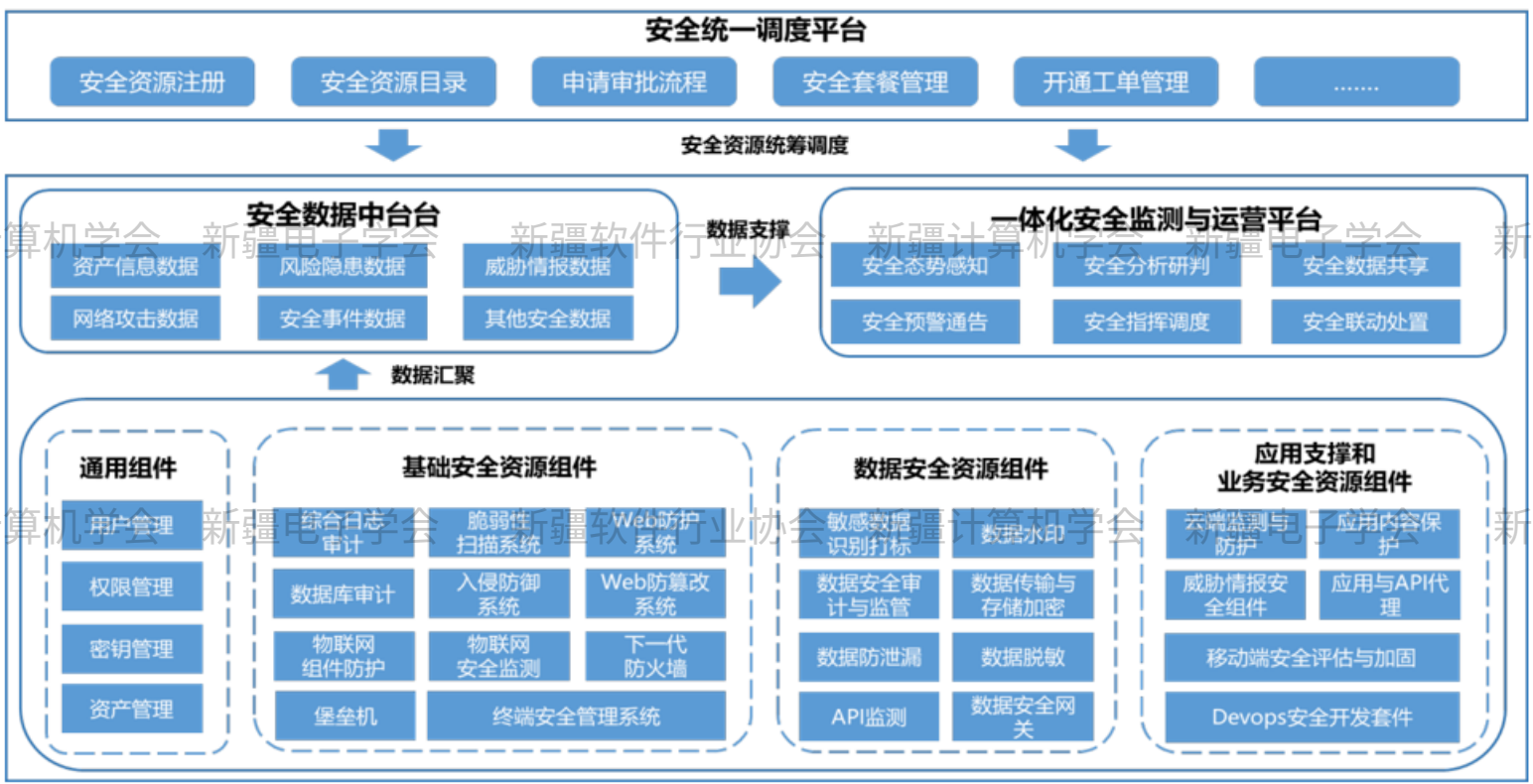
分级保护和监督指导

结果示例

表名	表中文名	字段名称	字段类型	字段描述	数据示例	数据来源	数据管理维度		业务应用维度			安全保护维度	数据对象维度	数据级别
							产生频率	...	共享属性	开放属性	...			
dwd_rk_gysy_fwwdxx_df	XX服务网点信息	dwd_zjid	string	dwd主键	2d36ef**********	区行政服务中心	每周		无条件共享	无条件开放		一般数据	组织	L1

