CSA GCR GREATER CHINA REGION cloud security alliance ®

企业网络安全合规框架体系

联盟简介

云安全联盟(Cloud Security Alliance,CSA)是中立、权威的全球性非营利产业组织，于2009年正式成立，致力于定义和提高业界对云计算和下一代数字技术安全最佳实践的认识，推动数字安全产业全面发展。

云安全联盟大中华区(Cloud Security Alliance Greater China Region, CSA GCR)作为CSA全球四大区之一，2016年在香港独立注册，于2021年在中国登记注册，是网络安全领域首家在中国境内注册备案的国际NGO，旨在立足中国，连接全球，推动大中华区数字安全技术标准与产业的发展及国际合作。

加入我们

CSA大中华区官网
(https://c-csa.cn)

点击会员

加入联盟

填写相关申请信息

成为CSA会员

JOIN US

我们的工作

联盟会刊下载地址
了解联盟更多信息

目　录

致　谢

《企业网络安全合规框架体系》由CSA大中华区专家撰写，感谢以下专家的贡献：

项目组组长：杨天识

主要贡献者：

吴潇、王玮、张建盛、刘旭、靳倩倩、秦柯、徐岩

贡献单位：

北京启明星辰信息安全技术有限公司

北京天融信网络安全技术有限公司

杭州安恒信息技术股份有限公司

深信服科技股份有限公司

（以上排名不分先后）

关于研究工作组的更多介绍，请在 CSA 大中华区官网（https://c- csa.cn/research/） 上查看。

在此感谢以上专家。如译文有不妥当之处，敬请读者联系CSA GCR秘书处给与雅正！联系邮箱research@c-csa.cn；国际云安全联盟CSA公众号。

