金融科技企业信息安全风控实践分享

马寅龙

点融网信息安全合规专家

他们（新闻工作者）是社会这条大船上的“瞭望者”，瞭望的对象则是各种不利於大船顺利行驶的事物。

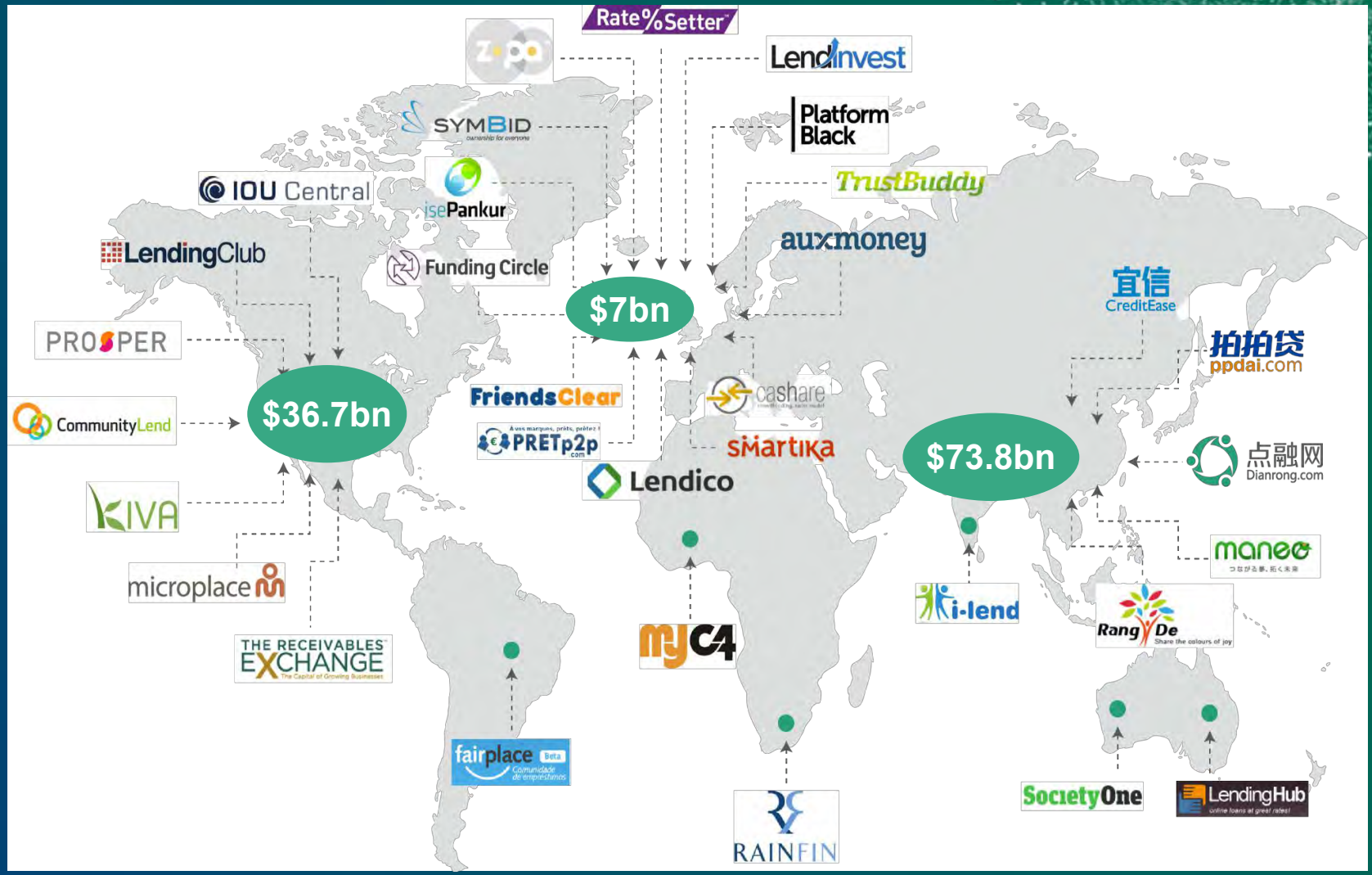
--普利策

互联网金融 – 风口与浪尖

全球市场规模

$5.73bn
2013 Loan

$117bn
2016 Loan Issuance

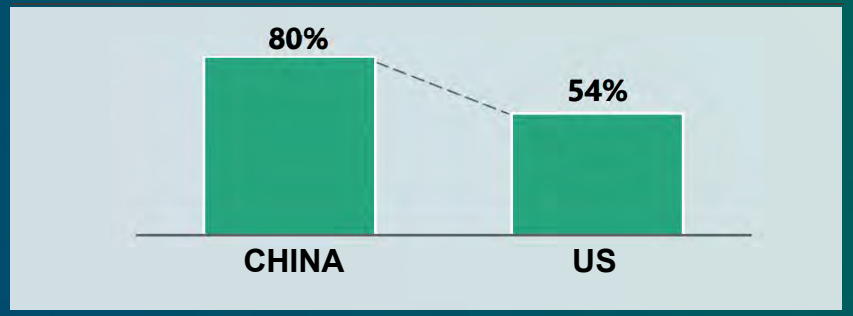


互联网金融 – 风口与浪尖

