《数字时代—基于行业最佳实践的安全保护框架》

数十位产业、行业安全专家智慧结晶

PCSA • 数世咨询 • 数说安全• CIO时代/安全学院

中国信息协会 信息安全专业委员会

2022年6月18日 联合出品

聚合中国关键安全能力，赋能数字智能时代

第三篇：《数字时代—基于行业最佳实践的安全保护框架》核心思想解读

郭峰，北大硕士，中科大工程博士在读。PCSA安全能力者联盟首席专家，中国信息协会信息安全专业委员会理事，多个监管单位和中央部委安全专家库专家，央企安全联盟智库特聘安全专家，中国电科太极股份首席安全官，电科云特聘首席安全专家，药品监管信息化研究专业委员会委员。

二十余年服务监管单位、中央政府、中央企业，承担数百项网络安全重点工程，长年提供网络安全重保及服务。

承担网信办、国家发改委网络安全等多个专项课题，发表研究成果核心期刊和专业刊物、学术论文、观点等十余篇。

获得MCSE/TCSB/CCNA/CISP/SM信息系统/ITILV3Foundtion认CISI/CISA等十余项专业认证。

近年致力于网络空间安全领域的研究与科技创新，聚焦关基安全、数据安全、供应链安全、资产安全、智能安全等。

研究背景：安全从合规走向实战&协同

信息化 体系化

第一阶段：合规基础驱动

2004-2016

- 等级保护 系列
- F级保护 系列
- **监管部门**推动完成基础合规、体系建设
- **运营单位**完成基础安全管理、技术……
- **网安产业**初成长，研发安全点能力，局部突破安全线能力，合规推动产业发展。

数据化 数字化

第二阶段：实战强化驱动

2016年-十四五

- 等级保护 2.0系列
- 新政策 关基、数据、供应链安全等系列
- **监管部门**推动新政策出台，组织实战演练
- **运营单位**需要满足监管新要求，实现看管监控一体化，面对实战化，实现平战结合一体化，安全走向场景业务化、平台化、运营化，亟待解决多年共性问题顽疾，实现管理、技术、运营的体系融合一体化.....
- **网安产业** 需要研发新型安全能力，聚合基础资源，打造一体化弹性平台

智能化、智慧化

第三阶段：协同保护驱动

未来

- 总体安全观强化，新形式、新政策
- **监管部门**协同关基单位、重要数据中心、重点行业、城市进行国防级协同保护联动
- **运营单位**逐步完成基础安全、强化安全、协同安全建设，满足数字化转型，解决基础资源数据化、安全能力生态化，逐步实现自动化、智能化和智慧化的协同保护安全
- **网安产业**AI+Sec智能化、信息情报共享、战略预警、多层协同监测、响应、分析与防御实现是主要发展方向

安全政策：密集出台 运营单位应接不暇

国际安全形势日趋严峻，监管日趋严格，安全法律法规密集出台，各行业开展十四五安全规划，如何进行多体系融合，需要一个能够参考的安全保护框架，将**安全战略与业务发展融合，原体系与新要求融合，安全管理、技术与运营融合一体化，监管视角看管监控融合一体化，实战场景下的平战融合一体化。**

一个安全保护框架的重要性凸显：

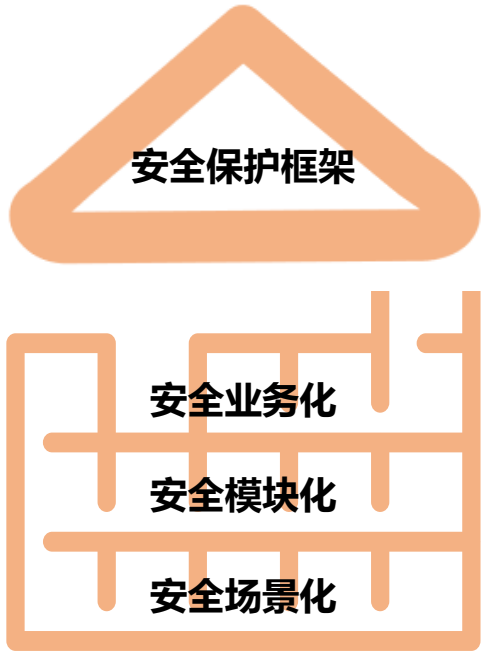
- 新监管要求、政策频出，如何有序落地
- 新监管要求、政策与现有安全体系如何融合
- 满足安全监管新要求：实现看管监控一体化
- 满足安全实战化趋势：实现平战结合一体化
- 满足行业数字化转型：实现安全管理、安全技术、安全运营融合一体化
- ……

安全工作：从困惑到清晰

角色	困惑及问题
监管部门	**如何落实：**指导、监督、检查、保护、保卫、保障……
安全运营单位 — 安全决策层	**全局视角：**安全战略？安全投入？业务匹配度……
安全运营单位 — 安全管理层	**战略一致性：**保护对象？攻防状态？风险隐患？考核评价……
安全运营单位 — 安全执行层	**模块化工作：**安全闭环？处置效率？一体化？实战效果……
安全运营单位 — 安全运营层	**运营操作：**资产？漏洞？安全能力？安全运营流程……
安全产业界	**如何助力：**安全标准？安全趋势？新需求？新安全能力……

持续研究

积木式积淀



感谢：数十个产业、行业安全专家共同研讨，凝聚智慧结晶，形成较为清晰、可落地实践的安全保护框架！

数字时代：基于行业最佳实践的安全保护框架

总体国家安全观/国家网络空间安全战略

网络安全法 数据安全法 保守国家秘密法 密码法 个人信息保护法 关键信息基础设施安全保护条例 网络安全审查办法等

网信办 公安部 保密局 密码管理局 工信部 国资委 人民银行 能源局等监管部门及各行业主管部门相关要求 业务战略及数字化规划

资源保障

安全战略宣贯

多机构
多部门
多角色
多环节

组织机制保障

决策层
管理层
执行层
运营层

持续资金保障

连贯性
延续性
敏捷迭代
弹性扩展

安全常态化

平战结合一体化

指挥协同保护层

组织内部协同 ⟷ 监管部门 行业主管部门协同 ⟷ 行业单位协同

最佳实践 情报信息 漏洞信息 安全事件 | 信息共享 | 安全场景化 决策智慧化 | 指挥协同 | 资源协同 能力协同 应急协同 生态协同

实战强化保护层

精准研判预测

规则算法 专题研判 精准预测
IP研判 ID研判 事件研判 多维威胁研判
攻击链研判...

多维多源 叠加计算

快速持续响应

多角色联动 高效响应
战时：备战 迎战 决战 复盘
平时：发布 执行 跟踪 闭环

持续快速 实时响应

安全运营体系

神经域
认知域 智能化引擎 识别域
可信任/可训练/可持续数据

动态纵深防御

主动 精准 快速 动态
技防策略动态评估 剧本编排 手动防御
半自动防御 全自动防御 适度反制 一键解封...

实时防御 编排调度

全维全域监测

实时动态 快速深度 能力生态化
暴露面 安全域边界 网络层 主机系统层
数据层 应用层 平台层 用户层 策略层...

可信降噪 实时监测

数据安全运营

底账普查 权益认定 准入准出 数据画像 加密脱敏 分层类级 动态监管 权限可控 状态可察 全程可视 流动追溯

资产安全运营

动态底账 准入准出 多维画像 分层画像 精准关联 快速定位 持续变更 历史实时 弱点可控 全景可视

神经中枢

业务中枢 数据中枢 平台中枢 安全中枢 运行中枢

保护对象

业务系统 基础网络 大型专网 云平台 大数据平台 物联网 工业控制系统 智能制造系统 新型互联网 新兴通讯设施 ...

融合

首席安全官 技能考核
保护计划 监督问责
多人专岗 强化培训

融合

关键业务链识别 攻防演练
协同联控 仿真验证
有效性检测 威胁情报

安全业务化

看管监控一体化

能力提升

匹配业务发展

业务愿景
数字化规划
行业特点
发展步调

强化安全同步

同步规划
同步标准
同步建设
同步使用

夯实软硬实力

安全意识
人才技能
平台工具
安全威慑

强化

强化

安全管理体系

管理制度 管理组织 人员管理 建设管理 运维管理 考核管理

安全技术体系

物理安全 网络安全 主机安全 应用安全 数据安全 平台安全

合规基础保护层

等级保护
一个中心 三重防护 五级保护
定级备案 建设整改 等保测评 监督检查

F级保护
严控红线 技管结合 三级保护
系统定密 系统建设 系统测评 上线运行

数据安全
主责数据保护 安全与开放 流动安全监管
分类分级 风险评估 应急处置 安全审查 出口管制

密码保护
核心 普通 商用 两类三级
四类机构 范围明确 密评合规审查

商业秘密
全程全域 四个阶段 两级要求
明确范围 系统对标 规划实施 运行废止

个人信息保护
信息处理规则 信息跨境规则
权利与义务 职责与法律保护

...

