Gdevops

全球敏捷运维峰会

云环境信息安全与隐私保护国际标准研究与实践

演讲人：万鑫 英国标准协会

BSI
专注标准、服务全球

51%
《财富》500强

75%
富时100 指数公司

68%
日经指数公司

80000
家客户

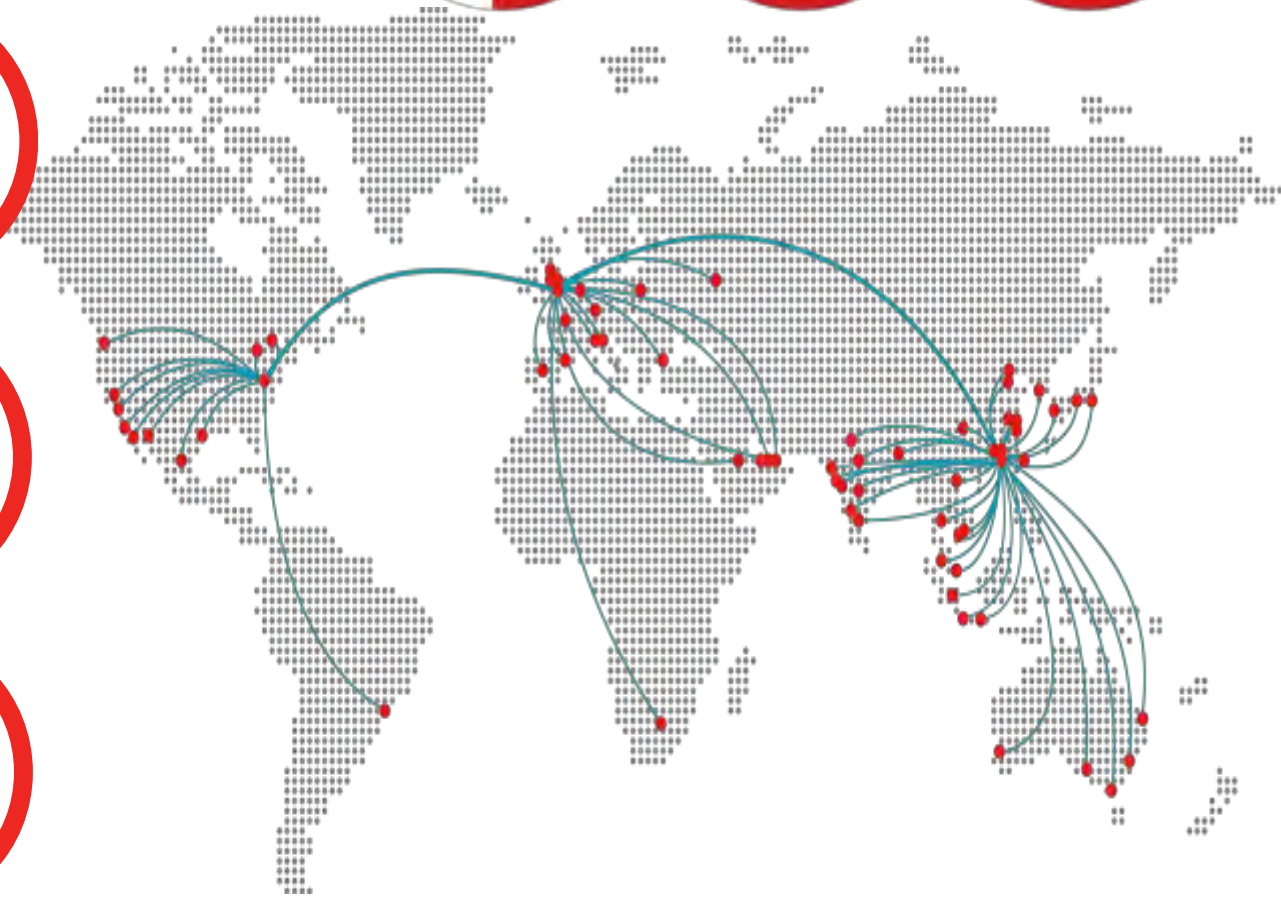
182 个国家/地区

3 个
区域中枢

全球 73
个分支机构

8家
国内分支

发布
37384
项标准



bsi.

1 互联网时代全球信息安全风险动态及趋势

2 云服务安全与隐私保护国际标准介绍

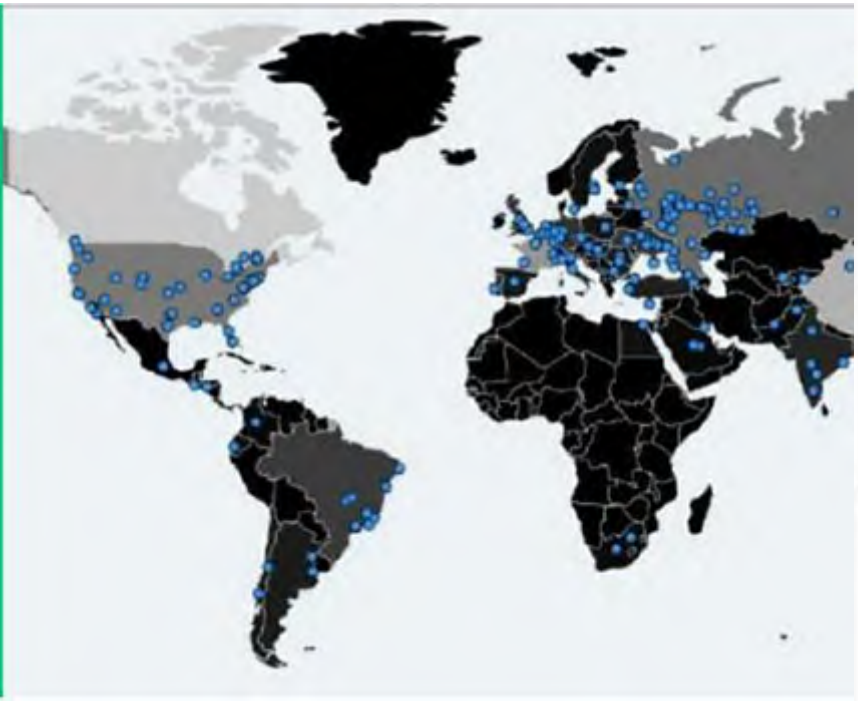
3 隐私保护方案制定与实施

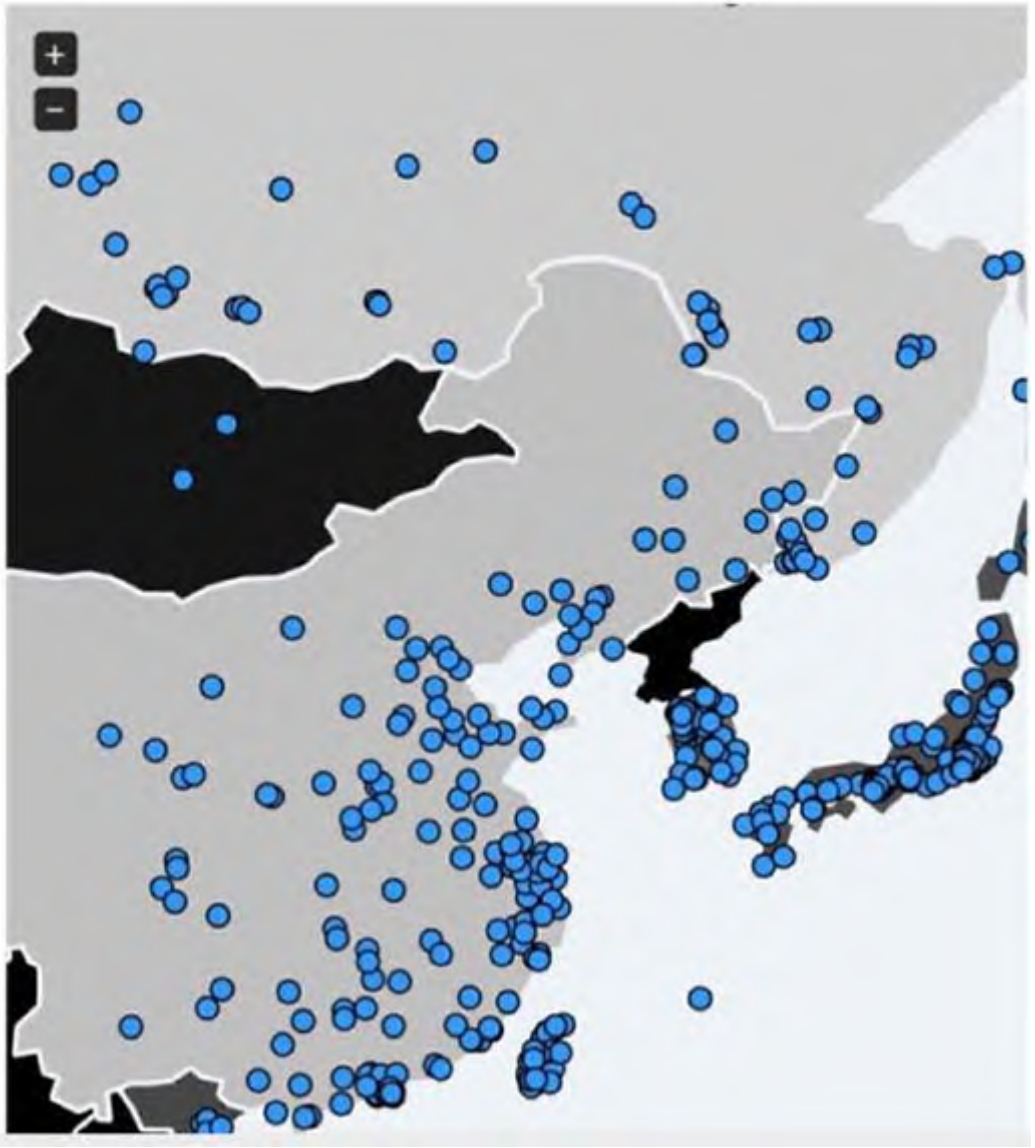
1 互联网时代全球信息安全风险动态及趋势

2 云服务安全与隐私保护国际标准介绍

3 隐私保护方案制定与实施

时代的挑战 – 隔离与互联





风险及挑战 – 企业营运面临的10威胁

74 countries

568 responding organizations

Source: Horizon Scan 2016 Survey Report (BCI & BSI)