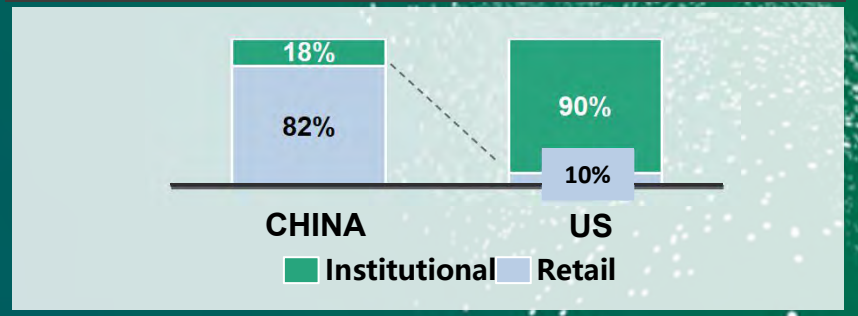
中国的市场机遇

- 强烈的投资需求
- 薄弱的融资支持
- 消费理念转型
- 金融科技的发展

存款占GDP的比例

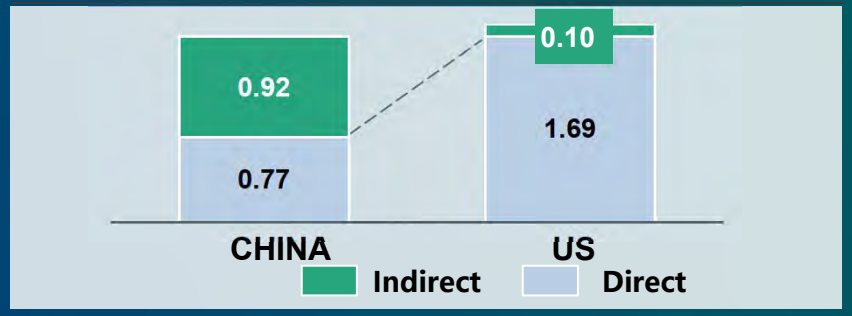


个人投资者 vs 机构投资者

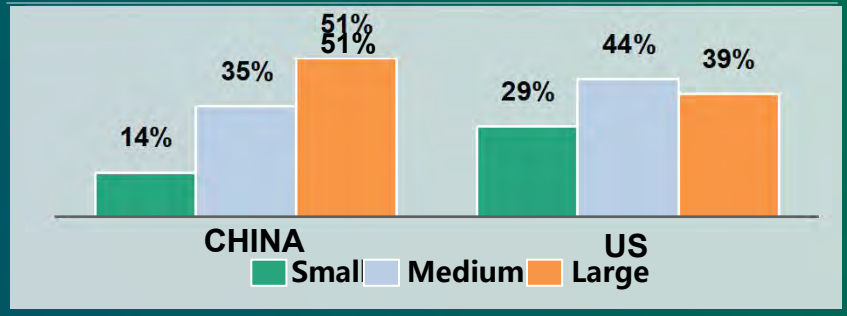


¥47 TN Investable wealth

直接融资 vs 间接融资



中小微企业的金融支持



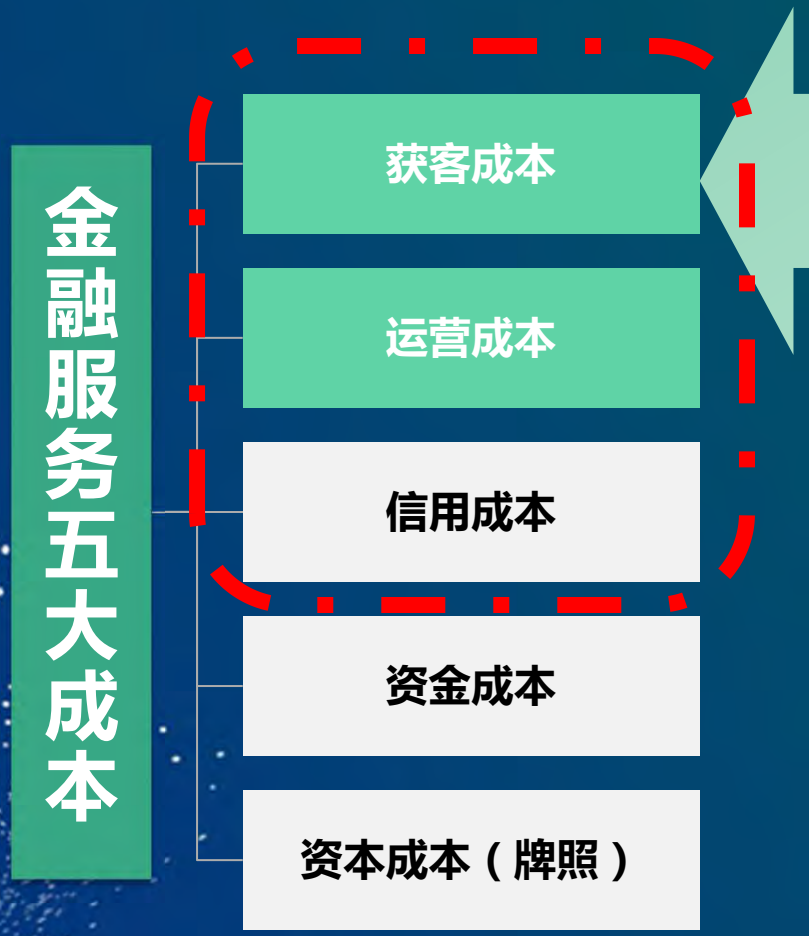
