ICS 03.060
A 11

JR

中华人民共和国金融行业标准

JR/T 0125—2015

商业银行内部控制评价指南

The guideline of internal control assessment in commercial banks

2015-10-21 发布　　2015-10-21 实施

中国人民银行　　发布

目　　次

前　言

本标准按照GB/T 1.1-2009给出的规则起草。

本标准由中国工商银行股份有限公司提出并具体制定。

本标准由全国金融标准化技术委员会（SAC/TC180）归口。

本标准起草单位：中国工商银行股份有限公司。

本标准主要起草人：刘卫星、仲安妮、马恒山、邱仁尔、严盖、顾红英、刘相勇、李宁、麻林涛、王路、刘叶梅、何小杨、刘畅、潘燕、赵立云、王勇飞、崔丽欣、陈海燕、王琪、钱晓军、张文甸、刘敏、周晔、黄太宏、施玲红、许嘉庆、许大庆、鲍婕、徐雯沁、林勇斌、许文嫣、陆继明。

引　言

本标准在遵循《企业内部控制基本规范》、《企业内部控制应用指引》、《企业内部控制评价指引》、《企业内部控制审计指引》、《商业银行内部控制指引》、《商业银行内部控制评价试行办法》、上海证券交易所《上市公司内部控制指引》、深圳证券交易所《上市公司内部控制指引》等法规和规范的基础上，根据中国商业银行的特点和内部控制评价的现状，提出了商业银行实施内部控制评价的操作指南，明确了“由谁评价”、“评价什么”、“如何评价”和“评价结果如何利用”的一系列问题。

本标准适用于指导中国商业银行开展的内部控制自我评价工作，旨在优化商业银行内部控制，提升风险管理水平和完善公司治理。各商业银行可以在指南的基础上根据本行业务实际和管理要求，调整、补充、细化评价指南，形成本行的评价操作指南。本指南非强制性要求。

商业银行内部控制评价指南

1 范围

本标准建立了以评价内容为基础，以评价标准、评价方法和评价程序为支柱，服务于评价目标的商业银行内部控制评价操作指南，明确了“由谁评价”、“评价什么”、“如何评价”和“评价结果如何利用”的一系列问题。

本标准适用于中国商业银行（以下简称商业银行）开展的内部控制评价工作。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

3 术语和定义

下列术语和定义适用于本文件。

3.1

内部控制 internal control

由董事会、监事会、高级管理层和全体员工共同实施的，旨在合理保证商业银行依法合规经营、资产安全和财务报告信息真实完整，促进商业银行提高经营效率与效果，实现发展战略目标的过程。

3.2

内部控制评价 internal control assessment

由商业银行董事会或类似权力机构按照规定的程序、标准、内容和方法，对商业银行内部控制有效性进行全面评价，形成评价结论，出具评价报告的过程。

3.3

评价主体 assessment subject

董事会或类似权力机构负责开展内部控制评价并出具评价报告。商业银行可以授权内部审计部门或专门的职能机构（以下统称评价机构）负责内部控制评价的具体组织实施工作。

3.4

评价目标 assessment objective

对银行内部控制状况开展监督评价，发现内部控制缺陷，促进相关问题的整改，提升和完善内部控制，以此促进商业银行内部控制目标的实现。

3.5

评价内容 assessment content

围绕内部环境、风险评估、控制活动、信息与沟通、内部监督五要素展开，具体可按公司、流程、信息科技等三个层面梳理的风险点和控制点开展测试和评价。

3.6

评价标准 assessment standard

衡量商业银行内部控制缺陷和控制有效性的重要指标，由业务标准和认定标准两部分组成。其中，业务标准是银行各项业务正常运行应遵循的控制要求；认定标准是衡量银行内部控制状况的依据和尺度。

3.7

评价程序 assessment procedure

实施内部控制评价的程序和步骤，分为计划准备、现场实施、报告编写和缺陷整改四个阶段。

3.8

评价方法 assessment method

为了达到内部控制评价目的而采取的途径、步骤、手段、工具、技术等的总称，主要包括风险评估、识别关键控制、风险控制矩阵、穿行测试、控制测试、专题讨论法、询问或访谈、问卷调查、流程描述、观察、实地查验、比较分析等方法。

4 内部控制评价框架

4.1 评价原则

内部控制评价宜该坚持以下原则：

a) 全面性原则。内部控制评价范围宜当包括内部控制的设计与运行，涵盖商业银行各项业务的全过程及所有机构、部门和岗位；

b) 重要性原则。内部控制评价宜在全面评价的基础上，根据本行风险管理状况挑选重点分行、高风险领域、重要业务单元和重大业务事项进行评价；

c) 客观性原则。内部控制评价宜以事实为依据，准确地揭示经营管理的风险状况，如实反映内部控制设计与运行的有效性；

d) 一致性原则。内部控制评价宜采用一致可比的程序、方法和标准，以确保评价过程的客观性及评价结果的可比性。

4.2 评价框架

商业银行的内部控制评价宜明确“由谁评价”、“评价什么”、“如何评价”和“评价结果如何利用”等一系列问题，因此，本操作指南构建了以评价内容为基础，以评价标准、评价方法和评价程序为支柱，最终服务于评价目标的屋型评价框架(见下图1)。

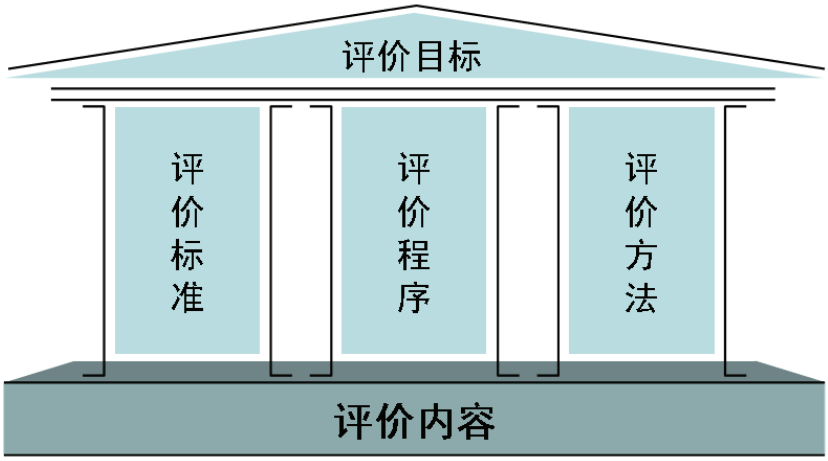

图 1　商业银行内部控制评价应用框架

在该框架中，内部控制评价目标处于统领和核心地位，是确定评价内容、评价标准、评价程序和评价方法时首要考虑的因素。

评价内容处于基础地位，评价目标决定评价内容的选择，评价内容决定评价标准、评价程序和评价方法的选择。

评价标准、评价程序和评价方法是内部控制评价的三大支柱。评价标准是内部控制评价的准绳；评价方法是内部控制评价的手段，方法的创新可以直接提高评价效率和质量；评价程序是内部控制评价的保障，遗漏某个评价环节可能直接影响评价结果的准确性。

4.3　评价组织

4.3.1　评价主体

内部控制评价的主体一般可以区分为责任主体和实施主体，责任主体是董事会或类似权力机构，实施主体是董事会或类似权力机构授权的专门评价机构。商业银行可以授权内部审计部门或专门的职能机构负责组织实施。

4.3.2　报告路线

为了保证内部控制评价的独立性和权威性，以及促使内部控制缺陷的有效整改，评价机构宜向董事会及其审计委员会报告工作，并在评价过程中加强与管理层的沟通。

4.3.3　组织分工

内部控制评价是针对内部控制开展的评价，不同层级的机构和人员按照分工，负有不同的内部控制评价职责。

a)　在治理层面：

1)　董事会是内部控制评价工作的决策机构，负责审议批准内部控制评价报告，并对内部控制评价报告的真实性负最终责任；审计委员会负责监督内部控制的有效实施和内部控制评价情况，审议内部控制评价报告，发表专项意见，并向董事会报告；

2)　监事会负责对董事会、高管层建立和实施内部控制情况进行监督，并对董事会审议通过的内部控制评价报告明确表示意见；

3) 高级管理层负责组织领导本行各级管理层开展与内部控制相关的监督和检查活动，接受和配合董事会开展的内部控制评价，并按照董事会的意见积极采取有效的措施整改内部控制缺陷。

b) 在部门和机构层面：

1) 各专业负责实施本专业的内部控制，开展专业自查，配合和接受评价机构评价，并落实内部控制的缺陷整改工作；

2) 各分支机构负责实施本机构的内部控制，协调机构内部检查监督资源，开展机构内部检查监督，配合和接受评价机构评价，并落实内部控制的缺陷整改工作；

3) 评价机构负责实施内部控制评价，在充分利用专业部门自查、各机构检查监督成果、评价机构开展的检查监督成果（若有）的基础上，对各专业、各层级机构实施的内部控制做出客观评价；

4) 评价机构宜从银行的整体发展战略和全行风险水平的角度出发，综合不同专业和机构的内部控制评价结果，对全行内部控制有效性开展整体评价。

4.3.4 评价周期

商业银行内部控制评价以一个会计年度为评价周期。一般为当年的1月1日—12月31日，并以12 月31 日作为年度内部控制评价报告的基准日。

4.3.5 评价频率

原则上，商业银行的内部控制评价宜每年开展一次。各商业银行也可根据经营业务调整、经营环境变化、业务发展状况、实际风险水平调整评价频率，并在对外披露的内部控制评价报告中予以说明。

4.4 评价目标

内部控制评价的目标是通过对银行内部控制状况的监督评价，发现内部控制缺陷，促进相关问题的整改，提升和完善内部控制，并以此促进商业银行内部控制目标的实现。具体目标包括但不限于以下方面：

a) 促进银行各项经营管理活动严格遵循国家法律法规、相关监管机构的要求和银行自身内部规章制度；

b) 促进银行提高财务报告及相关信息的真实性、完整性，增强本行信息披露的可靠性；

c) 促进银行提高风险管理水平，防范各类风险，保护银行资产安全；

d) 促进银行改进和优化内部控制程序，提高经营效率和效果；

e) 促进银行各级管理者和员工强化内部控制意识，保障内部控制体系的有效运行，促进自身发展战略目标的实现。

内部控制的建立和实施是一个不断优化和完善的过程，不同的商业银行内部控制的成熟程度也各不相同，宜根据本银行的实际情况逐步实现上述目标。

4.5 评价内容

4.5.1 评价内容概述

根据国家法律法规、监管要求及内部控制制度，围绕内部环境、风险评估、控制活动、信息与沟通、内部监督等内部控制五要素，按照公司、流程、信息科技等三个层面梳理风险点和控制点，形成全面覆盖商业银行集团各机构和各业务线的评价内容。

商业银行可根据自身的组织架构、业务条线管理模式，对评价内容进行动态调整。

在确定内部控制评价范围时，宜遵循全面性、重要性、客观性原则，在对集团总部、海内外分行及附属机构的不同业务进行全面、客观评价的基础上，重点关注重要业务机构、重大业务事项、高风险业务。

重要业务机构一般以资产、收入、利润等作为判定标准。包括集团总部，资产、营业收入、利润占集团合并总额比例较高的分行和附属机构。

重大业务事项一般是指重大投资决策项目，兼并重组、资产调整、产权转让项目，期权、期货等金融衍生业务，融资、担保项目，重大经营安排，采购大宗物资和购买服务，重大工程建设项目，年度预算内大额度资金调动和使用，以及其他大额度资金运作事项等。

高风险业务一般是指经过风险评估后确定为较高或高风险的业务。

4.5.2 公司层面

公司层面的内部控制主要指对整个商业银行各业务均有影响的一系列控制过程；旨在合理保证资产的安全目标、财务报告及相关信息真实完整目标、提高经营效率效果目标以及遵循国家法律法规和有关监管等基本目标得到实现，最终实现商业银行整体的战略目标。

公司层面的内部控制评价围绕内部环境、风险评估、控制活动、信息与沟通、内部监督等五大控制要素展开，分为35个领域。公司层面的评价内容具体如表1所示。

表1 公司层面的评价内容

序号	一级领域	二级子领域
1	内部环境	组织架构
2		发展战略
3		企业文化
4		内部审计
5		人力资源
6		社会责任
7	风险评估	风险管理体系
8		风险识别
9		风险评估
10		风险应对
11	控制活动	政策与流程
12		不相容职务分离控制
13		授权审批控制
14		会计系统控制
15		财产保护控制
16		预算控制
17		运营分析控制
18		绩效考评控制
19		重大风险预警控制
20		并表管理控制
21		反洗钱控制
22		关联交易控制
23		业务外包控制

序号	一级领域	二级子领域
24		业务连续性控制
25	信息与沟通	信息指标体系
26		信息系统建设
27		信息安全控制
28		信息交流机制
29		信息披露机制
30		反舞弊机制
31	内部监督	内部监督组织架构
32		内部监督制度
33		内部监督工作
34		整改监督机制
35		内部控制评价

4.5.3 流程层面

流程层面的内部控制主要指专门针对某项业务流程的一系列控制过程；旨在合理保证某项业务流程的经营效率和效果以及与该业务流程相关的财务报告及管理信息的真实、可靠和完整等基本目标得到实现。

流程层面的内部控制评价包括银行类和非银行类业务的8条业务线，主要是指公司业务、投行业务、零售业务、资产管理、资金业务、支付与结算、中间业务以及其他银行类业务；评价内容还包括基金、租赁等非银行类业务。流程层面的评价内容具体如表2所示。

表 2　流程层面的评价内容

序号	业务类	业务线	一级流程
1	银行类	公司业务	公司贷款
2			公司存款
3			票据融资
4			国际结算
5			贸易融资
6		投行业务	投资银行
7		零售业务	个人存款
8			个人贷款
9			银行卡
10			私人银行
11		资产管理	资产托管
12			养老金
13			贵金属
14			理财
15		资金业务	债券投资与交易
16			外汇交易
17			货币市场业务
18			衍生产品交易
19			债券承销发行
20		支付与结算	运行管理
21		中间业务	电子银行
22			代理业务
23		其他	财务会计管理
24			资产负债管理
25			产品创新管理
26	非银行类	非银行业务	租赁
27			基金

4.5.4　信息科技层面

信息科技层面的内部控制主要指合理保证商业银行内部使用计算机系统进行信息管理的机制得到有效运行的一系列控制过程。信息科技层面评价是对流程层面控制的重要支持，信息科技层面分为七部分：信息科技治理、信息科技风险管理、信息安全、信息系统开发测试和投产、信息科技运行管理、连续性管理、外包服务管理。信息科技层面的评价内容具体如表3所示。

表 3　信息科技层面的评价内容

序号	一级领域	二级领域
1	信息科技治理	治理架构
2		控制环境
3		信息与沟通
4		监督与评价
5	信息科技风险管理	风险管理策略
6		风险识别和评估
7		风险监测和应对
8	信息安全	总体管理
9		物理访问控制管理
10		网络安全管理
11		操作系统及数据库安全管理
12		数据安全管理
13		应用系统访问控制管理
14		终端设备安全管理
15	信息系统开发、测试和投产	总体管理
16		立项管理
17		需求管理
18		系统设计
19		编码及自测
20		项目测试
21		投产与推广
22		项目后评价
23	信息科技运行管理	总体管理
24		机房环境及设施管理
25		批处理管理
26		服务管理
27		性能容量管理
28		配置管理
29		事件、问题和变更管理
30	业务连续性管理	备份管理
31		业务影响性分析
32		业务连续性计划
33	外包服务管理	外包组织架构管理
34		外包战略风险管理
35		外包服务实施管理

4.5.5 内部控制评价的汇总层级逻辑框架

内部控制评价涵盖所有业务和流程，涉及商业银行网点、支行、二级分行、一级分行、附属机构、总行等多个层级。针对不同的机构和业务开展评价后，需要对评价发现（缺陷）进行自下而上的逐级汇总，上一层级的评价结论宜涵盖下一层级的评价发现，最终形成的银行集团层面的评价结论宜能客观反映商业银行的内部控制实际状况。在汇总过程中，可以按以下逻辑层级（图2）进行逐级归纳提炼。也可以根据管理需要，分别按业务条线汇总、按层面汇总、按机构汇总等。

第一层	集　团					
第二层	银行类			非银行类		
第三层	公司层面	流程层面	信息科技层面	公司层面	流程层面	信息科技层面
第四层		业务线			业务线	
第五层	一级领域	一级流程	一级领域	一级领域	一级流程	一级领域
第六层	二级子领域	二级子流程	二级子领域	二级子领域	二级子流程	二级子领域
第七层	产品/服务			产品/服务		
第八层	风险点/控制点			风险点/控制点		
注：二级子流程						
*二级子流程：是一级流程的细化分类。按照巴塞尔新资本协议（2004）中的分类方法，业务线下面可以划分一级流程，一级流程下还可以根据业务实际划分二级流程。如零售业务线下可以分为个人存款、个人贷款、私人银行、银行卡等四个一级流程。个人贷款又可向下细分为个人住房贷款、个人消费贷款、个人经营贷款等二级流程。						

图 2　集团评价层级逻辑框架

4.6 评价标准

4.6.1 业务标准

业务标准是商业银行各项业务正常运行宜遵循的控制要求，是对经营管理中内部控制有效性进行评价的参照对象。业务标准由监管法规、行业最佳实践以及商业银行内控制度组成，涵盖经营管理、业务操作、产品和信息系统等各个领域，细化到每个领域中的关键控制点。

业务标准与评价内容相对应，分为公司层面、流程层面、信息科技层面三个方面的标准：

a) 公司层面业务标准。围绕内部环境、风险评估、控制活动、信息与沟通、内部监督等内部控制要素展开，每个控制要素分为若干个控制领域，每个控制领域下细分为多个关键控制点，每个关键控制点均设置相应的业务标准；

b) 流程层面业务标准。围绕内部控制活动展开，商业银行的控制活动一般包括银行类和非银行类的 8 条业务线及其下属子流程，业务标准针对不同业务流程中的关键控制点设定；

c) 信息科技层面业务标准。围绕计算机系统及其管理活动展开，分别针对信息科技治理、信息科技风险管理、信息安全、信息系统开发测试和投产、信息科技运行管理、连续性管理、外包服务管理中的关键控制点设定。

这部分的具体内容详见5、6、7三章中相关领域的控制要求。商业银行在制定业务标准时宜结合本银行的业务特点和管理特征，注重平衡成本与效益、控制状况与风险偏好的关系，并随业务变化定期更新。

4.6.2 认定标准

认定标准是衡量商业银行内部控制状况的依据和尺度，由缺陷认定标准和有效性认定标准组成：

a) 缺陷认定标准。内部控制缺陷按其问题产生的成因分为设计缺陷和运行缺陷，按影响控制目标的严重程度分为重大、重要和一般三个等级。建议商业银行根据自身实际情况，采取定量和定性相结合的方法，参考如下标准[1]）（如表 4 所示），对不同等级的内部控制缺陷的认定标准进行具体定义，认定标准仅需满足其中任意一项即可认定；

表 4　内部控制缺陷认定标准

缺陷等级	定义	认定标准	
		定量标准	定性标准
重大	指一个或多个控制缺陷的组合，可能导致企业严重偏离控制目标。	1、财务损失按照损失金额占当年度集团营业收入的比例≥1%； 2、财务报告错报，按照错报金额占当年末集团资产总额的比例≥0.25%； 3、财务报金额占当年度利润总额的比例≥5%。	1、对本行整体控制目标的实现造成严重影响； 2、可能产生或者已经造成重大金额的财务损失或财务报告的错报； 3、违反有关法律法规或监管要求，情节非常严重，引起监管部门的严厉惩戒或其他非常严重的法律后果； 4、可能导致业务或服务出现严重问题，影响到数个关键产品/关键客户群体的服务无法进行； 5、造成的负面影响波及范围很广，引起国内外公众的广泛关注，对本行声誉、股价带来严重的负面影响；
重要	指一个或多个控制缺陷的组合，其严重程度和经济后果低于重大缺陷，但仍有可能导致企业偏离控制目标。	1、财务损失按照损失金额占当年度集团营业收入的比例区间为[0.05%-1%)； 2、财务报告错报，按照错报金额占当年末集团资产总额的比例区间为[0.0125%，0.25%)； 3、财务报金额占当年度利润总额的比例区间为[0.25%，5%)。	1、对本行整体控制目标的实现造成一定影响； 2、可能产生或者已经造成较大金额的财务损失或财务报告的错报； 3、违反有关法律法规和监管要求，情节比较严重，引起监管部门较为严重的处罚或其他较为严重的法律后果； 4、可能导致业务或服务出现一定问题，影响到一个或数个关键产品/关键客户群体的服务质量大幅下降； 5、造成的负面影响波及行内外，引起公众关注，在部分地区对本行声誉带来较大的负面影响；
一般	除重大缺陷、重要缺陷之外的其他控制缺陷。	1、财务损失按照损失金额占当年度集团营业收入的比例＜0.05%； 2、财务报告错报，按照错报金额占当年末集团资产总额的比例＜0.0125%； 3、财务报金额占当年度利润总额的比例＜0.25%。	1、对本行整体控制目标的实现有轻微影响或者基本没有影响； 2、可能产生或者已经造成较小金额的财务损失或财务报告的错报； 3、违反有关法律法规或监管要求，情节轻微，引起监管部门较轻程度的处罚或其他较轻程度的法律后果； 4、可能导致业务或服务出现一定问题，影响到一个或数个关键产品/关键客户群体，并且影响情况可以立刻得到控制； 5、造成的负面影响局限于一定范围，公众关注程度较低，对本行声誉带来负面影响较小。

b) 有效性认定标准。在内部控制缺陷认定标准的基础上，商业银行可根据自身实际情况建立内部控制有效性的认定标准，内部控制有效性可分为有效或无效，如表 5 所示。

1) 定量和定性标准在设计过程中，参考了国际四大会计师事务所实施财务报告内部控制评价中使用的领先实务，其中定性标准的设定还参考了美国 PCAOB 公众公司会计监管委员会对内部控制缺陷的定义。

表 5　内部控制有效性认定标准

	控制有效性等级	定义	认定标准
1	有效	被评价对象的内部控制建立健全并有效实施。如果某项控制由拥有必要授权和专业胜任能力的人员按照规定的程序与要求执行，能够实现控制目标，表明该项控制的设计是有效的。如果某项控制正在按照设计运行,执行人员拥有必要授权和专业胜任能力，能够实现控制目标，表明该项控制的运行是有效的。	被评价对象没有重大缺陷;内部控制设计适当且得到贯彻执行。
2	无效	被评价对象的内部控制未建立、不健全或已建立健全的内部控制体系未得到有效实施。	被评价对象存在重大缺陷;内部控制未建立或不健全,存在无控制或控制失效的情况;违反监管机构规定并受到重大处罚。

4.6.3　内部控制缺陷和有效性之间的关系

内部控制缺陷和有效性之间存在一种相互的对应关系，这种对应关系如表6所示。

单个控制点可以依据评价发现（即内部控制缺陷）出具有效或无效的评价结论。各控制点发现的内部控制缺陷可以按照4.5.5内部控制评价的汇总层级逻辑框架中所列示的层级,进行自下而上的逐级归纳、提炼、汇总。各业务条线、各机构的控制有效性结论应依据逐级汇总的评价发现产生，上一层级的评价结论应涵盖下一层级的评价发现，最终形成的银行集团层面的评价结论应能客观反映商业银行的内部控制实际状况。

表 6　缺陷标准与有效性标准对应关系表

缺陷标准	有效性标准	对应说明
重大缺陷	无效	当存在一个或多个内部控制重大缺陷时,应当作出内部控制无效的结论
重要缺陷	有效	存在重要缺陷时，如董事会和高级管理层能承受相应风险，仍可做出内部控制有效的结论。但重要缺陷应当引起董事会、经理层关注。
一般缺陷	有效	当存在一般缺陷，且缺陷数量在管理层可容忍范围内时，可以作出内部控制有效的结论