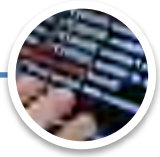
互联网关键风险及挑战之 – Cyber Attack

比特币交易Bitfinex被黑，11.97万个比特币被窃

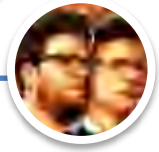
2016年5月三大邮件服务商超过2.7亿人email凭证外泄

2016年9月，黑客组织**“奇幻熊”**入侵世界反兴奋剂机构（**WADA**），多次曝光的禁药豁免权运动员名单，共40人。

2016年9月，雅虎承认网站在**2014年底即**遭到攻击，预计**5亿用户资料泄露**，疑似受某国支持。



2016年9月22日，Brian Krebs 的安全博客网遭到**665Gbps**的**DDoS攻击**，创造了新记录。



2014年11月全美Sony 影业员工的计算机沦陷

互联网关键风险及挑战之– Unplanned ICT Outage

Google GCE 宕机
日期: Feb 18-19, 2015
持续时间: 1 hours

Facebook & Instagram 服务中断
日期: Jan. 27, 2015
持续时间: 1+ hours

Microsoft Azure 云服务中断
日期: March.16、17, 2015
持续时间: 2 hours、24+hours

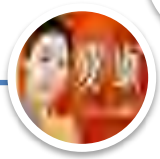
Apple 云服务中断
日期: March 11, 2015
持续时间: 12+ hours

Alipay 服务中断
日期: May. 27, 2015
持续时间: 2+ hours

Ctrip 无法访问
日期: May. 28, 2015
持续时间: 8+ hours

互联网关键风险及挑战之– Data Breach

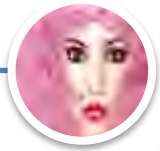
2014年5月小米泄露800万条数据：用户名、邮箱、密码、IP地址、Salt 等。



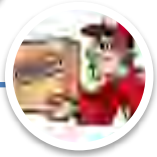
2014年7月爱康国宾泄露1200万条数据：姓名、身份证号、电话、地址等。

2013年5月多家宾馆泄露2200万条数据：姓名、证件号、性别、地址、电话、邮箱等

2014年12月12306网站泄漏1亿多数据：邮箱、用户名、密码、身份证号、手机号。



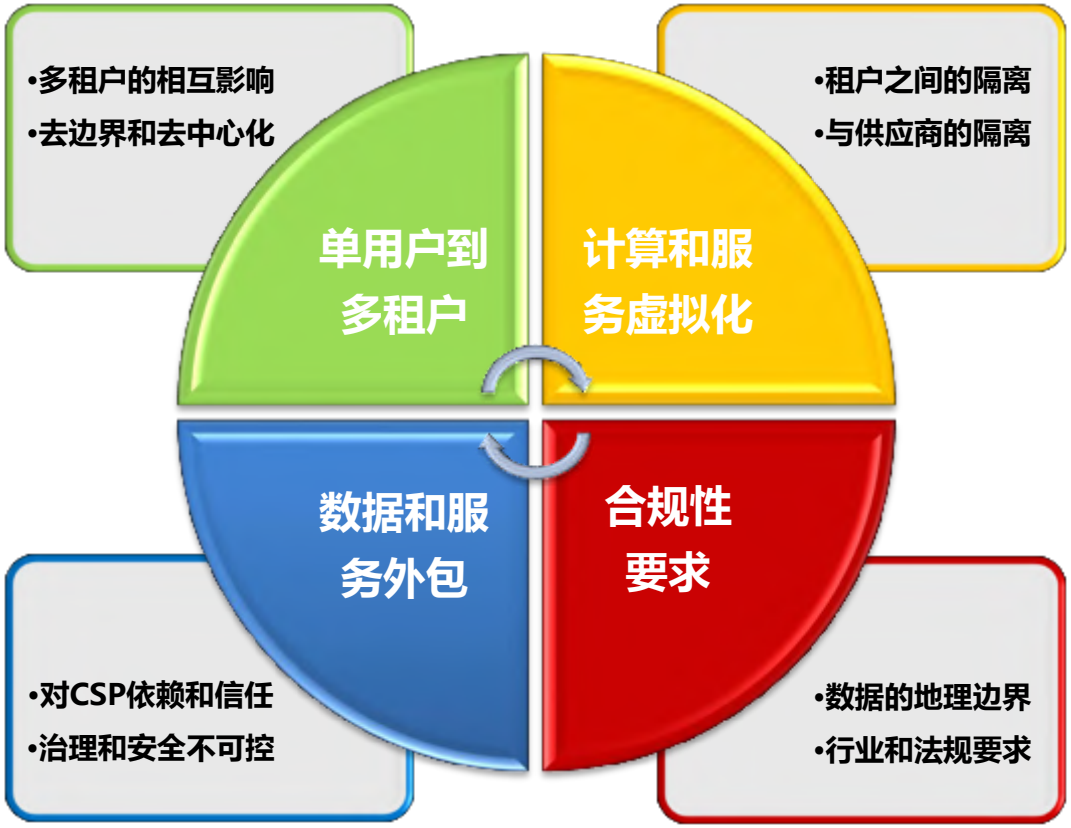
2013年5月乐蜂网泄露1.5亿条数据：邮箱、密码等。



2014年8月多家快递公司，泄露1400万数据：快递号、姓名、电话、邮箱、地址等。

数据来源：补天漏洞响应平台

云计算的特性与安全风险



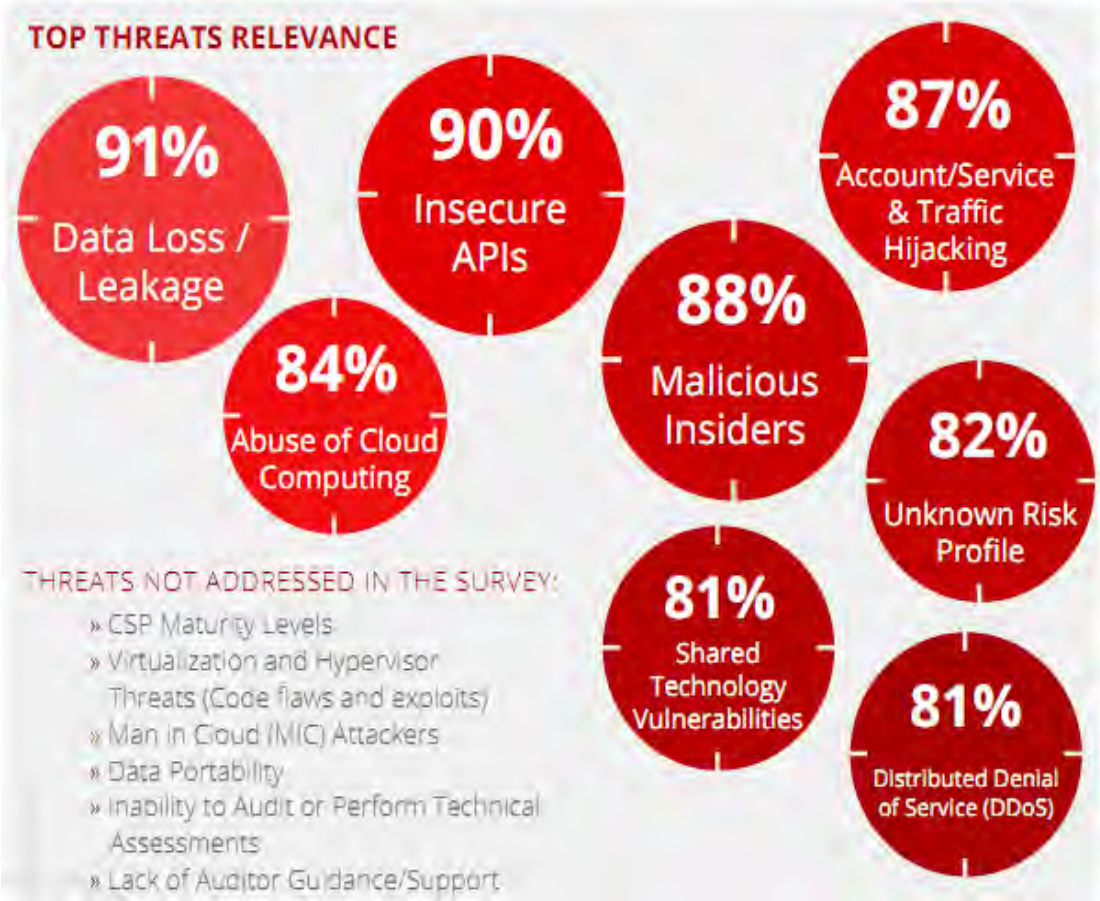
典型的云安全风险

- *治理缺失*
- *锁定云供应商*
- *隔离实效*
- *合规性风险*
- *管理接口漏洞*
- *数据保护*
- *不安全或不完整的数据删除*
- *恶意的内部人员*

Source: ENISA - Cloud Computing - Benefits, risks and recommendations for information security

