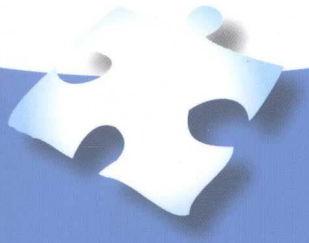
服务外包工程教育规划教材

全国服务外包人才培养高峰论坛组织编写



金融信息安全

徐成贤 主编

徐成贤 陈永强 陶利民 编著

清华大学出版社

服务外包工程教育规划教材

金融信息安全

徐成贤 主编

徐成贤 陈永强 陶利民 编著

清华大学出版社

北京

内 容 简 介

本书围绕金融信息化发展与金融服务创新过程中引起社会公众广泛关注的金融信息安全主题展开。第1章介绍金融信息化的内容、特点，分析其必然性和重要性及其系统的基本构成；第2章介绍金融信息化与服务外包中金融信息面临的安全问题及金融信息安全的重要性与复杂性；第3章涵盖金融信息安全体系，包括信息安全体系的基本结构、信息安全体系的组成、信息安全防御模型以及信息安全风险分析与评估；第4章重点介绍主要信息安全技术，包括物理层安全技术、网络层安全技术、系统层安全技术、应用层安全技术、数据安全技术与内容安全技术；第5章涵盖信息安全管理体系、信息安全规划、信息安全风险评估技术、信息安全策略的制订、信息安全管理标准、信息安全的法律法规与道德规范等；第6章分析金融服务外包所面临的各种新的金融信息安全问题以及对这些新金融信息安全问题的应对措施。书中包含大量金融信息安全的案例，每章后附有适量的练习与思考，供读者学习与复习。

图书在版编目（CIP）数据

金融信息安全/徐成贤主编. --北京：清华大学出版社，2013.1
服务外包工程教育规划教材
ISBN 978-7-302-30781-5

Ⅰ. ①金… Ⅱ. ①徐… Ⅲ. ①金融－信息系统－安全技术－教材 Ⅳ. ①F830-39

中国版本图书馆 CIP 数据核字(2012)第 287055 号

责任编辑：袁勤勇　张　玥
封面设计：常雪影
责任校对：白　蕾
责任印制：王静怡

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦 A 座　　**邮　　编**：100084
社 总 机：010-62770175　　**邮　　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质量反馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课件下载：http://www.tup.com.cn，010-62795954
印 装 者：北京鑫海金澳胶印有限公司
经　　销：全国新华书店
开　　本：185mm×260mm　　**印　　张**：16.5　　**字　　数**：380 千字
版　　次：2013 年 1 月第 1 版　　**印　　次**：2013 年 1 月第1 次印刷
印　　数：1～3000
定　　价：33.00 元

产品编号：049653-01

服务外包工程教育规划教材
编写委员会

丛书序

伴随着全球信息化浪潮，以信息技术为依托，利用外部专业服务商的知识劳动力，来完成原来由企业内部完成的工作，从而达到降低成本、提高效率、提升企业对市场环境迅速应变能力并优化企业核心竞争力的服务模式席卷全球。这种称之为“服务外包”的模式对新兴发展国家优化产业结构，转变贸易增长方式有着重要作用。印度、菲律宾、乌克兰等国家都在大力发展这种具有科技含量高、附加值大、资源消耗低、吸纳就业能力强的产业。

近年来，中国作为后起之秀，凭借在宏观经济环境、基础设施、政策支持、劳动力成本等方面的优势，已成为全球服务外包转移方首选的承接地之一。2011年，中国社科院发布的《中国服务外包发展报告》预测，10年之后，中国很有可能取代印度成为承接高科技服务最多的国家。伴随着产业的蓬勃发展，人才资源匮乏成了制约服务外包产业发展的主要瓶颈。但是，在传统教育体制下大量应届毕业生苦于就业无果，另一方面服务外包产业又需要大量人才。为此，以杭州为代表的21个国家服务外包示范城市专门针对服务外包产业需求建立了一批服务外包学院，形成政府、高校、服务外包企业、人才培训机构“四位一体”的服务外包人才培养体系，力求人才培养与企业需求无缝对接。

