银行信息系统中操作风险管理的框架①

A Framework of Operational Risk Management in Banks' IT Systems

吴 军 (中国科学院 研究生院 北京 100049; 中国农业银行 软件开发中心 北京 100161)

左 春 (中国科学院 软件研究所 北京 100190)

摘 要: 通过信息系统来加强对操作风险的管理越来越受到银行界的重视，总结了目前银行信息系统建设中在操作风险防范方面存在的问题，分析了银行信息系统中操作风险管理的需求。提出了一种基于全流程的银行信息系统操作风险管理的框架，阐述了交易前、交易中、交易后三个组成模块的具体功能和实现要点，最后说明在某大型商业银行的实践情况。该框架从操作风险控制的全局归纳出了共性的控制点，设计了主要的风险控制流程环节。

关键词: 操作风险 公共安全 身份认证 实时监控 批量分析

1 引言

当前，通过计算机信息系统来加强对操作风险的管理越来越受到国际银行业界的重视。一方面是因为银行机构越来越庞大，产品越来越复杂，银行业务对以计算机为代表的信息技术的高度依赖；另一方面是因为计算机技术的发展为操作风险的防范提供了必要的基础。在金融市场的全球化的今天，一些“操作”上的失误，可能带来很大的甚至是毁灭性的后果。过去这些年里，这方面已经有许多惨痛的教训[1]。

巴塞尔银行监管委员会定义操作风险是指由于不完善或有问题的内部操作过程、人员、系统或外部事件而导致的直接或间接损失的风险[2]。可以看出，操作风险管理是一个非常复杂的问题，包括组织结构、管理制度、系统建设等等诸多方面，而信息系统在银行操作风险防范中起的作用是非常关键的，目前也越来越受到各家银行的重视[3]。本文总结了目前银行信息系统在操作风险防范方面存在的问题，设计了一种基于全流程的银行信息系统操作风险管理框架。

2 目前系统建设存在的问题

(1) 缺乏统一规划，系统架构杂乱。

人们对于银行系统操作风险的认识是逐步加深和细化的，因此在计算机系统建设方面的表现就是始终滞后于业务系统的发展，缺乏统一的规划，大部分都是根据后来的要求在原系统上进行打补丁的操作。

(2) 缺乏统一管理，存在管理盲区。

由于缺乏统一的操作风险管理部门，而各个相关业务部门都会提出一些零星的操作风险管理要求，在应用系统中重复流程较多，一方面重复建设，投资浪费；另一方面操作重复，人力浪费。不同类型的操作风险由不同的部门负责，会存在管理盲区。

(3) 公共问题没有好的解决方式。

从历年发生的银行操作风险事件分析，大多是不按操作规范流程或者监管层督办不得力等导致[3]，尽管可以发现诸多共性问题，然而由于银行系统庞杂，还没有一种好的模式在实际中能有效解决相关问题。

