数据和隐私保护

Data & Privacy Protection


facebook
Google

Facebook

数据分析公司Cambridge Analytica未经用户许可，盗用5千万用户个人资料，影响2016总统大选

Facebook股价重挫超过6%，两天之内跌掉11.4%，蒸发600亿美元

将遭到2兆美元的天价罚款

2011年 比利时联邦法院 罚金15W EU$ 街景服务
2012年11月美国Federal Trade Commission 罚金 2250W Safari
2013年4月德国 罚金18.9W StreetView
2013年11月美国 37个州政府和哥伦比亚特区政府 罚金1700W Safari
2013年12月西班牙 罚金123W 产品整合用户信息
2014年1月法国CNIL 罚金20W Gmail & Google map
2014年4月 意大利DPA 罚金140W 街景拍摄车
2018年4月 美国FTC介入 Youtube涉嫌违反COPPA 面临数十亿美元罚金

数据和隐私保护 Data & Privacy Protection

百度董事长兼CEO李彦宏表示，“我想中国人可以更加开放，对隐私问题没有那么敏感，如果他们愿意用*隐私交换便捷性*，很多情况下他们是愿意的，那我们就可以用数据做一些事情。”

爱尔兰

《2018年数据保护法案》

中国

- 《网络安全法 》实施
- GB/T 35273《个人信息安全规范》获批发布

新加坡

通过《网络安全法案》

法国

法国国民议会通过新《数据保护法草案》

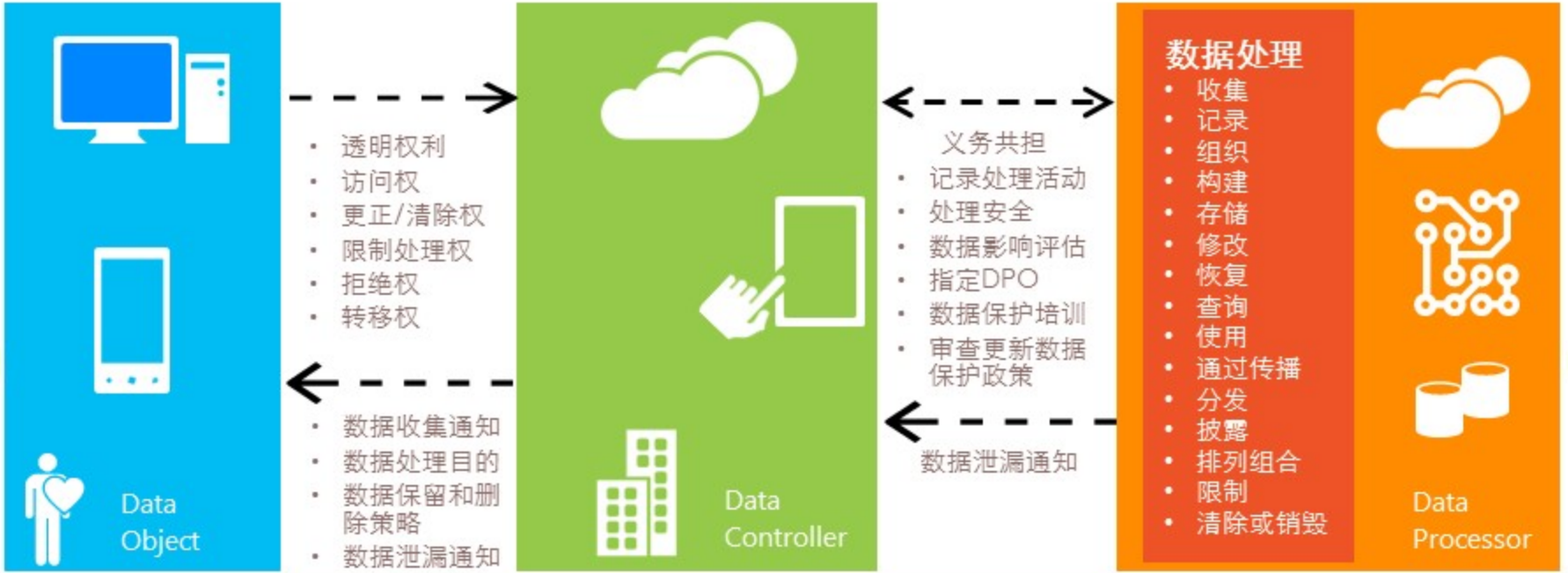

Guideline on the Protection of Privacy and Transborder Flows of Personal Data 1980
OECD Privacy Framework 2013
GLBA
COPPA
FERPA
HIPPA
Privacy Protection Act
ECPA
The Fair Credit Reporting Act
ID Theft Red Flags Rule
Privacy Shield
Elements of Effective Self Regulation for Protection of Privacy
Data Protection Act
EU DPD 1995
Data Retention Directive
EU Privacy and Electric Communication Directive
GDPR
Draft of Data Protection Act
The Russian Federal Law on Personal Data (No. 152-FZ)
Cyber Security Law
Personal information Protection Act
Personal Information Protection Act
Personal Data Protection Act
Australian Federal Privacy Act 1988
Protection of Personal Data Law 2001
APEC Privacy Framework
Australian Federal Privacy Act 1988
Privacy Act

