



Personal Information Protection Assessment (PIPA)

企業個人情報安全管理システムの構築

2018年7月

中国软件行业协会(CSIA)

1

背景紹介

2

PIPA概要

3

管理システム建設

4

評価と管理

1

背景紹介

2

PIPA概要

3

管理システム建設

4

評価と管理

個人情報とは

法律と標準の定義



出处	条款内容
2017-3月最高法 法释[2017]10号文件 解释： 刑法第二百五十三条	公民个人信息： 是指以电子或者其他方式记录的能够单独或者与其他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，包括姓名、身份证件号码、通信通讯联系方式、住址、帐号密码、财产状况、行踪轨迹等。
《中华人民共和国网络安全法》	个人信息，是指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自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。
GB/T 35273-2017 《信息安全技术 个人信息安全规范》	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。
T/SIA 001-2017 《企业个人信息安全管理规范》	个人信息：与特定个人相关、能够单独或参照其他相关信息识别该特定个人的各种信息。
DB21/T 1628 《信息安全 个人信息保护规范》系列	个人信息：依附于个人，并可描述个人基本形态的信息，包括： a)可通过视觉、听觉、触觉等感官直接识别个人的信息，如数字、文字、图像、影像、声音等； b)可借助各种手段间接识别个人的信息，如与个人相关各种信息对照、参考、分析等。

個人情報とは

法律と標準の定義



- 基本信息：姓名、性别、年龄、地址、电话、工作单位、职务等常用的个人信息；
- 私密信息：信用卡号、身份证号、银行卡号、密码等；
- 特殊信息：指纹、虹膜、录像、X光片、CD片、DNA、血型等；
- 隐私信息：犯罪史、婚姻状况、宗教信仰、情史、疾病等信息；
- 衍生信息：根据活动和行为分析出的取向、嗜好、位置等信息。

個人情報の唯一の属性：個人主体の私有性

個人情報とは

法律と標準の定義



◆ 知情权:

个人信息主体的知情权包括:

- a) 个人信息主体有权知悉个人信息处理的目的、方式、范围等相关信息;
- b) 个人信息主体有权查看与之相关的个人信息;
- c) 个人信息主体有权知悉个人信息的保护措施;
- d) 个人信息主体有权知悉个人信息的管理质量;
- e) 个人信息主体有权知悉个人信息的转移情况。



◆支配权

个人信息主体的支配权包括：

- a) 个人信息主体有权对是否提供个人信息做出选择；
- b) 个人信息主体有权修改、删除、完善与之相关的个人信息，以保证个人信息的完整、准确和最新状态；
- c) 个人信息主体有权在技术可行的条件下获取其个人信息副本；
- d) 个人信息主体有权决定如何使用与之相关的个人信息。



◆ 质疑权

个人信息主体的质疑权包括：

- a) 个人信息主体有权质疑或反对与之相关的个人信息处理目的、方式、范围等；
- b) 个人信息主体有权质疑个人信息保护措施；
- c) 个人信息主体有权质疑个人信息的管理质量；
- d) 如果个人信息处理目的、方式违背了个人信息主体意愿且无其他正当理由，个人信息主体有权要求企业停止相关的个人信息处理活动或要求销毁相关的个人信息。

国内個人情報安全状況

漏洩、盗み取り事件はしばしば発生する



- 中国互联网协会发布《中国网民权益保护调查报告（2016）》显示，2016年，有**37%**的网民因收到各类诈骗信息而遭受经济损失，全国网民因权益被侵犯造成的经济损失人均为**133元**，总体经济损失约**915亿元**，**9%**的网民近一年来由于各类权益侵害造成的经济损失在**1000元**以上，每个网民平均时间损失**3.6小时**。**54%**的网民认为个人信息泄露严重，其中**21%**的网民认为非常严重；**84%**的网民亲身感受到个人信息泄露带来的不良影响。

凯越酒店大量访客信用卡信息泄露

小米
800万
用户数据泄露

快递官网遭入侵，
1400万条用户信息被转卖



国内個人情報安全状況

漏洩、盗み取り事件がしばしば発生する



- 2018年3月16日，脸书（Facebook）被曝有超过**5000万**名用户（接近Facebook美国活跃用户总数的三分之一，美国选民人数的四分之一）资料遭“剑桥分析”公司非法用来发送政治广告，部分媒体将其视为 Facebook 有史以来遭遇的最大型数据泄露事件。
- 据华尔街日报报道，谷歌（Google）长期允许第三方企业借助软件甚至人工读取用户电子邮件内容，涉及用户数以**百万**计，那些企业向用户提供关联谷歌邮箱的服务，涉及购物比价、旅游规划和邮件管理等。谷歌明知那些企业阅读用户邮件内容却疏于管理。

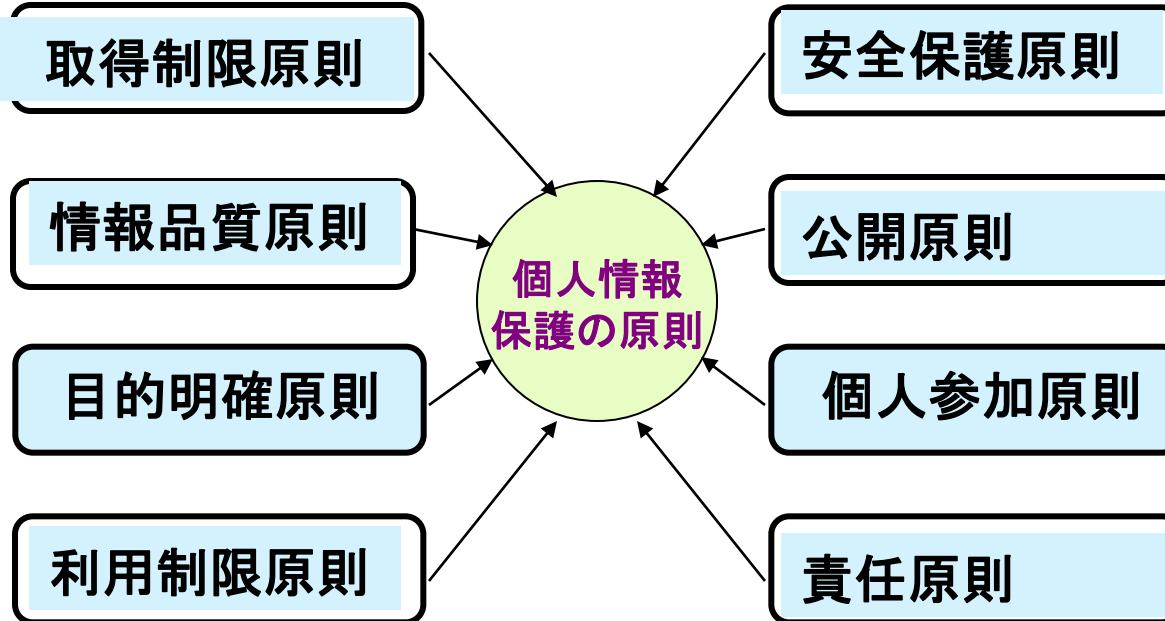


個人情報安全保護の世界共通の遵守の基本基準

OECD 八つ原則



OECD: 经济合作与发展组织 (Organization for Economic Co-operation and Development), 简称经合组织 (OECD), 是由34个市场经济国家组成的政府间国际经济组织, 成立于1961年, 目前成员国总数34个, 总部设在巴黎



OECDは1980年に公布された「プライバシー保護と個人データ超国流通指導原則」における個人情報保護に関する八つ原則

EU史上最高の個人情報保護法案

EUのGDPR



- 欧洲议会2016年4月27日投票通过《通用数据保护条例》（GDPR）并于2018年5月25日起实施。
- GDPR不仅仅是《欧盟数据保护指南》的范围扩大版，它还是总体上更为严苛的法规，包含更严厉的违规处罚。
- 非欧盟成员国的公司(包括免费服务)只要满足下列两个条件之一，就受到GDPR的管辖：
 - (1) 为了向欧盟境内可识别的自然人提供商品和服务而收集、处理他们的信息；
 - (2) 为了监控欧盟境内可识别的自然人的活动而收集、处理他们的信息。



EU個人情報保護の発展の流れ

EUのGDPR



- 根据通用数据保护条例，所有企业都必须删除已收集的用户数据。罚款标准：
- 一般违规行政罚款的上限是1000万欧元或该企业上一财年全球年度营业总额的2% (以较高者为准)；
- 严重违规行政罚款的上限是2000万欧元或该企业上一财年全球年度营业总额的4% (以较高者为准)”。
- 这个条例将对中国企业的移动应用安全，以及数据收集、处理和交易产生重大影响。

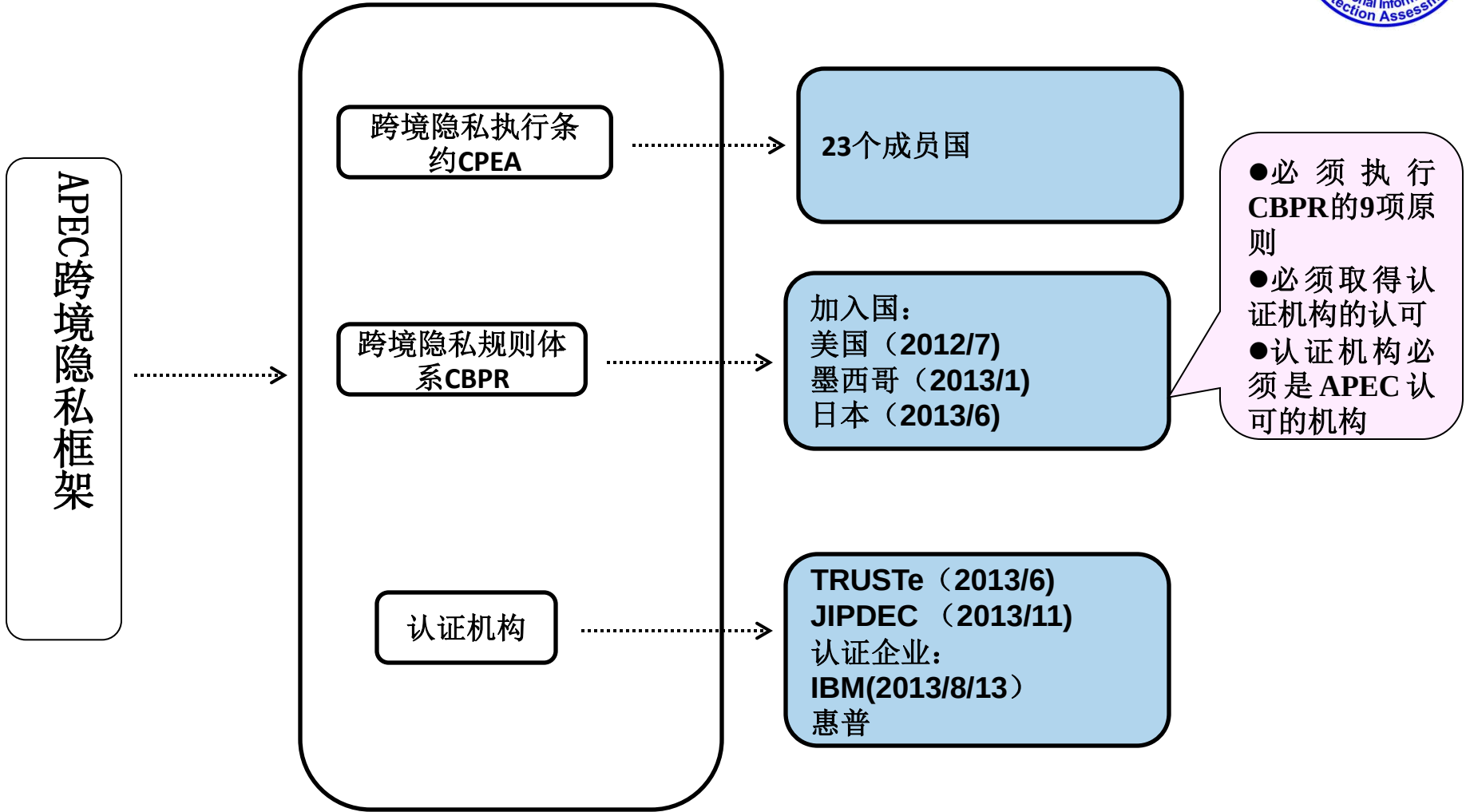
EU個人情報保護の発展の流れ

EUのGDPR——例



- 2018年5月25日，欧盟的通用数据保护条例（GDPR）出台第一天，就迎面痛击美国两大科技巨头脸书、谷歌，控诉它们收集用户私人数据，并欲给脸书和谷歌分别开出**39亿欧元**（约合人民币290亿元）和**37亿欧元**（约合人民币276亿元）的天价罚单。
- 目前，脸书及其旗下的两个社交平台Insagram和WhatsApp均受到指控，而谷歌也因安卓系统非法收集用户信息而被控诉。两家公司均称他们现在已根据GDPR的要求做出了相应的调整，出台了新的措施和产品。

アジア太平洋経済共同組織APEC国境 プライバシー体系(CBPR)





➤2005年，日本发布实施《个人信息保护法》，与《行政机关保有的个人信息保护法》、《信息公开、个人信息审查会设置法》、《独立行政法人等保有的个人信息保护法》、《伴随（行政机关保有的个人信息保护法）等的施行而整理相关法律的法律》等共同构成了日本的个人信息保护法律体系。

➤2017年5月30日，2015年日本发布的《个人信息保护法》修正案全面实施，日本的个人信息保护规则发生重大变化，按照国际惯例修改增加相关款项，变得更严格。



修正后主要的核心内容包括：

1、敏感的个人信息。参照欧美国家敏感的个人信息的界定标准及范围，将敏感信息限定在有关种族、信仰、社会地位、病史、犯罪记录、受害历史，以及其它可能引起社会歧视的信息，包括身体、智力和精神残疾以及体检结果等有限的范围内。收集敏感的个人信息时，必须得到个人的明确同意。

2、匿名个人信息处理。个人信息匿名化处理，删除可识别个人的相关信息，并不能复原。匿名处理的个人信息可提供第三方，但必须遵循相关规则。

3、向第三方提供。可以向第三方（包括日本以外的母公司或附属公司（affiliated company）和/或外包商等）提供个人信息，但需本人明示同意，或数据转移协议或适用于所有集团公司的政策规则。

4、记录保留义务。向第三方传输数据的记录必须保留，包括转让日期、受让人的姓名、可能识别个人的姓名和其他信息、提供或收到的个人信息项目、已获得个人同意的事实（基于个人同意的转让）等。但如果受让人位于日本境内，则不需要此类记录。从第三方收到的个人信息同样需要做类似记录。

5、退出同意。如果事先已经通知个人或在个人可以轻松访问的位置发布通知，则无需取得个人的明示同意，组织即可以向第三方提供个人信息。通知必须包含以下信息：（i）信息的使用目的之一为向第三方转让；（ii）要转让给第三方的项目；（iii）转让信息的方式；（iv）要求停止转让资料的权利（即退出权）；（v）个人如何就选择退出这一问题与转让方进行沟通。

