网络安全创新大会
Cyber Security Innovation Summit

个人信息安全影响分析实践分享

钱伟峰　安言 副总经理

目录

- 个人金融信息保护合规要求总览
- 个人信息/隐私影响分析标准简介
- 个人信息安全影响评估实践分享

常见个人信息安全保护合规要求

法律法规

- 网络安全法
- 数据安全法（待颁布）
- 个人信息保护法（待颁布）
- 最高法、最高检关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释
- App违法违规收集使用个人信息行为认定方法
- 关于加强银行卡安全管理预防和打击银行卡犯罪的通知
- 个人信息和重要数据出境安全评估办法（征求意见稿）
- 个人信息出境安全评估办法（征求意见稿）
- ……

行业合规要求

- 银行业金融机构数据治理指引
- 商业银行信息科技风险管理指引
- 银行业金融机构信息科技外包风险监管指引
- 中国人民银行关于进一步加强银行卡风险管理的通知
- ……

标准层面

- GB/T 35273-2020 个人信息安全规范
- GB/T 22239-2019 网络安全等级保护基本要求
- GB/T 39335-2020《信息安全技术 个人信息安全影响评估指南》
- JR/T 0171-2020 个人金融信息保护技术规范
- JR/T 0197-2020 金融数据安全 数据安全分级指南
- GB/Z 28828-2012 信息安全技术公共及商用服务信息系统个人信息保护指南
- ……

个人信息安全部影响评估参考标准

GB/T 39335: 2020

信息安全技术 – 个人信息安全影响评估指南

VS

ISO 29134: 2017

Information technology - Security techniques - Guidelines for privacy impact assessment

ISO 29134 快速解读

确定PIA必要性（阈值分析）阶段

当组织或项目涉及以下情景时，需要开展PIA：

- 开发或处理PII的信息系统进行重大改变时，应该进行PIA；
- 任何新项目的启动都应触发阈值分析，以确定是否需要进行PIA；
- 进行涉及PII资产和处理PII的所有系统的资产清单的建立、维护和更新时，需要参考PIA报告；
- 开发和维护库存时，需要从PIAS中提取关于信息系统处理PII 的信息元素；
- 当组织正在处理PII，组织应该建立进行PIA所需的程序；
- 为确保与PII处理相关的计划和服务符合隐私保护要求，组织应该执行PIA并实施所产生的隐私处理计划；

PIA 准备阶段

设立PIA小组

准备PIA计划并确定执行PIA的资源可用性

描述评估内容

确定评估流程

PIA执行阶段

识别PII

选定PII相关控制

识别现有控制措施

分析现有控制的符合程度

评估PII受侵害后的影响

隐私风险处理准备

PIA跟进阶段

报告编制

风险处理措施设计

实行隐私风险处理计划

PIA结果回顾

何时需要做个人信息安全影响评估

本次介绍的PIA工具适用于：

◆ 合规要求（包括但不限于）：

- ISO/IEC 27701: 2019 隐私信息管理体系
- GB/T 35273: 2020 个人信息安全规范
- ISO/IEC 29151: 2017 个人身份信息保护实践指南