统一技术能力：构建一体化安全技术防范体系

以数据安全防护需要为核心，分阶段分层级建设完善政务网络、政务云平台、政务数据、业务系统、终端等网络安全技术防护体系，利用全省统一的安全调度平台实现安全能力“统一注册、统一上架、统一申请、统一开通”，保障全省安全能力的统筹调度。



实现以等级保护为基础的安全合规建设能力

为云上政务信息系统提供等保合规的安全能力，相比于独立部署方式节省资源40%以上，降低资源占用成本并提升利用率。

实现以自主可控为目的的国产密码应用能力

通过标准化的密码改造能力，解决政务信息系统中存在的密码使用合规性、密码应用不足、应用集成难、管理难以及重复建设等问题，提高政务服务领域商用密码应用能力。

对不同租户支持不同的权限分配

根据权限级别的设置，租户能够实现本单位密码管理员设立、密码资源调度、资源监测的功能

对不同机构、应用实现密码资源的分配

根据各机构的业务需要，实现某项密码资源的按需分配

密码资源的状态监测

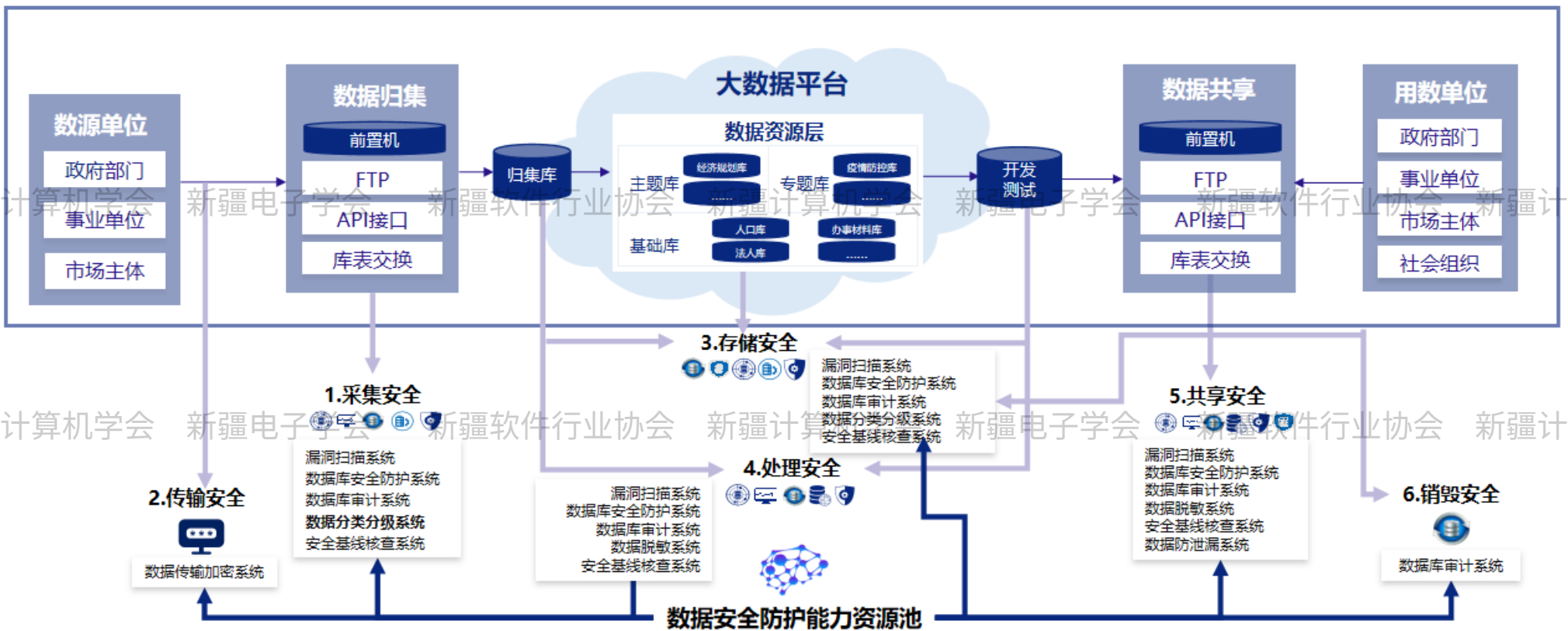
支持查看密码基础设施的负载情况，支持连接数、CPU、内存、磁盘等资源的组合或单独报表展现