延伸

健全制度 完善机制 构建组织 梳理底账 准入验证 安全审查 动态监测 持续改进

延伸

供应商
匹配性 可靠性 稳定性 信誉度 透明度 成熟度

第三方人员
保密协议 背景调查 权限管控 安全技能

信息服务
安全设计 安全建设 安全运行 评测审计

ICT供应链管理及网络安全审查

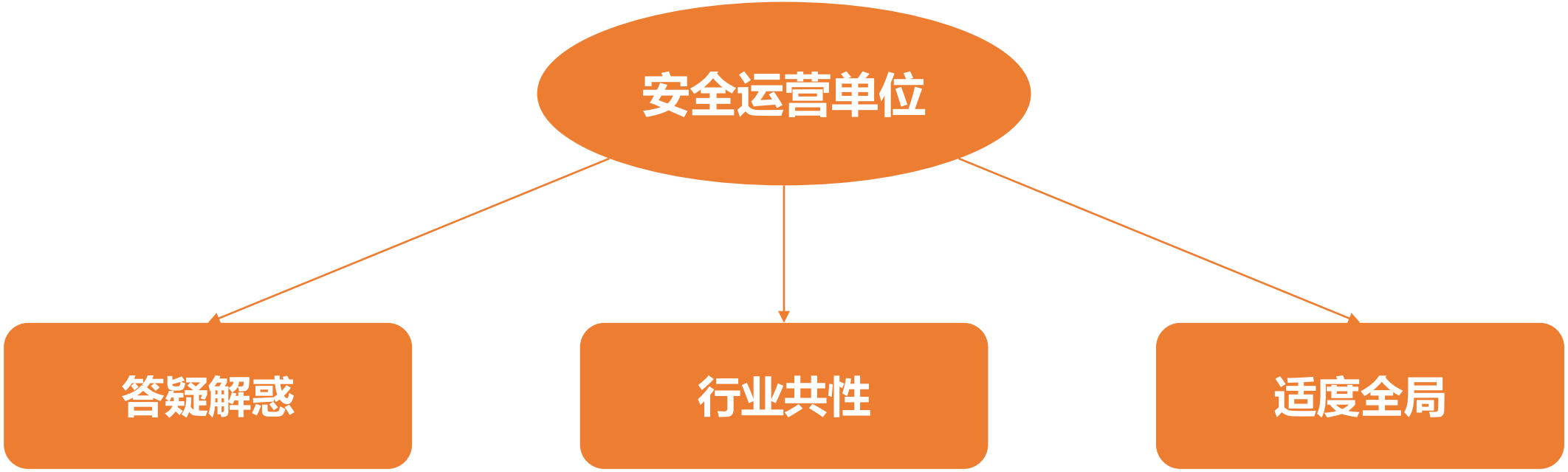
软件开发
开源检测 代码质量 上线评测 持续评估

系统硬件
稳定可用 安全可靠 冗余备份 信创可控

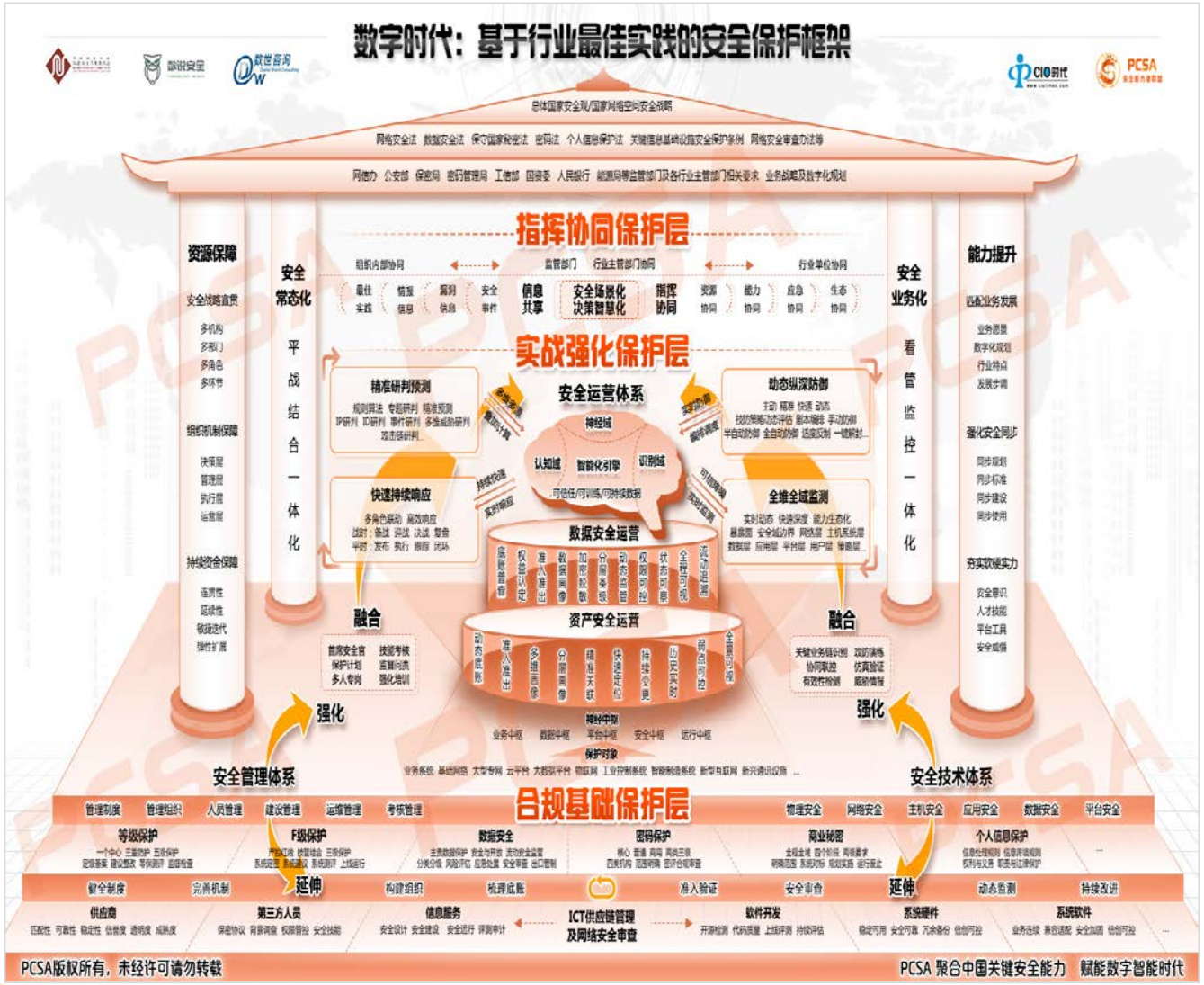
系统软件
业务连续 兼容适配 安全加固 信创可控 ...

PCSA 聚合中国关键安全能力 赋能数字智能时代

安全保护框架的定位


安全运营单位
答疑解惑
行业共性
适度全局
不同角色
不同视角
不同困惑
共性问题
共性顽疾
共性经验
宏观全局
中观架构
微观要素

安全保护框架：“1-3-3-4” 架构



一、“1”个顶层指引：自上而下

总体国家安全观：国家网络空间安全战略+（网络安全法律法规标准规范及监管要求、组织战略）

二、“3”个安全体系：融合一体化

安全管理体系、安全技术体系、安全运营体系

三、“3”个保护层次：模块化

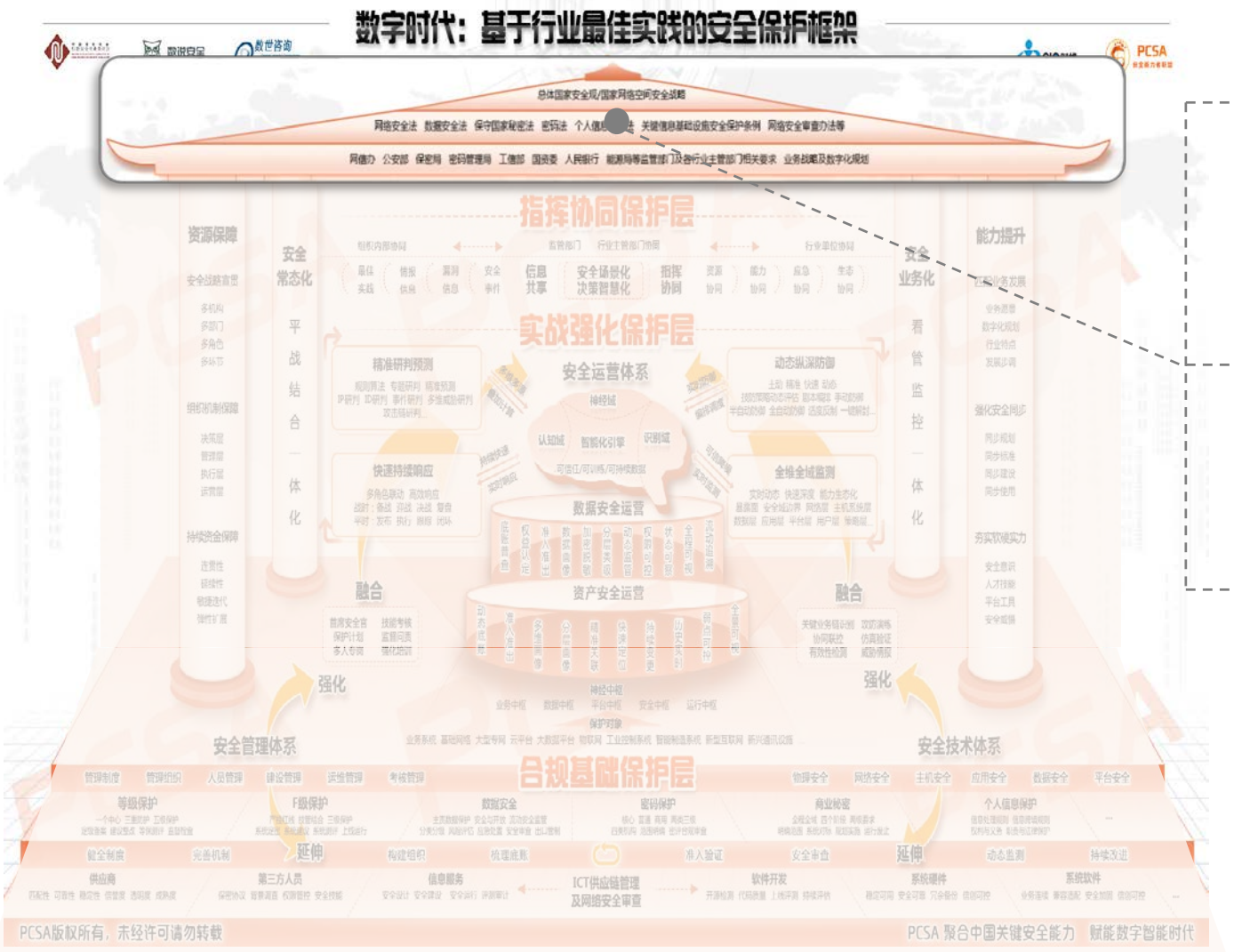
合规基础保护层、实战强化保护层、指挥协同保护层

四、“4”个重要支柱：有效落地

资源保障、能力提升

安全常态化背景、安全业务化趋势

安全保护框架：“1”个顶层指引



一、总体国家安全观

涵盖16种安全：政治安全、国土安全、军事安全、经济安全、文化安全、社会安全、科技安全、**网络安全**、生态安全、资源安全、核安全、海外利益安全、生物安全、太空安全、极地安全、深海安全等于一体的国家安全体系