2011年4月，第二届“全国服务外包人才培养高峰论坛”在杭州召开，与会代表在探索服务外包人才培养新思路、新模式、新方法的交流中深感服务外包教材的匮乏，专门就教材编写开展了热烈的讨论，并决定成立“服务外包工程教育规划教材”编委会，组织来自国内外服务外包一线企业工程师和高等院校教师共同策划和编写教材，并启动了首批18本教材的编写工作。这套教材针对外语应用、软件与信息服务、金融信息服务、创新管理、跨国界文化等，涵盖了服务外包领域从业所需的知识和技能。这套教材以产业需求为导向，是校企合作开展服务外包人才培养的一次有益实践，对探索我国服务外包产业和工程创新人才的培养具有积极的意义。

最后，我衷心希望“服务外包工程教育规划教材”能成为一套高等院校、培训机构培养服务外包人才行之有效的教材，使服务外包人才培养工作事半功倍。也希望这套教材能成为教师及学生的良师益友，得到大家的喜爱。

中国科学院院士　何积丰

2011 年 9 月于杭州

前言

随着金融信息化的日益快速发展，信息系统在金融行业的应用越来越广泛，信息越来越向上集中，金融行业对金融信息化的依赖程度越来越高。信息技术的应用正在深刻改变着金融行业的传统操作方式，同时也在不断地促进金融服务的创新。网上银行、电子商务、电子支付工具、金融服务外包等创新服务方式正在兴起，金融服务运行的模式正在发生着深刻的变化。金融信息化的发展在给金融企业和社会发展带来巨大利益和便捷的同时，金融信息安全问题也越来越突出，“货币+信息”的现代金融特征，使金融业成为高风险的行业。金融信息系统本身的不安全因素、人为的攻击破坏、安全管理的不完善或执行不到位，都使金融信息系统潜伏着很多安全隐患。如系统发生故障或网络遭攻击导致业务中断、电脑病毒入侵、利用电脑系统或应用软件进行的内部欺诈或外部攻击、信息泄露等事件不时见诸媒体与网络，给人们的经济生活造成巨大危害。

面对越来越严峻的金融信息安全形势，对从事或即将从事金融信息系统或金融软件开发、设计、维护、管理与从事金融服务的人员进行金融信息安全方面的知识教育已十分迫切，但国内用于金融信息安全教学的教材却难觅芳踪。为适应高校金融工程、金融服务、计算机技术与软件工程等专业进行金融信息安全教学的需要，我们有针对性地编著了这本《金融信息安全》教材。

本书紧紧围绕“金融信息安全”这个主题，在介绍金融信息化建设的必然性及重要意义之后，对金融信息系统面临的安全问题与金融信息安全的复杂性作了详细的介绍与细致的分析。本书主要篇幅用于介绍信息安全体系、信息安全技术与信息安全管理方面的知识与要求。之后，针对金融服务外包这一创新型金融服务模式，进一步分析了金融服务外包会对金融信息安全产生的影响，分别从接包方、发包方与监管机构的角度对金融服务外包中的信息安全问题与管控等进行了分析。

期望通过学习本教材，读者能实现以下几个目标。

1. 通过第1、2两章的学习，了解金融信息化建设的重要性、金融信息化对金融企业、金融市场与广大金融用户产生的重大影响，了解金融信息

系统可能面临的形形色色的安全风险，以及金融信息安全的复杂性。

2. 通过第 3、4、5 章的学习，了解信息安全保障体系，了解与熟悉主要的信息安全技术，理解规范信息安全管理的重要性，并了解主要的信息安全管理标准与要求。

3. 通过第 6 章的学习，明白金融服务外包既是金融企业为提升自身核心竞争力所进行的金融服务创新，也是金融信息安全的新风险点，发包金融企业、接包服务企业与相关的金融监管机构都应对金融服务外包中的信息安全进行有效监管。