4.7　评价程序

4.7.1　评价程序概述

内部控制评价是一个闭合式的循环过程（见图3），可以设定为四个阶段：计划准备、现场实施、报告编写和整改跟踪，每个阶段包含若干个评价步骤。

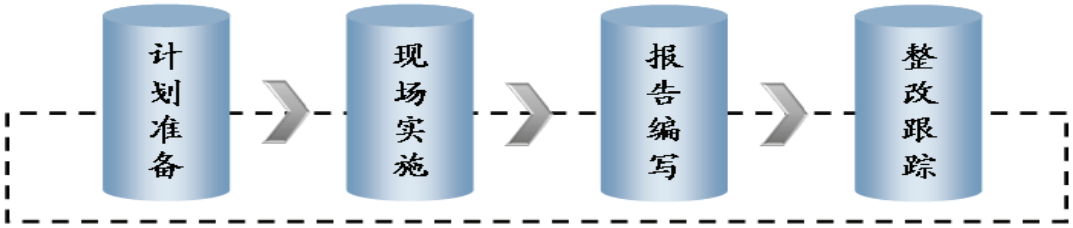

图 3　内部控制评价程序

4.7.2　计划准备阶段

主要包括收集资料、梳理流程、评估风险、建立评价标准、编制评价方案、开展非现场测试等六个步骤。

a) 收集资料。商业银行需要采集充分的内部控制信息，包括相关的法律法规和监管规章、银行自身的内部控制制度、操作手册和规程、银行业务流程等；

b) 梳理流程。评价工作开始前，评价人员需要先行梳理业务或管理流程，采用文字描述和绘制流程图相结合的方式，制作业务流程文档并定期更新；

c) 评估风险。结合内部控制评价目标，采用自上而下的方式，确定流程中的重要风险点和关键控制点，据此构建风险控制矩阵；

d) 建立评价标准。评价标准包括业务标准和认定标准，标准的建立应体现银行的业务特点；

e) 编制评价方案。评价方案包括评价目的、范围、对象、内容、标准、步骤、方法、时间进度和相应的资源配置等。方案一般附有评价操作手册、工作底稿等；

f) 开展非现场测试。商业银行信息化程度较高，可以利用信息系统开展数据挖掘，筛选可疑线索，确定抽样测试数据，以增强现场测试的针对性，提高评价效率。

4.7.3　现场实施阶段

主要包括开展穿行测试、开展控制测试、认定缺陷和综合评价等四个步骤。该阶段的各项工作过程及结果应当在工作底稿中予以准确和真实的反映。

a) 开展穿行测试。评价人员按照事先确定的不同层面和业务流程，逐个抽取一笔或若干笔业务样本，从头到尾检查业务实际处理过程，以验证所描述的内部控制设计是否存在，是否合理；

b) 开展控制测试。对已确认为设计有效的控制需要进行控制测试，以判断其运行是否有效。评价人员按照内部控制发生的频率和设定的置信度，采取抽样方法，选取一定数量的业务样本执行控制测试，判断其控制运行的有效性；

c) 认定控制缺陷。缺陷认定是指评价人员描述测试中发现的缺陷，并根据其对内部控制目标的影响程度将缺陷进行定性和归类的过程。如多个评价小组同时开展评价工作，可以用问题汇总表的形式对缺陷进行汇总、归纳、提炼和等级评定，发现的重大缺陷应及时以适当的形式向董事会报告；

d) 评价控制有效性。评价控制有效性包括对内部控制设计有效性和内部控制运行有效性的评价。商业银行可组成评价小组，综合分析缺陷产生的原因、潜在影响、性质、整改措施及整改结果等信息，对缺陷进行重新判断、对缺陷类型和缺陷等级进行调整和修正。与内部控制目标比较分析后综合得出整个银行的内部控制有效性评价结论。重大缺陷应当由董事会予以最终认定。

4.7.4 报告编写阶段

报告编写阶段主要包括报告编写、沟通交流和报告报送三个步骤。

a) 报告编写。评价报告应如实反映被评价单位内部控制状况、报告内部控制缺陷及其认定情况、提出改进建议、表明评价结论；

b) 沟通交流。评价报告在报送董事会及其审计委员会前，宜与被评价单位和相关管理层进行充分沟通和交流，听取反馈意见，并就整改措施达成共识；

c) 报告报送。内部控制评价报告宜报送商业银行董事会审定，并以适当的形式向监事会报告。董事会具有对重大缺陷及内部控制有效性认定的最终决定权，董事会对内部控制评价报告真实性承担最终责任。

4.7.5 整改跟踪阶段

针对内部控制评价报告中列示的问题制定整改计划并采取改进措施以优化控制，是被评价单位各级管理层的责任。

为了确保整改的效果，评价机构宜安排必要的资源，监督和跟踪各相关单位和业务管理部门的缺陷整改进度，必要时对整改的结果实施后续评价，后续评价可采用抽查或全查的方式，关注缺陷是否得到整改，整改效果如何，以确保相关整改措施落到实处。

4.8 评价方法

4.8.1 评价方法概述

内部控制评价需要各商业银行结合业务实际，采用一种或多种评价方法。这些评价方法可以结合评价程序依次展开，如风险评估、识别关键控制技术、编制风险控制矩阵、实施穿行测试、控制测试等 ；也可以结合评价需要同时实施，如询问和访谈、开展问卷调查、进行对比分析、召开专题讨论会等。不同的评价方法会用到不同的评价工具，如风险控制矩阵、穿行测试模板、控制测试模板等，本指南在介绍评价方法时进行了同步介绍。

4.8.2 风险评估

风险评估是在识别商业银行风险的基础上，通过评估固有风险、控制有效性水平，进而评估得出剩余风险的过程。这里所说的风险评估并非是对银行面临风险的准确计量，而是对评估对象风险等级的划分和排序。在开展内部控制评价前，可以使用风险评估方法确定评价机构、业务线和评价重点，并识别出对银行目标足以造成实质性影响的重大风险。

风险评估体系是由评价单元模块、风险集合模块、风险发生可能性模块、风险影响程度评估模块、有效性评估模块、固有风险评估模块以及剩余风险评估模块七部分构成（见图4）。

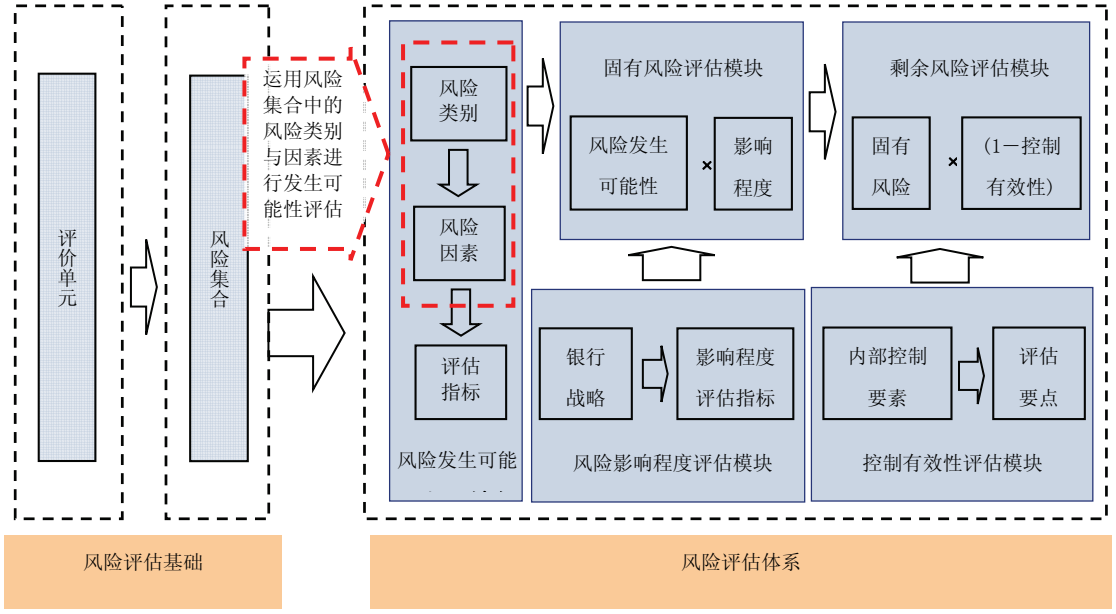

图 4　风险评估框架

a)　构建评价单元。开展风险评估首先要明确风险评估的对象，即评价单元。评价单元分为产品和机构两个维度。其中：产品维度包括产品线和管理线两类；产品线为对外提供的产品和服务；管理线为从各部门内部管理职能衍生出来的、无法与对外产品线进行明确对应的内部管理流程，可以理解为对内提供的产品；机构维度分为境内机构和境外机构两类。评价单元示例如表 7 所示。需要说明的是，评价单元不是一成不变的，随着商业银行战略目标和各类业务和机构的不断发展变化，评价单元的划分须不断更新调整；

表 7　评价单元示例

机构维度	产品维度				
	产品线			管理线	
	银团贷款	贸易融资	·	现金管理	·
××分行	评价单元 1	评价单元 3	……	评价单元 5	……
××部门	评价单元 2	评价单元 4	……	评价单元 6	……
……	……	……	……	……	……

b)　建立风险集合。风险集合存在于银行各个机构以及各类业务之中，在定义风险集合时，首先要确定评价对象面临哪些风险，即风险类别。根据 COSO、巴塞尔委员会、监管要求以及国内外银行的先进实践，商业银行面临的风险大致可分为 6 大类（见图 5）：战略风险、信用风险、市场风险、操作风险、声誉风险、流动性风险。每类风险又含有多种不同层次的风险因素，例如，操作风险的风险因素包括人员、系统等一级因素，同时人员因素可以细分为人员配备充足性、人员胜任能力、人员流动情况等二级因素，每个二级风险因素事先定义一个或多个评价指标；

图 5　风险集合图

c)　建立评价单元和风险集合的影射关系。评价单元和风险集合共同构成了风险评估的基础。评价单元构成风险评估的对象，但离开风险集合就不可能有风险评估。而风险集合则是一个概念，不与具体的评价单元结合同样没有意义。开展风险评估工作，需要将风险集合中包含的风险类别、风险因素、风险指标等等，映射到具体的评价单元中，与具体的机构、产品、管理、流程相结合，从而形成具体的风险点。实际上这些风险点才是真正的评估对象；

d)　建立评估模型。风险可以分为固有风险和剩余风险两种，其关系可以用以下公式表示：固有风险=风险发生可能性×风险程度；剩余风险 = 固有风险×（1－控制有效性）[2)]。对固有风险评估的目的在于从银行面临的众多风险中确定哪些风险是重要风险，以及这些风险分布在那些业务领域和环节。剩余风险表明：在已实施控制的情况下，银行尚存在的风险。对控制有效性的判定可以参考以往年度的专业检查成果和评价成果；

e)　进行风险排序。在对固有风险、控制有效性、剩余风险进行评估后，可以对风险进行排序，便于直接展示。

2)　控制有效性：此公式中的控制有效性指的是根据往年检查监督的结果，对以往年度的业务控制是否有效进行。给个案例。

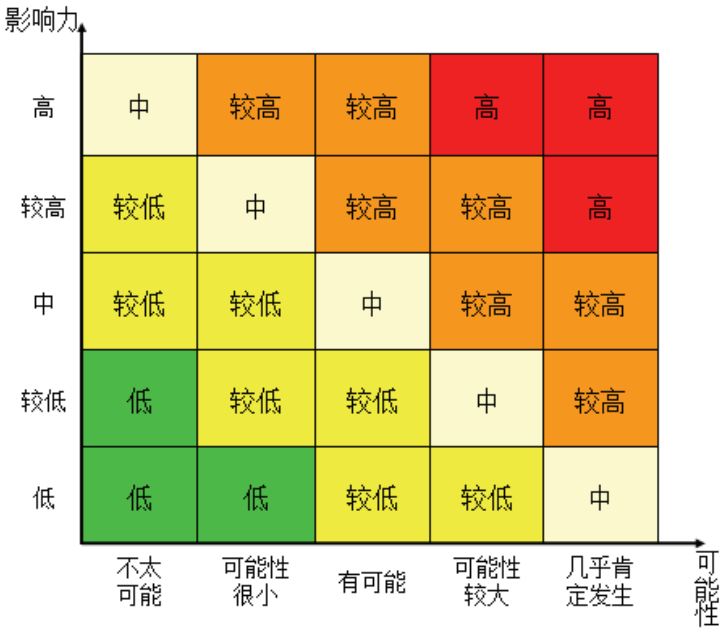

图 6　风险热图

从图6中可以看出，图中的红色区域代表着银行面临的最重要的风险领域，这些风险足以对银行目标产生实质性的不利影响，也是董事会和高管层关注的重点领域。风险导向的内部控制评价模式，要求评价部门把资源配置在与银行目标最相关的重大风险之上，实际上这些重大风险，就是董事会和高管层最关注的风险领域。

下面以理财业务为例，详细说明如何利用风险评估方法，找出影响力大、风险高的评价机构和业务产品，锁定评价重点：

a) 首先确定理财业务为评价单元；

b) 在全面分析理财业务发展现状基础上，确定理财产品面临的风险集合，包括信用风险、市场风险、操作风险和流动性风险等；

c) 从机构和产品两个维度，分别评估风险发生可能性和风险影响程度。如在开展机构风险评估时，可根据银行理财业务发展情况，设定如下影响力风险因素：产品收入、产品规模、项目推荐发生额和产品推广；设定如下可能性风险因素：操作风险、理财产品系统管理、内部检查和理财项目管理。在开展产品线风险评估时，可根据理财产品业务特点，设定理财产品线的影响力风险因素：规模占比、存量占比、战略导向，设定可能性风险因素为：系统控制程度、业务环节复杂程度、可能损失程度；

d) 根据确定下来的风险因素，结合银行实际对固有风险进行评分，绘制境内分行（营业部）理财业务机构和产品的风险视图；

e) 根据以往年度的检查监督成果和评价发现，评估不同机构和产品的控制有效性；

f) 参考固有风险和控制有效性的评估结果后，形成机构和产品的剩余风险评估结论，绘制产品及机构的风险热图，选择影响力大和高风险的机构及产品线作为审计重点。

4.8.3　识别关键控制技术

商业银行的内部控制纷繁复杂，从成本效益角度考虑，管理层应重点控制那些对银行目标有战略性影响的因素，包括关键性的活动、业务、产品和事件。这就需要引入关键控制的概念。

COSO认为，关键控制是指那些在评估整个内部控制体系是否能达成既定目标时，可以提供足够的支持来得出合理结论的控制。

关键控制对其他控制起着基础性作用、缺失这种控制就会增加风险。关键控制有效则整体控制就可能有效。

一般来讲，关键控制有以下六个特征：

a) 关键控制总是基于实现控制目标而言的且与重大风险相关的控制；
b) 关键控制是商业银行应有的和已设的所有控制中最关紧要的部分；
c) 关键控制是对商业银行行为具有战略性影响的控制；
d) 关键控制出现偏差将对商业银行造成很大危害；
e) 关键控制是在各项控制中必不可少和不可替代的控制，关键控制的失效可能会严重影响控制目标，而不会被其它控制及时发现；
f) 关键控制的执行可以防止其它控制的失效，或在对控制目标产生实质性影响前及时发现这些控制失效。

在资源有限的情况下，我们通过以上特征来识别关键控制，并且将这些控制作为内部控制评价的测试重点。

4.8.4 风险控制矩阵

控制矩阵是用表格的形式详细记录和汇总相关流程的关键风险点与关键控制，以及各控制点详细情况的文档。它提供了一个严谨的架构，将可能的风险与对应的控制直接联系起来，确保所有相关内部控制都得到充分的记录。

风险控制矩阵一般包括风险点描述、风险等级、风险类别、控制要求、控制依据、测试结果等内容，多角度、直观的记录和展示某一业务流程或风险事项的风险控制状况。风险控制矩阵对评价人员接下来开展的穿行测试和控制测试工作均能起到控制、引导及汇总的作用。风险控制矩阵工作底稿样例，详见表8。样例中罗列了常用的风险控制矩阵要素，商业银行可以根据本行业务实际，选取下表中的部分或全部栏目（标＊栏目为必选项），或补充其他新内容，构建符合本行特点的风险控制矩阵。

表 8 风险控制矩阵工作底稿样例

编号	栏目	填写内容
1	评价领域	最小控制领域，可细化到二级领域。
2	风险点编号	风险点的编号。
3	风险点描述（＊）	描述该流程在操作过程中存在的关键风险。
4	固有风险级别（＊）	引用风险评估结果，可分为 5 档，以分值展示，如 1 低,2 较低,3 中等,4 较高,5 高。
5	风险类别（＊）	同风险集合分类，可分为战略风险、信用风险、市场风险、操作风险、声誉风险、流动性风险等。
6	控制点编号	控制点的编号。
7	控制要求（＊）	为降低操作过程中存在的关键风险而应采取的最佳控制措施，与风险点描述存在明确的对应关系。
8	控制依据（＊）	描述相关的文件名称、文号和主要规定。控制 依据来自于外部监管要求、银行内部管理规定等方面。
9	评价目标	即银行内部控制评价目标：合理保证企业经营管理合法合规，资产安全，财务报告及相关信息真实完整，提高经营效率和效果，促进企业实现发展战略。

编号	栏目	填写内容
10	本行实际操作描述	描述被评价机构实际的控制活动情况，包括制度的设计和执行情况。
11	测试步骤及测试方法（*）	测试的具体步骤描述和方法介绍，用以明确统一操作步骤，统一测试方法。
12	测试结果（*）	评价人员开展测试后的结果描述，可以为正面的评价，也可以为发现缺陷的描述。
13	预防性控制或检查性控制	预防性控制主要应用在正常流程中的每一交易开始，防止错误的发生。检查性控制则主要检查流程中错误的发生可能。
14	控制行为出现的频率	可分为一天多次、每天、每周、每月、每季、每年、无法判断等。该栏目是决定控制测试抽样数量的关键因素。
15	控制活动种类	可为不相容职务分离控制、授权审批控制、会计系统控制、财产保护控制、预算控制、运营分析控制、绩效考评控制、其他等。该栏目主要用于控制点和发现问题的统计分析。
16	所属控制组	可分为人工、IT、人工依赖 IT。该栏目是决定控制测试抽样数量的关键因素。
17	应用控制类型	仅适用于 IT 控制组。人工和人工依赖 IT 不用填写。 下拉框：实时校验与编辑检查、配置控制、计算机计算、登录权限与岗位分离、自动系统接口/对账例行程序。该栏目主要用于信息科技层面的评价。
18	如为人工控制，能否通过系统实现	适用于人工和人工依赖 IT 控制组。填写是或否。该栏目为银行加强信息系统建设，利用系统硬控制提供参考。
19	适用的 IT 系统	填写具体的 IT 系统名称。

4.8.5 穿行测试法

穿行测试是指在每一类业务流程或业务循环中选择具有代表性的一笔或若干笔具体业务，按照业务流程规定从头到尾重新操作一遍，检查、验证业务流程中各个控制点的实际执行情况与所描述的内部控制是否一致，判断被评价单位内部控制完整性、真实性和健全性的一种方法。

穿行测试工作底稿中应详细记录测试的样本、穿行测试涉及的控制点、测试程序、获取的测试资料、发现的问题以及对该流程控制设计有效性评价等信息，穿行测试的工作底稿样例，详见表9。

表 9 穿行测试工作底稿样例

编号	栏目	填写内容
1	子流程名称及编号	填写子流程的名称和标准编号。
2	机构名称	填写被测试的机构名称。
3	测试人	填写执行测试的人员。
4	测试时间	填写测试完成的时间。
5	审阅人	填写对穿行测试进行复核的人员。
6	审阅时间	填写对穿行测试完成复核的时间。
7	流程概要	按照相关业务的操作流程依次填写相应的流程步骤。针对一项业务流程的穿行测试，该栏目填写完毕后应依次列示出整个流程中的各个步骤。
8	涉及控制点	按照相关业务的操作流程依次填写相应的控制点。此处填写的控制点应全部包含于“流程描述模板”中的“对应的控制”板块中。
9	穿行测试程序	针对测试控制点对相应的穿行测试程序进行简单描述。穿行测试可能使用的程序包括询问、观察、检查、实地查验等。在填写此栏信息时，对于不同的程序分别的具体要求为。

编号	栏目	填写内容
		1.询问：要求具体记录与谁进行的访谈、什么时间、访谈内容和结论。 2.观察：包括观察事项、什么时间、结论等。 3.检查：检查文档名称，检查的文档中是否有控制实施证据，结论。 4.实地查验：查验具体事项，结论。 5.重新执行：重新执行的方式，结论。
10	穿行测试资料	按照相关业务的操作流程依次填写测试流程所包含的全部资料名称。针对一项业务流程的穿行测试，该栏目填写完毕后应列示了该流程的全套文案资料。
11	穿行测试资料编号	将穿行测试获取的资料进行连续编号。此处填写相应文件的编号号码。
12	发现缺陷	此栏应对在穿行测试阶段发现的缺陷进行描述。描述不应只局限于问题的表象，还要写清楚问题产生的原因。
13	流程设计有效性评价	根据穿行测试执行情况，对流程设计有效性做出判断。

穿行测试可以全面检查业务流程的各个控制点的实际执行情况、发挥的作用、存在的问题，以此判断整个控制设计是否有效。如果在穿行测试过程中确认控制在设计上可以有效减少已识别的潜在风险，且已付诸实施并按设计运行，那么就可以将该控制确认为设计有效。如果在穿行测试过程中发现，控制未按设计运行或设计不能减少已识别的风险，那么就将该控制确认为无效。对已确认为设计无效的控制无需进行控制测试；对已确认为设计有效的控制则需要进行控制测试，以判断其运行是否有效。

4.8.6 控制测试法

控制测试是指通过选取一定数量的样本，对存在的关键控制进行测试，以检查、验证实际业务操作是否按照制度设计的控制要求执行，来判断被审计单位控制运行有效性的一种方法。控制测试的具体流程如图7。

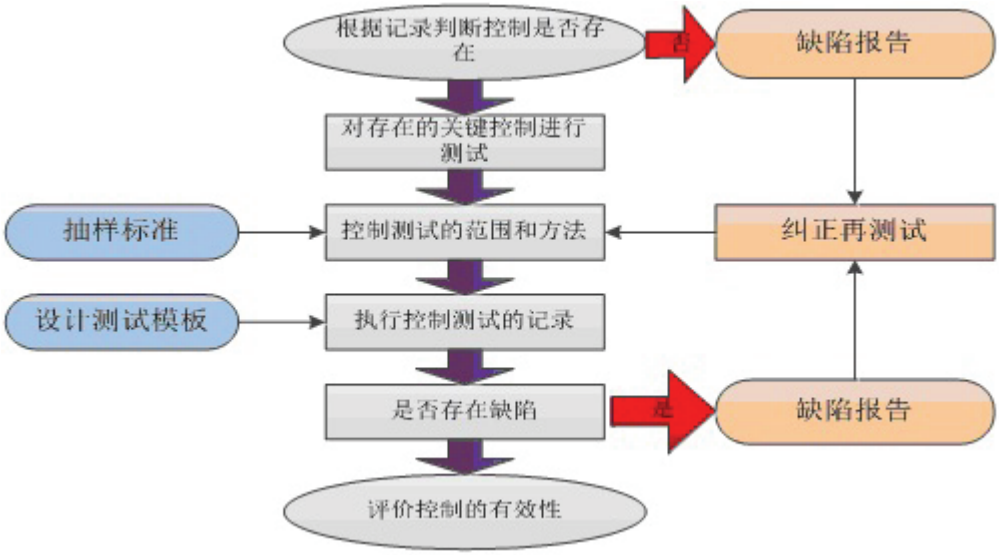

图 7 控制测试流程图

控制测试中一般采用抽样审计方法选择测试样本。抽取测试样本时，宜首先设定期望达到的置信度，然后再按控制发生频率随机抽取一定数量的业务样本，具体样本数量会根据控制种类与控制执行频率的不同有所差异，如将置信度设定为90%，样本数量的确定可参见表10。

表 10　控制测试抽样对应表

人工控制执行的频率	控制测试样本数量
一天多次	25
每天	25
每周	5
每月	2
每季	2
每年	1
对于无法判断发生频率的	该业务发生总笔数的 10%，但不超过 25 笔。