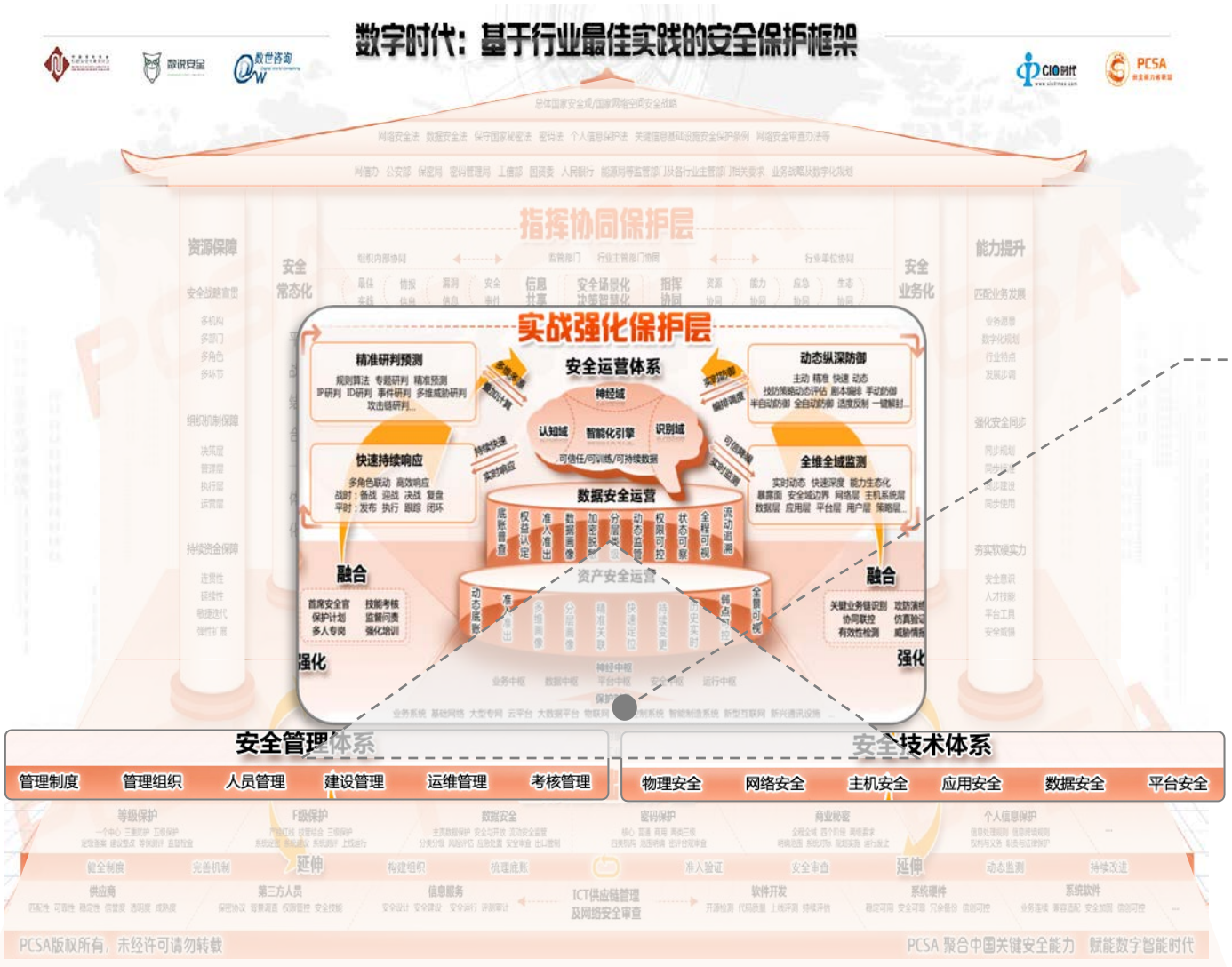
二、国家网络空间安全战略

维护国家网络空间主权、安全、发展利益，推动互联网造福人类，推动网络空间和平利用和共同治理

三、网络安全法律法规、标准规范、监管部门及行业主管部门要求、组织战略

- **法律法规标准规范：**覆盖网络安全、数据安全、密码安全、个人信息保护、供应链安全、关键信息基础设施安全等主要方面
- **监管部门及行业主管部门要求：**网信办、公安部、密码管理局、工信部、国资委、人民银行、能源局等监管部门及行业主管部门
- **组织战略：**业务战略，数字化规划等

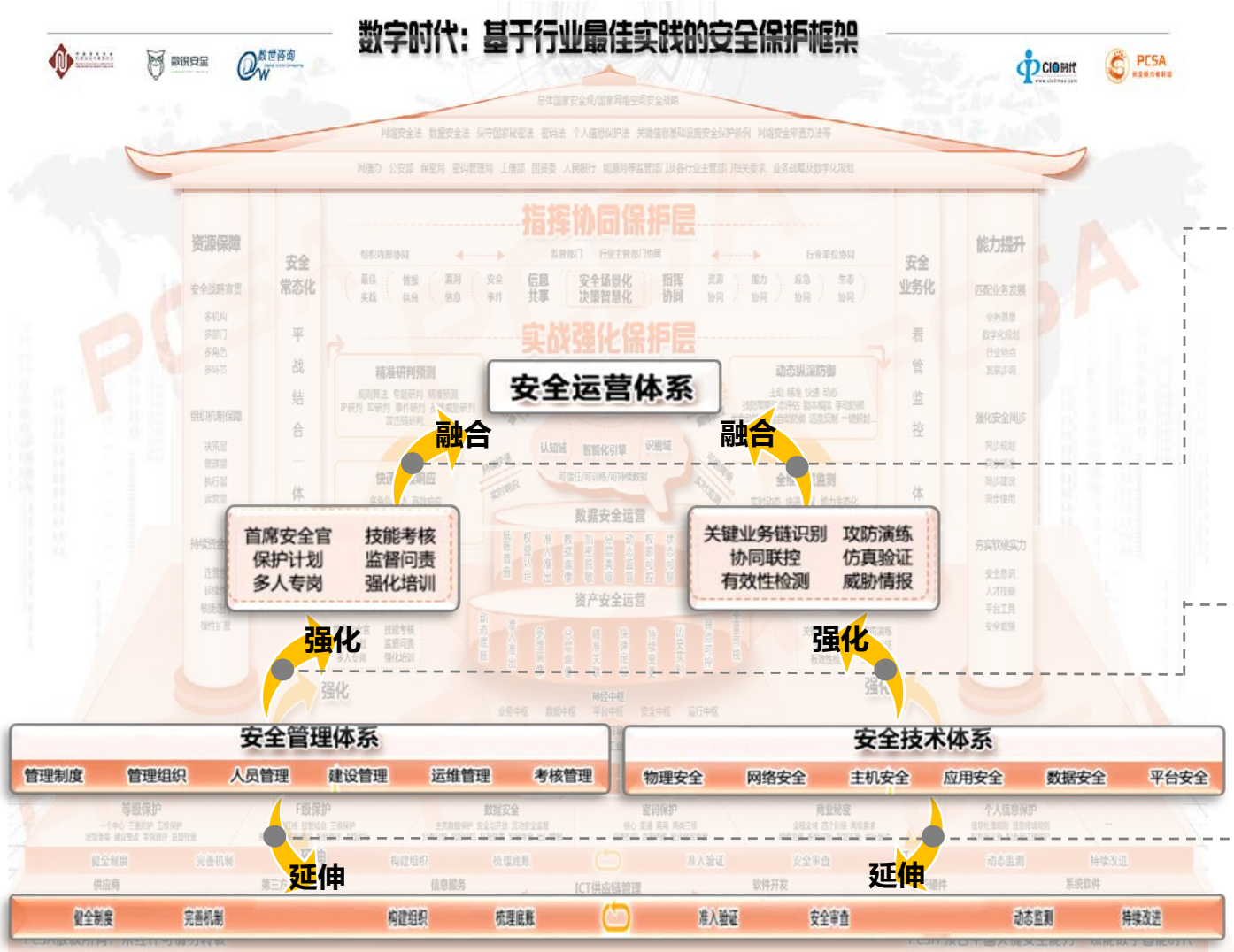
安全保护框架：“3”个安全体系



完善安全管理体系、安全技术体系，构建安全运营体系，实现安全管理、安全运营、安全技术的常态化运转

- **安全技术体系**：梳理保护措施、整合防护手段、构建异构安全能力
- **安全管理体系**：落实管理制度、优化管理组织、强化管理考核
- **安全运营体系**：组建运营团队、制定运营流程、搭建运营平台