4. 作为金融行业或与金融服务相关的人员，应熟悉并严格遵守金融信息安全的法律法规与道德规范。

期望本教材的出版能对我国金融信息安全的教育与研究有所贡献。限于时间与作者水平，书中难免存有疏漏与不当之处，敬请广大读者批评指正。

作　者

2012 年 8 月于杭州师范大学

目录

第 1 章　金融信息化概述 …… **1**

1.1　金融信息化概述 …… 1
1.1.1　金融信息化的基本概念 …… 1
1.1.2　金融信息化电子化的内容 …… 2
1.1.3　金融信息化的特点 …… 5
1.2　金融信息化的意义 …… 6
1.2.1　金融信息化的必然性 …… 7
1.2.2　金融信息化的意义 …… 7
1.2.3　金融信息化的影响 …… 9
1.3　国内外金融信息化的发展与现状 …… 10
1.3.1　国外金融信息化发展概况 …… 10
1.3.2　中国金融业信息化的发展过程与现状 …… 13
1.3.3　我国金融信息化面临的问题 …… 18
1.4　金融信息系统的组成 …… 20
1.4.1　金融信息系统的空间结构 …… 20
1.4.2　金融信息系统的逻辑结构 …… 22
1.4.3　银行事务处理系统的结构 …… 24
1.4.4　金融事务系统中的交易 …… 26
练习与思考 …… 27

第 2 章　金融信息安全 …… **28**

2.1　金融信息安全的基本概念 …… 28
2.1.1　信息安全的概念 …… 28
2.1.2　信息安全的发展过程 …… 29
2.1.3　金融信息安全的目标 …… 31
2.2　金融信息安全面临的风险 …… 32
2.2.1　金融信息安全的几个概念 …… 32
2.2.2　金融信息系统可能面临的安全威胁 …… 33

2.2.3 电脑病毒 …… 36
2.2.4 金融信息系统信息安全风险产生的原因 …… 37
2.2.5 金融信息安全的主要风险点 …… 39
2.2.6 金融交易中的风险点 …… 46
2.3 金融信息安全的重要性 …… 50
2.4 金融信息安全的复杂性 …… 53
2.4.1 金融信息系统本身的复杂性 …… 53
2.4.2 金融信息系统安全风险的科技特性 …… 54
2.4.3 计算机金融犯罪的特性 …… 55
2.4.4 金融信息安全的特性 …… 57
练习与思考 …… 61

第3章 信息安全体系 …… 62

3.1 金融信息安全体系概述 …… 62
3.1.1 面向目标的知识体系结构 …… 63
3.1.2 面向应用的层次型技术体系结构 …… 63
3.1.3 面向过程的信息安全保障体系结构 …… 66
3.2 信息安全体系框架 …… 67
3.2.1 技术体系 …… 67
3.2.2 组织体系 …… 72
3.2.3 管理体系 …… 72
3.3 信息安全防御模型 …… 73
3.4 信息安全风险分析 …… 76
练习与思考 …… 86

第4章 信息安全技术 …… 87

4.1 物理层安全技术 …… 87
4.1.1 物理访问控制 …… 87
4.1.2 防灾 …… 88
4.1.3 防信息泄露 …… 90
4.1.4 容错容灾 …… 91
4.2 网络层安全技术 …… 92
4.2.1 防火墙技术 …… 93
4.2.2 虚拟专用网(VPN)技术 …… 97
4.2.3 新一代安全网关 …… 98
4.3 系统层安全技术 …… 99
4.3.1 安全扫描技术 …… 99
4.3.2 入侵检测技术 …… 100

4.3.3 防病毒技术…… 106
4.4 应用层安全技术 …… 110
4.4.1 身份认证技术…… 110
4.4.2 访问控制技术…… 113
4.4.3 安全审计技术…… 119
4.5 数据安全技术 …… 123
4.5.1 数据加密技术…… 123
4.5.2 数字签名技术…… 131
4.5.3 数据备份与恢复技术…… 135
4.6 内容安全技术 …… 138
4.6.1 内容安全概述…… 138
4.6.2 内容安全监测技术…… 139
4.6.3 反垃圾邮件技术…… 142
4.6.4 数字水印技术…… 147
练习与思考…… 152

第 5 章 信息安全管理 …… 153

5.1 信息安全管理概述 …… 153
5.1.1 信息安全管理的概念…… 153
5.1.2 信息安全管理的重要性…… 154
5.1.3 信息安全管理的内容与要素…… 155
5.1.4 信息安全管理的原则…… 156
5.1.5 信息安全管理体系…… 157
5.2 信息安全规划 …… 158
5.2.1 信息安全规划的设计原则…… 159
5.2.2 安全规划基本构成…… 160
5.2.3 信息安全规划内容…… 160
5.2.4 金融机构信息安全管理实施内容…… 161
5.3 信息安全风险评估 …… 164
5.3.1 信息安全风险评估的概念…… 165
5.3.2 信息安全风险评估的目的和意义…… 165
5.3.3 信息安全风险模型…… 166
5.3.4 信息安全风险评估方法…… 167
5.3.5 风险评估工具…… 170
5.4 信息安全策略 …… 172
5.4.1 信息安全策略基本概念…… 172
5.4.2 制定信息安全策略的原则与要求…… 174
5.4.3 信息安全策略的制订过程…… 177