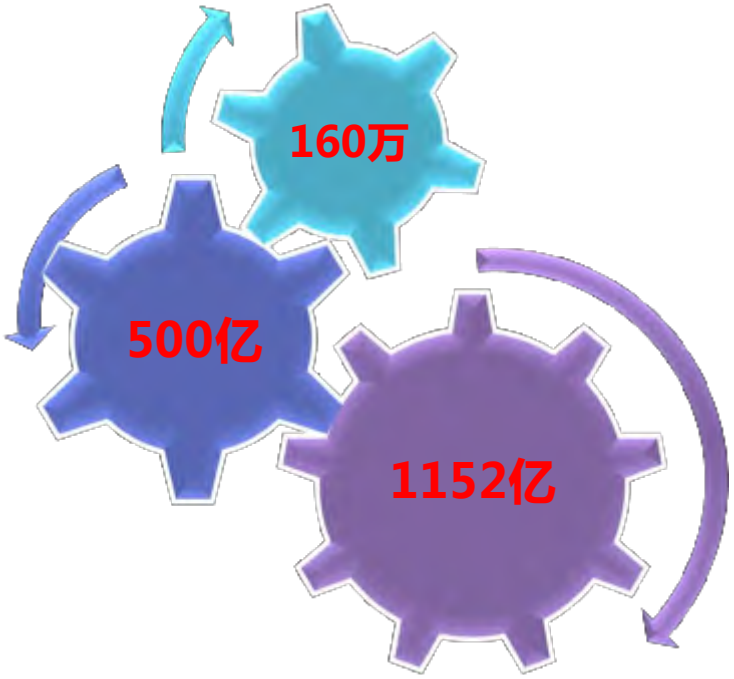
云计算面临的安全威胁

1. ***数据丢失/泄露***
2. ***不安全的API***
3. ***恶意的内部人员***
4. ***帐户/服务和流量劫持***
5. ***云计算的恶意使用***
6. ***未知风险***
7. ***共享技术的脆弱性***
8. ***分布式拒绝服务（DDoS）***



Source: CSA- Top Threats to Cloud Computing

个人信息泄密日趋猖獗



威胁信息安全的黑色产业链

1 互联网时代全球信息安全风险动态及趋势

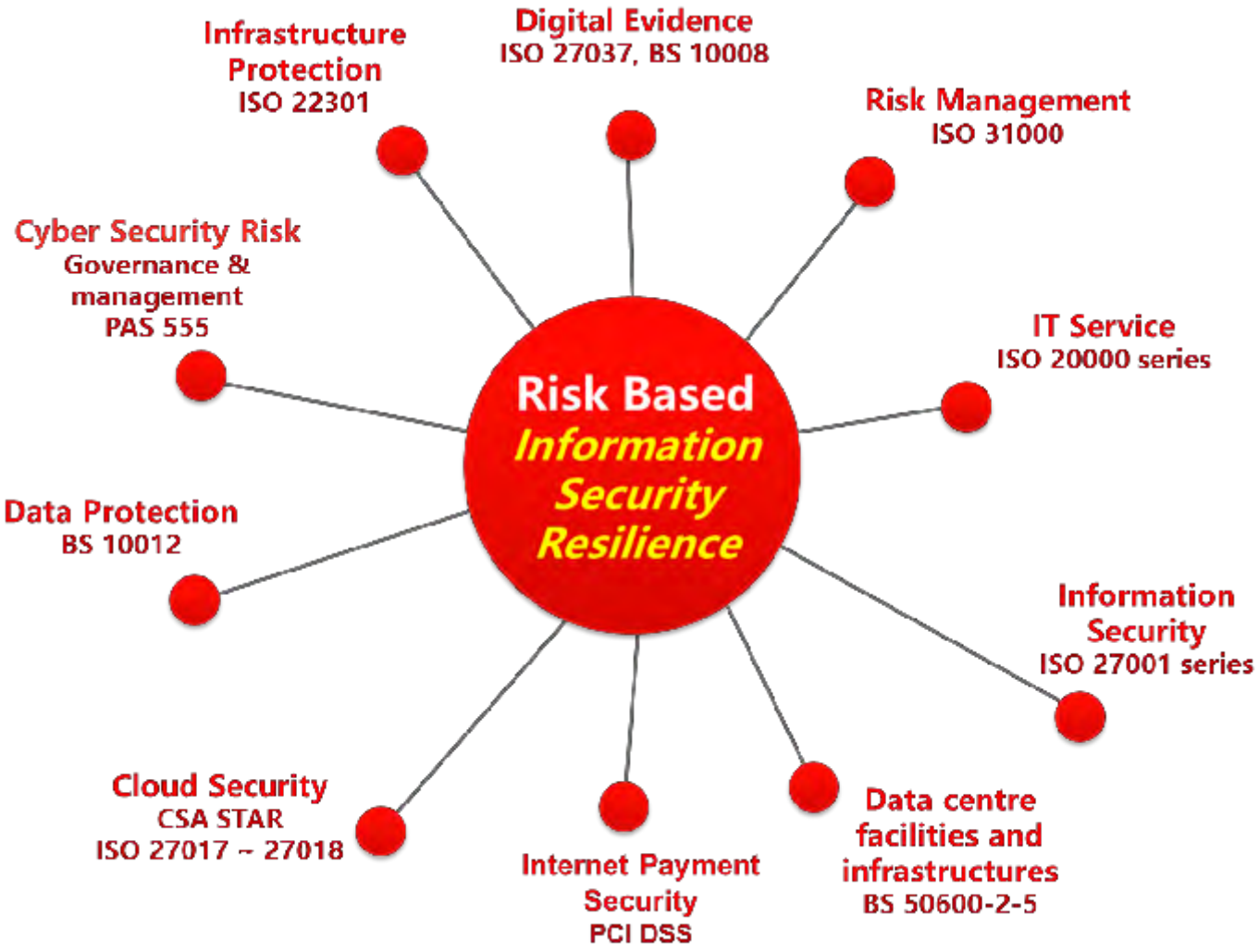
2 云服务安全与隐私保护国际标准介绍

3 隐私保护方案制定与实施

全面IT管理及标准化

IT管理是一个复杂的过程，组织应该从组织治理与战略出发，制定恰当的IT治理架构和战略，以最切合业务需要的某一IT管理主题切入，逐步提升，持续改进，最终达成全面的IT管理，發挥信息技术的最大价值，并规避风险。

CSP如何展现云服务整体管理绩效及治理承诺



其他国际云安全标准/指南 – ISO 27000系列

ISO/IEC 27017: 2015
参考指南 (已发布)

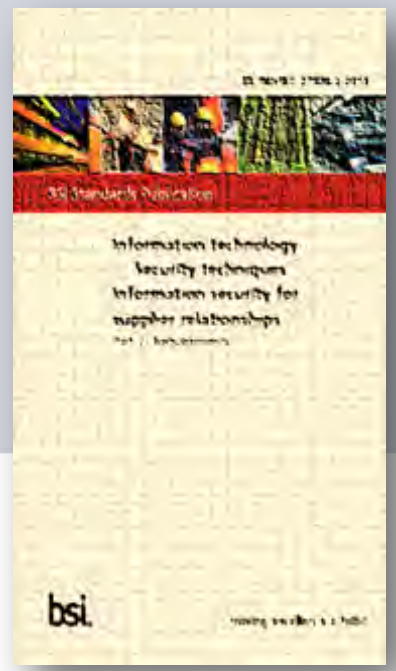
- **Code of practice** for information security controls for cloud computing services based on ISO/IEC 27002

ISO/IEC 27018: 2014
参考指南 (已发布)

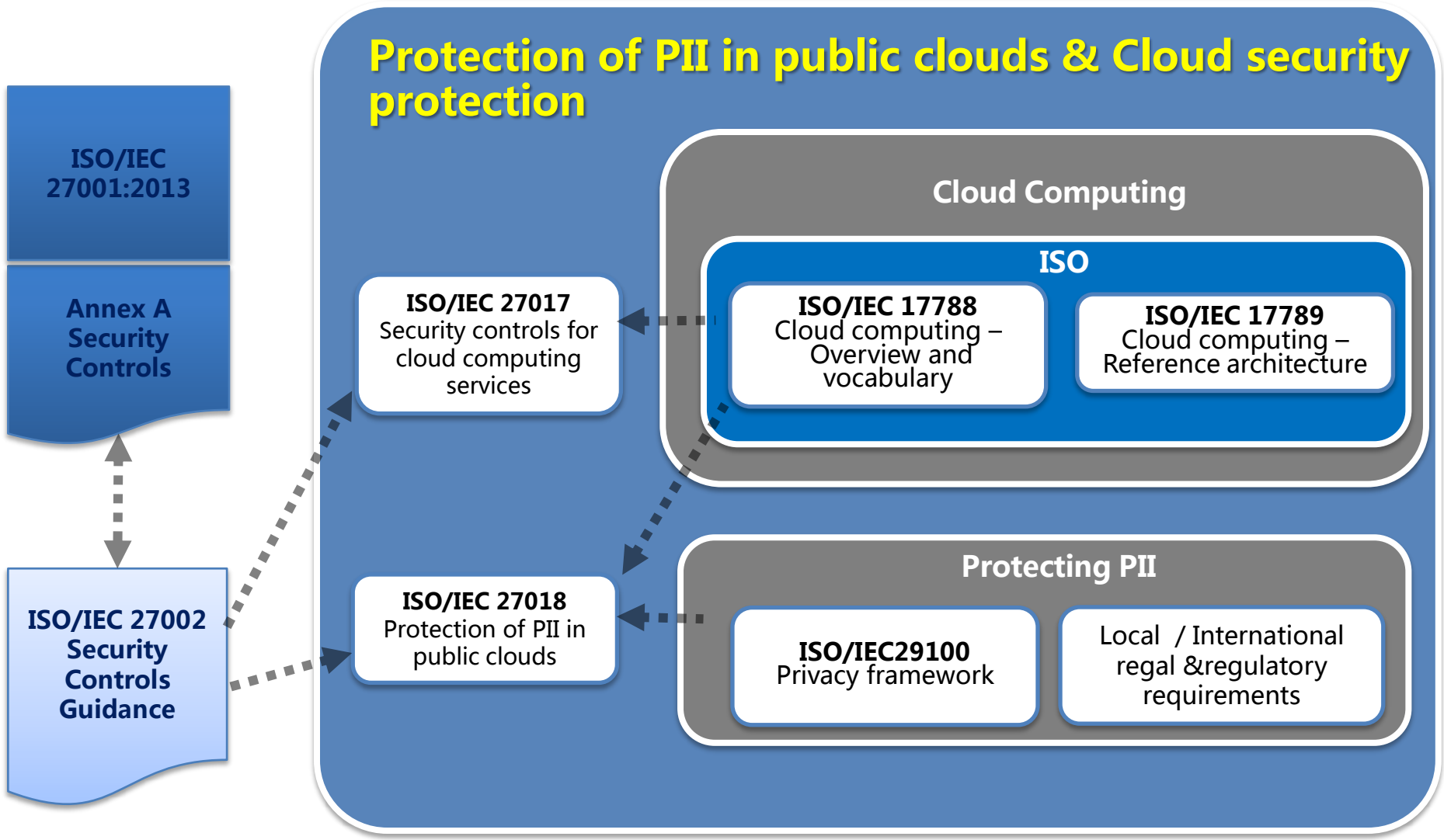
- **Code of practice** for protection of personally identifiable information (PII) in public clouds acting as PII processors