安全体系一体化：延伸、强化与融合



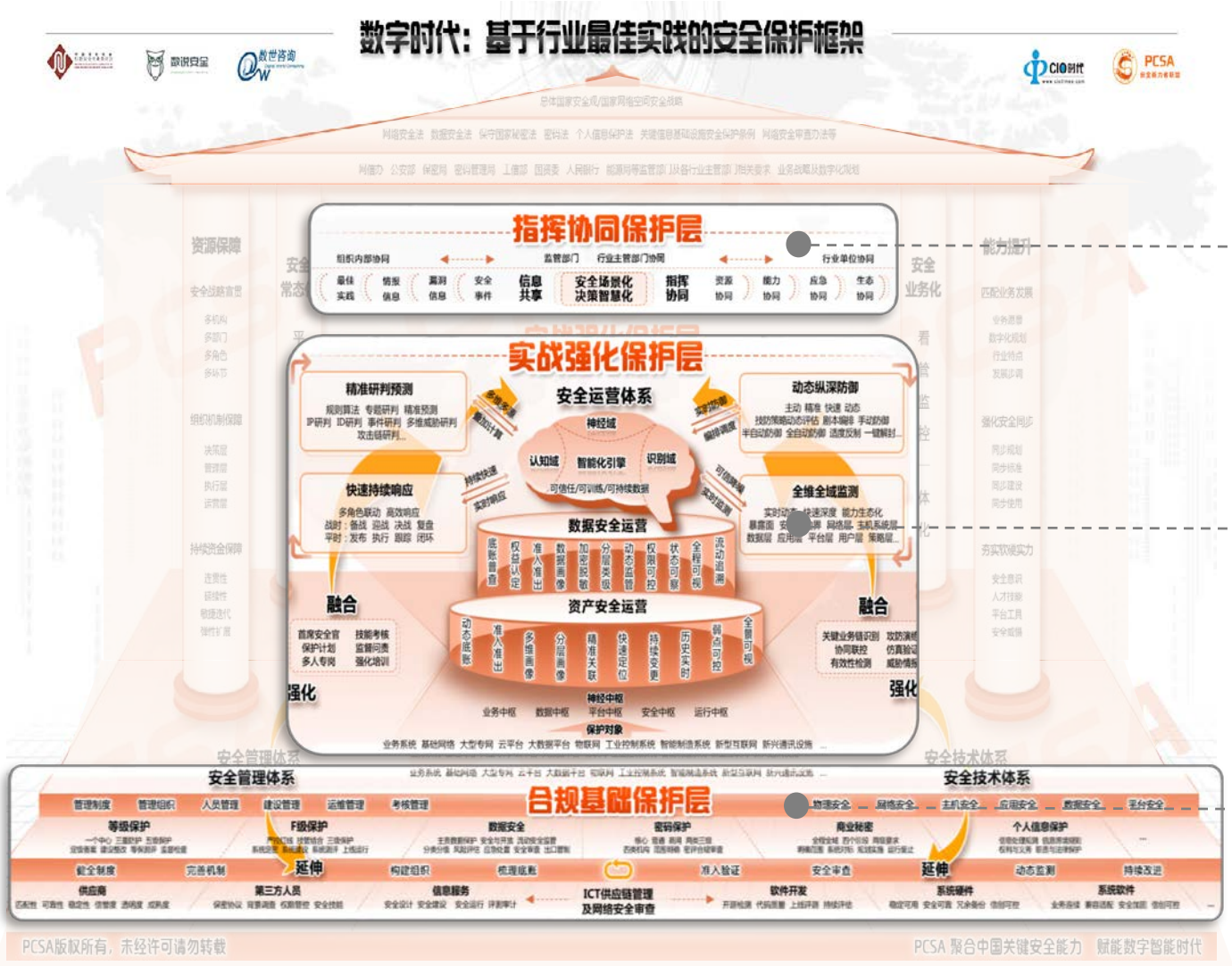
融合：将安全管理体系、安全技术体系融入到安全运营体系，实现一体化运转

- 将安全管理体系中建立的各类制度标准、组建的团队人才融入安全运营体系，实现安全管理指标化、管理运营团队一体化
- 将安全技术体系中建立的各类安全能力探针融入到安全运营体系，实现异构安全能力生态化横向打通

