

关于信息安全实践的思考

李鹏 | 2022.3.11



长安汽车
CHANGAN AUTO

科技长安
智慧伙伴

目录

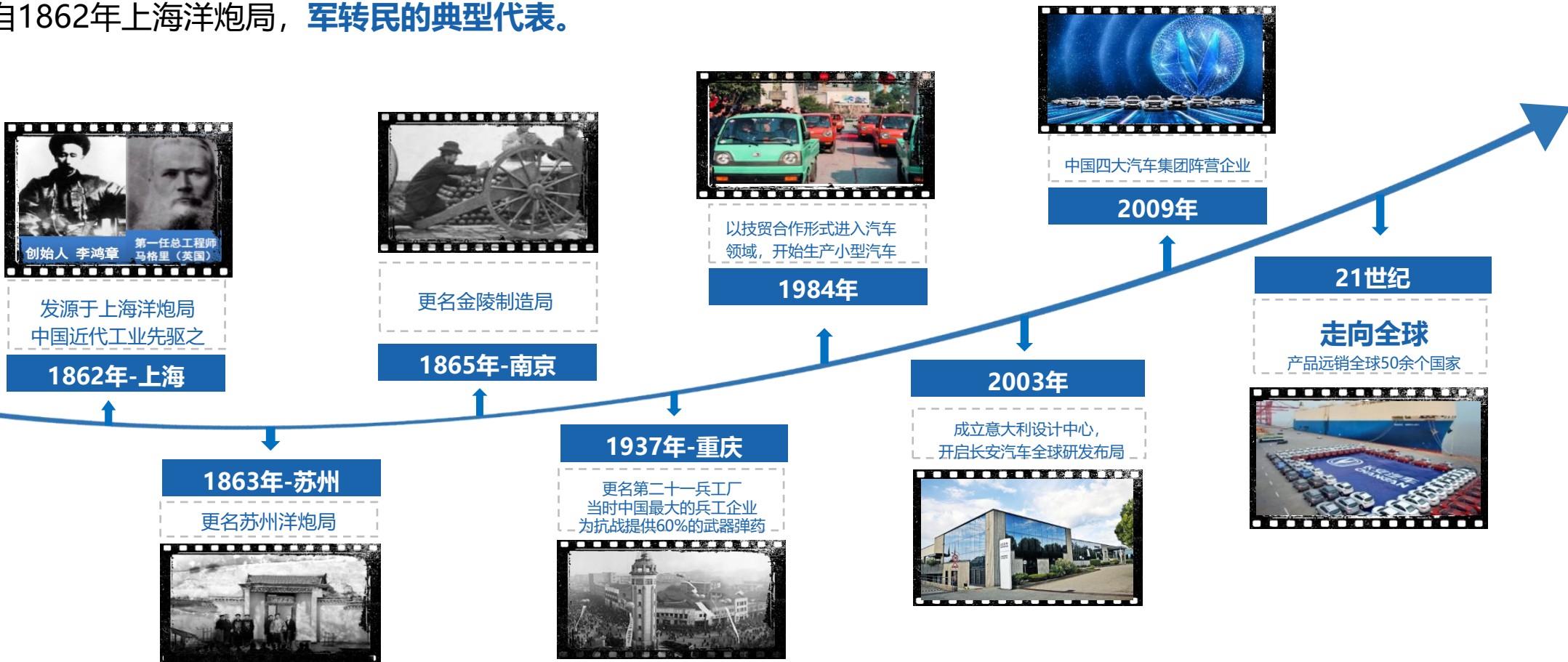
- 一 长安汽车简介
- 二 长安数字化历程
- 三 信息安全实践



1

160年历史沿革

- 中国兵器装备集团有限公司控股的上市公司。
- 源自1862年上海洋炮局，**军转民的典型代表。**





2 中国汽车品牌的典型代表

坚决贯彻落实习总书记“一定要把民族汽车品牌搞上去”指示精神。

2010年

长安系中国品牌汽车
销量累计突破

500万辆

2014年

长安系中国品牌汽车
销量累计突破

1000万辆

2021年

长安系中国品牌汽车
销量累计突破

2000万辆

坚持自主研发投入不低于销售收入的5%
始终坚定不移打造自主品牌



3 全球产业布局



14 个全球生产基地

33 个整车、发动机及变速器工厂

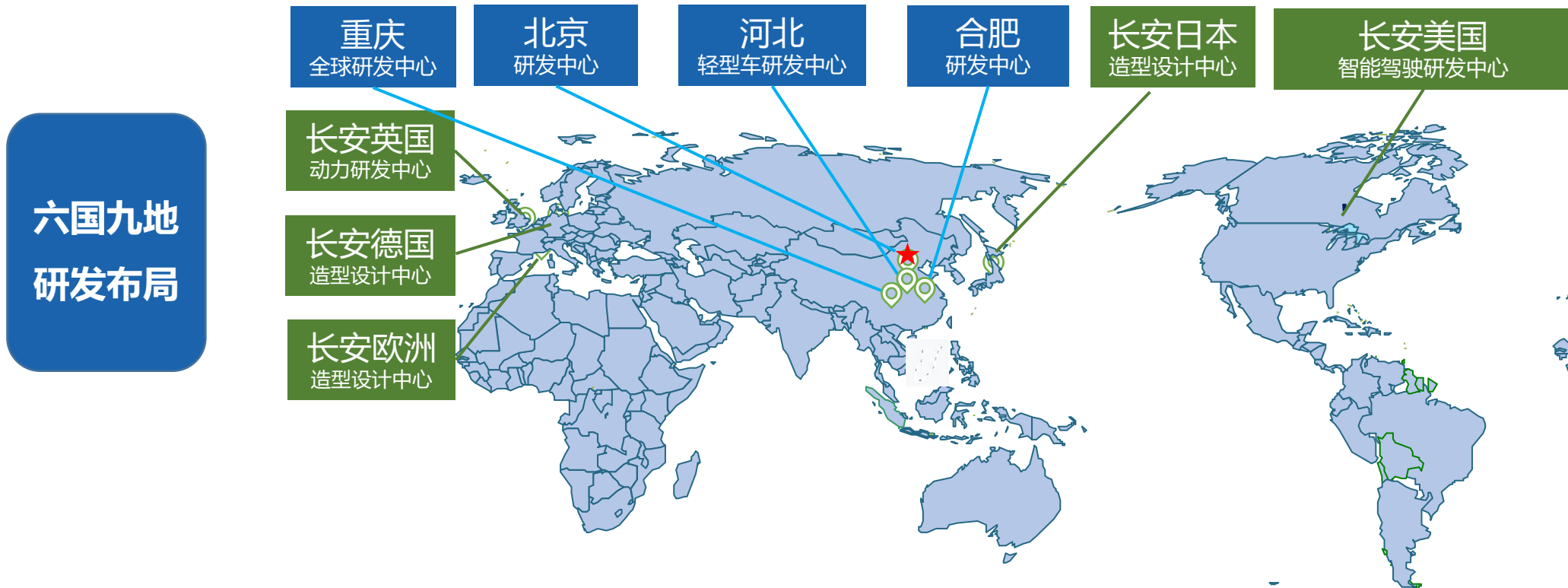
50 余个海外销售国家和地区

8700余家销售服务网点

近12万名专业服务人员

4 全球研发布局

- 在中国、意大利、日本、英国、美国和德国建立“六国九地”各有侧重的全球协同研发格局。
- 打造精细的研发体系，成立“7院3部4中心”（七大研究院、三大产品部、四大中心）。
- 拥有来自全球27个国家的工程技术人员**1万余人**。