企业安全需求的驱动力

CSA GCR cloud security GREATER CHINA REGION alliance®

合规驱动

《网络安全法》

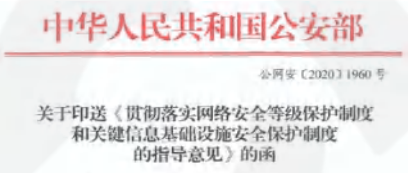
《数据安全法》

《个人信息保护法》

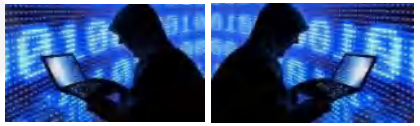
《密码法》


《关基条例》


等保 2.0



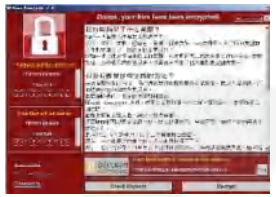
公安 1960 号文（三化六防）


HW 行动

关基信息基础设施/云中心/大数据中心

事件驱动

Struts 2 OpenSSL solarwinds LOG4J spring


勒索软件 Ransom


挖矿程序 Mining

风险驱动

网络安全法律法规政策合规要求分析

我国目前已经建立了比较完善的网络安全法律法规政策体系。

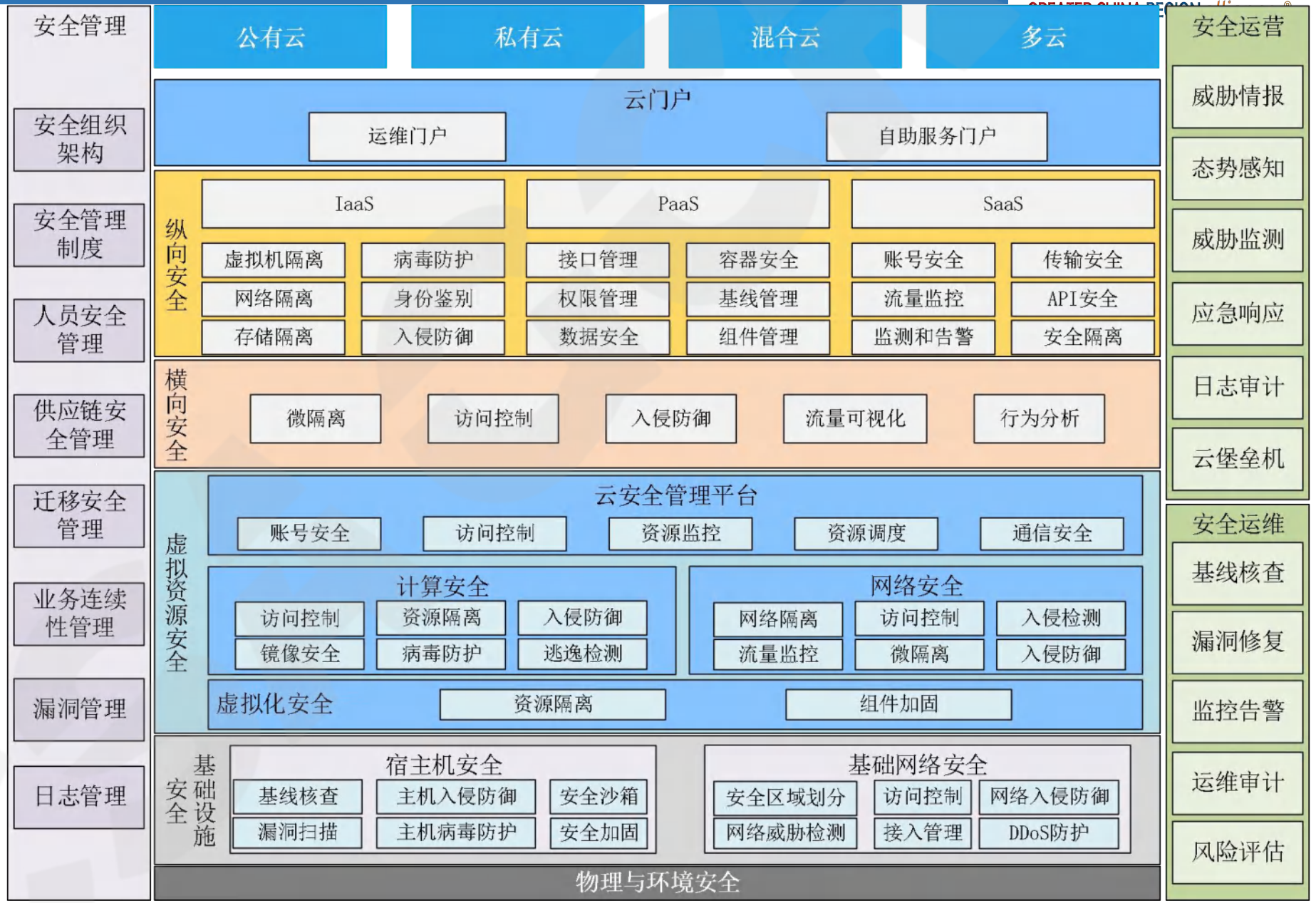
企业网络安全合规框架体系

CSA GCR cloud security GREATER CHINA REGION alliance ®

企业网络安全合规框架体系为“1+2+SEC+N+1”架构。

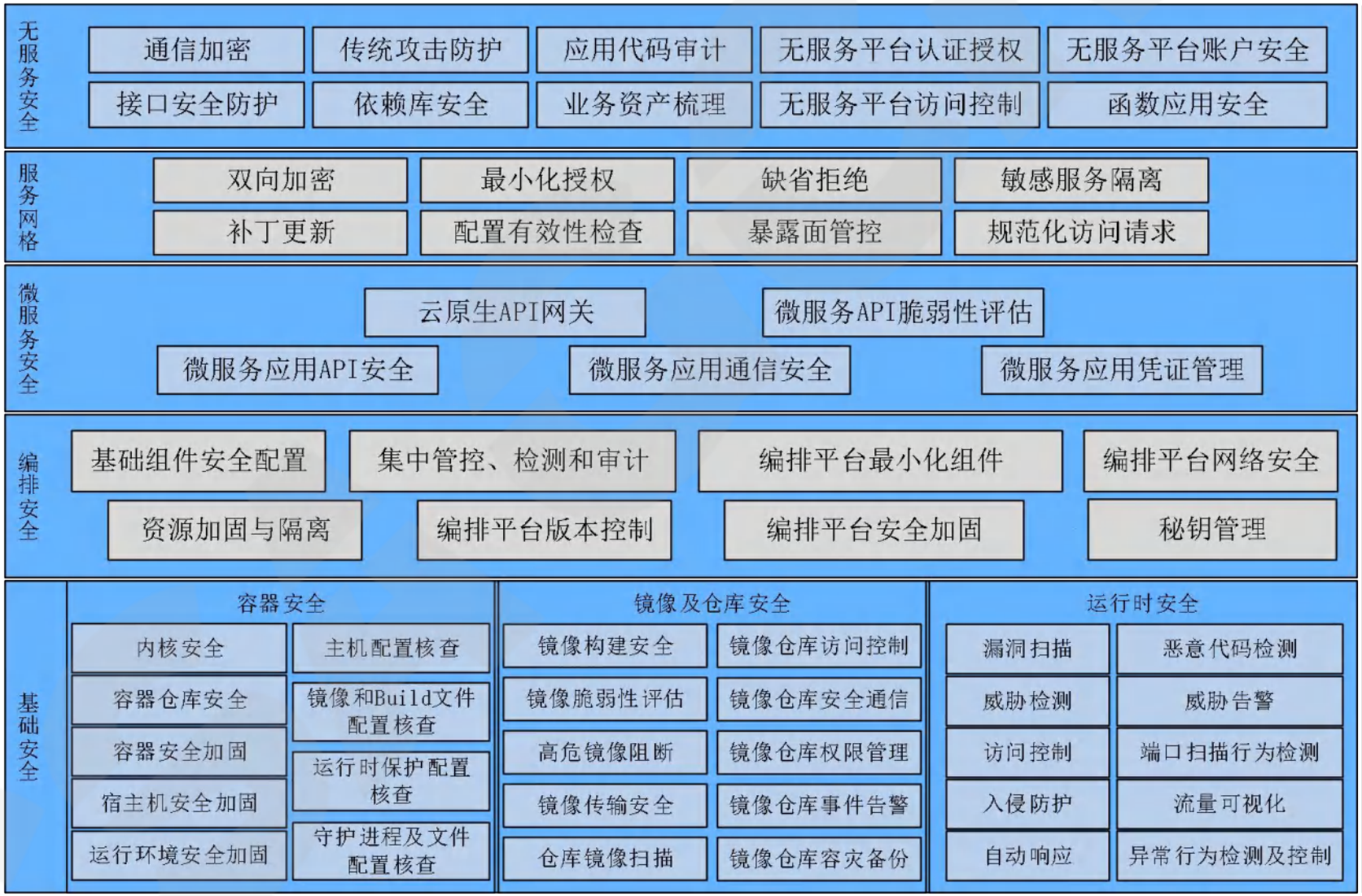
云安全合规建设框架

云安全合规建设框架涵盖公有云、私有云、混合云和多云场景，从安全管理、安全技术、安全运营和运维几个维度进行设计，安全技术从基础设施安全、虚拟化安全、租户侧横向流量安全和纵向安全展开设计。



