

支付安全风险及防范

大纲/目录

1 支付安全风险

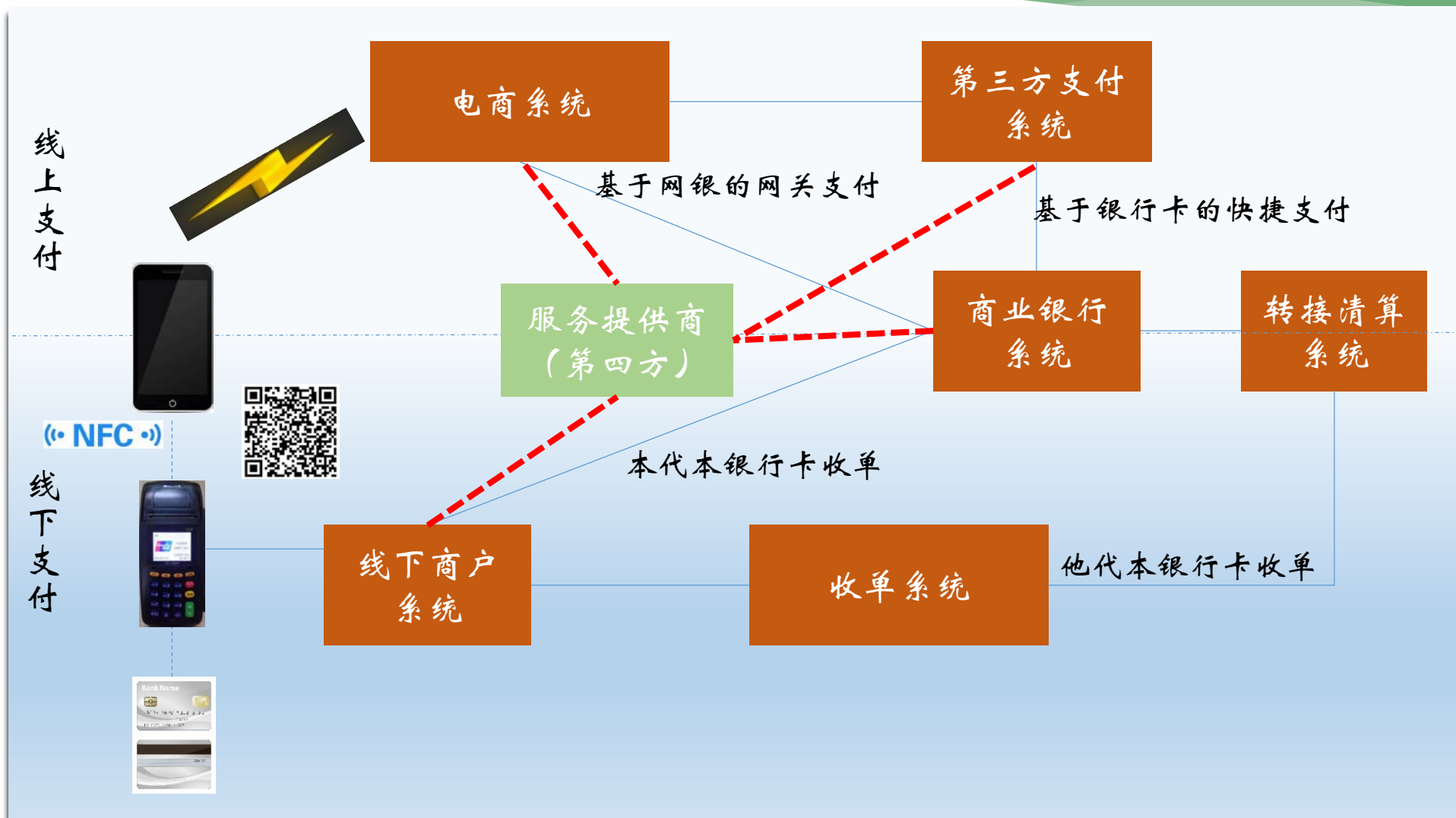
2 支付安全风险防范

3 监管要求及安全认证

4 PCI DSS合规评估

1. 支付安全风险

❖ 银行卡交易



1. 支付安全风险

❖ 银行卡线下支付风险

商户	服务提供商	支付机构	银行	转接清算机构