◆ 落地要求：

评估用于保护个人信息主体的各项控制措施的有效性，并根据评估结果改进控制措施，降低各项活动对个人信息主体权益造成的影响。

◆ **触发时机（合规要求）：**

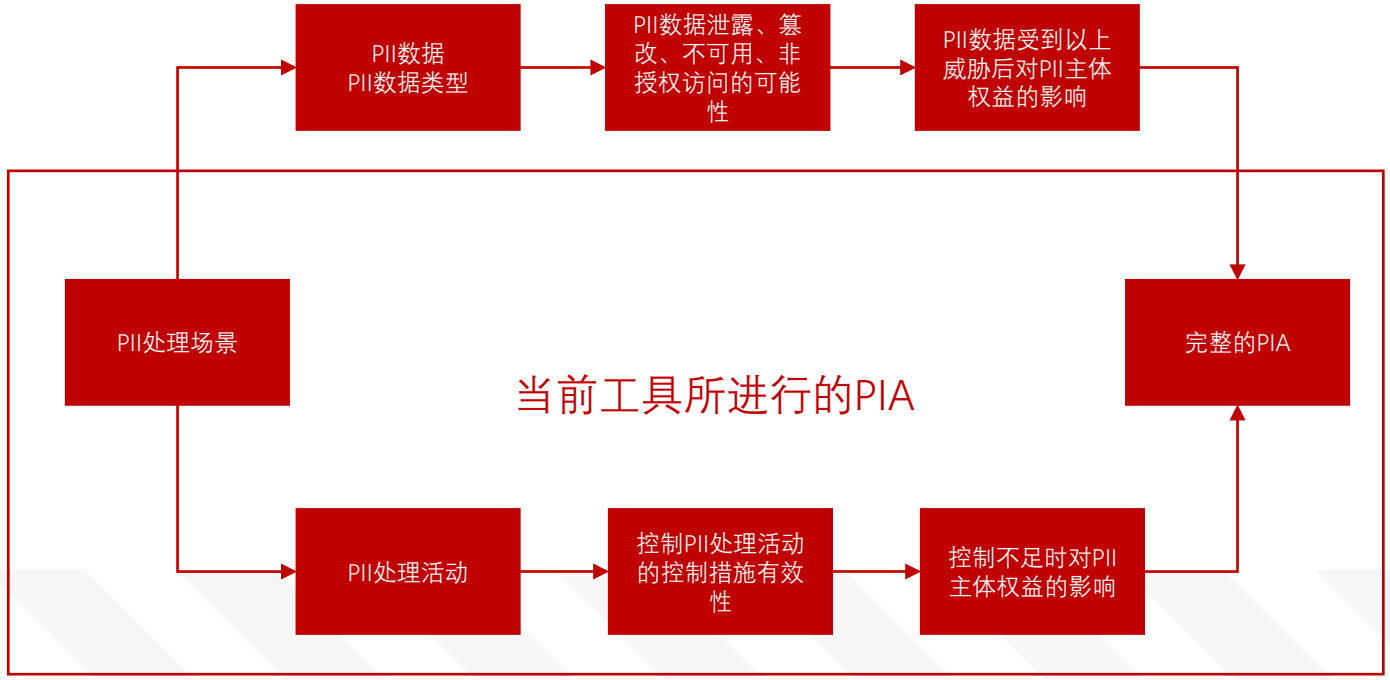
- 每年一次
- PII处理场景新增或发生变更时
- 内外部环境发生变化时
- 当发生重大个人信息安全事件时
- 信息安全领导小组确定有必要时

(*注：不同的合规要求中，对“PII”的命名方式可能不同，实施时需根据实际情况调整)