数据和隐私保护Data & Privacy Protection


General Data
Protection Regulation

数据和隐私保护 Data & Privacy Protection

数据和隐私保护 Data & Privacy Protection



数据处理原则

1.合法、公平和透明 2.目的限制 3.最小范围 4.准确性 5.存储期限限制 6.安全性 7.责任

数据和隐私保护Data & Privacy Protection

数据和隐私保护项目

数据分析

隐私影响评估

数据保护措施设计

数据和隐私保护 Data & Privacy Protection

前期调研
- 了解背景
- 内部沟通
- 资料调阅

访谈
- 编制访谈计划
- 编制访谈提纲
- 访谈
- 编制访谈纪要

补充访谈
- 补充访谈
- 更新纪要

差距分析
- 差距分析
- 成熟度评估
- 分析报告

数据和隐私保护Data & Privacy Protection

数据和隐私保护Data & Privacy Protection

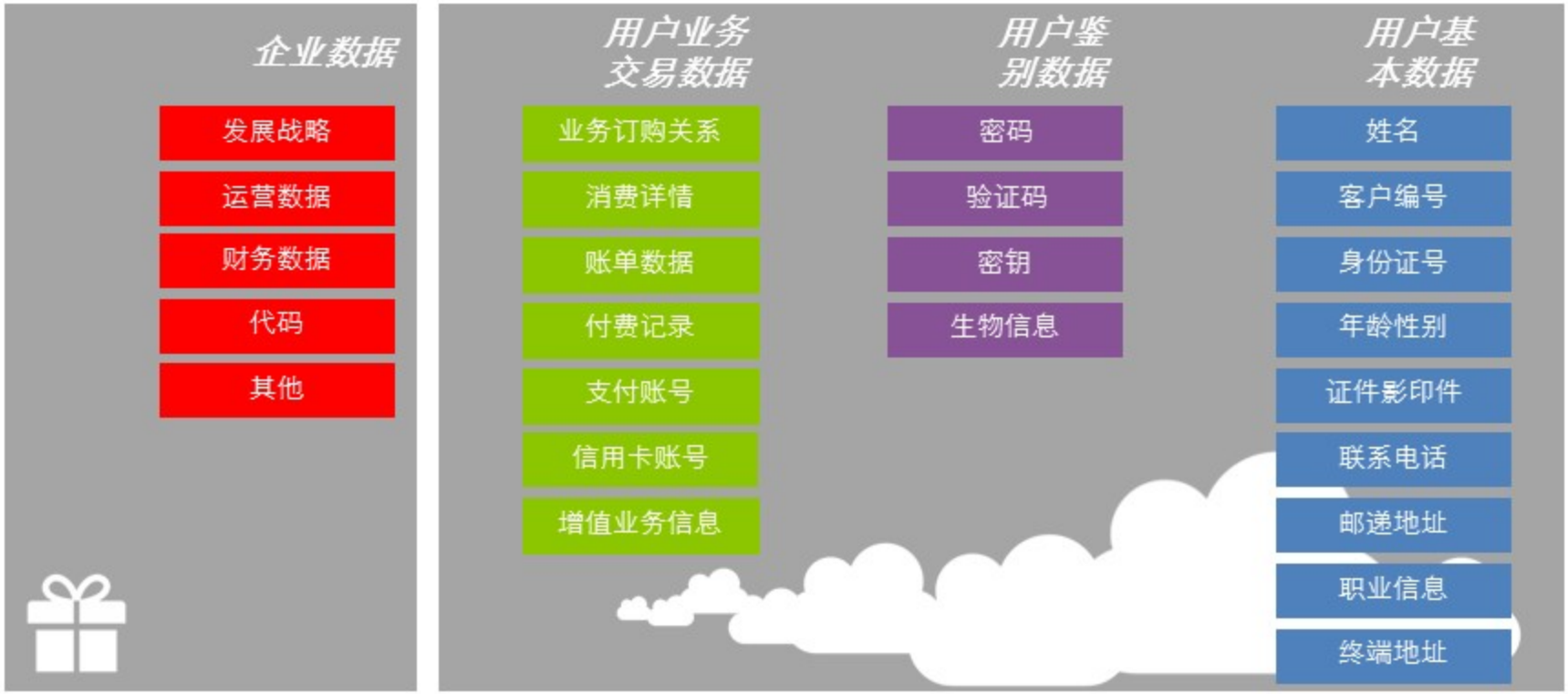
数据和隐私保护项目

数据分析

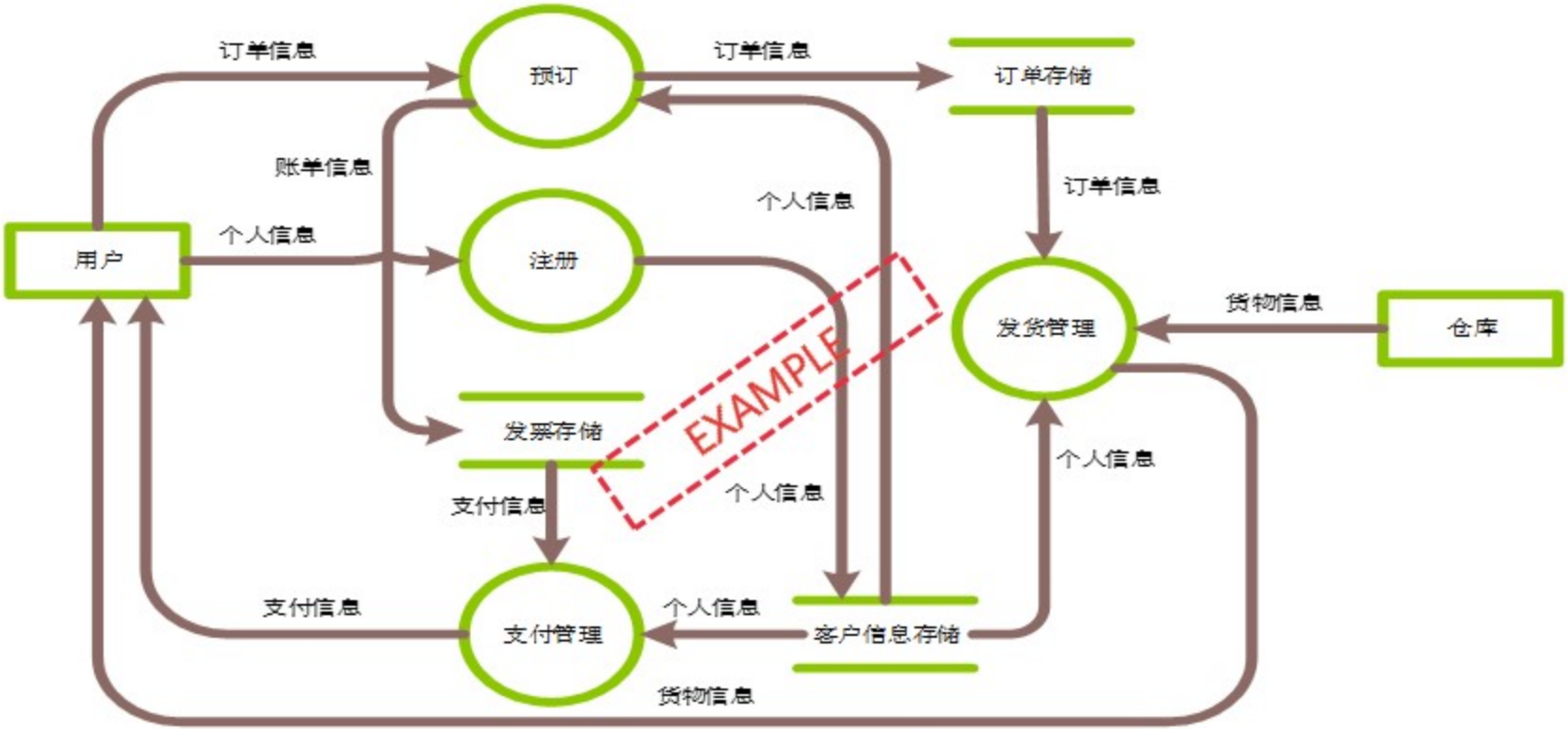
隐私影响评估

数据保护措施设计

数据和隐私保护 Data & Privacy Protection



数据和隐私保护 Data & Privacy Protection



数据和隐私保护 Data & Privacy Protection

基于数据生命周期的数据清单

序号	数据类型	涉及的系统组件	收集			存储		使用		披露		销毁
			目的	方法	控制措施	存储位置	控制措施	使用方式	控制措施	披露对象	控制措施	控制措施