“十四五”良好开局

- 2020年，长安汽车集团销量突破**200万辆**，跨入了新一轮上升通道。
- 2021年，长安汽车集团销售突破**230万辆**，同比增长**13.8%**，**市占率8.9%**，同比提升**0.9个百分点**



既有规模、又有效益的中国品牌
第一个突破2000万销量的中国品牌

目录

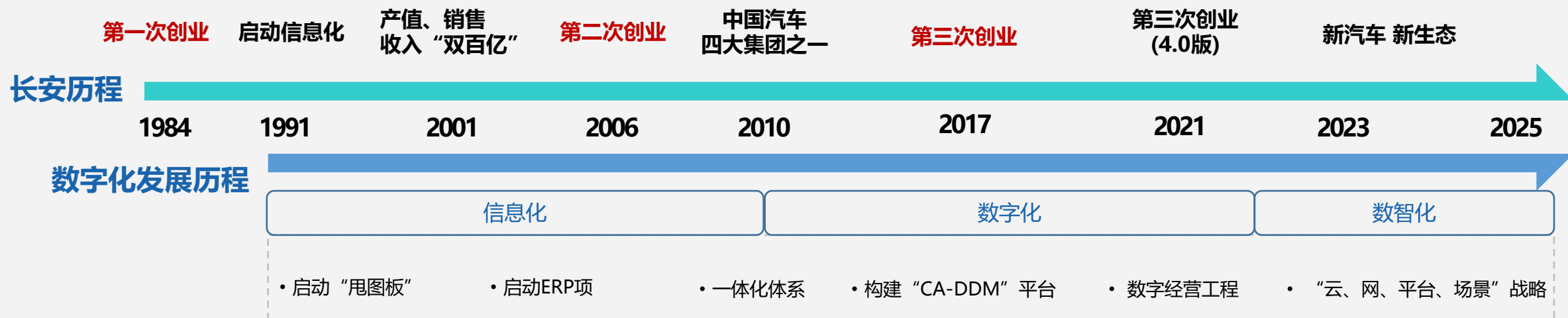
一 长安汽车简介

二 长安数字化历程

三 信息安全实践

1 数字化发展历程

- **信息化**: 1991年启动“甩图板”，开始长安信息化建设；2001年开始，以ERP为代表，开展集成应用，**全面E化和在线化**。
- **数字化**: 构建一体化体系，打造CA-DDM大数据云平台，实施全场景在线，以数据为驱动，**开展数据运营**。
- **数智化**: 围绕“天上一朵云、空中一张网、中间一平台，地上全场景”，重构以长安为主导的新产业合作架构，逐步实现“**现状可见，问题可察，风险可辨，未来可测**”，**向数据智能迈进**。



➤ 2020年被评为“数字化转型优秀案例”

➤ 被工信部评为全国首批智能制造试点示范企业

➤ 首批通过两化融合管理体系认证

➤ 2019年军工行业“数据治理优秀实践单位”

目录

- 一 长安汽车简介
- 二 长安数字化历程
- 三 信息安全实践**

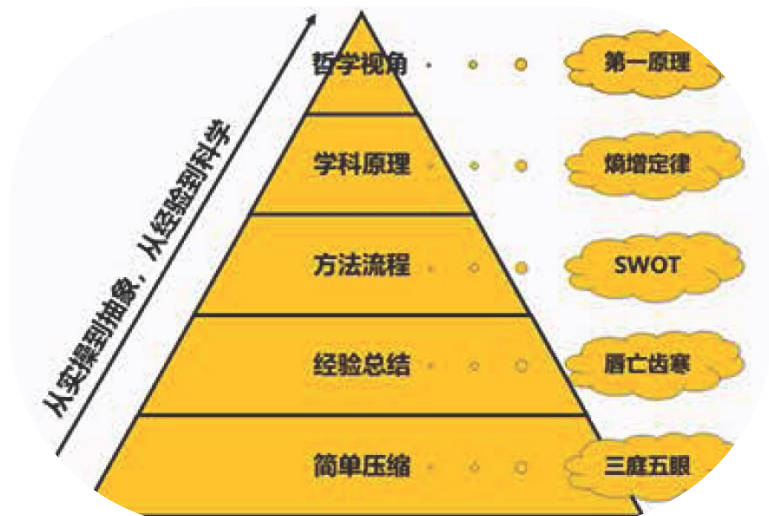
1 关于思考

WHY: 通过思维模型, 促进深度思考, 帮我们发现事物的本质 (知识收敛, 洞察本质)

□ **查理·芒格**: 你只有知道一个知识在什么情况下失效, 才配拥有这个知识。 (**适用边界, 多元思维**)

□ **刘润**: 不抽象就无法深入思考, 不还原就看不到本来面目。 (**既要抽象, 也要还原**)

What: 思维模型的层次



HOW: 提炼思维模型的方法

| 提炼方法 | 解释 | 技巧 |
|-------|--------------------------|-------------|
| 四字压缩法 | 任何知识点, 都可以简单压缩成四个字。 | 标关键词 |
| 原则复盘法 | 把你的复盘结果提炼成四个字的原则, 即思维模型。 | 痛苦+反思=进步 |
| 本质思考法 | 不断思考事物的本质, 提炼套路, 即思维模型。 | 经常多问自己几个为什么 |
| 数学建模法 | 试着用数学公式去解释你的模型。 | 尽量, 但不强求。 |
| 巨人思维法 | 站在巨人的肩膀上, 直接用巨人的思维模型。 | 学习重要学科的重要理论 |