对于控制执行频率为每月、每季或每年的控制点，如果所选测试样本中存在1个或1个以上的错误，则认为该控制点在执行的有效性方面存在缺陷；对于控制执行频率为一天多次、每天、每周的控制点，如所选测试样本中存在1个错误，则扩大样本量进行补充测试，如果在补充测试过程中仍发现有样本错误，则认为该控制点在执行的有效性方面存在缺陷，如果未发现错误，则该控制点出现错误的机率在可容忍范围内，控制仍被认为执行基本有效，即：测试对象的总体中可能发生的差错率不会超过10%，测试样本的置信度达到了90%。详见表11。

表 11　增加测试样本对应表

抽样顺序	样本量	差异数量	后续处理
第一次抽样	25	0	控制有效
第一次抽样	25	1	扩大测试样本至 40 个(增加 15 个样本)
第一次抽样	25	>=2	停止测试，控制无效
扩大抽样	15	0	控制依然有效
扩大抽样	15	>=1	控制无效

上述抽样样本数据仅针对单个评价分支机构。如要对商业银行集团整体做出评价，则需考虑分支机构的测试覆盖面。按照国内外同业领先实务，建议机构的覆盖面至少达到60%。

控制测试中宜对测试样本进行详细描述，记录测试具体步骤、测试内容、发现的问题以及评价结论等信息。控制测试工作底稿样例，详见表12。

表 12　控制测试工作底稿样例

编号	栏目	内容解释/建议填写内容
1	相应风险与控制编号	本控制测试中包括的风险点和控制点编号
2	测试负责人	填写执行测试的人员
3	测试日期	填写测试完成的时间
4	审阅人	填写对控制测试进行复核的人员
5	审阅日期	填写对控制测试完成复核的时间
6	总体样本描述	对样本库获取方式、范围做详细描述。

编号	栏目	内容解释/建议填写内容
7	抽取样本量和出现问题样本量	抽取样本量：从样本库中抽取的样本个数。 出现问题样本量：发现例外情况的样本个数。
8	控制测试步骤	填写该控制测试采取的步骤。测试步骤与关键控制点存在对应关系。
9	发现缺陷的文档编号	发现缺陷的的样本资料的编号，如凭证号、合同号、票据号等。便于日后核实例外样本。
10	发现缺陷描述	对发现的缺陷进行详细描述。描述不只局限于问题的表象，还需写明问题产生的原因。
11	缺陷涉及科目和金额	测试中发现的例外样本涉及的财务报表科目及其金额。
12	控制测试结论	根据控制测试执行情况，对制度执行的有效性做出判断。

4.8.7 其他方法

除了以上几种主要方法外，在开展评价的过程中还需要借助一些其他技术方法。这些方法主要包括：

a) 询问或访谈法。根据评价需要，对被评价单位员工进行单独访谈，或以小型座谈会的方式开展团体访谈，以获取被评价对象的有关信息；
b) 调查问卷法。设置问卷调查表，分别对不同层次的员工进行问卷调查，根据调查结果了解相关机构内部控制的实际情况；
c) 对比分析法。把两个相互联系的指标数据进行比较，从数量上展示和说明评价对象业务规模的大小，风险控制水平的高低，业务发展速度的快慢等；
d) 实地查验法。对资产进行盘点、清查，以及对存货出、入库等控制环节进行现场查验，以验证各项控制措施在实际操作中是否被真正运用；
e) 专题讨论会法。通过召集与业务流程相关的管理人员就业务流程的特定项目或具体问题进行讨论及评价的一种方法，主要通过集思广益的形式更加全面、清晰地认识和了解相关事项；
f) 其他检查成果的综合利用。内部控制评价包括日常监督、专项监督和年度评价。年度评价能最终反映出商业银行一个会计年度中内部控制的真实状况。内控评价要充分利用和借鉴专业条线的检查和自查和结果，行内检查监督部门的检查发现，以及其他形式的检查发现，实现行内检查成果的综合利用。在评价过程中，商业银行可根据自身的风险管理状况，有选择性的选取一些重要的风险领域、主要的分行，按照一定范围、频率，进行滚动评价，并积极应用非现场评价手段。

4.9 结果利用

4.9.1 评价报告

完整的内部控制评价报告至少体现以下内容：

a) 报告摘要。对报告正文中的主要内容和重要问题的高度概括和提炼；
b) 报告正文。包括以下五个部分：
   1) 评价概况：说明评价背景、评价目的和范围、评价重点及运用的程序和方法等；
   2) 评价标准的编制依据：主要包括依据的法律法规、监管规章、监管指引、商业银行的各项规章制度和国际内部控制领先实务等；

3) 评价结论：对商业银行内部环境、风险评估、控制活动、信息与沟通、内部监督等要素的设计、运行情况进行评价，做出内部控制是否有效的结论；
4) 评价发现：评价过程中对评价事实的客观确认，既要揭示与反映内部控制缺陷，也要对内部控制中好的做法予以认可，同时可以反映内部控制缺陷的整改情况等；
5) 评价建议：针对主要的控制缺陷提出改进内部控制的对应建议。

c) 报告附件。这是对报告正文的补充和详细说明。可以包括评价发现问题汇总表、对评价过程与缺陷的具体说明、被评价单位的反馈意见等。

4.9.2 报告路径

评价机构应当在年度内部控制评价工作的基础上，编制商业银行集团层面的内部控制评价报告，并报审计委员会审议。

审计委员会应当对内控评价部门提交的内部控制评价报告进行审议后报董事会审议。

董事会应当根据相关内部控制信息，对内部控制评价报告进行审议。经审议通过的内部控制评价报告可送交监事会。

经审议通过后的内部控制评价报告应根据监管要求进行信息披露。对外披露的内部控制评价报告的内容、格式及时间要求按照《企业内部控制评价指引》以及证券交易所的相关规定执行。

4.9.3 成果运用

股东及债权人、董事会、管理层、外部监管者和外部审计等均可利用内部控制评价报告及内部控制评价成果。

股东和债权人可以从内部控制评价中了解银行一定时期存在的重要风险及内部控制状况，知晓受托人是否有效履行受托责任。

董事会和管理层可以在实施内部控制评价过程中，提高内部控制意识，提升内部控制文化，推动完善和改进内部控制。各级管理部门可以在评价过程中及时发现内部控制缺陷，开展缺陷整改、实施奖惩制度，完善内部控制、提高经营管理水平和风险防范能力。内部控制评价报告及其成果还可以作为商业银行实施内部管理的依据，在制度完善、流程优化、新业务开发、绩效考核以及检查监督等方面发挥更多作用。

对于全体员工来说，通过内部控制评价，揭示并优化内部控制的薄弱环节，能更好地防止舞弊。

外部监管部门和外部审计可以借助银行出具的内部控制评价报告了解银行的内部控制状况，缩减检查时间，减少监管成本。

5 公司层面内部控制评价

5.1 评价步骤

公司层面的内部控制主要指对整个商业银行各业务均有影响的一系列控制过程。

公司层面内部控制评价包括以下主要步骤：

a) 确定公司层面内部控制的目标，旨在合理保证资产的安全目标、财务报告及相关信息真实完整目标、提高经营效率效果目标以及遵循国家法律法规和有关监管等基本目标得到实现，最终实现商业银行整体的战略目标；
b) 确定公司层面内部控制的内容，主要围绕内部环境、风险评估、控制活动、信息与沟通、内部监督等五大控制要素展开；

c) 构建公司层面的风险控制矩阵，包括识别公司层面的主要风险、梳理公司层面的风险点和控制要求、构建公司层面内部控制的领域树、构建公司层面的风险控制矩阵等步骤；
d) 开展控制测试，评价人员对已确认为设计有效的控制按照内部控制发生的频率和设定的置信度采取抽样方法进行一定数量的样本测试，判断其内部控制运行的有效性；
e) 确认、评估与汇总内部控制缺陷，包括样本记录、填写事实确认书、确认控制缺陷、评估缺陷等级等步骤；评价人员根据发现及汇总后的缺陷对实现内部控制目标的影响程度，按重大缺陷、重要缺陷和一般缺陷进行等级评定；
f) 提出整改的建议，反馈与沟通。评价人员就内部控制评价结果与被评价对象进行沟通，提出评价组的整改建议，并获取对方的反馈意见；
g) 对整改结果进行再测试。
h) 得出公司层面内部控制评价的结论，评价组综合整改跟踪评价后的结果，对被评价对象的内部控制有效性做出结论。

具体评价工作底稿可参考表 A.1 公司层面内控评价工作底稿。

5.2 内部环境

5.2.1 组织架构

主要风险点：

a) 商业银行公司治理机制不健全；
b) 董事会及专门委员会议事规则不完善；
c) 组织架构、内部机构设置缺乏制衡；
d) 缺乏对子公司（子行）投资的管理和控制。

控制要求：

a) 商业银行应设立股东大会、董事会、监事会和高级管理层，并履行相应职责。公司治理结构方面，股东大会作为权力机构，依法行使对商业银行重大事项的决定权；董事会作为决策机构，负责内部控制的建立健全，监督其有效实施并评价内部控制的有效性；监事会作为监督机构，对内部控制的建设与执行情况进行监督检查；高级管理层作为执行机构，负责组织实施董事会决议事项，组织开展内部控制的日常运行。商业银行还应建立独立董事制度，对董事会讨论事项发表客观、公正的意见；
b) 商业银行根据国家有关法律法规和公司章程制定详细的股东大会、董事会、监事会的议事、决策规则，以及高级管理层的工作细则和规程。对内部控制的重大事项应采用集体决策机制，依照法律法规和监管要求以及公司章程在董事会和管理层下设置相应委员会：董事会下设审计委员会，按公司章程履行内部控制相关职责；总行组织制定内控建设规划，研究分析内控管理中存在的重大缺陷，监督重大问题落实整改等；
c) 根据经营管理需要和内部控制要求，建立健全授权和分工合理、职责明确、制约平衡、报告关系清晰的内部控制组织架构。在确定职权和岗位分工过程中，应当体现不相容职务相互分离的要求。不相容职务通常包括：可行性研究与决策审批；决策审批与执行；执行与监督检查等；
d) 通过外派董事、监事，并监督其履职情况，加强对子公司（子行）的管控，建立科学的投资管控制度，通过合法有效的形式履行出资人职责、维护出资人权益，重点关注子公司特别是异地、境外子公司的发展战略、年度财务预决算、重大投融资、重大担保、大额资金使用、主要资产处置、重要人事任免、内部控制体系建设等重要事项。

5.2.2 发展战略

主要风险点：

a) 商业银行缺乏明确的发展战略规划；

b) 商业银行未在充分调查研究、科学分析预测和广泛征求意见的基础上制定发展战略目标。

c) 战略规划执行、落实不力。

控制要求：

a) 商业银行建立明确的发展战略规划，在公司层面健全战略决策的组织架构，在董事会下设立战略委员会，对战略发展规划进行审议，商业银行发展战略规划经董事会审议通过后，应当报经股东（大）会批准后实施；

b) 商业银行在制定发展战略目标过程中，应进行充分调查研究、科学分析预测并广泛征求意见，综合考虑宏观经济政策、国内外市场需求变化、技术发展趋势、行业及竞争对手状况、可利用资源水平和自身优势与劣势等影响因素；

c) 商业银行发展战略应保持一定的稳定性，将发展战略进行分解和落实，制定落实发展战略的工作方案，按照部门、机构等管理维度将战略规划进行落实。

5.2.3 企业文化

主要风险点：

a) 未培育全体员工认同的核心价值观，未形成企业文化；

b) 并购重组中存在文化冲突；

c) 未落实企业文化；

d) 未建立企业文化评估制度，企业文化建设流于形式。

控制要求：

a) 商业银行应培育健康的企业文化，对企业文化的内涵及其策划、渗透、评估与改进做出明确的规定，增强员工和社会公众对企业文化的理解和认可，提升商业银行竞争力和品牌价值。特别应向员工传达诚实守信、遵守法律法规和实施内部控制的重要性，引导员工树立合规意识和风险意识，提高员工职业道德水准，规范员工职业行为；

b) 加强并购中的文化整合，尤其是跨国并购或跨境并购，应对并购双方的文化差异进行识别和有效管理，以指导商业银行以吸纳式或渗透式对双方企业文化进行有效整合；

c) 企业文化的传播采用高层推动与基层实践相结合。高层管理者成为企业文化建设的倡导者、组织者和实践者。商业银行应当促进文化建设在内部各层级的有效沟通，加强企业文化的宣传贯彻；

d) 商业银行应当建立企业文化评估制度，明确评估的内容、程序和方法，落实评估责任制，避免企业文化建设流于形式。

5.2.4 内部审计

主要风险点：

a) 未建立垂直独立的内部审计组织体系；

b) 内部审计权限不明确；

c) 审计质量缺乏监控。

控制要求：

a) 商业银行设立垂直管理、具有充分独立性的内部审计部门，向董事会负责并报告工作，履行集团层面内部控制评价工作的牵头职责，协助完成内部控制评价报告的对外披露；

b) 商业银行应当以制度形式明确赋予内部审计部门履行职责所必需的权限。内部审计部门应有权及时、全面了解经营管理信息，并就有关问题向审计对象和人员进行调查、质询、举证；

c) 内部审计部门应建立审计回避制度，确保内部审计的客观性，内部审计部门应对审计发现与恰当的管理层沟通，监督整改活动的进行并执行后续审计，有权将发现的内部控制重大缺陷直接向董事会及其审计委员会、监事会报告。

5.2.5 人力资源

主要风险点：

a) 人力资源政策及开发机制不健全；
b) 缺乏人力资源选聘标准；
c) 人力资源薪酬与考核激励机制缺失；
d) 未对年度人力资源计划执行情况进行定期评估。

控制要求：

a) 商业银行根据战略发展规划，结合人力资源现状和未来需求预测，建立人力资源发展目标，制定人力资源总体规划和能力框架体系，优化人力资源整体布局，明确人力资源的引进、开发、使用、培养、考核、激励、退出等管理要求，健全关键岗位员工强制休假和定期岗位轮换，掌握国家秘密、重要商业秘密或知识产权员工脱密安排、竞业限制等管理机制；
b) 将职业道德修养和专业胜任能力作为选拔和聘用员工的重要标准，健全相关业务从业人员的资格认定与考核制度，保证从业人员具备必要的专业资格和从业经验。切实加强员工培训和继续教育，确保员工熟知相应岗位的业务操作流程、内控要求和经办业务的主要风险点，充分了解相关的规章制度、奖惩规定，以及在内部控制中的权利和责任；
c) 董事会下的薪酬委员会负责审议全行薪酬管理制度和政策，拟订董事和高级管理层的薪酬方案，并向董事会提出薪酬方案建议，监督方案实施。薪酬制度应与人力资源考核结果相挂钩，建立健全内部控制激励约束机制，将各机构、各部门和全体员工实施内部控制的情况纳入绩效考评体系，在绩效分配中予以体现；
d) 商业银行应当定期对年度人力资源计划执行情况进行评估，总结人力资源管理经验，分析存在的主要缺陷和不足，完善人力资源政策，促进企业整体团队充满生机和活力。

5.2.6 社会责任

主要风险点：

a) 商业银行未履行社会责任；
b) 危害、侵犯员工合法权益。

控制要求：

a) 商业银行应该切实履行社会责任，追求经济效益与社会效益、短期利益与长远利益、自身发展与社会发展相互协调，实现企业与员工、企业与社会、企业与环境的健康和谐发展；
b) 商业银行与员工签订并履行劳动合同，遵循按劳分配、同工同酬的原则，建立科学的员工薪酬制度和激励机制，不得克扣或无故拖欠员工薪酬。建立高级管理人员与员工薪酬的正常增长机制，切实保持合理水平，维护社会公平。商业银行应及时办理员工社会保险，足额缴纳社会保险费，保障员工依法享受社会保险待遇。避免在正常经营情况下批量辞退员工，增加社会负担。

5.3 风险评估

5.3.1 风险管理体系

主要风险点：

a) 风险管理架构不健全；
b) 风险管理目标不明确；
c) 风险管理制度体系不完善；
d) 风险管理信息系统不完备。

控制要求：

a) 商业银行应建立健全的风险管理组织体系，董事会下设立风险管理委员会，设立专门的风险管理部门牵头负责全面风险管理工作，商业银行能够预见、识别因经营环境、组织结构的变化等因素导致的风险；
b) 商业银行根据外部形势和内在发展要求，制定风险管理战略和目标，确定风险承受度，包括整体风险承受能力和业务层面的可接受风险水平；
c) 商业银行应当制定识别、计量、监测和控制风险的制度、程序和方法，以确保风险管理和经营目标的实现；
d) 商业银行应当建立涵盖各项业务、全行范围的风险管理系统，开发和运用风险量化评估的方法和模型，对信用风险、市场风险、流动性风险、操作风险等各类风险进行持续的监控。

5.3.2 风险识别

主要风险点：

a) 风险识别范围不明确；
b) 风险识别要素不明确；
c) 各类风险识别重点不明确。

控制要求：

a) 商业银行持续对各类风险进行有效的识别与评估。主要风险包括信用风险、市场风险（含利率风险）、操作风险、国家风险、流动性风险、法律风险以及声誉风险等；特别应考虑计算机系统的运用可能带来的风险；
b) 商业银行对各类风险进行识别时应充分考虑内部和外部因素。当环境和条件发生变化时，应及时对风险进行再识别和再评估，以确保任何新的和以前未曾予以控制的风险得到识别和控制。若涉及到组织结构、流程、计算机系统等方面的重大变更，应考虑可能产生的新风险；
c) 在信用风险识别方面，重点关注但不限于国家、地区、行业、客户、交易方式、集中度等因素。在市场风险识别方面，重点关注但不限于利率、汇率（包括黄金）、股票价格和商品价格等因素。在操作风险识别方面，重点关注但不限于人员、内部程序、系统、外部事件等因素。在流动性风险识别方面，重点关注但不限于存款客户支取、贷款客户提款、债务人延期支付、资产负债结构不匹配、资产变现困难、经营损失和衍生品交易风险等因素。对影响银行经营管理的声誉风险、战略风险、国别风险等其他各类风险，均应根据外部环境、监管要求和经营状况，开展风险识别工作。

5.3.3 风险评估

主要风险点：

a) 未建立风险评估程序、标准、方法；
b) 风险评估重点不准。

控制要求：

a) 商业银行应根据风险管理战略和目标，建立健全风险评估的程序、标准和方法，采用有效的工具和方法，对经营管理活动中的风险进行主动识别与准确评估，并采用定性与定量相结合的方法，按照风险发生的可能性及其影响程度等，对识别的风险进行分析和排序，确定关注

重点和优先控制的风险。在风险评估过程中，各商业银行应根据监管规定和自身的实际情况选择风险计量方法；

b) 商业银行合理分析、准确掌握董事、行长及其他高管人员、关键员工的风险偏好，采取适当的控制措施，避免因个人风险偏好给企业经营带来重大损失。

5.3.4 风险应对

主要风险点：

a) 未制定风险应对策略；

b) 风险报告程序不健全。

控制要求：

a) 商业银行应根据风险评估结果，结合风险承受度，权衡风险与收益，综合运用风险规避、风险降低、风险分担和风险承受等应对策略，实现对风险的有效控制，避免给本行经营带来重大损失；

b) 商业银行应根据风险管理的需求，编制不同层次和种类的风险报告，并按照制度规定的范围、程序和频率发送报告，以满足各机构、各部门对风险状况的多样性需求。

5.4 控制活动

5.4.1 政策与流程

主要风险点：

a) 控制活动措施不明确；

b) 未制定政策制度明确业务处理流程。

控制要求：

a) 商业银行应根据内部控制目标，结合风险应对策略，通过手工控制与系统控制、预防性控制与发现性控制相结合的方法，综合运用控制措施，对各种业务和事项实施有效控制，控制活动应覆盖各项经营管理的全过程；

b) 商业银行制定政策制度，明确业务流程，各项业务应结合实际建立全面、系统、成文的政策、制度和程序，编制业务操作指南，保持统一的业务标准和操作要求，并保证其连续性和稳定性。

5.4.2 不相容职务分离控制

主要风险点：

a) 未建立全面的不相容职务分离控制制度；

b) 未建立关键岗位人员轮换和强制休假制度。

控制要求：

a) 商业银行全面系统地分析、梳理业务流程中所涉及的不相容职务，实施相应的分离措施，形成各司其职、各负其责、相互制约的工作机制，明确关键岗位、特殊岗位、不相容岗位及其控制要求；

b) 建立关键岗位员工定期或不定期轮换和强制休假制度，明确轮岗范围、轮岗周期、轮岗方式等。

5.4.3 授权审批控制

主要风险点：

a) 授权管理制度、体系不完善；
b) 重大业务和事项未实行集体决策审批。

控制要求：

a) 根据各分支机构和业务部门的经营管理水平、内部控制和风险管理能力、地区经济和业务发展需要，建立相应的授权体系，实行统一法人管理和法人授权。明确各岗位办理业务和事项的权限范围、审批程序和相应责任。授权应适当、明确，并采取书面形式；
b) 各机构、各部门管理人员在授权范围内行使职权和承担责任，对须经集体决策审批的重大业务和事项，任何个人不得单独决策或者擅自改变集体决策的意见。确需调整集体决策意见且此调整可能导致风险敞口扩大的，须提请集体决策机构再议；风险没有扩大，无须提请集体决策的，应事先取得相应授权。

5.4.4 会计系统控制

主要风险点：

a) 未制定会计制度与规范；
b) 会计岗位设置未实行责任分离、相互制约的原则；
c) 未配备足够的会计从业人员。

控制要求：

a) 商业银行严格执行国家统一的会计准则制度，配备具有相应从业资格和资质的人员，加强会计基础工作，明确会计凭证、会计账薄和财务会计报告的处理程序，保证会计资料真实完整；
b) 会计岗位设置应当实行责任分离、相互制约的原则，严禁一人兼任非相容的岗位或独自完成会计全过程的业务操作。明确会计部门、会计人员的权限，各级会计部门、会计人员应当在各自的权限内行事，凡超越权限的，须经授权后，方可办理；
c) 银行应该依法设置会计机构，配备会计从业人员。

5.4.5 财产保护控制

主要风险点：

a) 未建立财产日常管理制度和定期清查制度；
b) 未明确规范职责分工、权限范围和审批程序；
c) 安全工作机制不健全、安防设施建设不完备；
d) 金库、营业网点安全存在风险隐患；款箱交接、ATM 加钞、款箱及运行环节存在风险隐患；

控制要求：

a) 建立财产日常管理制度和定期清查制度，采取财产记录、实物保管、定期盘点、账实核对等措施，确保财产安全；
b) 银行对财产保护的职责分工、权限范围和审批程序进行明确的规范，机构设置和人员配备科学合理，严格限制未经授权的人员接触和处置财产；
c) 提高安全管理的认识，切实加强对安全的保卫工作的组织领导，建立健全安全工作机制；加强对员工的安全意识教育，严格按照业务流程操作；加强安防设施建设。对全辖营业网点全面推行安防设施达标建设，保证所有营业场所有灵敏可靠、严密完善的技防、物防设施；
d) 加强营业网点日常安全管理，严格落实营业网点安全防范工作的相关操作规程；加强制度执行力度，款箱交接环节必须严格按照操作规程流程进行，加强对 ATM 的运行管理。

5.4.6 预算控制

主要风险点：

a) 未实施全面预算管理制度；
b) 未建立有效的预算考核、约束机制；
c) 预算方案及变更未经过适当的审批。

控制要求：

a) 实施全面预算管理制度，明确各责任单位在预算管理中的职责权限，规范预算的编制、审定、下达和执行程序，强化预算约束；
b) 银行建立严格的预算执行考核制度，对各预算单位和个人进行考核，切实做到有奖有惩、奖惩分明；
a) 银行董事会审核全面预算方案，银行下达的预算应当保持稳定，不得随意调整。由于市场环境、国家政策或不可抗力等客观因素，导致预算执行发生重大差异确需调整预算的，应当履行严格的审批程序。

5.4.7 运营分析控制

主要风险点：

a) 未建立经营管理情况分析制度；
b) 未对运营分析中发现的存在问题加以改进。

控制要求：

a) 建立经营管理情况分析制度，管理层综合运用各方面信息，通过因素分析、对比分析、趋势分析等方法，定期开展经营管理情况分析；
b) 对运营分析中发现的存在问题，及时查明原因并加以改进。

