

*“Face the challenge, Embrace the best practice”*

EISS - 2019  
企业信息安全峰会  
之深圳站  
2019.8.16

安全+



# 企业数据安全实践

黄鹏华(PH22)



# 目录

CONTENTS

01 数据安全的一些现状

02 数据安全建设一些思考

03 几个场景下数据安全的防护



Part 01

# 数据安全的一些现状



# 政策合规要求



2017年6月1号《网络安全法》生效



2019年2月1号《信息安全技术 个人信息安全规范（草案）》发布



2019年5月5号《App违法违规收集使用个人信息行为认定方法（征求意见稿）》发布



2019年5月28号《数据安全管理办法（征求意见稿）》发布



2019年12月1号 网络安全等级保护制度2.0生效



预计2019年会通过《数据安全法》

# 数据泄露事件频发



Facebook 2018年10月剑桥分析公司数据丑闻



2017年Equifax泄露近1.5亿人的个人信息和财务数据



2018年万豪集团旗下喜达屋酒店客房预定信息泄露



2013年雅虎30亿账户信息泄露



2018年英国航空公司数十万客户资料泄露

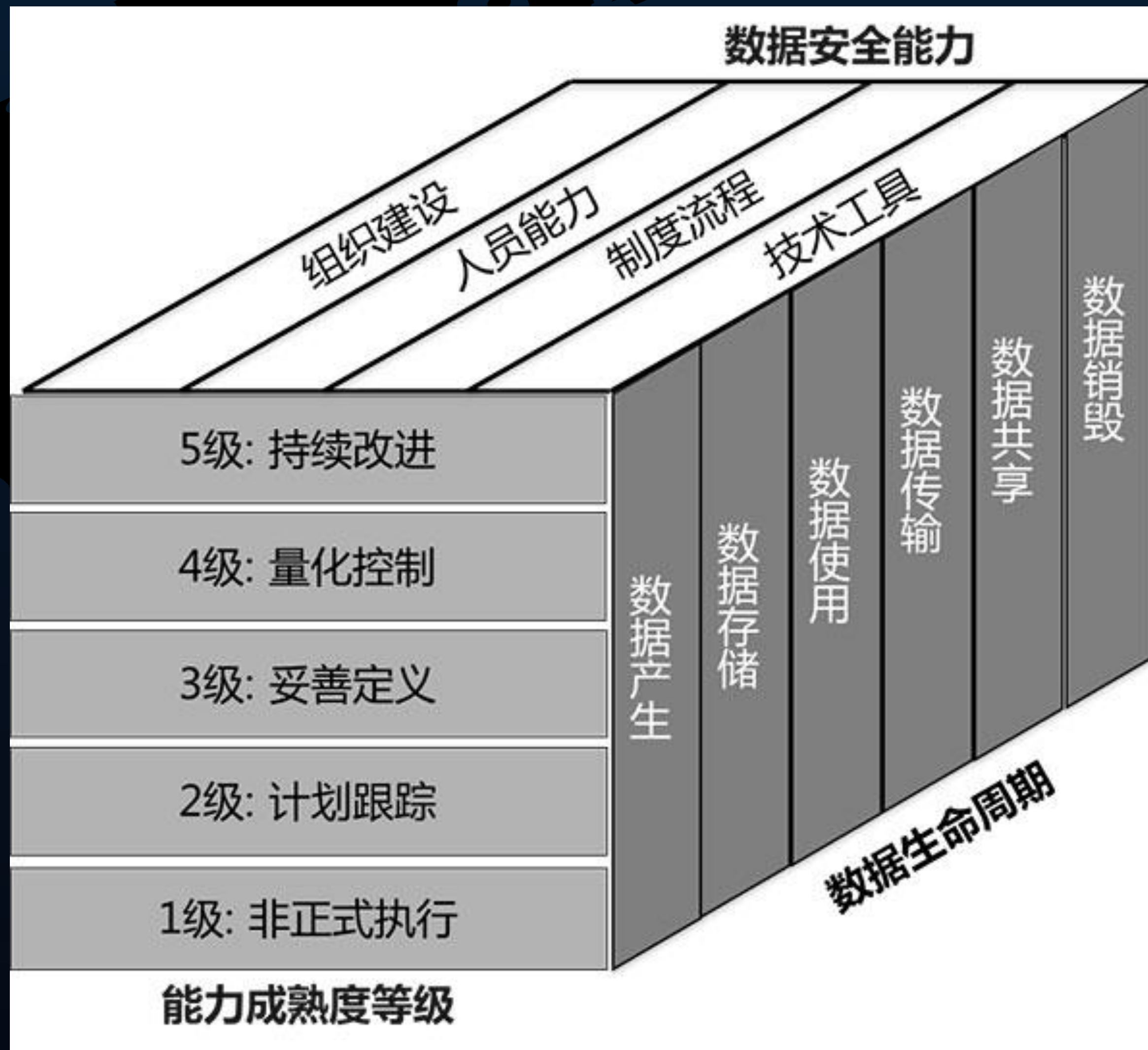


Part 02

# 数据安全建设的一些思考

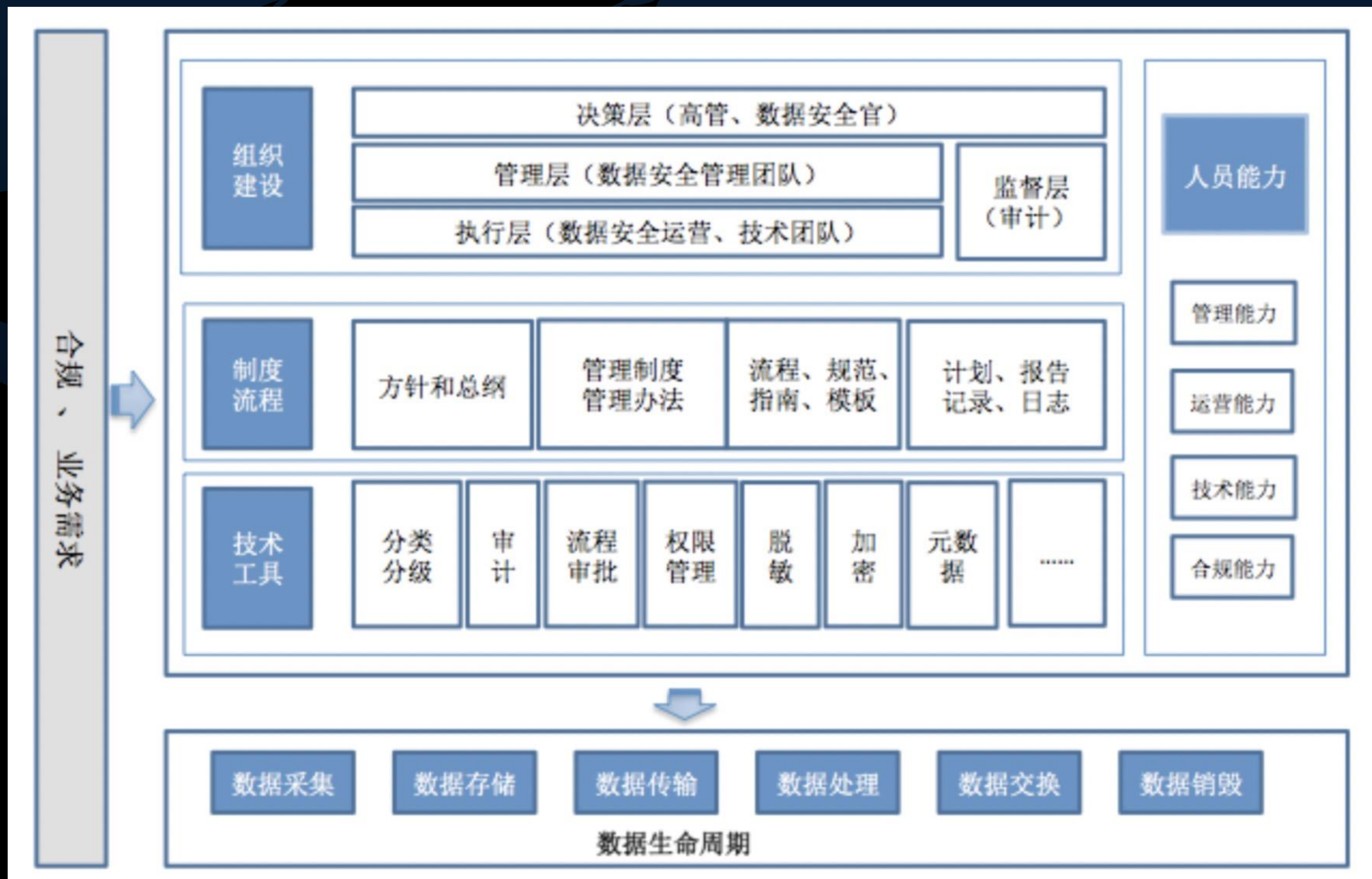


# 数据安全能力成熟度模型 (DSMM)





# 数据安全能力成熟度模型 (DSMM)





# 数据安全建设目标

01

进不来

通过认证授权、基础安全等措施控制对业务系统、服务器、数据库、文件等资源的访问

02

拿不走

通过访问控制、权限管理、部署DLP等方式及时进来也没有权限可以拿走数据

03

看不懂

在数据传输、存储等过程中使用各种加密技术、脱敏技术等措施保证无法看到原始数据

04

走不脱

通过部署日志审计、数据库操作审计、运维操作审计等措施可进行事后分析溯源



# 数据安全建设要求



**机密性**

不想被知道



**完整性**

不想被篡改



**可用性**

不想影响服务正常运行



**服务化**

业务侧无需关心具体的实现，只需要便捷的调用



**平台化**

依托平台通过具体场景有效推进数据安全落地