2 明晰概念—挑战来自哪里

国家、威胁、企业、新技术，身在其中，面临各方的要求。

总体国家安全观

- 统筹发展与安全
- 11种安全、16种安全
- 数据安全贯穿所有场景

企业数字化加速

- 后疫情业务数字化计划推进
- IT与OT融合，范围扩大
- 数据资产指数级爆发

持续变化的威胁态势

- 破坏性极强的勒索病毒
- 国家支持的攻击行为
- 网络犯罪集团APT

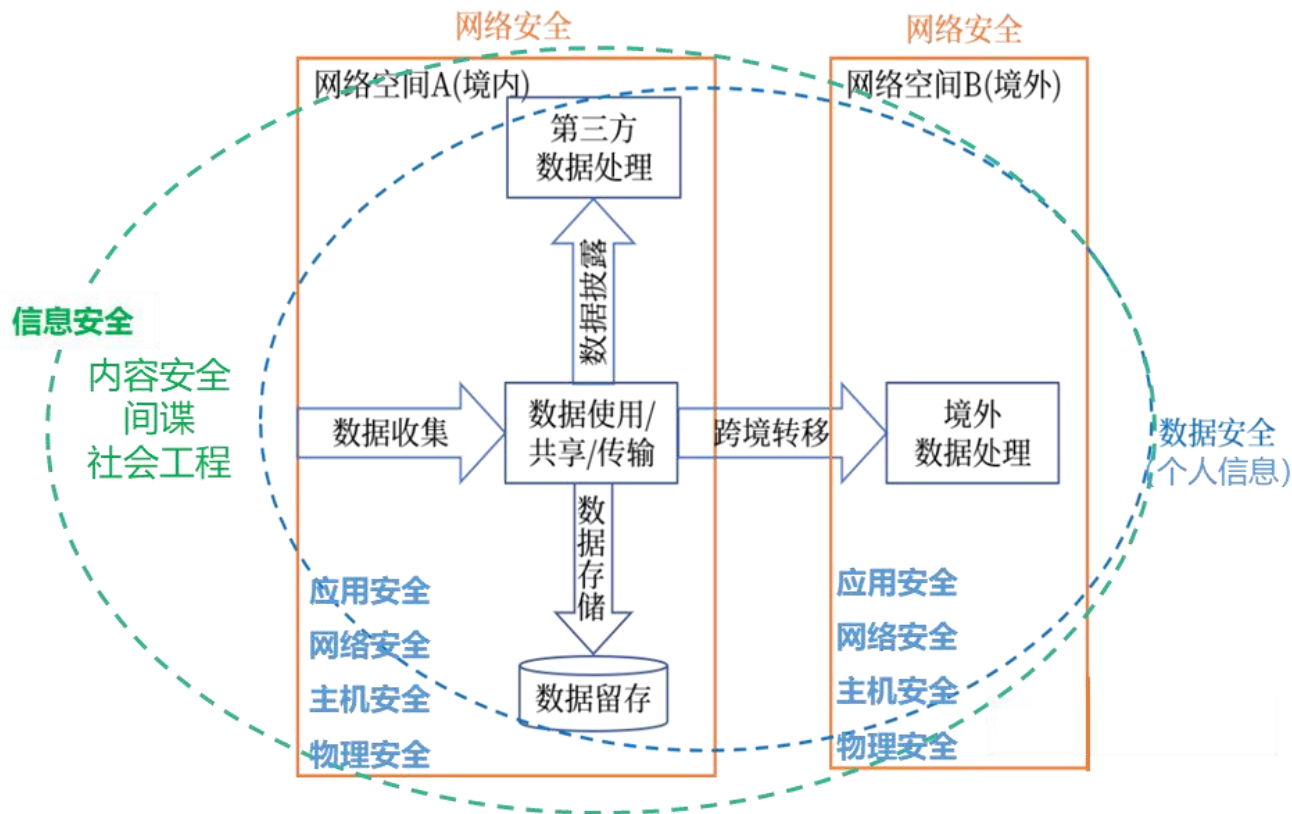
新技术驱动与挑战

- 混合式的办公方式
- 元宇宙
- 人工智能

2 明晰概念—网络安全/信息安全/数据安全

网络安全、信息安全、数据安全三者之间的关系是**包含与被包含关系**，网络安全（狭义：Network Security；广义：Cyberspace Security）包含信息安全和数据安全，三者之间所代表的有各自的领域和侧重点。