ISO/IEC 27036-4
参考指南 (制定中)

- Information security for supplier relationships -- Part 4: **Guidelines** for security of Cloud services



国际云服务安全相关标准/ 指南关系



ISO/IEC 27017:2015 的控制措施 (37+7)

Additional guidance based on ISO/IEC 27002

Clause	Security Domain	#of Control Guidance
5	Information security policies	1
6	Organization of info. security	2
7	Human resource security	1
8	Responsibility for assets	2
9	Access control	7
10	Cryptography	2
11	Physical and environmental security	1
12	Operations security	7
13	Communications security	1
14	System acquisition, development & maintenance	2
15	Supplier relationships	3
16	Information security incident management	3
17	Information security aspects of BCM	0
18	Compliance	5
		37

+ Cloud service extended control set

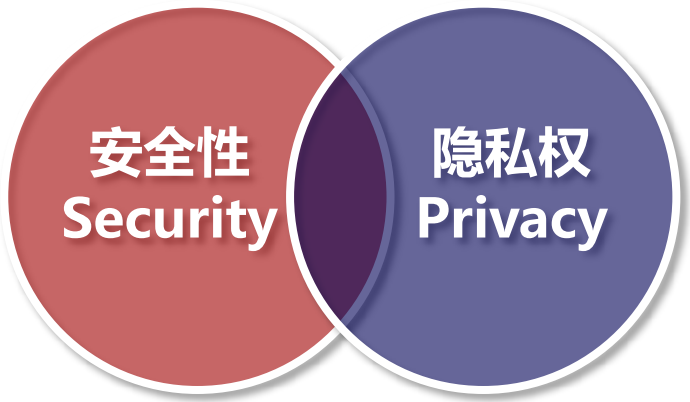
Clause	Additional Security Control Requirement
6	**CLD.6.3.1** Shared roles and responsibilities within a cloud computing environment
8	**CLD.8.1.5** Removal of cloud service customer assets
9	**CLD.9.5.1** Segregation in virtual computing environments **CLD.9.5.2** Virtual machine hardening
12	**CLD.12.1.5** Administrator's operational security **CLD.12.4.5** Monitoring of Cloud Services
13	**CLD.13.1.4** Alignment of security management for virtual and physical networks
	7

Data security and privacy 数据安全性与隐私权

观点1

数据安全

观点2



数据安全

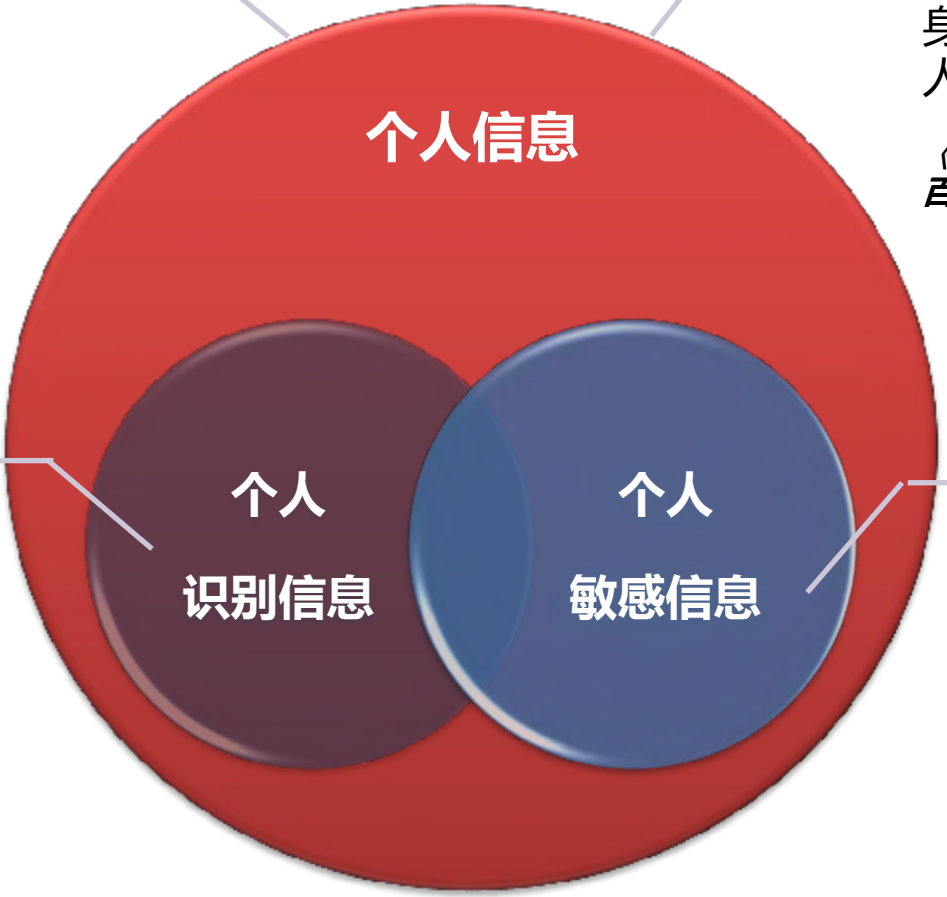
个人信息、个人可识别信息和个人隐私信息

个人信息：指与特定自然人身份或活动相关的信息，包括可用于识别出特定自然人身份的信息，以及体现特定自然人活动的信息。

《个人信息安全规范》

公民个人信息：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。

《中华人民共和国刑法》第二百五十三条之一



个人识别信息（PII）：任何可用于识别自然人，或者是可能与自然人存在直接或间接关联的信息。

《ISO/IEC29100:2011》

个人敏感信息：指一旦遭到非授权泄露或修改，会对自然人权益带来重大风险的个人信息。

《个人信息安全规范》

公民个人信息

- **公民个人信息**：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、账号密码、财产状况、行踪轨迹等。

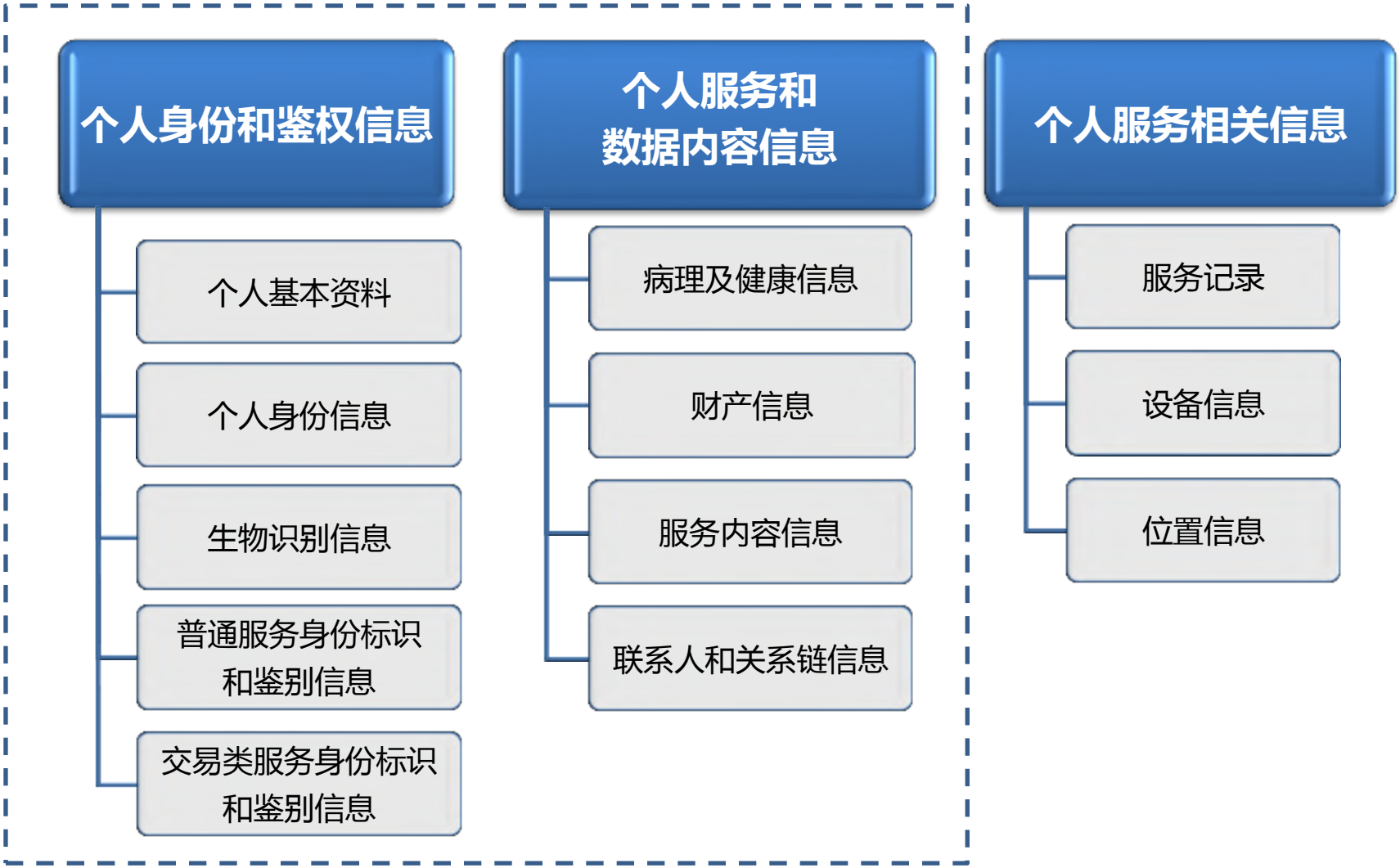
《中华人民共和国刑法》第二百五十三条之一

Personally Identifiable Information (PII) 个人可识别信息

- 弱势人群的年龄和特殊需要
- 关于犯罪行为的指控
- 接受健康卫生服务期间采集的任何信息
- 银行账户或信用卡卡号
- 生物辨识信息
- 信用卡报告
- 刑事定罪或裁决的违法行为
- 刑事侦查报告
- 客户编号
- 出生日期
- 诊断信息
- 伤残信息
- 医药费
- 员工薪资和人力资源档案
- 财务状况
- 性别
- GPS定位
- GPS轨迹
- 家庭住址
- IP地址
- 来源于通信系统的定位
- 病史
- 姓名
- 国家相关的辨识码（如：护照编号）
- 个人Email地址
- 个人识别码（PIN）或口令
- 根据互联网网站访问记录所知的个人兴趣爱好
- 个人行为档案
- 个人电话号码
- 可用于辨识某自然人的照片或视频
- 产品或服务偏好
- 种族或民族本源
- 宗教信仰或哲学信仰
- 性取向
- 工会成员资格
- 物业账单/公共设施账单