# 数据安全



数据加密



密钥管理



数据脱敏



资产管理



权限管理



日志审计



数据备份



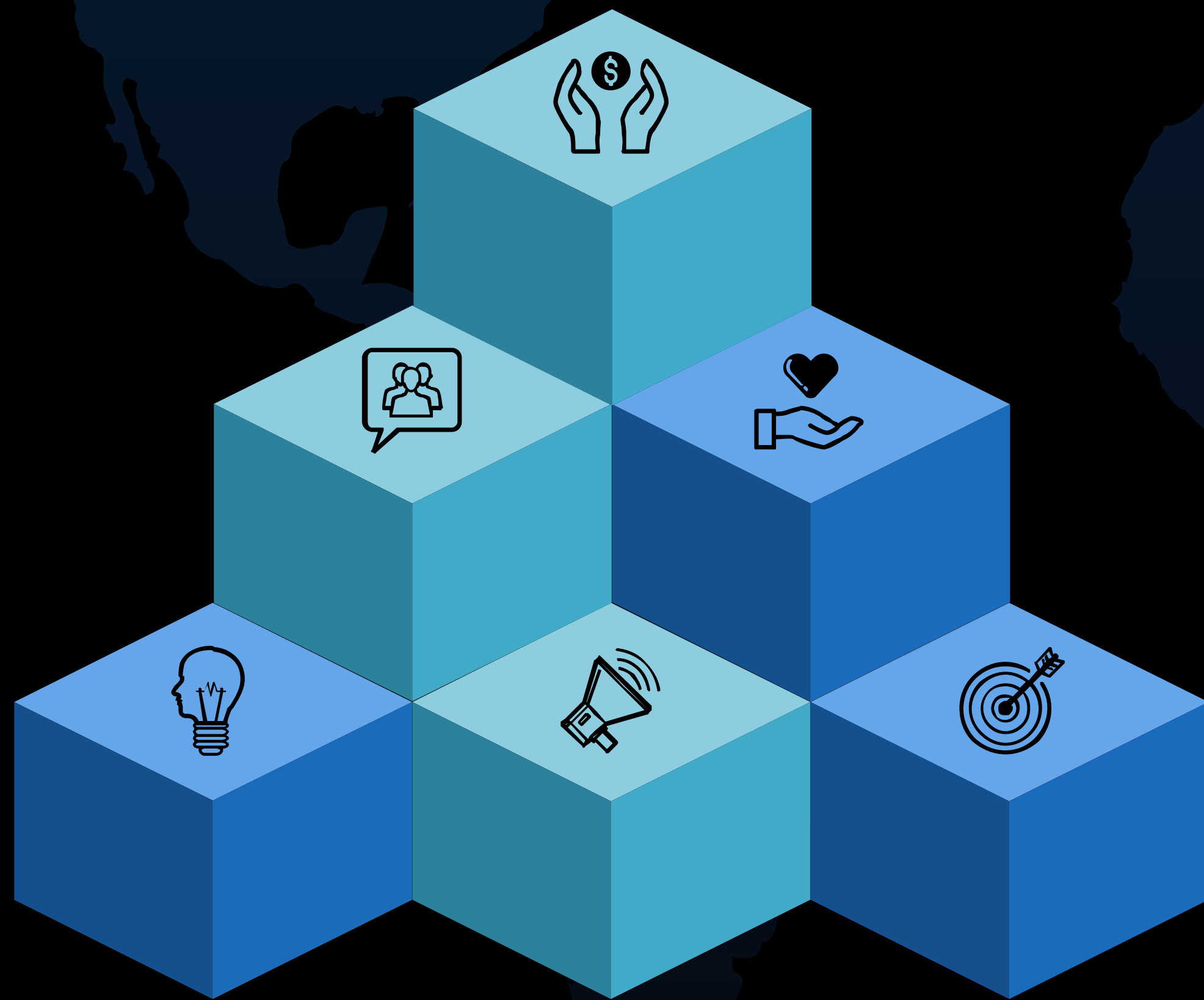
安全监控



安全运营



# 前置安全保障



安全域划分



蜜罐



WAF



堡垒机



HIDS



流量监控



# 数据安全生命周期-数据流动路径

数据产生



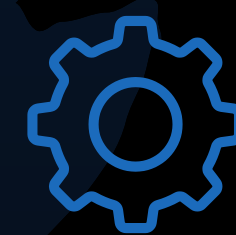
数据处理



数据交换



数据传输



数据存储



数据销毁



# 数据资产管理



## 数据资产梳理

企业数据在哪里、隐私数据有哪些



## 数据资产探测

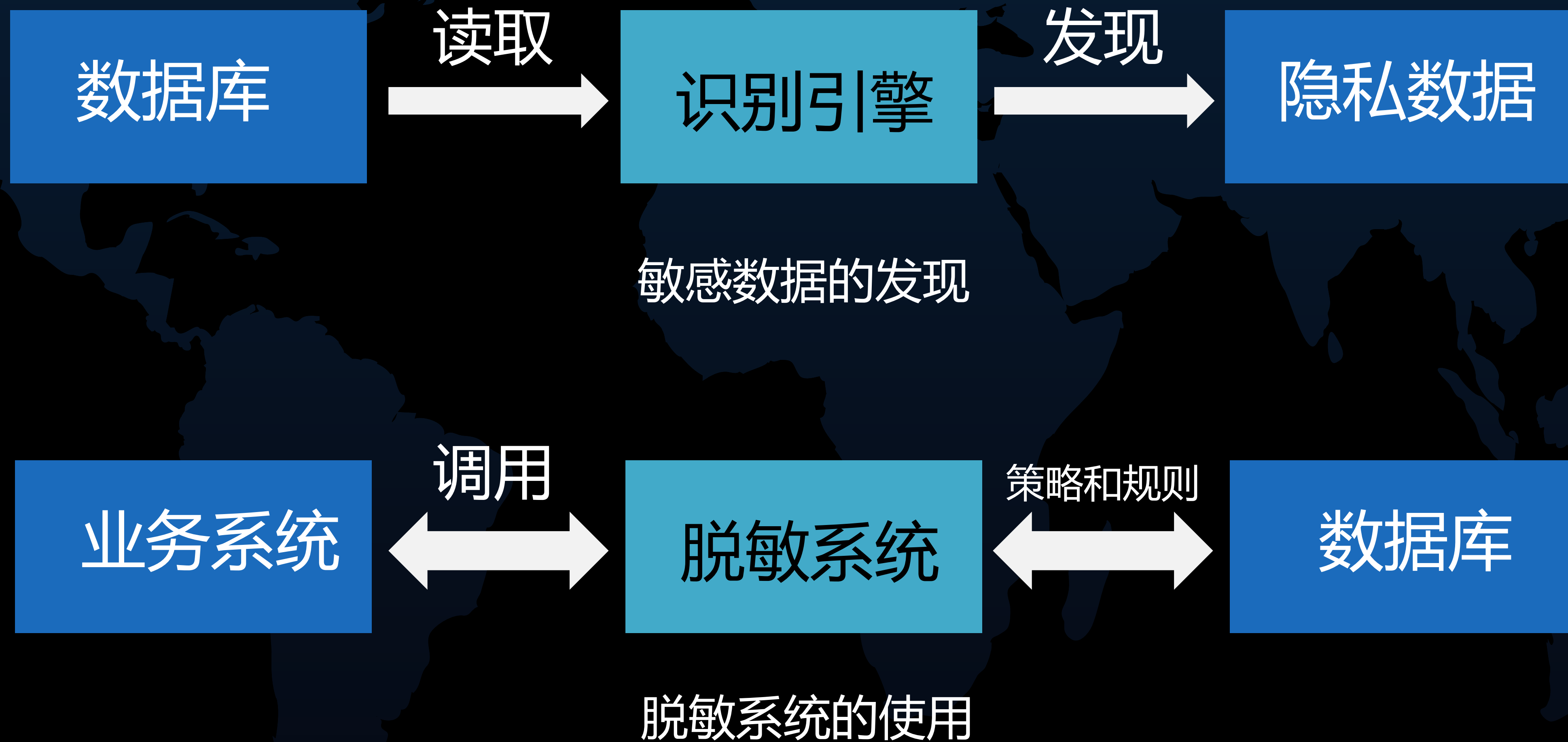
已知的数据资产是否齐全、是否有历史遗留等



## 数据分类分级

给数据进行分类分级，确定保护程度

# 脱敏系统





# 统一权限管理



## 单点登录

接入的后台系统统一单点登录方式



## 平台化

提供平台化接口，统一各后台系统的接入方式



## 业务方参与审批

分配权限时，业务方参与审批遵循最小权限原则