目前防范操作风险相关系统建设的现状如图 1 所示。

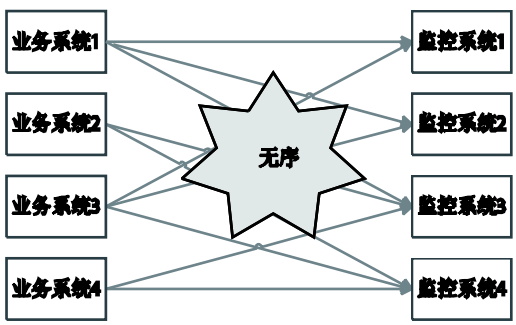

图 1 系统建设现状

① 收稿时间:2009-06-02

3　统一风险管理框架的设计

3.1 框架功能分析

根据对银行信息系统的特点和操作风险的特点的分析，整个操作风险管理框架为各个业务系统提供数据安全、行为监控、对账审核等服务，风险控制将主要体现在：

首先，对于业务流程的控制，在合理设计业务流程的基础上，通过一定的模型规则对操作内容进行监控和预警。

其次，对于银行操作者的风险控制，主要通过身份认证、权限管理等实现，保证操作角色的合法性和可用性。

再次，对于客户的风险控制，主要通过黑名单、反洗钱、国际收支申报等手段，防止虚假信息导致的恶意获利行为。

最后，通过人工审计及系统审计相结合，充分利用数据挖掘技术对业务数据进行批量分析，发现问题后通过反馈和纠正机制来控制操作风险。

3.2 框架总体设计

在总结操作风险控制措施的基础上，我们按照全流程控制的思路，将银行操作风险的控制点归纳为事前预防、事中约束、事后审核三个阶段。总体设计如图 2 所示：

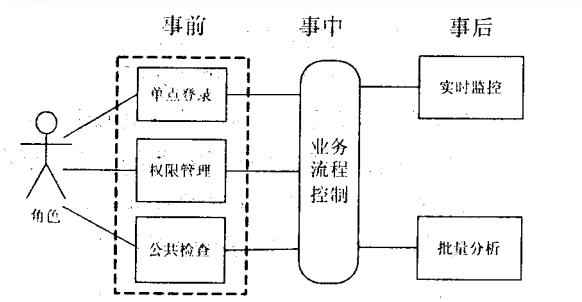

图 2　银行操作风险控制的总体设计

框架设计遵循如下理念：首先从风险控制的整体考虑，归纳出共性的控制点，减少重复控制，提高效率；其次从全流程的角度考虑，使风险控制能够环环相扣，避免管理漏洞。

3.3 框架概要设计

从系统的结构性考虑，可以根据处理的内容的性质分为如下几类：

① 身份认证及权限管理系统，可以统一登录，统一识别操作者身份是否合法，并进行权限控制。

② 事前的公共业务检查系统，可以提供银行共享信息的有效性检查。

③ 事中的业务检查和流程控制，由各业务系统来完成。

④ 事后实时的监控分析系统，可以实时根据关键信息进行分析，并将预警信息通知到管理人员。

⑤ 事后批量分析监控系统，可以结合影像技术进行审核，筛选业务流程产生的操作数据进行分析，上报管理部门要求的各类关注报表。

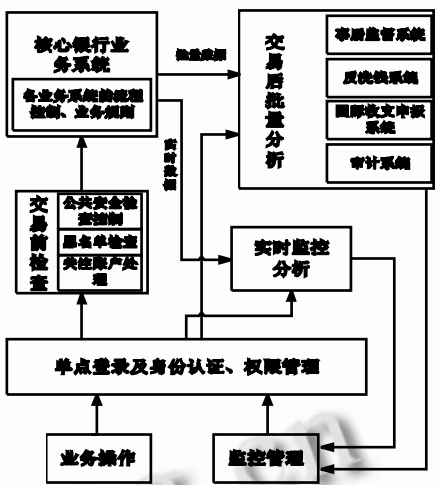

图 3　风险控制框架

图 3 是风险控制的总体框架，该框架提供了按流程识别的风险控制基础功能，将风险控制系统和核心应用系统统一成一个有机的整体，核心应用系统是风险控制系统分析的基础，风险控制系统则是核心应用系统的延伸，作为防范银行操作风险的管理设施，构建了以提前校验，实时反馈，事后监督为链条的控制机制。

3.4 设计说明

3.4.1 身份认证及权限管理模块

该模块是所有系统的接入门户，一般采用口令方式、PKI、数字签名、指纹等方式进行身份和权限的控制，为银行信息系统提供操作用户的身份识别、权限控制的能力。

身份认证是银行核心系统中最基础的安全屏障，主要包括银行内部人员的身份认证和外部客户的身份认证。身份认证采用 PKI 技术，由第三方 CA 签发数字证书，实现网络中数据加密的传输，负责交易数据的数字签名以及网上身份的证明[4]。柜员的数字证书采用 IC 卡作为存放介质，同时与生物指纹验证技术相结合，保障对银行核心系统操作的安全性和易用性。对银行客户的身份认证，则采用 USB Key、动态口令卡作为数字证书的存放介质。

权限管理包括基本权限管理及授权管理。其中，基本权限管理是对操作者的基本操作权限进行预先定义，在交易申请上来时，用来控制检查操作者的操作权限。授权管理又包括静态授权管理和动态授权管理两种。静态授权是对于一些已知的高风险操作进行预先定义，当该操作发生时，必须经过主管的授权。动态授权判断的依据是由操作的具体内容决定的，譬如金额，当该操作的金额大于一定的数量时，才需要得到一定级别的授权。

实现要点：采用基于 RSA 算法的身份认证技术、单点登录方案、授权策略等将银行核心系统中的身份认证、权限管理以及审计监控安全相整合，建立企业级的单点登录平台，提供统一的基础安全服务技术架构。