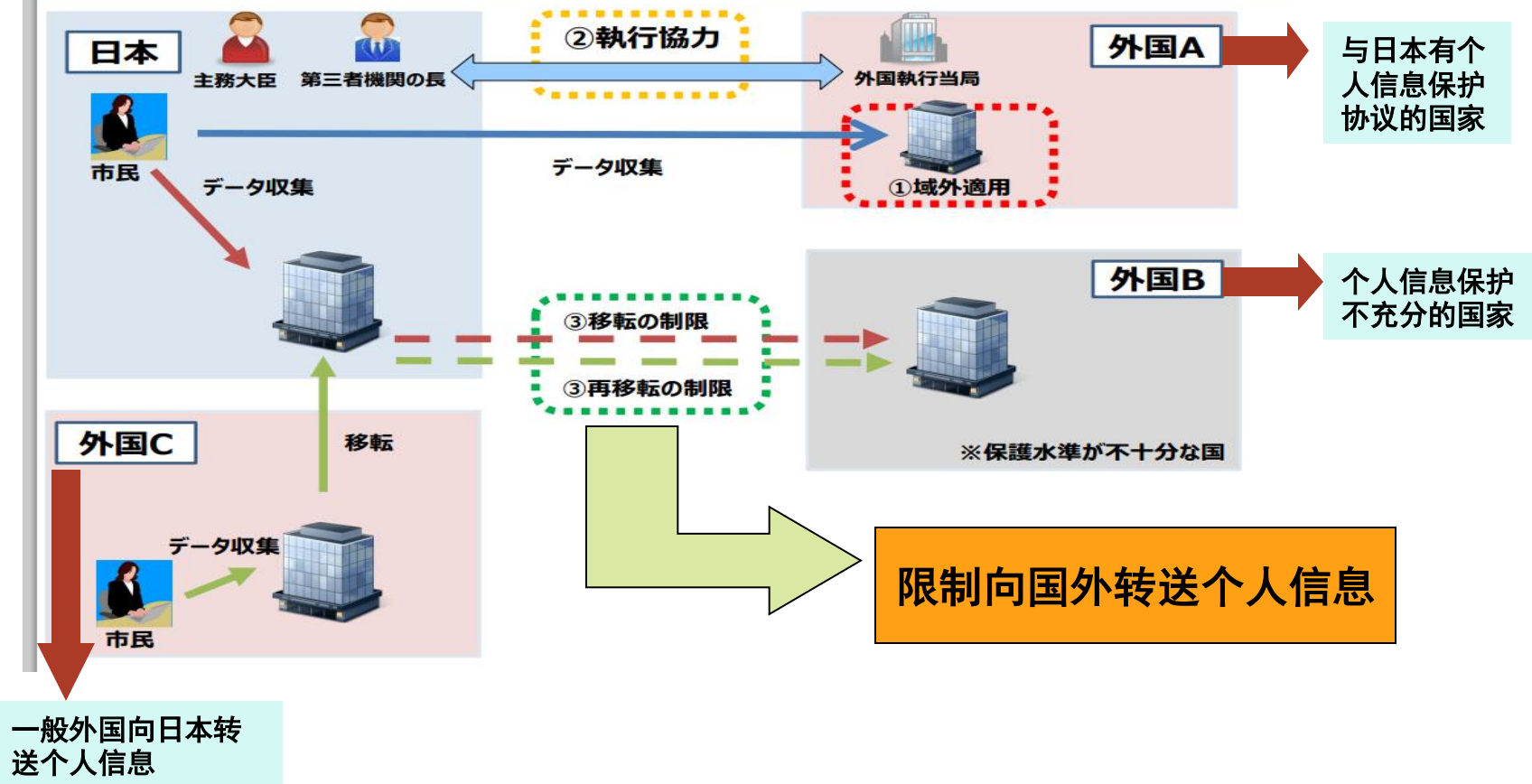
6、个人信息保护委员会。是修正案新增的第五章，主要规定了个人信息保护委员会的设置、所属、任务、管辖事务、组织、委员任期、委员身份保障和罢免、议事方式、所辖事务局、委员义务等。特别是个人信息保护委员会直属日本内阁总理大臣管辖，独立行使职权，地位相当高。

日本個人情報保護法



実現すべき事項

6



中国個人情報安全基準の確立の流れ



大連ソフトウェア及び情報サービス業
個人情報保護規範
2007.2.5

ソフトウェア及び情報サービス業
個人情報保護規範
(DB21/T 1522-2007)
2007.6.13

情報セキュリティ個人情報保護規範
(DB21/T 1628.1-2012)-2012.3.7

信息安全技術公共および商用サービス
情報システム個人情報保護ガイド
(GB/Z 28828-2012)-2012.11.5

情報技術サービスアウトソーシング
第2部: データ(情報)保護規範
(SJ/T 11445.2-2012)-2012.12.28

2006年

2007年

2008年

2012年

2015~2017年

大連ソフトウェア
及び情報
サービス業
個人情報保護規範
(試用版)
2006.4.1

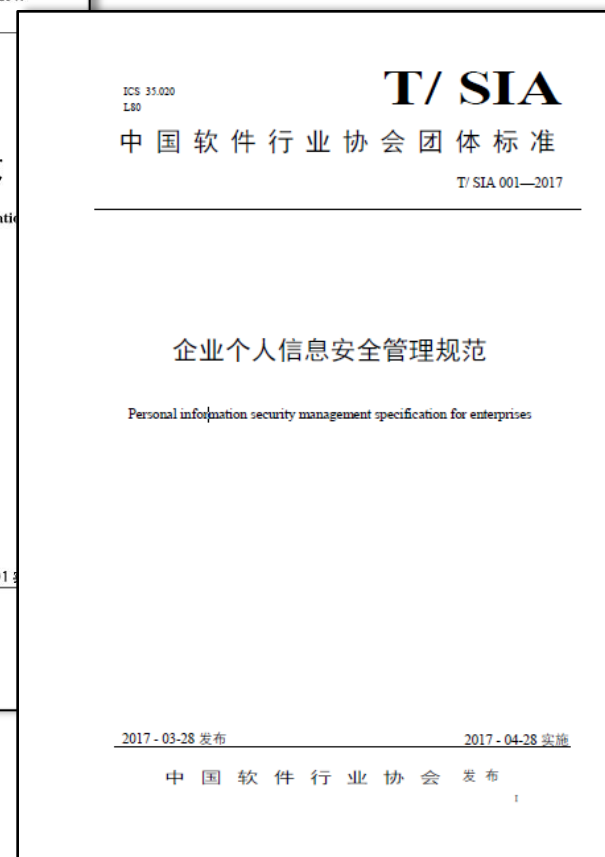
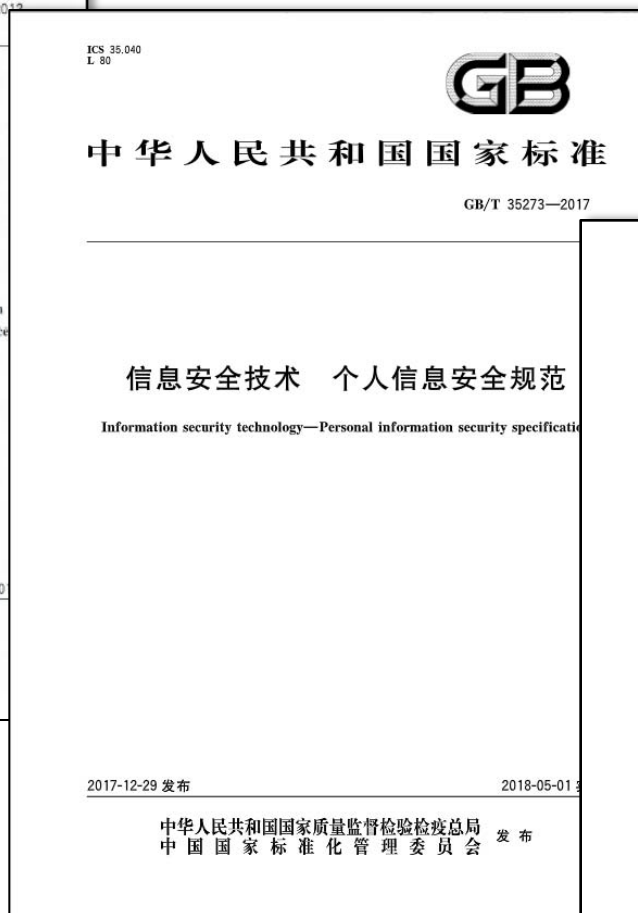
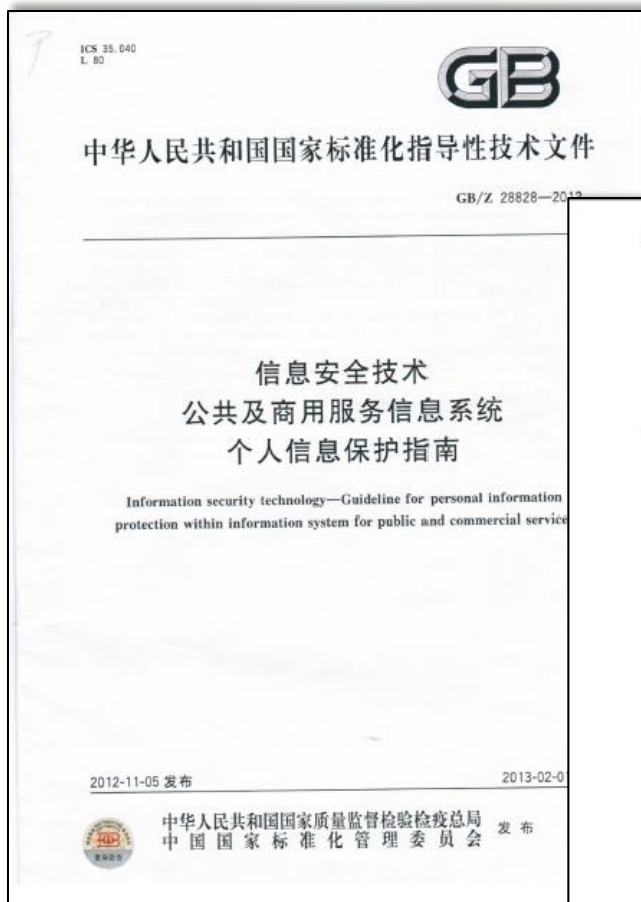
個人情報保護規範
(DB21/T 1628-2008)
2008.6.16

信息安全技術個人情報安全規範
(GB/T 35273-2017)

企業個人情報安全管理規範
(T/SIA 001-2017)

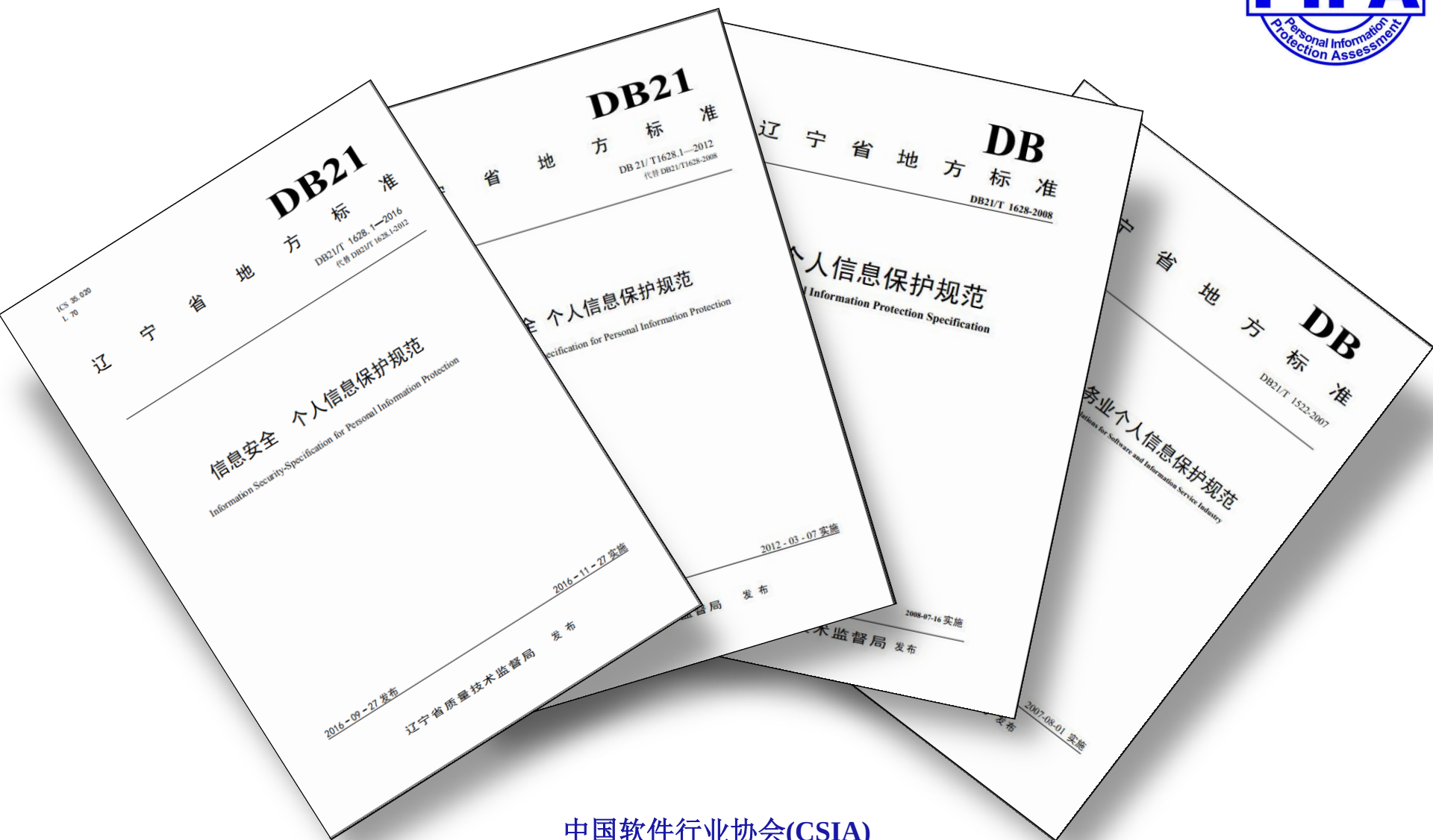
個人情報保護標準シリーズ(8部分)
個人情報安全管理システム評価シリーズ(11部分)

中国個人情報保護の基準



中国软件行业协会(CSIA)

地方における個人情報保護基準の流れ



個人情報保護標準シリーズ（8部分）



1

信息安全 个人信息保护规范(DB21/T 1628.1-2016)

2

信息安全 个人信息安全管理体系实施指南(DB21/T 1628.2-2013)

3

信息安全 个人信息数据库管理指南(DB21/T 1628.3-2016)