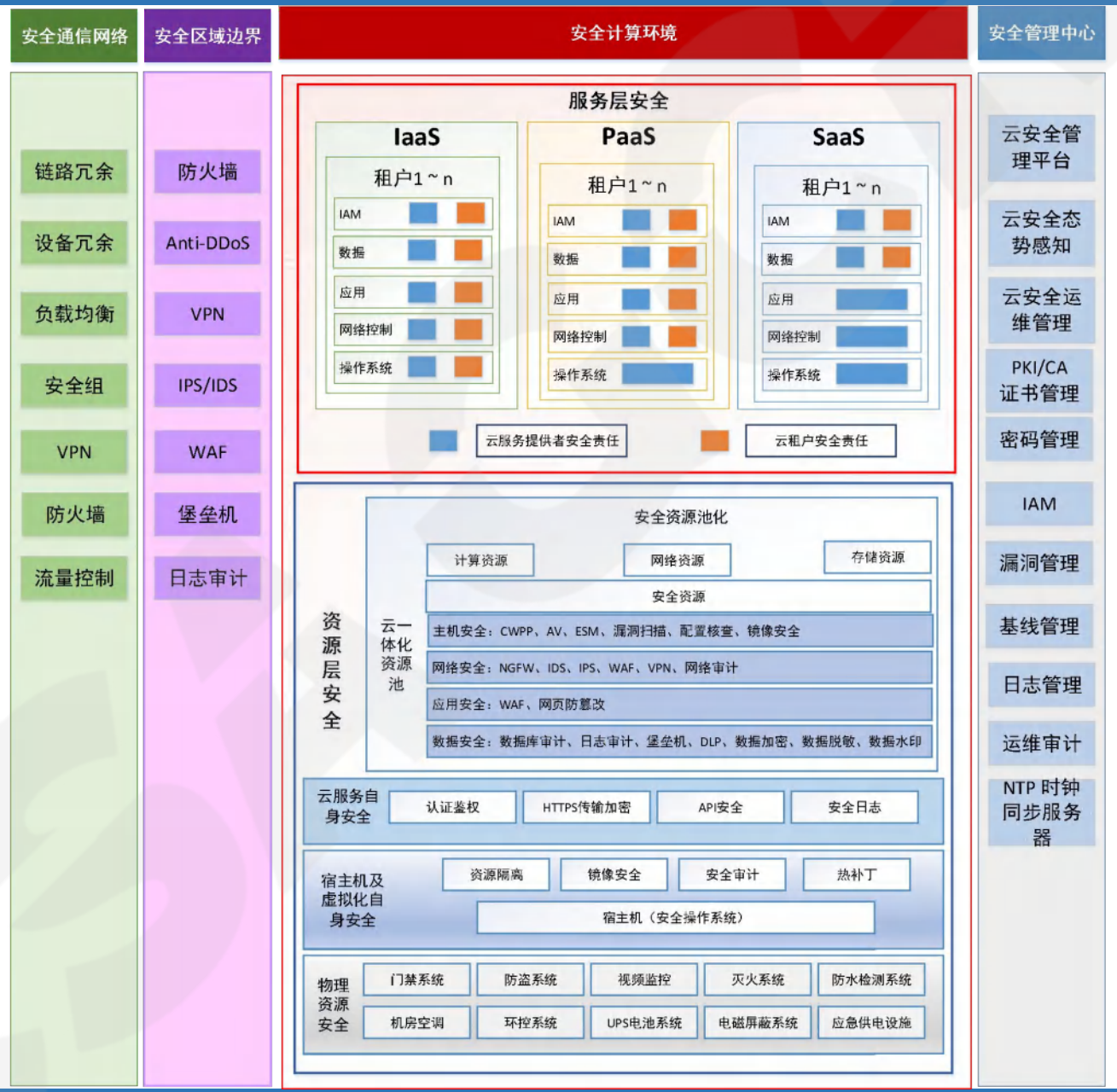
云原生安全合规建设框架

云安全合规建设框架涵盖公有云、私有云、混合云和多云场景，从安全管理、安全技术、安全运营和运维几个维度进行设计，安全技术从基础设施安全、虚拟化安全、租户侧横向流量安全和纵向安全展开设计。



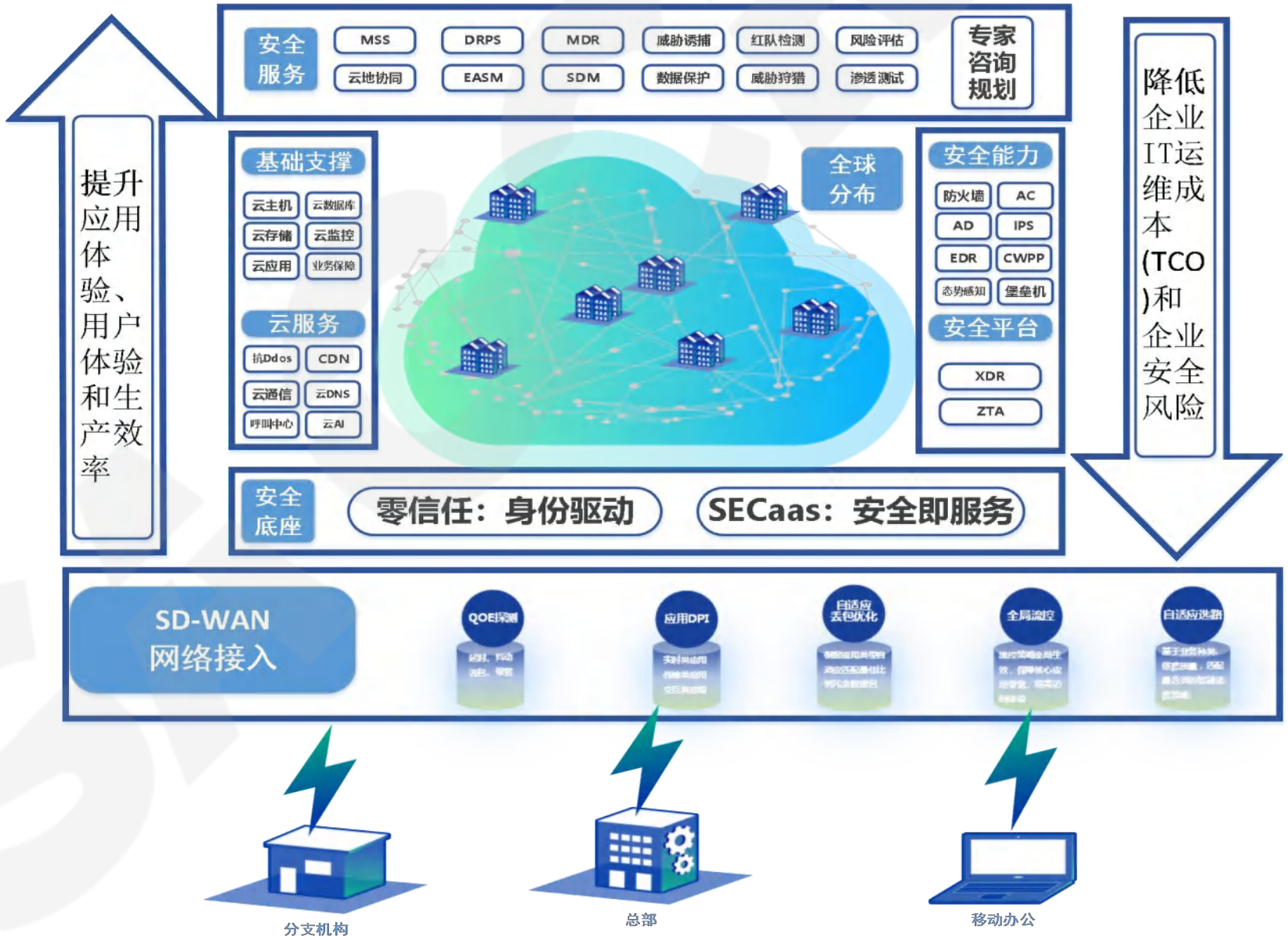
基于等级保护的云安全框架体系

基于等级保护“一个中心、三重防护”的云安全框架体系，体现出云平台和云租户安全责任分担的原则，并要求云计算资源对对IaaS、PaaS、SaaS层的租户提供不同的安全服务。