5.4.4 安全策略的评价准则 …… 178
5.4.5 信息安全策略框架 …… 179
5.5 信息安全管理标准 …… 180
5.5.1 信息安全标准概述 …… 180
5.5.2 信息安全管理体系标准 …… 181
5.5.3 信息安全评估标准 …… 183
5.5.4 我国的信息安全管理标准与 GB 17859—1999 …… 188
5.5.5 ISO/TC68 与银行业务有关的信息安全标准 …… 190
5.6 信息安全法律法规与道德规范 …… 190
5.6.1 国际的信息安全法律法规 …… 190
5.6.2 中国的信息安全法律法规 …… 192
5.6.3 信息安全道德规范 …… 193
5.7 我国金融信息安全管理对策 …… 195
练习与思考 …… 196

第 6 章 金融服务外包中的信息安全 …… 198

6.1 金融服务外包信息安全的重要性 …… 198
6.1.1 金融服务外包潜在的信息安全风险 …… 198
6.1.2 金融服务外包信息安全事故的影响 …… 199
6.2 金融服务外包影响信息安全的因素 …… 202
6.3 金融服务外包中产生信息安全风险的根源 …… 208
6.4 金融服务外包安全风险的内部管理与控制 …… 213
6.4.1 发包金融企业对外包业务安全的控制与管理 …… 213
6.4.2 接包商对外包项目安全的管理和控制 …… 217
6.5 对金融服务外包的安全监管 …… 218
6.5.1 金融监管概述 …… 218
6.5.2 相关国家与国际组织对金融服务外包的监管 …… 218
6.5.3 中国对金融服务外包的监管 …… 222
6.5.4 中国对金融服务外包监管的分析 …… 225
练习与思考 …… 227

附录 A 我国已发布的相关信息安全标准(至 2010 年) …… 228

附录 B 我国已颁布的信息安全管理体系标准 …… 232

附录 C 与银行业务有关的国际信息安全标准 …… 233

附录 D 我国涉及信息安全方面条款的法律法规 …… 237

附录 E　中国互联网协会颁发的行业自律规范 …… 239

附录 F　银监会《电子银行业务管理办法》第五章　对业务外包管理的有关规定 …… 240

附录 G　《银行业金融机构信息系统管理指引》第六章　外包风险控制 …… 241

附录 H　关于境内企业承接服务外包业务信息保护的若干规定 …… 242

附录 I　《商业银行外包风险管理指引》(征求意见稿) …… 244

参考文献 …… 248

第1章 金融信息化概述

1.1 金融信息化概述

自1958年第一台计算机进入美洲银行以来，作为国民经济命脉的世界金融业随着信息技术的飞速发展，以惊人的速度推动了金融业务电子化信息化的进程。金融电子化信息化的出现不但从根本上改变了金融业务的处理手段、经营方式，开拓了新的业务领域，而且仍在继续改变着人们的生活与消费观念。现今，一切社会组织与个人，无论其自觉与否，无不直接或间接地感受到金融电子化信息化的存在，并享受其提供的形形色色的服务。

1.1.1 金融信息化的基本概念

对于金融信息化，不同领域有不同理解，下面分别给出金融行业、信息技术行业以及通信网络、计算机、信息资源和人力资源对金融信息化的认识。

(1) 金融行业对金融信息化的认识。金融信息化是指在金融领域全面发展和应用现代信息技术，以创新智能技术工具更新改造和装备金融业，使金融活动的结构框架重心从物理性空间向信息性空间转变的过程。

(2) 信息技术领域对金融信息化的认识。金融信息化是指信息技术(如计算机技术、通信技术、人工智能技术)广泛应用于金融领域，从而引起金融理论与实务发生根本性、革命性变革的过程。