4

信息安全 个人信息管理文档管理指南(DB21/T 1628.4-2018)

5

信息安全 个人信息安全风险管理体系实施指南(DB21/T 1628.5-2014)

6

信息安全 个人信息安全管理体系安全技术实施指南
(DB21/T 1628.6-2018)

7

信息安全 个人信息安全管理体系内审实施指南(DB21/T
1628.7-2018)

8

信息安全 个人信息安全管理体系过程管理指南(DB21/T
1628.8-2018)

個人情報安全管理システム評価シリーズ（11部分）



1

信息安全 个人信息安全管理体系评价 要求

信息安全 个人信息安全管理体系评价 评价管理指南

3

信息安全 个人信息安全管理体系评价 评价员管理

信息安全 个人信息安全管理体系评价 评价指标

5

信息安全 个人信息安全管理体系评价 评价方法

信息安全 个人信息安全管理体系评价 资格审查

7

信息安全 个人信息安全管理体系评价 现场管理

信息安全 个人信息安全管理体系评价 保证方法

9

信息安全 个人信息安全管理体系评价 仲裁指南

信息安全 个人信息安全管理体系评价 审批指南

11

信息安全 个人信息安全管理体系评价 资格管理

2

4

6

8

10

中国個人情報保護立法の流れ

中国個人情報保護法の現状

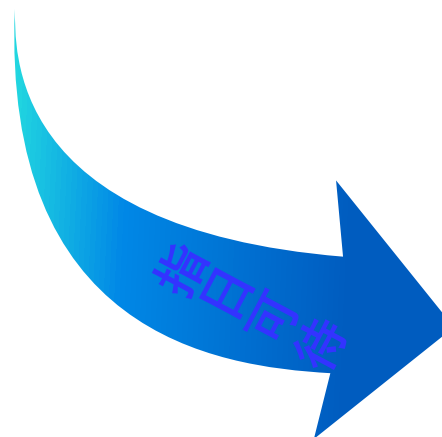


没有专门的个人信息保护法

03年起草《个人信息保护法》

05年提交国务院

2017年6月1日，
《中华人民共和国网络安全法》
正式实施



中华人民共和国
个人信息保护法

中国個人情報保護立法の流れ

個人情報に関連する法規の条項は以下の関連法律、法規の中で：



- 中华人民共和国宪法(33、38、51条)
- 中华人民共和国民法通则（99、100、101、103条）
- 中华人民共和国妇女权益保障法（42条）
- 中华人民共和国未成年人保护法（39条）
- 中华人民共和国邮政法（4、6条）
- 收养法（22条）
- 商业银行法（29条）
- 民事诉讼法
- 艾滋病监测管理的若干规定（21条）
- 互联网电子公告服务管理规定（12条、19条）
- 互联网电子邮件服务管理办法（9条）
- 医务人员医德规范及实施办法（5条）
- 中华人民共和国传染病防治法（68条）
- 中华人民共和国商业银行法（6条）
- 中华人民共和国母子保健法（34条）
- 中华人民共和国统计法（14、30条）
- 个人存款账户实名制规定（8条）
- 中华人民共和国计算机信息网络国际联网管理暂行规定实施办法（18条）
- 最高人民法院关于审理名誉权案件若干问题的解释（4条）
- 互联网电子邮件服务管理办法（3、9、13、15条）
- 《中华人民共和国网络安全法》（6、9、10、11、12、19、20、21、22、27、37、38、40、41、42、43、44、45、49、76条）

《中華人民共和国ネットワーク安全法》



- 2017年6月1日，《中华人民共和国网络安全法》正式实施。
- 《中华人民共和国网络安全法》是我国网络安全专门性基础法律，规范了基于网络的、与个人信息相关的行为、活动。是涉及个人信息保护条款最多的法律。
- 《中华人民共和国网络安全法》与个人信息安全相关条款有20条。

《中華人民共和国ネットワーク安全法》



- 《网络安全法》第22条第2款规定：“网络产品、服务具有收集用户信息功能的，其提供者应当向用户明示并取得同意；涉及用户个人信息的，还应当遵守本法和有关法律、行政法规关于个人信息保护的规定。”
- 《网络安全法》第42条规定：“网络运营者应当采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失。在发生或者可能发生个人信息泄露、毁损、丢失的情况时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。”
- 《网络安全法》第43条规定：“个人发现网络运营者违反法律、行政法规的规定或者双方的约定收集、使用其个人信息的，有权要求网络运营者删除其个人信息；发现网络运营者收集、存储的其个人信息有错误的，有权要求网络运营者予以更正。网络运营者应当采取措施予以删除或者更正。”

《中華人民共和国ネットワーク安全法》



➤ 《网络安全法》第54条规定：“网络运营者违反本法规定，侵害公民个人信息依法得到保护的权利的，由有关主管部门责令改正，可以根据情节单处或者并处警告、没收违法所得、处违法所得**一倍以上十倍以下**罚款，没有违法所得的，处**五十万元**以下罚款；情节严重的，可以责令暂停相关业务、停业整顿、关闭网站、撤销相关业务许可或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处**一万元以上十万元以下**罚款。”

违反本法规定，窃取或者以其他方式非法获取、出售或者非法向他人提供公民个人信息，尚不构成犯罪的，由公安机关没收违法所得，并处违法所得**一倍以上十倍以下**罚款，没有违法所得的，处**五十万元**以下罚款。”

中国は法律によると個人情報の安全な実施を開始する



2017年8月 “中央网信办、工信部、公安部、国家标准委等四部门组成的专家工作组结束对首批10款网络产品和服务的隐私条款评审。其后，淘宝、支付宝、京东、百度等互联网企业密集修改“隐私条款”，个人信息保护走向规范化。

支付宝隐私权政策

协议更新

【敬请阅读】亲，服务协议有更新哦！

协议中有对您权利义务特别约定以及管辖约定等重要条款，我们已以粗体下划线的读哦！

【特别提示】如您继续使用我们的服务，表示您已充分阅读、理解并接受协议的结果您有任何疑问，可向平台客服咨询。如您不同意协议中任何条款，您应立即停止

《淘宝平台服

《支付宝服务

《法律声明及

《京东隐私政策》更新

尊敬的京东用户：我们对《京东隐私政策》进行了更新。本次更新我们做出了诸多有利息的调整；明确了我们的产品与/或服务收集、使用及共享个人信息的类型方式和用途；时提示的方式在收集、使用及共享个人信息时给予用户明示选择权，并在产品设置中允授权。明确了用户查询、更正和删除其个人信息的方式。增加了用户账户的锁定/解锁供给了用户了30日注销后悔期。

【特别提示】

请仔细阅读《京东隐私政策》（尤其是加粗划线的内容）并确定了解我们对您个人信息的处理规则。任何疑问，可联系我们的客服咨询，如您不同意协议中的任何条款，您应立即停止访问京东。阅读协议不同意相关协议或其中任何条款约定，您应立即停止使用京东。

概述

我们如何使用Cookie、Beacon、Proxy等技术

我们如何使用个人信息

您如何访问和控制自己的个人信息

未成年人隐私权特别约定

本政策中关键词说明

我们如何收集个人信息

我们如何存储和保护个人信息

我们如何共享、转让和公开披露个人信息

对第三方责任的声明

本政策的适用及修订

本版发布日期：2017年8月23日

2017年9月22日

b)如您使用百度地图团购、酒旅、票务服务时，我们会收集您的订单信息（如您选定的酒店、住宿时间、选定的商家和影院）、身份和设备信息、交易状态、联系方式，您授权我们将该信息提供给为您提供服务的第三方，并授权我们间接向第三方获取相关信息，用以与第三方确认您的订单，为您提供相关服务，并为您提供查询及客户服务。

我知道了

中国软件行业协会(CSIA)

法律と標準的な関係

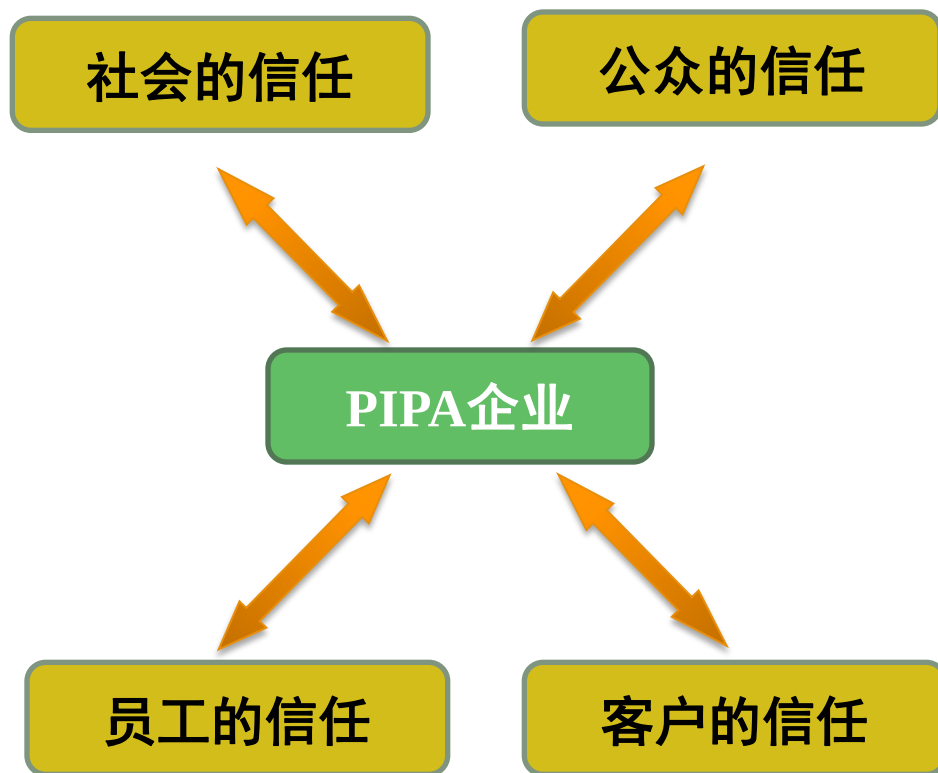
法律と標準の相互援助



- 法律与标准是内涵不同的2个层次，法律与标准之间不存在匹配，可以互为救济。在法律框架下统一行业自律标准，约束标准化过程，将标准的技术性规范与法律关系主体的法律责任和法律义务统一融合：立法强制、救济；标准弥补立法不足，提供技术支撑，约束自我管理、自我调节，实现标准与法律的互为救济。
- 法律救济是法律关系主体的合法权益受到侵犯并造成损害时，获得恢复和补救的法律制度。标准与法律的互为救济，是在标准框架内的行业自律机制遇到法律瓶颈时寻求法律的支撑；相关法律在实施过程中可能出现的边界效应，亦需要标准的填充和补救。

企業個人情報安全管理體系によって確立の意味

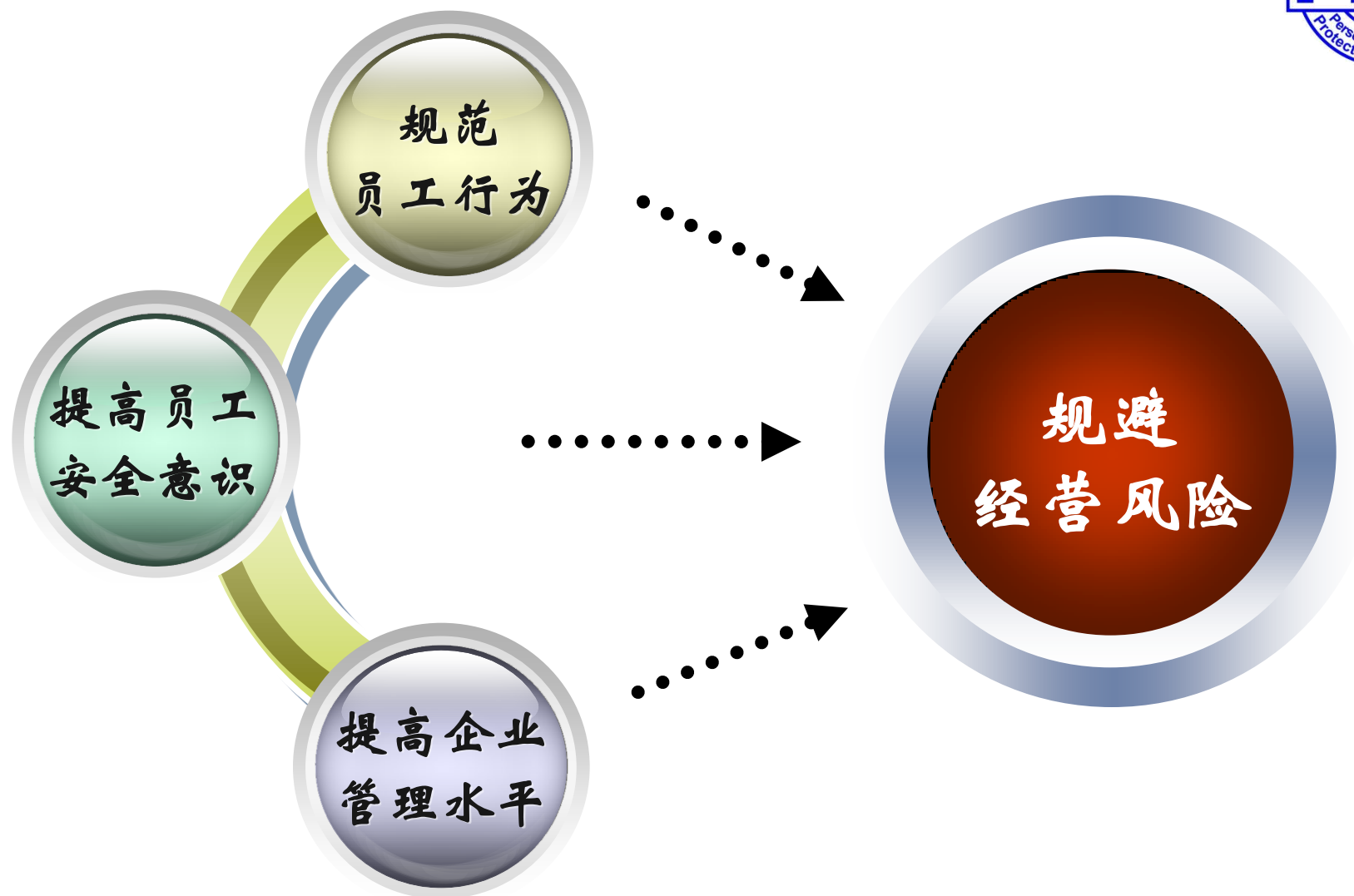
その一つ：企業の信用システムの確立に役立つ



- 提高个人信息保护意识
- 加强规范化管理
- 提高安全管理级别
- 提高企业信誉度
- 增强企业竞争力
- 争取到更多的潜在用户
- 从而持续提高企业经济效益