网络安全可以理解为手段，而数据安全（信息安全）可以理解为目标，正常实现资源共享。



安全的基本含义：客观上不存在威胁，主观上不存在恐惧，既客体不担心其正常状态受到影响。

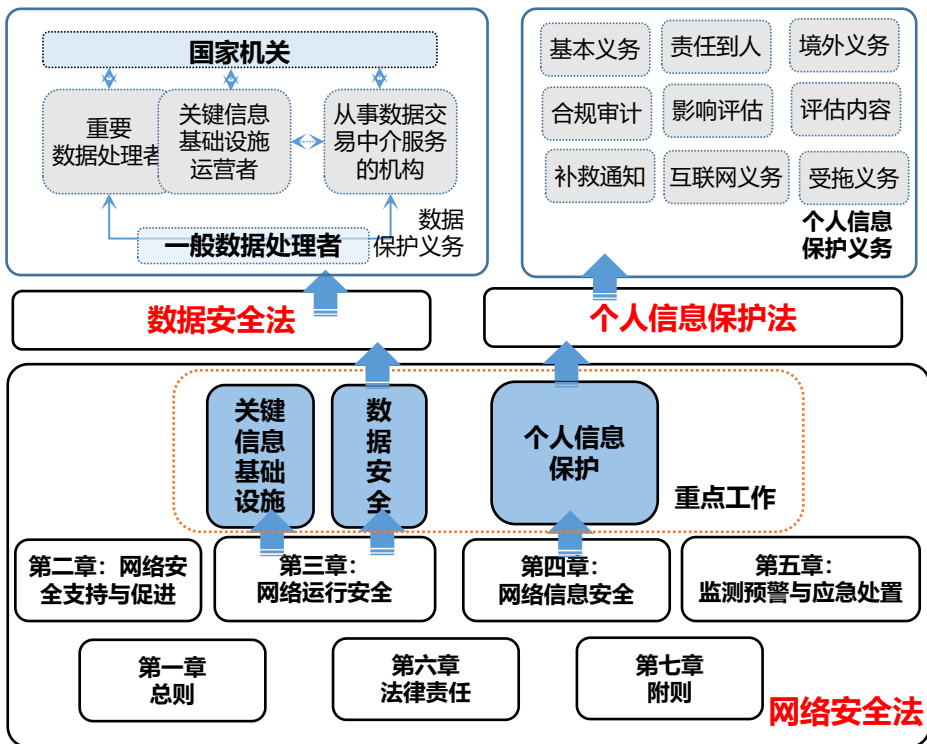
说明：橙色边框网络安全，绿色边框信息安全，蓝色边框数据安全

3 法规体系—1.关系地图

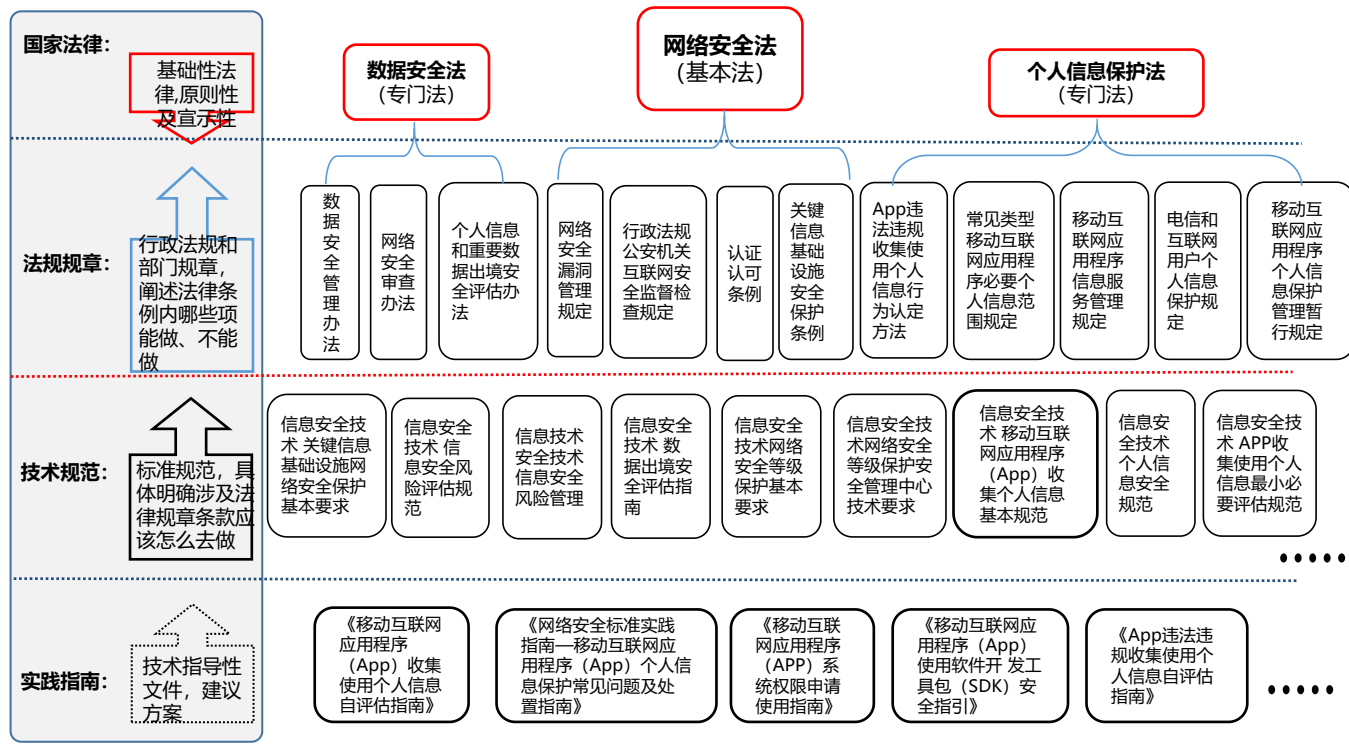
以国家总体安全观为指引，网络及数据安全三部法形成有机法律体系。

- 关联关系：网络安全法是基本法，数据安全法关注数据宏观层面安全，个人信息保护法解决个人信息相关问题，共同的关键词：“安全”、“网络”、“数据”和“个人信息”。
- 法规地图：根据三个基础性法律和规定、办法、条例及技术标准，逐渐构建完整的法规地图，加强网络及信息安全监督检查，安全管控措施落实执行。

三部法律的关联关系



网络安全法规地图

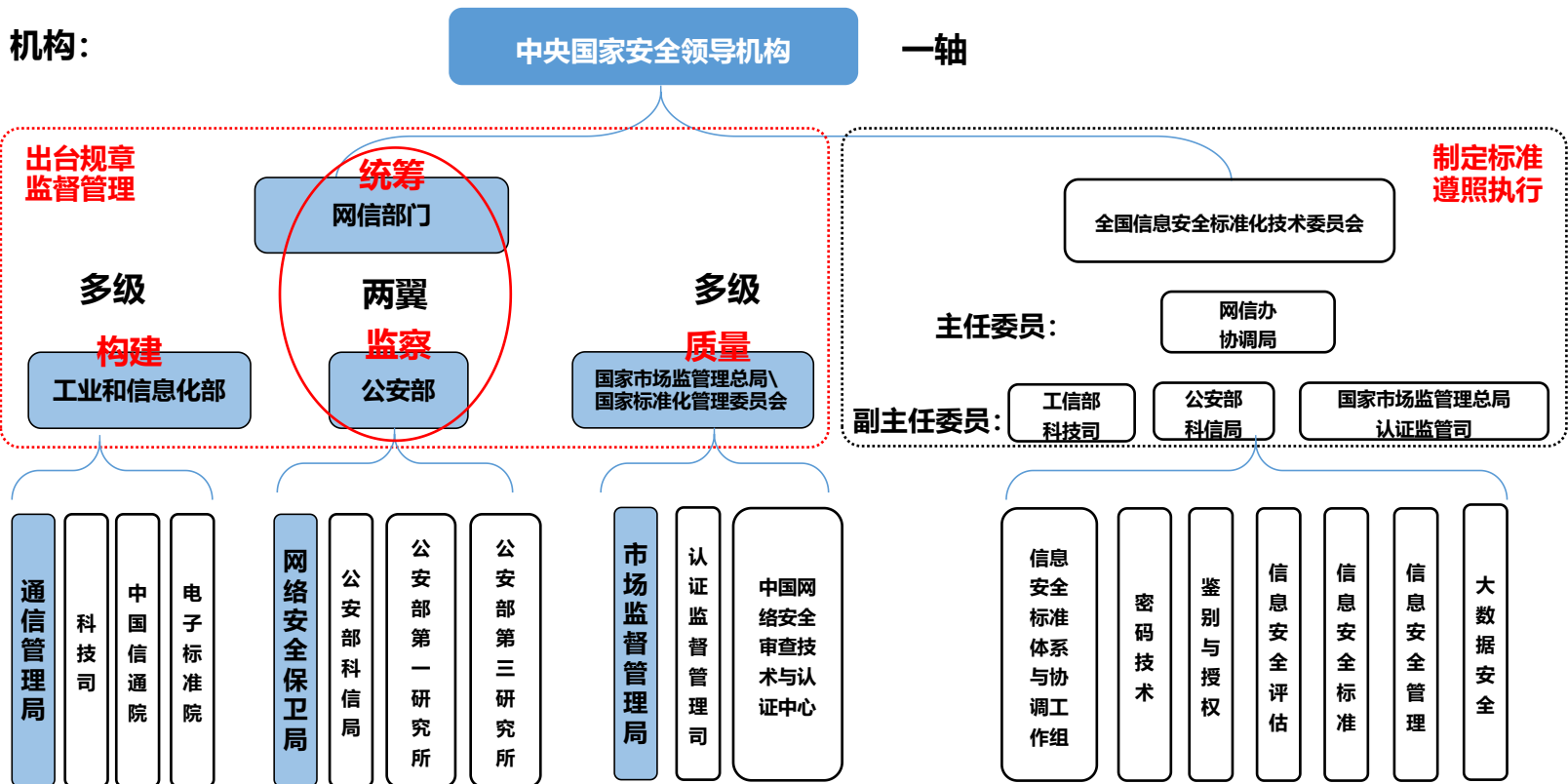


3 法规体系—2.国家监管机构及检查方式

国家实行“一轴、两翼、多级”的监管体系，通过综合和专项检查实施监管。

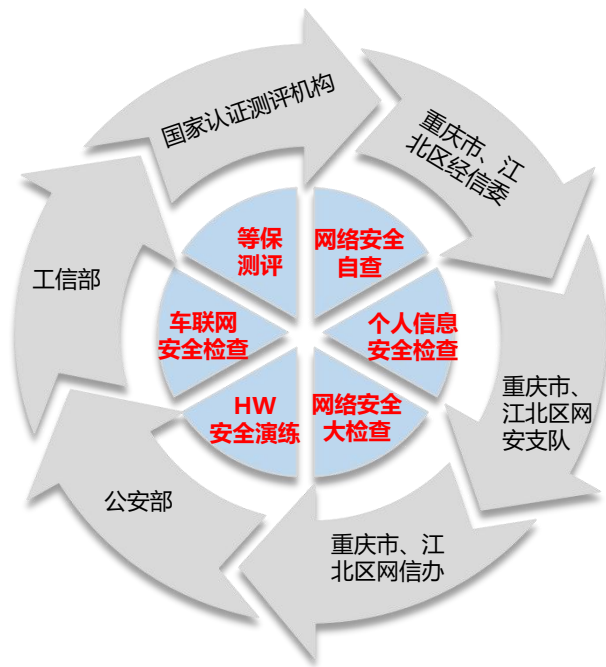
“一轴”指中央国家安全领导机构，两翼指公安机关和网信部门，多级指工业、电信、交通、金融等行业主管部门的共同参与。

