SSTG
安全产品技术部

滴滴出行

爱康集团信息安全建设

敏感数据守护之路

吴洋

共建安全新生态
2020滴滴网络安全峰会

2020.12.17

目录

01 背景介绍

01 背景介绍

国内

·中国人民共和国数据安全法
·中华人民共和国个人信息保护法
·中华人民共和国民法典，强调隐私权和个人信息保护

国际

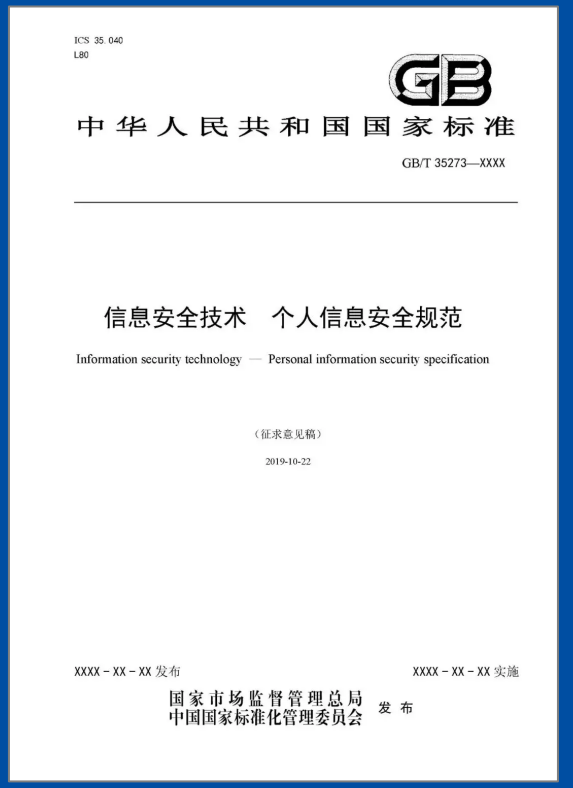
· ISO 27001
· GDPR
· ISO 27701

爱康集团

· 数据敏感
· 数据类型多
· 数据量巨大
· 群体特殊

02 个人信息保护思路

02 个人信息工作开展的依据



个人PII信息

GB/T 35273-2017：个人信息

以电子或者其他方式记录的，能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息。

可从信息本身的特殊性识别出特定自然人

已知特定自然人，由该特定自然人在其活动中产生的信息

ISO 29100：个人可识别信息PII

（a）可用于识别与此类信息相关的PII主体的任何信息，或

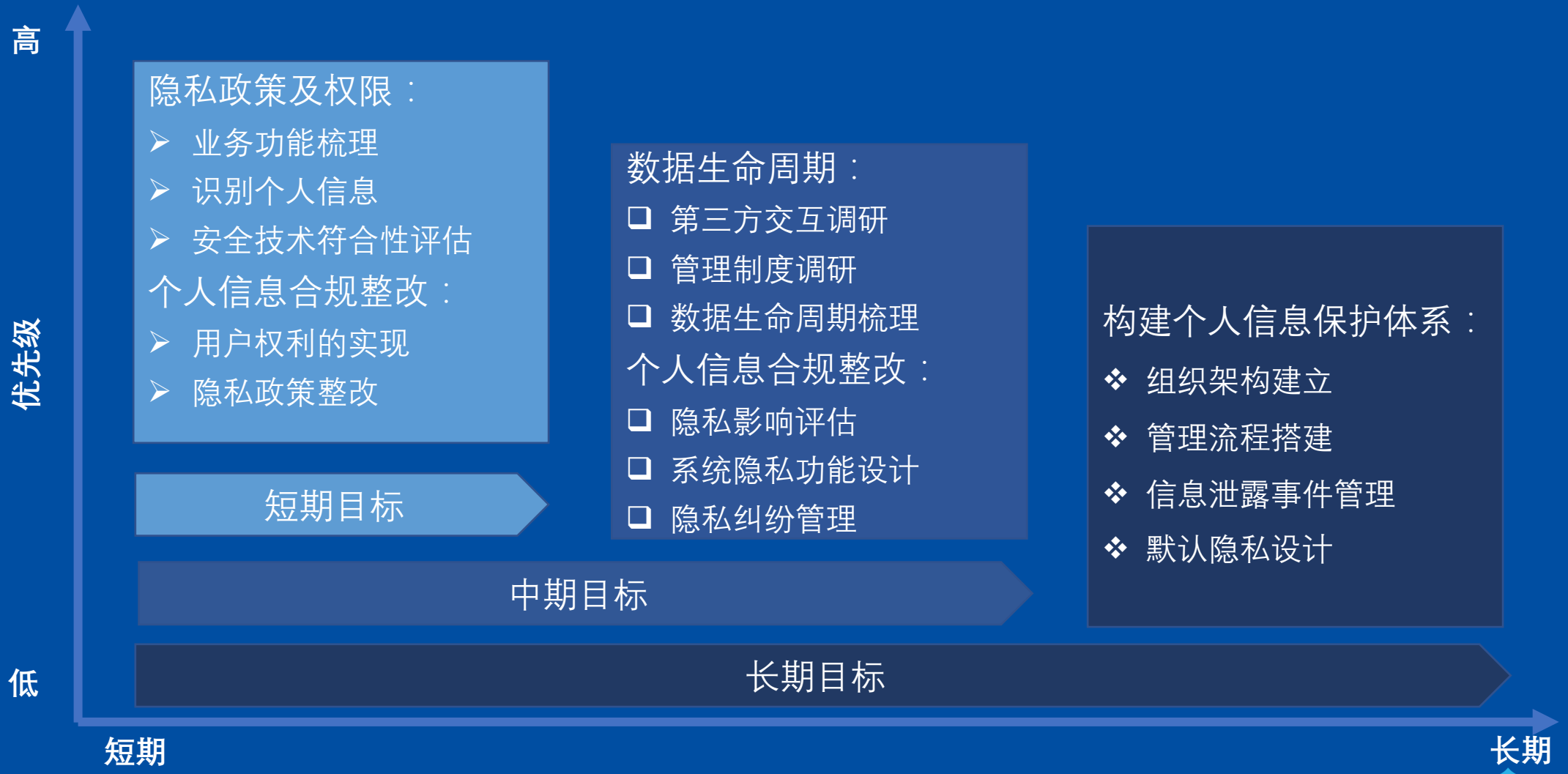