企業個人情報安全管理體系によって確立の意味

その二つ：企業のリスク回避に役立つ



企業個人情報安全管理體系によって確立の意味



その三つ：企業が国際協力能力を高め、国際的な信頼を得ることができる

欧盟、OECD、美国、日本、韩国等国际合作组织和国家在个人信息保护方面的法律、法规、标准和认证制度已经对我国的对外贸易造成影响。是否实行个人信息保护已经成为开展国际交流与合作的一个前提条件。

目前已有七十多个国家和地区建立了个人信息保护相关的法律、标准：



瑞典《个人数据法》



日本《个人信息保护法》



德国《联邦数据保护法》



法国《数据处理、档案与自由法》



韩国《个人信息保护法》



新加坡《个人信息保护法令》



加拿大《隐私保护法》



英国《数据保护法》



美国《隐私权法》
美国颁布《电子通讯隐私法》
美国政府公布《互联网保护个人隐私的政策》

1

背景紹介

2

PIPA概要

3

管理システム建設

4

評価と管理

PIPA発展の流れ



- 大連ソフトウェア業界協会は、2004年8月から国際個人情報保護状況や中国のソフトウェア及び情報サービス業の影響を注目し、研究し始めた。
- 2005年8月に専門機関を設立し、個人情報保護基準を作成。
- 2006年5月にPIPA評価システムを設立。
- 現在全国で評価されている企業は109社。



PIPA発展流れ

政府の強力な支持



- **大连市政府**
 - 立法工作启动
 - 设专项资金支持PIPA
- **辽宁省信息产业厅**
 - 批准省标准
 - 全省推广PIPA
- **工信部**
 - 委托编制国家《个人信息保护规范》
 - 2009年国家软件及信息服务业个人信息保护试点城市

09年被工信部授予

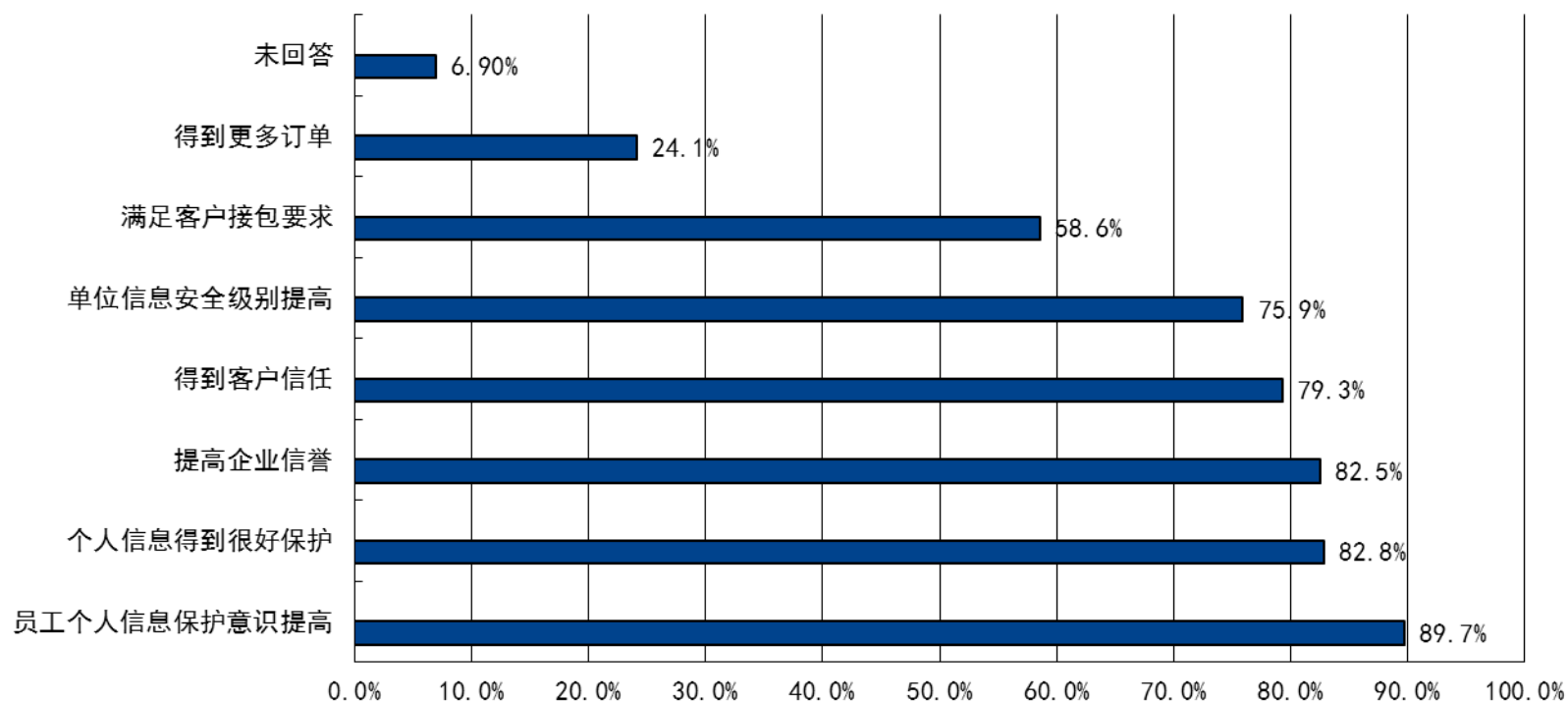
《软件及信息服务业个人信息保护试点城市》



PIPAに対する企業の認可



通过PIPA后对企业产生的实际效果



DSIA对PIPA企业的问卷调查报告

PIPA紹介

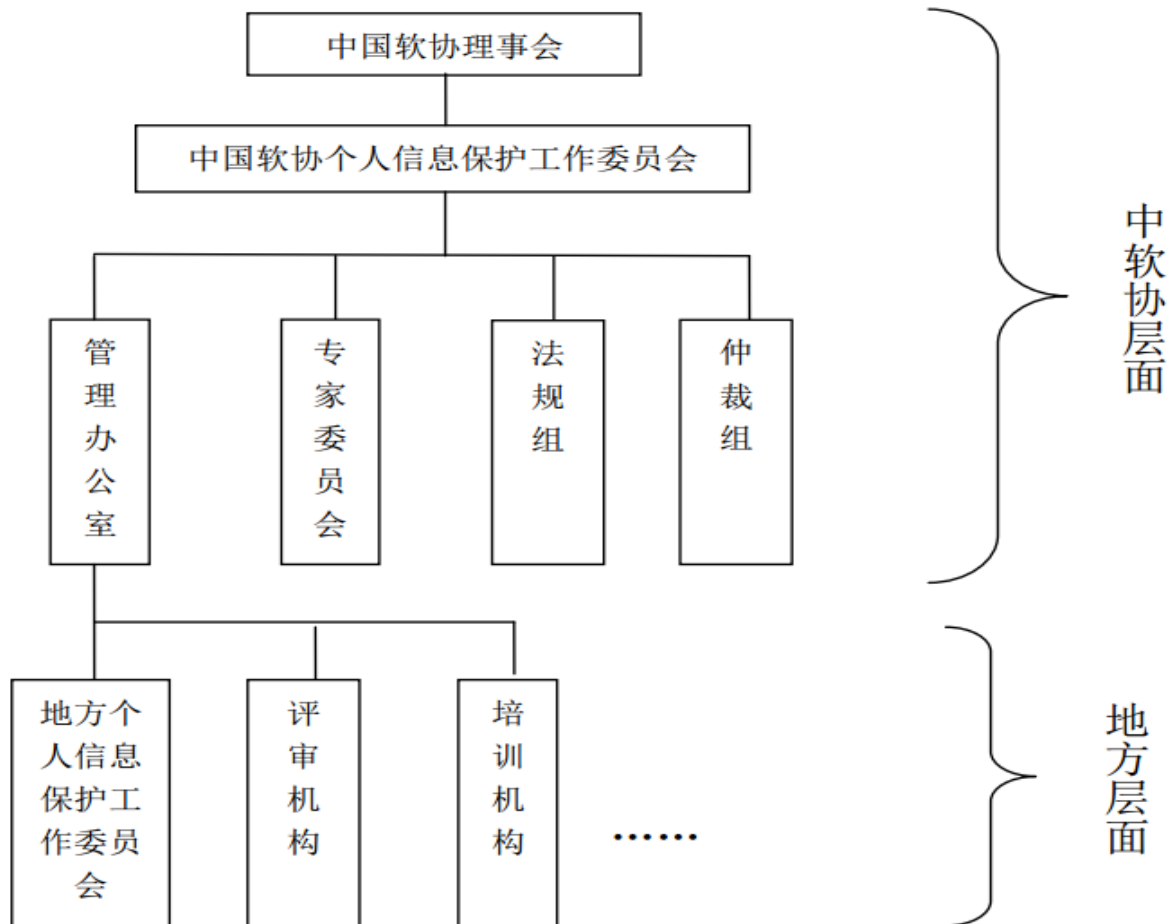


中国ソフトウェア産業協会は、中国で個人情報の安全評価管理プラットフォームの構築に基本条件を満たしている。

- ◆ PIPA全名：個人情報プロテクター評価
- ◆ 英語名：Personal information protection assessment
- ◆ 標準：
 - GB/T 35273-2017 《情報安全技术 個人情報安全規範》
 - T/SIA 001-2017 《企業個人情報安全管理規範》
- ◆ 認定機構：中国ソフトウェア産業協会
- ◆ 評価機構：大連ソフトウェア産業協会
- ◆ 開始时间：2018年7月



PIPA組織機構圖



PIPAの目的の確立と適用範囲



建立目的

该体系是为帮助企业建立个人信息保护规章制度、提高企业个人信息保护能力而设立的。适用于全部社会领域，目前主要应用于软件及信息服务业。

适用范围

适用于自动或非自动处理全部或部分个人信息的机关、企业、事业、社会团体等组织



PIPAマークと証明書



010123456 (01)

评价编号
依据标准
互认编号
颁证日期
有效期



单位名称
单位地址

发证机构

中国软件行业协会(CSIA)



1

背景介绍

2

PIPA概况

3

管理体系建设

4

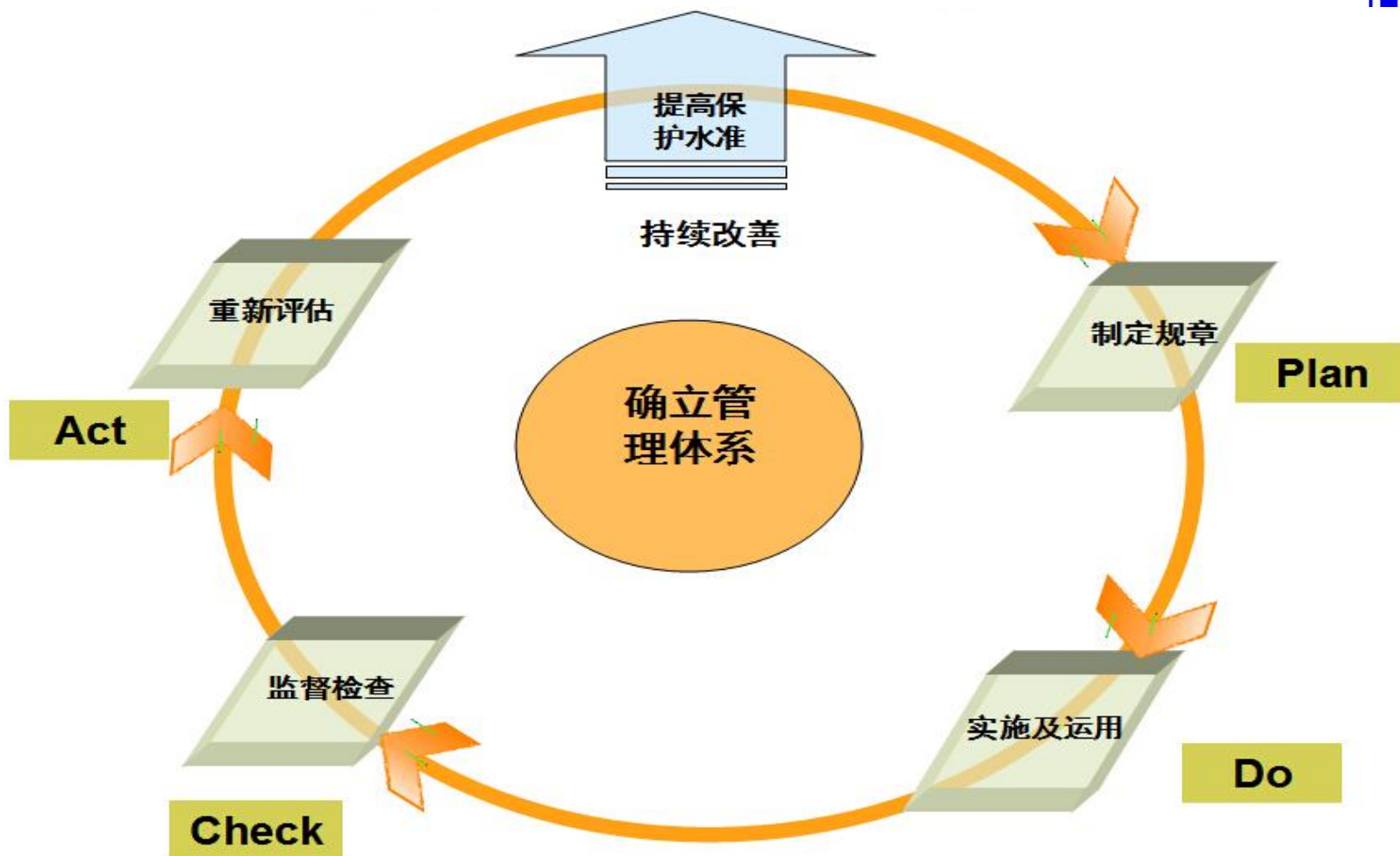
评价与管理

企业启动PIPA前的准备



- 个人信息管理相关法规、标准的选择和学习
- 明确目的和意义（个人信息管理者的责任和义务）
- 建立组织明确相关责任人的工作任务和职责
- 体系融合问题
- 根据管理、业务目标和范围，梳理本单位所涉及的个人信息种类
- 制定管理计划（个人信息生命周期的管理计划、个人信息安全管理体系建立和实施计划等系列工作计划）

