长安汽车
CHANGAN

关于信息安全实践的思考

李鹏 | 2022.06

160th SINCE 1862 世纪长安 创领未来

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。**

发源于上海洋炮局
中国近代工业先驱之

1862年-上海

1863年-苏州

更名苏州洋炮局

更名金陵制造局

1865年-南京

1937年-重庆

更名第二十一兵工厂
当时中国最大的兵工企业
为抗战提供60%的武器弹药

以技贸合作形式进入汽车
领域，开始生产小型汽车

1984年

2003年

成立意大利设计中心，
开启长安汽车全球研发布局

中国四大汽车集团阵营企业

2009年

21世纪

走向全球

产品远销全球50余个国家

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

第一个突破2000万销量的中国品牌

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

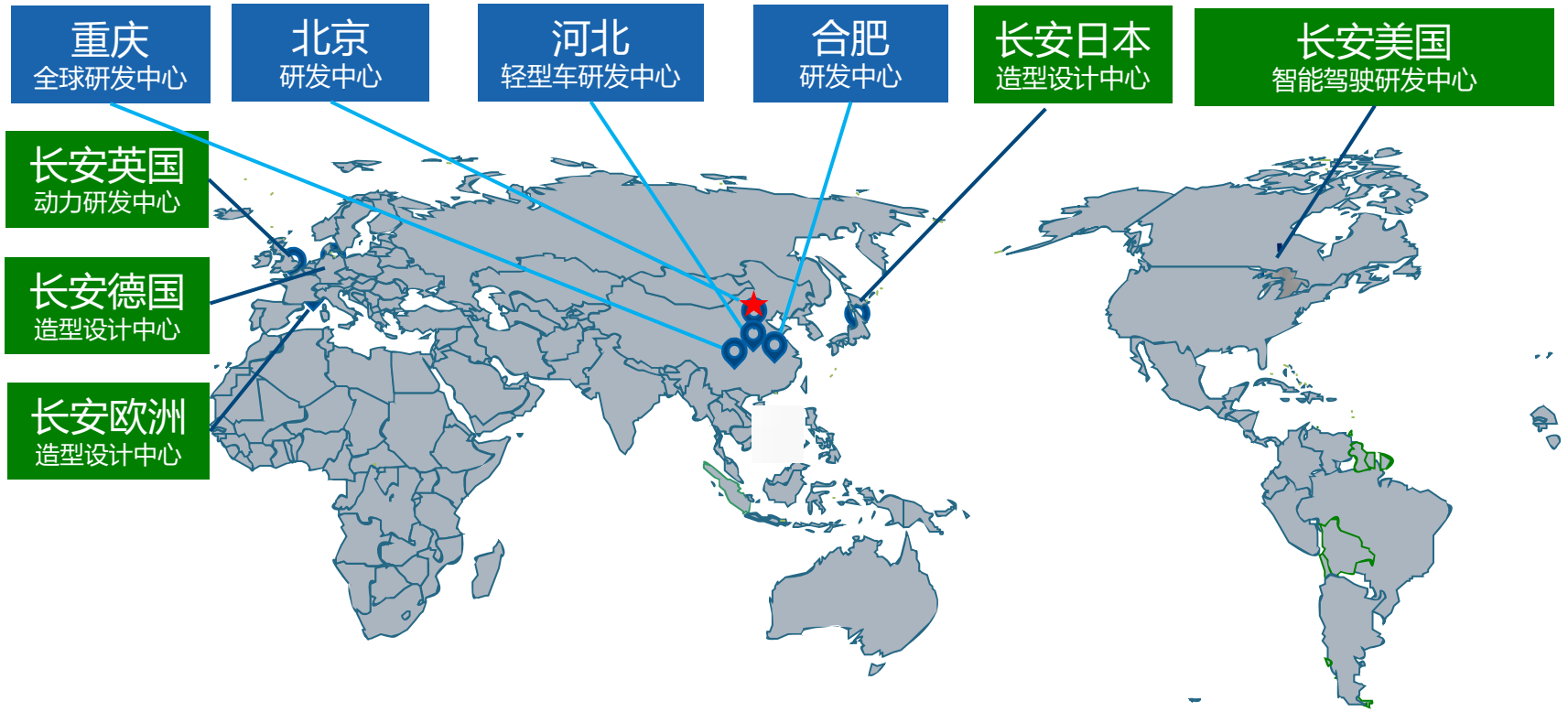
50 余个海外销售国家和地区

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**。

六国九地研发布局



5 “十四五”良好开局

- 长安汽车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，2017年启动“第三次创业——创新创业计划”，坚持运用数字化手段，推动企业转型升级和高质量发展，目前已迈入“数字化3.0”阶段，长安汽车逐步成长为“**既有规模、又有效益**”的自主品牌。

- 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**

目录

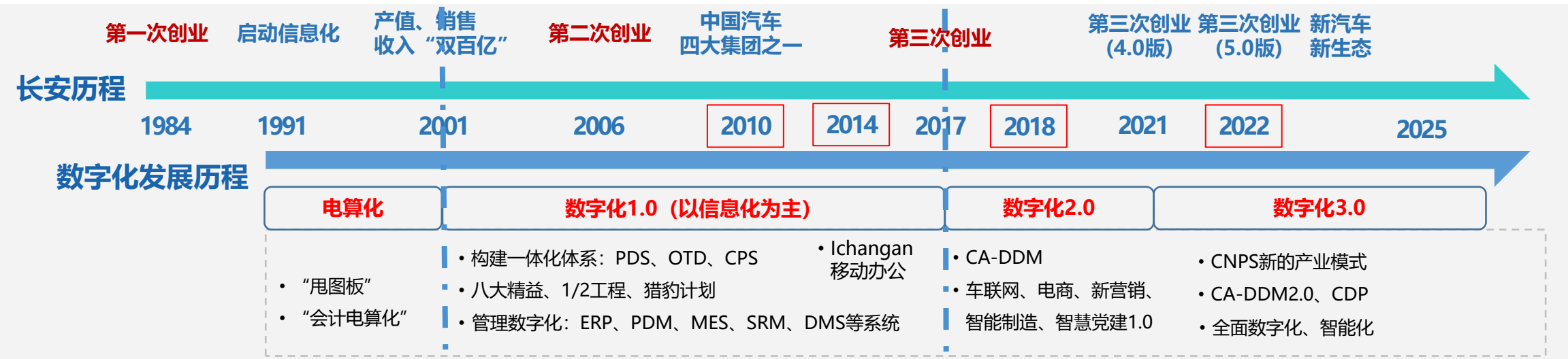
一 长安汽车简介

二 **长安数字化历程**

三 信息安全实践

1 长安汽车已进入数字化3.0阶段

- **电算化**：2001年之前主要实施**“甩图板”“会计电算化”**等。
- **数字化1.0**：以管理体系构建为牵引，管理水平提升为目标，对标一流，全面构建业务流程，**信息化支撑**，打造**现代化管理体系。**
- **数字化2.0**：以**CA-DDM**为标志，拉通内部数据，融合外部数据，推进点状创新（营销、运营等），初步构建“三统一”（统一数据、统一平台、统一运营）的数字化体系。
- **数字化3.0**：基于第三次创业-创新创业计划（5.0版）要求，数字化转型助力长安汽车构建“天上一朵云、空中一张网、中间一平台、地上全场景” 的**新的平台化产业模式**，实现与用户和合作伙伴的直通直联，创造新的商业价值。