# 安全监控



## 扫号和爬虫

对扫号和爬虫行为监控，及时响应拦截



## 数据蜜罐

通过部署蜜库、蜜表等形式发现异常操作



## github信息泄露监控

及时发现敏感信息被上传github泄露



## 内部wiki信息泄露监控

监控内部wiki平台出现的一些敏感信息



# 安全审计



## 数据库操作审计

对数据库操作，特别是高危操作的记录



## 各业务系统操作审计

业务方自己用的系统的操作记录



## 防护系统的操作审计

各安全防护系统的操作记录

# 数据安全运营



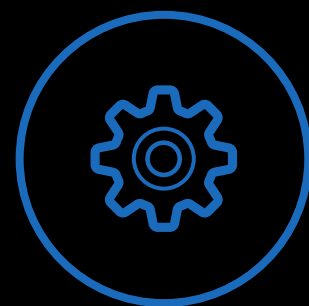
## 数据安全建设中重要一环

更大程度发挥各防护措施的联动效果



## 持续监控识别风险，跟进修复

不间断监控各个风险点，对异常情况及时响应



## 保障各个安全措施运行正常

监控各个安全防护系统的运行状态



## 数据安全红蓝对抗

持续使用蓝军来验证防护能力





Part 03

# 几个场景下的数据安全防护

# 几个场景下的数据安全防护



场景：运营/客服人员通过后台业务系统泄露用户信息



防护：

1. 通过权限管理系统收紧相关人员的操作权限
2. 相关业务系统接入脱敏系统，敏感信息脱敏展示
3. 业务系统操作审计记录，用于事后审计溯源
4. 通过开放接口等方式减少业务系统数据本地导出操作



# 几个场景下的数据安全防护



场景：研发/运维人员访问线上数据库泄露用户信息



防护：

1. 收紧相关人员线上数据库访问权限，关闭不必要的访问
2. 部署数据蜜罐，发现异常人员操作
3. 数据库实现字段级别的加密
4. 收紧密钥的使用权限
5. 敏感数据操作审计

# 工作推进一些思考



心态上我们是职能部门要服务于业务方，提高用户体验




沟通上让对方理解我们的需求，不拘于实现的策略



先解决增量问题，再去处理存量问题





PH22 

福建 厦门



扫一扫上面的二维码图案，加我微信

# 谢谢观看

“安全+”专注于信息安全行业，通过互联网平台、线下沙龙、培训、峰会、人才招聘等多种形式，培养安全人才，提升行业的整体素质，助推安全生态圈的健康发展。

官方网站：[www.anquanjia.net.cn](http://www.anquanjia.net.cn)

微信公众号：anquanplus