EXAMPLE

数据和隐私保护Data & Privacy Protection

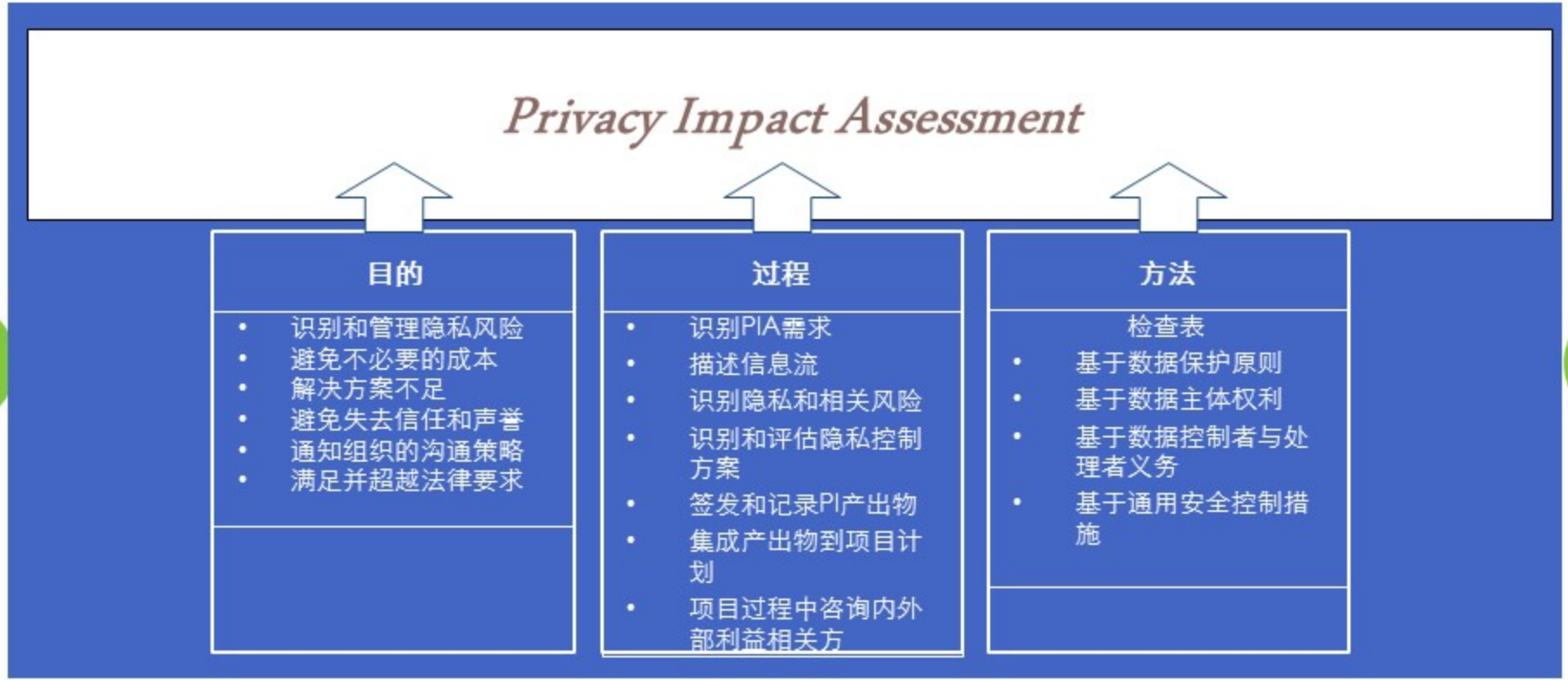
数据和隐私保护项目

数据分析

隐私影响评估

数据保护措施设计

数据和隐私保护Data & Privacy Protection



数据和隐私保护Data & Privacy Protection

Fundamental Principals:
分析保证遵守基本原则的控制措施评估控制措施，

- 确保数据处置的合理性和必要性
  - 目的的解释
  - 合法性的解释
  - 数据最小化的解释
  - 数据质量
  - 存储期限
  - 安全控制

- 评估保护数据主体权利的控制措施
  - 数据主体控制/访问数据的权利
  - 获得同意的权利
  - 控制访问权限和数据可移植性
  - 纠正和删除的权利
  - 限制处理的权利
  - 通过合同管理处理者的权利
  - 数据转移控制的权利

- 数据必要性（数据最小化）
- 使用，保留和处置
- 向第三方披露并转发
- 选择和同意
- 获得和个人权利
- 数据完整性和质量
- 安全
- 透明度

数据和隐私保护Data & Privacy Protection

隐私影响评估报告

- 描述设想的处理操作和处理目的
- 结论
- 控制清单-数据保护原则
- 控制清单-安全控制措施（组织治理，逻辑安全、物理安全）
- 风险地图(风险源，威胁，事件，风险级别)
- 改进计划

数据和隐私保护Data & Privacy Protection

数据和隐私保护项目

数据分析

隐私影响评估

数据保护措施设计

数据和隐私保护 Data & Privacy Protection

- NIST
- PCI DSS
- BS10012
- ISO/IEC
- IAPP
- TRUSTe
- AICPA

数据和隐私保护 Data & Privacy Protection

技术细则

ISO/IEC 29101:2013
Privacy architecture framework

ISO/IEC 29134:2017
Requirements for partially anonymous,

ISO/IEC DIS 20889
Security Privacy enhancing data de-identification techniques

技术指导

ISO/IEC CD 27550
Security techniques -- Privacy engineering

ISO/IEC CD 29184
Guidelines for online privacy notices and consent

ISO/IEC 29190:2015
Security techniques -- Privacy capability assessment mode

最佳实践

ISO/IEC 29134:2017
Guidelines for privacy impact assessment

ISO/IEC CD 27552
Enhancement to ISO/IEC 27001 for privacy management -- Requirements

ISO/IEC 29151:2017
Code of practice for personally identifiable information protection

ISO/IEC 27018:2014
Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

Base on **ISO/IEC 27002:2013** Code of practice for information security controls

通用框架

ISO/IEC 29100:2011
Information technology -- Security techniques -- Privacy framework

数据和隐私保护 Data & Privacy Protection

ISO/IEC 27018:2014

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

ISO/IEC 27002:2013

Code of practice for information security controls

14 domains

35 objects

114 controls

Implementation guidance Provide more detail information to support the implementation of the control and meeting the objectives