强化：面向体系化对抗，强化安全管理和安全技术要求，全面提升管理和技术能力

延伸：面向系统性风险，聚焦供应链安全，延伸安全管理和安全技术要求

安全保护框架：“3”个保护层次



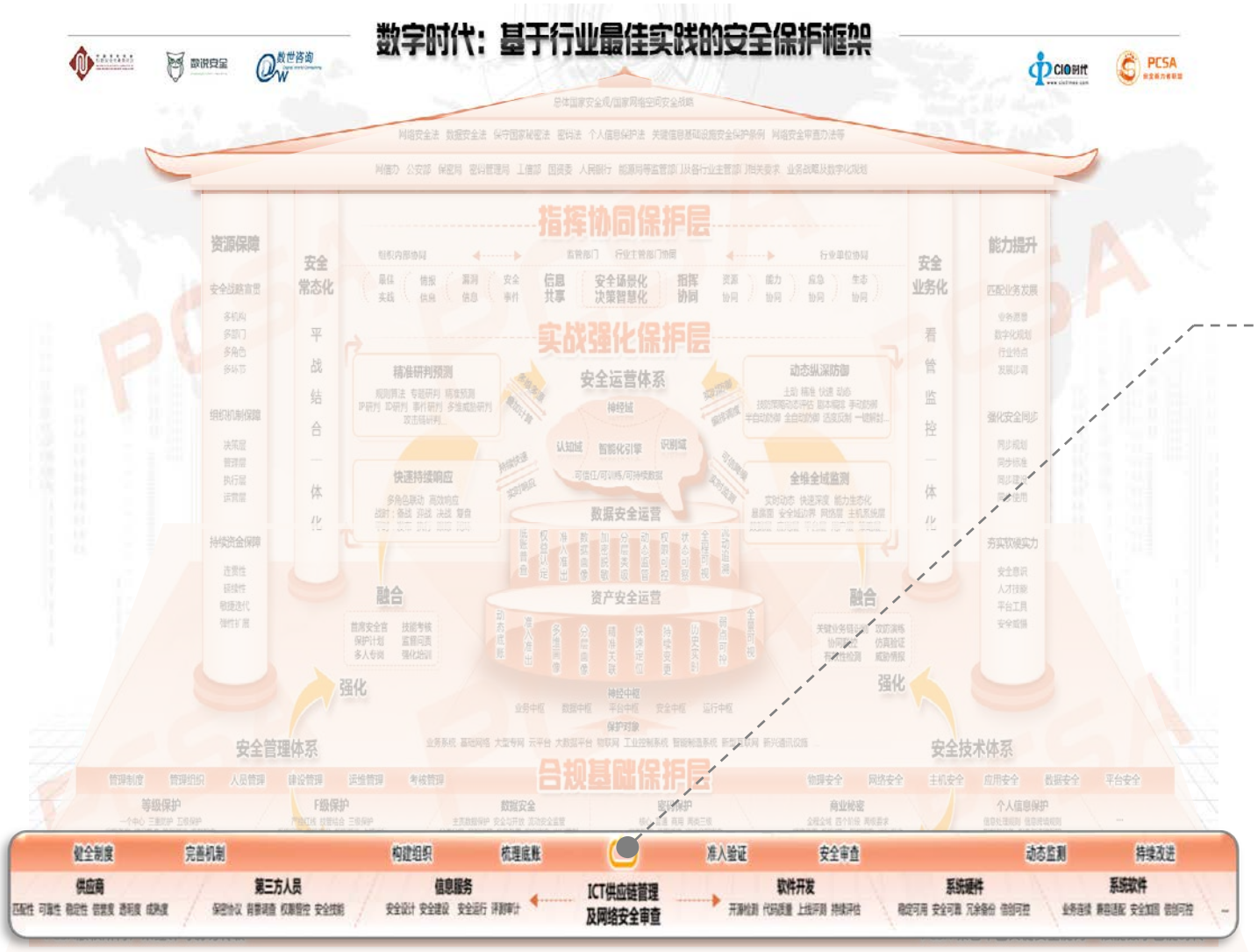
基于不同的安全成熟度、保护对象重要程度、体系建设完整度，循序渐进完善安全保护。

指挥协同保护层： 聚焦多场景、多角色、多视角下的联合协同（“海、路、空等多军种协同”），实现一体化指挥

实战强化保护层：重点强化高精尖装备配置（“侦查雷达、精准打击武器、导弹防御系统等”），提升情报侦察分析精准度和响应处置的效率

合规基础保护层：主要完成IT基础环境中供应链安全（“清洁的空气、干净的水、安全的食物”）和合规安全等基础工作（“城墙、步兵、弓箭手、陷阱、烽火台等能力”）

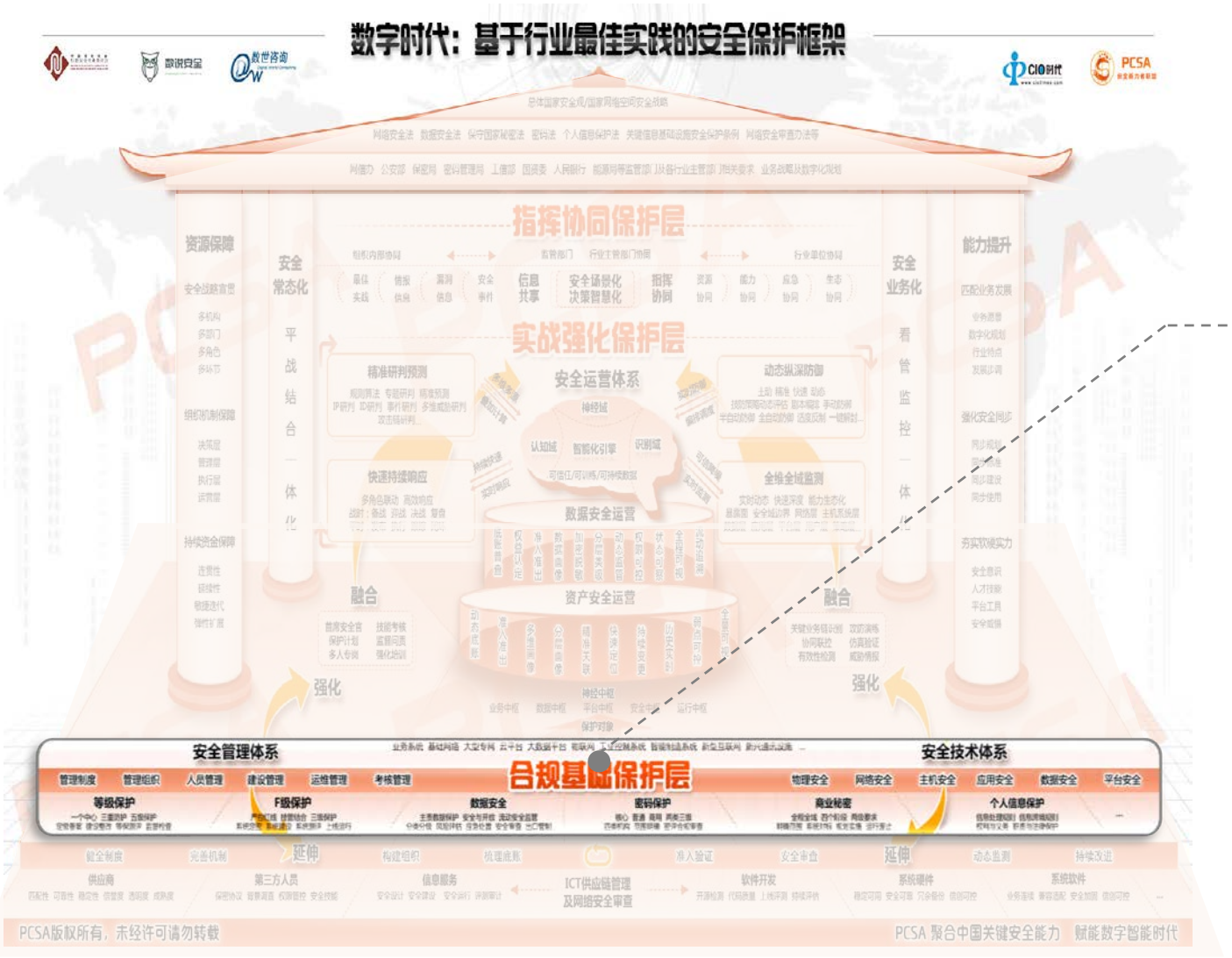
合规基础保护层：供应链安全



供应链安全：加强ICT供应链管理，落实网络安全审查要求，提升供应链条上网络产品及服务的安全保障能力

- 在安全管理层面，不断健全制度、完善机制、构建组织、梳理底账；在安全技术层面，通过准入验证、安全审查、动态监测、持续改进，形成有效闭环
- 面对供应商、第三方人员、信息服务、软件开发、系统硬件及系统软件等不同对象，有针对性地落实网络安全审查重点，从关键环节提升安全保护能力

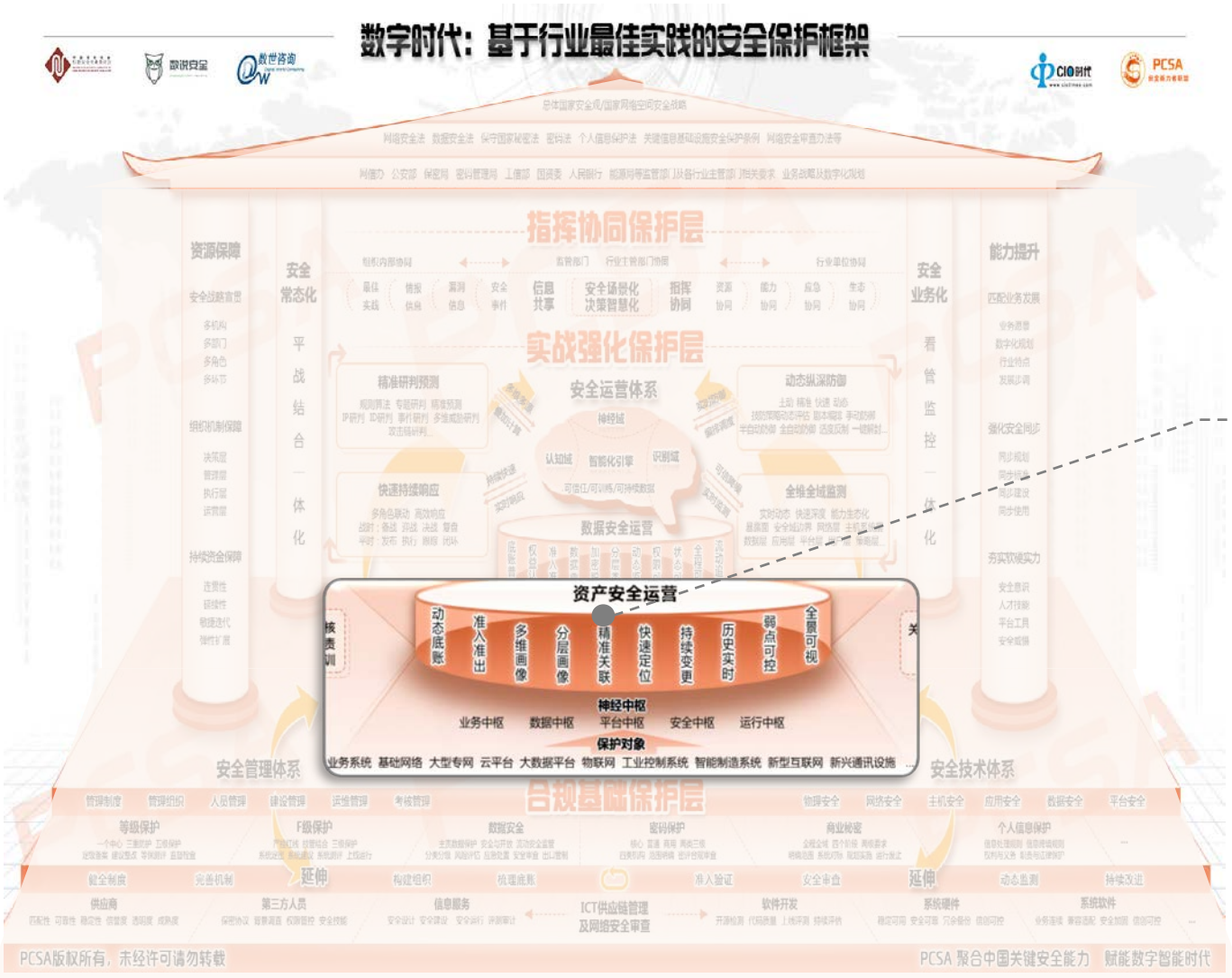
合规基础保护层：合规安全



合规安全：通过等级保护、F级保护、数据安全、密码保护、商业秘密保护、个人信息保护等合规工作的开展，逐步积淀出安全管理体系、安全技术体系

- 安全管理体系：聚焦管理制度、管理组织、人员管理、建设管理、运维管理和考核管理等内容
- 安全技术体系：聚焦物理安全、网络安全、主机安全、应用安全、数据安全和平台安全等内容