(3) 通信网络、计算机、信息资源与人力资源等部门的认识。金融信息化是构建在由通信网络、计算机、信息资源和人力资源四要素组成的国家信息基础框架之上，由具有统一技术标准，通过不同速率传送数据、语音、图形图像、视频影像的综合信息网络，将具备智能交换和增值服务的多种以计算机为主的金融信息系统互联在一起，创造金融经营、管理、服务新模式的系统工程。

虽然各种观点的说法多少有些不同，但简言之，金融信息化是指在金融业务与金融管理的各个方面充分应用现代信息技术，深入开发、广泛利用金融与经济信息资源，加速金融现代化的进程，这个进程是发展的、动态的和不断深化的。金融信息化是国家信息化的一个重要组成部分，它与整个社会的信息化，与其他宏观管理部门的信息化，与居民、企业的信息化密切相关，相

辅相成。在不断发展的信息技术和经济全球化的推动下，金融服务与金融创新构成了现代经济的核心。

金融信息化的实质，是新兴的信息技术对传统金融业的一场经济革新，主旨在于把金融业改造成为典型的基于信息技术的产业，信息系统成为金融业战略决策、经营管理和业务操作的基本方式。金融业的信息化可以概括为以数据大集中为前提，以完善的综合业务系统为基础平台，以数据仓库为工具，以信息安全为技术保障，打造出现代化、网络化的金融企业。

信息系统即指提供信息服务，使人们获得信息的系统，它是人、规程、数据库、软件与硬件等各种设备、工具的集合，突出的是计算机、网络通信及信息处理等技术的应用[1]10。

1.1.2 金融信息化电子化的内容

金融信息化电子化主要包括如下内容[2]7。

1. 传统柜台业务的电子化

图 1.1 给出了一般银行的传统柜台业务，这些业务原来都是手工处理的。目前，它们依然是国内金融业务的主流，在门市业务中占用大量的人力。传统柜台业务电子化的主要目的是提高业务处理的效率，减轻劳动强度，增强服务能力。