传输加密服务：为多类型的终端提供传输加密服务，包括需集成改造的字段级传输加密、通过网络配置修改的流量拦截式加密；

存储加密服务：提供不同颗粒度的存储加密服务，包括需集成改造的字段级存储加密、通过安装加解密软件的表级别存储加密。

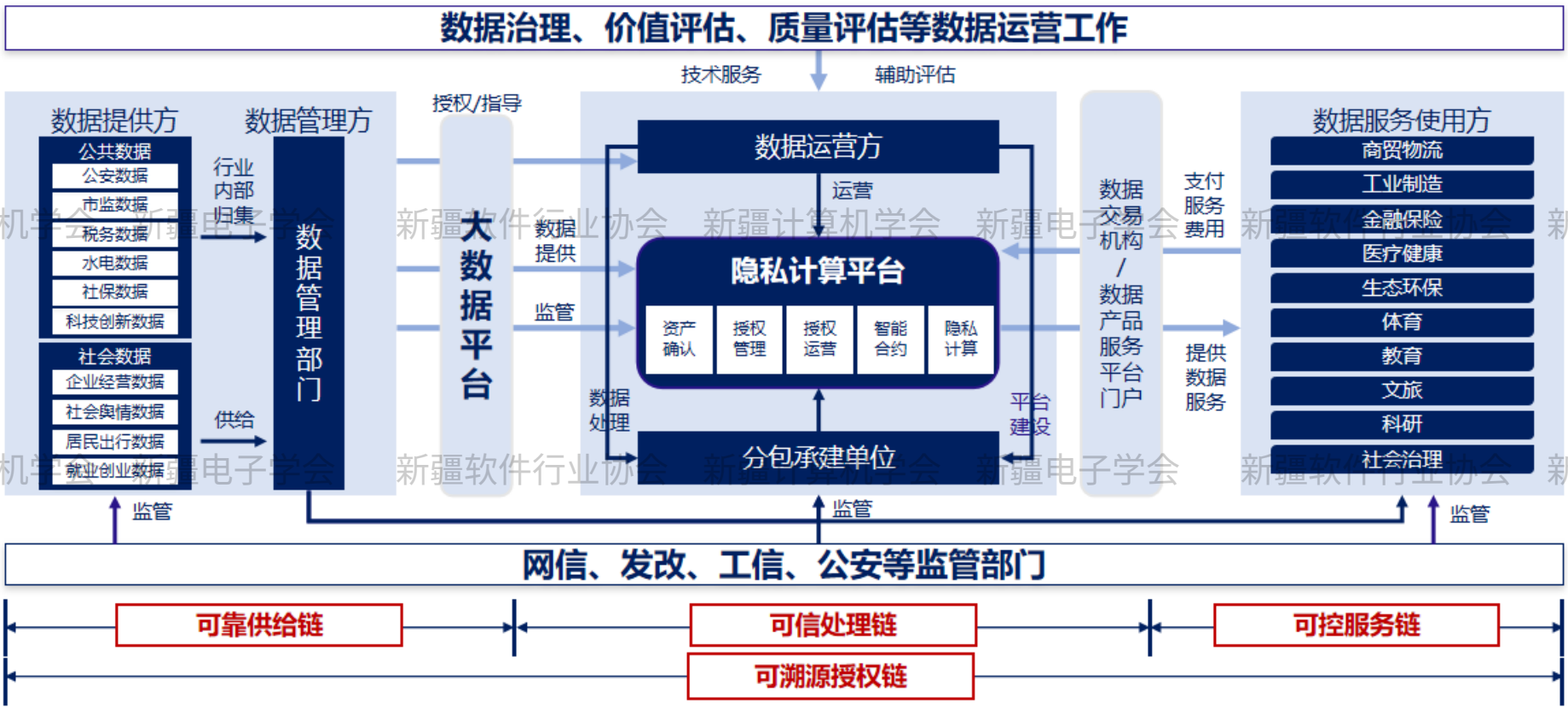
实现以数据保护为核心的安全防护能力

针对数据流转路径，开展数据安全防护建设，在数据连起来、跑起来、用起来的情况下，全面系统又有重点的保障数据安全的可用性和安全性。

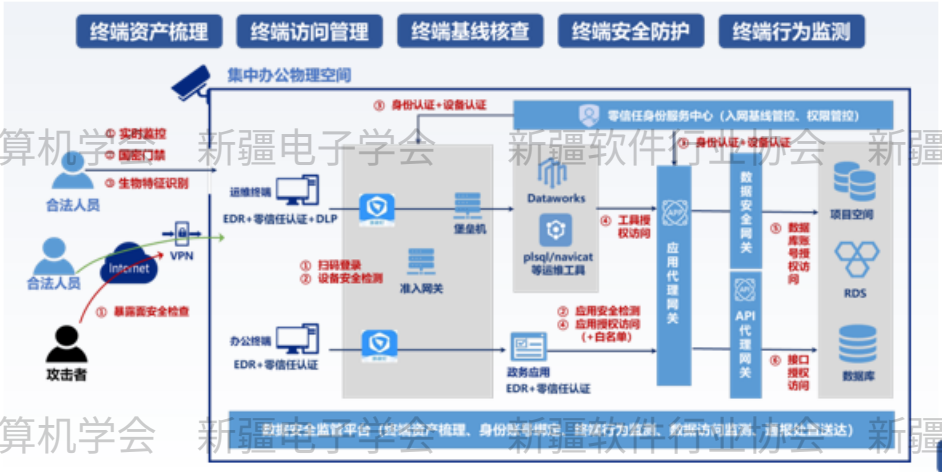


实现“数据可用不可见”的流通加工安全环境