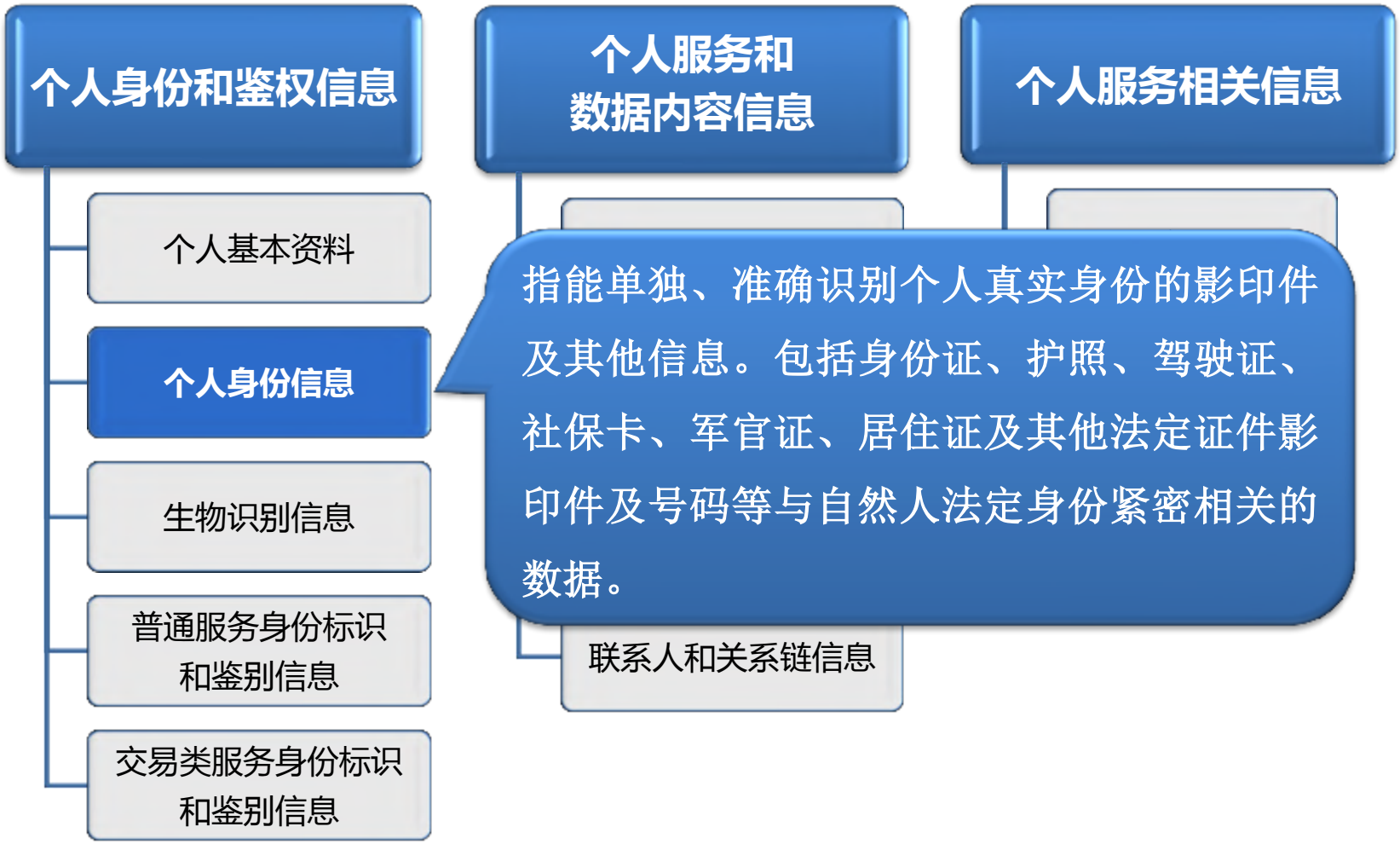
可识别的自然人的属性 – ISO/IEC 29100:2011

个人身份与个人敏感信息



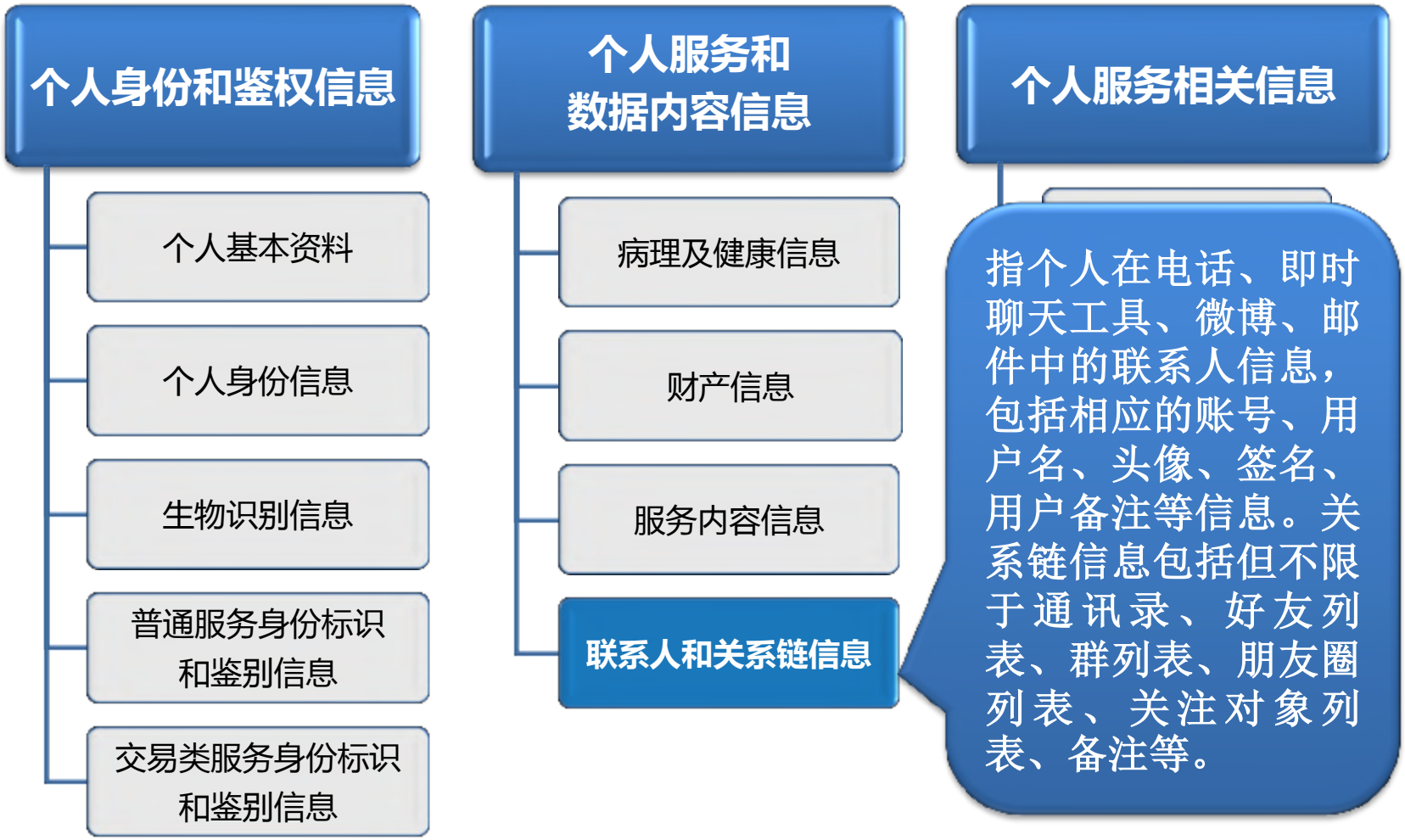
个人信息安全规范（征求意见稿）

个人身份与鉴权信息



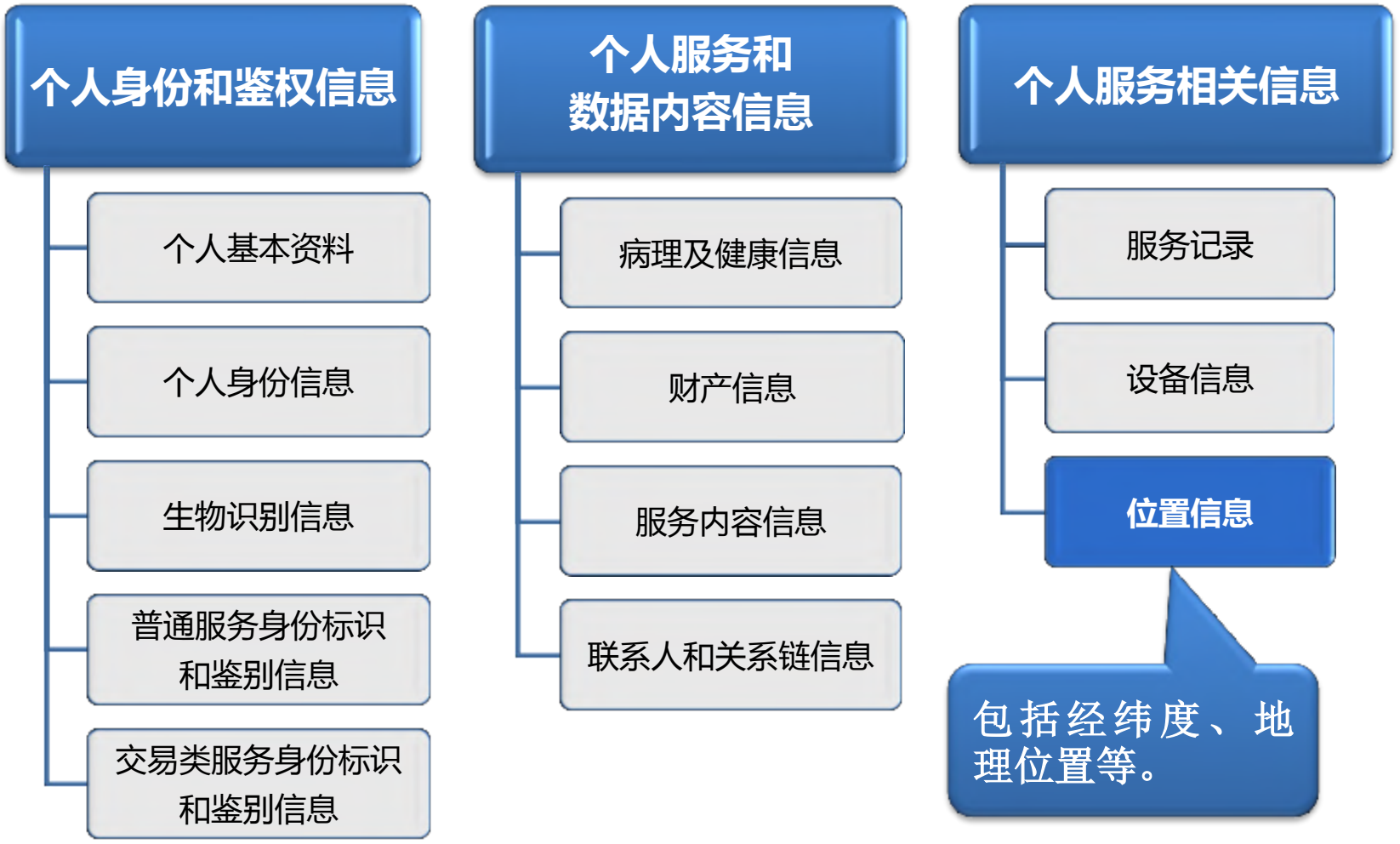
个人信息安全规范（征求意见稿）

个人身份和数据内容信息



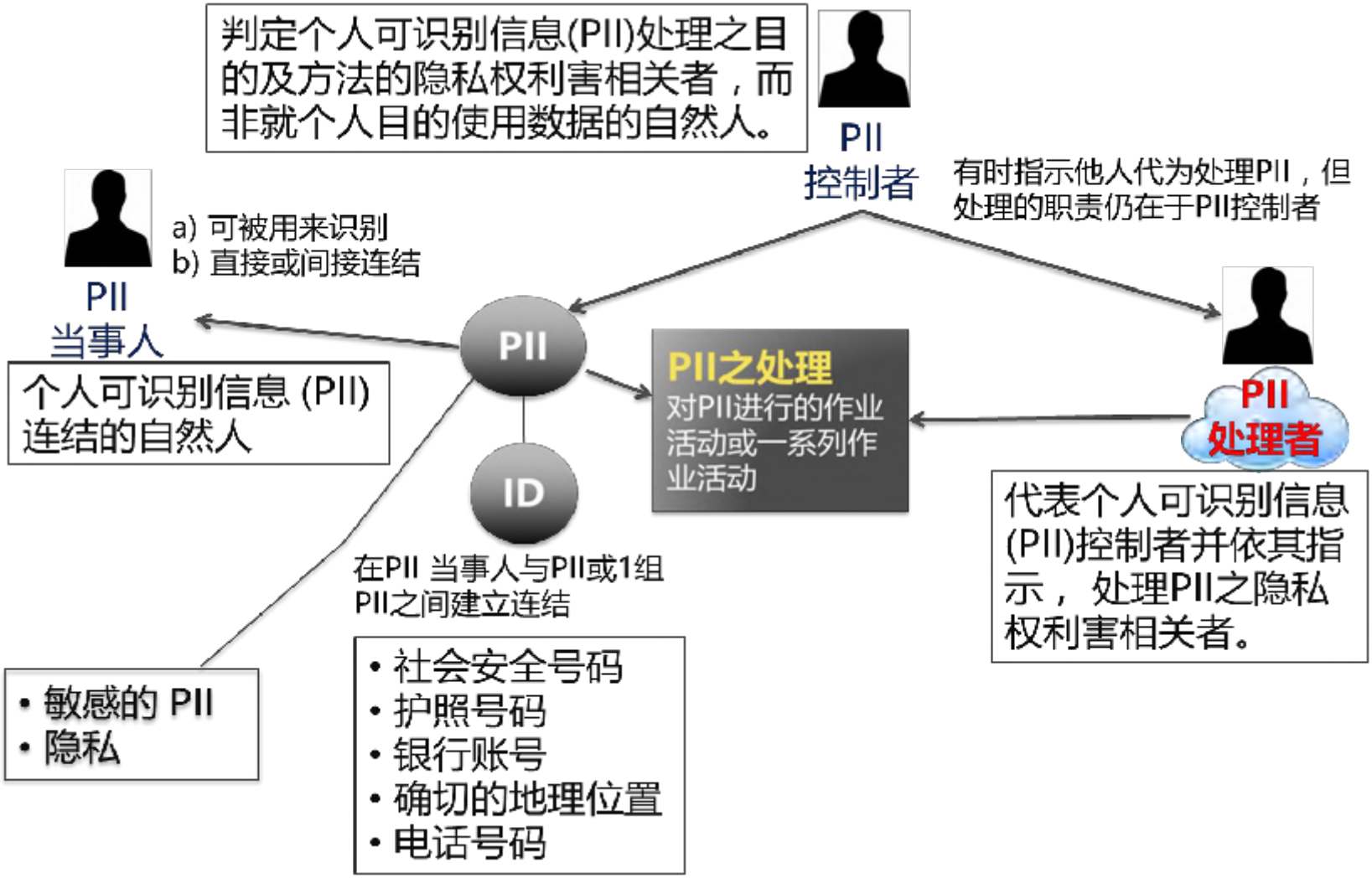
个人信息安全规范（征求意见稿）

个人服务相关信息