MIS系统 前置	前置系统 业务系统 POS等终端	前置 业务系统 终端	发卡系统 ATM 前置	CUPS



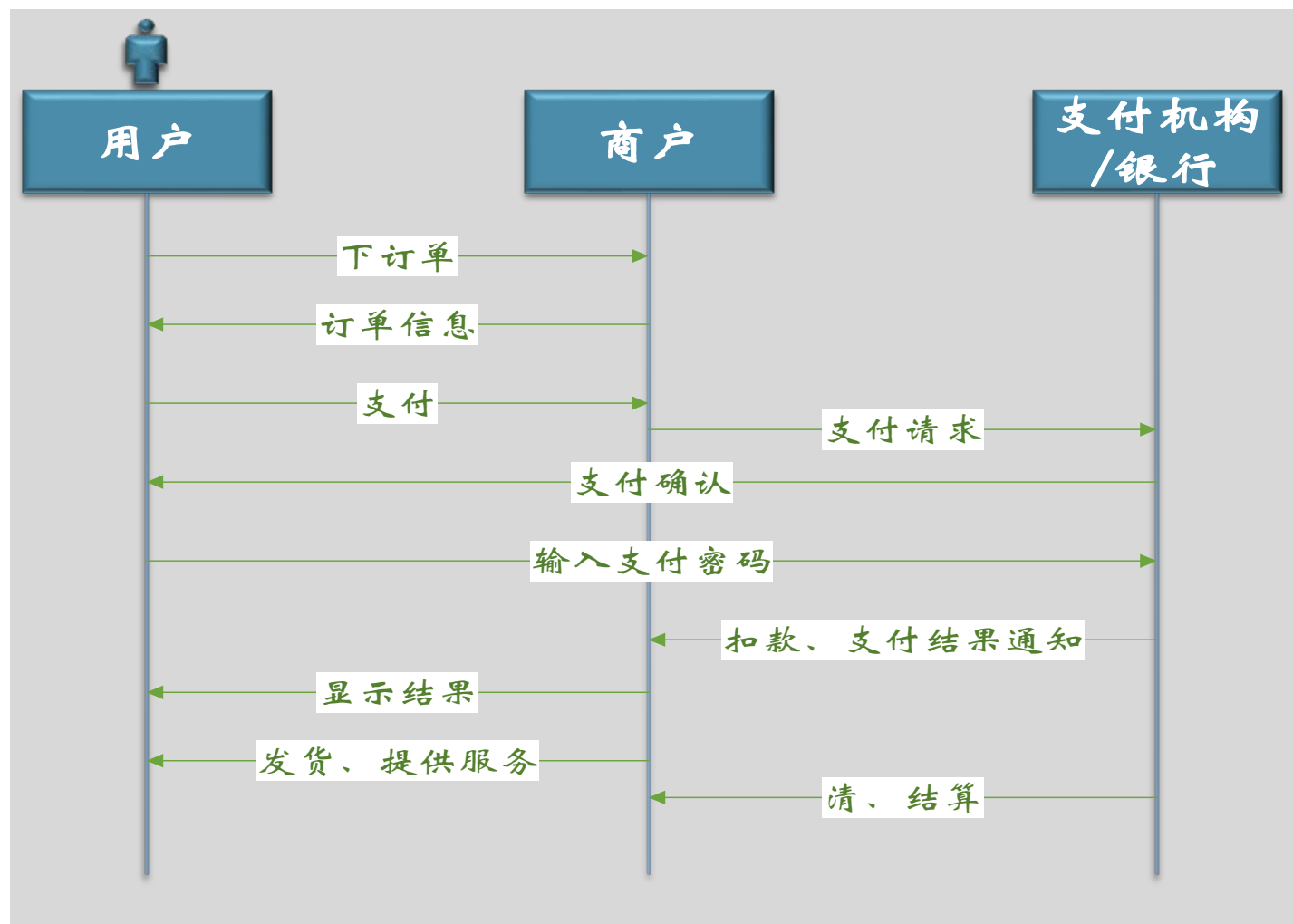
1. 支付安全风险

❖ 线下支付风险



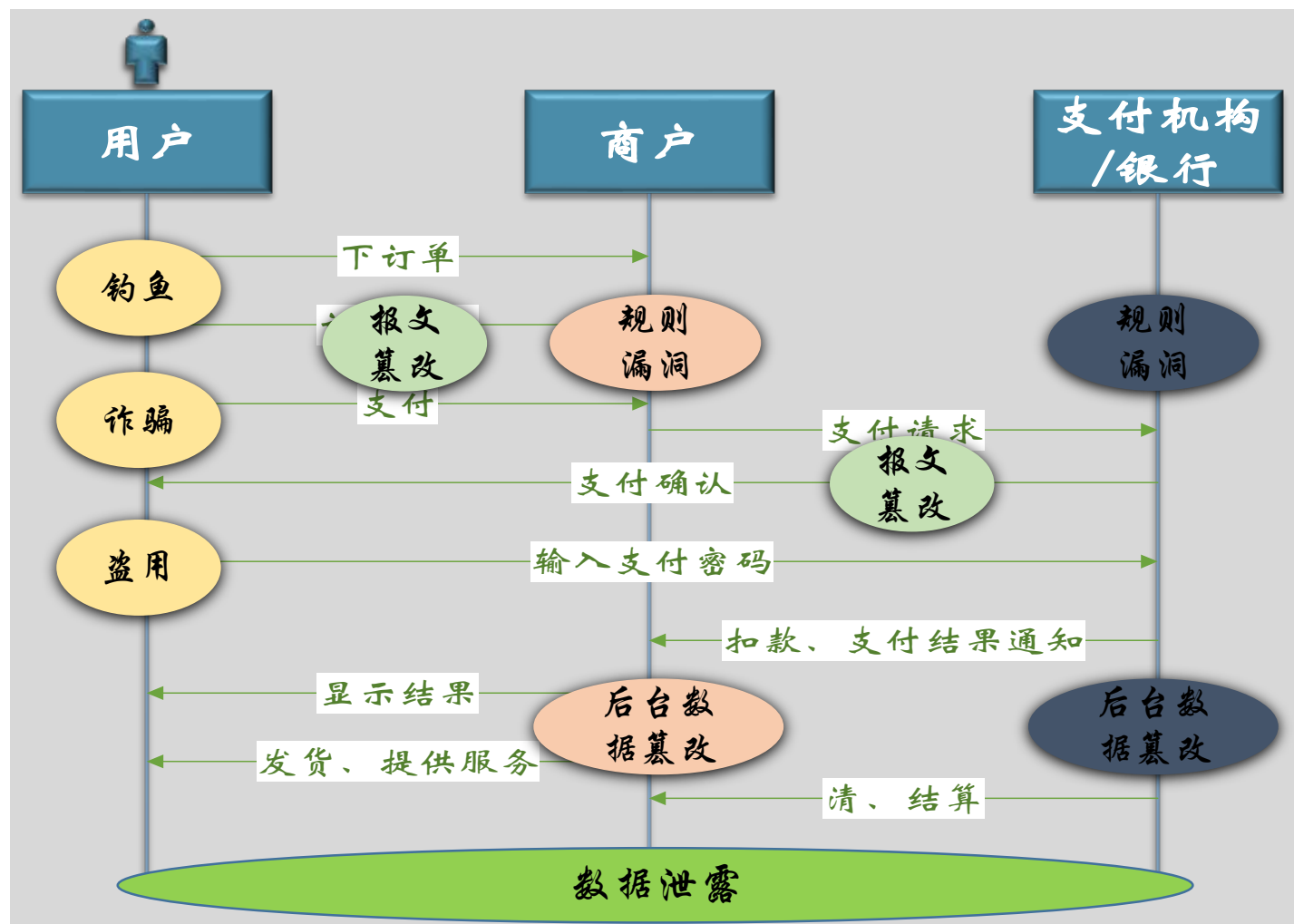
1. 支付安全风险