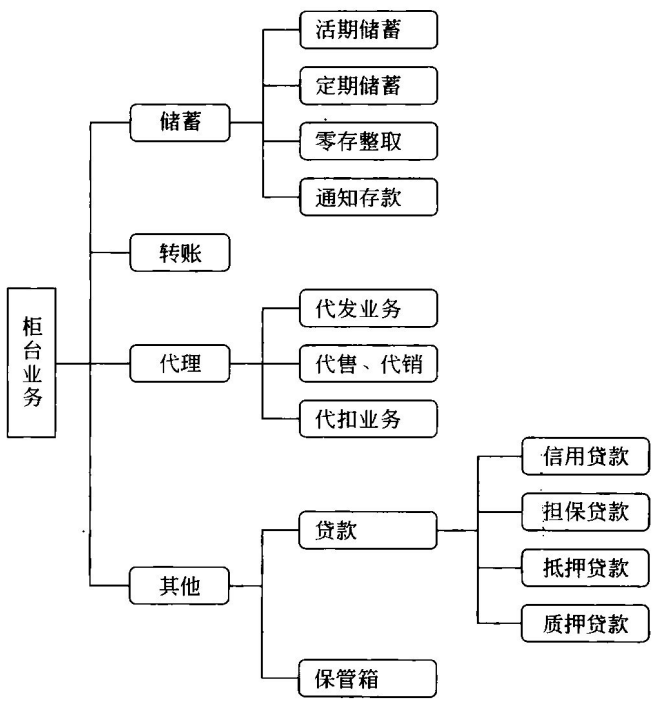


图 1.1 银行传统柜台业务

金融业务信息化电子化之后，部分（乃至大部分）柜台业务已转移至非柜台业务。图 1.2 给出了金融信息化电子化后的非柜台业务。

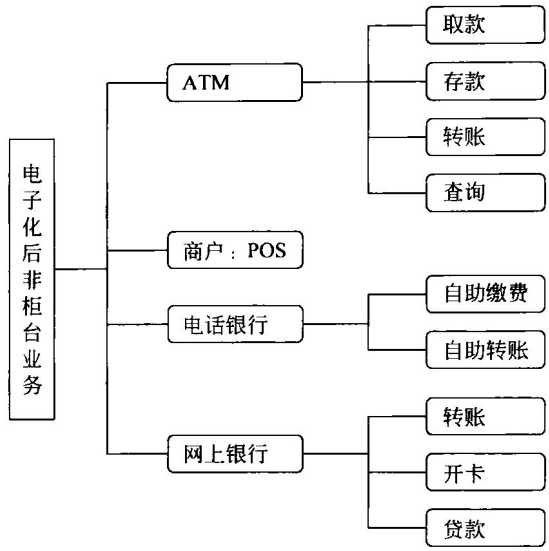


图 1.2　金融电子化后的部分非柜台业务

2. 外汇业务电子化

外汇业务主要涉及国际间的金融业务往来，电子化主要包括如下内容。

(1) 国际贸易结算业务电子化。

(2) 国际非贸易结算业务电子化。

(3) 外汇资金业务电子化。

(4) 外币存款业务电子化。

(5) 外汇清算电子化。

(6) 外汇会计核算电子化。

(7) 外汇外贸客户服务电子化。

(8) SWIFT 与 EDI 电子化。

3. 银行新型业务电子化

计算机与信息技术的广泛应用，使得金融行业有能力在传统柜台业务的基础上不断开拓新的业务领域，并实现这些新兴业务的电子化。这些新兴业务主要包括如下内容。

(1) 代发工资。

(2) 代收公共事业费(水、电、气、电话等)。

(3) 代理证券交割。

(4) 客户自助服务。

(5) 电子付款。

(6) 信用卡业务。

(7) 电话银行。

(8) 网上银行、手机银行。

(9) 理财。

(10) 网上交易。

4. 资金清算电子化

银行资金清算用于处理金融机构之间资金的相互流动,其运转速度的快慢制约着银行资金的周转,有着巨大的经济、社会效益。主要业务有如下内容。

(1) 同城资金清算电子化。

(2) 异地资金清算电子化。

5. 支付系统电子化

支付系统是银行为广大客户提供全面金融服务和中央银行为各商业银行提供支付资金最终清算的综合性金融服务系统。它以全国性跨行计算机通信网络为运营环境,将支付服务与清算功能有机融合为一体。下层支付服务系统是商业银行与其他金融机构为客户提供全面金融服务的基础金融业务系统,上层支付资金清算系统是中央银行为商业银行提供资金清算服务,并通过服务实施其货币政策职能的基础设施。

6. 其他非银行金融机构的电子化业务处理系统

其他非银行金融机构的电子化业务系统有会计业务系统、保险业务系统和证券业务支持系统等。会计业务系统是以会计数据为处理对象的计算机信息系统。它能对企业的会计数据进行收集、输入与存储、加工处理、输出与传递,为人们提供有用的会计信息,以支持一个组织有效运行和辅助管理决策的人机结合系统。

保险业务系统本质上是一个"综合"管理信息系统,重点围绕"合同管理"和"项目管理"进行。"合同管理"反映保险企业与客户之间的契约管理,它是保险企业服务和业务管理的综合体现,"项目管理"反映保险企业内部组织过程管理,它既涉及合同管理,也涉及企业内部的组织管理、核算和资源的合理运用。

证券业务支持系统是证券公司信息系统的主要组成部分,它支持证券公司证券业务的展开,包括柜台系统和周边委托系统,并能充分利用银行在营业网点与客户资源方面的优势,开展银证转账业务与银证通业务,提高了证券行业为客户服务的水平和运行效率。

7. 稽核工作电子化与计算机稽核

稽核工作电子化是借助计算机、通信等先进技术和工具,改进传统的稽核业务工作,提高稽核效率和稽核质量。计算机稽核是指用人工和计算机辅助等方法,对金融电子化各部门进行全面监控,即对计算机系统的开发、维护、运行和安全等进行审查和评价,以保证数据、交易、处理过程及处理结果的完整性、可控性以及故障情况下系统不间断运行和事故、差错责任的可追踪性,是金融电子化后稽核工作的新领域。两者的稽核对象不同,稽核内容和稽核方式也不同,但又同属于稽核这一大的概念。

8. 金融管理信息系统(Management Information System,MIS)

金融管理信息系统是金融企业经营管理的中心环节,是一个集成了计算机网络技术、通信技术、信息处理技术,对金融信息进行收集、传递、存储、处理,用于进行金融业务处理和辅助决策的一种智能化计算机系统。它通过采集并整合金融企业的业务信息,实现对客户信息、业务交易信息和经营管理信息的集成和一体化,为金融企业的各级管理人员、