PIPA遵循的是PDCA管理办法

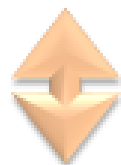


PIPA是对个人信息在生命周期内的保护



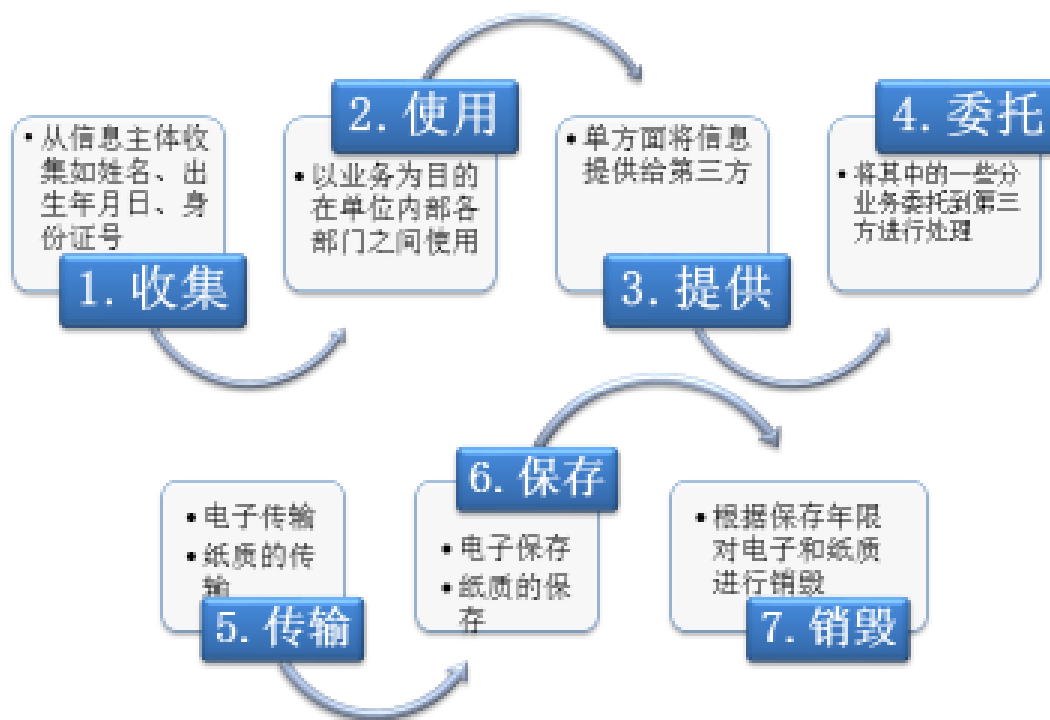
个人信息的生命周期

个人信息主体



个人信息管理者

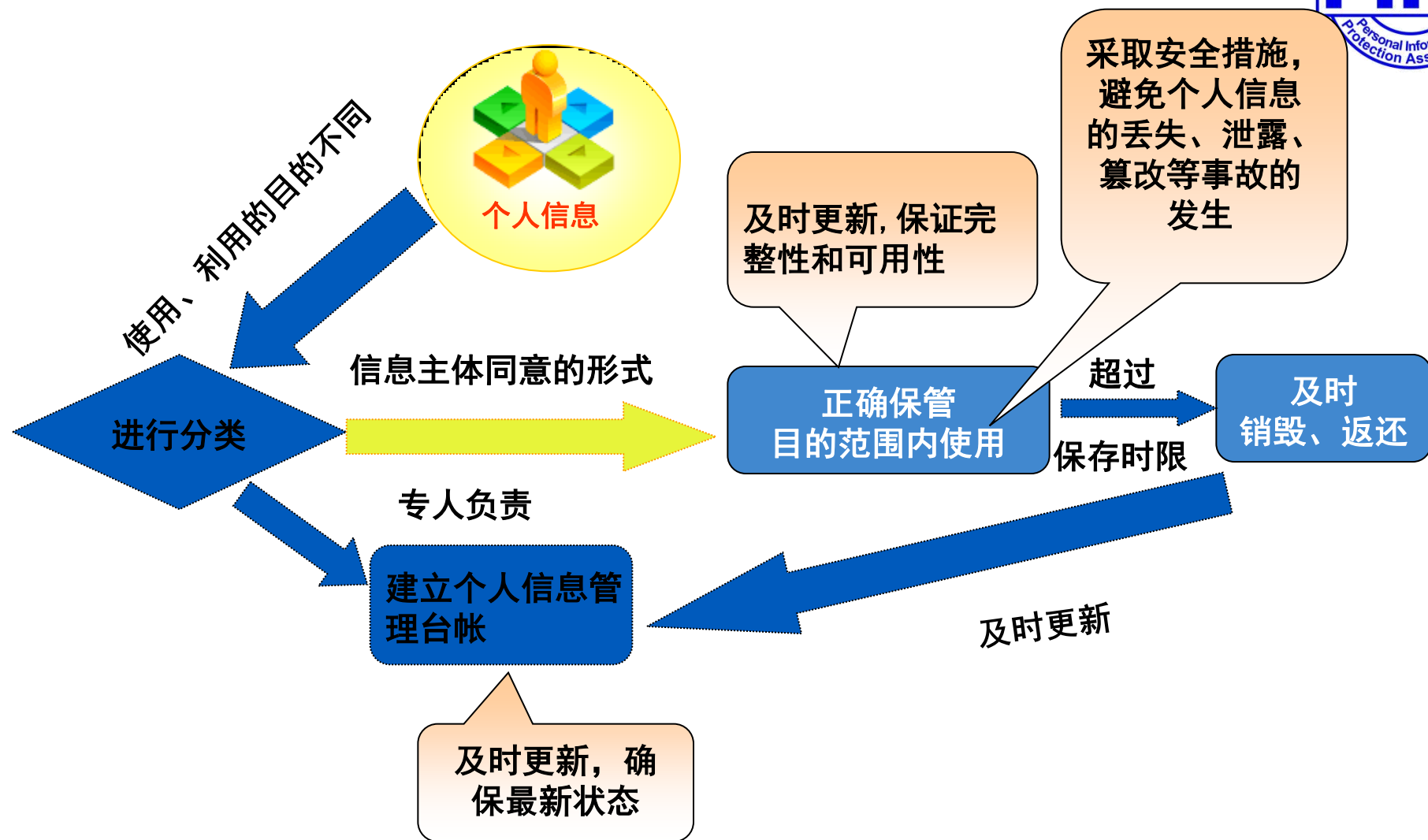
对收集的个人信息的生命周期进行管理



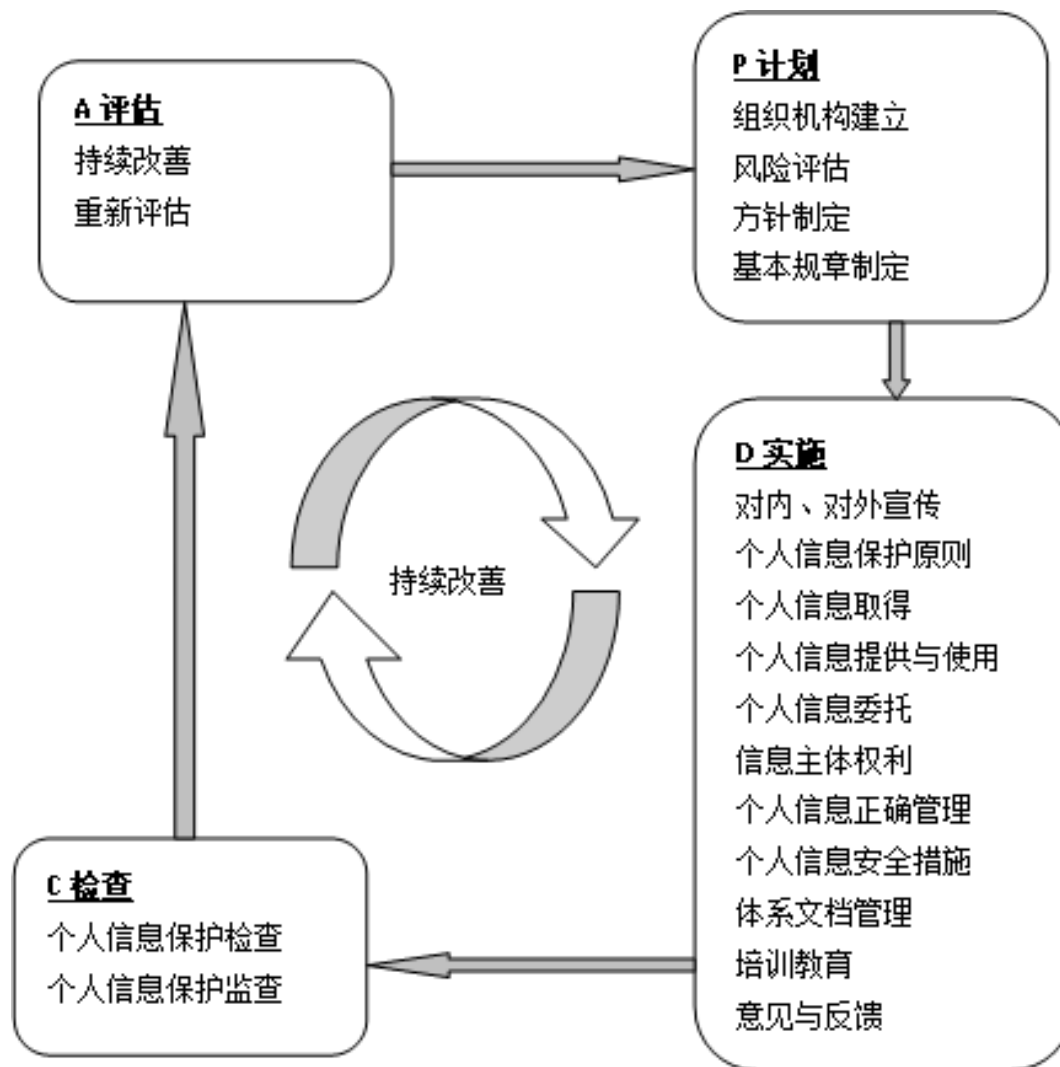
完整性、准确性、可用性、安全性

个人信息安管理体系建立和实施

个人信息数据库建立与管理

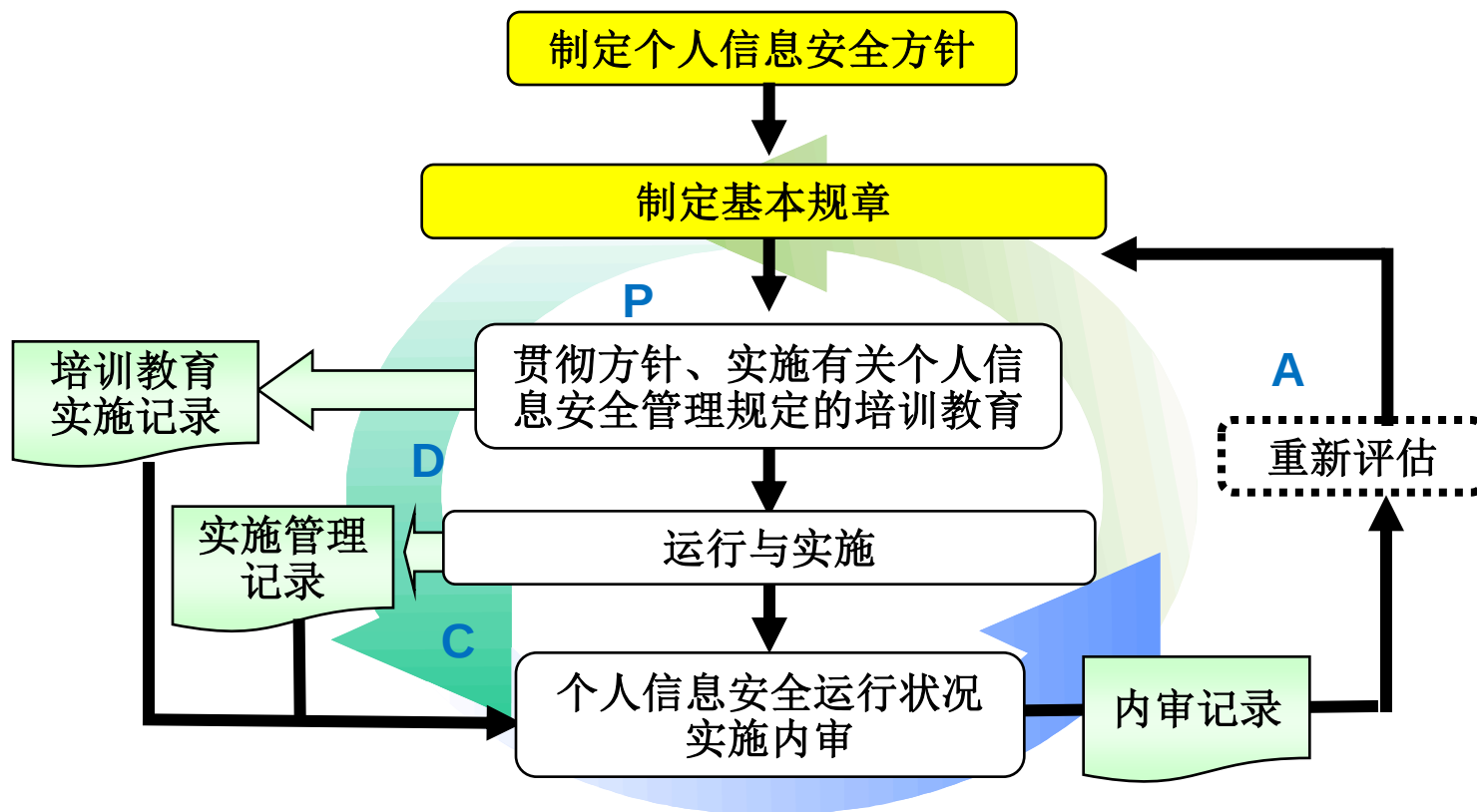


PDCA循环



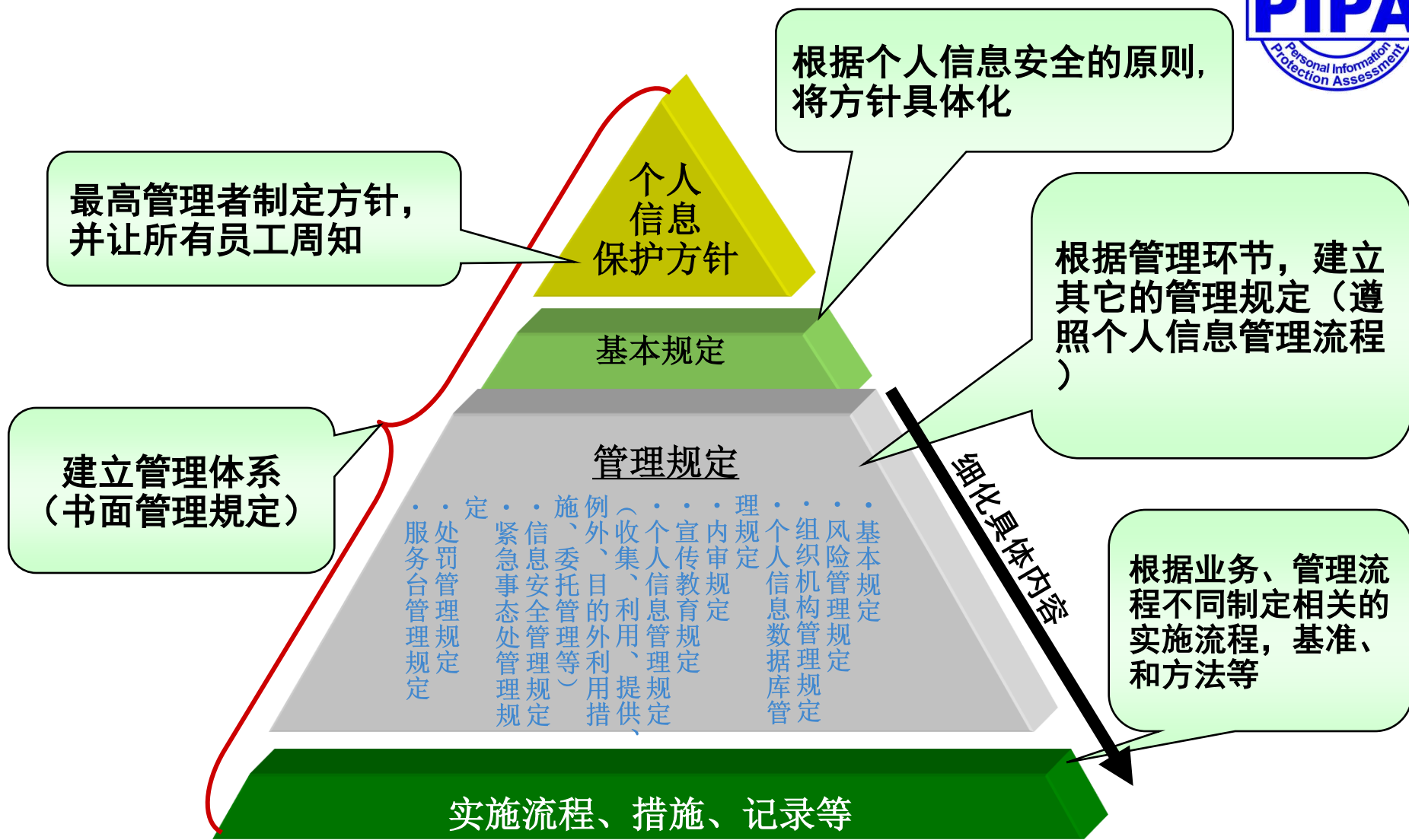
个人信息安管理体系建立和实施

实施流程图



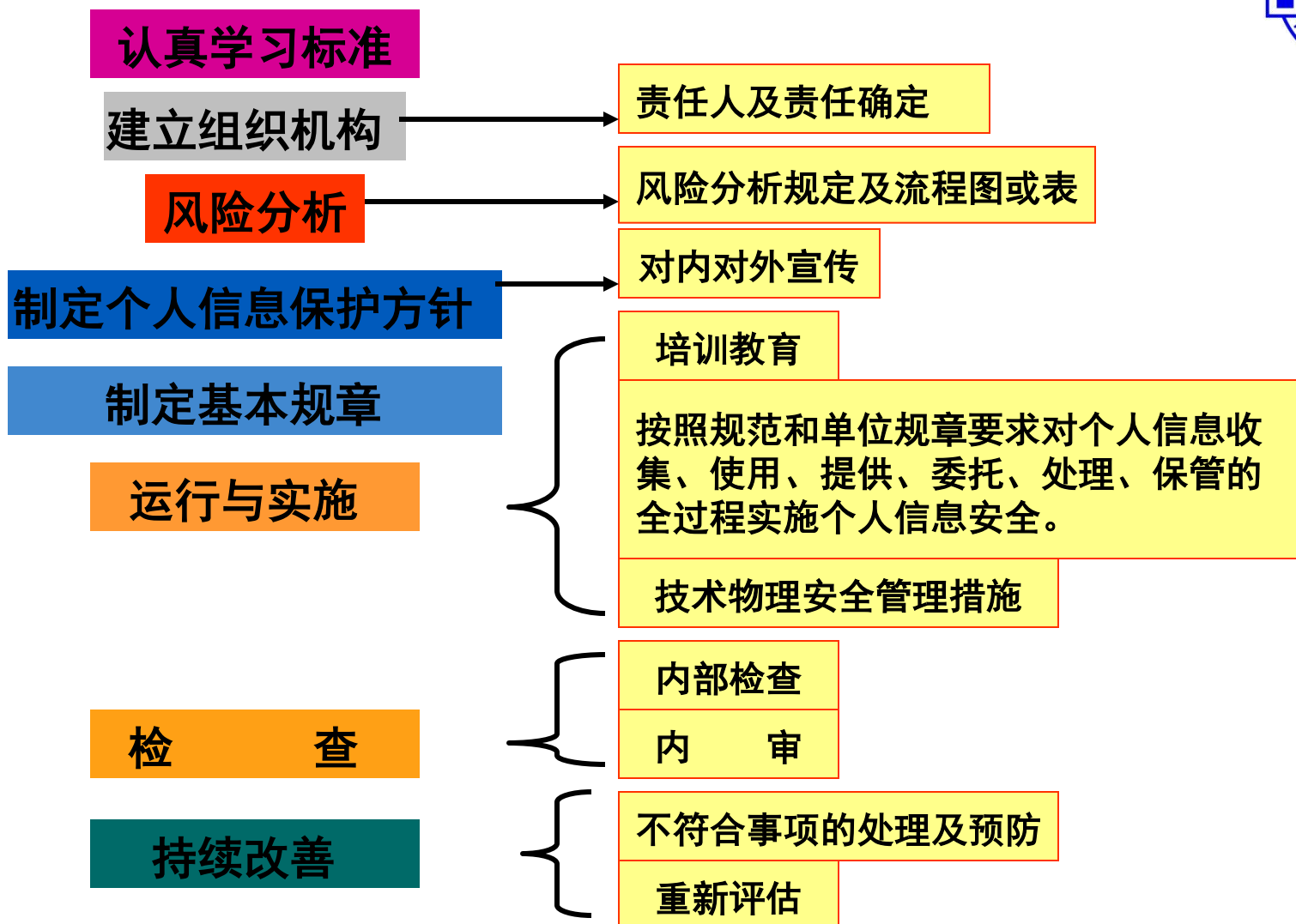
个人信息安管理体系建立和实施

规章制度的构建图