以隐私计算为核心技术，在数据的“可用不可见”的情况下融合多方数据，输出可利用的结果，促进敏感数据在合规的前提下高效流通使用，推动政务服务，赋能经济发展。



完善基于场景的精细化管控能力

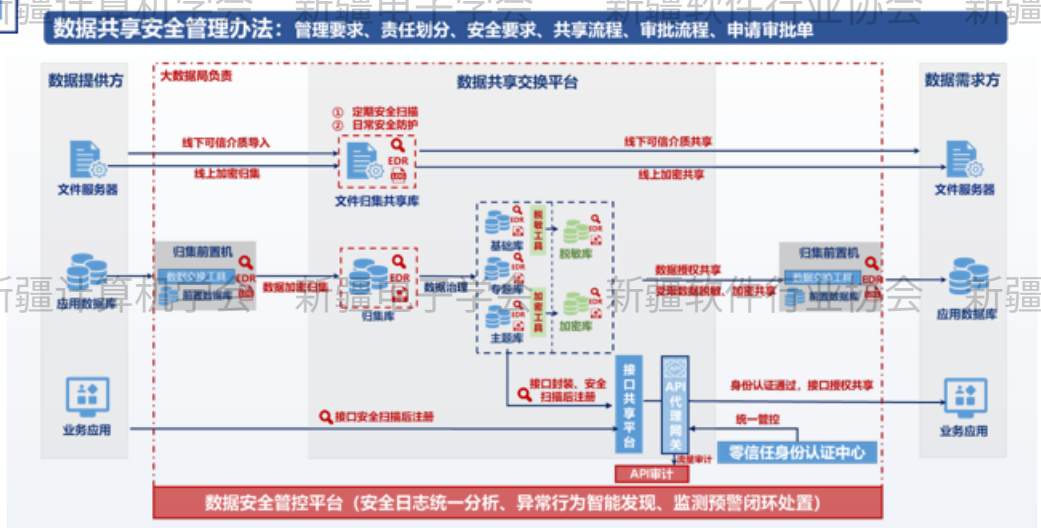


数据开发运维场景

依次通过物理环境管控、终端风险识别、身份认证、权限识别、脱敏加密等，在人员和数据中间建立可信的访问通道，确保风险人员“进不来”，受控数据“拿不走”，保障开发运维过程中的数据安全。

数据共享交换场景

针对文件共享、数据批量共享、数据接口共享三种数据共享交换方式，通过服务器安全防护、数据审批授权、共享日志分析、策略规则匹配等，实现“事前管审批、事中全留痕、事后可追溯”的共享安全闭环管理。



