商盟商务服务有限公司信息安全在第三方支付行业的落地和推广



鲁晋

风控及安全管理部(副总经理)

H3CSE & CISP & ISO27001 LA & ITIL & ISO20000 & Cobit

luj@sumpay.cn

15267060898



第三方支付行业简介

第三方支付监管要求

第三方支付安全体系建设

第三方支付行业简介-发展历程简述



1999年3月

2002年前

2005年

2010年

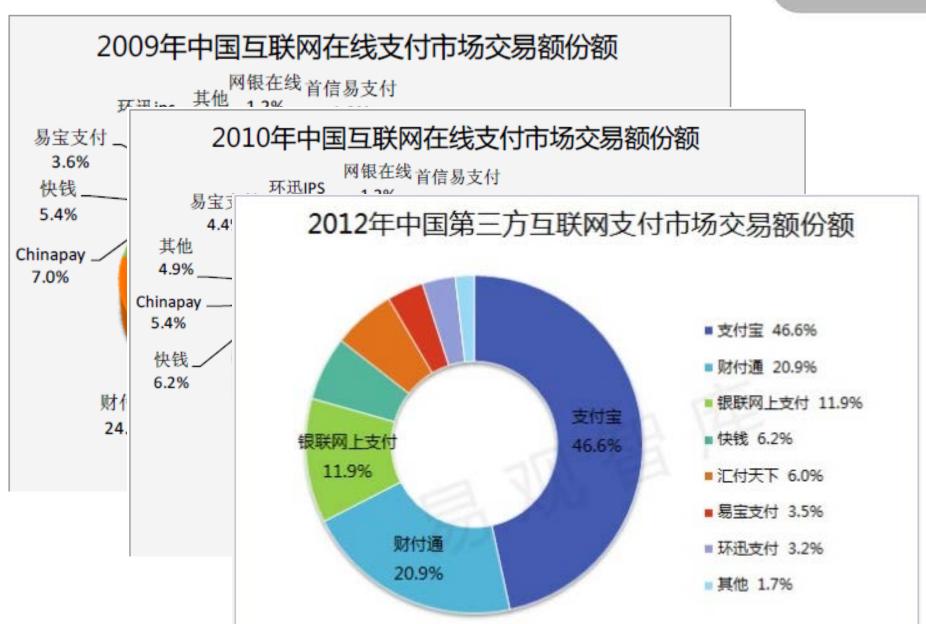
至今

首信易支付是中国最大的电子的主义的主义的服务。

截止2013年 7月6日,全 国共计发牌 250家企业 事业单位

第三方支付行业简介-历年交易额份额





第三方支付行业简介-浙江省第三方支付行业简介



Bim www.sumpay.cn			
序号	公司名称	业务范围	支付业务种类
1	支付宝(中国)网络技术有限公司	全国	互联网支付、移动电话支付、预付卡发行与受理(仅限于线上实名支付账户充值)、银行卡收单
2	杭州银通数码信息技术有限公司	全国	互联网支付、移动电话支付
3	商盟商务服务有限公司		预付卡发行与受理(浙江省、上海市)、互联网支付 (全国)
4	宁波银联商务有限公司	宁波市	银行卡收单
5	浙江易士企业管理服务有限公司	浙江省	预付卡发行与受理
6	网易宝有限公司	全国	互联网支付
7	浙江贝付科技有限公司	全国	互联网支付
8	浙江航天电子信息产业有限公司		预付卡发行与受理(浙江省)、互联网支付(全国)
9	浙江余姚中国塑料城网上交易有限 公司	全国	互联网支付
10	杭州盛炬网络技术有限公司		银行卡收单(浙江省、上海市)
11	舟山市明生商盟科技服务有限公司	浙江省	预付卡发行与受理
12	浙江银付通信息科技有限公司	浙江省	预付卡发行与受理
13	杭州市民卡有限公司		预付卡发行与受理(仅限浙江省)、 互联网支付(全国)、移动电话支付(全国)
14	温州之民信息服务有限公司	浙江省	预付卡发行与受理
15	杭州通策会综合服务有限公司	浙江省	预付卡发行与受理
16	浙江快捷通网络技术有限公司	全国	互联网支付