Other information Provides further information that may need to be considered, such as legal considerations and references to other standards

+ 16

ISO/IEC 29100:2011

Information technology -- Security techniques -- Privacy framework

11 Principals

Control define the specific control statement to satisfy the control objective

Implementation guidance Provide more detail information to support the implementation of the control and meeting the objectives

+ 25

数据和隐私保护 Data & Privacy Protection

- A.1 Consent and Choice
- A.2 Purpose legitimacy and specification
- A.3 Collection limitation
- A.4 Data minimization
- A.5 Use, retention and disclosure limitation
- A.6 Accuracy and quality
- A.7 Openness, transparency and notice
- A.8 Individual participation and access
- A.9 Accountability
- A.10 Information Security
- A.11 Privacy Compliance

数据和隐私保护 Data & Privacy Protection

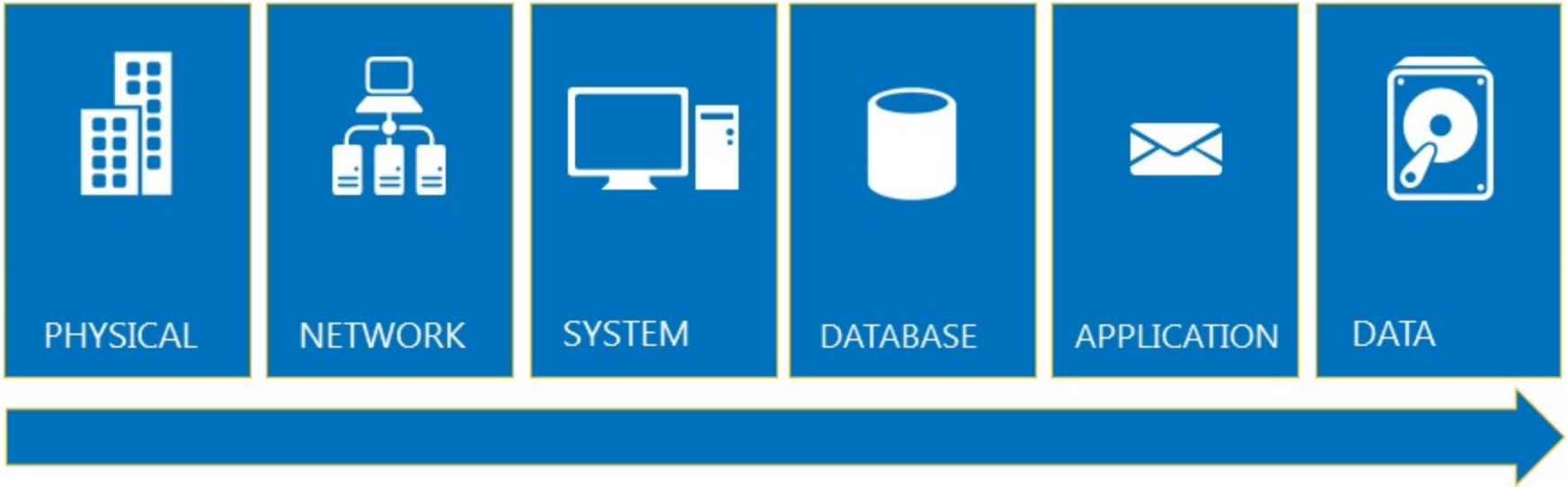
6 改进个人资料管理系统
6.1 改正与预防措施
6.2 持续改进

3.1 建立与管理PIMS
3.2界定PIMS 适用范围及设定目标组织
3.3个人资料管理政策
3.4政策内容
3.6 资源提供

4.1责任的配置
4.1访问控制
4.1隐私事故的管理
4.1保留及处置
4.5 持续更新

5.1 内部审核
5.2 管理评审

数据和隐私保护 Data & Privacy Protection



数据和隐私保护 Data & Privacy Protection

Thanks

Data & Privacy Protection

宽恕　2018.04