¥22 TN Financing Gap

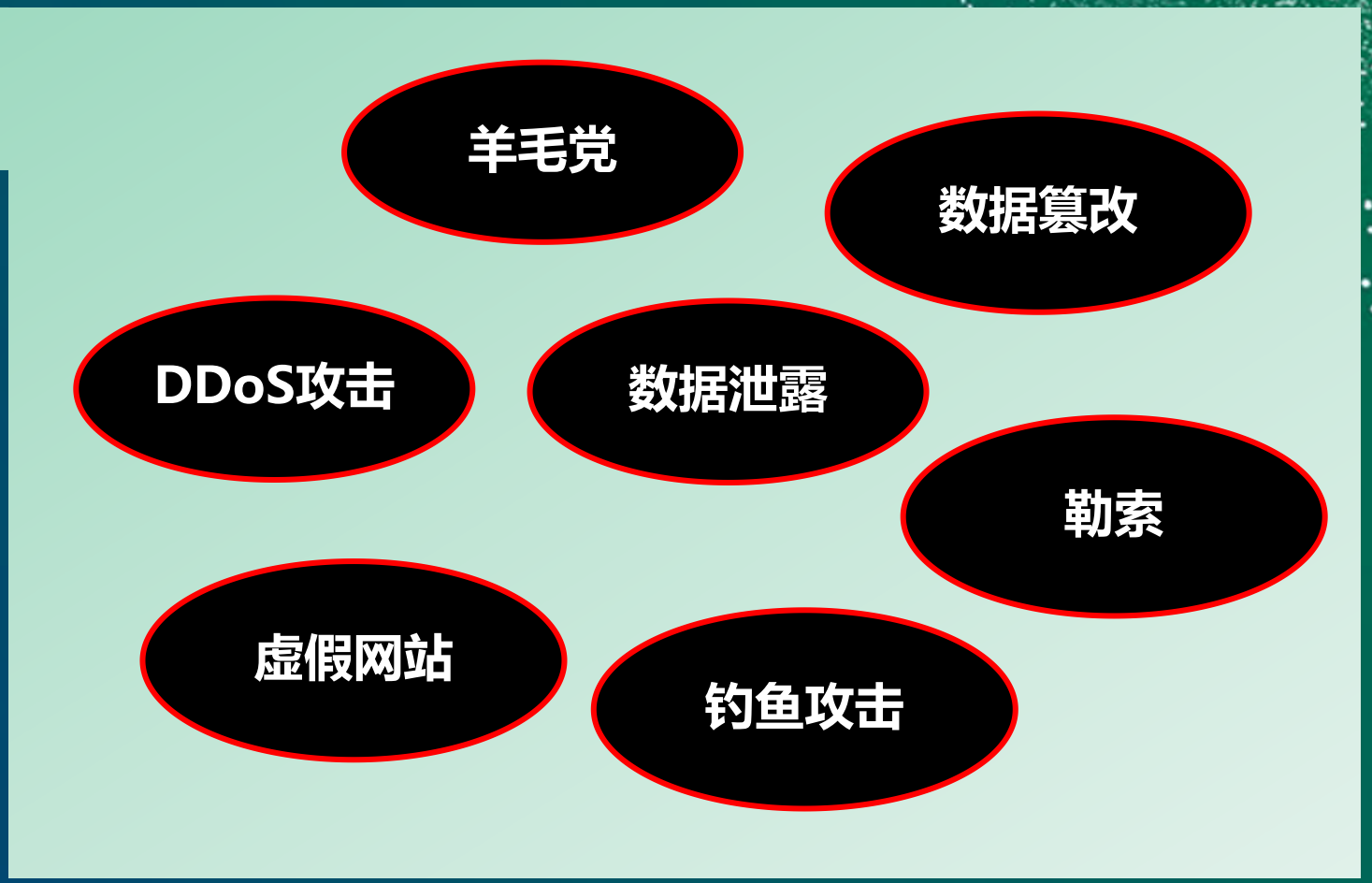
互联网金融 – 风口与浪尖

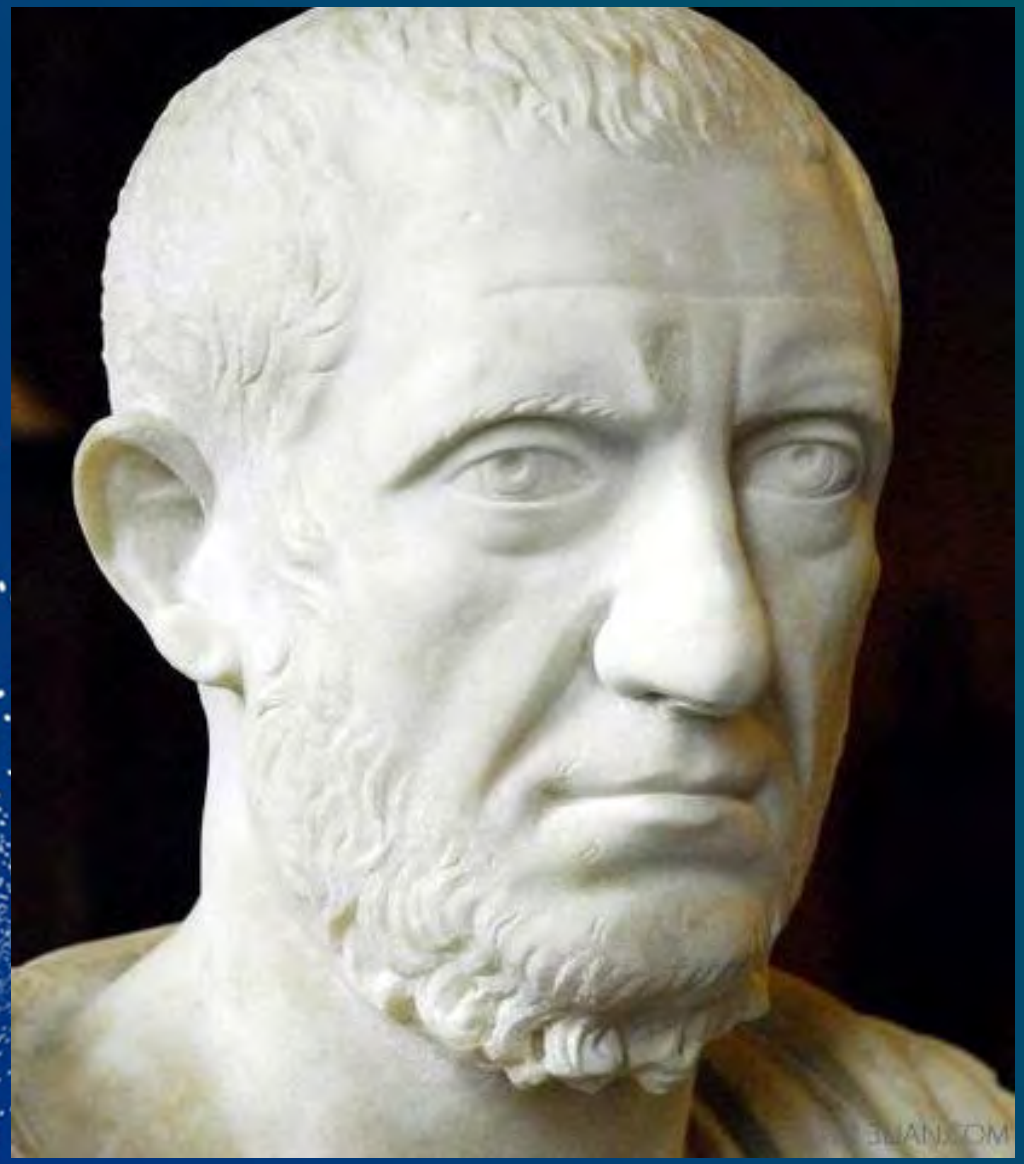
中国的互联网金融平台的一组数据

- 互联网金融平台数累计**11173**
- 互联网金融平台活跃用户数**6.27亿**
- 互联网支付累计交易金额**44万亿**
- 网络借贷金额**3万亿**
- 互联网众筹金额**400亿**
- 运营中互联网金融平台数**6928**
- 涉嫌违规互联网金融平台数**2420**
- Web漏洞数**950** / App漏洞数**150**
- 互联网金融网站攻击**75.8万次**
- 互联网金融仿冒网站**4320个**
- 受害人数 **7.5万人**

互联网金融 – 风口与浪尖


金融服务五大成本
获客成本
运营成本
信用成本
资金成本
资本成本（牌照）


羊毛党
数据篡改
DDoS攻击
数据泄露
勒索
虚假网站
钓鱼攻击



当你能够想你愿意想的东西，并且能够把你所想的东西说出来的时候，这是非常幸福的时候。

--塔西佗

金融科技企业为什么要做信息安全合规

合法经营要求

- 全国人民代表大会常务委员会于2016年11月7日正式发布了**《网络安全法》**，自2017年6月1日起施行。
- 2016年8月24日银监会联合四部委联合发布**《网络借贷信息中介机构业务活动管理暂行办法》**，明确提出了执行信息系统等级保护管理、灾备系统建设、客户信息保护、交易信息保存等要求。

对外业务合作要求

- 银监会2014-272号文对金融机构的外包工作提出了明确的管理要求，点融与各类银行机构有大量业务往来，如果不能满足这些要求，很多业务合作将会面临无法开展的困境。