- 首批通过两化融合管理体系认证
- 工信部全国首批智能制造试点示范企业
- 连续6年评为国资委A级企业
- 2019年军工行业“数据治理优秀实践单位”
- 2020年国资委“数字化转型优秀案例”

图示：规划年

目录

一 长安汽车简介

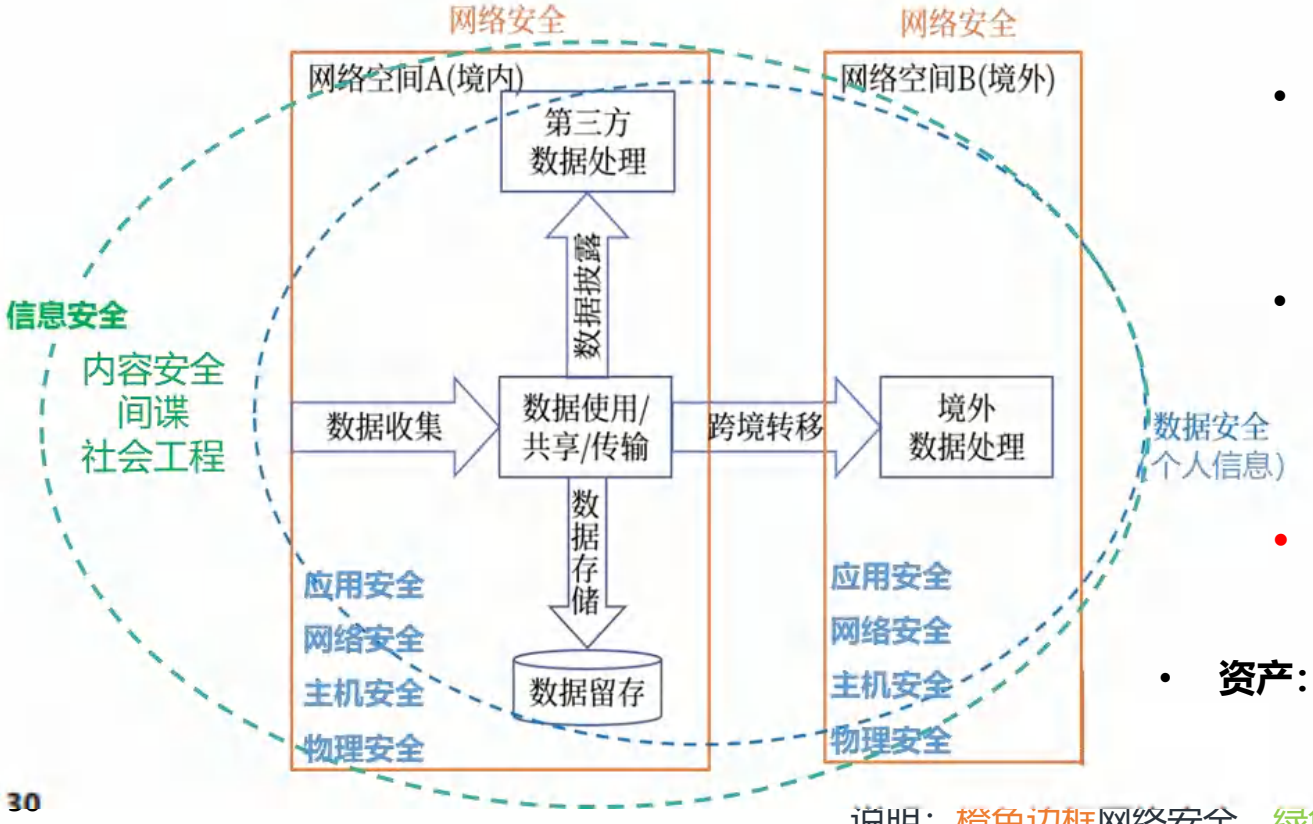
二 长安数字化历程

三 **信息安全实践**

1 定义：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。



- **XX安全的本质**其实就是**增加确定和可控因素，降低不确定因素（风险）。**
- **XX安全工作的核心**就是寻找各种方法**提升对要素的确定性和可控性，并转化不确定因素。**
- **风险=（资产 * 隐患）* 威胁**
- **资产：人员、网络、边界、终端、主机、组件、应用、数据、信息**

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

2 范围：保护对象的演变

从主机时代、网络时代、互联时代逐渐演变到数字智能时代，保护对象的形态已转变为“**大系统、大数据、大平台、数字化城市、智慧化行业**”，未来将走向**城市大脑、行业大脑、工业大脑和国家大脑。**