零信任与SASE建设框架

SASE 可以为云租户提供网络弹性接入、安全服务、可以有效提升用户体验以及降低企业IT运维成本。



我国数据安全法律体系

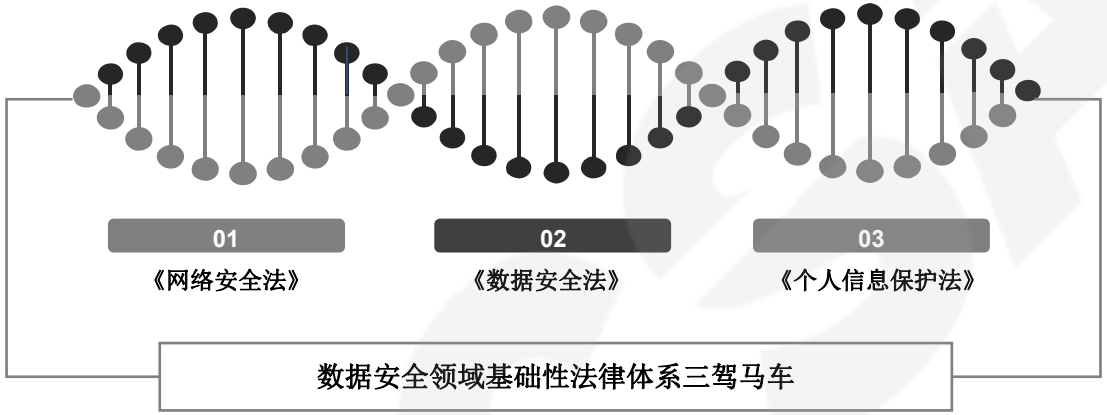
国家法律是开展数据安全保护的依据

- 2017年习主席在中共中央政治局第二次集体学习时强调，“要切实保障国家数据安全，要加强关键信息基础设施安全保护，强化国家关键数据资源保护能力，增强数据安全预警和溯源能力。”
- 2020年4月9日，中共中央、国务院印发《关于构建更加完善的要素市场化配置体制机制的意见》，明确提出“加快培育数据要素市场”，包括推进政府数据开放共享，提升社会数据资源价值，加强数据资源整合和安全保护。

国家层面新高度

数据安全治理体系

数据安全有法可依

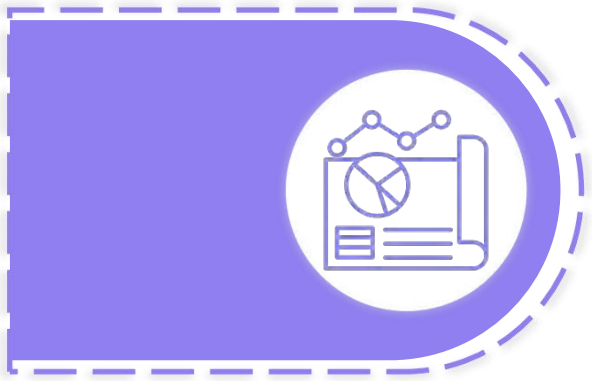


国内各行业数据安全监管要求

CSA GCR cloud security GREATER CHINA REGION alliance ®

金融行业	《中国人民银行网络数据安全管理指南》	《金融科技（FinTech）发展规划（2019-2021年）》	《网上银行系统信息安全通用规范》	《关于开展金融科技应用风险专项摸排工作的通知》
	《银行业金融机构数据治理指引》	《金融数据安全数据安全分级指南》	《金融数据安全 数据生命周期安全规范》	……
电信行业	《电信和互联网用户个人信息保护规定》（24号令）	《关于做好2020年电信和互联网行业网络数据安全管理工作的通知》	《2021年基础电信企业行业数据安全标准贯标工作方案的通知》	《基础电信企业数据分类分级防范》
	《电信和互联网数据安全评估规范》	《电信领域重要数据和核心数据识别指南》	《电信和互联网行业数据安全标准体系建设指南 》	……
能源行业	《电力行业网络与信息安全管理办法》	《中华人民共和国能源法(征求意见稿）》	《《国资监管数据管理暂行办法》	……
政务行业	《政务信息资源共享管理暂行办法》	《关于政务信息系统整合共享实施方案的通知 》	《中华人民共和国国民经济和社会发展第十四个五年规划和2035年远景目标纲要 》	《关于加强数字政府建设的指导意见》
	《信息安全技术 政务信息共享数据安全技术要求 》	《政务数据安全管理指南》	《河南省政务数据安全管理暂行办法》	……

云中需要保护的数据类型



云服务客户数据

基于法律或者其他方面的原因，由云服务客户所控制的一类数据对象。这些数据对象包括输入到云服务的数据，或云服务客户通过已发布的云服务接口执行云服务所产生的数据。

云服务衍生数据

由云服务客户和云服务交互所产生的云服务提供者控制的一类数据对象。包括：日志数据、授权用户数以及授权用户的身份、配置数据和定制化数据。其中，日志数据记录了谁在什么时间使用了服务，使用了什么功能和数据等。

云服务提供者数据

由云服务提供者控制，与云服务运营相关的一类数据对象。包括但不限制于资源的配置和使用信息，云服务特定的虚拟机信息，存储和网络资源配置信息、数据中心的整体配置和使用信息、物理和虚拟机资源的故障率和运营成本等。