第三方支付行业简介

第三方支付监管要求

第三方支付安全体系建设

第三方支付机构监管要求-中国人民银行公告



【2010】 第2号 【2010】 第17号 【2011】

第14号

第17号

【2011】

【2012】

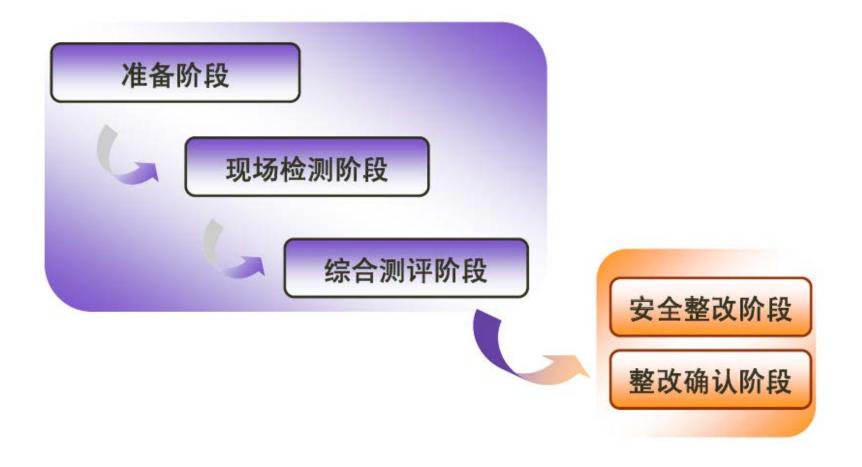
第6号

非金融机构 支付服务管 理办法 非金融机构 支付服务管 理办法实施 细则 非金融机构 支付服务业 务系统检测 认证管理规 定

非金融机构 支付服务业 务系统检测 机构名单及 检测业务范 围 非金融机构 支付业务设 施技术认证 名单

第三方支付机构监管要求-检测流程





第三方支付机构监管要求-检测指标





- 必测项居多,达到90%
- 安全方面的检测指标居多,达到67%



第三方支付行业简介

第三方支付监管要求

第三方支付安全体系建设

第三方支付安全体系建设-公司级战略目标落实



战略问题 确认

战略发展

资源分配

预定目标

落实目标

历史回顾

支付供需 分析 公司资源 分配

战略目标

实施发展 策略

现状分析

趋势判断

支付政策 分析

支付业务 建议 公司能力 分析

备选行业 研究

战略扩展 建议 运营目标

市场目标

财务目标

产品目标

安全目标

风控目标

第三方支付安全体系建设-主要关注点



- □人治与法治;
- □ 岗位职责及部门沟通;
- □产品管理及竞争分析:
- □项目管理及需求提交;
- □业务连续性及可用性:
- □ 专业技术及知识积累;

第三方支付安全体系建设-信息安全整体保障框架体系



公司

战略目标

信息安全 组织/方针/策略

信息安全 管理制度/流程/人员

预防为主、职责明晰、 有效识别 主动防御、及时响应、 集中管控

体系完善、流程通畅、 全员参与

可管

可控

可信

信安管保体

信安技保体

应业安保体系

信安运保体系



定义层

信息系统安全技术保护要求

管控层

物理安全 管控目标 数据安全 管控目标 网络安全 管控目标 主机安全 管控目标 应用安全管控目标

防护层

风险评估服 务实施指南

安全设备安全配置指南

应用安全开 发指南

堡垒机系统 配置指南 安全加固服 务实施指南

网络设备安 全配置指南

WLAN设备 安全功能和 配置指南

Web防护系 统配置指南 安全巡检服 务实施指南

操作系统安 全配置指南

防火墙系统 配置指南

上网行为管理系统配置指南

应急响应服 务实施指南

数据库系统 安全配置指 南

入侵防御系 统配置指南

数据库审计 系统配置指 南 IT审计服务 实施指南

IT终端系统 安全配置指 南

准入控制系 统配置指南

*** ***



决策层

信息安全管理策略

管理层

信息安全组织建设管理规范

人员信息安 全管理规范 信息系统建设安全管理规范

信息系统运维安全管理规范

信息安全检查管理规范

执行层

员工信息安 全管理指南

物理环境安

全管理指南

IT安全监控

与预警安全

信息系统上

线验收安全

管理指南

管理指南

第三方信息 安全管理指 南

IT终端安全 管理指南

IT业务连续 性管理指南

信息系统维 护与变更管 理指南 文档安全与 信息保护管 理指南

信息系统账 号权限与密 码管理指南

信息安全事 件应急响应 管理指南

IT财务管理 指南 网络安全域 管理指南

信息系统防 病毒管理指 南

信息系统数 据备份与恢 复管理指南

IT供应商管 理指南 信息系统网 络接入管理 指南

信息系统安 全补丁管理 指南

基线达标考 评细则

... ...



定义层

信息安全运维体系建设要求

职能层

信息安全事件监控

信息安全 事件分析 信息安全紧急响应

安全审计

ITSM 标准法规

执行层

事件管理指

服务水平管理指南

IT服务台管 理指南 问题管理指

可用性管理 指南

支付平台系统监控指南

配置管理指 南

能力管理指 南

购卡网系统 监控指南 变更管理指

IT财务管理 指南

信息系统连 通性监控指

发布管理指南

IT服务连续 性管理指南

信息安全事件监控指南



体验层

支付平台系统安全体验和保障要求

支撑层

支付平台系统安全体验目标

支付平台系统安全保障目标

保护层

支付系统安 全网购指南

数字证书使 用指南 支付系统风 控策略指南 (涉密)

商盟支付盾 使用指南 安全控件使 用指南

时间动态令牌使用指南

手机动态令牌使用指南

挑战动态令 牌使用指南

第三方支付安全体系建设-落地及推广的难点



- □ 系统复杂及基础架构;
- □资源协调及资源配比;
- □ 部门职责及人员素质;
- □ 配置管理及知识传递;



第三方支付行业简介

第三方支付监管要求

第三方支付安全体系建设



- □ 建立行业联盟,整合资源,安全资讯的共享;
- □建立完善的安全管理体系&风控管理体系&内控管理体系;
- □一站式安全服务;



THANK YOU! Q&A