3.4.2 交易前检查模块

该模块主要负责交易报文进入后台业务系统前的一系列公共安全检查，包括交易场景合法性的检查、黑名单账户检查、关注账户检查及处理。交易前检查通过控制公共信息渠道，完成各信息系统操作的业务公共检查，是操作人员身份校验后和处理任务需求前的无缝连接器。

实现要点：

① 黑名单、关注账户的维护是可以动态配置的，但是需要在实现时注意系统的性能，一般要放在共享内存中处理。

② 该检查模块是可以根据系统压力的大小做物理级的并行部署。

3.4.3 交易实时监控模块

该模块对实时交易数据进行实时分析，根据预先设计好的风险监控规则，对满足监控条件的交易信息转为预警信息，然后由相应监管人员进行处置。通过实时监控，可以及时发现操作风险并采取相应措施。

实现要点：

① 建设独立系统。考虑到不能对业务系统的性能有太大的影响，因此要独立建立该模块，需要通过消息中间件将各业务系统的交易流水信息发送到该系统进行处理，并且该系统的后续处理的结果与业务系统没有直接关系。

② 注重处理性能。数据实时采集分析必然会碰到性能问题，需要采用负载均衡、系统并发、分布处理及软件固化等技术来提高实时处理的性能。

③ 强调规则灵活配置。规则可以动态配置，根据需要可以及时调整。

3.4.4 综合批量分析模块

该模块实现对银行业务操作数据进行批量分析处理，其中包括若干不同功能的子模块。其数据来源主要是业务系统的各类数据，通过批量传递的方式传导。

批量分析首先是根据设定的风险查找规则对业务数据进行批量分析，从海量的业务数据中挖掘符合特定监控模型的风险点。

事后监督系统是相对独立的系统，将银行操作后留存的原始单据扫描成代电子影像，通过 OCR 识别匹配对应关键数据，对于匹配不上的，人工根据影像内容进行校对输入[5]。通过人工校对还可以发现操作者的操作规范程度，譬如对于一些非关键信息输入的完整性等等。同时，还可以通过该系统对实时监控系统产生的待核查信息进行核销。

反洗钱系统和国际收支申报系统都是根据外部监管要求而做的信息报送模块。通过数据分析，找出符合监控规则的数据内容，对于缺失的要素，还需要通过人工补录的方式来完善。

审计系统是根据外部或内部的审计要求，通过数据挖掘技术，提取符合审计要求的数据内容[6]。

实现要点：

① 事后监督系统需考虑好扫描后影像数据的保存和使用方式，可以和电子档案系统相连接，减少投资。另外，需要注意和实时监管系统的联动，提高劳动效率，减少重复的监管工作。

② 反洗钱和国际收支申报等外部监管要求的系统，要充分利用数据挖掘技术，尽量自动补齐缺失的信息，减少人工补录的工作。

③ 批量分析中的风险查找规则是实时监控规则的有效补充，要注重规则模型的设置，提高风险监控的有效性。

3.5 框架特点

① 安全性：该框架的设计借鉴国内外成熟模式，遵循国家有关部门的相关规范和管理规定。采用 PKI 技术实现身份认证、数据加密和交易签名保证各种应用的高度安全。

② 可靠性：该框架的结构清晰，这是稳定运行的基本前提。另外，在采用的软/硬件产品本身选择上，如消息中间件的使用，在对整个系统的高可用性的设计上，如数据分流设计等，也保证了整体的可靠性。

③ 可用性：由于统一的流程设计，减少了重复的人工监管处理，加强了统一的数据分析，提高了监管报表的准确度，从而减轻监管人员的负担，提高了整体的可用性。

④ 标准化和开放性：该框架支持业界通用的规范和标准，具有良好的开放性和兼容性。每一模块的设计都考虑了和其它模块的交互衔接，标准统一、接口规范。

⑤ 可扩展性：该框架针对不同的业务进行了分类管理可以提供灵活的规则配置，具有良好的功能扩展性。同时在设计上还应充分考虑到各功能的应用扩展接口，保障新的应用可以方便地融入该管理框架中，为其它新应用提供风险控制服务。

⑥ 高效性：通过流程梳理，统一建设管理框架，从而比原先的分散控制方式减少了重复处理，在联机交易中，提高了单笔业务的处理速度；在批量的数据分析方面，仅原始业务数据提取这一项，就比原先分散的模式提高了数倍的速度，另外，通过统一的批量分析规则，减少了对数据的重复访问，从而减少了整体分析的处理时间。