5.4.8 绩效考评控制

主要风险点：

a) 未建立和实施绩效考评制度；
b) 绩效考评结果未能得到有效利用；
c) 绩效考评指标体系修订不及时。

控制要求：

a) 建立和实施绩效考评制度，科学设置考核指标体系，对内部各责任单位和全体员工的业绩进行定期考核和客观评价；
b) 银行将考评结果作为确定员工薪酬以及职务晋升、评优、降级、调岗、辞退等的依据；
c) 银行应该定期审核关键业绩指标，将其与战略目标进行比较，及时修改和改进银行关键业绩指标体系。

5.4.9 重大风险预警控制

主要风险点：未建立重大风险预警机制。

控制要求：建立重大风险预警机制和突发事件应急处理机制，明确风险预警标准，对可能发生的重大风险或突发事件，制定应急预案、明确责任人员、规范处置程序，确保突发事件得到及时妥善处理。

5.4.10 并表管理控制

主要风险点：

a) 未制定并表管理制度；
b) 并表管理责任未落实；

c) 未建立大额风险暴露的管理政策和内控制度；
d) 未建立监测、报告、控制和处理内部交易的政策与程序。

控制要求：

a) 银行应制定并表管理制度，明确并表管理的机构确认原则与标准、相关组织架构、各相关单位工作责任、以及具体管理要求；母行应与附属机构，以及附属机构之间建立健全防火墙制度，实现风险隔离；
b) 董事会应承担并表管理最终责任，并负责制定银行集团并表管理的总体战略方针，审批和监督并表管理具体实施计划的制定与落实，以及建立定期审查和评价机制。高级管理层应对并表管理体系的充分性和有效性进行监测和评估；
c) 应建立大额风险暴露的管理政策和内控制度。明确相关的政策、程序来识别、计量、监测和控制集团层面的风险暴露。明确大额风险暴露的预警报告制度，以及与风险限额相匹配的风险分散措施等。应实时监控大额风险暴露；
d) 建立监测、报告、控制和处理内部交易的政策与程序。集团内部交易条件不得优于独立第三方。制定相应措施有效控制附属机构所产生信用、市场、流动性、操作、声誉等其他风险和损失对母行所带来的风险。

5.4.11 反洗钱控制

主要风险点：

a) 未建立反洗钱制度；
b) 未明确各部门、各岗位的反洗钱工作职责；
c) 未建立反洗钱监测系统；
d) 未建立洗钱风险评估体系；
e) 未开展员工培训；
f) 未按规定执行客户身份识别制度、大额和可疑交易报告制度和客户身份资料及交易记录保存制度。

控制要求：

a) 制定集团层面反洗钱标准、反洗钱合规管理制度、业务部门将反洗钱合规要求嵌入业务制度和操作流程；
b) 设立反洗钱专门机构或指定内设机构负责反洗钱工作；明晰各条线（部门）和各类人员的反洗钱职责；
c) 应建立与本行业务规模相适应的反洗钱监测系统，包括建立反洗钱风险名单监控系统、大额交易监控系统和可疑交易监测分析系统，为反洗钱岗位人员提供技术支持；
d) 应从全流程的角度对各项金融业务及产品、系统进行洗钱风险评估，强化高风险领域的反洗钱合规管理措施；建立客户洗钱风险评级系统，对所有客户的洗钱风险等级进行评定，并根据客户风险等级采取相应的风险控制措施；
e) 应制定反洗钱培训计划，持续地开展反洗钱培训；
f) 应全面履行客户身份识别制度、客户身份资料及交易记录保存制度、大额和可疑交易报告/反恐融资和反扩散融资报告制度等。

5.4.12 关联交易控制

主要风险点：

a) 未建立关联交易制度；
b) 未明确各部门、各岗位的职责权限；

c） 未建立关联交易管理体系；
d） 未进行关联交易信息的统计、报告与披露。

控制要求：

a） 银行应建立健全满足监管部门要求的关联交易制度，管理层应合理界定关联方和关联交易的范围、关联交易的定价和授权等；
b） 合理设置职能部门和工作岗位，明确各部门、各岗位的职责权限，形成各司其职、各负其责、便于考核、相互制约的关联交易工作机制；
c） 银行应建立有效的关联交易管理体系，相关部门、各分支机构、并表机构应按照授权规范开展关联交易；
d） 银行应当通过建立关联交易档案台账等多项措施，确保关联交易数据的真实性、准确性和完整性，满足对关联交易数据采集统计、事后检查、报告与披露的需要。

5.4.13 业务外包控制

主要风险点：

a） 未建立董事会高管层承担最终责任的外包组织架构；
b） 不宜外包的核心管理职能进行外包；
c） 未有效开展外包活动的风险管理和控制；
d） 未对外包活动开展监督检查。

控制要求：

a） 银行的董事会和高管层承担外包业务的最终责任，董事会审议批准外包战略发展规划、外包风险管理制度、外包范围、外包报告、外包审计等，高管层制定外包战略发展规划、外包风险管理政策和内控制度、确定外包范围、实施监督职责等，外包管理团队执行外包风险管理政策、操作流程和内控制度，并向高管层报告；
b） 银行的战略管理、核心管理以及内部审计等职能不宜外包；
c） 银行应评估外包活动的战略风险、法律风险、声誉风险、合规风险等，对外包服务提供商进行尽职调查，签订书面合同，确保客户信息安全；
d） 银行定期对外包活动进行全面审计与评价，向银监会报送评估报告和重大影响事件。

5.4.14 业务连续性控制

主要风险点：

a） 未制定业务连续性管理战略并建立组织架构；
b） 业务连续性管理未纳入全面风险管理体系；
c） 未识别和评估业务中断的影响和损失；
d） 未开展业务连续性资源建设和演练。

控制要求：

a） 银行根据业务发展总体目标、经营规模以及风险控制的基本策略和风险偏好，确定适当的业务连续性管理战略，建立业务连续性管理的组织架构，制定业务连续性计划，有效处置运营中断事件，董事会是决策机构，对业务连续性管理承担最终责任，高管层制定业务连续性管理政策，连续性管理委员会落实管理职责，主管部门、执行部门负责业务条线和信息技术的应急响应和恢复；
b） 银行应将业务连续性管理纳入全面风险管理体系，建立与全行战略目标相适应的业务连续性管理体系；

c) 银行通过业务影响分析识别和评估业务运营中断所造成的影响和损失，根据业务重要程度实现差异化管理，至少每三年开展一次全面业务影响分析并形成报告；
d) 银行开展业务连续性计划所需的资源建设，满足业务恢复目标和重要业务持续运营的要求，建立统一的运营中断事件指挥中心，建立灾备中心、关键岗位备份人员等，开展业务连续性演练和应急处置机制。

5.5 信息与沟通

5.5.1 信息指标体系

主要风险点：
a) 未构建信息数据平台；
b) 未建立内、外部信息指标体系。
控制要求：
a) 构建信息数据平台，实现管理信息集中处理。银行各机构、各管理部门定期开展数据分析工作，为市场营销、风险管理等各项经营管理活动提供数据分析平台，为管理层精细化决策提供系统支持；
b) 全面分析外部经济金融环境，同业信息以及国内外监管法规制度的最新变化情况，全面梳理影响银行发展的重要外部信息来源，完善外部信息资料指标体系，根据发展战略执行情况建立内部信息报告体系，为管理层定期提供内部信息报告。

5.5.2 信息系统建设

主要风险点：
a) 未开发信息系统；
b) 缺乏数据质量考核；
c) 客户端安全控制不健全。
控制要求：
a) 根据各级管理层对信息数据的需求，有针对性地开发信息系统，提升系统数据质量，根据管理需要建立识别、管理大量数据的工作机制，有力地支持管理需求；
b) 定期考核银行数据质量情况，将数据质量纳入到内控管理及银行经营绩效综合考核，逐步建立较为完善的数据质量激励约束机制；
c) 商业银行应加强客户端安全控制，明确客户端安全管理要求，防范客户端信息安全风险，严格执行客户端网络准入、软硬件使用控制、互联网访问以及客户端操作行为等方面的安全管理要求，做好客户端安全使用管理。

5.5.3 信息安全控制

主要风险点：
a) 信息系统安全管理缺失；
b) 信息使用缺乏权限管理。
控制要求：
a) 商业银行加强对信息系统开发与维护、访问与变更、数据输入与输出、文件储存与保管、网络安全等方面的控制，保证信息系统安全稳定运行。确定信息及信息系统的安全等级，明确应用系统中各类信息使用的安全管理要求，实施分等级安全管理；

b) 严禁员工之间擅自转让信息系统的用户密码信息，人员调离时，应移交全部技术资料及有关密钥资源的介质，停止其使用、维护和管理的权限，及时更换密码信息，必要时执行有关脱密期的规定。

5.5.4 信息交流机制

主要风险点：

a) 内部交流机制不健全；
b) 外部交流机制不健全；
c) 未建立重大信息报告制度。

控制要求：

a) 要保证信息自上而下和自下而上的传递顺畅，各机构之间和各部门之间应按信息管理权限，加强各类信息资源的共享，确保信息横向交流和互通，促进提升信息使用效率；
b) 通过行业协会、业务合作机构、客户、市场调查、来信来访、媒体网络以及有关监管部门等多方有效获取外部信息，对外部信息尤其是客户信息及时进行筛选、核对、整合和分析，及时跟进管理措施，强化内部控制，有效防范和化解经营风险；
c) 规范信息传递的工作机制，按照真实、准确、完整、及时的原则，将重大信息及时传递给董事会、监事会和管理层。建立重大信息报告联系人制度，保证重大信息在银行内部的顺畅传递；在完善内部信息搜集机制的基础上，规范与监管机构信息传递的途径和方式。

5.5.5 信息披露机制

主要风险点：信息披露制度和流程不完善。

控制要求：商业银行应诚实尽职履行信息披露义务，提高信息披露质量和效率，完善信息披露的风险控制机制，确保信息披露的稳健性与透明性。完善信息披露流程、内涵及风险控制机制。理顺信息披露内部流程，按照监管要求定期做好强制性信息披露工作；建立信息反馈机制，主动了解投资者信息需求，逐步增加主动信息披露内容，拓展信息披露的广度和深度，建立多样化信息披露途径，明确信息披露参与各方的职责，建立全面的信息披露风险控制体系和应急反应措施。

5.5.6 反舞弊机制

主要风险点：

a) 反舞弊工作的重点不突出；
b) 案件举报处理工作不落实；
c) 未建立举报投诉制度和举报人保护制度。

控制要求：

a) 银行确定反舞弊工作的重点，明确舞弊行为的类型，包括未经授权或者采取其他不法方式侵占、挪用银行资产，牟取不当利益；在财务报告和信息披露等方面存在的虚假记载、误导性陈述或者重大遗漏等；董事、监事、经理及其他高级管理人员滥用职权；相关机构或人员串通舞弊；
b) 建立举报处理制度，对举报的案件线索和瞒案不报问题进行核查处理。制定反舞弊工作责任制量化检查办法，对各级机构负责人和部门负责人履行反舞弊职责检查的可操作性，并将检查结果纳入经营绩效考核；查处违法违纪案件，治理商业贿赂，提高执纪办案水平，发挥查处案件的综合效应；

c) 设置举报专线，明确举报投诉处理程序、办理时限和办结要求，确保举报、投诉成为商业银行有效掌握反舞弊信息的重要途径。建立举报投诉制度和举报人保护制度，举报途径应当及时传达至全体员工。

5.6 内部监督

5.6.1 内部监督组织架构

主要风险点：

a) 未建立内部监督组织架构；

b) 内部监督职责权限不明确。

控制要求：

a) 建立并完善监督组织架构。从商业银行治理层面建立监事会、董事会审计委员会、内部审计部门和其他内部机构在内部监督中的职责权限，明确内部审计机构和其他内部机构在内部监督中的职责权限，规范内部监督的程序、方法和要求；

b) 商业银行应指定不同的机构或部门分别负责内部控制的建设、执行和内部控制的监督、评价，内部控制建设与内部控制评价部门进行分离。

5.6.2 内部监督制度

主要风险点：

a) 检查监督办法缺失；

b) 未妥善保存内部控制资料。

控制要求：

a) 商业银行应制定内部控制检查监督办法，该办法至少包括如下内容：董事会或相关机构对内部控制检查监督的授权；各部门及下属机构对内部控制检查监督的配合义务；内部控制检查监督的项目、时间、程序及方法；内部控制检查监督工作报告的方式；内部控制检查监督工作相关责任的划分；内部控制检查监督工作的激励制度；

b) 商业银行应以书面或者其他适当的形式，妥善保存内部控制建立与实施过程中的相关记录或者资料，确保内部控制建立与实施过程的可验证性。

5.6.3 内部监督工作

主要风险点：

a) 内部监督工作流于形式；

b) 内部审计工作覆盖范围不全面；

c) 未开展内部控制评价工作。

控制要求：

a) 建立健全商业银行日常监督检查工作机制与流程，制定日常监督检查管理制度，明确各级机构、各部门在日常监督检查工作中的职责定位，规范检查流程、报告路线及作业标准等方面要求；开展专项监督，根据风险评估结果及日常监督有效性确定专项监督工作重点；

b) 内部审计重点关注董事会所关注的重要风险领域，建立健全内部审计监督范围，对内部控制、风险管理和治理过程三大领域开展审计监督检查，开展内部控制评价工作；

c) 董事会开展内控评价。董事会开展内控评价应依据上交所、深交所的要求，至少按照年度进行一次内控评价。完善内控评价指标体系，根据业务发展需要，适时修订完善内控评价指标体系，强化指标内涵的深度和覆盖的广度，督促内控管理持续改进和提高。

5.6.4 整改机制

主要风险点：

a) 未建立内部控制缺陷标准体系；
b) 内控缺陷报告机制不健全；
c) 重大缺陷缺乏整改跟踪机制。

控制要求：

a) 建立内部控制缺陷标准体系，明确内部控制设计缺陷与运行缺陷的认定标准，结合影响程度确定内部控制缺陷轻重等级，确保各类监督检查成果统一可比。制定内部控制缺陷的认定标准，按重要性划分内部控制缺陷等级；
b) 对于检查中发现的内部控制缺陷，应在内部控制报告中据实反映，采取适当的形式及时向董事会、监事会或者经理层报告，并在报告后进行追踪，以确定相关部门已及时采取适当的改进措施；
c) 跟踪内部控制缺陷整改情况，并就内部监督中发现的重大缺陷，追究相关责任单位或者责任人的责任，并将评价结果作为经营绩效考核的重要依据。

5.6.5 内部控制评价

主要风险点：

a) 未定期开展内部控制评价工作；
b) 内控评价报告披露风险。

控制要求：

a) 商业银行应结合内部监督情况，董事会定期对内部控制的有效性进行评价，出具内部控制评价报告。内部控制评价的方式、范围、程序和频率，应根据经营业务调整、经营环境变化、业务发展状况、实际风险水平等自行确定。评价范围应覆盖内部控制活动的全过程及所有的系统、部门和岗位，并应按照规定的时间间隔持续进行，当经营管理环境发生重大变化时，应及时重新评价。在方法上，评价应依据风险和控制的重要性确定重点，关注重点区域和重点业务；
b) 上市商业银行董事会应在年度报告披露的同时，披露年度内部控制评价报告，并披露会计师事务所对内部控制评价报告的审计意见。

6 流程层面内部控制评价

6.1 评价步骤

流程层面的内部控制主要指专门针对银行某项业务流程的一系列控制过程，旨在合理保证某项业务流程的经营效率和效果以及与该业务流程相关的财务报告及管理信息的真实、可靠和完整等基本目标得到实现。

流程层面内部控制评价是对银行内部控制体系有效性的重要环节。流程内部控制评价主要包括以下程序：

a) 梳理业务流程与管理流程。梳理业务流程是流程层面控制评价特有的一个工作步骤。评价工作开始前，评价人员需要先行梳理银行的主要业务和管理流程；
b) 流程层面控制目标是指流程描述中各主要环节可能要实现的目标；
c) 构建业务流程与管理流程风险控制矩阵。主要包括识别各业务流程和管理流程中的风险点、识别控制点和业务流程中的关键控制、构建各业务流程和管理流程的风险控制矩阵等步骤；

d) 执行穿行测试。这是流程层面内部控制评价的特有步骤，执行穿行测试的目的在于验证业务流程中的重要控制设计与实际操作的一致性，了解相关流程中的设计和执行控制的现状，对控制设计的完整性、充足性和有效性进行判断；
e) 实施控制测试；
f) 确认、评估与汇总内部控制缺陷，包括样本记录、填写事实确认书、确认控制缺陷、评估缺陷等级等步骤；
g) 提出整改的建议，并就该整改建议与被评价对象进行沟通；
h) 对整改结果进行再测试；
i) 得出流程层面内部控制评价的结论。

具体评价工作底稿可参考表 A.2 流程层面内控评价工作底稿。

6.2 公司贷款

6.2.1 客户评级与统一授信

主要风险点：

a) 客户不符合国家法律法规认定的借款人条件或不符合银行准入要求；
b) 客户评级未按照规定的时限和规定的流程完成或评级信息与借款人实际情况不符；
c) 未按照规定的方法合理测算客户最高授信额度；
d) 未能有效识别集团、关联客户，未纳入集团关联客户授信管理。

控制要求：

a) 客户经理应通过实地调查与间接调查相结合的方式,收集整理客户基本资料和业务所需资料，建立客户档案，提出业务受理建议；
b) 客户经理应对有融资余额的客户和拟办理融资的客户定期进行信用等级评定，选择适当的客户评级模型，采集评级相关信息使用银行评级系统发起评级流程，评级流程应由独立于评级发起人的评级认定人员进行认定，应当保留评级过程和结果信息；
c) 应根据不同企业规模和类型选择相适应的授信额度测算模型，在对客户资信情况及融资风险进行综合分析与评价的基础上，核定银行对客户愿意和能够承受的风险限额，包括承担客户信用风险的表内外业务、本外币业务、流动资金和固定资产贷款业务；
d) 应关注和搜集集团客户及关联客户的有关信息,有效识别授信集中风险及关联客户授信风险。

6.2.2 调查和审查审批

主要风险点：

a) 调查内容不完全或调查失实；
b) 商业银行已实行债项评级的，债项评级的依据不充分，结果不准确；
c) 贷款风险分析、评价不充分；
d) 审查未确定合理的贷款结构，并拟定适当的风险控制防控措施；
e) 调查、审查、审批未有效分离，审批人未经授权或超授权审批。

控制要求：

a) 客户经理应通过实地调查与间接调查相结合的方式，按照客户申请的业务品种进行准入条件的初步分析或向客户推荐更适当的融资产品，收集整理该产品所需各类资料和信息，提出业务受理建议，并录入信贷管理系统；
b) 商业银行已实行债项评级的，客户经理应根据银行债项评级的具体要求，将债项相关信息准确输入系统并开展债项等级评价；

c) 调查、评估、审查人员应根据融资业务品种的不同，充分分析和评价贷款风险。流动资金贷款，应根据客户的经营和风险特点，结合其经营周期、上下游客户情况、结算方式等信息，分析真实借款原因和融资风险，测算营运资金需求；固定资产贷款，应落实具体的责任部门和岗位进行全面的风险评价，并形成风险评价报告，建立完善的固定资产贷款风险评价制度，设置定量或定性的指标和标准，从借款人、项目发起人、项目合规性、项目技术和财务可行性、项目产品市场、项目融资方案、还款来源可靠性、担保等角度进行贷款风险评价；

d) 审查人员应根据融资业务品种不同，对客户提交的资料进行核对，并分析客户融资需求的合理性，结合风险分析评价结果，合理确定融资额度、期限、担保方式、还款方式、利率等贷款要素，同时分析合作机构风险状况，揭示客户以及合作机构不符合准入条件、保证人不具备担保能力、抵质押率不足等主要风险并提出防范措施；

e) 应根据贷审分离、分级审批的原则，建立规范的贷款评审制度和流程，确保风险评价和信贷审批的独立性。应建立健全内部审批授权与转授权机制，审批人员应在授权范围内按规定流程审批贷款，不得越权审批。

6.2.3 发放和支付管理

主要风险点：

a) 未经有权人审批即与借款人签订借款合同；

b) 未采用融资产品对应的格式化合同文本，或使用非格式文本但未经法律部门审查同意；

c) 未落实审批前提条件即向借款人发放贷款，或超过授信限额发放贷款，会计核算不准确；

d) 未执行支付管理相关规定，符合受托支付条件的未执行受托支付。

控制要求：

a) 应根据有权人签署的审批意见书，与借款人及其他相关当事人签订书面借款合同、担保合同和其他相关协议，合同要素应当明确，且与审批意见书一致；

b) 应根据融资产品选择银行统一制定的合同文本，包括借款合同、担保合同及其他协议文本，如需使用非格式文本或增加其他条款应当经过法律部门审查同意；

c) 应设立独立的部门或岗位负责贷款发放和支付审核，发放贷款前应确认抵质押物登记手续等审批前提条件已落实，借款人满足合同约定的提款条件。应确保贷款发放额度在客户、集团或其他维度的统一授信/限额管理的额度之内。应按照银行统一规定进行贷款业务的会计核算；

d) 应设立独立的部门或岗位负责贷款发放和支付审核，，符合受托支付条件的应执行受托支付，应按照合同约定通过贷款人受托支付或借款人自主支付的方式对贷款资金的支付进行管理与控制，监督贷款资金按约定用途使用。采用受托支付方式的，应根据约定的贷款用途,审核借款人提供的支付申请所列支付对象、支付金额等信息是否与相应的商务合同等证明材料相符，支付是否及时。

6.2.4 贷后管理

主要风险点：

a) 未按规定进行资金用途检查、贷后检查、风险监测，检查发现风险隐患未采取应对措施；

b) 未按规定进行贷款风险分类或分类结果不准确；

c) 风险拨备计提不合规；

d) 还本付息管理不到位。

控制要求：

a) 贷款发放后，贷款人应当对借款人执行借款合同情况及借款人的经营情况、融资担保情况进行追踪调查和检查。对于自主支付的借款人应核查贷款支付是否符合约定用途。对于受托支付的借款人也应关注资金的最终流向是否异常。应定期或不定期通过现场检查与非现场监测，分析借款人经营、财务、融资情况的变化，监测担保保障能力的变化，掌握各种影响借款人及其债务偿还能力和意愿的风险因素。应通过非现场和现场检查，及时发现潜在风险并发出预警风险提示，及时采取提前收贷、追加担保等有效措施防范化解贷款风险；
b) 应至少每季对全部贷款进行一次分类，根据银监会的贷款分类类别和标准或银行自定的贷款分类类别和标准进行分类，并及时调整分类结果；
c) 应当按照谨慎会计原则，合理估计贷款可能发生的损失，及时计提贷款损失准备；
d) 应当提示借款人按照合同约定按时足额还本付息。对逾期的贷款和欠息要及时催收。对借款人申请提前还款的，应及时给予回复。

6.2.5 不良贷款管理

主要风险点：

a) 现金清收不力；
b) 以物抵债政策执行存在偏差；
c) 债务重组不符合条件；
d) 呆账核销不合规。

控制要求：

a) 根据不良贷款到期、逾期及计息情况，及时向借款人、担保人等还款义务人催收不良贷款本息，密切关注不良贷款诉讼时效、保证及抵（质）押担保期间、申请执行期限、资产查封与续封期限等，及时主张权利，确保主债权及担保权利受法律保护；
b) 贷款到期后，贷款行应积极采取有效措施进行清收，包括依法变卖抵（质）押物或债务人、保证人，第三人的合法财产，以现金形式收回贷款本息。只有在债务人确实难以以现金形式偿还贷款本息的情况下，方可实施以物抵贷。信贷员在进行借款人申请以物抵债时，采用双人现场勘查制，并且出具现场勘查报告；
c) 对不良贷款进行重组应符合相关条件，在实施改制前须将客户改制方案按规定报批。债务重组对借款人减免部分本息，应满足借款人无力按期足额偿还贷款本息，经与借款人、担保人及其他还款义务人协商一致，确保减免和重组后能如期偿还剩余债务的条件；
d) 审查审批部门要严格审查核销数据，核销材料要件要求规范、完整。加强对不良贷款处置预案的指导和管理，控制和预防不符合核销认定条件的项目。