机构：



检查及评估：

频率：一年一次



法规体系—3.法律处罚与追究责任

明确网络及数据安全参与者的基本义务，对违规行为采用罚款、关闭吊销的处罚。

核心：按照网络安全等级保护制度（既网络安全为基础）

网络安全法：

| 序号 | 违规行为 | 处罚 | 关键重点风险点 | 序号 | 违规行为 | 处罚 | 关键风险点 |
|----|------------------------------|---|----------------------------------|----|------------------------------------|--|-----------------------|
| 1 | 未实施等保，未设定安全应急预案，发生安全事件，未上报。 | <ul style="list-style-type: none"> 单位:1-1万 负责人: 0.5-5万 | 网络日志≥6个月；重要数据加密；发生事件上报 | 5 | 采购未经安全审查或者安全审查未通过的网络产品 | <ul style="list-style-type: none"> 采购金额 1-10倍 | 采购通过国家安全审查网络产品， |
| 2 | 未执行三同步，为履行安全义务，未每年开展至少1次安全评估 | <ul style="list-style-type: none"> 单位: 10-100万 负责人: 1-10万 | 应急演练；保密协议；每年风评 | 6 | 网络服务不得设置恶意程序 | <ul style="list-style-type: none"> 单位: 5-50万 负责人: 1-10万 | 提供产品不能有恶意程序；存在漏洞及时上报。 |
| 3 | 在境外存储网络数据，或者向境外提供网络数据 | <ul style="list-style-type: none"> 单位: 5-50万 负责人: 1-10万 关闭吊销 | 个人信息和重要数据境内存储；因需向境外提供，报网信部门评估 | 7 | 对法律、行政法规禁止发布或者传输的信息未停止传输、采取消除等处置措施 | <ul style="list-style-type: none"> 单位: 10-50万 负责人: 1-10万 关闭吊销 | 用户发布的信息的审核管理， |
| 4 | 违法收集、使用、篡改、出售公民信息，未妥善保护公民信息 | <ul style="list-style-type: none"> 单位: 1-10倍所得罚款 负责人: 1-10万 关闭吊销 | 合法收集、使用个人信息；使用技术手段防止泄露，损毁、丢失个人信息 | | | | |

数据安全法：

| 序号 | 违规行为 | 处罚 | | | 关键重点风险点 |
|----|---|---|--|----------------|-----------------------------------|
| | | 一般 | 情节严重 | 国家安全 | |
| 1 | 未履行数据安全保护义务，定期风险评估，报送有关主管部门，或未采取必要安全措施。 | <ul style="list-style-type: none"> 单位:5-50万 负责人:1-10万 | <ul style="list-style-type: none"> 单位50-200万 个人5-20万 关闭吊销 | 200-1000万，关闭吊销 | 数据安全管理制度；数据安全组织，数据处理风险监控，定期数据风险评估 |
| 2 | 未按照网信部门出境管理办法要求，向境外提供重要数据 | <ul style="list-style-type: none"> 单位:10-100万 负责人:1-10万 | <ul style="list-style-type: none"> 单位100-1000万 个人10-100万 关闭吊销 | | 根据个人信息出境安全评估办法，报网信部门评估 |
| 3 | 拒不配合公安机关、国家安全机关数据调取 | <ul style="list-style-type: none"> 单位:5-50万 负责人:1-10万 | | | 配合公安机关、国家安全机关数据调取 |
| 4 | 未经主管机关批准向外国司法或者执法机构提供数据 | <ul style="list-style-type: none"> 单位:10-100万 负责人:1-10万 | <ul style="list-style-type: none"> 单位:100-500万 负责人:5-50万 关闭吊销 | | 根据个人信息出境安全评估办法，报网信部门评估 |

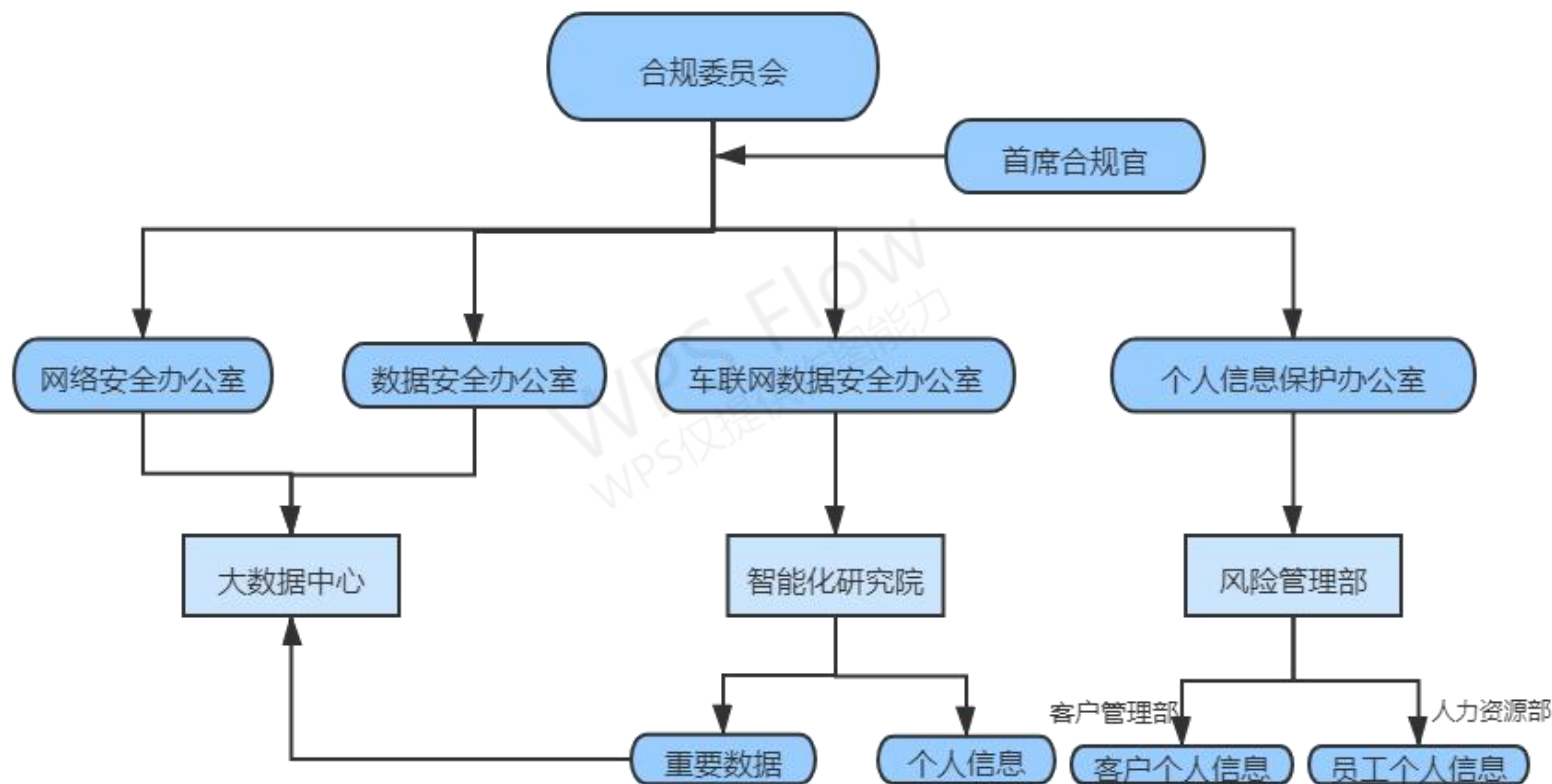
个人信息保护法：

| 序号 | 违规行为 | 处罚 | | 关键风险点 |
|----|--|--|--|---|
| | | 一般 | 情节严重 | |
| 1 | 违反本法规定处理个人信息，或者处理个人信息未按照规定采取必要的安全保护措施 | <ul style="list-style-type: none"> 单位:100万以下 负责人:1-10万 | <ul style="list-style-type: none"> 单位:5000万元以下或上一年度营业额百分之五 负责人:10-100万 | <ol style="list-style-type: none"> 合法合理收集、处理个人信息； 保障个人信息用户权利； 制定内部管理制度和操作规程； 个人信息分类管理； 采取加密、去标识化安全措施； 个人信息处置风险评估，评估报告及处置记录三年； 外部成员组成的独立机构，对个人信处理活动进行监督； 个人信息泄露应急处置； 第三方保密协议，保障措施。 个人信息出境上报评估。 |
| 2 | 个人信息权益因个人信息处理活动受到侵害，个人信息处理者不能证明自己没有过错的 | 实际情况确定赔偿数额 | | |
| 3 | 个人信息处理者违反本法规定 | | | 构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。 |