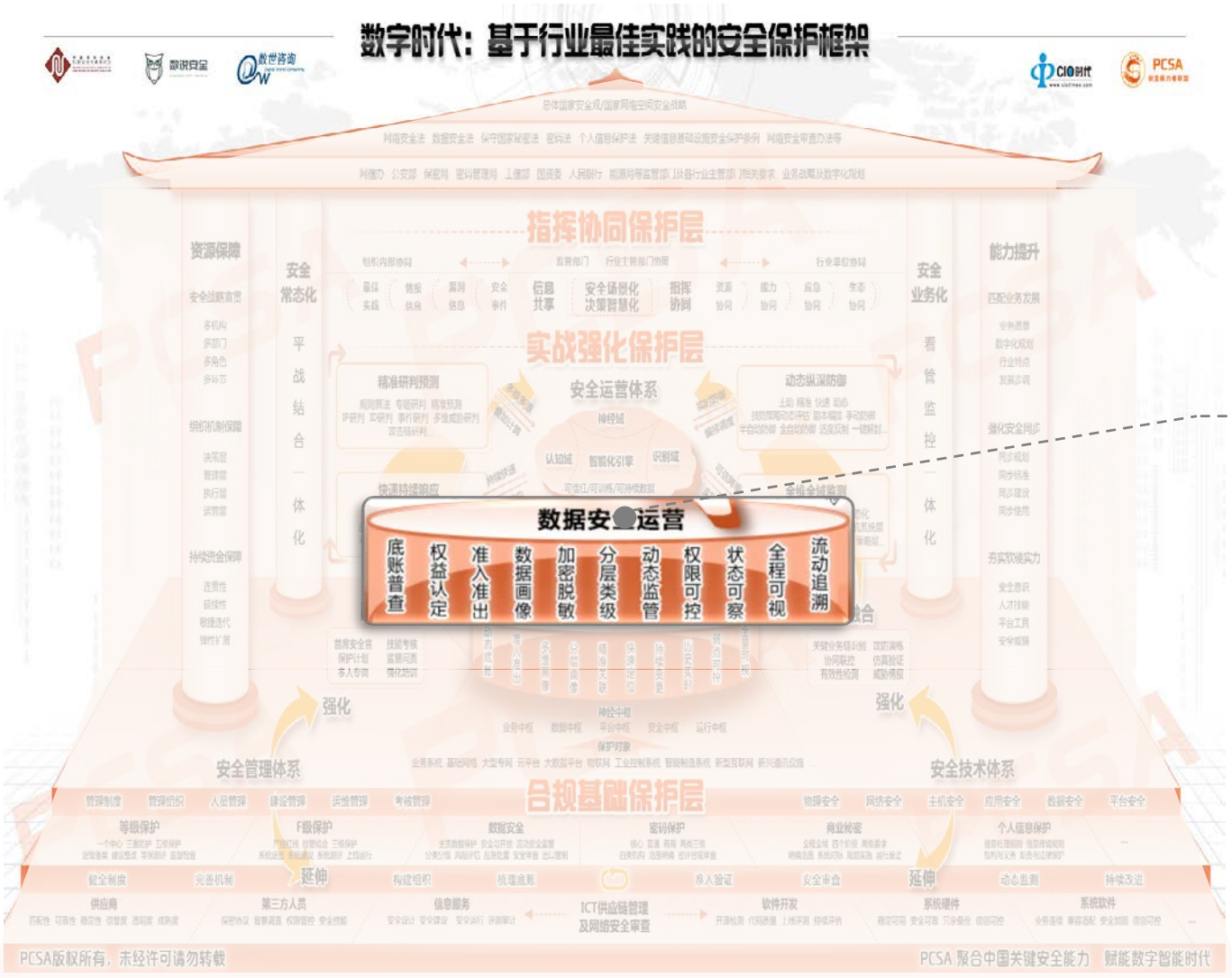
实战强化保护层：重点关键点-资产安全运营



资产安全运营：建立以保护对象为核心的资产安全运营中心

- 保护对象由信息系统、云计算、工业控制系统、物联网、移动互联等向神经中枢演变
- 围绕保护对象，清晰梳理IT资产动态底账，绘制多层级、多维度的全视角资产画像
- 构建资产与业务、服务、端口、权责等细粒度的关联分析模型
- 实现轻量与全量、历史与实时、动态与静态的资产安全运营

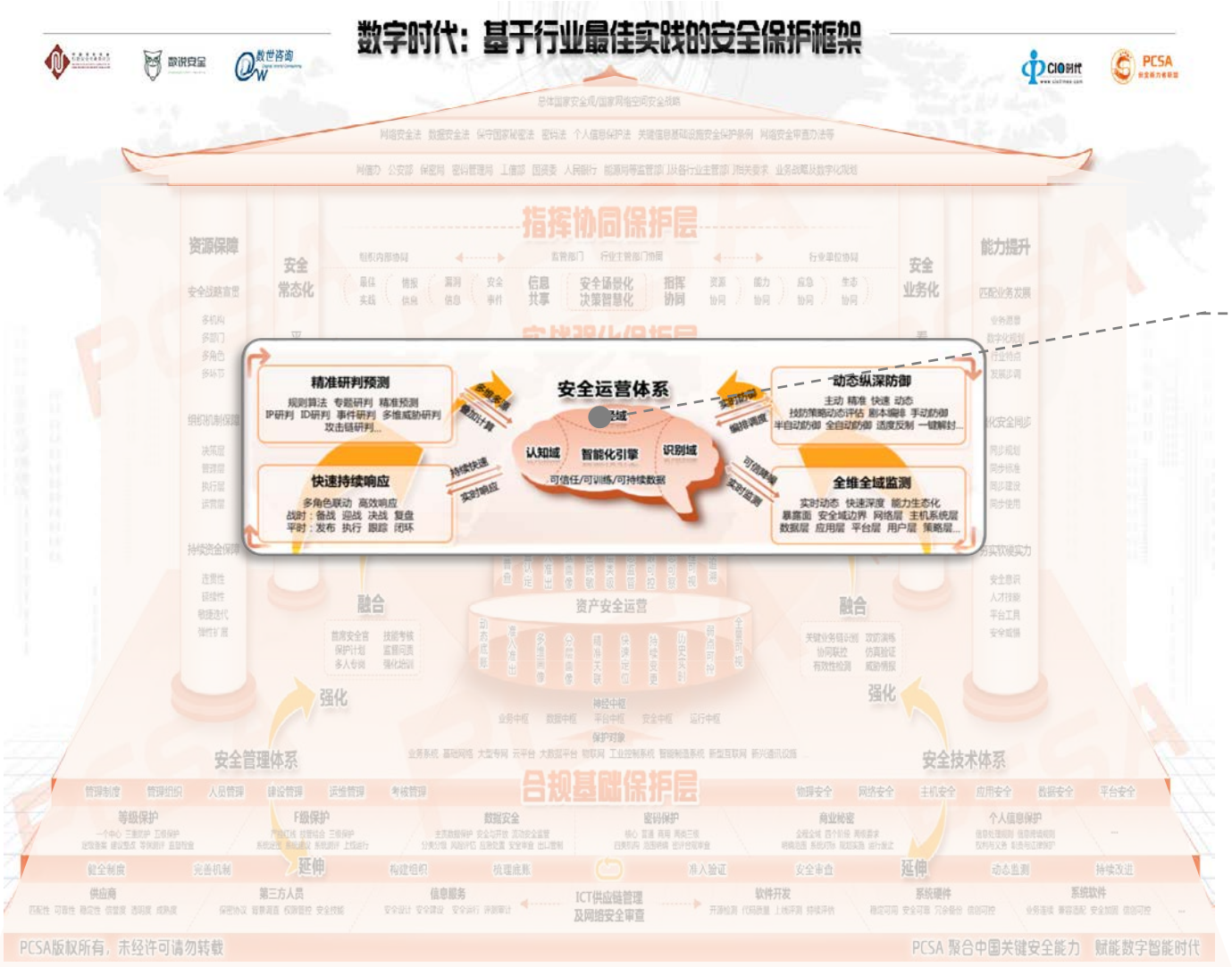
实战强化保护层：重点关键点-数据安全运营



数据安全运营：建立以数据权益保护为核心的数据安全运营中心

- 明确数据管理和安全管理责权利，清晰分工和边界
- 在数据全生命周期保护的基础上，聚焦数据价值释放流动场景，明确流动角色、流动场景、流动阶段
- 紧抓数据分类分级分层保护、数据确权、主责数据控制与保护、流动安全监管、数据流动审计追溯等关键点，构建数据权益和数据交易证明链
- 打造数据安全运营中心，深度融合数据安全技术、管理、运营、监管，实现安全监管一体系、数据态势一张图 ，流动监管一条线

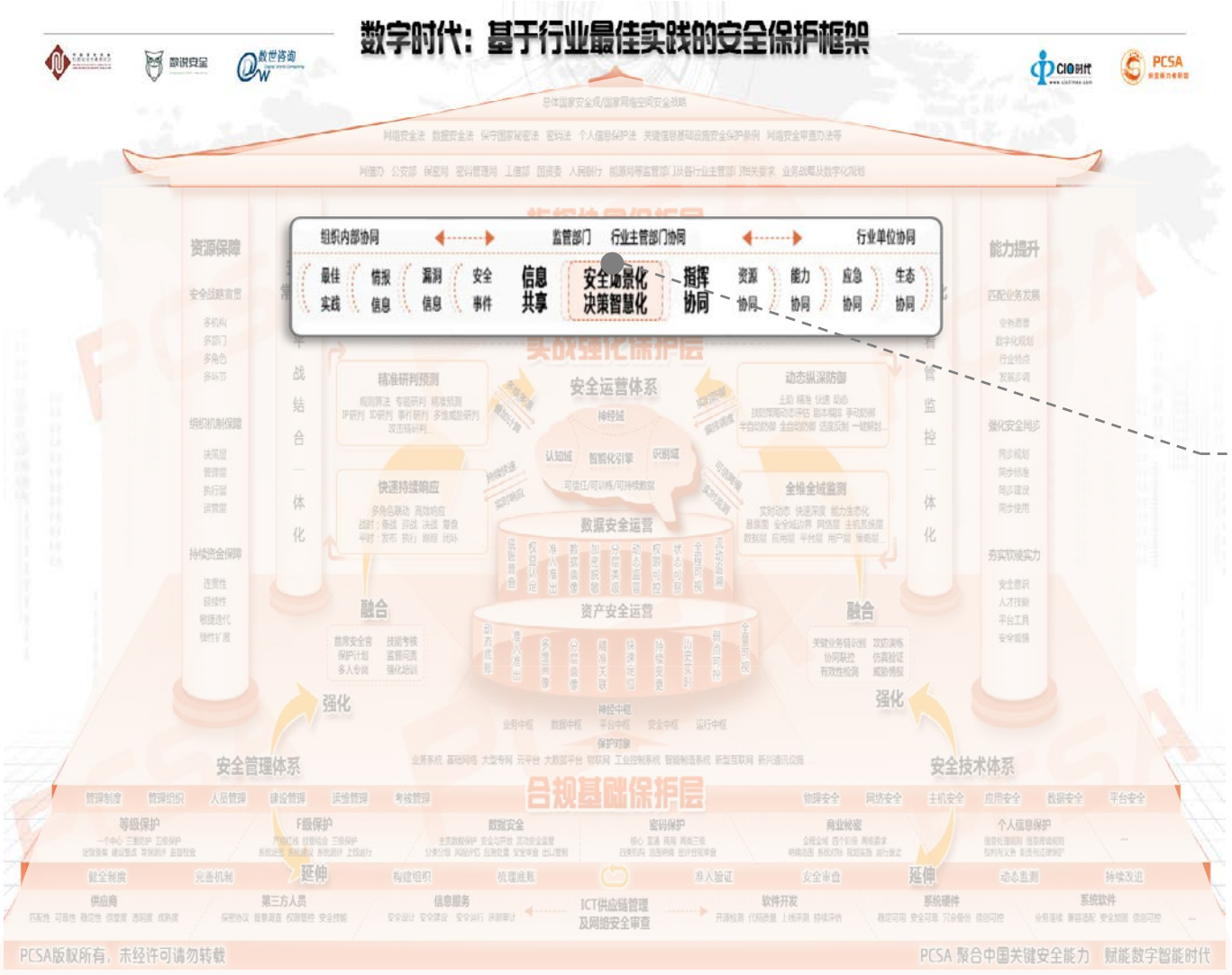
实战强化保护层：重点关键点-智能化安全运营



智能化安全运营：建立以智能化、实战化为核心的一体化安全运营中心

- **智能安全中枢：**聚合可信任、可训练、可持续的数据，利用智能分析与算法对抗主引擎，构建由“认知域、神经域、识别域”组成的智能安全中枢
- **全维全域监测：**建立横向到边、纵向到底全方位监测能力，实现能力生态化支撑下的多维度安全状态与风险的实时监测
- **快速持续响应：**建立平战结合、多角色联动的快速持续响应能力，实现过程跟踪与闭环管理
- **精准研判预测：**基于可信数据源，利用多类规则算法进行精准分析研判，预测事件发展趋势
- **动态纵深防御：**根据研判预测结果，基于剧本自动化编排，对告警和风险进行多方式防御，动态评估技防策略