个人信息安全规范（征求意见稿）

PII信息处理的相关主体



个人信息的全生命周期保护

Collection
采集

Transfer
传输

Use
使用

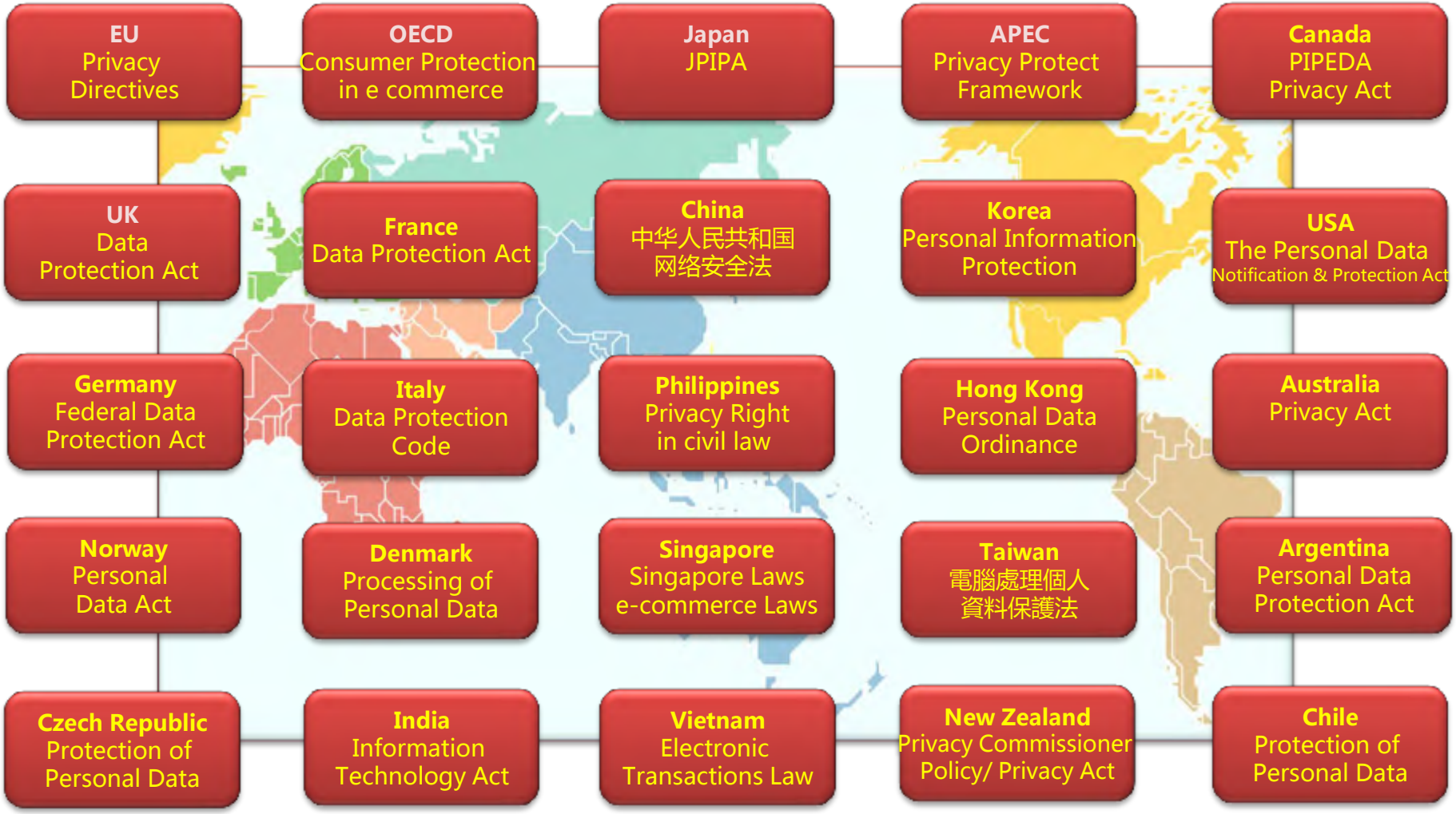
Storage
存储

Disposal
销毁

我国云服务面临的隐私安全挑战

- 互联网应用出于商业目的大量搜集用户信息；
- 我国缺乏对个人隐私保护的法律法规；
- 云供应商的安全防护水平参差不齐，且对客户不透明；
- 云供应商对保护用户隐私信息的重视不够；
- 发展大数据业务与用户隐私保护的矛盾：信息的收集、分享和使用；
- 缺乏个人信息泄露、调查、通知和应对机制。