4 实践要点—2.治理架构

构建合规+管理+技术+业务的治理架构，落实责任。

安全部门职责：提升信息安全意识，保护网络基础环境，指导（赋能）业务/应用安全。



4 实践要点—3.安全运营

信息安全本质是控制风险，重在运营。

运营目的是以预防为主，发现并控制征兆。

以运营改善为目标设定评价指标，衡量信息安全工作成效。

信息安全工作目标：2个0

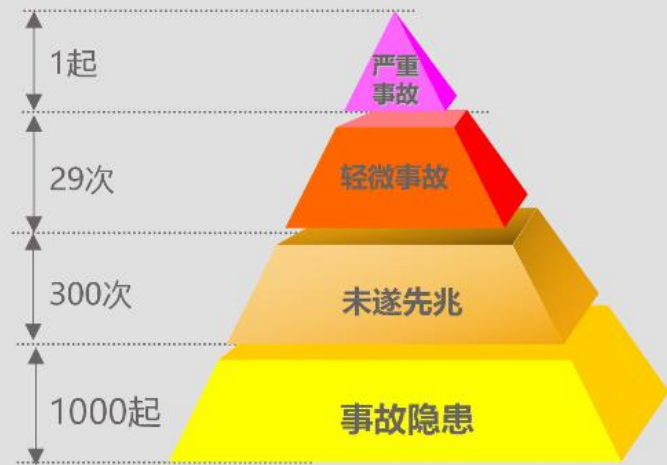
□ 重大信息安全事故“0”

□ 重大失泄密事故“0”

海恩法则-基本概念



海恩进一步指出：每一起严重事故的背后，必然有29次轻微事故和300起未遂先兆以及1000起事故隐患。



4 实践要点—3.安全运营- (1) 指标在线—示例

- 周报：** 聚焦在应用系统建设“三同时”结果和办公环境合规性，每周管理并及时给出运营结果。
- 月度：** 按照在线指标的工作机制，通过每月运营，更新指标结果，反映信息安全的管理结果。

示例—常态化管理

一、信息安全问题标准与评价

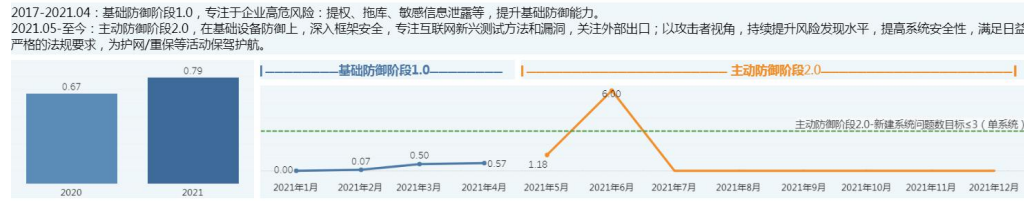
示例-周报

| 评价范围 | 评价对象 | 评价标准 | 年度值 (个) | 本月值 (个) | 状态评价 |
|-------|------|------------------------|---------|---------|------|
| 全公司 | 安全事件 | 2个0 | 0 | 0 | ● |
| | 应用系统 | 新建系统单系统问题数≤3 | 0.79 | 6 | ● |
| | | 在线服务器单服务器问题数≤2 | 0.01 | 0 | ● |
| | 办公环境 | 百台办公终端问题数≤5 | 0.43 | 0 | ● |
| 大数据中心 | 应用系统 | 人员行为合规率≥95% | 99.64% | 100% | ● |
| | 办公环境 | 年度事故隐患小于850个 (月 < 71个) | 156 | 12 | ● |
| | | 年度事故隐患小于150个 (月 < 13个) | 4 | 0 | ● |

③海恩法则：每一起严重事故的背后，必然有29次轻微事故和300起虚惊事件以及1000起事故隐患。针对大数据中心，以对象数量为分配原则，将海恩法则的1000起事故隐患分配为办公环境300个，应用系统700个。②2个0：1、重大信息安全事件为“0”；2、重大失泄密事件为“0”。

二、安全问题趋势图

新建系统问题数趋势 (单系统)



办公终端问题数趋势 (百台终端)



人员行为合规率



| | | |
|----------------------------------|-----------------------------------|-------------------------------|
| 安全管理水平 (目标≥95分) 99.87分 | 人员行为合规率 (目标≥95%) 99.62% | 百台终端问题数 (目标≤5) 0.44 |
|----------------------------------|-----------------------------------|-------------------------------|

一、信息安全常态化管理

| 分类 | 区域 | 1月 | 2月 | 3月 | 4月 | 5月 | 6月 | 7月 | 8月 | 9月 | 10月 | 11月 | 12月 |
|------|------|----|----|----|----|----|----|----|----|----|-----|-----|-----|
| 日常检查 | 全体 | G | G | G | G | G | B | B | B | B | B | B | B |
| | 工厂区域 | | G | | G | G | | | B | | | | |
| 现场检查 | 研发区域 | G | | G | G | G | | | | B | | | |
| | 职能部门 | | | G | G | G | B | | B | | | B | |
| 培训 | 全体 | G | | | G | | | B | | | | B | |
| 宣传 | 全体 | G | G | G | G | G | B | B | B | B | B | B | B |