（b）与或可能直接或间接与PII主体相关联的任何信息。

个人信息一旦泄露，将导致个人信息主体及收集、使用个人信息的组织和机构丧失对个人信息的控制能力

一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的个人信息

某些个人信息在被超出授权合理界限时使用（如变更处理目的、扩大处理范围等），可能对个人信息主体权益带来重大风险

02 个人信息保护实施


高
优先级
低
短期
长期
隐私政策及权限：
➢ 业务功能梳理
➢ 识别个人信息
➢ 安全技术符合性评估
个人信息合规整改：
➢ 用户权利的实现
➢ 隐私政策整改
短期目标
数据生命周期：
❑ 第三方交互调研
❑ 管理制度调研
❑ 数据生命周期梳理
个人信息合规整改：
❑ 隐私影响评估
❑ 系统隐私功能设计
❑ 隐私纠纷管理
中期目标
构建个人信息保护体系：
❖ 组织架构建立
❖ 管理流程搭建
❖ 信息泄露事件管理
❖ 默认隐私设计
长期目标

02 个人信息保护工作内容

02 分级矩阵

	机密	秘密	限制	公开
用户数据	PII	用户记录	用户浏览轨迹	
员工数据	工资	密码	除PII外基本信息	经员工同意的奖励信息
公司数据	商业计划，秘钥	核心代码	内网IP分布	公司宣传材料