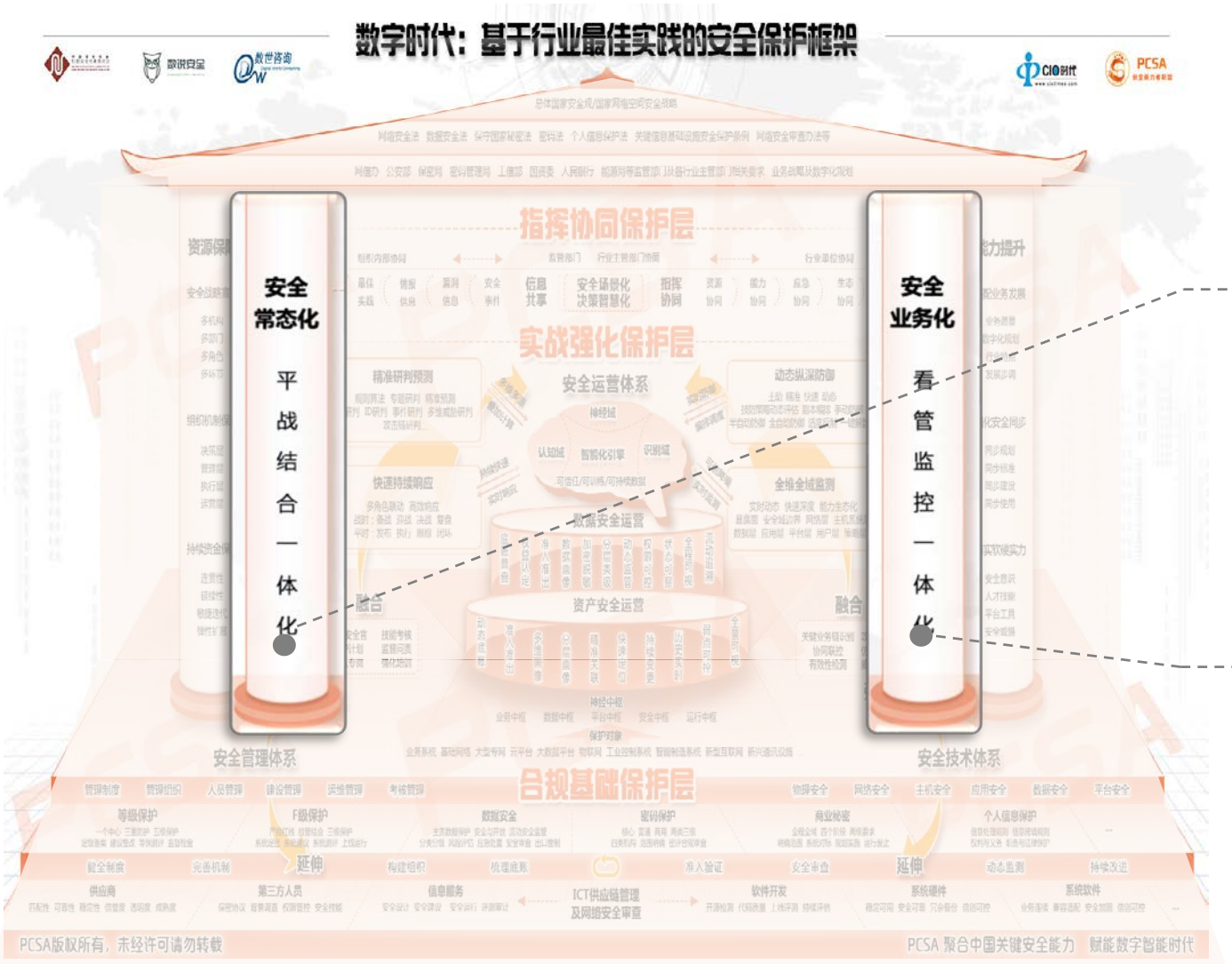
指挥协同保护层



协同保护落实监管：建立组织内部、与监管部门/行业主管部门、与行业单位之间的协同机制，实现安全场景化，支撑决策智慧化

- **组织内部协同**：明确组织内部安全相关人员的责权利边界，细化基础分工，建立内部协同机制
- **监管部门、行业主管部门协同**：从安全监管视角，协同指导、监督、检查、保护、保卫、保障工作
- **行业单位协同**：基于各行业特性，建立行业运营单位看管监控一体化协同机制
- **信息共享**：建立信息共享机制，实现安全事件、漏洞信息、情报信息、最佳实践等在组织内部、行业、监管部门之间的有效传递及共享
- **指挥协同**：建立协同指挥机制，聚焦资源协同、能力协同、应急协同、生态协同等，实现组织内外部统一指挥协同及动态联动

安全保护框架：“4”个重要支柱—背景与趋势



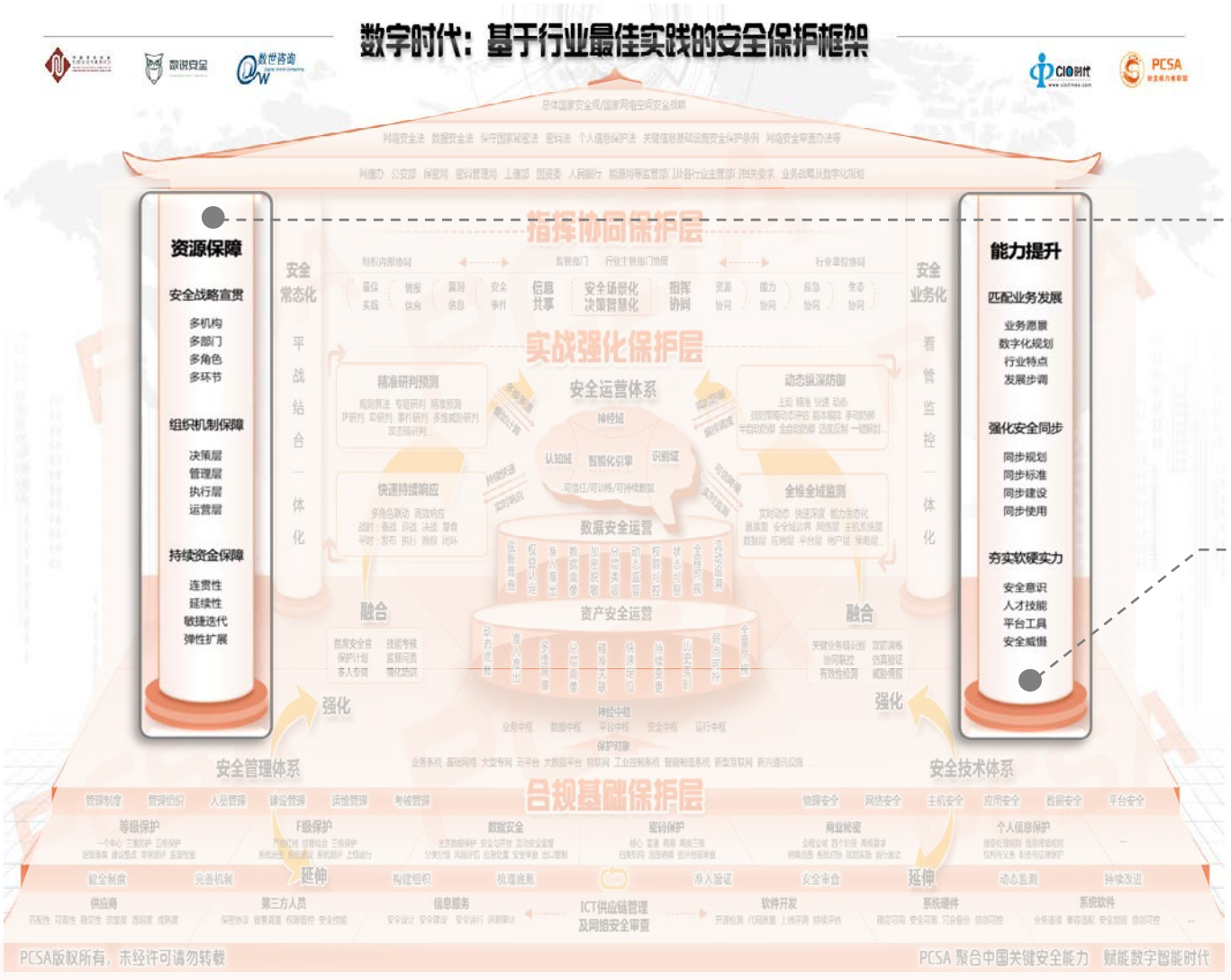
安全常态化背景：平战结合一体化

- **平时**：夯实日常工作，做好基础合规，重点强化
- **战时**：侧重上下信息共享、指挥协同、预警通报
- **一体化**：组织机构转换、流程精简快速

安全业务化趋势：看管监控一体化

- **看**：看清全局关键资产、风险
- **管**：管好保护对象边界、权责
- **监**：监好安全事件处置全过程
- **控**：控住全局安全防护的底线

安全保护框架：“4”个重要支柱—保障与提升



资源保障：确保战略层-组织层-资金层持续保障

- 战略层：全组织、全流程宣贯
- 组织层：决策-管理-执行-运营组织架构
- 资金层：统一规划、分阶段持续投入

能力提升：提升综合能力

- 业务洞悉能力：洞悉并匹配业务愿景、数字化规划、行业特点、发展步调
- 四同步能力：同步规划、同步标准、同步建设、同步使用
- 软硬实力：提升安全意识、人才技能，打造平台工具，具备安全威慑能力