❖ 一般支付流程



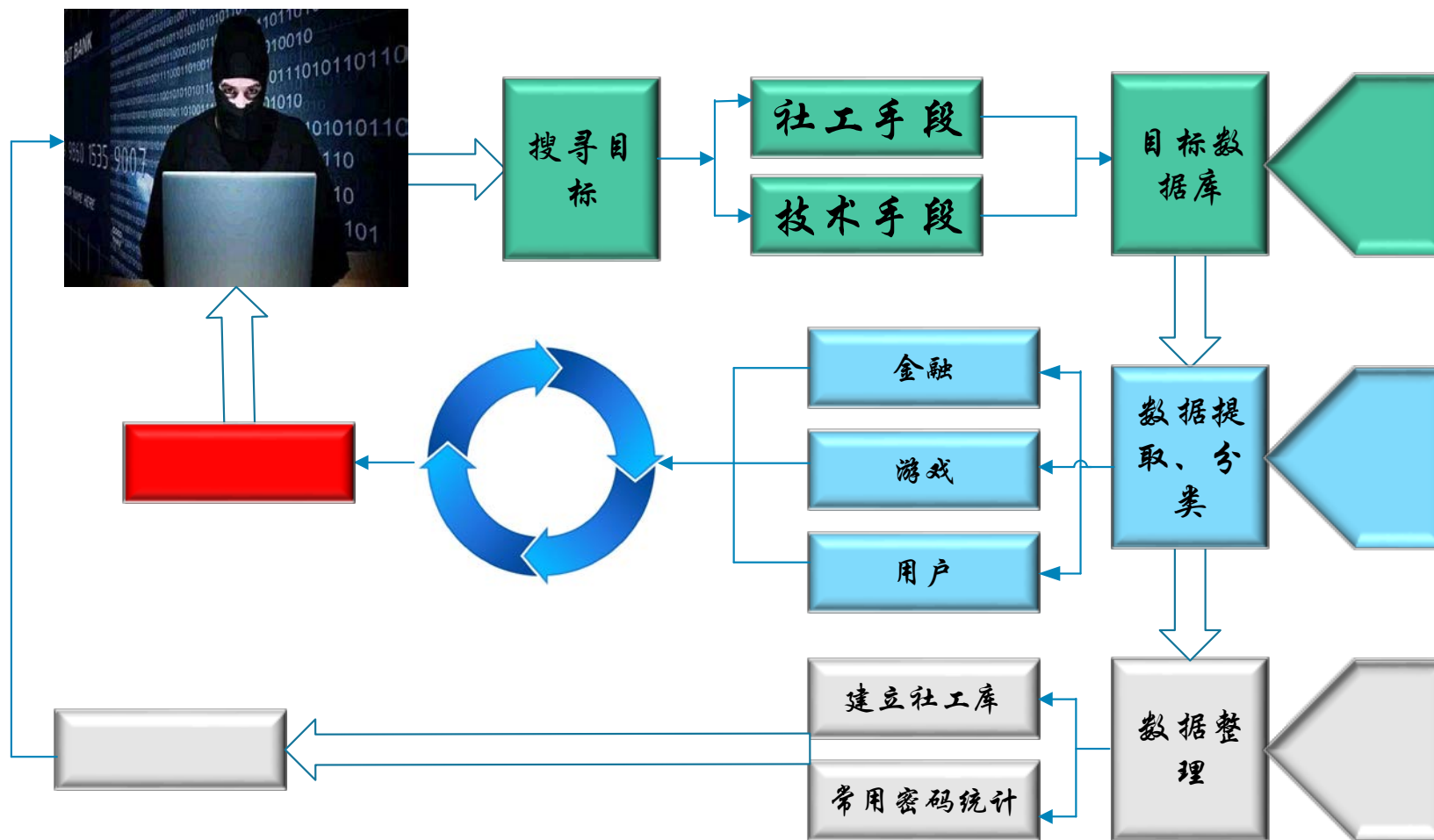
1. 支付安全风险

❖ 线上支付安全风险

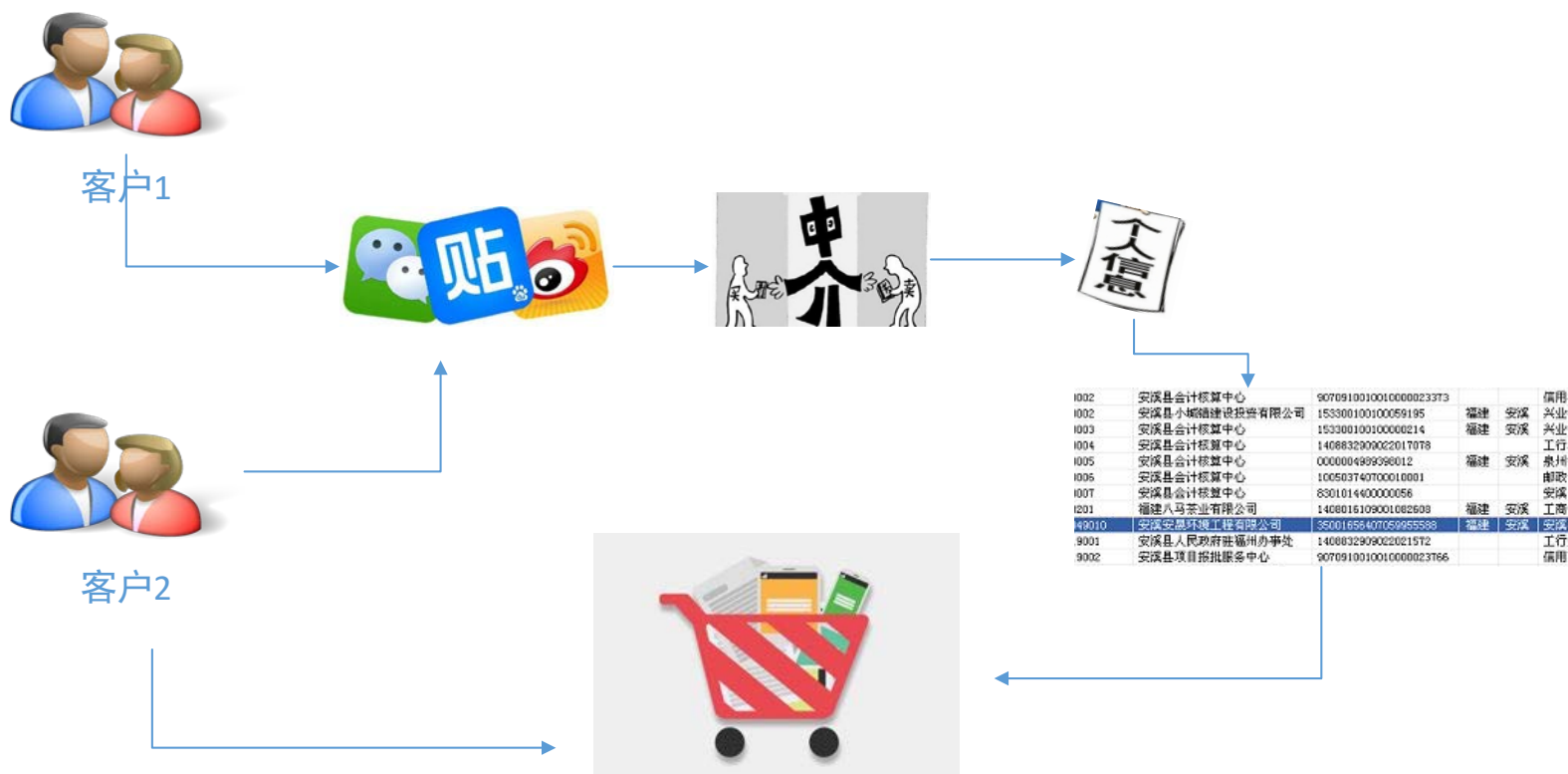


1. 支付安全风险

❖ 线上支付安全风险



❖ 用户与中介勾结套现模式



大纲/目录