实施方法与步骤

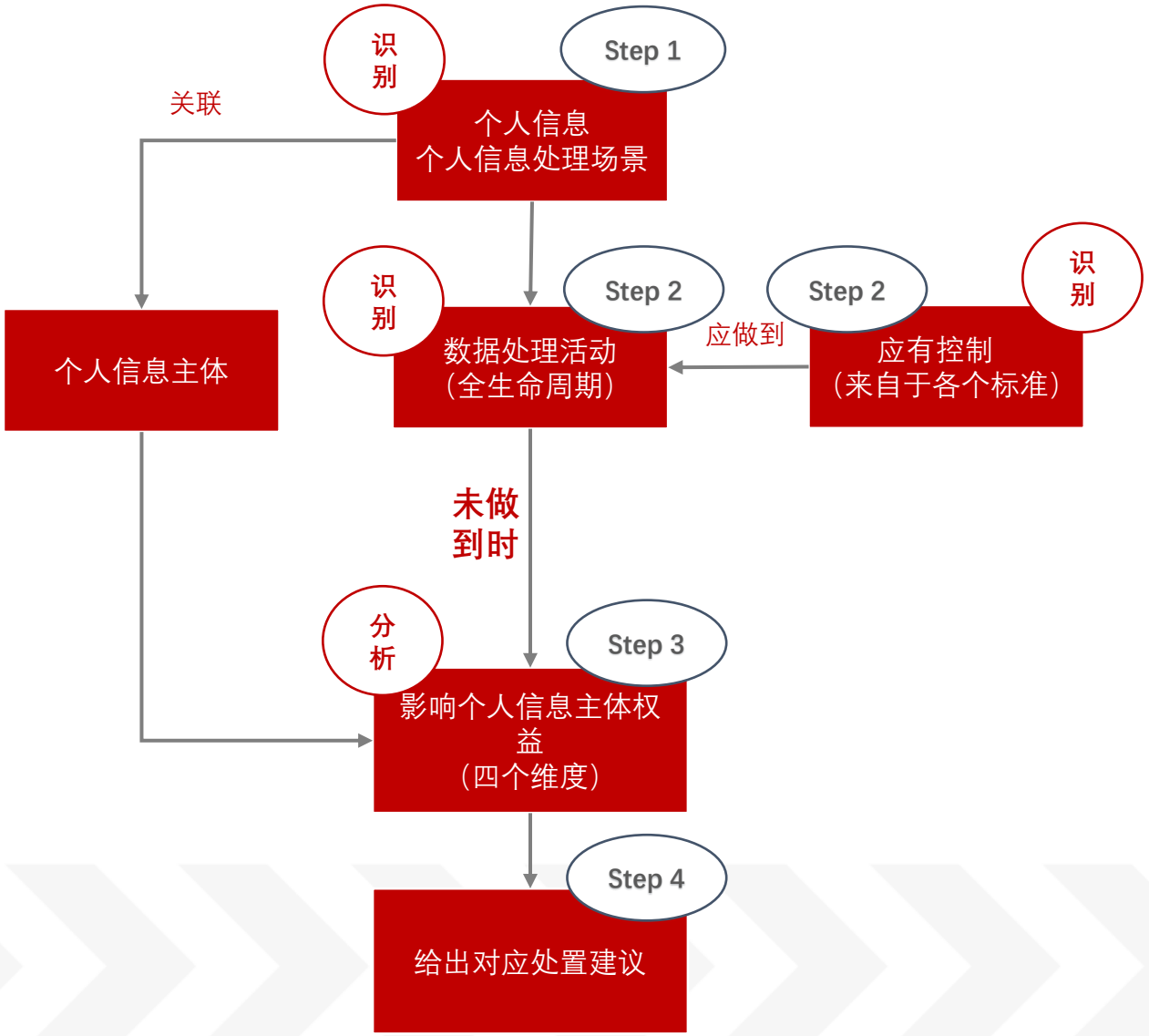
- PIA评估的不再是个人信息（PII数据）本身，而是对个人信息主体（PII主体）权益的影响。
- 在一个完整的PIA中，对PII主体权益的影响有两部分组成：

1. 数据处理活动本身对PII主体权益造成的影响；
2. 数据受泄露、篡改、不可用、非授权访问的威胁时，对PII主体权益造成的影响。



针对PII处理活动，评估用于保护PII主体的各项控制措施的有效性，以判断其对PII主体合法权益造成损害的各种影响。

个人信息安全影响评估方法



- **Step 1：**识别PII处理场景，识别各个场景下的PII字段、数据量、涉及的第三方等，同时分析所对应的PII主体是否存在需特别考虑的群体特征。
- **Step 2：**识别各个PII处理场景下的数据处理活动（收集、存储、传输、使用、第三方交互等）；同时根据各个标准、法律法规、发文要求，识别在各个PII处理活动下应有的控制要求。
- **Step 3：**分析对各个处理活动的控制是否能满足应有控制的要求，如不满足，则对相应的PII主体造成了何种权益影响（四个维度）。
- **Step 4：**针对“对PII主体造成中、高级别影响的处理活动”给出处置建议。

个人信息字段及场景识别

隐私信息基本情况						
编号	数据名称	隐私信息类型	系统-系统模块	所属部门	保有数据量	涉及委托处理、共享、转让的第三方

个人信息字段		是否涉及?	处理场景1	涉及处理活动1	涉及系统1	(可选)处理场景2	(可选)涉及处理活动2	涉及系统2
基本信息	个人姓名							
	生日							
	性别							
	地址							
	手机号							
	电子邮箱							
身份信息	身份证号码							
	社保号码							
	护照号							
	居住证号码							
网络标识	个人网络唯一账号							
	平台互通个人标识号							
	个人IP地址							
	个人数字证书							
	个人唯一设备标识码							
财产信息	交易记录							
	银行账户							
	第三方个人支付识别码							
	征信信息							
通信信息	通话内容（包括即时通讯）							
	通话时间（包括即时通讯）							
	相关通讯录							
偏好行为	Cookies							
	网页浏览记录							
	链接点击记录							
	个人定位信息							
	个人运动信息							
其他信息	*【可自行添加】*							
	【可自行添加】							

基础版—底线要求：梳理客户方PII现状，形成一份PIA报告所必要的PII背景信息。

- 评估对象涉及哪些PII数据?
- 哪些部门/系统/系统模块中使用到了这些数据?
- 保有量分别是多少？（500条以上为入刑标准）
- 是否涉及了第三方处理?