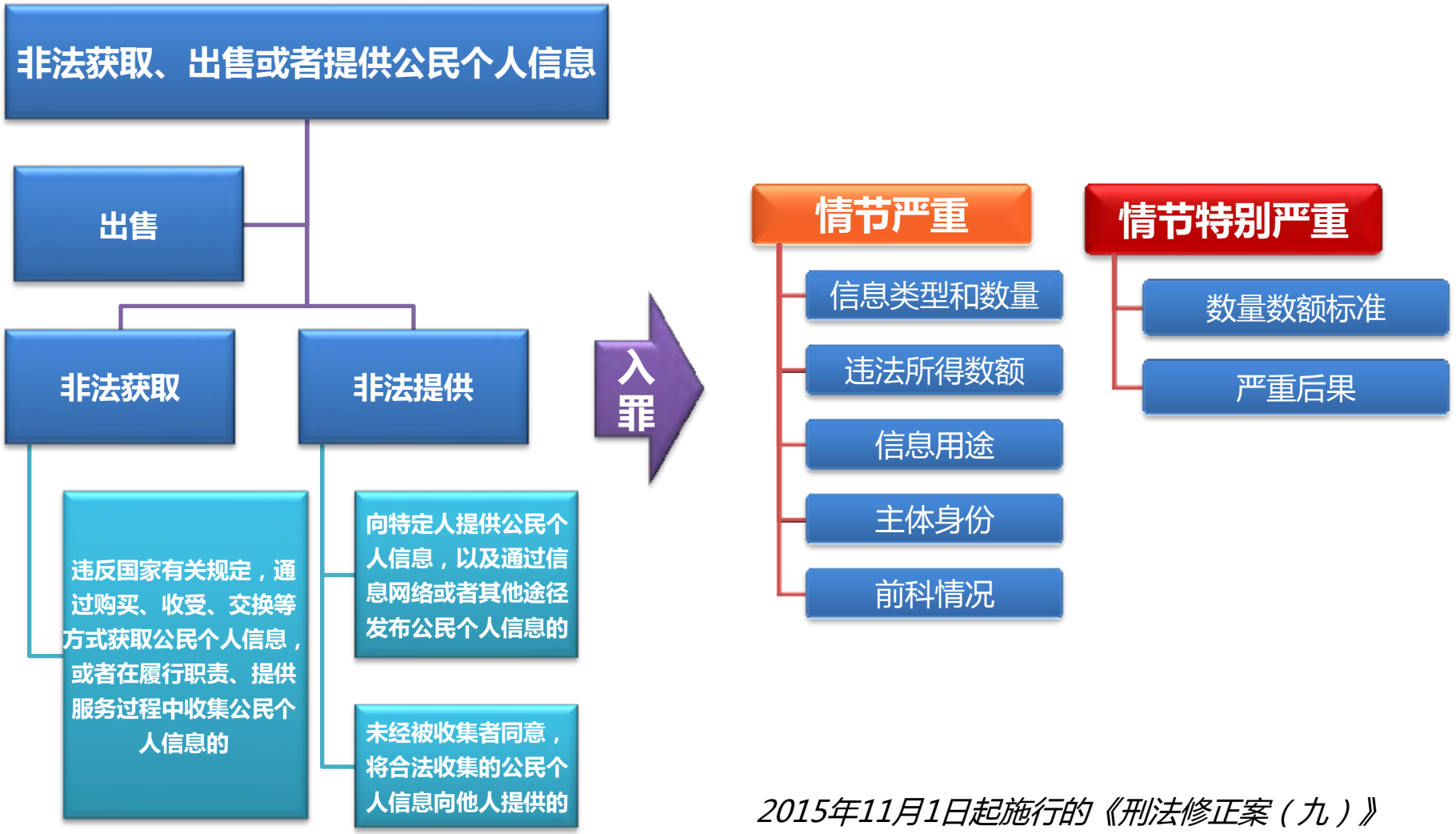
隐私保护已是全球共识


EU
Privacy
Directives
OECD
Consumer Protection
in e commerce
Japan
JPIPA
APEC
Privacy Protect
Framework
Canada
PIPEDA
Privacy Act
UK
Data
Protection Act
France
Data Protection Act
China
中华人民共和国
网络安全法
Korea
Personal Information
Protection
USA
The Personal Data
Notification & Protection Act
Germany
Federal Data
Protection Act
Italy
Data Protection
Code
Philippines
Privacy Right
in civil law
Hong Kong
Personal Data
Ordinance
Australia
Privacy Act
Norway
Personal
Data Act
Denmark
Processing of
Personal Data
Singapore
Singapore Laws
e-commerce Laws
Taiwan
電腦處理個人
資料保護法
Argentina
Personal Data
Protection Act
Czech Republic
Protection of
Personal Data
India
Information
Technology Act
Vietnam
Electronic
Transactions Law
New Zealand
Privacy Commissioner
Policy/ Privacy Act
Chile
Protection of
Personal Data

乐购集团的信息泄密巨额罚款

2016年11月，乐购银行承认有超过9000名客户的账户存款被盗，乐购银行将赔偿直接损失250万英镑，同时根据欧盟《通用数据保护条例》(GDPR) 的规定，乐购集团或将面临19亿英镑的罚款。

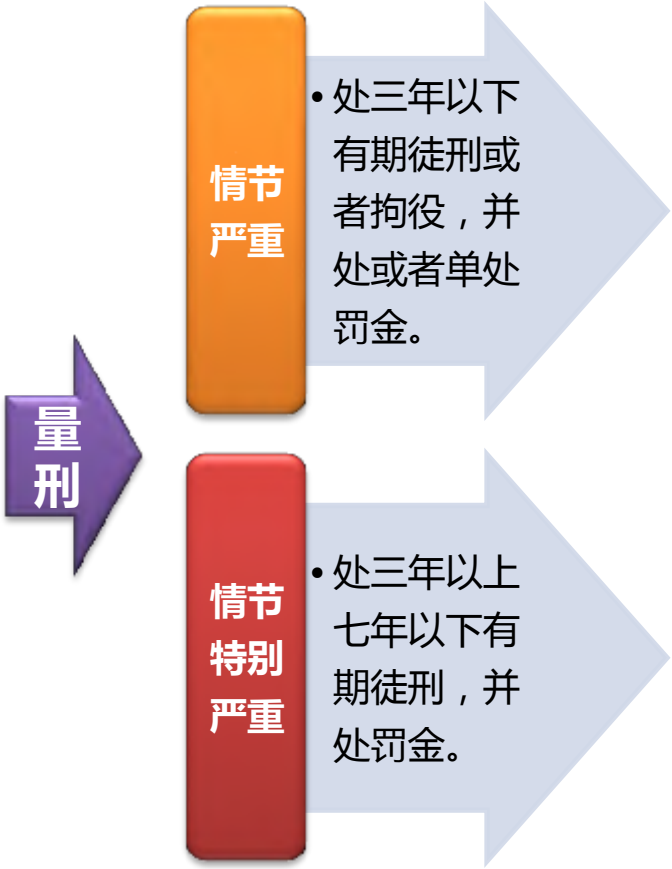
个人信息犯罪的刑事处罚



2015年11月1日起施行的《刑法修正案（九）》

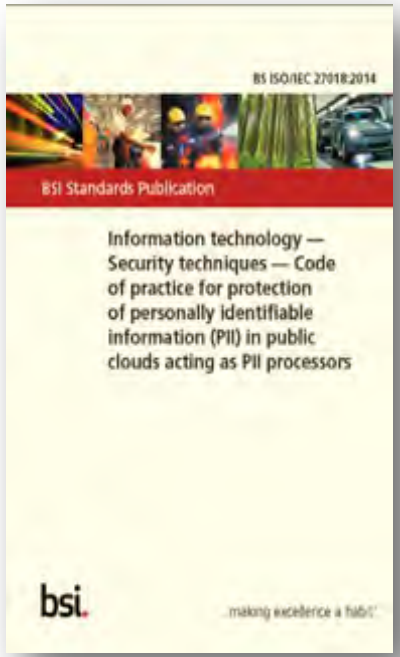
个人信息犯罪的刑事处罚

情节严重	情节特别严重
非法获取、出售或者提供**行踪轨迹信息、通信内容、征信信息、财产信息**50条以上的；	500条以上
非法获取、出售或者提供**住宿信息、通信记录、健康生理信息、交易信息**等其他可能影响人身、财产安全的公民个人信息500条以上的；	5000条以上
非法获取、出售或者提供上述两项规定以外的公民个人信息5000条以上的；	50000条以上
违法所得5000元以上的；	50000元以上
为合法经营活动而非法购买、收受公民个人信息获利50000元以上的；	造成被害人死亡、重伤、精神失常或者被绑架等严重后果的；造成重大经济损失或者恶劣社会影响的。



ISO/IEC 27018-公有云个人数据保护的国际标准

- 第一个聚焦公有云环境下个人数据保护的国际标准。
- 继承了ISO27001和ISO29100中的云服务供应商处理个人信息的内容，包括合规要求、合同条款、PII目的、PII披露、安全控制以及PII生命周期管理。
- 帮助云服务供应商和客户通过合同及协议达成一致
- 促使公有云供应商将相关问题透明化，帮助客户选择安全和治理更好的云服务商。
- 向使用云服务的客户提供了一种行使审计和合规权利的机制.