1 支付安全风险

2 支付安全风险防范

3 监管要求及安全认证

4 PCI DSS合规评估

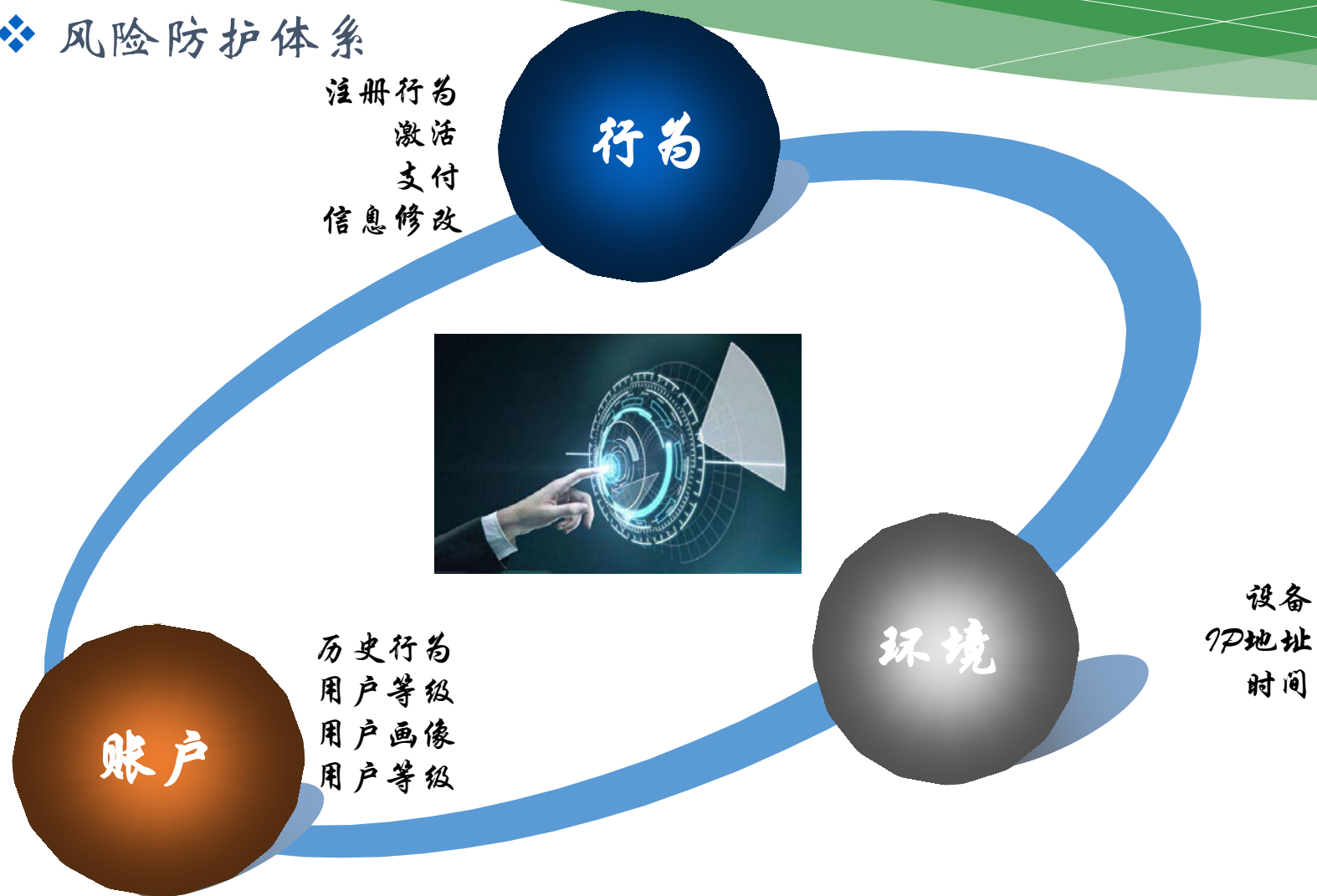
1. 支付安全风险防范

❖ 基础安全防护



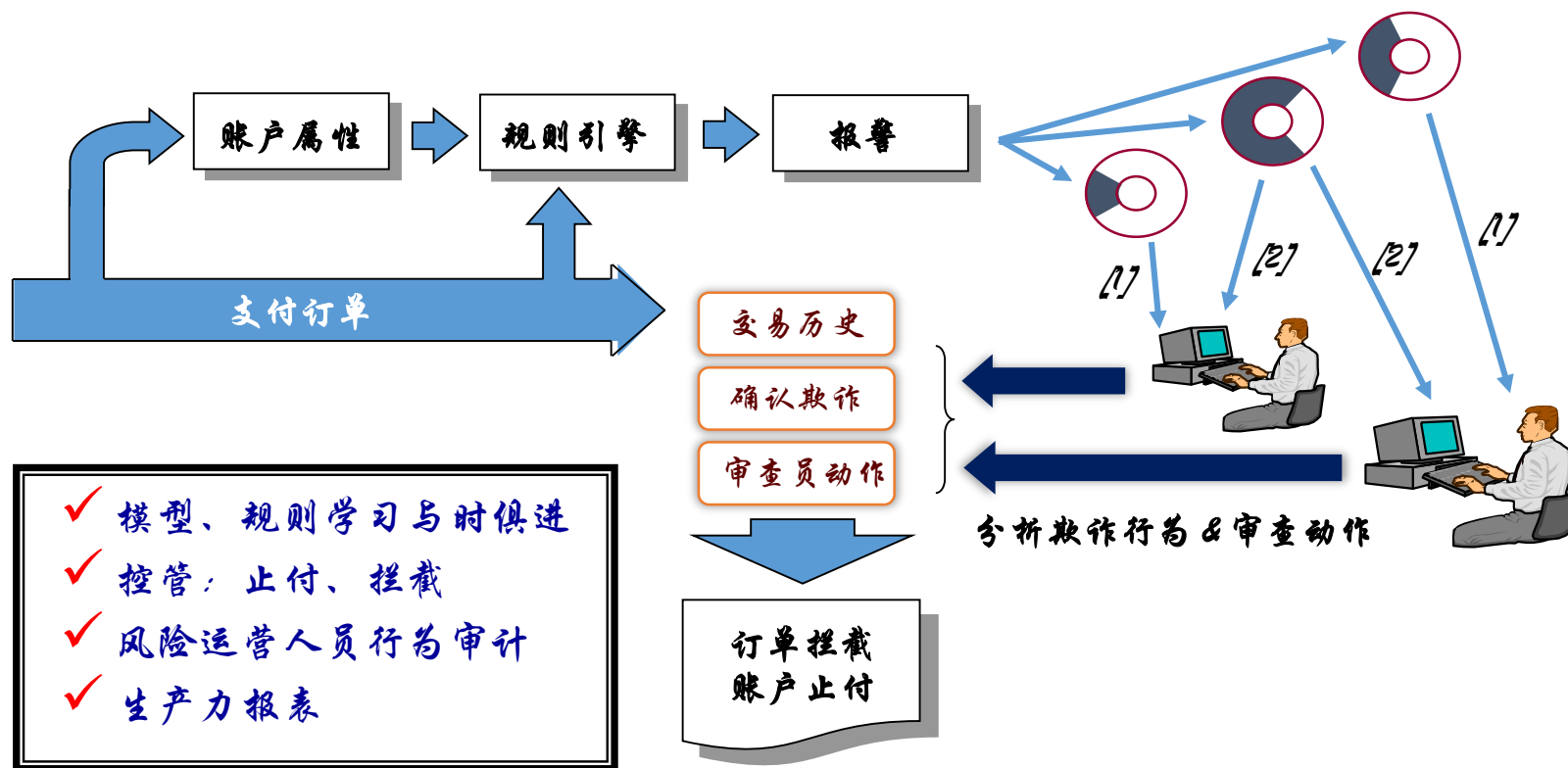
1. 支付安全风险防范

❖ 风险防护体系



1. 支付安全风险防范

交易监控风险体系



大纲/目录

1 支付安全风险

2 支付安全风险防范

3 监管要求及安全认证

4 PCI DSS合规评估

3.监管要求及安全认证

❖ 相关标准

- PCI DSS: 支付卡行业数据安全标准
- IOS信息安全认证
- 信息安全等级保护
- 非金融机构支付业务设施检测规范
- ADSS: 银联卡收单机构账户信息安全管理标准

3.监管要求及安全认证

❖ 认证内容

PCI DSS	IOS	等级保护	支付系统检测规范	ADSS
建立并维护安全的网络和系统	27001信息安全管理体系 (14个安全域和114个安全控制措施项)	技术要求: 物理、网络、主机、应用、数据安全及备份恢复	网络	政策制定
保护存储的持卡人数据			主机	组织管理
维护漏洞管理计划			应用	访问控制
实施强效访问控制措施	20000 IT服务管理	管理要求: 管理制度、管理机构、人员安全、系统建设、系统运维	数据	账户信息生命周期安全
实施强效访问控制措施			运维	系统及网络安全
定期监控并测试网络			业务连续性	银联卡受理终端及支付应用软件安全
维护信息安全政策			文档、功能、性能	