二、各单位安全管理情况

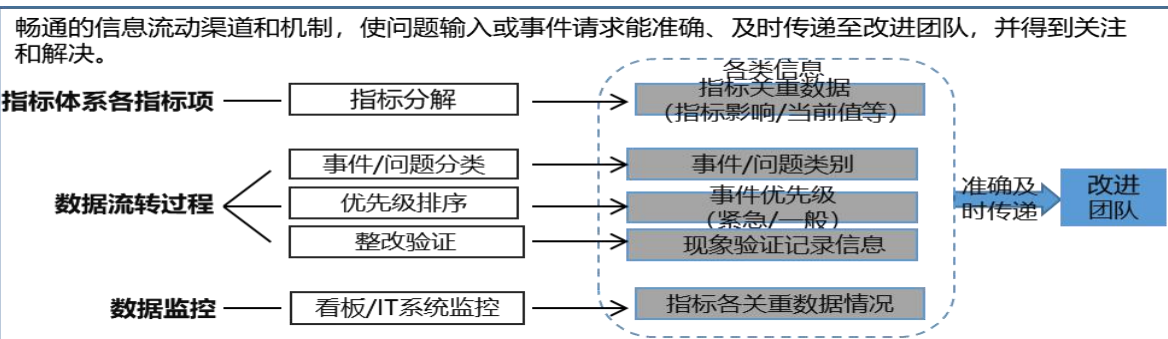


4 实践要点—3.安全运营- (2) 运营机制

让指标体系通过安全运营”跑“起来

- 事件/问题驱动的安全运营机制
- QIP: 从信息流、组织机构、时间与数据管理、工具与方法四个要素解决问题、持续提升。

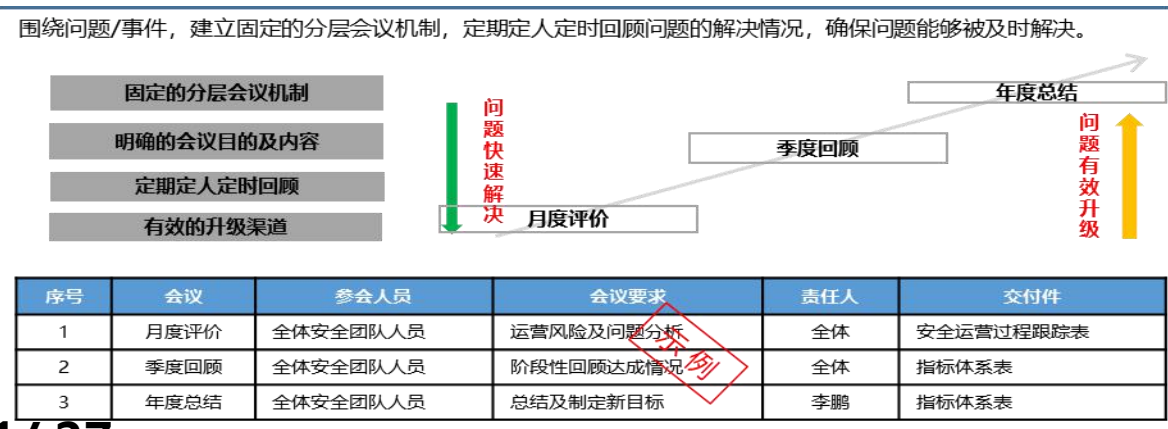
信息流



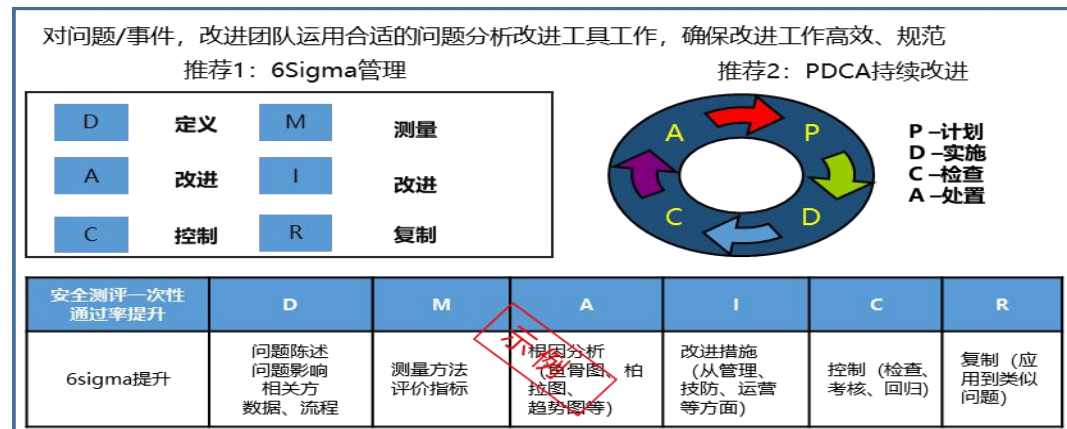
组织机构



时间与数据管理



工具与方法



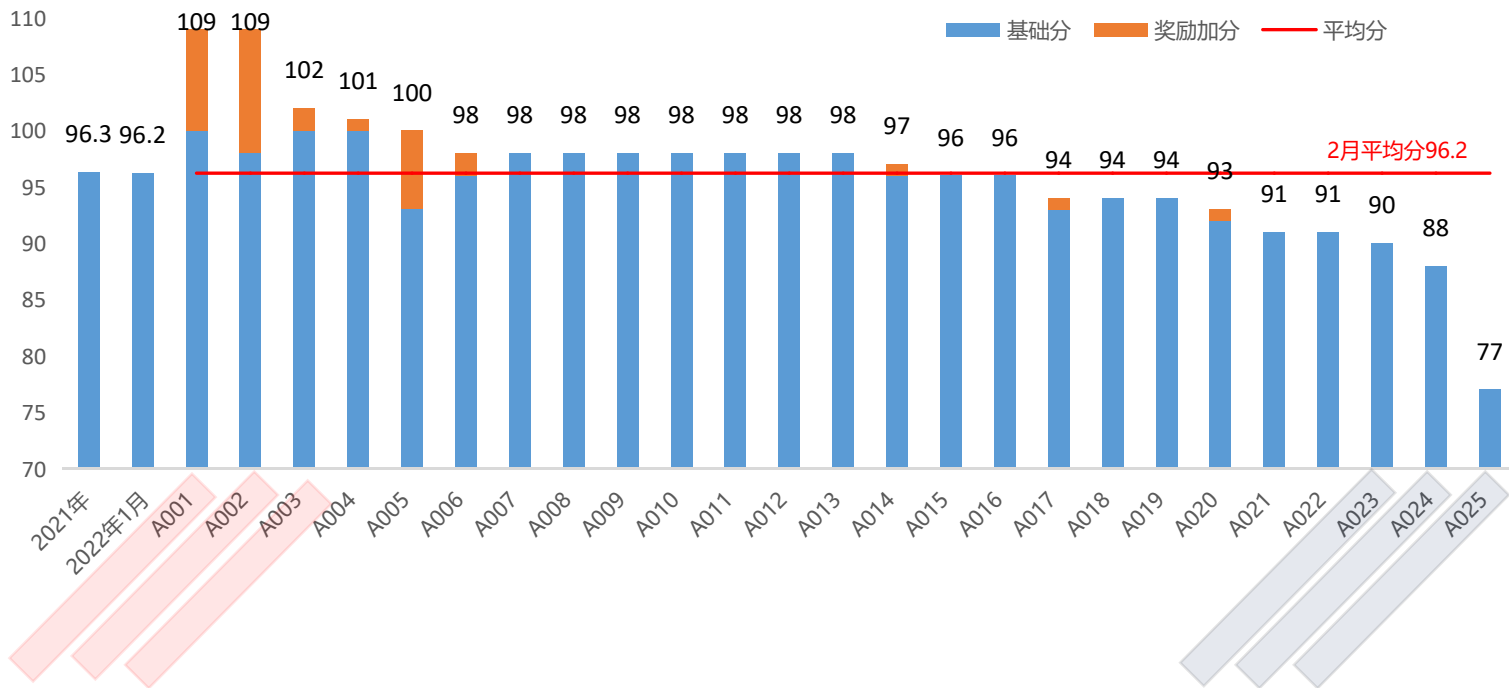
4 实践要点—4.安全管理

落实信息安全常态化管理机制，月度有检查、季度有排名，年度有评优，各单位信息安全整体水平有显著提升。

常态化信息安全管理：“8+3”要素

| 序号 | 评价维度 |
|-----|---------------------|
| 1 | 落实一把手负责制，加强组织领导 |
| 2 | 完善信息安全组织机构，支持日常工作开展 |
| 3 | 持续开展培训宣传，提升全员安全意识 |
| 4 | 细致管理各项清单，自查自纠降低风险 |
| 5 | 建立业务应急机制，应对异常问题发生 |
| 6 | 加强督促检查，终端及人员不合规 |
| 6.1 | 终端防病毒软件部署 |
| 6.2 | 社会工程学攻击防范 |
| 6.3 | 弱口令 |
| 7 | 发现风险异常，立即沟通上报 |
| 8 | 严格考核机制 |

