课后报告四

银行账户交易管理系统的系统运行安全管理的目标是确保系统运行过程中的安全性，主要包括可靠性、可用性、保密性、完整性、不可抵赖性和可控性几个方面。系统运行安全管理包括系统评价、系统运行安全检查、变更管理、建立系统设置参数文件和运行日志以及建立科学的管理制度等方面。

该系统的性能指标包括：处理正确性；处理效率性能；操作界面友好性；系统易维护性；数据保密性；数据完整性；数据精确性；交易安全性；交易不可抵赖性等。

银行账户交易管理系统的操作管理是信息安全管理的重要方面。主要内容包括操作权限管理、操作规范管理、操作责任管理和操作监控管理。

银行应当建立健全客户身份识别机制。为客户开立支付账户的，应当对客户实行实名制管理，登记并采取有效措施验证客户身份基本信息，按规定核对有效身份证件并留存有效身份证件复印件或者影印件，建立客户唯一识别编码，并在与客户业务关系存续期间采取持续的身份识别措施，确保有效核实客户身份及其真实意愿，不得开立匿名、假名支付账户。

银行应当与客户签订服务协议，约定双方责任、权利和义务，至少明确业务规则（包括但不限于业务功能和流程、身份识别和交易验证方式、资金结算方式等），收费项目和标准，查询、差错争议及投诉等服务流程和规则，业务风险和非法活动防范及处置措施，客户损失责任划分和赔付规则等内容。

银行应根据客户身份对同一客户在本机构开立的所有支付账户进行关联管理，并对个人支付账户进行分类管理；应当确保交易信息的真实性、完整性、可追溯性以及在支付全流程中的一致性，不得篡改或者隐匿交易信息；对于客户的网络支付业务操作行为，银行应当在确认客户身份及真实意愿后及时办理，并在操作生效之日起，真实、完整保存操作记录。客户操作行为包括但不限于登录和注销登录、身份识别和交易验证、变更身份信息和联系方式、调整业务功能、调整交易限额、变更资金收付方式，以及变更或挂失密码、数字证书、电子签名等。

应当综合客户类型、身份核实方式、交易行为特征、资信状况等因素，建立客户风险评级管理制度和机制，并动态调整客户风险评级及相关风险控制措施。应当根据客户风险评级、交易验证方式、交易渠道、交易终端或接口类型、交易类型、交易金额、交易时间、商户类别等因素，建立交易风险管理制度和交易监测系统，对疑似欺诈、套现、洗钱、非法融资、恐怖融资等交易，及时采取调查核实、延迟结算、终止服务等措施；应当向客户充分提示网络支付业务的潜在风险，及时揭示不法分子新型作案手段，对客户进行必要的安全教育，并对高风险业务在操作前、操作中进行风险警示；为客户购买合作机构的金融类产品提供网络支付服务的，应当确保合作机构为取得相应经营资质并依法开展业务的机构，并在首次购买时向客户展示合作机构信息和产品信息，充分提示相关责任、权利、义务及潜在风险，协助客户与合作机构完成协议签订。

银行应当建立健全风险准备金制度和交易赔付制度，并对不能有效证明因客户原因导致的资金损失及时先行全额赔付，保障客户合法权益；应当依照中国人民银行有关客户信息保护的规定，制定有效的客户信息保护措施和风险控制机制，履行客户信息保护责任。不得存储客户银行卡的磁道信息或芯片信息、验证码、密码等敏感信息，原则上不得存储银行卡有效期。因特殊业务需要，支付机构确需存储客户银行卡有效期的，应当取得客户和开户银行的授权，以加密形式存储。应当以最小化原则采集、使用、存储和传输客户信息，并告知客户相关信息的使用目的和范围。支付机构不得向其他机构或个人提供客户信息，法律法规另有规定，以及经客户本人逐项确认并授权的除外。应当通过协议约定禁止特约商户存储客户银行卡的磁道信息或芯片信息、验证码、有效期、密码等敏感信息，并采取定期检查、技术监测等必要监督措施。

因交易超时、无响应或者系统故障导致支付指令无法正常处理的，应当及时提示客户；因客户原因造成支付指令未执行、未适当执行、延迟执行的，应当主动通知客户更改或者协助客户采取补救措施。应当告知客户相关服务的正确获取途径，指导客户有效辨识服务渠道的真实性。