大纲/目录

1 支付安全风险

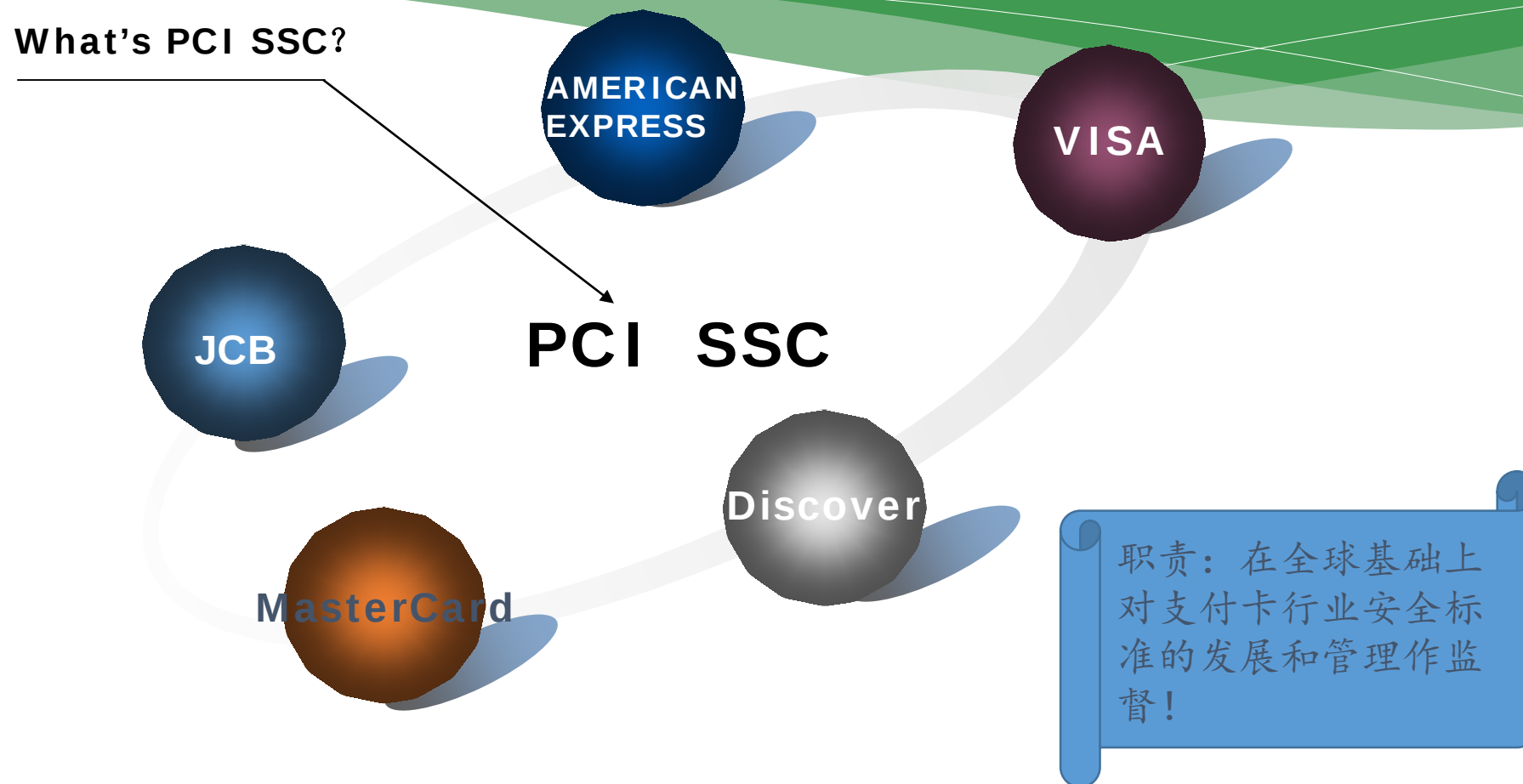
2 支付安全风险防范

3 监管要求及安全认证

4 PCI DSS合规评估

4. PCI DSS

What's PCI SSC?



4. PCI DSS

❖ 国内机构PCI DSS 认证需求

合作机构要求

申请资质要求

海外业务

自身安全要求

4. PCI DSS

❖ PCI DSS规范概述 (v3.2)

目标	内容	要求	内容
1	建立并维护安全的网络和系统	1	安装并维护防火墙配置以保护持卡人数据
		2	不要使用供应商提供的默认系统密码和其他安全参数
2	保护存储的持卡人数据	3	保护存储的持卡人数据
		4	加密持卡人数据在开放式公共网络中的传输
3	维护漏洞管理计划	5	为所有系统提供恶意软件防护并定期更新杀毒软件或程序
		6	开发并维护安全的系统和应用程序
4	实施强效访问控制措施	7	按业务知情需要限制对持卡人数据的访问
		8	识别并验证对系统组件的访问
5	定期监控并测试网络	9	限制对持卡人数据的物理访问
		10	跟踪并监控对网络资源和持卡人数据的所有访问
6	维护信息安全政策	11	定期测试安全系统和流程
		12	维护针对所有工作人员的信息安全政策

QSA机构资质

Qualified Security Asses

https://www.pcisecuritystandards.org/assessors_and_solutions/qualified_security_assessors

Find a Qualified Security Assessor Company

Beijing Zhihuiyunce Technology Co., LTD.

SUBMIT

Filter by:

PLACE OF B...

SERVICING ...

LANGUAGE

EXPORT LIST <->

Page: 1

Results: 1

COMPANY	PLACE OF BUSINESS	PRIMARY CONTACT	SERVICING MARKETS	SUPPORTED LANGUAGES
Beijing Zhihuiyunce Technology Co., LTD.	China	Tianning Huang huangtn@dplslab.com T: +81-10-87162569-802	China	Chinese, English

Page: 1

信息安全风险评估资质

ISCCC

信息安全服务资质认证证书

证书编号: ISCCC-2017-ISV-RA-192

兹证明

北京智慧云测科技有限公司

的信息安全风险评估服务资质符合

ISCCC-SV-001:2015《信息安全服务资质认证实施规则》

三级服务资质要求。

注册地址: 北京市门头沟区莲石湖西路 98 号院 7 号楼 701

受审核地址: 北京市门头沟区莲石湖西路 98 号院 7 号楼 701

颁证日期: 2017 年 1 月 20 日

证书需每年接受监审, 无监审标志证书无效。



魏昊

Signed: Wei Hao



中国信息安全认证中心

中国·北京·朝外大街甲10号(100020)

www.isccc.gov.cn
证书通过上述网站查询

北京智慧云测科技有限公司



谢谢！

联系方式：

010-60801696

15910912957

jiangx@dplslab.com

wuxf@dplslab.com