3 安全挑战来自哪里

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
- 16种安全
- 数据安全与网络安全并列

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

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

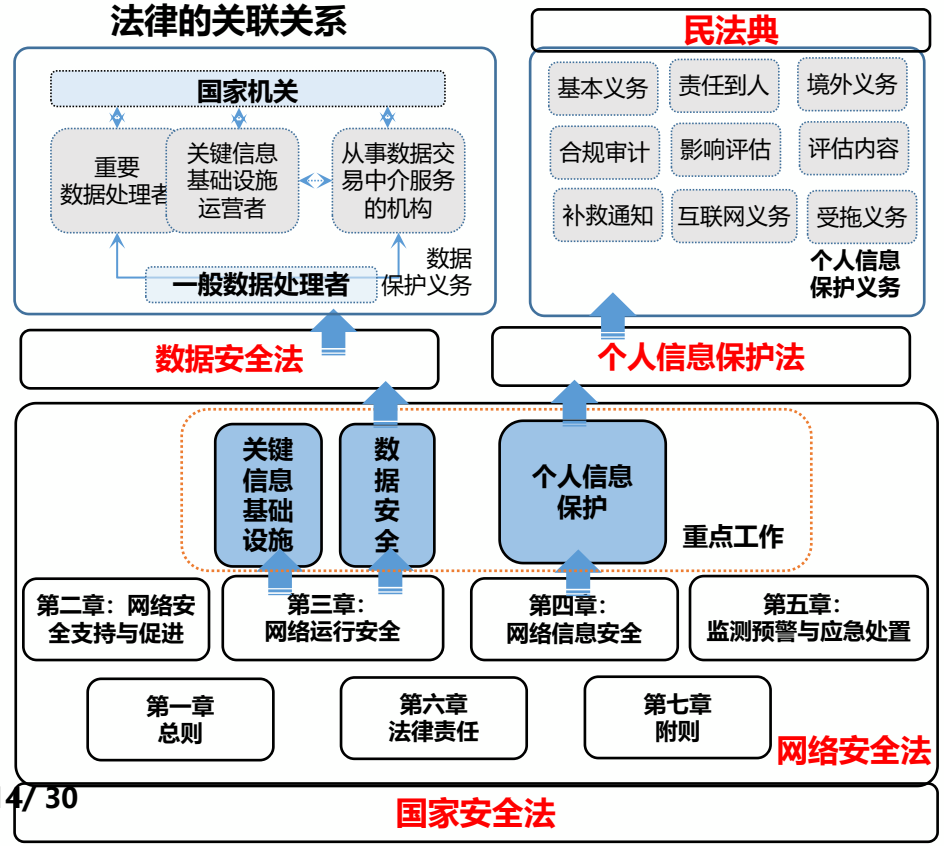
新技术驱动与挑战

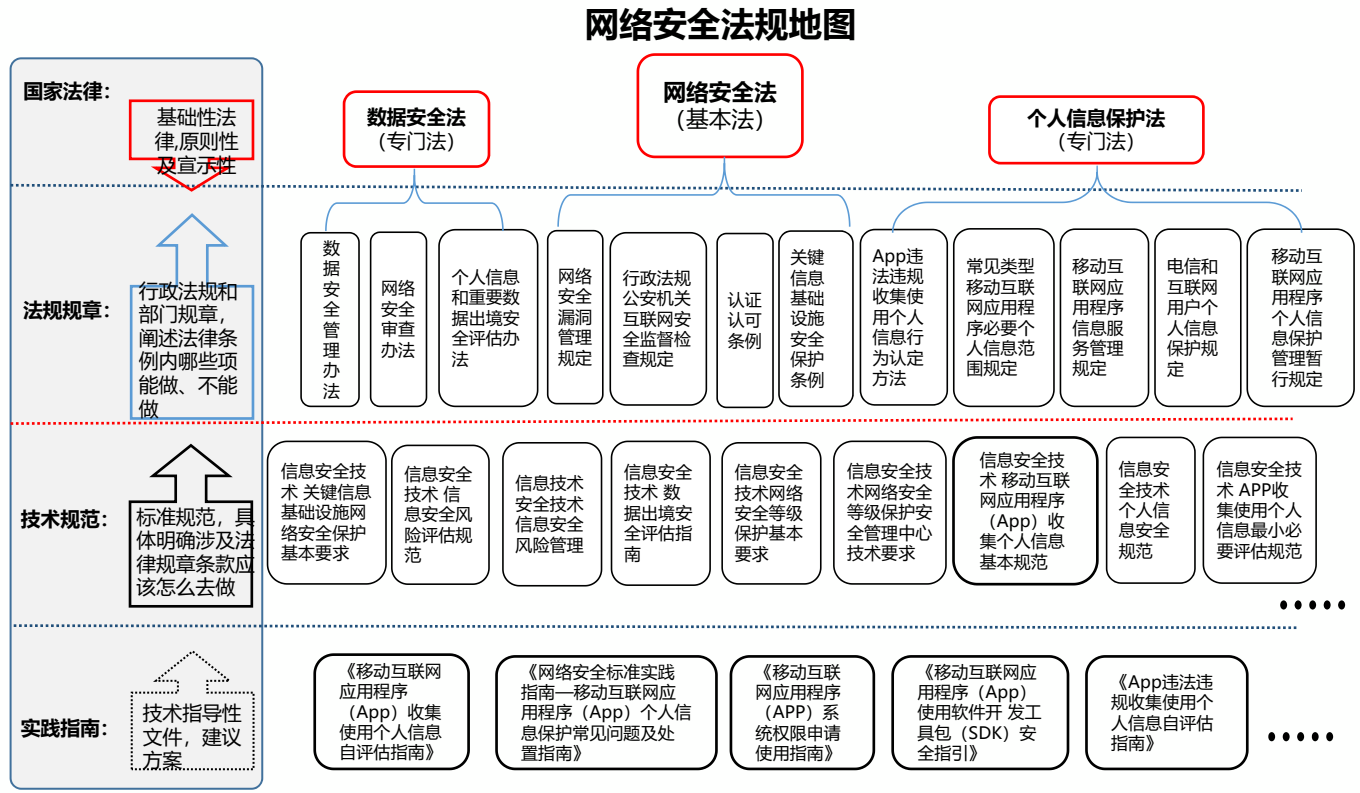
- 混合式的办公方式
- 元宇宙
- 人工智能

4 法规体系—1.关系地图

以国家总体安全观为指引，网络及数据安全强合规监管深化鞭子效力。

- **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。



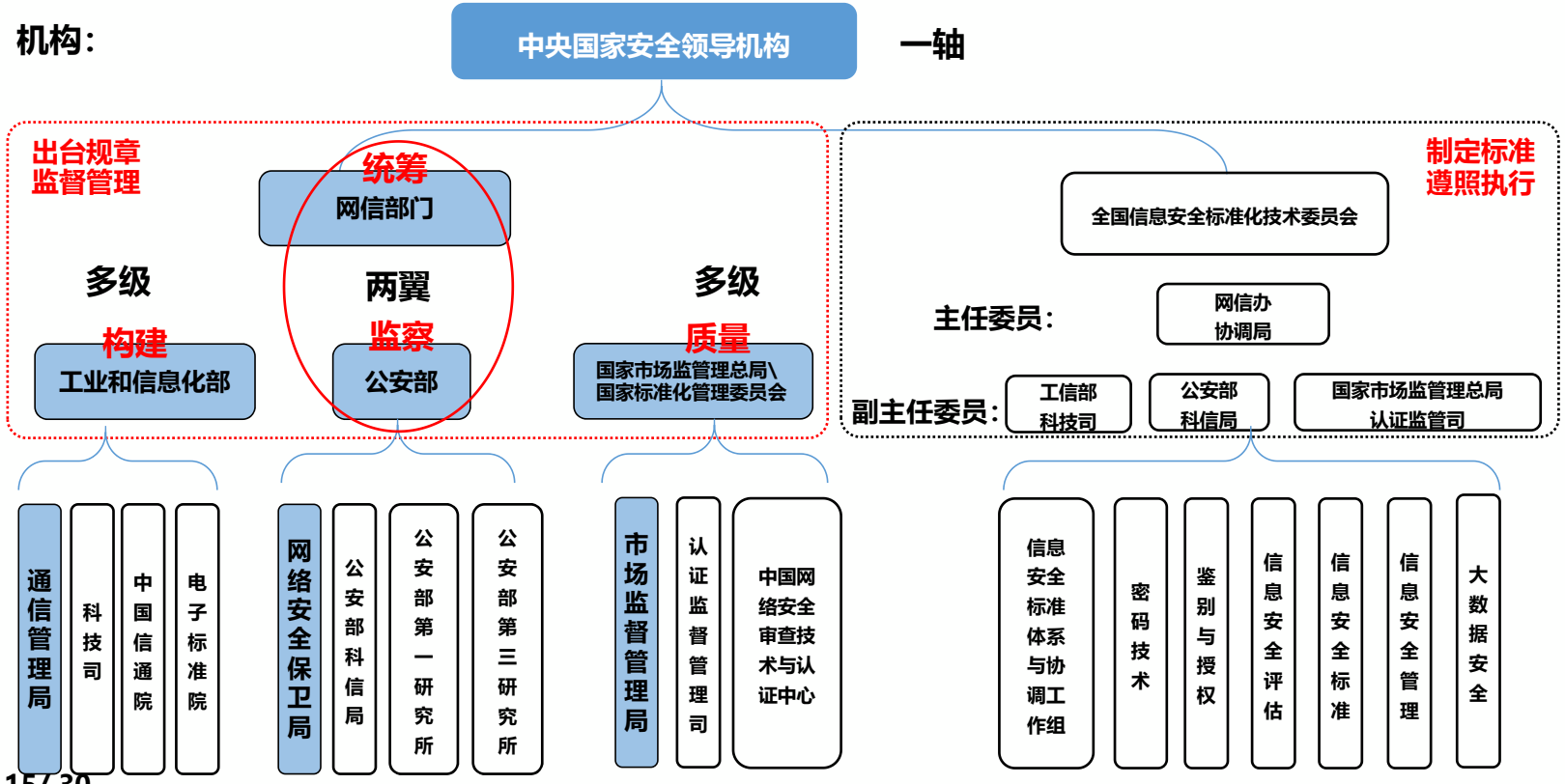


4 法规体系—2.国家监管机构及检查方式

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。

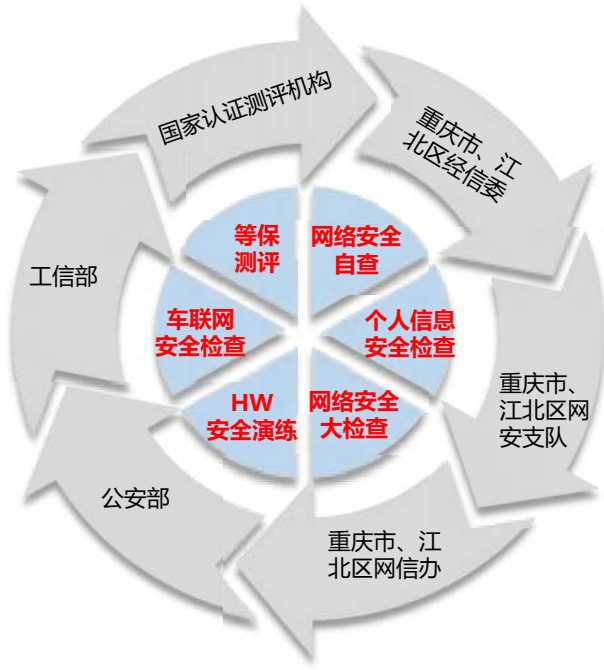
“一轴”指中央国家安全领导机构，两翼指公安机关和网信部门，多级指工业、电信、交通、金融等行业主管部门的共同参与。

机构：



检查及评估：

频率：一年一次



4 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。	• 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	• 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	• 单位：10-100万 • 负责人：1-10万	应急演习；保密协议；每年风评	6	网络服务不得设置恶意程序	• 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	• 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	• 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	• 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。	