6.3 公司存款

6.3.1 开户

主要风险点：

a) 申请人开户资料或身份证明不真实，外汇账户不符合外管政策；
b) 代理人身份不合规；
c) 开户凭证、协议上无客户签名盖章或签名不正确；
d) 开户风险提示不充分。

控制要求：

a) 严格审核存款人身份和账户资料（营业执照、组织机构代码证、法人代表身份证等等）的真实性、完整性和合法性，外汇账户开户时需审核其提供的资料与国家外汇管理局相关管理要求一致；
b) 对公客户经理不可为其服务的客户代办开户业务；营业网点员工不可直接代理客户办理任何金融业务；授权人必须审核申请人（代理人）的证件类型、证件号码等相关资料，对于客户授权委托书需明确被授权人及授权经办的业务种类，同时确认申请人（代理人）在业务办理现场；柜员须审核开户凭单或账户协议书上的客户签名盖章正确无误；
c) 柜员须审核开户凭单或账户协议书上的客户签名盖章正确无误；
d) 柜员须主动向客户进行风险提示，包括：客户与银行间的风险责任；客户要妥善保管账户预留印鉴、支付密码及U盾等支付介质；对于大额取款业务须提前预约，并携带身份证件等。

6.3.2 存取款

主要风险点：
a) 支付凭证上无客户预留印鉴或印鉴、支付密码错误；
b) 未核实取款人（代理人）身份，或员工为客户代办存取款业务；
c) 客户存取款金额与凭证打印记录不一致。

控制要求：
a) 柜员须审核支付凭证、记载事项、预留签章等的真实性、完整性、合规性，约定使用支付密码时须校验支付密码，核对无误后方可支付；
b) 严格审核存取款人及代理人身份。对大额存款支取实行分级授权和双签制度。客户经理不可为其服务的客户代办存取款业务；
c) 柜员须审核凭证打印输出的内容正确无误。若为大额现金业务，授权人须审核现金及交易输入金额与客户凭证填写金额相符；若为大额转账业务，授权人须审核转出账户及款项合规性。

6.3.3 账户变更

主要风险点：账户更改名称、印鉴、支付密码或法定代表人等其他开户资料未提供相关证明；

控制要求：开户行需严格审核银行账户变更申请，核对预留印鉴、授权书等，对于重大开户资料的变更需核对营业执照等相关证明文件，并及时报备人民银行。

6.3.4 挂失冻结

主要风险点：
a) 无挂失申请或者申请书内容不完整；
b) 未实施换人复核，擅自冻结或解冻客户账户。

控制要求：
a) 柜员受理挂失申请时，须认真审核申请人（挂失人或代理人）的挂失申请书内容的真实性、完整性，核对客户提供的挂失公函、账户信息的准确性，核查确认申请人的身份，确认无误后及时办理挂失止付手续；
b) 建立复核制度，确保交易的记录完整和可追溯。专人复核柜员操作结果，同时确认柜员登记的挂失、冻结登记簿无误。有权冻结部门持有关公函，文件，通知来银行办理冻结或解冻账户或账户余额业务时，需经银行业务主管人员审核，涉及有关账户余额确实未被冻结或已被冻结的情况下，办理冻结或解冻手续并打印相关记录。银行业务主管人员据此登记协助有权机关查询、冻结、扣划登记簿，并在执行通知书等文件回执上签字，加盖业务公章后交执法人员。

6.3.5 对账

主要风险点：未与客户进行对账或对账结果不符时未及时核实。

控制要求：建立和完善对账制度，对对账频率、对账对象、可参与对账人员等做出明确规定并确保对账的实时有效。对纳入余额对账单对账的单位，应定期与单位进行对账。对账人员收到企业反馈对账信息后，对“银企余额对账单”中不符的，开户行应及时与企业逐笔核查未达账项，确认未达原因，发现异常情况应及时采取有效措施。

6.3.6 销户

主要风险点：

a) 客户未正确填写撤销银行结算账户申请书,办理销户前未清理核对在途票据并交回未用票据；
b) 授权人未核实申请人（代理人）身份；
c) 销户信息未输入系统。

控制要求：

a) 柜员须审核客户撤销银行结算账户申请书，确保填写完整、准确，通过系统审核该账户是否有未归还的记账费用，是否有未归还的贷款、欠息，以及在途票据，确保未用票据空白凭证已全部交回或清理；
b) 授权人须确认销户申请人（代理人）身份；
c) 账户结清撤销后，须及时将销户信息录入系统，并按规定上报人行账户系统。

6.4 票据融资

6.4.1 业务受理

主要风险点：

a) 汇票承兑人不具备承兑资格或贴现申请人/转贴现申请行不具备业务资格；
b) 申请资料不完整或不真实。

控制要求：

a) 应对承兑人范围、贴现申请人和转贴现卖出行范围进行明确界定。客户经理收到贴现、转贴现申请后，应对承兑人、贴现申请人或转贴现申请行开展资信调查、授信调查、贸易真实性调查并收集相关资料；
b) 应对票据融资的申请人和贸易背景进行调查,收集客户基本资料和证明贸易背景的交易合同、增值税发票或普通发票。

6.4.2 审查审批

主要风险点：

a) 票据不真实或有瑕疵；
b) 业务未经过适当审查、审批，或审批人超授权审批。

控制要求：

a) 票据应提交会计柜面，通过现场核查和人行系统等核查票面要素是否真实相符，他行是否已办理查询和贴现，是否办理了挂失支付和公司催告，核实票据背书是否连续；
b) 应制定票据融资审批流程、标准和授权机制，由专人开展独立性初复审，有条件的银行可以开发票据业务系统，采用系统审批方式。

6.4.3 资金核算

主要风险点：资金核算不规范。

控制要求：贴现资金应划付至贴现申请人账户，贴现利息应准确计算并在贴现时扣收。

6.4.4 票据出入库

主要风险点：票据出库、移存、入库过程中票据遗失或毁损。

控制要求：应对票据进行出入库管理，应定期对库存票据进行盘点，与账户信息进行核对。

6.4.5 票据托收

主要风险点：

a) 托收不及时；

b) 收款销账出现错误。

控制要求：

a) 由专人负责查询票据到期日，匡算托收日程，与邮局等收件人员办理交接手续；

b) 收款凭证到达后，及时制作表内外凭证，由会计人员进行账务处理。

6.4.6 票据保全

主要风险点：

a) 挂失止付通知书发出不及时；

b) 未及时向票据支付地法院申请公示催告；

c) 发生拒付时未采取追索等保全措施。

控制要求：

a) 一旦发生贴现票据的灭失，应立即通知承兑人挂失止付；

b) 在挂失止付 3 日内依法向票据支付地人民法院申请公示催告，或提起诉讼；

c) 收到拒付证明时，应对拒付事由进行审查，并及时向前手背书人追索或采取其他保全措施。

6.5 国际结算

6.5.1 业务受理

主要风险点：

a) 客户准入及业务办理条件不符合国家政策、监管规定和银行内部管理制度；

b) 客户申请资料凭证不完整、不准确。

控制要求：

a) 严格按照国家政策及外部监管和银行内部管理制度开展尽职调查和业务审查审批；

b) 审核客户申请资料凭证，确保客户提交的业务申请资料和凭证完整准确。

6.5.2 单证处理

主要风险点：

a) 单证审查不严，与国际惯例和监管规定不符；

b) 单据保管或传递失误导致银行出现资金损失或声誉风险；

c) 业务处理缺乏依据导致纠纷。

控制要求：

a) 业务具有真实的贸易背景；符合单证相符等国际惯例；单证处理符合反洗钱、反恐等外部监管规定；严格执行有关业务金额和期限的银行内部授权管理和系统控制；业务部门出具单证审查意见；
b) 建立并执行严密的单据保管和交接制度；
c) 涉及单据处置、往来函电、资金收付等业务处理均应获得客户或交易对手的书面指令或授权，指令不明确或授权不完整的应要求澄清后再进行业务处理。

6.5.3 收付汇

主要风险点：
a) 出口收汇延误、解付错误或不及时；
b) 进口承付（付汇/承兑/拒付）差错或延误；
c) 收付汇（含预收付）手续不符合监管要求。

控制要求：
a) 确保收汇指令汇路清晰、业务要素准确无误；建立和执行查询查复催收制度，确保客户收汇及时解付准确；对已办理融资的收汇应先行归还银行融资本息；
b) 提前落实付汇资金或办妥承兑/拒付手续，及时回复国外催收报文，确保承付报文准确及时发送；
c) 严格执行收付汇（含预收付）审核要求以及国际收支申报、结售汇、信息统计等相关监管规定。

6.5.4 资金清算及会计核算

主要风险点：
a) 未严格执行有关资金清算的审查审批授权规定，清算操作失误和保全措施不力导致银行资金损失、业务纠纷等不良后果；
b) 会计核算和账务处理差错；
c) 费用收取不符合规定。

控制要求：
a) 建立和执行清算授权制度并从严审核，操作环节减少人工干预，确保资金清算准确及时；发生清算失误时及时采取保全措施；
b) 会计处理严格遵循有关会计准则，通过系统自动进行会计核算和账务处理；定期对账并及时纠错，确保账账相符、账实相符；
c) 严格执行监管规定和银行内部规定收取相关费用。

6.6 贸易融资

6.6.1 业务受理

主要风险点：
a) 借款人不具备主体资格；
b) 业务资料不全、协议条款文本不规范。

控制要求：
a) 严格审核借款人主体资格，确保满足外管部门和行内管理制度相关要求，营业执照、贷款卡等证照有效，视具体业务还应取得必要的许可和批复；

b) 根据统一的操作规程受理业务，确保业务办理前资料齐全；使用统一的业务申请书和协议文本，非格式文本经法律部门审定后使用。

6.6.2 审查审批

主要风险点：

a) 贸易背景不真实或存在交易未履约记录；
b) 信用审查不严；
c) 融资额度、期限、利率费率等设定与贸易背景不匹配；
d) 调查、审查、审批未有效分离，审批人未经授权或超授权审批。

控制要求：

a) 严格审查客户提供的合同等贸易资料，综合研判过往履约记录和交易习惯；
b) 应从政策风险、行业风险、企业经营风险、担保能力等角度对贸易融资业务的信用风险进行审查，出具审查意见；
c) 应根据贸易合同以及融资产品特点、信用审查结论等，合理设定融资金额、期限以及利率、费率等要素；
d) 应根据贷审分离、分级审批的原则，建立规范的贷款评审制度和流程，确保风险评价和信贷审批的独立性。应建立健全内部审批授权与转授权机制，审批人员应在授权范围内按规定流程审批贷款，不得越权审批。

6.6.3 贷后管理

主要风险点：

a) 实际融资用途与约定不符；
b) 未定期开展融资跟踪监控。

控制要求：

a) 严格执行受托支付有关规定发放贷款后，持续跟踪贷款资金流向，防止贷款资金被挪用；
b) 应关注客户经营活动和交易进展情况，加强对物流、单据流、资金流的跟踪监控，对融资担保情况进行追踪调查和检查。

6.7 投资银行

6.7.1 银团贷款

主要风险点：

a) 银团贷款审批超授权；
b) 未履行信用风险审批职责；
c) 银团贷款档案管理不规范。

控制要求：

a) 投资银行业务部门根据申请对项目进行审批，各级审批权限在审批系统中严格设定。项目评审委员会的主要职能是负责评价、审议需协调或审批的投资银行项目；
b) 对于承担声誉风险和信用风险的业务，应按规定履行审查审批程序。投资银行业务与关联的融资业务应分别按照各自的业务流程独立地进行审批；
c) 银团贷款协议签署后，融资顾问工作及银团贷款筹组过程中的各项有效文件统一管理，具体文件包括：基础资料类、协议类、报批类、服务类。

6.7.2 信贷资产转让

主要风险点：

a) 信贷资产转让申请要件不齐备；
b) 未履行信用风险审批职责；
c) 信贷资产转让审批超授权。

控制要求：

a) 信贷资产转让申请项目审核时要提供以下要件：申请中应说明拟办理的业务类型、交易对手、交易方式、收益分配等问题，拟签署的资产转让与交易协议及法律意见，拟交易资产的原贷款调查报告，对买断型银团资产转让与交易业务，须提供拟买入资产的信用审批文件；
b) 信贷资产转让业务需开展信用风险审批，与关联的融资业务应分别按照各自的业务流程独立地进行审批；
c) 分支机构拟交易的资产转让与交易项目逐级报送，并在授权范围内审批，要按照投资银行业务授权将协议复印件（签署本）、资金往来的会计凭证复印件、系统操作方式等材料上报备案。

6.7.3 重组并购

主要风险点：

a) 项目未开展立项审查；
b) 评估人不具备并购交易主评估人及分析员资格；
c) 项目未经过投资银行项目评审委员会评审。

控制要求：

a) 重组并购项目实施前必须立项审查，建立严密的内部审核工作规则，认真核查各类文件的真实性、准确性和完整性，加强对重大业务的合同与法律文书的审查；
b) 配备符合要求的并购业务从业经验人员，主评估人要具有 3 年以上并购从业经验；
c) 项目评审委员会负责评价、审议需协调或审批的重组并购类投资银行项目。

6.7.4 常年财务顾问

主要风险点：

a) 业务审批时越权审批；
b) 常年财务顾问业务监督检查机制不完善。

控制要求：

a) 商业银行各级机构严格按照审批权限进行审批，对于协议金额超出权限范围的常年财务顾问业务，报有权审批机构审查批准；
b) 商业银行定期开展常年财务顾问业务检查，检查内容包括审批制度执行情况、业务流程规范性、档案管理情况等。

6.8 个人存款

6.8.1 开户

主要风险点：

a) 申请人开户资料或身份证明不真实；
b) 代理人身份不合规；
c) 开户凭证上无客户签名或签名不正确；
d) 开户风险提示不充分。

控制要求：

a) 严格审核个人客户身份和开户资料的真实性、完整性和合法性，按规定进行身份证件联网核查；
b) 个人客户经理不可为其服务的客户代办业务；营业网点员工不可直接代理客户办理任何金融业务，柜员亦不可为自己办理任何业务。授权人必须审核申请人（代理人）的证件类型、证件号码等相关资料，同时确认申请人（代理人）在业务办理现场；
c) 柜员须审核开户凭单上的客户签名正确无误；
d) 柜员须主动向客户进行风险提示，包括：客户与银行间的风险责任；客户要妥善保管个人信息、介质及密码。

6.8.2 存取款

主要风险点：

a) 未能识别假币和伪造的存单、国债、存折等；
b) 银行打印凭证内容与客户交易提示内容不一致；
c) 大额存取款业务未经授权办理。

控制要求：

a) 柜员须提高对现金和存单（折）、国债真伪的甄别能力，对其真实性开展审核；
b) 业务操作完成后，柜员（授权人）须审核凭证打印输出内容与客户交易内容一致，并在凭单上签章确认；
c) 柜员须按权限规定办理存取款业务，大额交易须经授权；授权人须审核申请人（代理人）的证件类型、证件号码等相关资料，同时确认申请人（代理人）在业务办理现场。

6.8.3 挂失冻结

主要风险点：

a) 挂失申请缺失或者挂失申请书内容不完整；
b) 未实施换人复核，擅自冻结或解冻客户账户。

控制要求：

a) 柜员受理挂失申请时，须认真审核挂失申请人（代理人）的挂失申请书内容的真实性、完整性，核对客户提供的个人信息、账户信息的准确性，联网核查申请人的身份，确认无误后及时办理挂失手续；
b) 建立复核制度，确保交易的记录完整和可追溯。有权冻结部门持有关公函，文件，通知来银行办理冻结或解冻账户或账户余额业务时，需经银行业务主管人员审核，涉及有关账户余额确实未被冻结或已被冻结的情况下，办理冻结或解冻手续并打印相关记录，专人复核柜员操作结果，同时确认柜员登记的冻结登记簿无误。银行业务主管人员据此在执行通知书等文件回执上签字，加盖业务公章后交执法人员。

6.9 个人贷款

6.9.1 调查和审查审批

主要风险点：

a) 借款人不符合法律法规或银行规定的资格；
b) 贷款申请资料提供不完整或不真实；
c) 信用审查不严；

d) 调查、审查、审批未有效分离，审批人未经授权或超授权审批。

控制要求：

a) 借款人应具有民事行为能力，借款人应具有还款能力，无不良信用记录；
b) 应执行面谈制度，调查借款人身份、诚信状况、借款用途、还款来源、担保方式的真实性，收集相关调查资料，应同时调查按揭贷款的开发商、汽车贷款的经销商、消费贷款的收款方等的资格和资信情况；
c) 应对贷款调查内容进行风险审查，关注借款人偿还能力、诚信状况、担保情况、合作机构风险情况，全面动态地客户以及合作机构准入条件、保证人担保能力、抵质押物价值以及变现能力等进行风险评估；
d) 应根据贷审分离、分级审批的原则，完善授权管理制度，规范审批操作流程，明确贷款审批权限，审批人员应在授权范围内按规定流程审批贷款，不得越权审批。

6.9.2 发放和支付管理

主要风险点：

a) 个人贷款未经有权人审批即与借款人签订借款合同；
b) 未落实抵押担保等前提条件即发放贷款，会计核算不准确；
c) 未执行个人贷款支付管理要求。

控制要求：

a) 应根据有权人签署的审批意见书，与借款人及其他相关当事人签订书面借款合同、担保合同和其他相关协议，应采用统一格式文本，合同要素应当明确，且与审批意见书一致；
b) 应落实独立的放款部门或岗位，负责落实放款条件。应规范担保流程，加强对抵押或保证的核保。应按照银行统一规定进行贷款业务的会计核算；
c) 个人贷款资金采取受托支付方式的，应在贷款资金发放前审核借款人相关交易资料和凭证是否符合合同约定条件，支付后做好有关细节的认定记录。采取借款人自主支付方式的，必须符合银监办法规定的条件，并要求贷款人定期报告或提供贷款资金使用情况。

6.9.3 贷后管理

主要风险点：

a) 个人贷款贷后检查未按要求进行；
b) 未执行贷款风险分类并足额计提拨备。

控制要求：

a) 应采取有效方式对贷款资金的使用、借款人的信用及担保情况变化等进行跟踪检查和监控分析；
b) 对零售贷款如自然人主要依据贷款逾期时间长短直接划分风险类别。应当按照谨慎会计原则，合理估计贷款可能发生的损失，及时计提贷款损失准备。

6.9.4 不良贷款管理

主要风险点：

a) 对不良贷款未按要求管理；
b) 个人贷款核销未按规定办理。

控制要求：

a) 应根据风险分类结果制定逾期催收、违约清收、不良贷款转化处置等管理措施，仍未归还的应通过诉讼、抵押物拍卖、以物抵债等方式进行资产保全；

b) 个人贷款呆账核销须限定核销范围、保证手续要件齐备，贷款经办行申报核销前，必须查清贷款损失形成原因、明确责任认定与追究。个人贷款呆账核销按“尽职追索、逐户组卷、逐级审查、集体审核、授权审批”的程序进行。核销完成后，还需账销案存，继续追收，最大限度减少损失。

6.10 信用卡

6.10.1 审批与开户

主要风险点：

a) 申请人身份不真实或提供资料不实；
b) 申请人存在信用不良记录或其他不良记录；
c) 未经本人或本单位同意申办信用卡；
d) 对高风险人群发卡。

控制要求：

a) 经办人员对申请办卡资料进行审核。个人申请办卡的，需提供身份证件复印件或影像材料及其他相关证明材料；企业申请办卡的，需提供《开户许可证》、组织机构代码证书、经过年检的营业执照副本的复印件，并加盖公章；
b) 银行应建立资信调查与资信审查制度，对信用卡申请材料出现疑点信息或系统审核记录缺失等情况的，不得核发信用卡；
c) 申请材料必须由申请人本人亲自签名，不得在客户不知情或违背客户意愿的情况下发卡。发卡银行受理的信用卡附属卡申请材料必须由主卡持卡人以亲自签名、客户服务电话录音、电子签名或持卡人和发卡银行双方均认可的方式确认；
d) 银行设立独立审批人，根据开卡人的综合资信状况，职业，收入水平等因素对个人资信进行审查，授予信用额度。超过审批人批准限额部分报上一级分管领导审批。对符合高风险特征的人群，审慎发卡。

6.10.2 卡片管理

主要风险点：

a) 空白卡保管不严；
b) 制卡岗位未做到岗位分离，制卡过程存在操作风险；
c) 打卡、打密数据信息泄露；
d) 非本人启用信用卡。

控制要求：

a) 坚持定期、不定期查库，定期轮岗。严密领用、使用过程交接手续；
b) 制卡员应保持相对稳定，与密码信封管理岗、空白卡保管岗岗位分离。设立专用机房，制卡在监控下进行，专人负责，人离上锁；打卡机应加密上锁；微机应设置密码；设立打卡机登记簿和运行日志；
c) 制卡员、打密员应在制卡和打印密码信封后立即删除制卡、打密信息；制卡数据的保留时间不得过长，商业银行经营信用卡业务，应当依法保护客户合法权益和相关信息安全。未经客户授权，不得将相关信息用于本行信用卡业务以外的其他用途；
d) 建立信用卡激活操作规程，激活前应当对信用卡持卡人身份信息进行核对。不得激活领用合同（协议）未经申请人签名确认、未经激活程序确认持卡人身份的信用卡。

6.10.3 交易监控

主要风险点：

a) 未对信用卡异常交易进行监测并采取适当措施；

b) 未对信用卡套现交易进行监测并采取适当措施。

控制要求：

a) 银行应建立持续监测记录和追踪预警异常业务行为（含入侵事故或系统漏洞）的流程并认真执行。对信用卡日常交易开展系统监测，对异常交易开展实时调查，必要情况下采取止付、降额等处理措施；

b) 强化日常交易监控力度，规范用卡行为，严禁持卡人参与信用卡套现或为他人提供套现便利。采取切实措施防范收单风险，严格执行特约商户的准入条件，认真审核查访商户的资信状况，并落实特约商户的巡查巡访制度。加强特约商户的日常管理，关注商户的交易行为，对存在疑似套现或确有受理伪卡、盗录信息、欺诈交易等的特约商户，及时采取切实有效的处置措施。

6.10.4 透支管理

主要风险点：

a) 对透支款逾期的客户未能及时提醒、催收；

b) 合作催收管理不规范，客户信息外泄。

控制要求：

a) 对于逾期客户，按照透支逾期期限的长短采取短信提醒、电话提醒、信函催收、上门催收、司法催收等不同催收措施；

b) 信用卡合作催收单位应符合准入条件，按照监管机构外包风险管理指引，做好日常检查辅导工作，与外包方签订客户信息保密合同，并跟踪验证合作催收效果。

6.10.5 额度调整

主要风险点：

a) 对不符合调额信用条件的客户调整信用额度，或调额不符合信用政策规定；

b) 超权限调额。

控制要求：

a) 审批人员根据客户的历史用卡情况、其他资信状况及其所申请的额度综合考虑调额比例，并对客户调额目的进行联系确认后开展调额，发卡银行应当建立信用卡授信管理制度，根据持卡人资信状况、用卡情况和风险信息对信用卡授信额度进行动态管理；

b) 银行设定调额条件、调额标准和调额权限，由独立审批人审批。超过调额权限的要报上一级审批人员审批。

6.10.6 交易清算

主要风险点：

a) 垫款业务未经过审批；

b) 清算不规范不准确。

控制要求：

a) 如出现业务垫款，按金额大小逐级审批后方可办理；

b) 记账人员认真审核凭证，记账后有专人开展事后监督。

6.10.7 卡片挂失

主要风险点：

a) 申请挂失的客户证件无效，签名不符或未签名；

b) 持卡人未委托代办挂失。

控制要求：

a) 柜员必须严格审查客户提交的身份证件，确保证件的真实、有效。个人代办挂失业务时，代办人须持本人和持卡人身份证原件办理。《业务申请书》内容填写正确、完整；必须有客户签名，代办业务还需登记代办人和持卡人身份证件类型、号码、发证机关；对于通过核实的持卡人信息，应注明已核实内容。持卡人的证件丢失，本人提供相关证明办理挂失，如代办挂失，则注明相关情况办理；

b) 卡片挂失时，代办人须持本人和持卡人身份证原件办理挂失，密码挂失及补换卡业务必须确认为本人办理。

6.10.8 拒付调单

主要风险点：

a) 拒付调单未在规定时间内查询答复；

b) 外卡调单业务未及时、准确处理。

控制要求：

a) 业务主管不定期检查，对查询查复业务存在的不足及时纠正，防范因拖延时间超过拒付期限而形成损失；

b) 外卡调单时，清算部门审核客服部门提交的客户拒付申请，查询交易明细后判断处理方式，不需要调单的申请，直接进入一次拒付，需要调单的申请，调阅并审核单据，获取持卡人答复；如单据不符合要求或持卡人否认，则向国际组织提出争议，如单据符合要求，且持卡人确认，则进行清算。