统一运行管控：基于态势感知平台实现闭环管理

早发现、早预防、快响应、高协同

日常安全运维管理模式

SOAR
SOAR智能编排

自动化编排和响应处置

通报和处置

应急处置组

安全运维团队

- 风险评估组
- 威胁监测组
- 应急处置组
- 安全情报组
- 建设加固组

操作流程规范

- 风险评估组
- 威胁检测组
- 应急处置组

运维流程优化

安全运维工作

资产管理 → 风险评估 → 监测预警 → 闭环处置 → 安全检查、日常培训等强化工作 → 定期总结复盘

警告

处置

绩效考核

制度完善

安全统一运行中心

资产管理中心	安全防御中心	安全监测中心	安全响应中心	评价提升中心
安全数据中台		安全能力中台		

制度规范体系

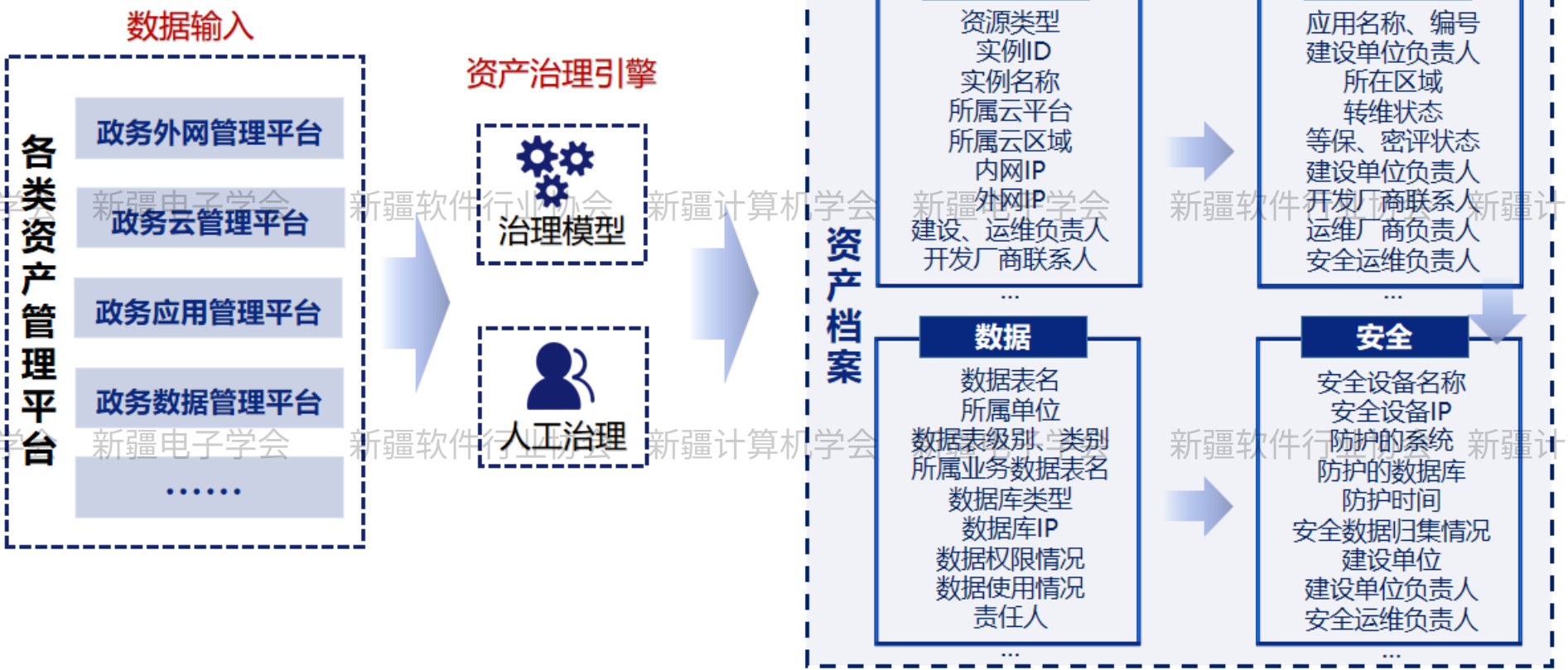
资产入网管理制度	安全考核管理制度
新系统风险管理制度	风险评估管理办法
安全漏洞管理制度	....