控制内部风险的要求

- 公司业务开展严重依赖信息系统的稳定可靠，而近年来信息安全事件频发，为了有效保障业务的开展，必须通过有效的控制流程，防控信息安全风险的发生。

如何建立信息安全合规体系

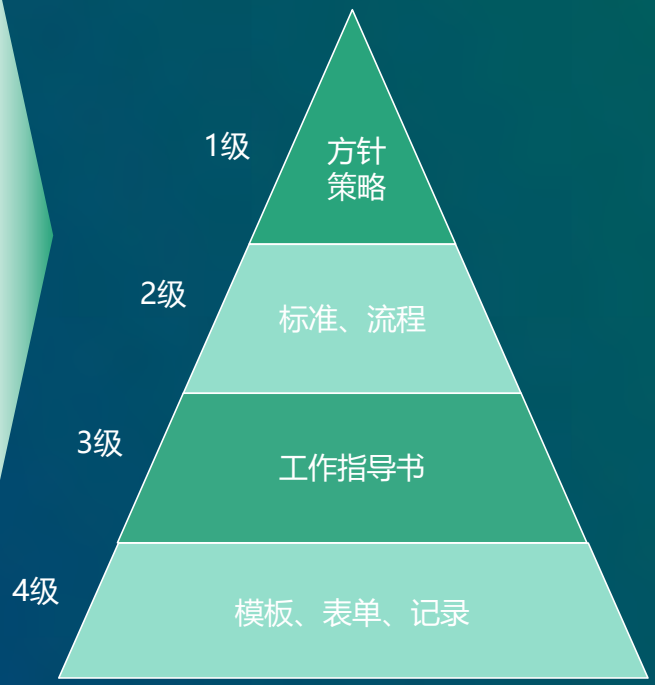
三级等保框架

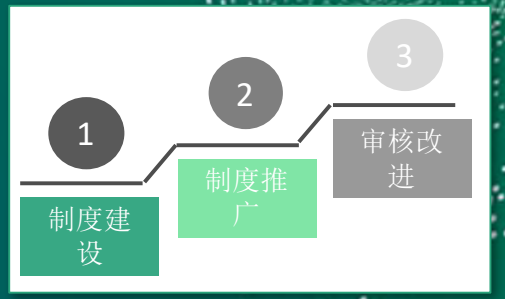
技术要求	物理安全	S 安全性	A 可用性	G 一般要求
	主机安全			
	网络安全			
	应用安全			
	数据安全			
管理要求	安全管理制度			
	安全组织架构			
	人员安全			
	系统建设安全			
	系统运维安全			

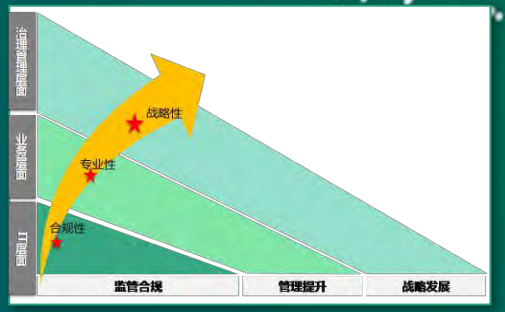
ISO27001 ISMS框架

A.5 信息安全策略					
A.6 信息安全组织					
A.7 人力资源安全					
A.8 资产管理					
A.9 访问控制	A.10 密码学	A.11 物理及环境安全	A.12 操作安全	A.13 通信安全	A.14 系统获取、开发与维护
A.15 供应商关系					
A.16 信息安全事件管理					
A.17 业务连续性管理的信息安全方面					
A.18 合规性					