PCSA
安全能力者联盟

再次感谢各位专家的真知灼见！！！

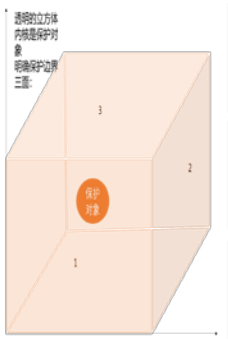
研究团队将持续研究 落地行业 欢迎联系研究组

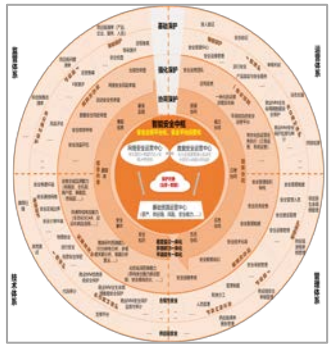
联系人：徐研究员 <xuyuhui@cnpcsa.org>

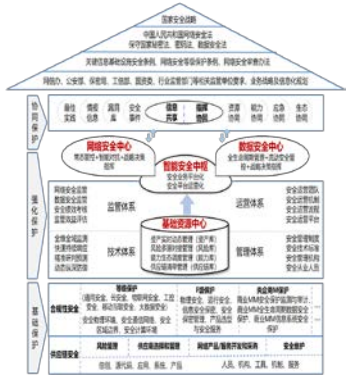
淮研究员<huaihuarui@cnpcsa.org>

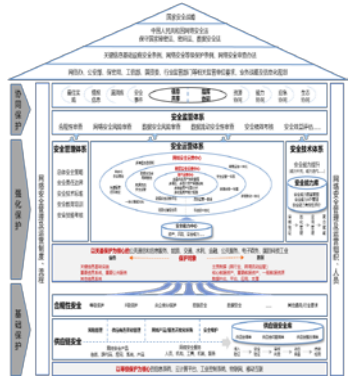
推演过程

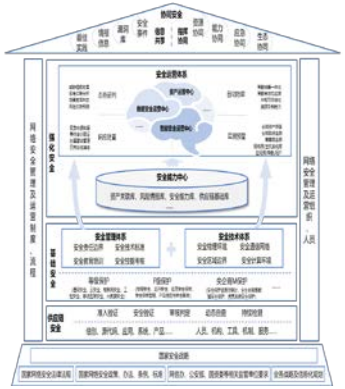
以安全场景化、安全模块化、安全业务化为积淀，结合多年安全实战经验，参考并借鉴国际安全保护框架优秀思路，经历持续、大量的研讨、评判、推翻、重来、修订的推演打磨，形成了《数字时代—基于行业最佳实践的安全保护框架》。

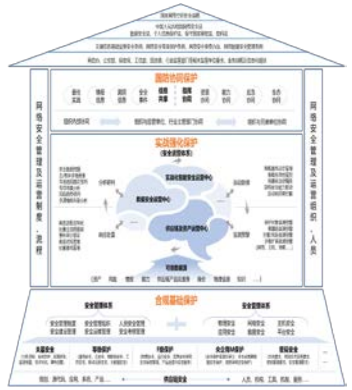


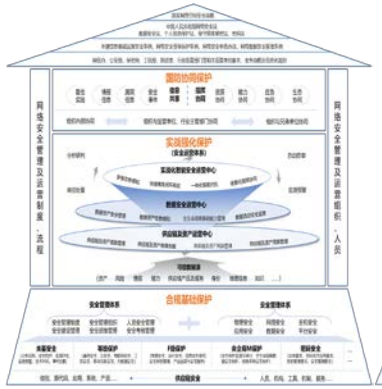


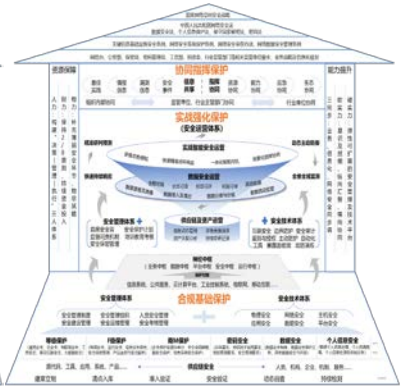


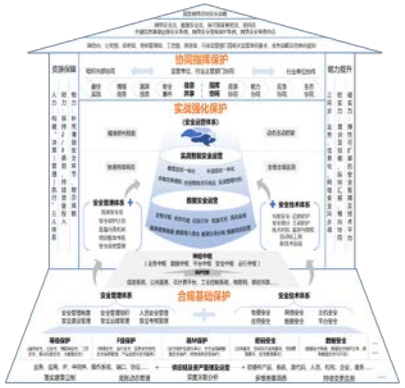


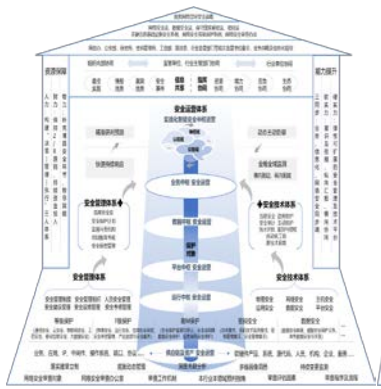


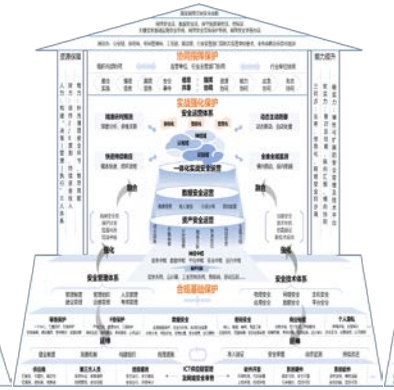


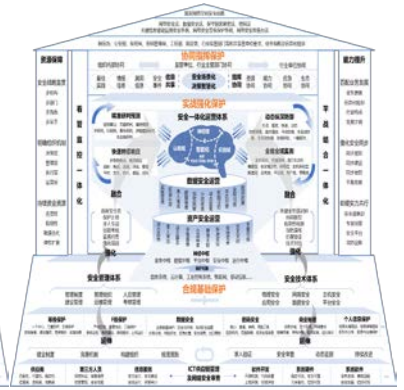












聚合中国关键安全能力　赋能数字智能时代

研究团队简介

中国信息协会 信息安全专业委员会	**简介：**中国信息协会信息安全专业委员会（简称“信安委”）是中国信息协会直属的专业委员会。于1998年10月在中国信息协会指导下筹建并由民政部批准成立，领导机构为主任委员会，聘请何德全、沈昌祥、方滨兴院士为顾问，理事及会员单位成员涵盖了信息安全的各个领域，包括信息安全主管部门、国家重要基础设施单位、信息安全保障机构、军方代表及信息安全龙头企业。 **公众号：**中国信息协会信息安全专业委员会
PCSA安全能力者联盟 /安全研究院	**简介：【愿景】**聚合中国关键安全能力 赋能数字智能时代；**【使命】**聚焦关基安全、数据安全、资产安全、供应链安全、智能安全等领域，解决行业长期共性顽疾与共性痛点，持续为用户打造安全中枢；**【定位】**数字安全业务化：数字安全业务场景化、数字安全业务平台化、数字安全业务运营化；**【致力于】**研究问题与趋势（网络空间安全长期共性问题及未来共性需求）、创新解决与突破（网络空间安全落地共性顽疾及关键技术和模式）、研发服务与平台（网络空间安全整体服务运营及生态共性平台）。 **公众号：**PCSA安全能力者联盟
数世咨询	**简介：**北京数字世界咨询有限公司（简称“数世咨询”）是国内数字产业第三方调研咨询机构，主营业务为网络安全产业领域的调查研究、资源对接与行业咨询。 **公众号：**数世咨询
数说安全	**简介：**数说安全是赛博英杰旗下专注于网络安全垂直领域的智库平台， 是中国网络安全行业内最专业且具影响力的研究媒体，以数据为基础，结合科学的方法论进行行业研究和企业分析，提供决策工具和有力资源。 **公众号：**数说安全
CIO时代/安全学院	**简介：**北京希艾欧管理技术有限公司（简称“CIO时代”）成立于2003年3月，主要从事信息化的培训、咨询及CIO时代网运营，是一个服务于企业信息化和政府信息化的专业平台。作为一个资源整合的平台，公司主要为CIO（信息总监）、IT从业人员以及所有对企业信息化、电子商务和电子政务感兴趣的个人提供专业化的知识与资源服务，同时为IT企业、实施信息化的传统企业以及政府部门提供各种专业化的会员服务和增值服务。 **公众号：**CIO时代网