Office 365 Windows Azure amazon web services Dropbox Ribose TKC グループ workday mimecast unified email management

ISO/IEC 27018:2014 的控制措施(16+25)

Additional guidance based on ISO/IEC 27002 ✚ ISO/IEC 29100 extended control set

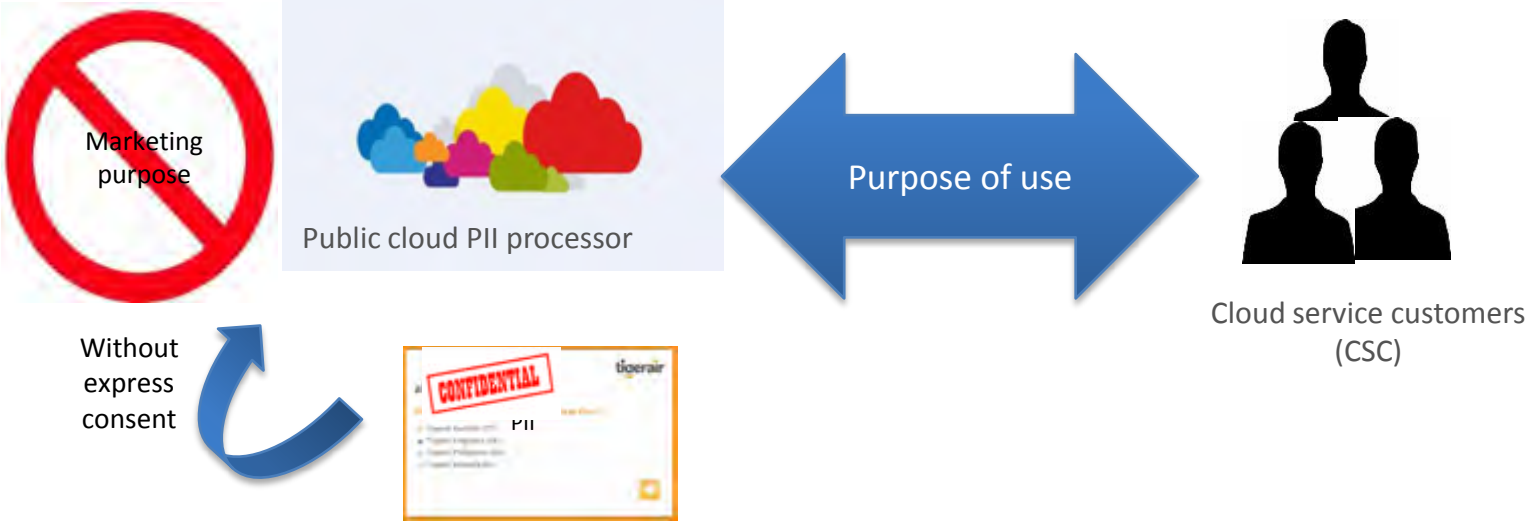
Clause	Security Domain	#of Control Guidance
5	Information security policies	1
6	Organization of info. security	1
7	Human resource security	1
8	Responsibility for assets	n/a
9	Access control	3
10	Cryptography	1
11	Physical and environmental security	1
12	Operations security	4
13	Communications security	1
14	System acquisition, development & maintenance	n/a
15	Supplier relationships	n/a
16	Information security incident management	2
17	Information security aspects of BCM	n/a
18	Compliance	1
		16

Additional controls - Privacy principles of ISO/IEC 29100	#of Control Guidance
A.1 Consent and choice	1
A.2 Purpose legitimacy and specification	2
A.3 Collection limitation	n/a
A.4 Data minimization	1
A.5 Use, retention and disclosure limitation	2
A.6 Accuracy and quality	n/a
A.7 Openness, transparency and notice	1
A.8 Individual participation and access	n/a
A.9 Accountability	3
A.10 Information security	13
A.11 Privacy compliance	2
	25

ISO/IEC 27018 的控制要求举例

A.2.2 公有云PII处理者的商业用途

Type of cloud service	Aplly
IaaS	
PaaS	
SaaS	



PII processed under a contract should not be used by the public cloud PII processor for the purposes of marketing and advertising without express consent. Such consent should not be a condition of receiving the service.

应基于合同要求（而不是未经明确同意的营销和广告目的）来处理PII。这种同意不应是接受服务的条件。

ISO/IEC 27018 的控制要求举例

A.10.4 保护离场存储介质中的数据

Type of cloud service	Aplly
IaaS	
PaaS	
SaaS	

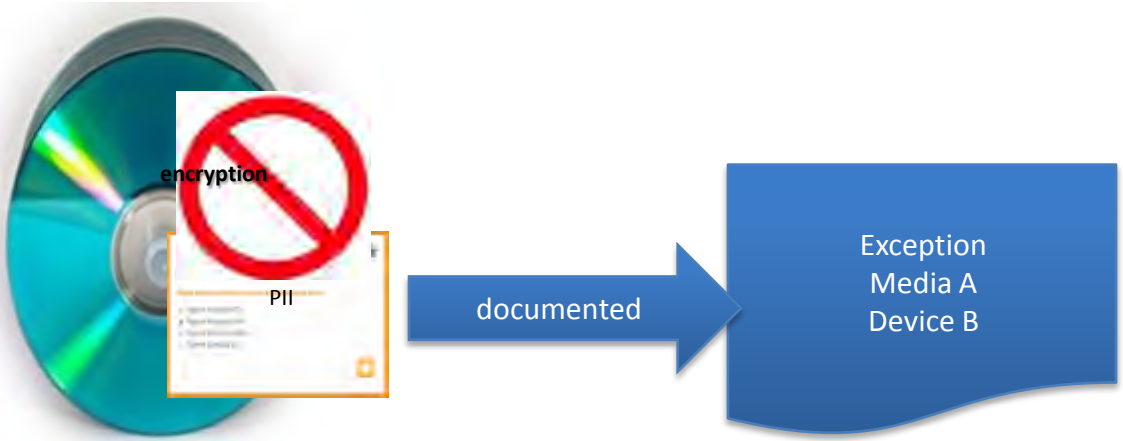
PII on media leaving the organization' s premises should be subject to an authorization procedure and should not be accessible to anyone other than authorized personnel (e.g. by encrypting the data concerned).

对于离开组织场所的介质中的PII，应遵循授权规程，并避免让任何非授权人员访问（如：通过对相关数据进行加密）。

ISO/IEC 27018 的控制要求举例

A.10.5 使用未加密的移动介质和设备

Type of cloud service	Aplly
IaaS	
PaaS	
SaaS	



Portable physical media and portable devices that do not permit encryption should not be used except where it is unavoidable, and any use of such portable media and devices should be documented.

除非无法避免，否则不应使用无法加密的移动介质和设备，且任何使用移动介质和设备的行为应被记录。

1 互联网时代全球信息安全风险动态及趋势

2 云服务安全与隐私保护国际标准介绍

3 隐私保护方案制定与实施

根据云服务特性选择适用的云安全标准

Cloud Service Customers (CSC)

合同/协议

Cloud service Providers (CSP)

上传/下载信息

管理

Privacy law

IAAS 处理
Infrastructure-as-a-service

PAAS
Platform-as-a-service

SAAS
Software-as-a-service

PII处理的范例包括 (但不局限于) PII的搜集、储存、修改、检索、咨询、揭露、匿名化、拟匿名化、传播或以其他方法使其可利用、删除或销毁。

ISO/IEC 27018

证明其处理操作符合隐私保护法律法规的要求

企业如何选择适合的云安全国际标准方案

一、云安全国际标准方案概述

标准	是否可认证	是否需先通过ISO/IEC 27001认证	认证对象	云服务模式	云部署模式
ISO/IEC 27018	是	是	依据合同及协议要求，处理个人信息的云服务提供商	IaaS / PaaS / SaaS	公有云
ISO/IEC 27017	是	是	云服务客户、云服务提供商	IaaS / PaaS / SaaS	适用于任何云部署模式

二、云安全国际标准内容概述

标准	对法律法规的关注	对技术手段的关注	实施难度	控制域	信息安全控制措施涵盖范围及要求
ISO/IEC 27018	多	少	中	25	关注于隐私保护相关的控制措施，在ISO/IEC 27002及ISO 29100基础上补充41个控制措施要求。
ISO/IEC 27017	中等	中等	中	14	在ISO/IEC 27002基础上补充44个控制措施要求。

个人信息保护的风险管理流程

CSP依据ISO/IEC 27018建立PII保护框架

ISO/IEC 27001 Control	Control Requirement
A.13.2.1 Information transfer policies and procedures	Formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities.

ISO/IEC 27002 Implementation Guidance (13.2.1)

a) procedures designed to protect transferred information from interception, copying, modification, mis-routing and destruction;

b) procedures for the detection of and protection against malware that may be transmitted through the use of electronic communications (see 12.2.1);

c) procedures for protecting communicated sensitive electronic information that is in the form of an attachment;

ISO/IEC 27018 Implementation Guidance (13.2.1)	Additional controls based on privacy principles of ISO/IEC 29100
Whenever physical media are used for information transfer, a system should be put in place to record incoming and outgoing physical media containing PII, including the type of physical media, the authorized sender/recipients, the date and time, and the number of physical media. Where possible, cloud service customers should be asked to put additional measures in place (such as encryption) to ensure that the data can only be accessed at the point of destination and not en route.	**A.10.6 Encryption of PII transmitted over public data-transmission networks** In some cases, e.g. the exchange of e-mail, the inherent characteristics of public data-transmission network systems might require that some header or traffic data be exposed for effective transmission.

making excellence a habit!

让追求卓越成为一种习惯

Gdevops

全球敏捷运维峰会

THANK YOU！