YD/T 4060-2022 《云计算安全责任共担模型》

云计算场景下的8类数据安全责任

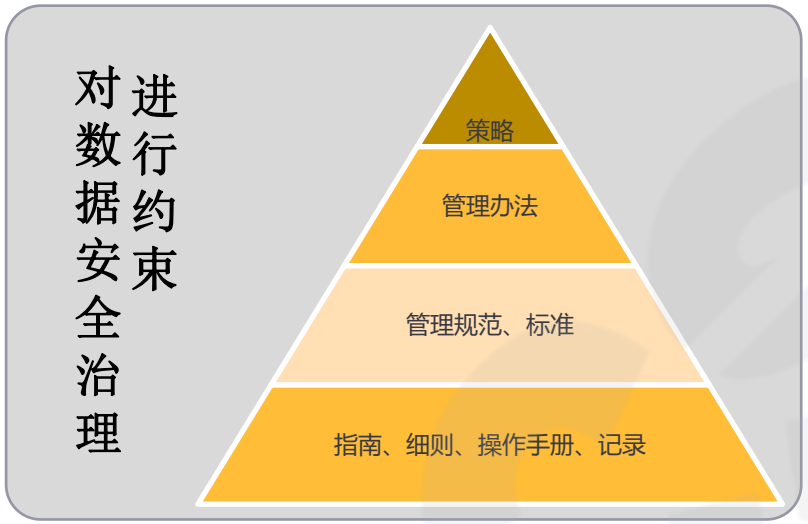
YD/T 4060-2022 《云计算安全责任共担模型》

建立“以数据为中心”的安全体系

建立“以数据为中心”的安全体系包括组织、管理、技术能力三个维度，通过治理评估持续改进，通过数据安全运营能力确保数据安全治理体系持续有效运行。

数据安全保障体系的四个维度

决策层 （高级管理人员及数据安全官）	
管理层 （数据安全管理团队）	监督层 （审计部门、人员）
执行层 （数据安全运营、技术团队）	
参与层 （员工及合作伙伴）	



运行维护

- 安全咨询
- 安全评估
- 威胁情报
- 安全整改
- 上线检查
- 运维保障
- 应急响应
- ……

数据全生命周期安全防护技术

采集 → 存储 → 处理 → 交换 → 传输 → 销毁

大数据安全管控

- 授权许可
- 访问控制
- 安全审计
- 溯源审计
- 数据脱敏
- 访问控制
- 安全审计
- 属地限制
- 数据加密
- 授权许可
- 访问控制
- 安全审计
- 溯源审计
- 数据脱敏
- 授权许可
- 访问控制
- 安全审计
- 溯源审计
- 数据脱敏
- 授权许可
- 属地限制
- 授权许可
- 安全审计
- 安全擦除