• 单位:5-50万 • 负责人:1-10万	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	• 单位:10-100万 负责人:1-10万	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	• 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	• 单位:10-100万 负责人:1-10万	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**	单位:100万以下 负责人:1-10万	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	1、合法合理收集、处理个人信息； 2、保障个人信息用户权利； 3、制定内部管理制度和操作规程； 4、个人信息分类管理； 5、采取加密、去标识化安全措施； 6、个人信息处置风险评估，评估报告及处置记录三年； 7、外部成员组成的独立机构，对个人信息处理活动进行监督； 8、个人信息泄露应急处置； 9、第三方保密协议，保障措施。 10、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。		

5 实践要点—1.整体评价

落实网络安全等级保护制度，整体基本符合要求，监管重心由技术层面向业务和数据管理转移。

- **合规概况**：根据对法律法规解读，相关检查项392项，**整体基本符合法规要求**。
- **监管重点**：由IT基础设施及应用安全的**技术层面向业务安全合规及数据安全**管理转移。

		业务合规（业务）																
		用户权益合规							内容信息合规			数据管理合规						三方
		隐私政策	最小化收集	用户授权	明确用途	注销删除	存储期限	用户投诉举报	身份审核	发布审核管理	违法信息屏蔽	数据处理管理	数据出境审核	数据交易审核	个人信息管理	备案许可	日志管理合规	第三方安全管理
网络安全	网络安全法																	
	网络安全等级保护基本要求2.0																	
	网络安全等级保护安全管理中心技术要求																	
	网络产品安全漏洞管理规定																	
	关键信息基础设施安全保护条例																	
数据安全	数据安全法																	
	移动互联网应用程序信息服务管理规定																	
	公安机关互联网安全监督检查规定																	
个人信息保护	个人信息保护法																	
	个人信息安全规范																	
	移动互联网应用程序必要个人信息范围规定																	
	App违法违规收集使用个人信息行为认定方法																	
意见征集中	移动互联网应用程序个人信息保护管理规定																	
	数据安全管理办法																	
	移动互联网应用程序收集个人信息基本规范																	