运营效果考量

管理制度完善

实现全网络的资产统一管理

基于多平台对接，通过模型和人工治理的方式，梳理云网、应用、数据、安全等主要资产的管理要素，厘清关联关系，建立全网安全资产一本账。



制定分级别的数据安全管控规则

• 公共数据授权访问分级管理

针对数据、人员级别，制定数据访问权限矩阵

人员级别 \ 数据级别	L1不敏感	L2低敏感	L3较敏感	L4敏感
L4人员	无条件访问	无条件访问	无条件访问	授权访问 脱敏访问
L3人员	无条件访问	无条件访问	授权访问 脱敏访问	授权后 脱敏访问
L2人员	无条件访问	无条件访问	授权后 脱敏访问	无权访问
L1人员	无条件访问	授权访问	无权访问	无权访问

• 公共数据共享与开放分级管理

针对数据级别和条数，制定数据共享开放矩阵

数据条数 \ 数据级别	L1不敏感	L2低敏感	L3较敏感	L4敏感
3000以上	无条件共享	无条件共享	评审后 受限共享	不共享
3000条				
1000~3000	无条件共享	无条件共享	授权后 变形脱敏 受限共享	不共享
1000条				
0~1000	无条件共享	无条件共享	授权后 遮盖脱敏 受限共享	评审后 受限共享
0条				

构建精准智能的安全预警规则

基于对安全数据的统一治理，明确网络和数据安全告警规则，规定每个告警项目的日志源、规则策略、结果输出，规范化安全预警工作，利于平台对接，实现全域预警告警规则共建共享。

对接要素

- 终端
- 应用
- 数据
- 云网

- 资产清单
- 日志数据
- 流量数据

风险监测规则

资产	类型	规则名称	规则说明
应用	波动检查	用户访问量的同比	用户访问总量同期比翻倍
		响应时长（RT）同比	用户请求时长同期比翻倍
		……	
	访问异常	VPN账号来源地址较多	一天内VPN登陆的来源地址较多，多于10个时为高危
		用户访问响应超时	用户访问请求时长大于5秒
		……	
	百分比检查	用户访问成功率	用户访问成功率低于90%
		用户访问失败率	用户访问失败率高于10%
		……	
	主动探测	应用漏洞情况	存在的已知漏洞
数据	任务检查	任务执行超时	数据采集任务执行时长
		任务执行状态异常	数据采集任务状态异常
	安全感知	数据批量导出不合规	导出表字段与申请不匹配
		接口异常-url中存在密码信息	接口传输过程中未对密码进行加密
		……	
云网	ECS等	CPU、内存使用率	CPU、内存使用率超过 80%
		挖矿病毒	资源使用率超99%，疑似挖矿
		……	

规则模型 | AI模型 | 统计模型 | 关联模型 | 情报模型

风险监测结果

风险结果	示例
预警告警名称	响应时长超阈值
预警级别	预警
应用编码	A20230220000001
应用名称	XX应用系统
连续预警次数	2
告警时间	2023-03-31 8:31
是否响应	是
响应时间	2023-03-31 8:33
是否处置	是
处置时间	2023-03-31 8:35
告警内容	响应时长超阈值
规则名称	用户访问响应超时
资产id	S20230322000001
阈值	>5秒
实际告警值	9秒
预警告警发生时间	2023-03-31 8:30