03 PIMS体系落地

管理层的支持

03 落地过程

安全评估

- 理解业务场景
- 识别个人信息
- 风险评估
- 制定方案

敲定策略

- 方案对比
- 涉及部门交流
- 脑暴意外情况
- 管理层敲定

实施

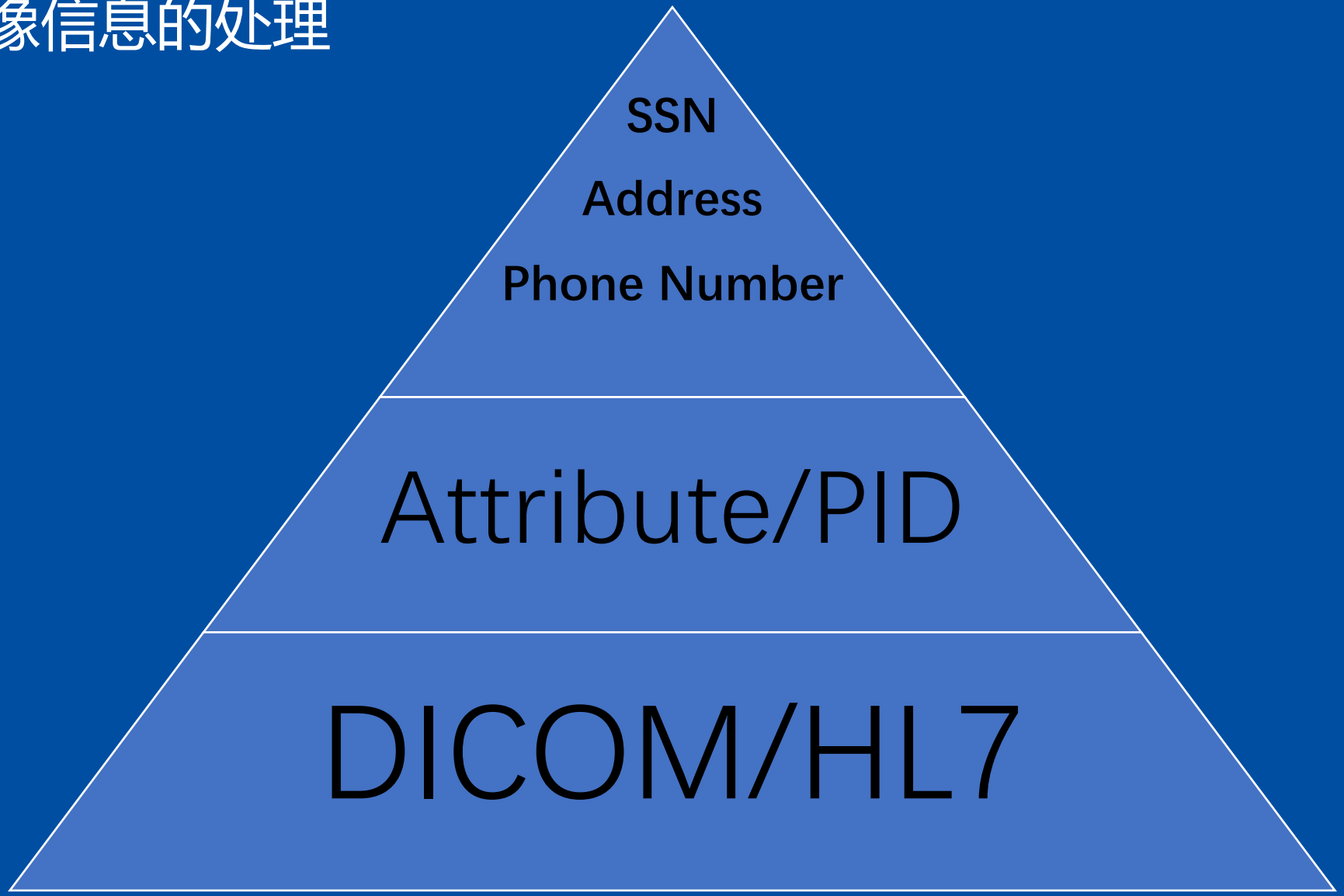
- 确立总协调人/实施负责人
- 方案break down
- 资源分配
- 意外情况处理
- 验收

03 理论指导

管理层的认可

04 敏感数据保护实践

04 影像信息的处理



04 弱密码真的弱吗？

长度>8位

字母+特殊字符

根本记不住

定期修改

禁止明文存放

谢谢观看

THANK YOU