6.10.9 坏账核销

主要风险点：

a) 坏账核销未经过适当审批；

b) 核销客户信息未录入黑名单系统，或未进行账销案存管理。

控制要求：

a) 坏账款项的核销需要经过逐级审批，按一定条件实行核销；

b) 应将客户信息录入黑名单系统，应实行账销案存、继续追索。

6.11 私人银行

主要风险点：

a) 私人银行客户准入、交易委托未经过适当权限审批；

b) 未将私人银行销售产品信息及风险充分告知客户；

c) 未对产品基础信息开展尽职调查并经过独立风险评估。

控制要求：

a) 客户准入需经过适当的审批，金融资产符合准入标准，对暂不符合准入标准，但客户的金融资产丰富、资质良好的客户可以发展为私人银行客户，但需要报有权人审批并备案，客户委托交易需进行客户有效授权并经有权人审批；

b) 客户经理、财富顾问和投资顾问根据客户风险等级向客户推介与其风险属性相匹配的理财产品，并全面准确地揭示产品风险。对于非保证收益型私人银行产品，严禁做出任何形式的收

益承诺。对于市场风险较大特别是与衍生交易相关的投资产品，客户经理、财富顾问和投资顾问不应主动向无相关交易经验或经评估不适宜购买该产品的客户推介或销售。风险评估结果显示客户不适宜购买某产品但客户仍坚持要求购买的，须要求客户在产品说明书或其他销售文件上完整抄录风险提示并签字；

c) 私人银行客户投资项目在授权范围内审查审批，对私人银行销售的产品开展现场调查、文件资料的审查、当事人的访谈、第三方调查、关联情况分析评价等尽职调查，对产品的风险、收益进行综合评价，做出独立的风险评估。

6.12 资产托管

6.12.1 托管账户开立

主要风险点：

a) 账户设置不符合监管部门要求及协议规定；

b) 托管资产不独立。

控制要求：

a) 办理托管业务应开展合规检查，严格按照制度规定审核开户资料，严格按授权规定签订托管协议，规范开立和管理托管账户，按规定使用和保管托管业务印鉴，监督投资运作；

b) 受托托管资产应与自有资产及托管的其他资产相互独立，对不同委托人的资产、同一委托人托管的不同产品分别建账、独立核算、分账管理（委托人有特殊要求的除外），确保不同托管资产的相互独立。

6.12.2 托管账户监控

主要风险点：未监控托管资产的投资范围、投资比例、投资限制。

控制要求：通过在系统中设置监督指标对交易进行监督控制，通过交易监督系统和手工相结合的方式对法规和托管合同约定的比例和非比例方面的要求进行全面监控。

6.12.3 托管账户资金清算

主要风险点：

a) 托管业务资金清算不规范；

b) 清算与核算岗位未有效分离。

控制要求：

a) 资产托管业务资金清算应按照托管协议和相关制度办理，未经托管承办行授权批准，任何机构和个人不得动用托管账户资金；

b) 负责办理资金清算的人员与负责估值核算的人员实行岗位分离；资金清算应遵循时效性、合规性、保密性、托管人不垫款原则；建立定期对账制度，确保账账、账证、账实相符。

6.13 养老金

主要风险点：

a) 受托人与托管人、托管人与投资管理人未有效分离；

b) 未防范受托管理的违约风险。

控制要求：

a) 同一企业年金计划中，受托人与托管人、托管人与投资管理人不得为同一人；建立企业年金计划的企业成立企业年金理事会作为受托人的，该企业与托管人不得为同一人；受托人与托

管人、托管人与投资管理人、投资管理人与其他投资管理人的总经理和企业年金从业人员，不得相互兼任。建立养老金业务授权管理制度，对超授权业务逐级进行审批管理，制定规章制度和操作流程，明确岗位职责，对从业人员进行职业道德教育，防止养老金信息错误、损失或泄露等风险；

b) 办理受托管理业务要防范其他管理人的违约风险，在业务实际运营中，严格监督其他管理人的履约情况；办理账户管理业务要确保按签订的备忘录或合同约定的业务处理时效进行各项业务操作和信息传递。

6.14 贵金属

6.14.1 实物贵金属

主要风险点：

a) 实物贵金属原料准备存在市场风险；

b) 实物贵金属运输、库存管理不规范。

控制要求：

a) 品牌金的原料的准备主要采用向境外商业银行借贷的方式，对于从金交所买入的黄金原料，则采用境外账户黄金对冲的方式锁定黄金原料的价格，避免黄金原料因市场价格变动而遭受损失；对白银原料通过套期保值方式规避市场风险；

b) 实物类贵金属应双人封装入库（箱）、双人保管，调拨手续严密，定期盘点，确保账实相符；应与客户当面核验实物，双方签章、交接手续明晰；建立严密的贵金属运输管理流程和制度。

6.14.2 交易类贵金属

主要风险点：

a) 客户拒绝提供所承诺的保证金或无力按时和全额偿还所欠的保证金；

b) 贵金属报价存在异常；

c) 自营业务超授权或超过市场风险限额。

控制要求：

a) 适度提高客户贵金属延期交易业务保证金比例，并且在节假日期间适用更高的保证金比例；

b) 完善金交所系统和网银系统的衔接，加强交易报价的监控；

c) 制定贵金属自营投资业务市场风险限额：投资敞口限额、年度止损限额等，制定交易员授权制度，并监测执行情况，严禁超授权或超市场风险限额。

6.14.3 融资类贵金属

主要风险点：

a) 融资类贵金属未开展信用风险审批；

b) 缺乏租后检查监督；

c) 贵金属价格变动造成抵押率不足。

控制要求：

a) 融资类贵金属依托信用管理机制来控制风险。客户需通过系统内的信用等级评定和授信额度核定，单笔业务均需比照流动资金贷款进行审批，应严格抵押手续，核验贵金属实物的权属、规格、成色、重量等；

b) 加强租后检查监督，比照流动资金贷款要求明确信贷作业监督岗位职责，贷款资金不得用于证券、期货和金融衍生品交易以及其他违反国家有关规定的用途；

c） 持续监控贵金属价格，规范处置并适时增加抵押物等。

6.15 理财

6.15.1 资金募集

主要风险点：

a） 理财产品宣传和销售风险揭示的不足；

b） 产品客户适合度评估机制不完善；

c） 客户投诉处理机制不健全。

控制要求：

a） 商业银行总行统一管理和授权理财产品宣传销售文本，全面、客观反映理财产品的重要特性和与产品有关的重要事实，不得虚假记载、误导性陈述或者重大遗漏。理财产品宣传销售文本中出现表达收益率或收益区间字样的，应当在销售文件中提供科学、合理的测算依据和测算方式。理财产品销售文件应当包含专页风险揭示书；

b） 商业银行销售理财产品，应当遵循风险匹配原则，禁止误导客户购买与其风险承受能力不相符合的理财产品，销售人员除应当具备理财产品销售资格。商业银行应当根据风险匹配原则在理财产品风险评级与客户风险承受能力评估之间建立对应关系；应当在理财产品销售文件中明确提示产品适合销售的客户范围，并在销售系统中设置销售限制措施。商业银行应当在客户首次购买理财产品前在本行网点进行风险承受能力评估；

c） 商业银行应当建立全面、透明、快捷和有效的客户投诉处理体系，有专门的部门受理和处理客户投诉。客户投诉处理机制至少包括处理投诉的流程、回复的安排，调查的程序及补偿或赔偿机制。商业银行应为客户提供合理的投诉途径、确保客户了解投诉的途经、方法及程序，采用统一的标准，公平和公正的处理投诉。商业银行应配备足够的资源，确保客户投诉处理机制有效执行。

6.15.2 投资运作

主要风险点：

a） 未实行岗位分离控制；

b） 未遵循投资比例管理；

c） 投资超越监管范围，缺乏投资品管理机制；

d） 未遵循公允价格交易以及价格验证工作缺失。

控制要求：

a） 理财业务与自营业务分离。理财业务应遵循前台销售、中台投资与风控、后台核算估值的三分离原则，负责投资管理的部门也应实行投资交易、运行风控等岗位分离；

b） 严格按照理财产品说明书的投资范围和投资比例进行资金运作，理财产品资金投资于高流动性、本金安全程度高的存款、债券等产品实行比例管理。理财资金用于向单一借款人及其关联企业发放融资的总额实行比例管理；遵守理财业务相关的风险限额；

c） 理财资金投资范围符合监管规定，建立相应的风险管理体系和内部控制制度，严格实行授权管理制度，建立投资品的审核、审查机制；

d） 理财业务与银行自营业务之间要建立防火墙，实行风险隔离，采取公允价格交易，避免产生利益输送的交易行为。理财产品之间的交易应依法合规，采取公允价格交易，避免产生不同产品之间利益输送的交易行为。

6.15.3 会计核算与托管

主要风险点：

a) 理财产品未独立核算；

b) 理财产品收入核算、资金清算不及时准确；

c) 理财产品资金未进行托管管理。

控制要求：

a) 商业银行应对每个理财计划单独核算，覆盖资金募集、投资过程、各类标的资产的明细、到期清算的全过程。每个理财计划建立托管明细账。计划终止计算每个理财计划单独兑现的收益；

b) 投资管理人要根据按照产品说明书约定的方式支付理财产品承担的销售手续费、托管费、投资管理费、业绩报酬等费用，公允地进行资产管理业务中间业务收入的分配工作。各项手续费应按规定的范围、标准和费率严格收费，并纳入账内核算，防止收费流失。产品募集成立后，销售部门应最晚于产品起息日将募集资金划入指定的理财产品托管账户。投资管理人必须在理财产品申购、赎回、付息及到期的资金兑付日前将兑付款项足额划至清算账户，确保履约；

c) 理财产品资金必须进行托管，托管机构与运行管理部门定期开展会计核算和估值结果等对账。

6.15.4 项目管理

主要风险点：

a) 项目管理未实现前中后台分离；

b) 项目前提条件不落实或不符合准入标准；

c) 项目未纳入融资风险限额管理。

控制要求：

a) 理财项目管理应做到前、中、后台相分离，即项目营销、风险审批、投资审批与投资后管理相分离；

b) 理财项目前提条件必须在投资前全部落实和审核完毕。投资监管机构确定风险权重不为零的金融机构债券（不包括次级债券）、非金融企业债务融资工具，信用评级须达到投资级以上。股权投资数额和投资项目应当与现有生产经营规模、财务状况、技术水平和管理能力等相适应，不得用于与主营业务无关的高风险投资；

c) 商业银行的董事会或高级管理层应当根据理财计划及其所包含的投资产品的性质、销售规模和投资的复杂程度，针对理财计划面临的各类风险，制定清晰、全面的风险限额管理制度，建立相应的管理体系。理财计划涉及的有关交易工具的风险限额，同时应纳入相应的交易工具的总体风险限额管理。商业银行对信用风险限额的管理，应当包括结算前信用风险限额和结算信用风险限额。商业银行的各相关部门都应当在规定的限额内进行交易，任何突破限额的交易都应当按照有关内部管理规定事先审批。

6.16 债券投资与交易

主要风险点：

a) 债券投资与交易未按规定审批；

b) 未执行市场风险限额管理；

c) 债券发行体的授信管理不落实；

d) 债券投资分类不准确。

控制要求：

a) 交易人员根据债券投资决策会议的决议，对债券投资方案进行修订和完善，按照授权权限审批，审批内容主要包括：信用风险审查、投资额度审查、投资策略审查等。制定债券投资与交易的授权规定，明确允许交易的业务品种和单笔最大交易额度等交易权限。未经上级机构批准，下级机构不得开展任何资金交易；
b) 银行市场风险限额包括名义限额、止损限额、敏感度限额和 VaR 限额等，根据银行账户和交易账户的划分管理要求，针对不同账户的业务和交易组合，采用不同种类的市场风险限额指标进行管理；
c) 对债券发行主体实行授信管理，开展授信尽职调查并在授信额度内开展债券投资，对金融债券、企业债等涉及信用风险的债券投资，实施信用风险限额管理，开展债券投资后信用风险管理检查；
d) 交易人员在进行债券买入时，应根据持有意图确定债券资产的账户分类。交易人员在持有债券期间，根据业务需要或持有意图变化等情况可根据不同的资产账户对已持有的债券资产进行账户重分类，并报送资产负债管理委员会审议。

6.17 外汇交易

主要风险点：
a) 外汇交易前、中、后台未分离；
b) 办理外汇交易业务的客户未落实信用风险缓释措施；
c) 未对交易限额、交易对手授信进行有效监控。

控制要求：
a) 开展外汇交易业务应遵循职责分离原则，前台交易或营销、中台价格验证和限额管理等风险控制和后台账务核算、证券结算及资金清算需相互分离，不得由同一部门承担；
b) 对于按“T+1”“T+2”方式交割的即期、远期外汇交易业务，经办行应落实信用风险管理措施，采取占用客户授信、收取风险保证金等低风险担保措施控制信用风险；
c) 商业银行应当建立资金交易中台和后台部门对前台交易的反映和监督机制。中后台监控部门应当核对前台交易的授权交易限额、交易对手的授信额度和交易价格等，对超出授权范围内的交易应当及时向有关部门报告。

6.18 货币市场业务

主要风险点：
a) 融资超授信或超融资额度；
b) 未实行流动性风险限额管理；
c) 融资业务处理不规范。

控制要求：
a) 审查交易对手信用风险，对单一交易对手的拆出余额不得超过商业银行对其核定的融资专项授信额度，运用系统进行控制；
b) 通过明确设定货币市场业务的流动性风险限额或主要账户余额来确保资金流动性；
c) 在授权范围内开展货币市场业务，规范操作融资业务的申请受理、审批、协议签署、资金汇划及清算、后续管理等，并纳入系统管理，任何同业融资清算均不得使用现金支付，不得滥用会计科目核算，业务办理后要及时建立从审查至收回全过程的融资情况档案。

6.19 衍生产品交易

主要风险点：

a) 申请衍生产品交易客户风险评估不到位；
b) 交易授权和止损管理制度不完善；
c) 交易对手信用风险控制缺失；
d) 未定期对未到期金融衍生合约进行公允价值评估。

控制要求：

a) 客户首次办理衍生产品交易前，商业银行营业机构应对代客衍生产品交易适合度进行评估。按照评级授信的相关要求对客户履行尽职调查程序，评定客户信用等级并核定衍生产品交易专项授信额度，同时明确专项授信使用条件；
b) 商业银行建立并严格执行授权和止损制度，制定并定期审查更新各类衍生产品交易的风险敞口限额、止损限额、应急计划和压力测试的制度和指标，制定限额监控和超限额处理程序，在因市场变化或决策失误出现账面浮亏时，应当严格执行止损制度；
c) 商业银行制定完善的衍生产品交易对手信用风险管理制度，选择适当的方法和模型对交易对手信用风险进行评估，并采取适当的风险缓释措施；
d) 风险管理人员应定期对未到期金融衍生合约进行公允价值的评估，并建立有效的风险监督、控制和报告制度。

6.20 债券承销发行

主要风险点：

a) 超授权办理主承销项目；
b) 债券承销持有比例违反监管规定；
c) 未对二级市场交易情况监测。

控制要求：

a) 建立承销发行业务授权审批制度，在完成主承销协议本文的法律审查后，对于超出权限范围的主承销项目逐级上报有权人审批；
b) 债券承销持有比例符合监管规定；
c) 承销人员负责收集并监测承销债券的信用风险情况，并关注预警信息：客户已发行金融债券二级市场交易是否出现重大异常波动，客户信用风险影响已发行的金融债券本息的偿付。

6.21 运行管理

6.21.1 账户管理

主要风险点：

a) 存款人出租出借账户或利用存款账户从事违法欺诈活动；
b) 利用签章、票据进行诈骗或从事违法活动；
c) 利用内部账户、通过内部特种转账业务从事违法活动。

控制要求：

a) 按照操作流程开立账户，严格执行账户开立操作与审批管理相分离的制度，保证新开立账户资料的真实性、完整性和合规性；
b) 加强客户预留印鉴管理，严格客户预留印鉴建立、启用和变更环节的审核，加强对预留印鉴的保管，认真核对预留印鉴；
c) 加强内部账户和内部特种转账业务管理，内部账户的开立、使用、变更和撤销应遵循统一管理、明晰核算、防范风险、降低成本的原则，对内部特种转账业务实行授权审批管理，加强对内部账户核对和监督检查，确保内部账户管理合规安全。

6.21.2 会计核算要素管理

主要风险点：

a) 冒领、冒用他人权限卡实施从事违规、违法活动；

b) 利用空白重要凭证与其共同构成支付要件的会计印章、密押机具等从事内、外部违 规、违法欺诈活动。

控制要求：

a) 加强权限卡的申请、审批、使用、变更管理。权限卡密码应不定期更换，严禁随意放置权限卡或转交他人使用；

b) 加强对空白重要凭证、会计核算专用印章、密押机具的管理：

1) 空白重要凭证及与其共同构成支付要件的会计印章、密押机具等实行分人使用、分开管理；空白重要凭证上不得预先加盖印章备用，内部员工不得为客户代购、保管和传送各类空白重要凭证，重要空白凭证应按规定定期盘点,重要空白凭证的领取、使用要做好登记手续；

2) 会计核算专用印章实行“统一管理、分级刻制”的原则，会计核算专用印章领取时做到双人签收、双人领取，使用时做到专人使用、专人负责，保管时做到专匣保管、固定存放、临时离岗、人离章收；

3) 密押机具按照重要物品机具进行管理，坚持专人保管、专人负责的原则。使用和保管密押机具人员保持相对稳定。

6.21.3 账务组织管理

主要风险点：

a) 业务核算人员未按照记账规则进行操作，引发操作风险；

b) 未按规定程序办理查询查复业务，引发客户资金风险和商业银行法律及声誉风险。

控制要求：

a) 业务核算人员须严格按记账规则进行操作：

1) 业务核算人员应严格按照规定的记账规则,正确使用会计科目和会计凭证进行业务核算，发生核算差错应经有权人授权或审批后进行更正；

2) 业务核算必须有账有据，及时记账，当日结账，做到账账、账款、账实、账表、账据、账簿、账卡（折）和内外账务等全部相符。

b) 受理司法机关等有权部门查询应符合规定程序；查询查复应做到有疑速查，查必彻底，有查速复，复必详尽。

6.21.4 现金业务管理

主要风险点：

a) 现金业务岗位混乱，职责不清；

b) 现金出入库交接手续不清、现金收付核算不正确，造成现金损失或引发案件；

c) 金库和自动柜员机（ATM 机）管理不当，引发操作风险和道德风险。

控制要求：

a) 落实现金业务岗位分离制度，坚持现金业务管库员、记账柜员和授权柜员等岗位分离，做到各司其职，互相制约；

b) 加强网点钱箱及现金收付管理，现金收付款应凭合法、有效的凭证办理，坚持先收款后记账、先记账后付款原则，按券别操作，当面清讫，一笔一清，日清日结，现金、实物交接应责任分明、有据可查；
c) 加强金库和自动柜员机（ATM 机）管理。金库管理应坚持金库主任负责制，严格执行业务操作规程，加强金库门锁（密码）管理，现金、实物出入库遵循先入库后记账、先记账后出库的原则，日结日清，确保账账、账实、账款相符，有效控制金库管理风险。加强自动柜员机（ATM 机）控制，严格按规定执行业务操作，加强密码和钥匙或其他密钥管理，有效防范操作风险。

6.21.5 支付结算管理

主要风险点：
a) 利用虚假凭证或因客户身份识别不到位，违规支付引发交易风险，导致客户及商业银行资金损失；
b) 违反支付结算原则办理支付结算业务引发客户资金风险和商业银行的声誉风险；
c) 延迟支付结算，截留挪用客户资金。

控制要求：
a) 落实客户身份要求，规范支付操作行为，认真审核支付凭证、记载事项、签章等的真实性、完整性、合规性，约定使用支付密码时须校验支付密码；
b) 办理支付结算应准确、及时、安全，并做到恪守信用，履约付款；谁的钱进谁的账，由谁支配；银行不垫款；
c) 不得以任何理由压票、任意退票、截留挪用客户资金，不得无理拒绝支付应由银行支付的票据款项，不得拒绝受理代理他行正常结算业务。

6.21.6 清算管理

主要风险点：
a) 资金清算事前、事中、事后的全程管理不到位，未建立清算风险准备金的筹集及使用规则，引发流动性风险；
b) 资金清算过程中人工干预动作过多，引发操作风险；
c) 关键性操作缺乏必要的复核及授权，引发操作风险。

控制要求：
a) 建立清算的风险准备金筹集及使用规则；
b) 对有疑问的报文按查询查复管理要求进行处理，按照清算对账管理要求进行系统内各级清算机构之间、相关部室之间以及与人民银行、同业机构之间的账务核对，及时处理清算差错；
c) 资金清算须在规定的清算时间内统一进行，并实行清算业务录入、复核、授权、对账的分离制度，本外币资金调拨业务应凭资金管理部门及相关前台部门的支付指令办理。

6.21.7 参数管理

主要风险点：
a) 参数维护权限和责任权限不清晰，维护权限管理、监控不当，造成业务数据非法修改，产生舞弊风险；
b) 系统参数控制变量的设置、维护错误、功能测试不充分，引发系统逻辑风险和商业银行的声誉风险。

控制要求：

a) 参数管理实行统一设计、集中管理原则，健全参数管理制度，按职责分离的方式落实参数变更申请审批，将参数维护、数据录入、监督控制的职能分开；
b) 参数设置应准确完整、安全合规，参数维护应依据有效的业务需求凭据，履行必要的审批手续，严格按岗位流程进行。参数监控应遵循重点监控原则，对参数管理的重要环节和重要参数表进行监控和检查。

6.22 电子银行

主要风险点：
a) 未对电子银行系统、数据库和应用程序建立授权控制和进入特权制度；未在电子银行系统、数据库和应用程序中采取适当措施保证不相容职责的分离；
b) 开展电子银行服务未采取适当措施对客户身份和授权情况进行认证；未对客户作业权限、资金转移或交易限额实施有效管理；
c) 未对电子银行客户证书实施有效管理，未能促进交易的不可否认性和明确电子银行交易责任；
d) 未建立业务连续性计划、应急计划和事故处理预案，不能确保电子银行系统和服务的连续可用性；
e) 未实施数据交换与转移的有效管理，未采取适当措施确保客户信息与隐私安全。

控制要求：
a) 商业银行应规范电子银行业务岗位人员设置，按照“事权划分、岗位牵制、权限可控”的原则，为电子银行相关业务系统、数据库和应用程序的用户设置操作权限，并有效实施不相容职责的分解。商业银行应明确电子银行管理、运营等各个环节的主要权限、职责和相互监督方式，有效隔离电子银行应用系统、验证系统、业务处理系统和数据库管理系统之间的风险；
b) 客户注册、变更、注销电子银行服务，商业银行应对客户身份进行审核；个人电子银行注册、变更业务应由客户本人办理，企业电子银行业务应由企业授权办理相应电子银行业务的人员办理；为客户提供电子银行服务，应使用个人身份号码、密码、智能卡、生物测量技术和数字证书等方法对客户身份进行认证。客户使用的身份认证方式应与其办理业务的风险程度相适应，对使用不同身份认证方式的客户设置不同的交易权限和额度权限；
c) 向客户发放的客户证书应作为重要物品管理，商业银行应对其保管、传递、交接、发放等进行准确、及时记载，并进行定期清理；已制作未发放的客户证书在商业银行内部应严格保管和交接，严禁由具有证书解冻权限的柜员保管；证书解冻必须在确认客户已领取证书后才能办理。商业银行应采用适当的加密技术和措施，保证电子交易数据传输的安全性与保密性，以及所传输交易数据的完整性、真实性和不可否认性；
d) 商业银行应制定电子银行业务连续性计划，并充分考虑第三方服务供应商对业务连续性的影响并采取适当预防措施；应制定电子银行应急计划和事故处理预案，并定期进行测试与演练；
e) 商业银行应控制客户信息的知悉范围，避免无关人员获取客户信息，客户数据的使用不能超越客户允许的范围；不应向无业务往来的机构转移电子银行客户信息；由于业务发展需要向其他机构转移电子银行客户信息应在法律法规或客户许可范围内，并与信息接收机构签订书面保密合同，指定专人监督有关数据使用、保管、传递和销毁；为电子商务提供网上支付平台，应严格审查合作对象，签订书面合作及保密协议，建立有效监督机制。