终端DLP
- 行为监控
- 泄漏阻断
- 泄漏审计

存储DLP
- 数据扫描
- 分级分类
- 智能加密

数据库安全网关
- 访问控制
- 操作审计

网络DLP
- 网络监控
- 泄漏阻断
- 泄漏审计

存储DLP
- 文件扫描
- 安全擦除

备份容灾
- 数据备份
- 数据恢复

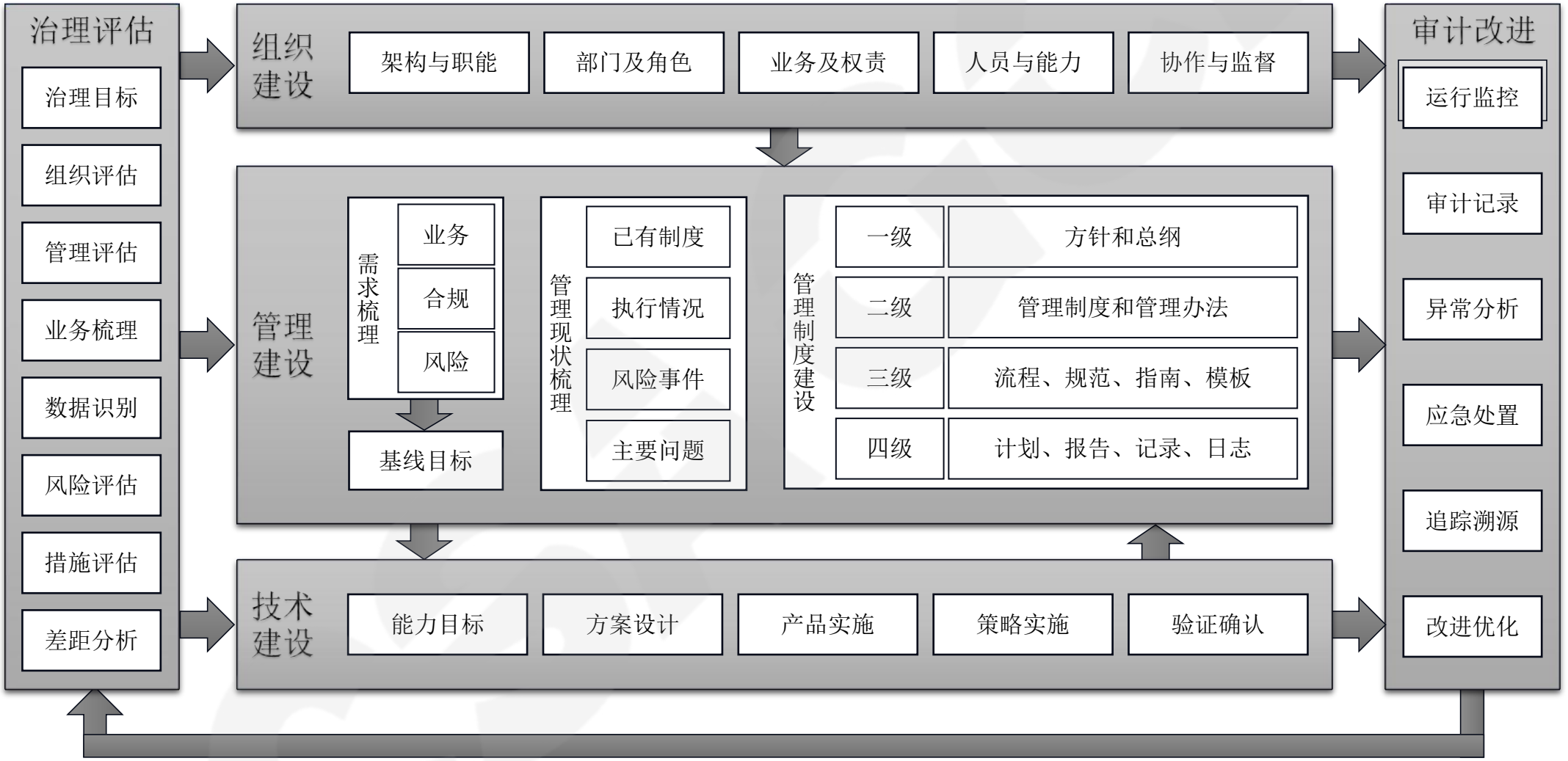
文档安全管理
- 权限控制
- 外发审核

VPN
- 传输加密

备份存储
- 数据归档

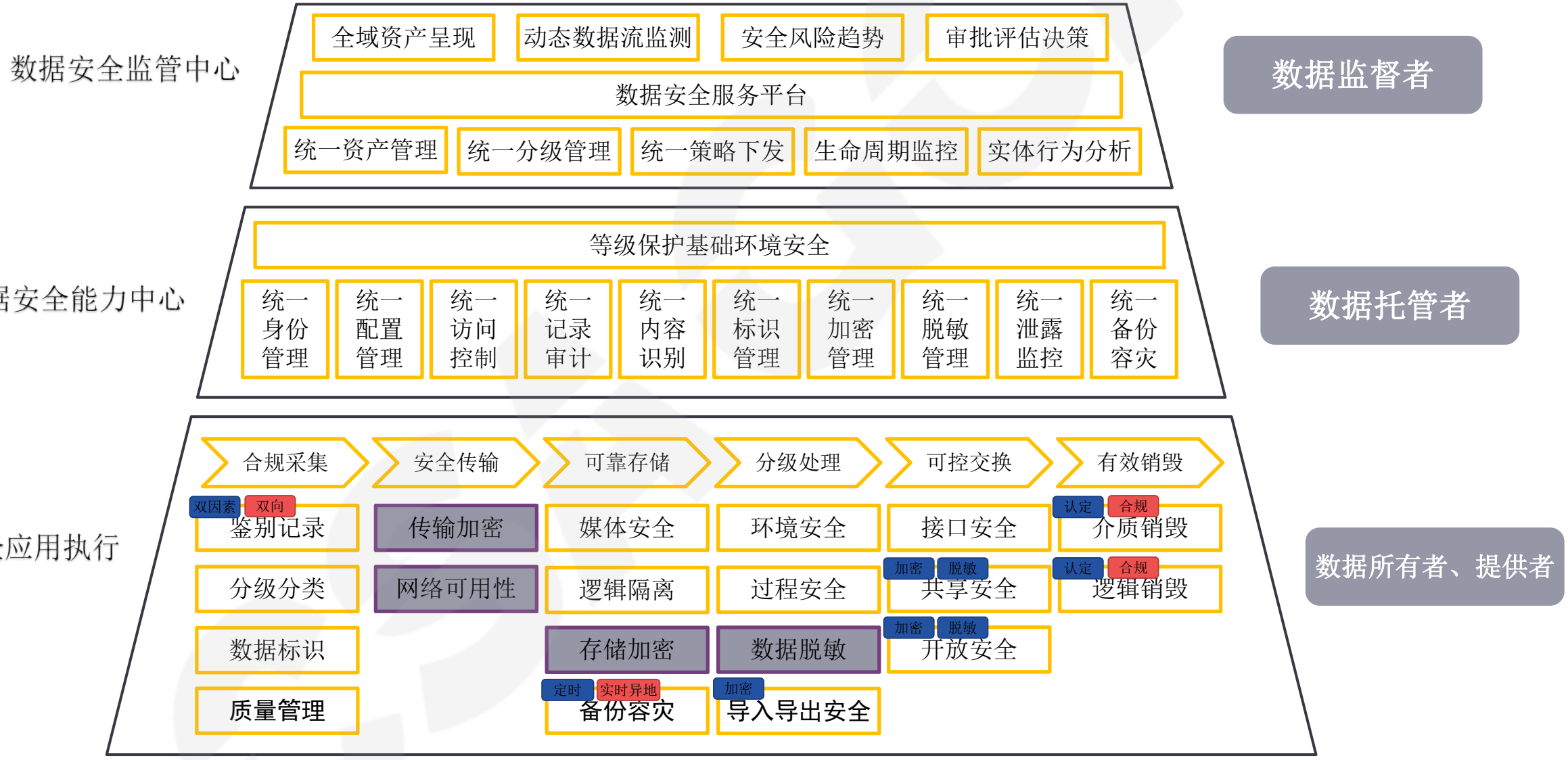
数据安全治理体系运行过程

数据安全治理体系运行过程包括围绕组织、管理、技术三个维度进行建设，通过定期治理评估发现差距不断完善体系的建设，通过定期审计发现问题，使得数据安全治理体系持续改进。