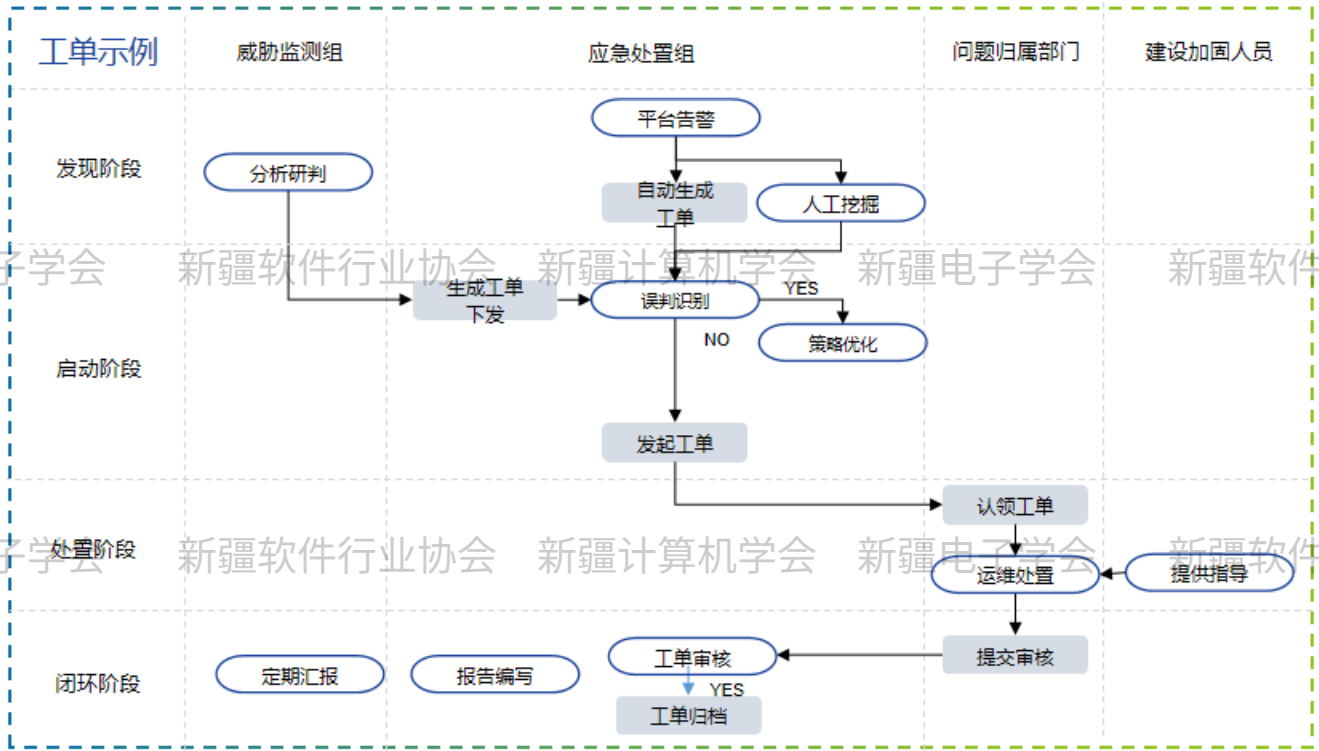
建立高效协同的应急处置规则

基于对安全风险和事件的分析，建立应急处置规则，并实现应急处置知识共建共享，提高全域应急效率，降低损失。

完成闭环的风险事件处置

建立健全安全风险和事件的闭环处置流程，实现重大风险隐患1小时内定向通知到指定责任人，方便快速响应处置风险隐患事件，各单位响应和处置过程全程流痕。

- 预警发布
- 应急响应
- 日常工单
- 安全巡检
- 变更流程
- ……



快响应 | **快通知** | **快止血** | **快恢复** | **快复盘**

统一能力指标：制定安全建设及评估指标

建立省市县三级的网络和数据安全评估指标，对各单位的三大体系安全建设情况进行量化评估，实现**以评促建、以评促优**的目标。

得分	标识	组织机制建设	管理制度落地	技术能力应用	运行管控规范
基础	★	有兼职安全管理和运维人员	部分制度制定	技术防护能力建成	有风险能处置
达标	★★	有专职安全管理和运维人员	制度建设完备	技术防护能力基本应用（通用规则）	有规范化的预警和处置流程
良好	★★★	组建安全管理和运维团队	制度完备并全域推行	技术防护能力根据场景配置规则	重点资产具备预警处置闭环管理
优秀	★★★★	组建安全管理和运维团队并明确责任	制度完备并有效执行	技术能够覆盖重点资产并配置规则	横纵联动，实现闭环管理并迭代优化

省市县（区）三级分阶段有序推进

全省安全能力建设应统筹规划，按照“省级”“市级”“县级”三个层级开展，并按照四星评价来衡量每项能力建设的完备程度。

序号	能力项	省级	市级	县（区）级
1	等保合规能力	★★★★	★★★★	★★★
2	密评合规能力	★★★★	★★★★	复用上级
3	分类分级	★★★★	★★★★	★★★
4	零信任身份认证	★★★	★★★	★★
5	权限管控	★★★★	★★★★	★★★
6	接口审计	★★★★	★★★★	★★★
7	态势感知	★★★★	★★★★	★★★
8	数据加密	★★★	★★	★★
9	数据脱敏	★★★★	★★★	★★
10	数据水印	★★★	★★	★★
11	隐私计算	★★★	★★★	复用上级
12	区块链	★★★	★★	复用上级
13	数据销毁	★★	★★	★
14	……	……	……	……

新时代新征程

势必守好网络和数据安全!