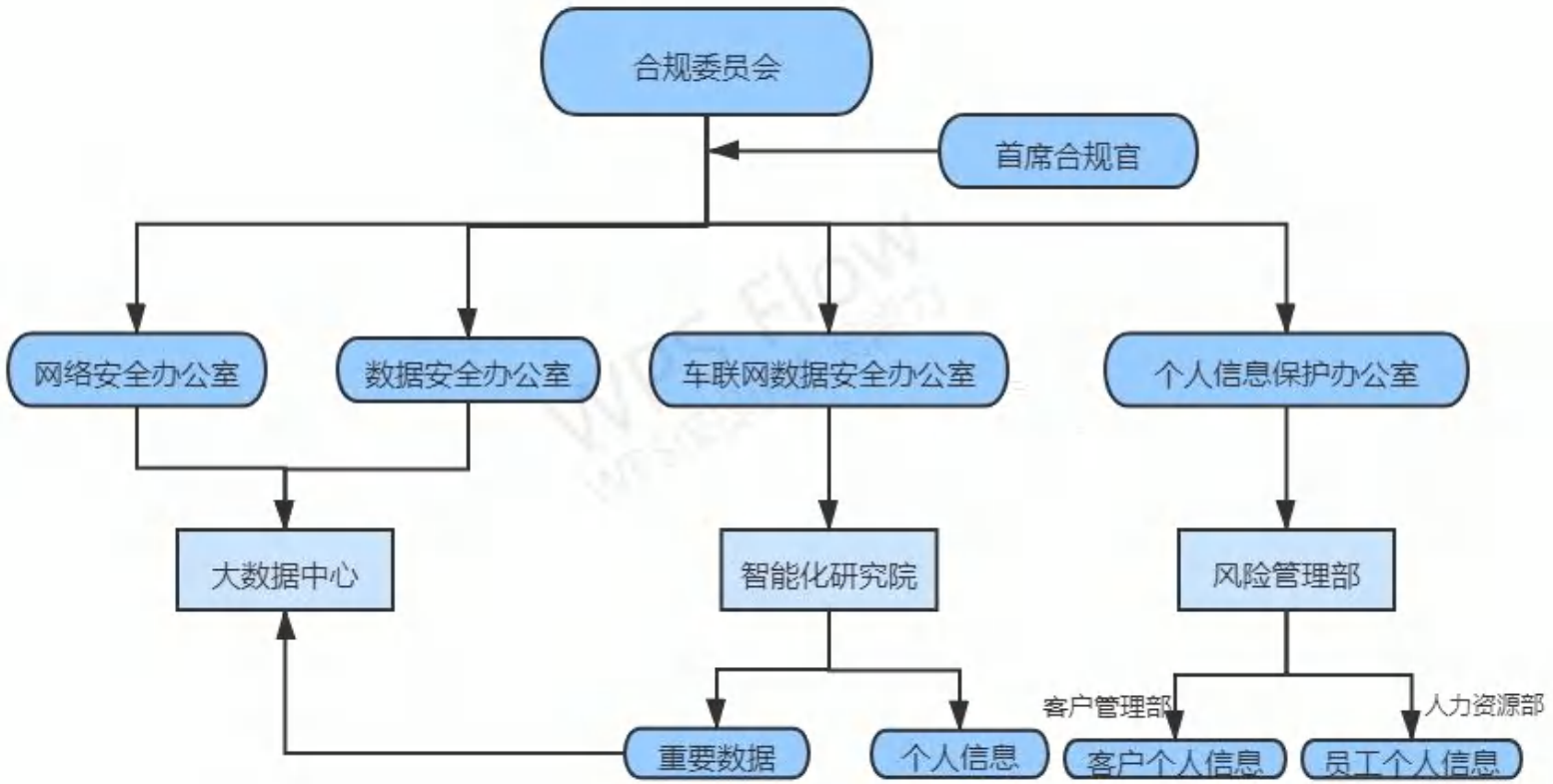
		应用系统及基础设施合规性（IT应用）																								
		物理	通信网络				安全计算环境（主机系统）					开发配置安全				功能安全						重要数据保障				
		机房物理安全	网络架构	通信传输	边界防护	访问控制	身份鉴别	访问控制	账户管理	系统介质安全	数据备份	安全开发	合法证书	APP客户端	组件功能安全	账号认证	权限控制	通信加密	接口安全	文件安全	密码管理	分级分类	数据脱敏	备份恢复	数据完整	数据保密
网络安全	网络安全法																									
	网络安全等级保护基本要求2.0																									
	网络安全等级保护安全管理中心技术要求																									
	网络产品安全漏洞管理规定																									
	关键信息基础设施安全保护条例																									
数据安全	数据安全法																									
	移动互联网应用程序信息服务管理规定																									
	公安机关互联网安全监督检查规定																									
个人信息保护	个人信息保护法																									
	个人信息安全规范																									
	移动互联网应用程序必要个人信息范围规定																									
	App违法违规收集使用个人信息行为认定方法																									
意见征集中	移动互联网应用程序个人信息保护管理规定																									
	数据安全管理办法																									
	移动互联网应用程序收集个人信息基本规范																									

		信息安全能力（基础）																					
		安全组织机构			安全合规要求				安全管理制度							安全技防能力							教育
		组织机构	安全岗位	安全人员	定级评测	风险评估	安全产品资质	安全服务商资质	安全三同时	数据保护	应急响应	监测报告	权限分离	操作规范	安全合规审计	入侵防御	病毒防范	安全加固	漏洞管理	边界防护	监测预警	日志溯源	安全培训
网络安全	网络安全法																						
	网络安全等级保护基本要求2.0																						
	网络安全等级保护安全管理中心技术要求																						
	网络产品安全漏洞管理规定																						
	关键信息基础设施安全保护条例																						
数据安全	数据安全法																						
	移动互联网应用程序信息服务管理规定																						
	公安机关互联网安全监督检查规定																						
个人信息保护	个人信息保护法																						
	个人信息安全规范																						
	移动互联网应用程序必要个人信息范围规定																						
	App违法违规收集使用个人信息行为认定方法																						
意见征集中	移动互联网应用程序个人信息保护管理规定																						
	数据安全管理办法																						
	移动互联网应用程序收集个人信息基本规范																						