Plus版—数据地图：颗粒度更细，能够形成数据流向图，以符合ISO27701要求，需基于场景调研结果更新工具。

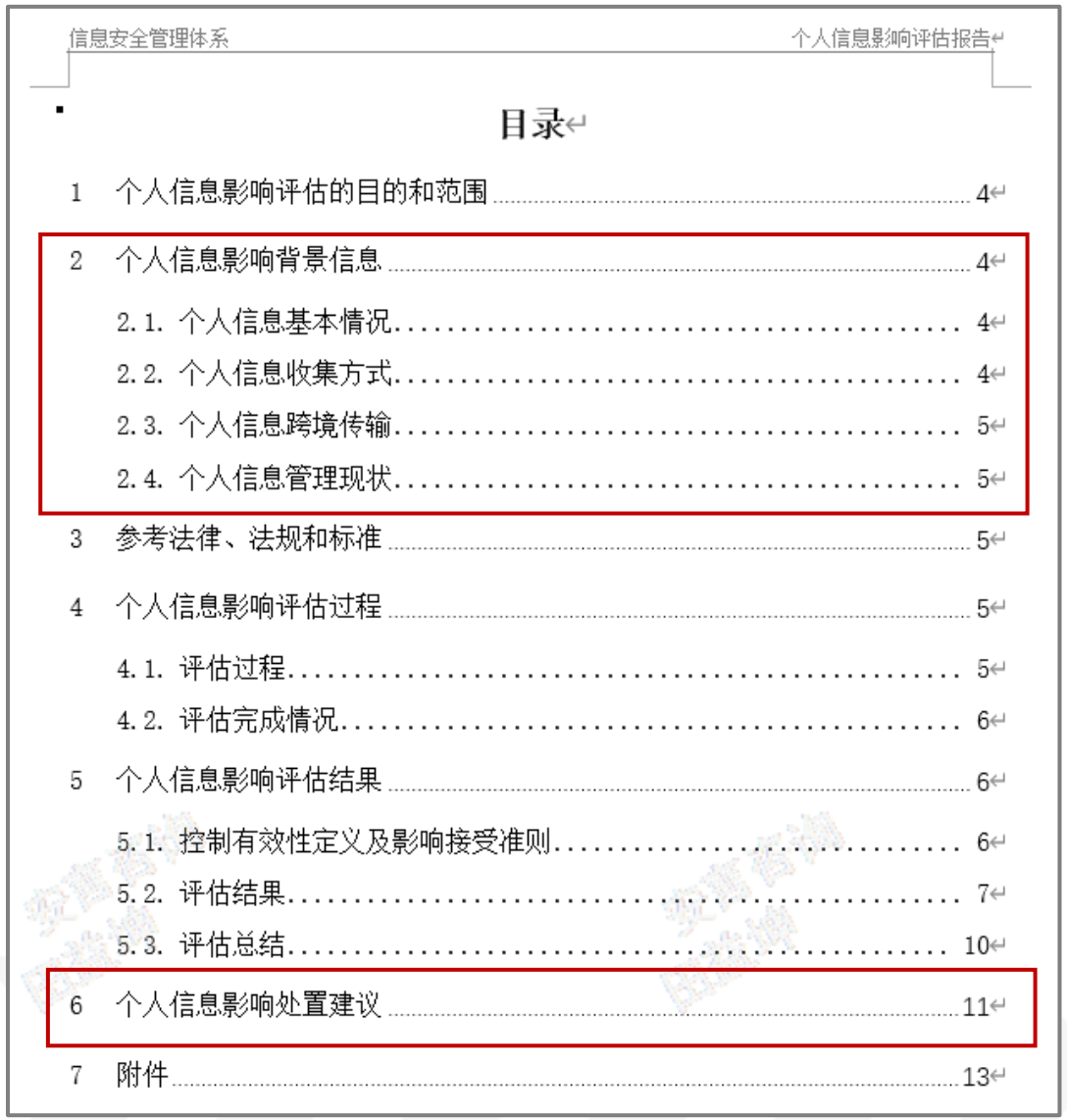
- 涉及的PII字段（参考GB/T 35273梳理）
- 在什么场景下处理了该PII数据?
- 数据上下游?