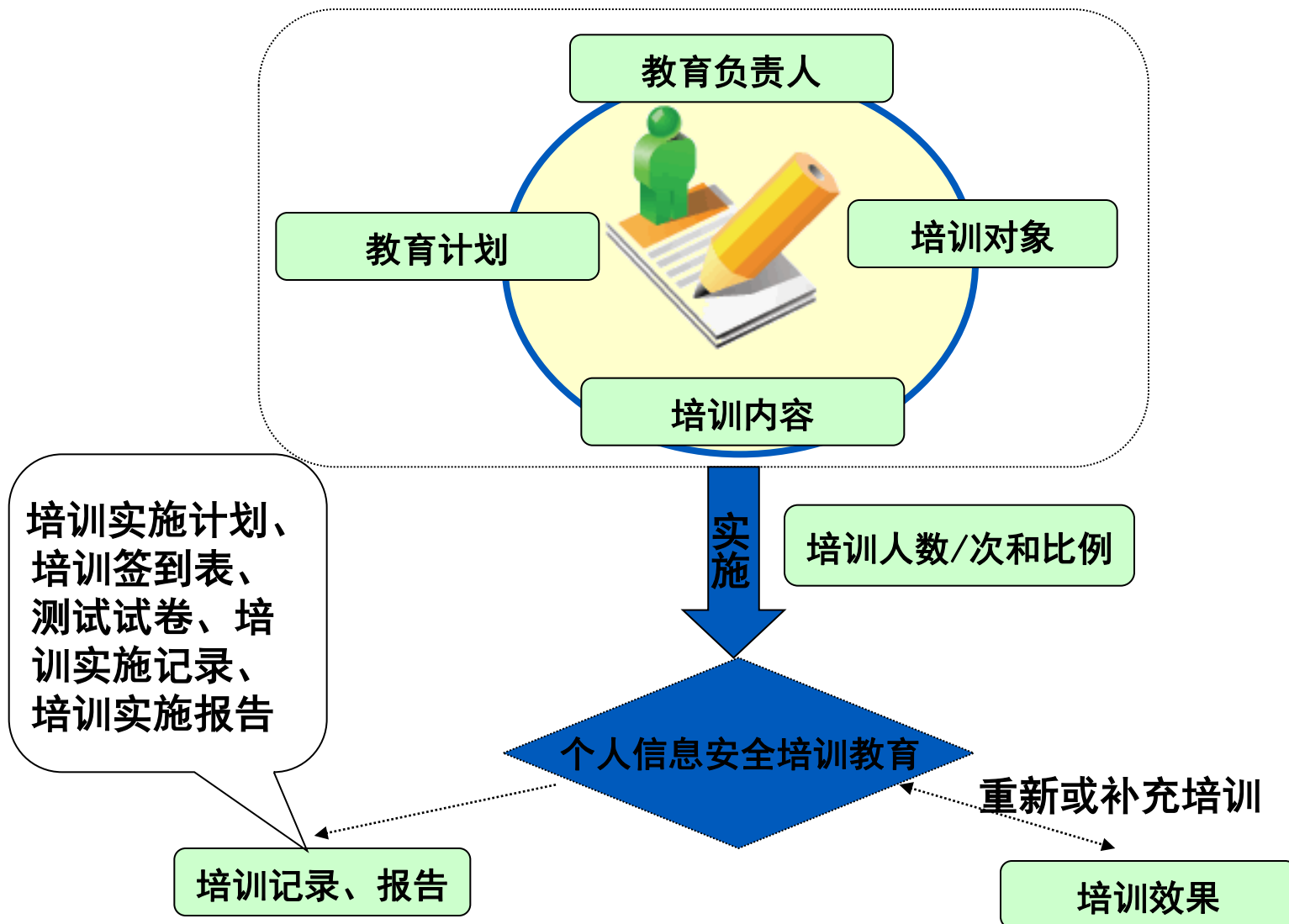
个人信息安管理体系建立和实施

规章制度的建立



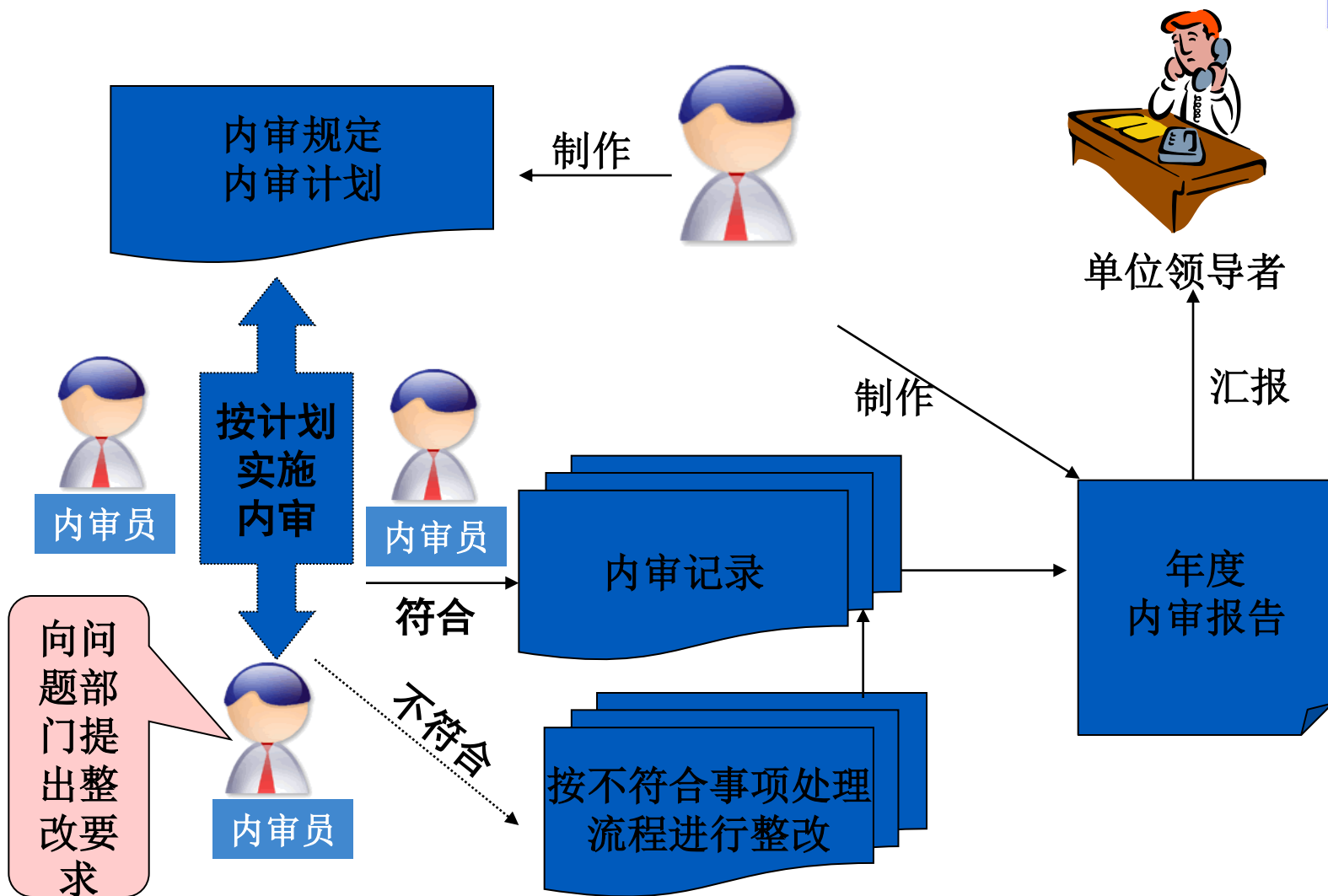
个人信息安管理体系建立和实施

培训教育的实施



个人信息安管理体系建立和实施

内审的实施

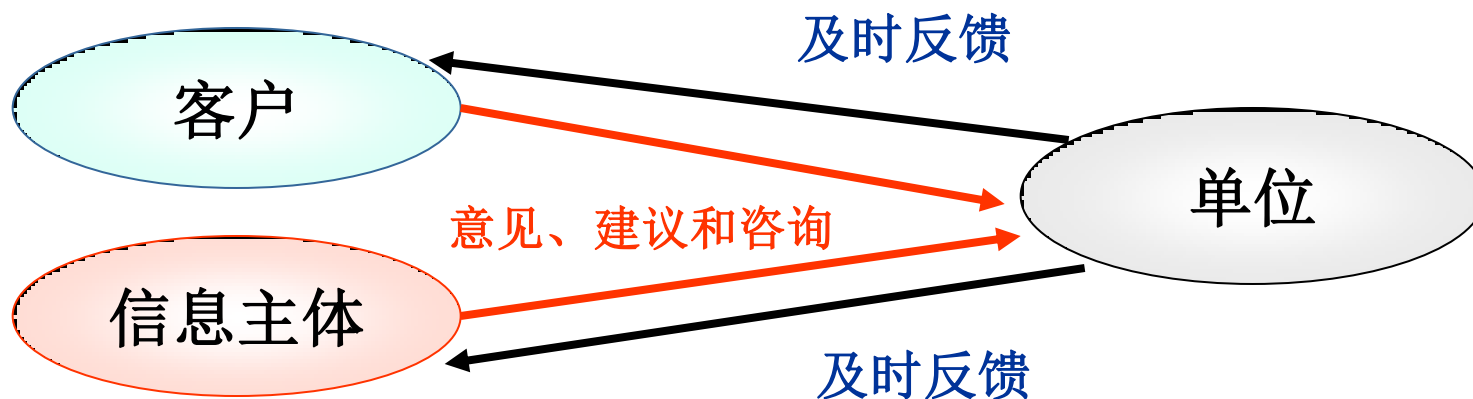


个人信息安管理体系建立和实施

服务台管理



单位对信息主体和客户在个人信息安全方面提出的意见、建议和咨询要及时做出反馈和适当处理，并记录 and 保存。



个人信息安管理体系建立和实施

持续改进与重新评估



不符合事项的处理及预防

最高管理者应根据个人信息保护负责人和内审负责人提供的报告和业务发展情况，要求对不符合个人信息安全的事项进行改进，并修改完善预防措施。处理不符合事项的工作流程：

- a) 不符合事项的确认；
- b) 分析发生不符合事项的原因，制定改进办法和预防措施；
- c) 限定期限进行改进；
- d) 对不符合事项的改进过程及修订的预防措施记录备案；
- e) 对改进结果及修订的预防措施进行评估。