不适用或不涉及　符合　部分符合　不符合不紧急　不符合且紧急

5 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。

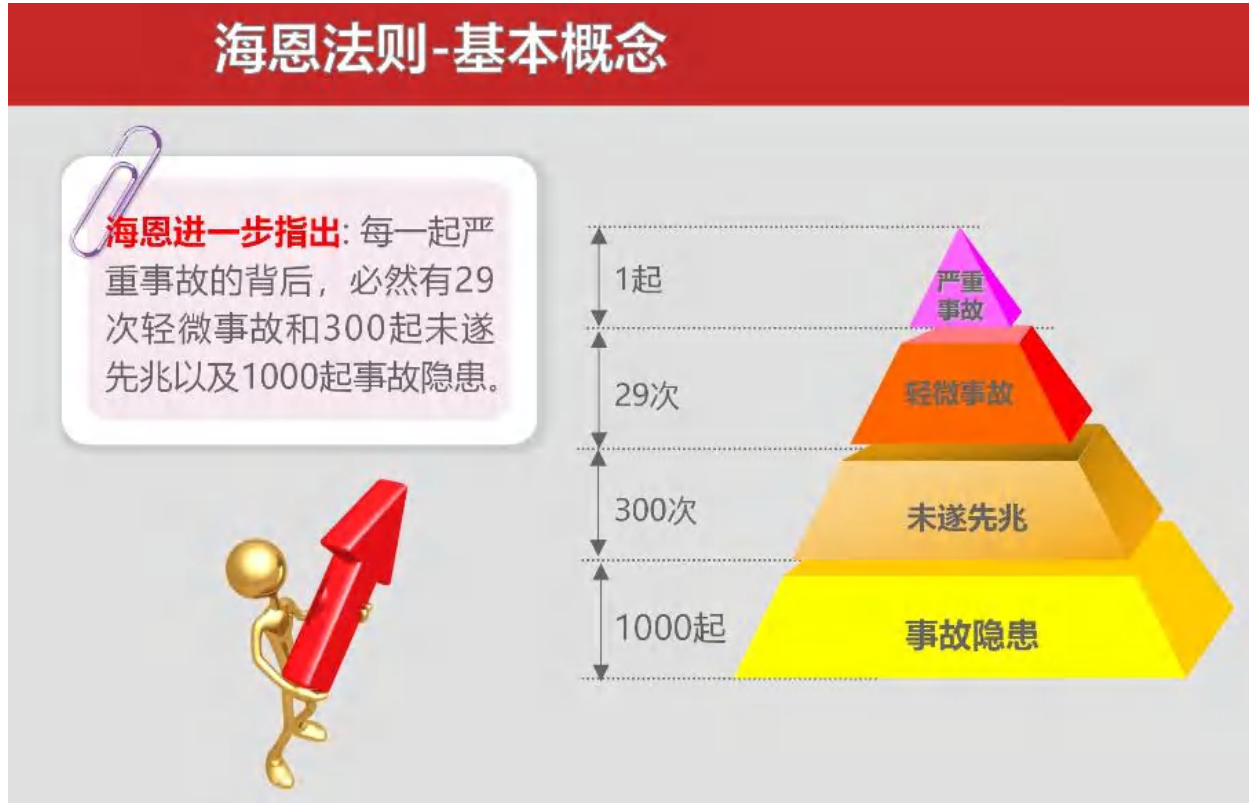


5 实践要点—3.安全运营

- 安全本质是增加确定和可控因素，**降低不确定因素（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”



5 实践要点—3.安全运营-（1）数据驱动（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-周报

一、信息安全问题标准与评价

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	
		人员行为合规率≥95%	99.64%	100%	
大数据中心	应用系统	年度事故隐患小于850个（月＜71个）	156	12	
	办公环境	年度事故隐患小于150个（月＜13个）	4	0	

①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）

2017-2021.04：基础防御阶段1.0，专注于企业高危风险：提权、拖库、敏感信息泄露等，提升基础防御能力。
2021.05-至今：主动防御阶段2.0，在基础设备防御上，深入框架安全，专注互联网新兴测试方法和漏洞，关注外部出口；以攻击者视角，持续提升风险发现水平，提高系统安全性，满足日益严格的法规要求，为护网/重保等活动保驾护航。

基础防御阶段1.0　主动防御阶段2.0

0.67　0.79　2020　2021

0.00　0.07　0.50　0.57　1.18　6.00

2021年1月　2021年2月　2021年3月　2021年4月　2021年5月　2021年6月　2021年7月　2021年8月　2021年9月　2021年10月　2021年11月　2021年12月

主动防御阶段2.0-新建系统问题数目标≤3（单系统）

办公终端问题数趋势（百台终端）

1.40　1.60　0.43　2019　2020　2021

0.876　0.683　2.439　0.000　0.088　0.000　0.000　0.000　0.000　0.000　0.000　0.000

2021年1月　2021年2月　2021年3月　2021年4月　2021年5月　2021年6月　2021年7月　2021年8月　2021年9月　2021年10月　2021年11月　2021年12月

办公终端问题数目标≤5（百台终端）

人员行为合规率

94.60%　95.00%　99.64%　2019　2020　2021

98.3%　96.2%　99.7%　99.6%　99.8%　100.0%　100.0%　100.0%　100.0%　100.0%　100.0%　100.0%

2021年1月　2021年2月　2021年3月　2021年4月　2021年5月　2021年6月　2021年7月　2021年8月　2021年9月　2021年10月　2021年11月　2021年12月

人员行为合规率目标≥95%

示例—常态化管理

安全管理水平（目标≥95分）	人员行为合规率（目标≥95%）	百台终端问题数（目标≤5）
99.87分	99.62%	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
日常检查	全体	G	G	G	G	G	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			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	

二、各单位安全管理情况

各领域安全管理水平

独立事业部　生产基地　研发　营销　职能

94.67　102.33　82.31　101.63　94.57　100.43　98.80　100.00　92.90　98.79

1季度　2季度　1季度　2季度　1季度　2季度　1季度　2季度　1季度　2季度

各单位安全管理水平

领域	单位	
职能	科技及项目管理部	87.00
	物流中心	90.20
	长安汽车大学	92.00
	研发园区综合事务部	95.00
	安全环保部	98.80
	产品策划部	100.00
	人力资源部	100.00
	党群工作部	100.00
	公司办公室	100.00
	印度及东盟项目组	100.00
	合资合作部	100.00
	品牌公关部	100.00
	大数据中心	100.00
	客户服务公司	100.00
	客户管理部	100.00
	战略规划部	100.00