6.23 代理业务[3)]

3) 商业银行的代理业务是指银行接受客户的委托，以代理人的身份代表委托人办理一些双方议定的经济事项的业务。主要包括代收代付业务，代理证券业务，代理保险业务及代理保管业务等内容。

主要风险点：

a) 开办代理业务未满足相关准入要求，未取得有关主管部门核准的机构资质、业务人员从业资格及商业银行内部的业务授权；未建立对合作方的准入管理制度，未对拟合作方的资质进行审慎调查；
b) 未建立代理业务相关的规章制度和操作规程，未对代理合同或协议实施统一管理，导致合规性及有效性问题；
c) 未为代理资金设立核算专户，代理资金的拨付、回收、核对等手续不完善，未做到专款专用；
d) 未对代理资金支付进行审查和管理，未按照代理协议进行资金划转；未遵循银行不垫款原则，介入委托人与其他人交易纠纷；
e) 未按照会计制度正确核算和确认代理业务收入;未对代理业务实行收支两条线管理，出现代理业务收入被截留或挪用的情况；
f) 开展代保管业务时场地、设备等未符合国家标准，未对客户身份进行有效验证。

控制要求：

a) 商业银行开展代理业务应履行相关审批程序，确保取得合法的机构资质、人员从业资格和内部授权许可；建立合作方准入管理制度，并对代理业务拟合作方的资质进行审慎调查；
b) 建立代理业务相关规章制度和操作规程，统一代理合同及相关协议的管理；
c) 商业银行办理代理业务，应当设立专户核算代理资金，完善代理资金的拨付、回收、核对等手续，防止代理资金被挤占挪用；
d) 应建立和遵循代理资金支付的审查和管理流程,按照代理合同或协议约定办理资金划转手续；遵循银行不垫款的原则，不介入委托人与其他人的交易纠纷；
e) 商业银行应当完善代理业务收入核算和确认的会计制度，并严格按照会计制度进行收支核算与管理；
f) 商业银行开办保管箱业务，应当在场地、设备和处理软件等方面符合国家安全标准，对用户身份进行核验确认。对进入保管场地和开启保管箱，应当制定相应的操作规范，明确要求租用人不得在保管箱内存放违禁或危险物品。

6.24 财务会计管理

6.24.1 经营发展规划及计划

主要风险点：

a) 缺少中长期发展规划和年度经营计划，或发展规划和经营计划不健全，导致经营缺乏约束；
b) 经营目标设计不合理，与发展战略目标不统一，或违背监管政策和宏观政策；
c) 计划执行不力，经营计划流于形式。

控制要求：

a) 制定计划编制制度，明确计划框架、指标口径、编制内容和流程；
b) 建立科学的计划编制指引，明确编制依据、程序和方法，确保经营计划和发展规划具有预见性、先进性和可操作性；
c) 建立计划执行监督考核制度，加强监测、监督，明确相应奖惩措施。

6.24.2 会计科目管理

主要风险点：

a) 未制定统一的会计科目政策，会计科目设置不够完整准确，存在随意设置会计科目、随意改变会计科目核算内容，任意增加、取消、合并会计科目、分户账现象；

b) 会计科目使用不正确，使用已停用、撤销的会计科目，乱用、串用、混用会计科目，混淆科目的使用币种、级次以及科目对应关系。

控制要求：

a) 严格遵循统一规划、集中管理、规范使用、定期监控的原则，加强会计科目的设置、调整、编号及核算标准的控制；
b) 规范会计科目的使用，定期开展定性定量的监控分析，提高会计信息质量。

6.24.3 财务收支

主要风险点：

a) 超越权限的财务事项未上报审批，存在分拆财务事项绕开权限管理的情况，未财务权限实行刚性控制，未对财务授权审批情况实施有效监控；
b) 财务收入不真实，收入确认不符合权责发生制原则，不属于本期的收入未按规定进行分期确认；
c) 支出确认不符合权责发生制原则，虚列成本支出，存在违反规定列支财务费用、营业外支出等情况；
d) 资产减值准备计提范围不完整，计提方法不符合新财务会计制度要求，计提金额与预计损失金额不一致；
e) 存款应付利息计提范围不完整，计提利率不准确，未按规定比例计提职工教育经费、工会经费；
f) 重大支出没有经过财务审查委员会审议。

控制要求：

a) 建立财务授权和转授权制度，各级机构、部门和人员要在授权范围内实施财务管理活动、审批决策财务事项并对财务结果负责，严禁越权审批或超绕授权指标办理业务；
b) 各项收入要按照会计核算制度及时、完整、准确确认，不得截留或以任何理由坐支，严禁提前或延迟确认收入。任何机构、部门及个人都不得少计、少收、转移、挪用、截留收入；
c) 严格区分本期成本和下期成本、收益性支出和资本性支出、成本性支出和营业外支出的界限；
d) 按规定提取和使用各项准备金，确保风险拨备完整和准确；
e) 对应计、应提、应列、应摊、应并的财务收支应按规定进行核算，确保损益真实、准确、完整，严禁隐瞒、虚造损益，严禁截留利润；
f) 严格贯彻执行财务审查委员会工作规则，财务审查委员会对固定资产、无形资产和费用投入等财务资源配置的必要性、合理性、合规性进行审议对审议项目执行情况进行检查、监督。

6.24.4 财务集中业务

主要风险点：

a) 未建立适应财务集中核算要求的内部控制措施；
b) 财务集中处理流程各环节衔接不紧密，未对报账机构备用金账户进行定期对账等有效管理，备用金账户收支范围不符合规定；
c) 未对财务中心进行定期检查和持续监督。

控制要求：

a) 建立统一的财务集中制度，制定财务集中办法，明确组织机构、核算管理模式、财务集中事项和主要核算流程，制定机构岗位责任制文件，财务核算中心内部制定并实行定期或不定期的岗位轮换制度和人员强制休假制度，推行离岗审计制度；

b) 严格执行财务集中业务操作规程等制度办法，规范备用金账户和集中支付账户的使用，通过财务管理综合系统进行财务管理、控制、核算、支付等各项工作，规范操作程序，加强财务集中数据的日常核对与监测控制，实施有效的过程与事后控制；
c) 对财务中心进行定期检查和持续监督，建立一套满足本行财务集中风险控制要求的监测分析指标体系，开展对各项监测指标的监测分析，对财务核算中心进行全面审计，建立规范的风险控制责任认定和严格的责任追究制度。

6.24.5 固定资产控制

主要风险点：
a) 配置需求不符合实际，重大项目配置没有进行可行性论证，投入产出达不到预期成效，配置后形成闲置；
b) 核算内容不真实、不准确，虚列固定资产；
c) 未定期对自有及租入固定资产进行实物盘点，造成账实不符，或被其他单位无偿占用，或丢失。

控制要求：
a) 建立健全固定资产管理制度，科学编制固定资产投资预算，科学编制网点建设预算，优化固定资产配置资源，固定资产配置实行统一规划、授权管理；
b) 规范固定资产的核算和处置管理，严格按照固定资产的确认条件和价值标准，对固定资产进行分类和初始计量、后续计量，及时对固定资产增减变动进行会计处理；
c) 加强自有及租入固定资产日常管理，严格固定资产权属管理，确保资产完整；建立固定资产实物维修、保养、定期清查制度，明确使用部门、实物管理部门和价值管理部门的职责权限，固定资产的处置应按照规定权限和处置方案执行，通过分类整合和专业化处置，实现资产回收价值最大化。

6.24.6 集中采购管理

主要风险点：
a) 集中采购制度体系不健全、不适用或制度维护不及时；
b) 采购申请审批流程不合规，或集中采购审查委员会和专家小组未依据有关规定对集中采购项目有效履行职责，存在超权限实施集中采购；
c) 采购合同文本使用和签署不规范，未按合同验收采购项目，财会部门未对付款事项进行审核；
d) 供应商推荐方式不符合规定，未定期开展供应商的综合评价，建立健全供应商退出机制；
e) 未建立集中采购考核办法，或集中采购考核办法不能有效提高集中采购的质量和效果。

控制要求：
a) 建立健全集中采购管理制度，严格划分职责权限，执行使用人、主管人、审批人、采购人和监督人分离的管理模式；
b) 规范采购申请审批流程，严格按照所授权限实施集中采购，严禁越权、擅权审批；
c) 严格采购合同文本和签署程序，严格按照合同条款验收付款；
d) 建立供应商评估和准入管理，健全集中采购工作后评价工作机制；
e) 完善集中采购考核管理。

6.24.7 应税事务管理

主要风险点：对税收法规理解不到位，未严格执行税收政策，造成应纳税额计算差错，未按时申报纳税，申报资料不全；未及时支付税款或税款支付数额出现差错。

控制要求：加强税收政策培训，明确分工管理，落实责任，建立并完善涉税台账，按税法落实对不同申报事项的具体要求，规范对各类涉税证明、发票、凭证资料及涉税台账的复核与监测工作，精确计算，严格申报，准确计缴。

6.25 资产负债管理

6.25.1 人民币资金管理

主要风险点：

a) 利率管理制度不健全、利率政策执行不到位造成利率风险或经营决策风险；
b) 资金内部转移价格制定不合理或执行不到位，造成资金使用效果不佳或经营风险；
c) 审批不严格、操作行为不规范，造成流动性支付风险及操作风险。

控制要求：

a) 加强利率管理：
   1) 认真执行国家利率政策，健全利率管理制度，加强利率定价议价管理，按照利率政策、规章制度与合同约定规范利率执行；
   2) 加强利率风险监测、报告和监督检查工作。
b) 根据全行资产负债管理要求、市场利率情况综合确定，并根据外部市场环境变化和全行经营策略定期或不定期调整，完善内部资金转移价格管理；
c) 严格资金运营审批和监督：
   1) 按照事权划分和岗位分离要求，对加强对资金运营的审查和监督，包括利率设定、额度限制及其对全行资金头寸的影响等。编写资金运营分析报告，对全行的利率风险、流动性风险，资金配置状况等进行分析并报资产负债管理部门负责人审阅；
   2) 加强系统参数管理，对参数设置、维护的进行权限控制。

6.25.2 外汇资金管理

主要风险点：

a) 汇率使用不准确或由于外汇买卖业务所导致资产负债的错配所引发的汇率风险；
b) 市场利率波动，导致外币业务遭受损失的风险；
c) 由于资产负债期限不匹配、突发的大额支取或结汇而导致的流动性风险。

控制要求：

a) 所有外汇业务的汇率均由总行统一规定，同时利用系统对汇率进行硬控制；建立对汇率波动的实时监测制度，防范汇率波动所产生的损失风险；
b) 执行人民银行关于外币存款的利率政策，执行询价、报批制度，及时平盘，确保利率风险净敞口为零；
c) 加强对资金运营的审查和监督，保持合理头寸。

6.25.3 本外币资金运营

主要风险点：

a) 未按规定缴纳法定存款准备金及备付金；
b) 头寸匡算不准确，出现资金缺口或流动性支付风险；
c) 超权限进行资金调拨，调拨金额与实际匡算金额不一致。

控制要求：

a) 严格按照规定统一调缴法定存款准备金，合理安排超额存款准备金比例，提高资金头寸周转效率，减少低息资金占用；
b) 强化资金头寸管理：加强资金头寸管理，实时监控本级和下级行的资金来源和运用情况，准确匡算资金头寸；建立覆盖各级机构的大额资金预测预报管理体系，加强上下级行之间、部门之间的信息交流和协调配合，对大额资金变动进行及时、准确的预测预报，做好对账及跟踪监测，减少资金在途损失，保证支付与清算，严防支付风险。
c) 强化资金调拨清算控制，严格按照前后台分离要求设置资金调拨岗位权限，在严格授权管理下进行资金调拨。

6.25.4 经济资本管理

主要风险点：
a) 资本充足率未达到监管部门的要求；
b) 经济资本的目标不合理，不能对银行的业务起到指导作用；
c) 经济资本的计量方法不统一或未经有效性验证。

控制要求：
a) 每年年初总行对全行的资本充足率进行预算，编制当年的经济资本限额指标，资本充足计划和经济资本配置计划，按季向银监会报送其各项资本充足率指标，确保资本充足率达到监管部门的要求；
b) 按国家宏观经济政策和企业经营发展战略，及时优化调整各项业务经济资本配置系数，鼓励发展低经济资本占用、较高收益的业务，控制风险资产盲目扩张；
c) 经济资本计量原则和计量模型由总行统一制定并定期进行合理性评估，计量方法实行系统硬控制。

6.25.5 国债业务

主要风险点：
a) 超计划发行、串档或串期发行；
b) 缴存国债的路径、缴存款项错误，收取的兑付本金或代理手续费错误。

控制要求：
a) 准确完成相关参数设定，建立双人复核制度，防止超计划发行、串档或串期发行；
b) 及时与财政部核对缴款路径和款项，根据代销量与国债公司核对兑付本金及手续费。

6.26 产品创新管理

主要风险点：
a) 新产品的开发管理混乱，存在重复开发等资源浪费情况；
b) 未根据市场、客户需求，同类产品情况等综合比较后进行新产品研发，所开发的新产品不适销对路或不符合监管机构的规定。

控制要求：
a) 对新产品开发立项实行统一管理，加强新产品在全行的推广和运用；
b) 建立执行立项审批制度，及时按规定向监管机构报备。

6.27 租赁

6.27.1 业务审查与授信管理

主要风险点：

a) 客户经理尽职调查内容不完备、不真实、缺乏有效性；

b) 授信环节未按照业务规定进行严格审查。

控制要求：

a) 前台业务部门对客户的相关情况进行尽职调查，加强对企业股东方及偿债能力的调查和分析；

b) 风险管理部门受理授信业务后，对前台业务部门提交的授信预案提出审查意见，项目评审委员会对授信方案进行审议。

6.27.2 业务审批

主要风险点：

a) 未对租赁物的价值、所有权属和抵押物价值和权属进行评估；

b) 未对调查评估报告进行有效审查；

c) 未按照授权规定审批租赁业务方案。

控制要求：

a) 前台业务部门应对租赁物进行调查评估，评估内容包括租赁物的价值、所有权属和抵押物的价值和权属；

b) 风险管理部门受理租赁业务后，审查岗位人员遵循客观、独立、公正的原则，对前台业务部门提交的调查报告及相关资料提出审查意见，项目评审委员会集体审议；

c) 租赁业务方案须经决策层审议通过。

6.27.3 业务办理

主要风险点：

a) 未按审批要求落实前提条件；

b) 未对租赁资产进行投保，或购买的保险不符合规定；

c) 未按规定办理租赁标的物所有权转移的手续。

控制要求：

a) 前台业务部门落实租赁前提条件，风险管理部审核岗位人员核准；

b) 租赁业务应执行对项目租赁物保险的要求；

c) 前台业务部门完成租赁物所有权转移手续。

6.27.4 后续管理

主要风险点：

a) 未按规定对承租人进行监测；

b) 未按照规定检查租后情况；

c) 未提示客户按时支付租赁本金和租赁利息。

控制要求：

a) 前台业务部门定期编制租后检查表与分析报告；

b) 租后检查表与分析报告应交风险管理部门审查岗位人员进行风险分析；

c) 在租赁业务存续期内，提示客户按时给付租赁本金和租赁利息，进行租金催收，催收未果的按照不良租赁资产管理的相关规定进行处理。

6.28 基金

6.28.1 公募基金

主要风险点：

a） 基金产品开发未逐级授权审批；

b） 基金产品发行未履行信息披露审批流程；

c） 基金销售未开展客户风险能力测试；

d） 基金投资管理未执行授权制度；

e） 基金公司未按不同基金设立账户进行核算。

控制要求：

a） 公募基金产品研发后，按照授权管理规定逐级授权审核批准，并审批产品定价方案；

b） 招募说明书、发售公告、发行文件（基金合同、托管协议、招募说明书及发售公告）、基金净值履行信息披露审批流程，定期披露；

c） 基金销售人员应取得基金销售业务资格，建立基金销售适用性管理制度，对基金投资人开展风险能力测试，投资人应购买与其风险承受能力相适合的基金产品。对于购买基金产品与个人风险承受能力不相匹配的投资人，要求投资人签订投资人意愿声明书；

d） 基金公司明确投资决策委员会、分管投资的高管人员、基金经理等各投资决策主体的职责权限划分，合理确定各基金经理的投资权限。基金经理在授权范围内可以自主决策，超过投资权限的操作需要经过严格的审批程序；

e） 基金公司对所管理的基金应当以基金为会计核算主体，独立建账、独立核算，保证不同基金之间在名册登记、账户设置、资金划拨、账簿记录等方面相互独立。基金会计核算应当独立于基金公司会计核算。

6.28.2 专户理财

主要风险点：

a） 专户理财产品未授权审批；

b） 基金公司固有财产与委托财产未有效分离；

c） 专户理财业务投资经理与基金经理相互兼任。

控制要求：

a） 专户理财产品研发完成后，按照授权逐级审核批准，对专户理财产品进行审核，评估表决形成决议，同拟任基金经理人选上报有权人进行审批；

b） 基金公司从事特定资产管理业务，委托财产独立于资产管理人和资产托管人的固有财产，并独立于资产管理人管理的和资产托管人托管的其他财产，资产管理人、资产托管人不得将委托财产归入其固有财产；

c） 基金管理公司办理特定资产管理业务的投资经理与证券投资基金的基金经理不得互相兼任。

7 信息科技层面内部控制评价

7.1 评价步骤

信息科技层面的内部控制主要指对计算机、通信、微电子和软件工程等现代信息技术所采取的一系列内部控制过程，旨在确保商业银行安全、持续、稳健运行，推动业务创新，提高信息科技应用水平，增强核心竞争力和可持续发展能力。对信息科技层面内部控制的评价主要包含以下评价步骤：

a） 确定信息科技层面内部控制的目标；

b） 确定信息科技层面内部控制的范围与内容；

c) 构建信息科技层面的风险控制矩阵，包括梳理信息科技相关流程，评估公司、流程等层面的信息科技风险，识别重要风险和关键控制点，构建信息科技层面内部控制的领域树，设计相应的评价程序，形成书面的风险控制矩阵及评价方案和工作底稿等；
d) 进行穿行测试，填写穿行测试工作底稿；
e) 实施控制测试，填制控制测试工作底稿；
f) 确认与评估内部控制缺陷，包括样本记录、填写事实确认书、确认控制缺陷、评估缺陷等级等步骤；
g) 提出整改建议，并就该整改建议与被评价对象进行沟通；
h) 对整改结果进行再测试；
i) 得出信息科技层面内部控制评价的结论。

具体评价工作底稿可参考表 A.3 信息科技层面内控评价工作底稿。

7.2 信息科技治理

7.2.1 治理架构

主要风险点：

a) 未制定符合全行整体发展战略的信息科技发展战略规划，没有考虑利益相关方的要求，系统战略规划与运行管理能力不能适应商业银行发展战略要求；
b) 未建立清晰的信息科技组织治理结构，部门分工不合理、职责不明确，缺少制衡制约，汇报渠道不明确；
c) 董事会职责中未包括审查批准信息科技战略；
d) 董事会未审阅信息科技风险管理年度报告；
e) 未建立来自高级管理层、信息科技部门和主要业务部门的代表组成的专门信息科技管理委员会；
f) 未设立首席信息官。

控制要求：

a) 商业银行在制定信息科技战略计划的过程中，应从业务发展战略出发，充分考虑业务部门内部和外部利益相关者的监管要求，使信息科技战略计划符合业务目标；
b) 商业银行在建立良好的公司治理的基础上进行信息科技治理，形成分工合理、职责明确、相互制衡、报告关系清晰的信息科技治理组织结构；
c) 商业银行董事会应负责审查批准信息科技战略，确保其与银行的总体业务战略和重大策略相一致。评估信息科技及其风险管理工作的总体效果和效率；
d) 商业银行董事会应每年审阅并向银监会及其派出机构报送信息科技风险管理的年度报告；
e) 商业银行应设立一个由来自高级管理层、信息科技部门和主要业务部门的代表组成的专门信息科技管理委员会，负责监督各项职责的落实，定期向董事会和高级管理层汇报信息科技战略规划的执行、信息科技预算和实际支出、信息科技的整体状况；
f) 商业银行应设立首席信息官，直接向行长汇报，并参与决策。首席信息官的职责包括：直接参与本银行与信息科技运用有关的业务发展决策；确保信息科技战略，尤其是信息系统开发战略，符合本银行的总体业务战略和信息科技风险管理策略；负责建立一个切实有效的信息科技部门，承担本银行的信息科技职责；确保信息科技风险管理措施落实到相关的每一个内设机构和分支机构等。

7.2.2 控制环境

主要风险点：

a) 未建立一个切实有效的信息科技部门承担本银行信息科技职责；
b) 未建立科学的信息科技制度、规范、标准和管理流程，未形成规范的信息科技制度体系；
c) 未定期开展人力资源评估，不及时掌握人力资源实际状况，不清楚员工的真实履职能力；
d) 信息科技部门职能和岗位职责定义及描述不够清晰，未明确不相容岗位和信息科技关键岗位，难以实现不相容岗位的职责分离；
e) 未对信息科技部门员工在其入职前进行背景调查；
f) 未针对员工工作岗位变化制定响应机制；
g) 未建立信息科技资产清单和指定相关责任人；
h) 没有对信息科技资产的物理环境进行保护与控制。

控制要求：

a) 商业银行应建立组织结构清晰、部门职能明确的信息科技部门，确保其履行：信息科技预算和支出、信息科技策略、标准和流程、信息科技风险管理和内部控制、专业化研发、信息科技项目发起和管理、信息系统和信息科技基础设施的运行、维护和升级、信息安全管理、灾难恢复计划、信息科技外包和信息系统退出等职责；
b) 商业银行应建立完善的信息科技制度体系，包括管理程序和操作流程，并保证其得以严格执行；
c) 商业银行的信息科技管理层应定期对信息科技人力资源状况进行评估，科学配置人力资源，为信息科技战略目标的实现提供资源保障。评估内容主要包括当前的信息科技人力资源能否满足信息科技发展需要，信息科技人员能否胜任当前的工作岗位等；
d) 商业银行的信息科技部门应明确关键岗位，并在岗位设计上实现了职责分离。此外，定期或不定期的对职责划分的合理性进行评价，以符合组织发展变化的要求；
e) 商业银行应在信息科技部门员工入职前进行人员背景调查（内容主要包括：核验有效身份证件、学历证明、工作经历和专业资格证书等信息）；
f) 商业银行应建立相应的人员调动、离职机制，确保员工调动到新的工作岗位或离开商业银行时，及时变更相关信息,系统及时检查、更新或注销用户身份；评估关键岗位信息科技员工流失带来的风险，做好安排候补员工和岗位接替计划等防范措施；
g) 商业银行应对所有关键信息科技资产（固定资产、重要系统、软件产品和数据）编制清单，并为其指定所有者。资产的所有者必须对其负责的资产承担维护以及安全保护的责任；
h) 商业银行应建立信息系统物理安全管理制度，保证重要资源安全。

7.2.3 信息与沟通

主要风险点：

a) 未持续关注外部监管和审计的要求，并配合外部检查；
b) 商业银行未及时披露信息科技风险状况；
c) 针对员工缺乏职业道德和行为规范的教育；
d) 未使员工了解、遵守信息科技策略、信息保密、信息科技风险管理制度和流程等要求。