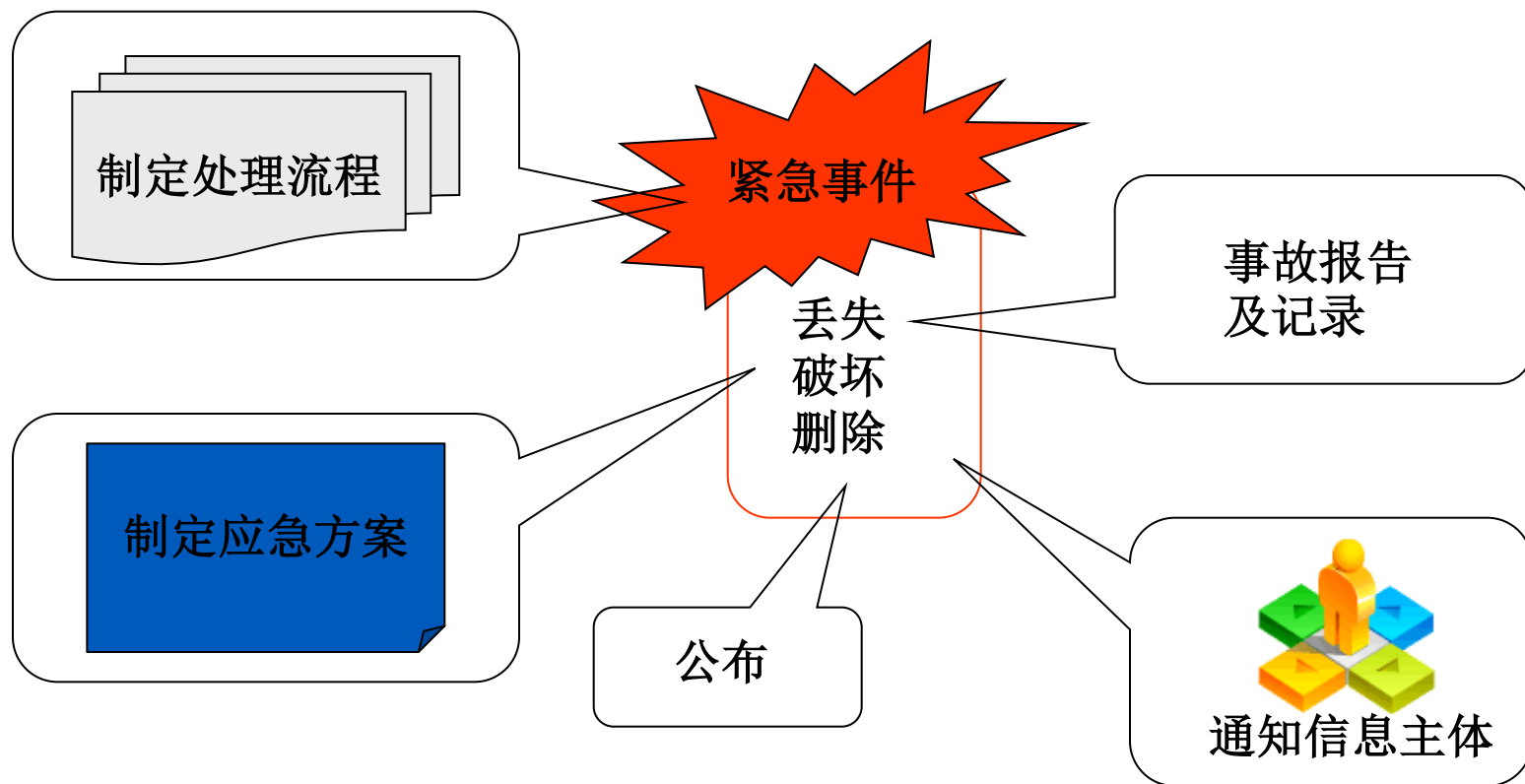
重新评估

应对本单位个人信息安全管理体系进行定期评估、不断改进和完善。在改进与完善过程中应参考以下内容：

- a) 内审负责人和个人信息保护负责人的报告；
- b) 投诉及内部、外部的意见及建议；
- c) 对每次改进和修订后执行情况的跟踪；
- d) 国家相关法律、法规的颁布和修改；
- e) 社会形势、公众意识、技术进步的变化；
- f) 单位业务领域及经营范围的变化。