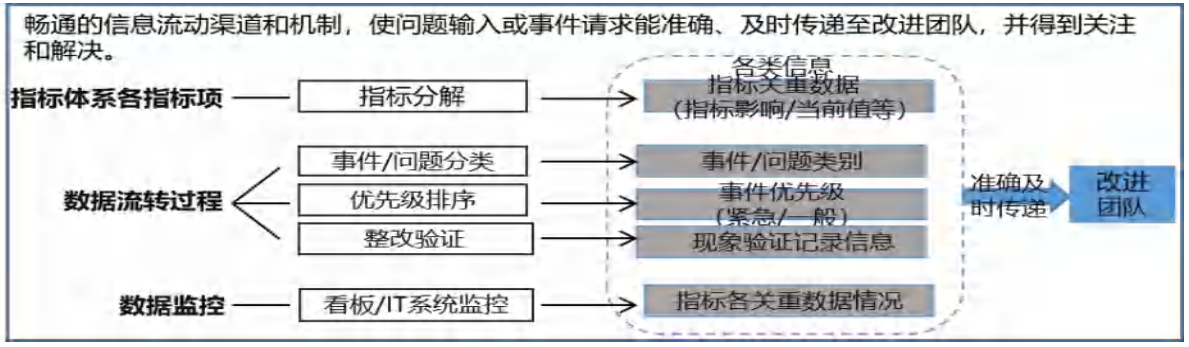
5 实践要点—3.安全运营-（2）运营机制

让 指标 通过安全运营”跑“起来（QIP）

- 数据驱动的安全运营机制：指标-事件/问题
- 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。

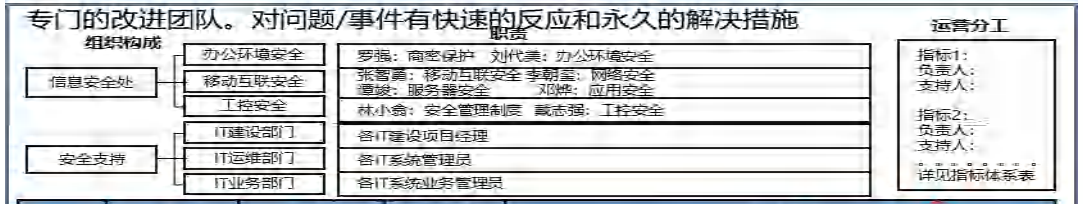
信息流

畅通的信息流动渠道和机制，使问题输入或事件请求能准确、及时传递至改进团队，并得到关注和解决。



组织机构

专门的改进团队。对问题/事件有快速的反应和永久的解决措施



序号	团队名称	团队成员	团队角色	职责分工
1	安全测评一次性通过率提升团队	李鹏	团队负责人	1.负责项目选择和项目范围的制定； 2.项目管理，为项目消除障碍，并提供资源支持。
2		邓烨	牵头人	1.带领团队用6Sigma方法和工具完成项目； 2.同团队成员一起完善具体的维持措施。
3		张智勇/李朝玺/谭骏	团队成员	1.参与项目推进过程 2.评价项目改进效果

时间与数据管理

围绕问题/事件，建立固定的分层会议机制，定期定人定时回顾问题的解决情况，确保问题能够被及时解决。

序号	会议	参会人员	会议要求	责任人	交付件
1	月度评价	全体安全团队人员	运营风险及问题分析	全体	安全运营过程跟踪表
2	季度回顾	全体安全团队人员	阶段性回顾达成情况	全体	指标体系表
3	年度总结	全体安全团队人员	总结及制定新目标	李鹏	指标体系表

工具与方法

对问题/事件，改进团队运用合适的问题分析改进工具工作，确保改进工作高效、规范

推荐1：6Sigma管理

D	定义	M	测量
A	改进	I	改进
C	控制	R	复制

推荐2：PDCA持续改进

P –计划
D –实施
C –检查
A –处置

安全测评一次性通过率提升	D	M	A	I	C	R
6sigma提升	问题陈述 问题影响 相关方 数据、流程	测量方法 评价指标	根因分析 （鱼骨图、柏拉图、 趋势图等）	改进措施 （从管理、 技防、运营 等方面）	控制（检查、 考核、回归）	复制（应 用到类似 问题）