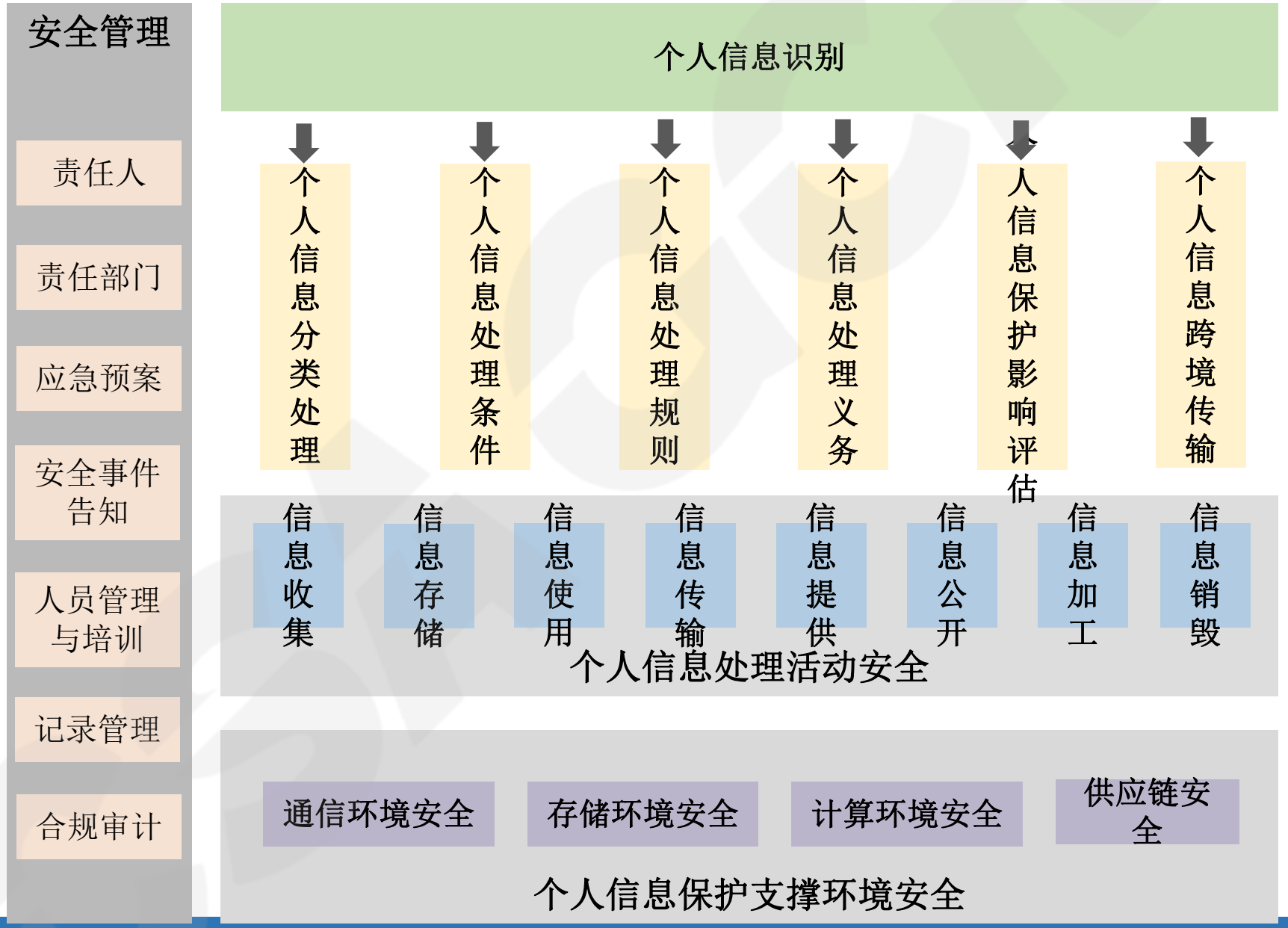
数据安全技术体系技术框架及建设分工

数据监督者通过数据安全监管中心集中下发管控策略，管理和监控数据安全资产、数据安全风险态势的总体情况；数据托管者接收数据安全能力中心统一的安全技术能力，包括基础环境安全能力和数据安全技术能力，同时接收数据安全监管中心下发的策略；数据所有者、提供者的数据受到统一管理和保护，数据全生命周期的数据执行情况被审计和监控。



企业个人信息保护体系

企业个人信息保护体系的建设主要包含个人信息识别、个人信息处理活动安全、个人信息支撑环境安全、安全管理、个人主体权益组成。首先要从个人信息识别作为起点，逐步囊括个人信息分类处理，个人信息处理条件、个人信息处理规则等需求和场景。其次以个人信息支撑环境安全为基础，在实现通信、存储、计算、供应链等安全的基础上，加强个人信息全生命周期的安全保障，个人信息生命周期包含了从信息收集到信息销毁等一系列个人信息处理活动。同时，还应建立配套的安全管理要求贯穿始终，明确的个人主体权益保障，逐步提高企业个人信息数据合规水平，实现企业个人信息安全体系的建设。



企业安全合规视角安全运营框架体系

企业安全合规视角安全运营框架体系，依托安全技术体系，为安全管理合规提供必要的支撑与输入，在当前多样安全标准、安全监管的态势下，形成符合企业自身的合规图谱，实现安全合规可量化、可展示，提升合规响应效率，降低安全合规风险。