个人信息影响分析

控制有效等级评价				无控制时PII主体影响分析				影响程度	适用数据活动							
控制项编号	应有控制	现有控制描述（需填写）	控制有效等级（需选择）	影响自主决定权	引发差别性待遇	名誉受损和遭受精神压力	个人财产受损		收集	存储	使用	委托处理	共享	转让	公开披露	删除
CP-001	不应从未知或不正当来源获得隐私信息。	1. 从PII主体处直接获得的隐私信息会勾选/确认隐私协议 2. 从第三方获得的隐私信息待确认签订的协议内容（是否明确了来源或责任）	基本符合	3	3	3	3	低	Y							
CP-002	收集隐私信息时，应通过弹窗等明显方式告知PII主体收集、使用隐私信息规则，并获得PII主体的明示同意。	1. 从***网页端***进行注册时，未进行隐私政策阅读提示和PII主体授权过程，仅能通过主页底部进入隐私政策页面； 2. 通过该方式进行注册时，仅收集手机号和密码； 3. 登录后进行PII补全时，同样不提醒隐私政策阅读与同意授权。	无控制	3	3	1	1	高	Y							
CP-003	当收集个人生物识别信息时，应单独向PII主体告知个人生物识别信息的收集、使用规则，并征得PII主体的明示同意。	公司收集了内部员工的个人生物识别信息（用于考勤、门禁等），当前未明确告知信息主体	无控制	2	3	1	1	高	Y							
CP-004	从第三方获取隐私信息时，第三方应提供PII主体的授权证明。	合同中暂未要求第三方提供相关证明、未明确相关责任	无控制	3	2	3	2	高	Y							
CP-005	向PII主体征得同意时，应确保明确、清晰地告知用户具体的隐私信息处理目的，不存在内容用户难以阅读或理解的情况。	隐私政策中包含收集的内容，且清晰易读	完全符合	3	3	1	1	低	Y							
CP-006	收集的隐私信息类型应与实现产品或服务有直接关联，其类型、范围、频率、数量等不超过系统或业务开展的需要。	隐私政策中：从功能模块出发，列明各个PII处理目的及其需收集的PII及收集的时机	完全符合	3	2	2	1	低	Y							
CP-007	不应通过捆绑产品或服务各项业务功能的方式，要求PII主体一次性接受并授权同意其未申请或使用的业务功能收集隐私信息的请求。	隐私政策中提及的业务功能模块均与快递业务有直接或间接关联	完全符合	3	2	2	3	低	Y							

- **应有控制：**参考各个标准、监管发文、法律法规中整理出在某一数据处理活动中应有的控制，如不涉及某一活动则不需要评定。以《GB/T 35273 个人信息安全规范》为主。
- **有效等级：**根据控制现状进行评定，“基本符合”和“控制不足”的差异主要体现在“是否于客户方或同行业内因此发生过安全事件”。
- **无控制时对PII主体的影响：**当前赋值暂未考虑PII主体群体特征，具有一定主观性。

个人信息安全影响评估的输出与注意事项



信息安全管理体系　　个人信息影响评估报告

目录

1 个人信息影响评估的目的和范围 4
2 个人信息影响背景信息 4
2.1. 个人信息基本情况 4
2.2. 个人信息收集方式 4
2.3. 个人信息跨境传输 5
2.4. 个人信息管理现状 5
3 参考法律、法规和标准 5
4 个人信息影响评估过程 5
4.1. 评估过程 5
4.2. 评估完成情况 6
5 个人信息影响评估结果 6
5.1. 控制有效性定义及影响接受准则 6
5.2. 评估结果 7
5.3. 评估总结 10
6 个人信息影响处置建议 11
7 附件 13

- 进行PIA需形成报告，以作为PIA的结果。
- 《PIA报告》可参考《风险评估报告》进行，其中较为重要的两部分为“PII背景信息”和“PIA处置建议”。

PII背景信息：

- 厘清客户方PII的处理现状和管理现状，作为评估的输入项之一，同时告知客户方应倾斜的管理资源。

PIA处置建议：

- 针对“高”和“中”等级影响给出处置建议（某些情况下，即时“控制不足”也只会造成“低”等级影响）。

网络安全创新大会
Cyber Security Innovation Summit

THANKS

安言咨询公众号