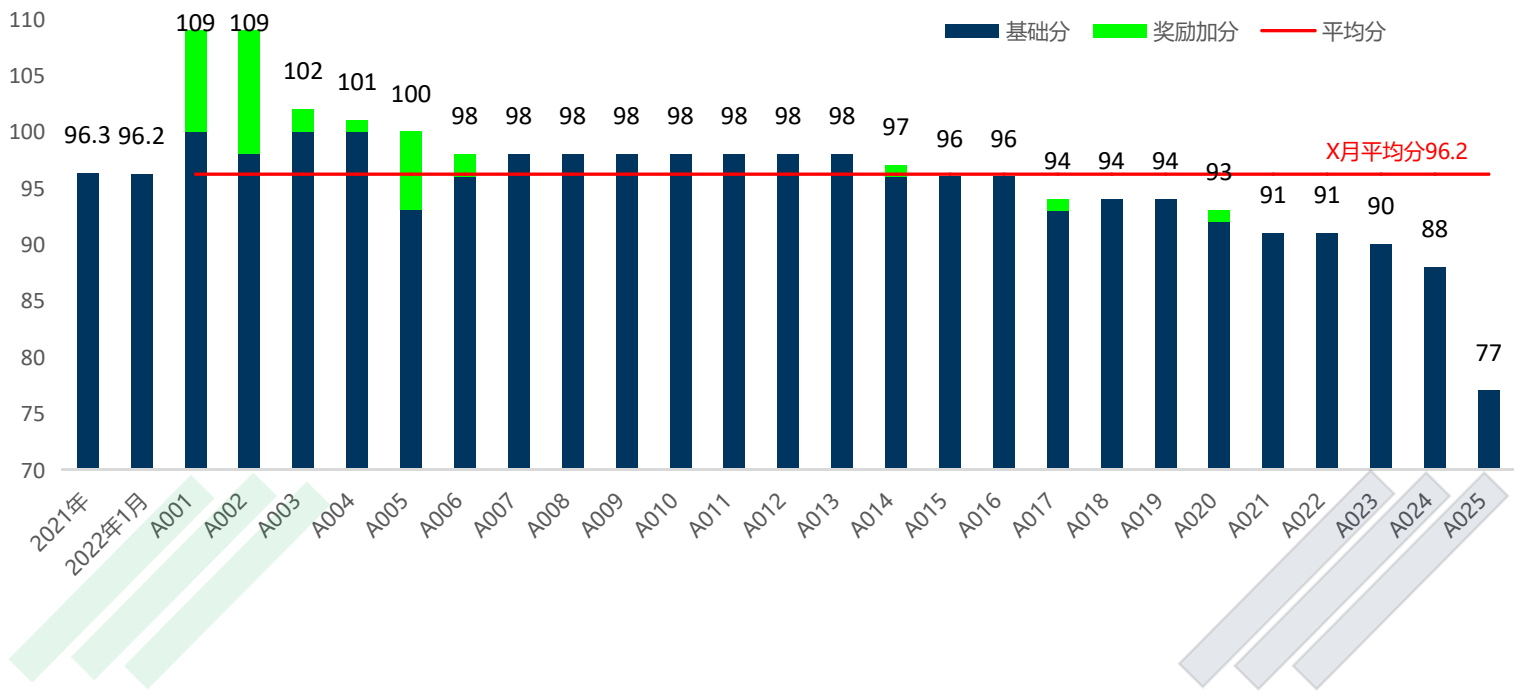
5 实践要点—4.安全管理

- 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

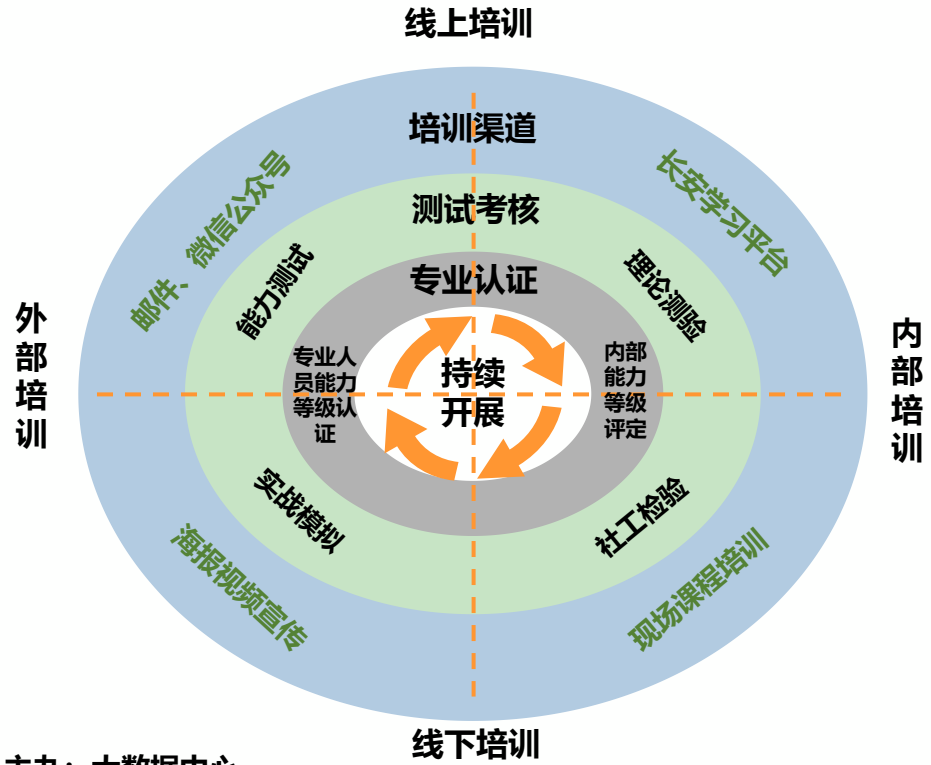
X月各单位信息安全履职情况



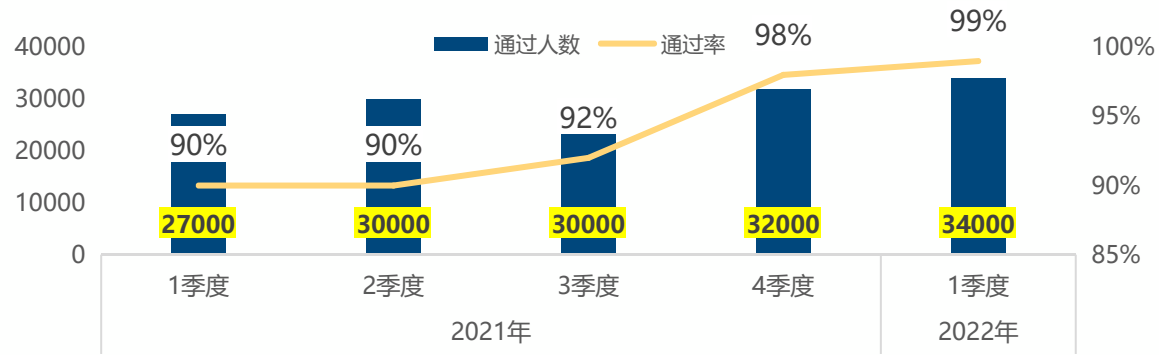
5 实践要点—5.安全意识

□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。

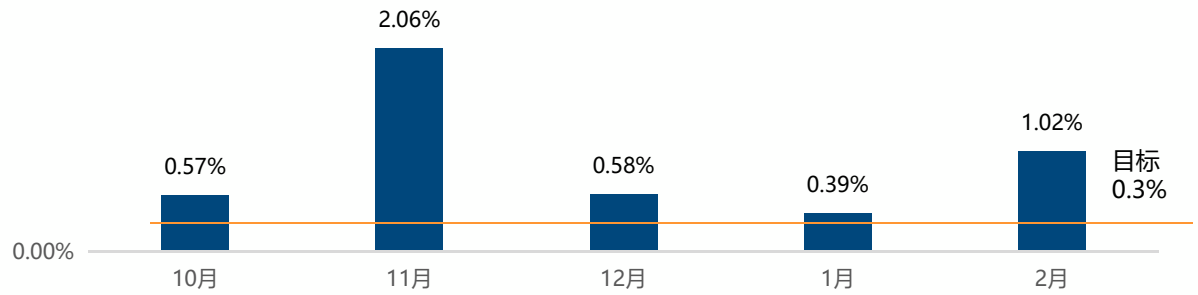
信息安全培训机制



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

6 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。

7 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，安全能力水平提升9%。

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

8 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

9 几点思考

- 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

世纪长安
创领未来