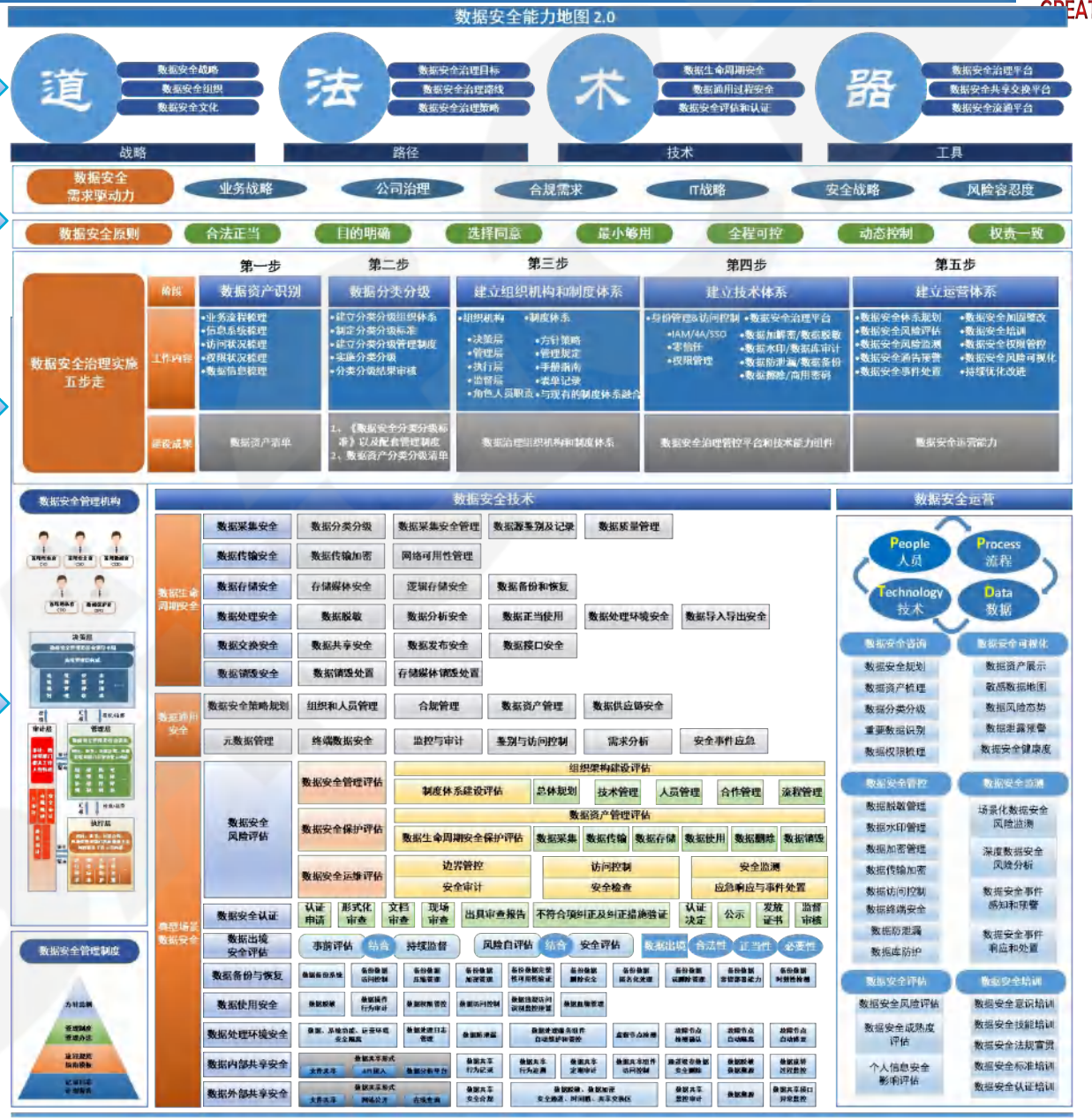
数据安全能力地图

数据安全能力地图描绘的是企业开展数据安全治理工作应该遵循的能力要素，顶层视角包括“道、法、术、器”

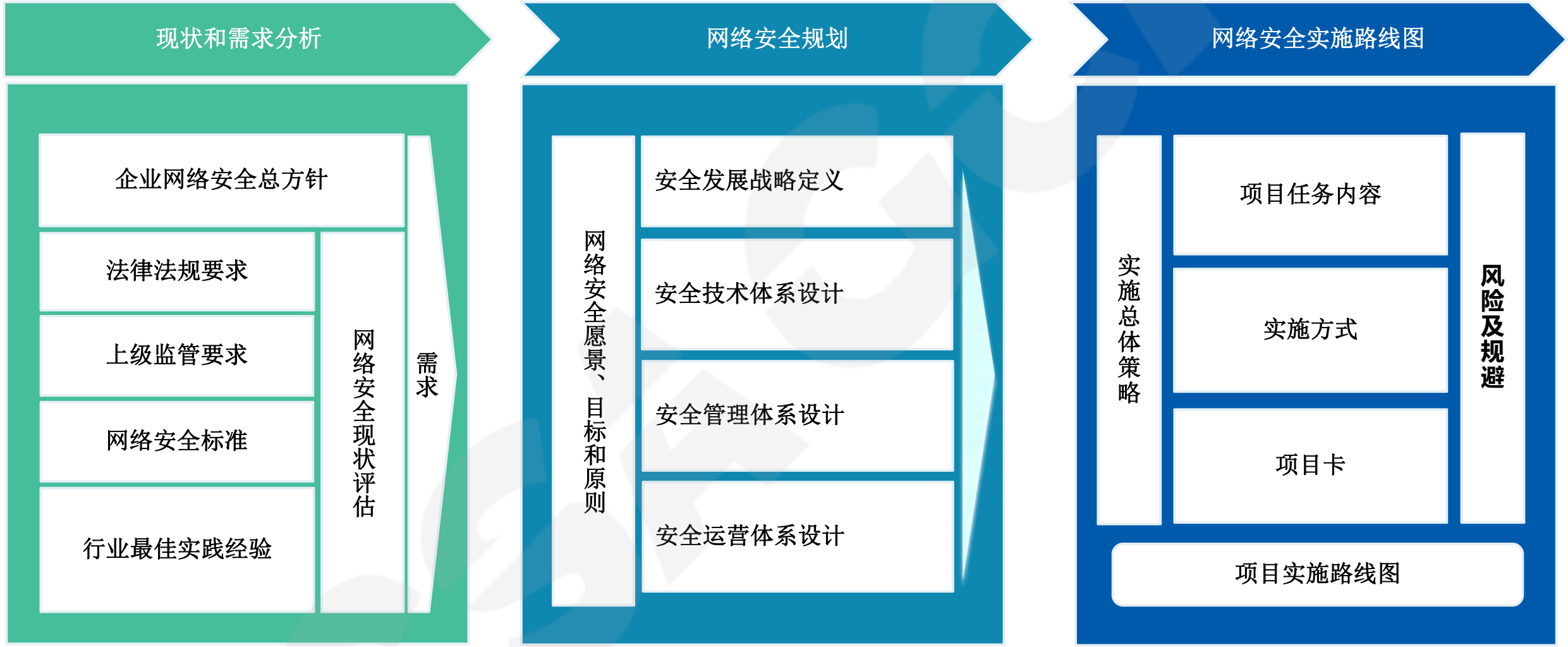
数据安全需求的驱动力和企业开展数据安全治理的原则。

企业数据安全治理实施五步走。

企业开展数据安全治理的技术体系、管理体系、运营体系。



网络安全规划方法论


现状和需求分析
企业网络安全总方针
法律法规要求
上级监管要求
网络安全标准
行业最佳实践经验
网络安全现状评估
需求
网络安全规划
网络安全愿景、目标和原则
安全发展战略定义
安全技术体系设计
安全管理体系设计
安全运营体系设计
网络安全实施路线图
实施总体策略
项目任务内容
实施方式
项目卡
风险及规避
项目实施路线图

CSA GCR cloud security alliance GREATER CHINA REGION

Cloud Security Alliance Greater China Region

扫码获取更多报告

云安全联盟大中华区
官网:https://c-csa.cn 电话:0755-86548359

地址:上海市浦东新区东育路255弄5号3FB30(前滩国际经济组织集聚区)/
广东省深圳市南山区粤海街道北京航空航天大厦1号楼905