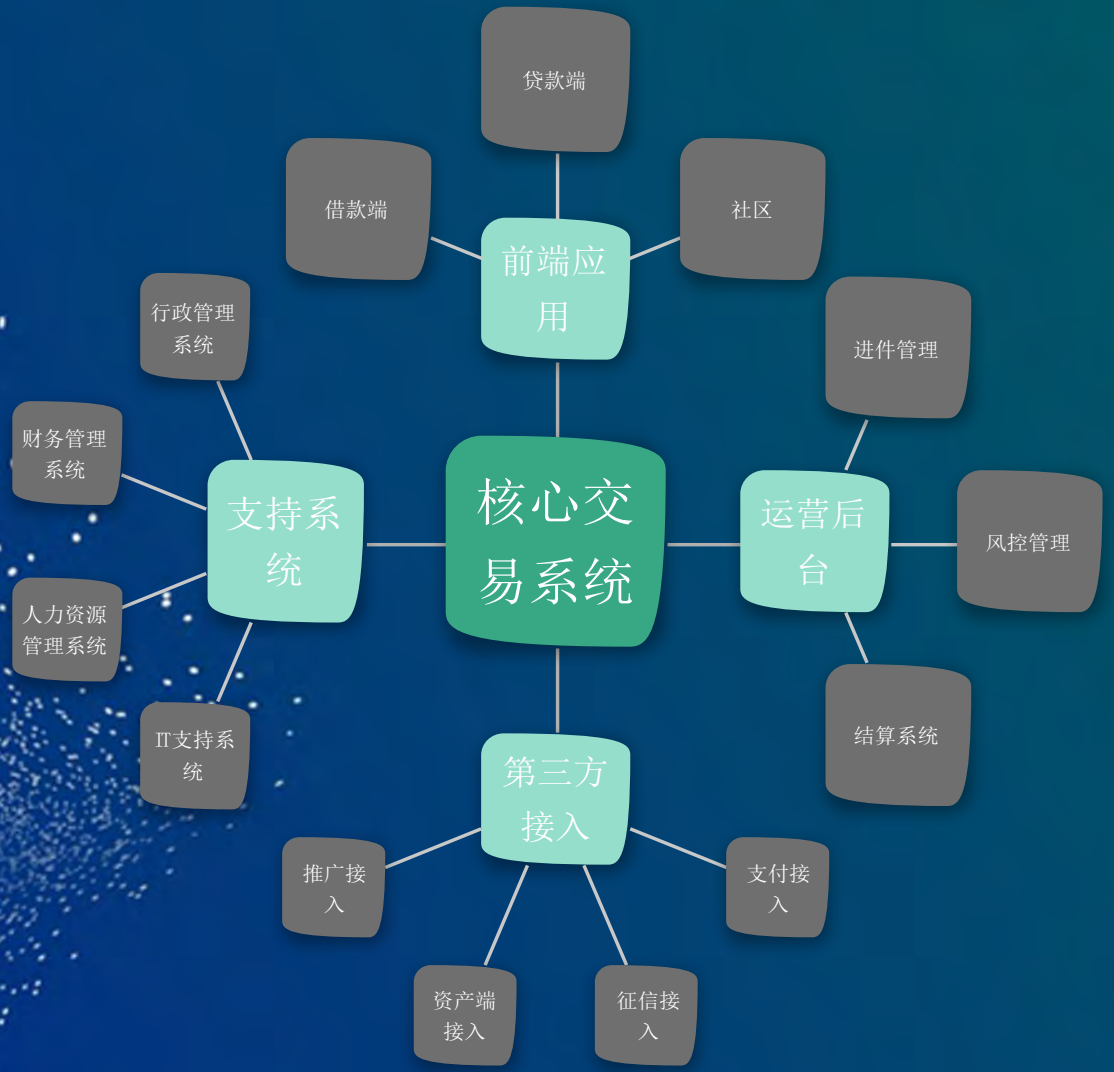
信息安全管理制度体系框架







痛点与实践分享1 – 账号和权限管理



痛点与实践分享1 – 账号和权限管理

建立全局视图

- 账号类型
- 应用系统
- 管理员
- 管理要求

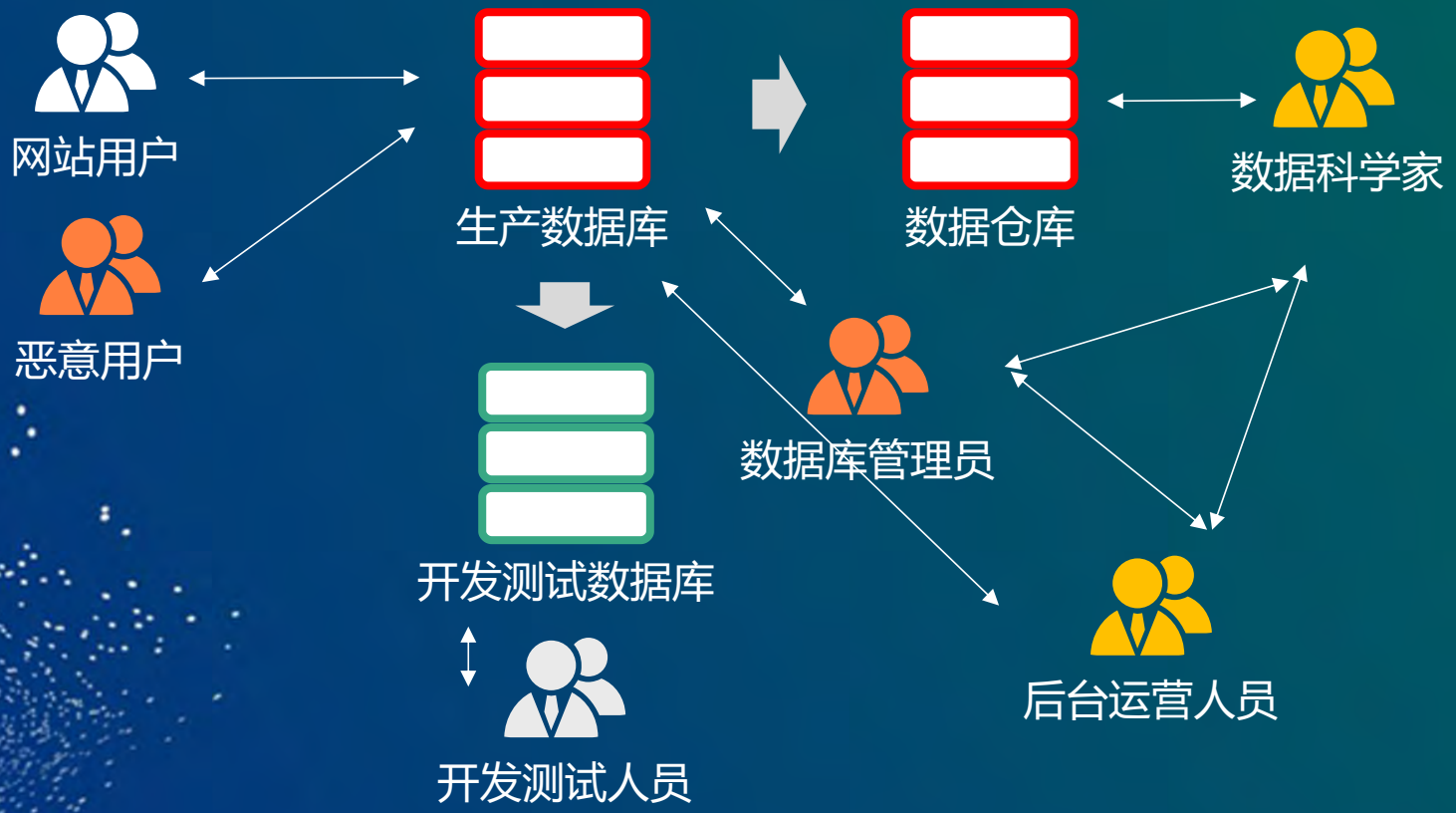
识别管控重点

- 应用特权账号
- 高危操作账号
- 系统运维账号

账号管理活动

- 一致性安全策略
- 账号开关流程
- 账号审阅
- 教育、警示

痛点与实践分享2 – 敏感信息泄露防护



主要防护措施

- Web安全防护
- 数据库加密
- 数据脱敏（透明）
- HDLP/NDLP
- 日志、流量审计

痛点与实践分享3 – 操作日志审计

日志审计目的

- 预警
- 发现
- 调查

日志审计难点

- 海量数据
- 格式、字段缺陷
- 交叉分析难
- 自动化分析模型误报
- 分析人员能力

基于场景的分析方法

- 网络攻击预警、分析
- 羊毛党及恶意贷款风险分析
- 高危运维操作
- 数据访问、下载操作

点融网信息安全团队

- 业务反欺诈
- 安全测试
- 安全合规
- SRC

Thanks!