4 实际应用效果

国内某大型商业银行(以下简称 A 银行)经过若干年的信息技术发展，在操作风险防范上有了很多的经验和成果，但是也存在如前述那些问题。目前正在按照该框架进行操作风险管理系统的整合和建设，并取得了很好的效果。

(1) 解决了缺乏规划，重复建设，浪费投资的问题。

原先的 A 银行会计监控系统和反洗钱管理系统是两套独立系统，其功能是非常类似的，但是在建设上各自独立，投资浪费。根据新的操作风险管理框架，按照交易前，交易中，交易后三个组成模块进行部署，将会计监控系统和反洗钱系统中对实时交易流水进行实时分析的部分，统一归入到交易实时监控模块。同时，将两个系统中用来对银行业务操作数据进行批量分析处理的部分，统一归入交易后批量分析模块。由此，各风险控制要素依照各自特点纳入到整体框架中，解决了银行内部重复建设系统，浪费投资的问题。

(2) 通过统一整合批量分析，提高了性能。

在 A 银行原先的管理体系中，批量分析是由分散的系统完成的，不同的系统分别提取数据，多个系统通过各种方式(FTP、网页下载、UDP 等)获取业务数据，同样的数据内容会因为分析的角度不同而被重复处理。由于数据量较大，处理时间长，消耗资源多。按照新的框架进行整合后，采用了综合批量分析的方法，采用一个包含了数据采集、加工、存储、交换和管理的综合性服务平台，整合分析规则，减少对数据的重复访问，统一分析结果的管理方式、统筹结果数据的访问策略，从而大幅提高了系统整体的性能。

(3) 通过统一身份认证和权限管理，降低了管理风险。

原先 A 银行的员工可能拥有多个系统的 ID 和密码，当该员工调换岗位时，可能取消了其中的一个用户，但是漏掉了一个。而用户的权限管理更是分散在不同的应用中，这样带来了身份的混乱和大量的交叉关系，管理隐患很大。按照操作风险管理框架，目前正在采用统一的单点登录及身份认证、权限管理方式，着重解决个人身份多 ID 的管理漏洞问题，该平台提供了统一的基础安全服务技术架构，使业务系统可以很容易的集成到平台中，对业务系统中的身份信息、认证、审计、角色等进行统一管理，有效堵住了

(下转第 14 页)

(上接第 4 页)

管理漏洞。

(4) 通过完善流程控制机制，提高了风险管理的连续性和有效性。

在原先系统中，存在大量的各自为战的管理规则，有的控制点被重复处理，有的控制点被漏掉。目前，正在根据管理规则的性质，按照整体处理流程来部署，通过统一的流程控制机制，减少重复控制，堵住控制漏洞，提高有效性。

A 银行在新的操作风险管理框架中，结合银行系统实际业务需求，在全流程统一管理下，操作风险已经被大大减低。全行有 24 万柜员通过统一的安全认证平台进行身份控制，操作监控规则覆盖现金、支付、电子银行等，平均每天处理 6 千万笔以上的交易监控。整体信息系统的操作风险防范能力处于业内领先水平。

5 结语

通过计算机系统来实现操作风险的防范是非常复杂的问题，需要不断发展完善。本文通过对目前银行信息系统中关于操作风险防范相关系统的分析，描述了这个全流程的操作风险防范系统框架，并根据 A 银行的实际应用情况进行了深入分析。该框架层次分明、可扩展性好，可以作为各银行业务系统的有效补充。另外，需要注意计算机系统自身也是操作风险点之一，因此要重视计算机系统的安全管理、灾备等等。

参考文献

1 银监会.商业银行操作风险管理指引, 2007.

2 巴塞尔委员会.新巴塞尔资本协议, 2004.http://www.bis.org/publ/bcbs107.htm

3 张吉光.商业银行操作风险识别与管理.北京:中国人民大学出版社, 2005.1－5.

4 Stallings W. Cryptography and Network Security: Principles and Practice.3rd ed., Prentice Hall Inc., 2003.257－279.

5 汉王 OCR 识别技术在银行单证综合处理系统中的应用. http://www.hw99.com/tech/ocr-1.htm

6 艾林.基于数据挖掘技术的金融机构操作风险研究.[硕士学位论文].重庆:重庆大学, 2006.