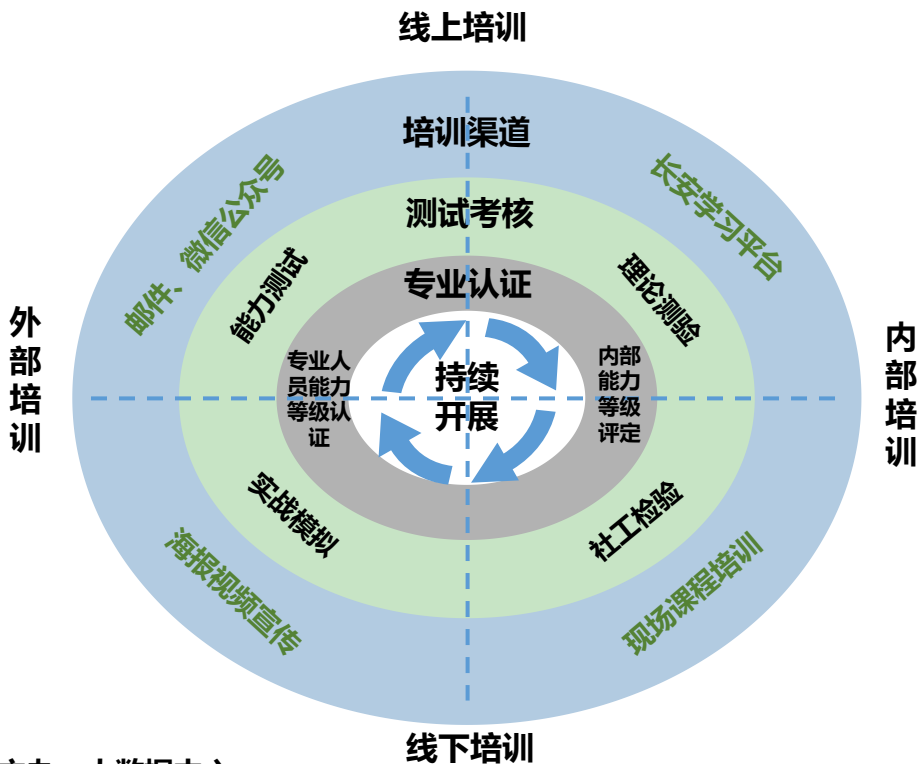
X月各单位信息安全履职情况



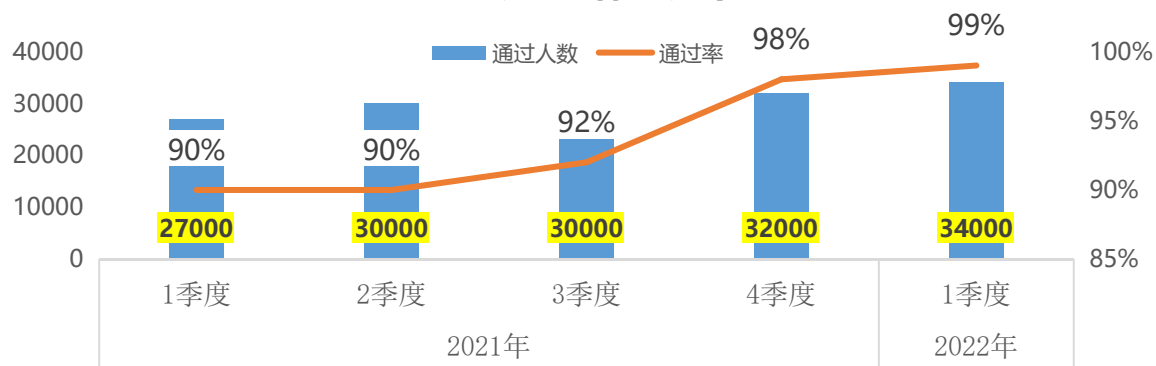
4 实践要点—5.安全意识

全渠道培训机制：构建全渠道、全天候、全覆盖的培训机制，达到人均培训学时超10小时。

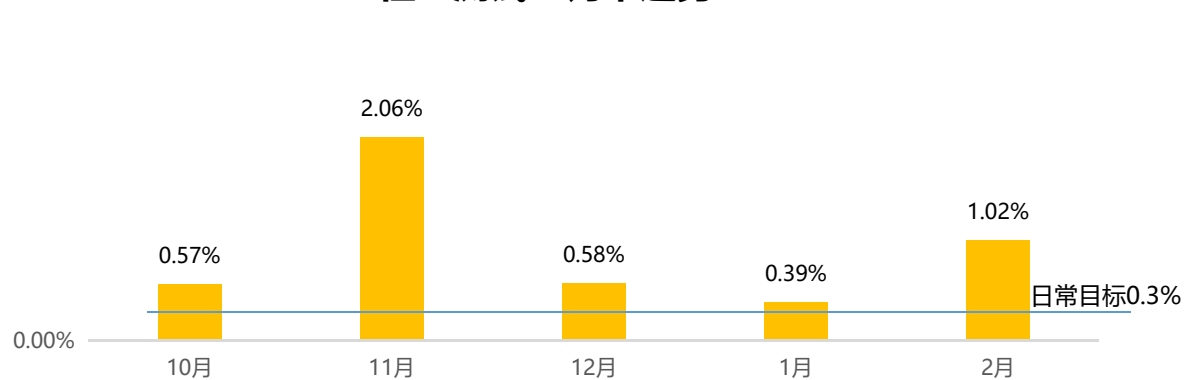
信息安全培训机制



全员线上培训统计



社工测试上钩率趋势



主办：大数据中心

协办：人力资源部、长安学习中心、安全环保部、风险管理部、党群工作部

5 体系规划—架构蓝图

按场景划分对象，六大能力项基于“流程+要素”承接，全景呈现企业面对的信息安全要求，PDCA持续改进。



6 2022年目标和策略

目标：基于数字化服务平台，落实网络安全、数据安全和个人信息保护要求，确保双0。

关键举措：

- ❑ **办公环境：** 深入落实信息安全常态化管理，持续提升主观能动性和安全意识；提升商密防护能力，支撑管理要求落地，降风险，提合规。
- ❑ **智能管理：** 完善安全管理体系，深化纵深防御，贯通安全运营流程，实现常态化、实战化运营能力，实现智能威胁收集，风险分析，智能预警，防御阻断。
- ❑ **智能制造：** 提升生产基地工控防护能力，落实管理和运营，确保生产基地安全风险可控，不因网络安全事故而停线，整体水平提升到65分。
- ❑ **数据安全：** 建立数据全生命周期管理机制，完善安全管理体系，落实数据安全技术，数据安全运营平台，实现数据有效保护与合法利用。

| | 安全管理 | 安全开发 | 安全技术 | 安全运营 | 安全合规 | 数据管控 |
|-----------|---------|---------|---------|---------|---------|---------|
| 办公环境 | • XXXXX | • XXXXX | • XXXXX | • XXXXX | • XXXXX | • XXXXX |
| 智能管理 | • XXXXX | • XXXXX | • XXXXX | • XXXXX | • XXXXX | • XXXXX |
| 智能制造 | • XXXXX | • XXXXX | • XXXXX | • XXXXX | • XXXXX | • XXXXX |
| 数据安全&隐私保护 | • XXXXX | • XXXXX | • XXXXX | • XXXXX | • XXXXX | • XXXXX |
| 云平台安全 | • XXXXX | • XXXXX | • XXXXX | • XXXXX | • XXXXX | • XXXXX |



- **世界观：国家安全，落实发展与安全的关系**
- **大局观：数字转型，提升全员信息安全能力（主体、客体、载体）**
- **角色观：一岗双责，管业务管安全，管好效率与安全的关系**
- **运营观：持续改善，目标+指标，具体行动有沉淀**



长安汽车
CHANGAN AUTO

科技长安
智慧伙伴