个人信息安管理体系建立和实施

应急管理（紧急事态的预防与处理）





1

背景介绍

2

PIPA概况

3

管理体系建设

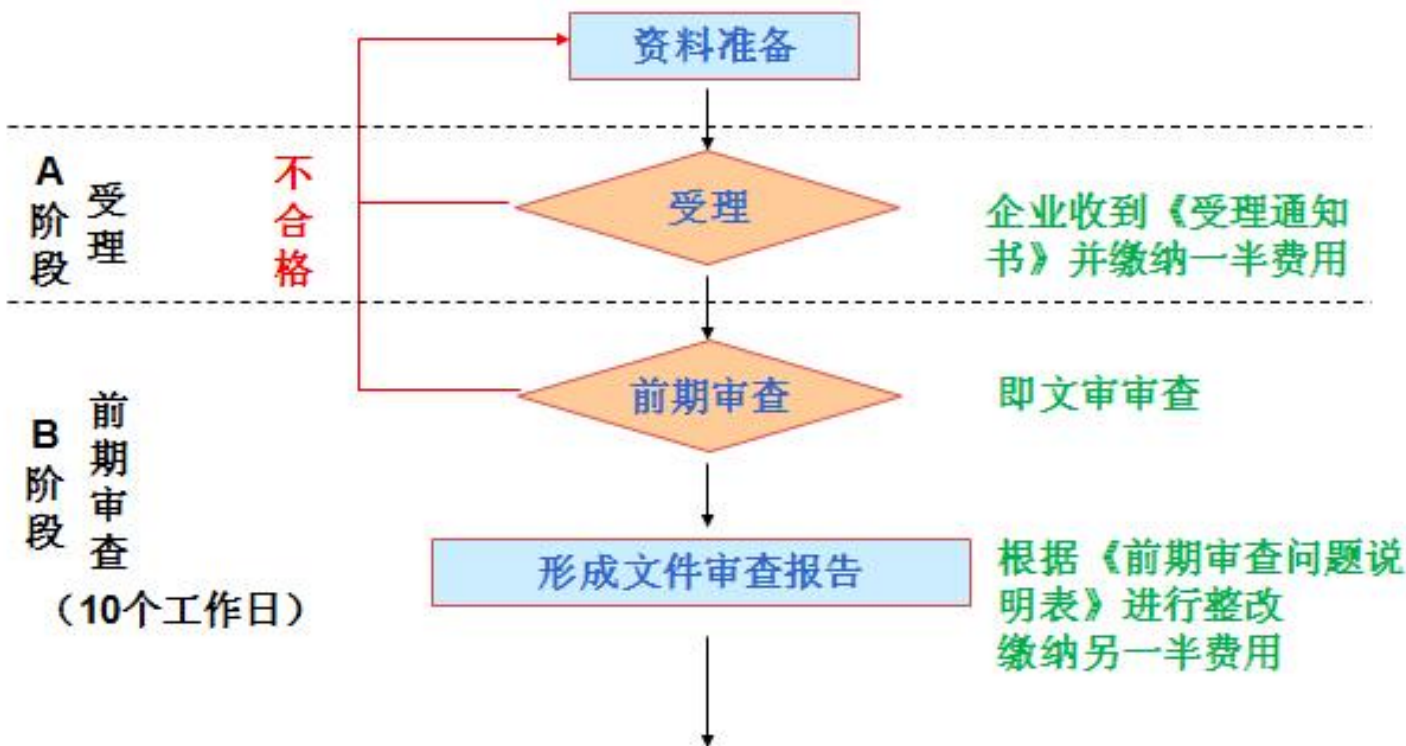
4

评价与管理

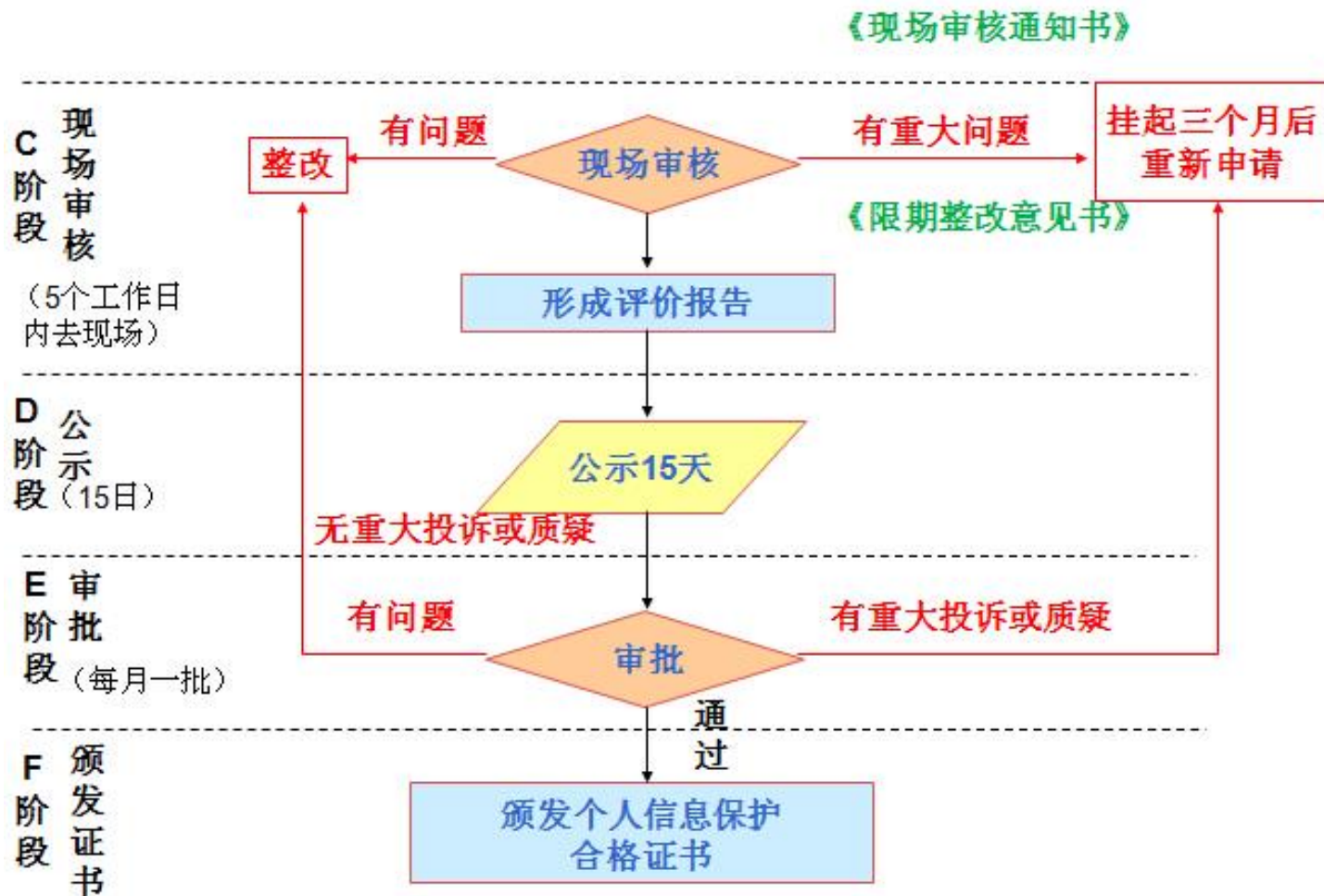
评价流程图



PIPA评价流程



评价流程图（续）

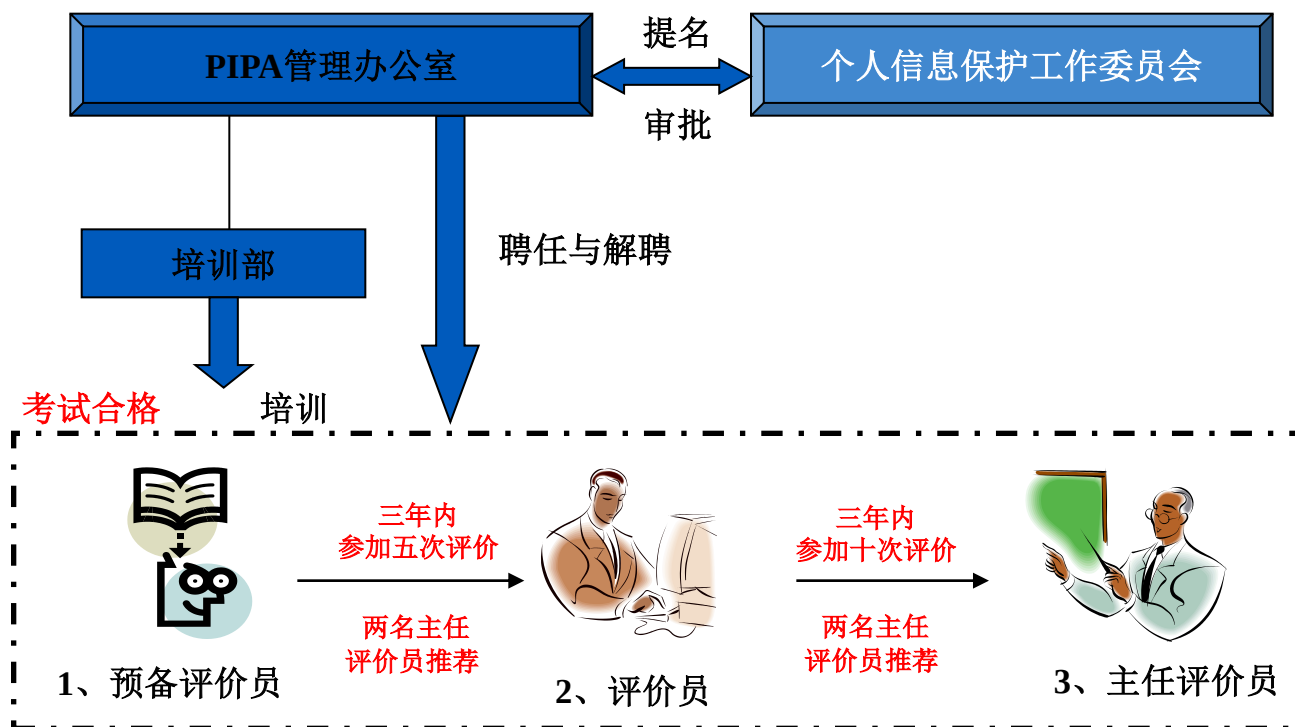




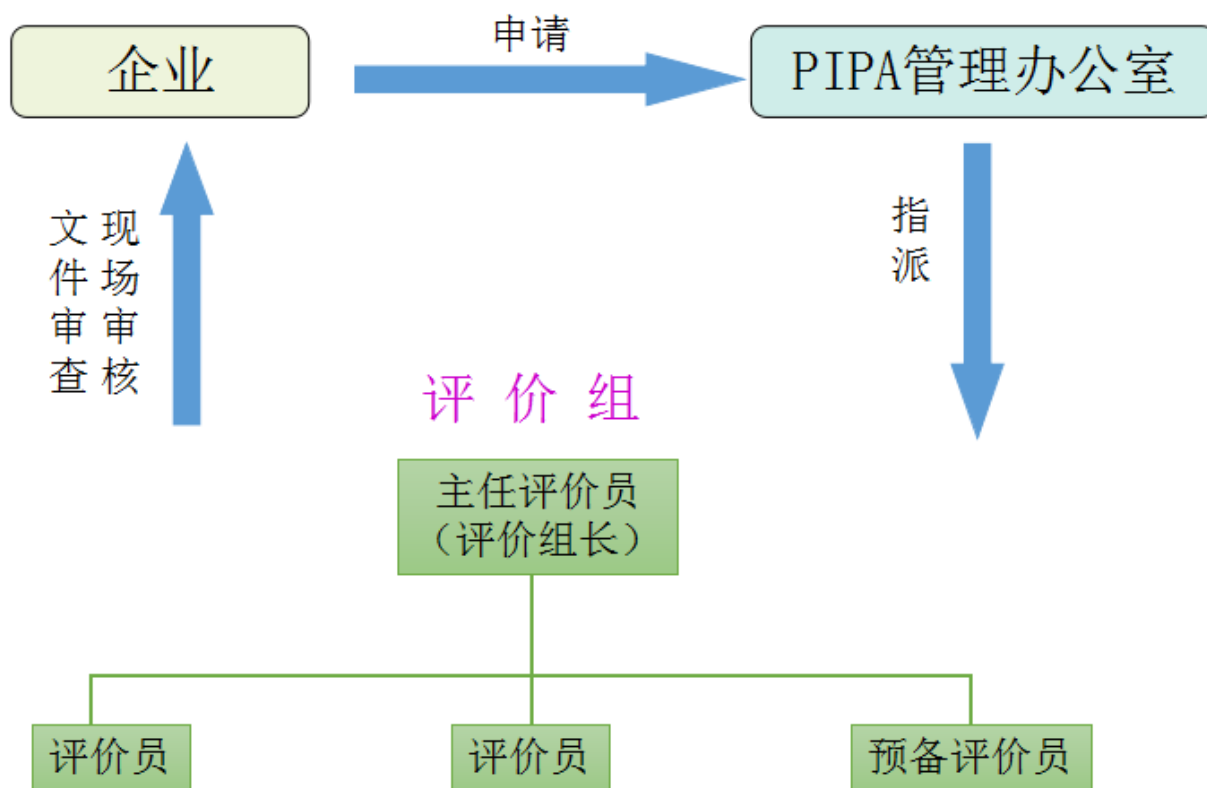
结合评价流程，将评价分为如下几个阶段：

- ◆ 意向受理阶段
- ◆ 正式申请阶段
- ◆ 评审准备阶段
- ◆ 文件评审阶段
- ◆ 现场评审阶段
- ◆ 公示阶段
- ◆ 符合性审批阶段
- ◆ 合格证书及标志(互认标志) 管理
- ◆ 评价企业管理

评价员选聘流程



评价员参加评价工作流程





管理与监督

1

评价机构对PIPA企业的监督与管理

2

个人信息保护工作委员会对评价过程的监督与管理

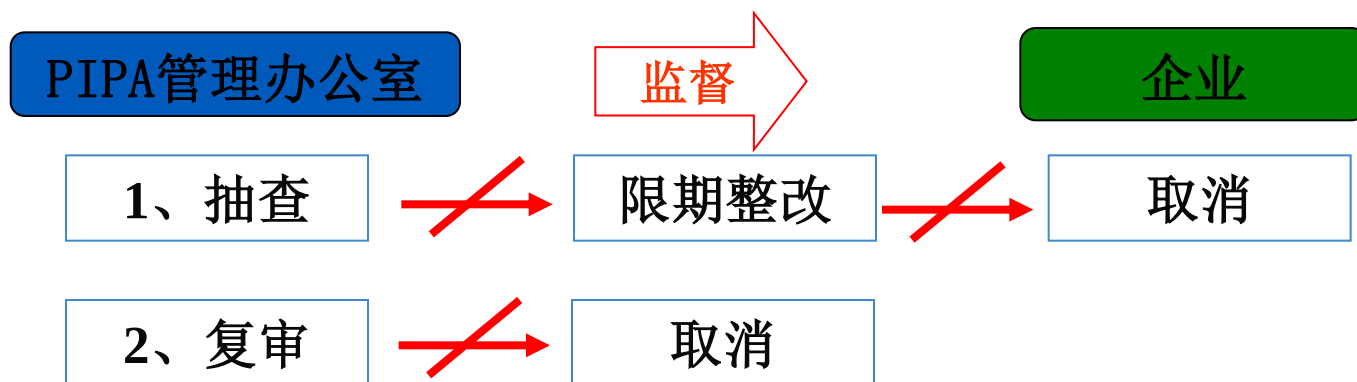
3

对评价员的监督与管理

4

建立投诉及事故报告制度

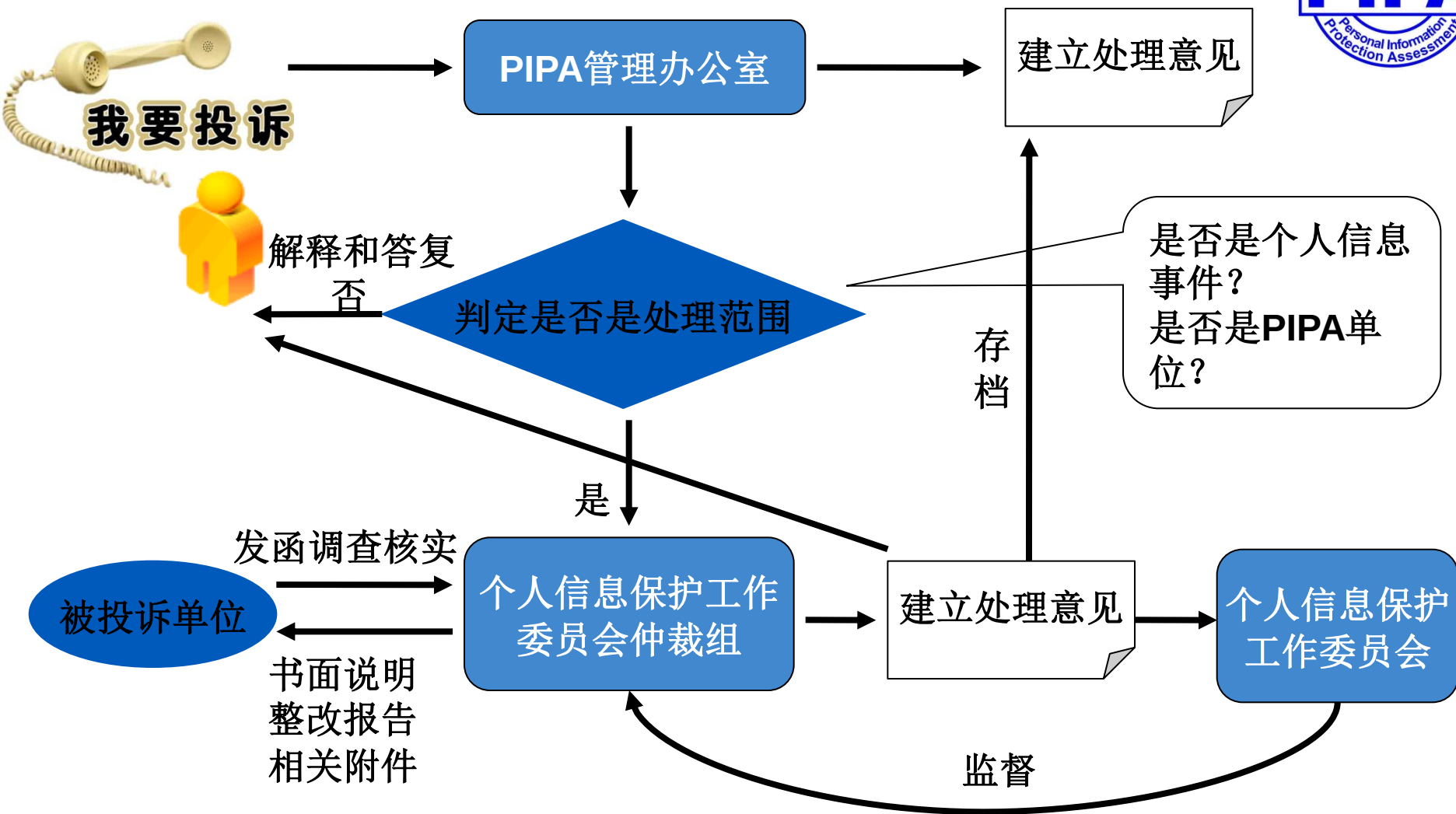
对PIPA企业的监督检查



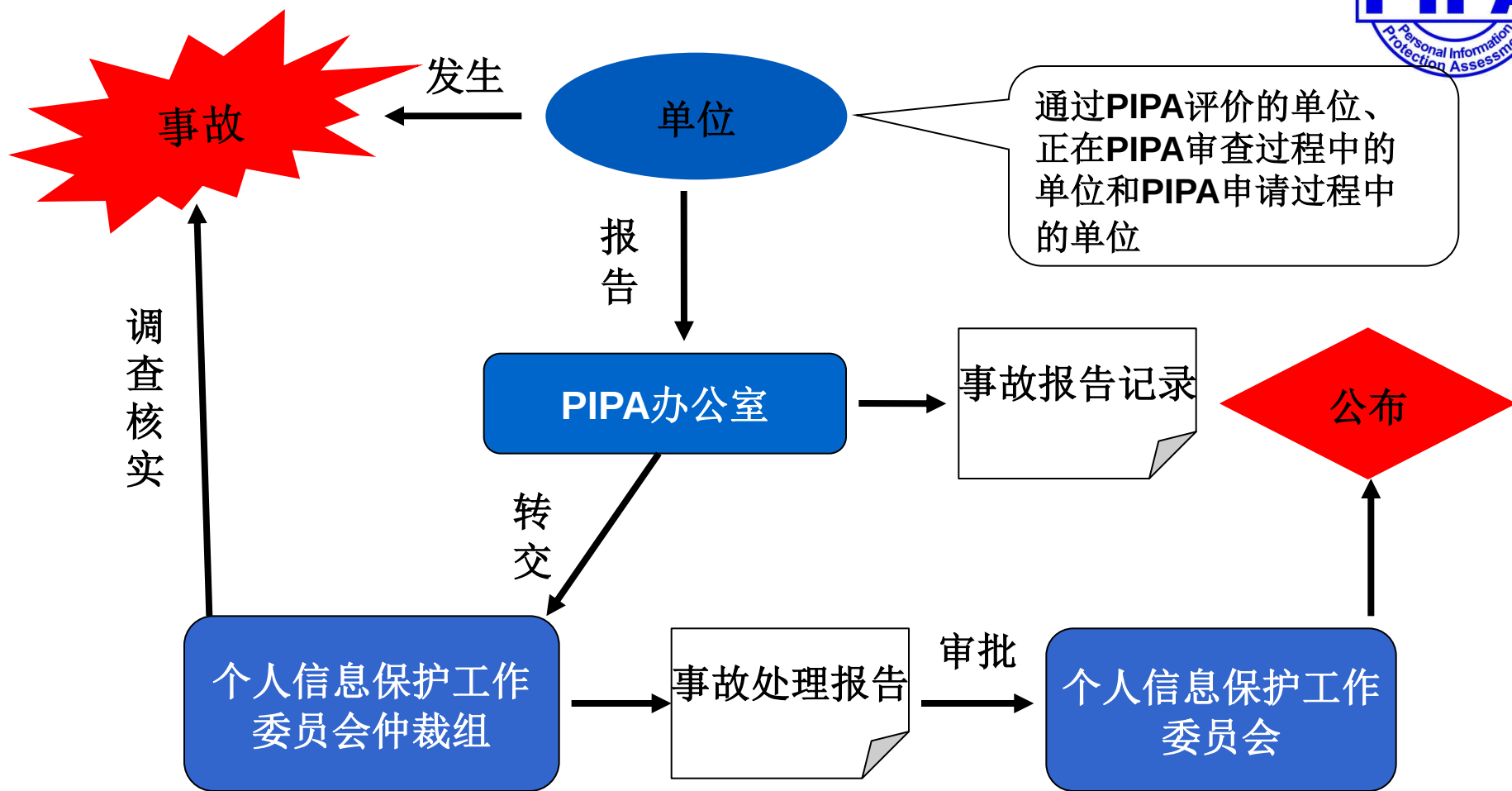
- (1) 客户或消费者对申报单位在个人信息保护方面有重要举报和投诉并确认为事时;
- (2) 在个人信息保护方面发生重大事故的单位;
- (3) 企业更名、办公场所或业务有重大变化的单位。

可在三个月后重新申请

投诉处理流程



事故报告流程



事故级别判定表



事故级别	性质	影响	原因	损失
3	非法搜集、非法使用、违反法规	对社会影响很大	故意或有组织的	信息量大，损失大
2	违反《规范》	对社会影响较大或对信息主体影响大	管理制度严重漏洞	信息量大，损失较大
1	违反本单位个人信息保护管理制度的	对社会影响较小或对信息主体影响较大	管理制度不完善或个人原因	信息量较大，损失较小
0	没有违反规定	对信息主体影响较小	不是人为因素	信息量小，没有造成损失



谢谢!

中国软件行业协会(CSIA)