控制要求:

a) 商业银行应持续关注与信息科技管理相关的法律、规章等外部监管要求，及时采取相应的措施；配合外部监管和审计对本行的检查，并将检查结果及时报告董事会、高管层和内部审计等相关部门；
b) 商业银行应依据有关法律法规的要求，规范和及时披露信息科技风险状况；
c) 商业银行应定期对员工开展有关职业道德和行为规范、内部控制和安全管理意识方面的培训；

d) 商业银行应建立信息传导与沟通机制，确保员工（包括正式员工、临时员工和其它相关外来人员）及时了解经董事会批准的信息科技发展战略。通过同员工签订相关协议、借助信息化手段等宣传方式，帮助员工理解并遵守信息科技管理制度和流程等。

7.2.4 监督与评价

主要风险点：

a) 董事会和高管层对信息科技管理缺少适当的监督；
b) 商业银行未建立信息科技风险管理三道防线；
c) 作为第一道防线的信息科技部门没有对信息科技日常运营管理开展持续的检查，未对外部监管和内部检查发现的问题进行跟进且未及时采取相应的措施；
d) 作为第二道防线的内控合规、风险管理部门未监控与评估信息科技部门为业务部门提供服务的效果，未对信息科技部门合规运营、风险管理效果进行监督评价；
e) 商业银行未在作为第三道防线的内部审计部门设立专门的信息科技风险审计岗位；
f) 商业银行内部审计部门未对信息科技风险开展有效的监督与评价。

控制要求：

a) 商业银行的董事会和高管层对于信息科技战略计划的执行情况进行监督，并使其满足业务发展需要，促进信息科技战略目标的实现；
b) 商业银行应建立由信息科技部门、内控和风险管理部门、内部审计部门组成的信息科技风险管理三道防线机制，并在该机制下各相关部门分别承担对信息科技风险的日常管理、内控监督以及审计评价；
c) 商业银行的信息科技部门应基于其自身开展的风险评估结果，制定信息科技管理检查计划；开展的信息科技检查能够发现问题和潜在风险，并将检查结果及时报告董事会、高管层和内部审计部门等有关方；对检查发现的问题及时跟进，及时制定整改措施，并及时将整改结果报告董事会、高管层和内部审计部门等相关方；
d) 商业银行应设定或指派内控或风险管理部门承担信息科技风险管理职责，为业务部门和信息科技部门提供合规建议，监控信息安全威胁和不合规事件的发生，监控信息科技部、各中心、各分行为业务部门提供的服务，并将检查结果及时报告高管层，并抄送内部审计部门；
e) 商业银行内部审计部门应配备足够的资源和具有专业能力的信息科技审计人员，负责信息科技审计制度和流程的实施，制定、实施和调整信息科技审计计划，检查和评估信息科技系统和内控机制的充分性和有效性，对信息科技整个生命周期和重大事件等进行审计；
f) 商业银行内部审计部门根据业务性质、规模和复杂程度，信息科技应用情况，以及信息科技风险评估结果，决定信息科技内部审计范围和频率，但至少每三年实现审计范围的全面覆盖。

7.3 信息科技风险管理

7.3.1 风险管理策略

主要风险点：

a) 未制定全面的信息科技风险管理策略；
b) 未依据信息科技风险管理策略实施全面的风险防范措施；
c) 中资商业银行在境外设立的机构未遵守境内外监管要求。

控制要求：

a) 商业银行应建立全面的信息科技风险管理策略，针对信息分级与保护、信息系统开发、测试、运行和维护，以及访问控制、物理安全、人员安全、业务连续性计划与应急处置建立风险识别与评估流程；
b) 商业银行应依据信息科技风险管理策略，制定明确的信息科技风险管理制度、技术标准和操作规程等，定期进行更新和公示；
c) 商业银行在境外设立的机构及境内的外资商业银行，应当遵守境内外监管机构关于信息科技风险管理的要求，并防范由于监管差异所造成的风险。

7.3.2 风险识别和评估

主要风险点：
a) 未制定持续的风险识别和评估流程，无法确定信息科技中存在隐患的区域；
b) 未依据信息科技风险评估结果确定应该关注的主要风险。

控制要求：
a) 商业银行应制定持续的风险识别和评估流程，确定信息科技中存在隐患的区域，评价风险对其业务的潜在影响，对风险进行排序，并确定风险防范措施及所需资源的优先级别（包括外包供应商、产品供应商和服务商）；
b) 商业银行应依据信息科技风险评估结果，确定应该关注的主要风险，并对这些风险进行详细和独立的监控，实现风险最小化。

7.3.3 风险监测和应对

主要风险点：
a) 未建立持续的信息科技风险计量和监测机制；
b) 风险评估没有清晰的管理流程和报告路线。

控制要求：
a) 商业银行应建立持续的信息科技风险计量和监测机制。包括：建立信息科技项目实施前及实施后的评价机制；建立定期检查系统性能的程序和标准；建立信息科技服务投诉和事故处理的报告机制；建立内部审计、外部审计和监管发现问题的整改处理机制；安排供应商和业务部门对服务水平协议的完成情况进行定期审查；定期评估新技术发展可能造成的影响和已使用软件面临的新威胁；定期进行运行环境下操作风险和管理控制的检查；定期进行信息科技外包项目的风险状况评价；
b) 商业银行应根据实际情况明确制定风险评估管理流程的负责部门，并制定风险评估管理流程和风险评估报告制定路线。

7.4 信息安全

7.4.1 总体管理

主要风险点：
a) 缺乏完善的信息安全管理制度；
b) 未落实信息安全管理职能和组织架构；
c) 员工缺乏必要的信息安全培训；
d) 未建立用户管理机制和访问控制流程；
e) 未建立生产系统活动日志管理策略和流程。

控制要求：

a) 商业银行应负责建立和实施信息分类和保护体系，并负责建立信息安全管理机制，包括信息安全标准、策略、实施计划和持续维护计划，并定期更新。商业银行应建立全行统一的信息分类标准，应对各类信息都有合理的安全级别及控制措施，定期对安全级别进行评估和相应的修改，并应建立对重要数据和信息的使用、审批制度。商业银行应建立详细完整的信息安全管理制度，经管理层审批后发布，并应定期对信息安全管理制度进行复核，如果环境发生了变化，必须做出相应的修订；
b) 商业银行应建立信息安全管理组织框架，落实管理职能，以启动和控制信息安全的实施，并在部门和岗位职责分工中定义并分配信息安全的关键职责；
c) 商业银行应使所有员工都了解信息安全的重要性，并组织提供必要的培训，让员工充分了解其职责范围内的信息科技安全管理制度和信息保护流程,提高全体员工的信息安全意识,以达到信息安全控制的要求；
d) 商业银行应建立有效的用户认证管理机制和访问控制的流程，建立完整的用户管理流程，包括各类应用系统、安全系统、网络系统、数据库和操作系统的用户的开立、变更和销户。同时应明确定义终端用户和信息科技技术人员在各信息系统安全中的角色和职责。对用户权限的授予应遵循岗位职责分离和知所必须的最小授权原则；
e) 商业银行应制定相关策略和流程，管理所有生产系统的活动日志，以支持有效的审核、安全取证分析和预防欺诈。活动日志应包括交易日志和系统日志，其中交易日志由应用软件和数据库管理系统产生，内容包括用户关键交易、登录尝试、数据修改、错误信息等，交易日志应按照国家会计准则要求予以保存，但不得少于三年；系统日志由操作系统、数据库管理系统、防火墙、入侵检测系统和路由器等生成，内容包括管理登录尝试、系统事件、网络事件、错误信息等，系统日志保存期限按系统的风险等级确定，日志保存期限不能少于一年。

7.4.2 物理访问控制管理

主要风险点：

a) 物理安全管理制度不完善；
b) 未能有效实施对重要信息科技设备的保护；
c) 重要信息安全区域的出入访问控制措施不完善；
d) 重要信息安全区域和关键位置缺乏视频监控和录像设施。

控制要求：

a) 商业银行应建立完善的信息系统物理安全管理制度，保证重要资源安全；
b) 商业银行应确保设立物理安全保护区域，包括计算机中心或数据中心、存储机密信息或放置网络设备等重要信息科技设备的区域，明确相应的职责，采取必要的预防、检测和恢复控制措施。应根据职能和安全等级不同划分不同安全区域，并且根据员工工作岗位和职责不同开放相应区域，对安全区域进行保护；
c) 商业银行应制定人员登记管理制度和流程，对需要访问重要信息科技设备环境（如机房）的人员进行审批和详细记录，确保只有经授权人员才能访问。商业银行应使用电子门禁系统对不同安全区域人员出入进行管理，制定相关门禁系统管理办法。对于外来人员（如第三方技术支持人员或服务商等），特别是从事敏感性技术相关工作的人员，应制定更为严格的审查程序，包括身份验证和背景调查；
d) 商业银行应该对重要安全区域（如核心机房及其出入口）进行不间断的视频监控和录像，出入口应配备保卫人员，并安装警报系统保证保卫人员及时到达现场。

7.4.3 网络安全管理

主要风险点：

a) 网络的安全管理和规划设计缺乏制度性安排；
b) 对网络结构和配置的变更没有完善的控制措施；
c) 缺乏对网络的监控；
d) 网络隔离和访问控制手段不足；。
e) 未对网络设备进行安全参数配置；
f) 未对网络设备划分等级实施保护。

控制要求：

a) 商业银行应制定网络安全管理制度，将内部网络划分为相对独立的安全域，制定和维护相关访问控制和边界控制策略。网络设计须从服务商的选择、网络设备和网络链路的规划等多方面充分考虑到业务连续性要求；
b) 商业银行应对网络结构和配置的变更进行管理，建立相应的管理制度和变更流程，对变更情况进行记录；
c) 商业银行应对内部网络进行实时监控和网络设备日志定期检查，并应建立自动报警机制和紧急事件响应流程，保证及时发现异常事件和安全隐患；
d) 商业银行的生产环境网络和办公网络应逻辑或物理隔离。对于生产网的接入应有相应的管理办法和控制措施；对远程访问应进行严格控制，并建立相应的管理制度，控制远程访问的方式与范围，远程访问应该经过授权和审批；对远程访问活动应该进行记录，以便进行跟踪查询，并且对记录进行定期的检查；防火墙、入侵检测机制应合理布局，配置遵循安全原则，定期进行漏洞扫描及时发现并处理安全漏洞；应对网络设备特权用户进行管理；
e) 商业银行应根据业界标准对网络设备配置安全参数；
f) 商业银行应按照人民银行《金融行业信息系统信息安全等级保护实施指引 JR/T 0071-2012》标准对网络设备实施等级保护。

7.4.4 操作系统及数据库安全管理

主要风险点：

a) 未针对各类操作系统和数据库制定最低安全管理基线；
b) 操作系统和数据库用户权限配置不合理；
c) 未对高权限用户的操作进行管理；
d) 未对关键的高风险操作系统漏洞及时修复；
e) 缺少对操作系统权限变更的有效控制；
f) 未对操作系统和数据库活动日志进行定期的检查；
g) 没有安装防病毒软件，或未及时更新、分发病毒库，未定期开展病毒扫描。

控制要求：

a) 商业银行应制定每种类型操作系统和数据库系统的基本安全管理基线，确保所有系统满足基本安全要求；
b) 商业银行应明确定义包括终端用户、系统开发人员、系统测试人员、计算机操作人员、系统管理员和用户管理员等不同用户组的访问权限。对用户的授权应符合岗位职责分离和最小授权原则，应定期检查操作系统和数据库的用户权限，如发现与用户岗位职责不符的情况，及时进行调整；
c) 商业银行应制定最高权限系统账户的审批、验证和监控流程，并确保最高权限用户的操作日志被记录和监察；

d) 商业银行应要求技术人员定期检查操作系统可用的安全补丁，并报告补丁管理状态，及时修复关键的高风险漏洞；
e) 商业银行应当建立操作系统访问权限的批准程序，操作系统中所有用户账号以及权限的变更需经过正确的授权；
f) 商业银行应在操作系统和数据库的交易日志和活动日志进行定期的检查，审阅系统出现的任何异常事件，定期汇报监控情况；
g) 商业银行应在操作系统上安装防病毒软件，并确保防病毒软件均更新到最新病毒码。商业银行应部署扫描软件，及时发现未安装授权防病毒的计算机，应定期生成防病毒报告，提交给相应负责人。

7.4.5 数据安全管理

主要风险点：
a) 缺乏对数据的分类标准、安全级别定义和安全控制措施；
b) 未制定对客户信息的保护制度和流程；
c) 存储介质的访问控制措施不完善；
d) 未能对重要文档进行安全管理；
e) 未使用适当的加密技术对涉密信息进行加密；
f) 缺乏完善的密钥管理制度流程；
g) 密钥管理不符合制度要求。

控制要求：
a) 商业银行应根据安全及保密政策对信息资产进行分类，并采取相应的安全处理措施；
b) 商业银行应制定相关制度和流程，严格规范客户关键和敏感信息的采集、处理、存贮、传输、分发、备份、恢复、清理和销毁等环节的管理；
c) 商业银行应建立存储介质的存放、借用、运输交接和销毁等管理规定，包含敏感信息的存储介质应该有专责部门或人员负责保管，调阅、复制这些存储介质等操作应该得到适当的授权；
d) 商业银行应对包含有商业秘密、敏感信息、信息资产等重要数据文档的存放和使用进行管理，从而保证重要文档的安全；
e) 商业银行应使用符合国家要求的加密技术和加密设备，防范涉密信息在传输、处理、存储过程中出现泄露或被篡改的风险。应对管理、使用密码设备的员工进行严格审查和专业培训。应确保加密强度满足信息机密性的要求。应建立密码设备管理制度，制定并落实有效的管理流程，尤其是密钥和证书生命周期管理；
f) 商业银行应建立完善的密钥管理制度流程，以支持组织使用密码技术；
g) 商业银行应根据密钥管理制度，对密钥的产生、变更、撤销、销毁、分发、认证、存储、登记、使用和归档流程进行适当稳妥的管控，以免密钥遭到修改或泄露。

7.4.6 应用系统访问控制管理

主要风险点：
a) 用户对数据和系统的访问权限设置不正确；
b) 未对应用系统中用户的访问权限定期进行审核；
c) 未对系统的输入输出进行安全控制；
d) 未对交易操作日志进行妥善保存和定期审阅。

控制要求：

a) 商业银行应建立有效的用户认证管理和访问控制的流程。用户对数据和系统的访问必须选择与信息访问级别相匹配的认证机制，并且对用户的授权应符合岗位职责分离和最小授权原则，对关键或敏感岗位进行双重控制。用户调动到新的工作岗位或离开商业银行时，应在系统中及时检查、更新或注销用户身份。明确定义终端用户和信息科技技术人员在信息系统安全中的角色和职责；
b) 商业银行应保留应用系统管理员和其他超级用户的系统日志，指定专人定期对系统用户权限和日志进行审核，监控和审查未成功的登录和用户账户的修改；
c) 商业银行在关键的接合点进行输入验证或输出核对，采取安全的方式处理保密信息的输入和输出，防止信息泄露或被盗取、篡改。系统按预先定义的方式处理例外情况，确保系统被迫终止时，能够向用户提供必要信息；
d) 商业银行应对应用软件和数据库管理系统产生的交易日志按照国家会计准则要求予以保存并定期审阅，但不得少于三年。

7.4.7 终端设备安全管理

主要风险点：商业银行对重要终端设备缺少安全保护措施。

控制要求：商业银行应配备切实有效的系统，确保所有终端用户设备（如：台式个人计算机（PC）、便携式计算机、柜员终端、自动柜员机（ATM）、存折打印机、读卡器、销售终端（POS）和个人数字助理（PDA）等）的安全，并定期对终端设备进行安全检查，及时发现控制漏洞并进行整改。

7.5 信息系统开发、测试和投产

7.5.1 总体管理

主要风险点：

a) 未建立信息系统开发、测试和维护管理制度，相关流程缺乏规范；
b) 未采取适当的系统开发方法，有效管理信息科技项目生命周期；
c) 对信息科技项目相关风险缺少认识和管理；
d) 未针对不同的技术平台、技术架构、信息系统建立适用的技术规范；
e) 缺乏对项目全过程的质量控制；
f) 未能按计划完成项目各关键时间节点的进度任务；
g) 缺乏对信息系统相关文档的编写质量控制和统一管理。

控制要求：

a) 商业银行应制定相关制度，规范信息系统需求分析、规划、采购、开发、测试、部署、维护、升级和报废等流程，管理信息科技项目的优先排序、立项、审批和控制；
b) 商业银行应结合自身实际情况，根据信息科技项目的规模、性质和复杂度，采取适当的系统开发方法，管理信息科技项目的生命周期。项目生命周期包括可行性研究、需求定义、系统分析、设计、开发或外购、测试、试运行、部署和维护；
c) 商业银行应在信息科技项目管理各环节中，及时识别并跟踪信息科技项目相关的风险（包括潜在的各种操作风险、财务损失风险和因无效项目规划或不适当的项目管理控制产生的机会成本），并报告利益相关方，及时采取适当的项目管理方法，控制信息科技项目相关的风险；
d) 商业银行应制定并印发正式的技术规范，对不同平台下的数据库、存储、中间件、操作系统、性能容量、灾备和自动化等方面，以及信息系统的架构设计、参数设计、日志设计、风险防范设计等方面做出具体规定，确保信息系统的正常运行以及数据的完整性、保密性和可用性；

e) 商业银行应建立项目质量控制机制，监督项目全过程质量，对发现的问题（含不符合项）进行跟踪处理，确保项目符合开发规范，并对项目过程的实际执行情况进行客观评价；
f) 商业银行应按照各任务时间节点的要求，按时完成各节点工作任务。应确保对项目进度的监督，及时沟通项目进程中遇到的问题，对项目进度进行有效的控制，以避免影响项目目标的实现；
g) 商业银行应参照 GB8567-88 等相关国家标准和行业标准，提高项目开发计划、软件需求说明书、系统设计说明书等系统开发相关文档的编写质量，并应建立相应的文档管理制度，集中存放和保管信息系统相关文档。

7.5.2 立项管理

主要风险点：
a) 未对项目进行全面的可行性分析和审核流程；
b) 未建立项目计划或计划不完整。
控制要求：
a) 商业银行应对项目进行技术、经济和社会方面的可行性分析，并出具可行性分析报告，确定项目立项的可行性，保证资源的合理使用，避免浪费。应制定立项审批流程，由管理层、技术和业务人员共同对项目的成本、安全、风险、技术可行性、投入产出比等方面进行审核，审核通过后方可进入研发流程；
b) 商业银行应根据信息系统开发项目的重要性、紧急程度、规模等要素，建立信息科技项目实施的优先级原则，并据此确定项目的先后次序。并应依据项目的规模和重要程度，选择适当的项目计划的审批流程。在项目实施之前，需制定实施计划，以应明确各阶段（如需求定义、系统分析、设计、开发或外购、测试、试运行、部署等）的主要任务、执行顺序与优先级，任务工期、成本和预算，所需资源、人员分工与职责等内容。

7.5.3 需求管理

主要风险点：
a) 业务需求、范围界定和目标不明确；
b) 未能正确进行对业务需求的分析；
c) 开发人员对需求的分析结果没有经过业务部门的确认；
d) 未建立完善的需求变更流程；
e) 未建立对项目规模进行评估；
f) 项目工作组成员缺乏相关业务知识和技术经验。
控制要求：
a) 商业银行应由需求部门提出具体的业务需求，明确描述业务目标与范围，详细列出业务对系统的要求，包括功能和风险控制要求；
b) 商业银行应组织需求提出相关业务人员和科技人员共同对业务需求进行分析，将用户需求转化为系统需求，确定系统效率、效果、保密性、完整性、可用性、符合性和可靠性等非功能性需求，同时确定需求实现方式是采用自行开发或者购买现成的商品化软件；
c) 商业银行应确保最终交付开发人员的需求分析结果经过业务人员和开发人员的共同确认，并经过业务主管人员的审核，以避免项目后期再调整需求造成的成本增加和资源浪费，同时避免开发人员对业务需求的理解产生偏差，影响系统开发的效用；
d) 商业银行应建立完善的需求变更流程。应由需求牵头部门发起需求变更，向项目承担部门提供详细的需求变更材料。项目承担部门应组织相关人员对需求变更进行分析评估，对项目规

模的变化、工作量、项目进度、项目质量等方面的影响进行评估，并将变更评估意见反馈需求牵头部门；

e) 商业银行应针对大型或关键信息科技项目的规模建立评估和计量方法，用以确定项目资源、成本与预算；

f) 商业银行应针对项目指定项目经理和相关专业经理，并建立项目工作组。项目工作组由业务人员、技术人员和管理人员组成，具体负责整个项目的开发工作。项目工作组人员应具备与项目要求相适应的业务经验与专业技术知识,小组负责人需具备组织领导能力,保证信息系统研发质量和进度。

7.5.4 系统设计

主要风险点：

a) 未确定系统关键内容和评审流程；

b) 系统性能安全分析、环境需求分析不详尽。

控制要求:

a) 商业银行应确定系统总体架构设计、技术实现手段、系统与其他外部系统的接口定义及逻辑关系、系统内部的关键数据结构、界面及模块流程、系统错误处理和资源要求等内容，并对这些重要内容进行正式评审，评审必须有产品使用部门的有关人员参与；

b) 商业银行应由项目承担部门根据项目实际需要组织编制针对系统性能安全和环境需求等方面内容的分析文档，并组织召开项目运行部门参加的评审会。项目运行部门应分析研究上述内容对生产系统的影响，并结合生产运行维护要求提出有关建议。

7.5.5 编码及自测

主要风险点：

a) 缺乏规范的编程方法和编码规范；

b) 未及时制定代码检查计划或代码检查方式；

c) 缺乏项目版本管理。

控制要求:

a) 商业银行应确立统一的编码方法和代码规范，从而确保编码的质量和一致性，以便于独立审核和软件维护；

b) 商业银行应按项目计划要求及时制定代码检查计划，同时根据每个程序特点确定不同的检查点。项目组根据项目自身特点，编制合适的代码检查表，检查点的内容必须详细、准确。编码完成后，开发人员和负责代码检查人员应进行程序代码检查，登记代码检查表，跟踪问题的解决；

c) 商业银行应建立项目版本控制管理制度。应对项目配备版本管理人员，在进行程序开发时，确保每次在最新的代码基础上进行更改；当多名程序员同时进行更改工作时，能够做好相互协调；在交付版本制作过程中，版本管理员应对程序包内容与版本说明书中的程序内容进行检查比对，确保程序包内容与版本说明书程序内容一致。

7.5.6 项目测试

主要风险点：

a) 测试人员未经过项目测试相关内容的培训；

b) 业务相关部门人员未参与测试；

c) 测试方案、测试计划等文档缺失；

d) 测试与业务需求不一致或测试内容不完整；
e) 未能有效按测试计划实施测试方案。
f) 测试结束未见测试验收报告。

控制要求：

a) 商业银行应针对项目组织测试培训，确保测试人员能很好地掌握版本的基本要求，以保障测试质量和测试进度；
b) 商业银行应组织需求提出部门和相关业务人员参与版本测试及验收；
c) 商业银行应编制测试方案、测试计划等文档。应按照项目计划的要求确定测试目标、测试范围、测试软硬件配置、测试规模分析等内容，具体文档包括《测试计划》、《测试方案》和《测试案例》等；
d) 测试内容应依据业务需求进行，具体应包括用户功能、业务流程、安装测试、备份恢复等方面的测试。测试内容应该尽量全面和完整，还须包括性能容量、系统兼容性、业务特殊时间点（计利和年终结算）等，如有非功能性需求也必须包含在内；
e) 商业银行应根据测试计划组织实施验收测试及适应性测试工作并全面监控测试质量，控制测试整体进度。应根据测试发现问题轻重缓急程度进行分类，实施相应的分级报告和处理；
f) 商业银行在适应性测试完毕及验收后，编写《验收测试报告》或《投产确认书》，并经业务主管部门审批。

7.5.7 投产与推广

主要风险点：

a) 缺乏有效的投产问题管理制度流程；
b) 对应用系统的投产没有进行风险评估；
c) 未制定完善的应用系统投产流程；
d) 系统推广缺乏完整可行的推广计划。

控制要求：

a) 商业银行应建立并完善有效的投产问题管理流程，以确保全面地追踪、分析和解决信息系统问题，并对问题进行记录、分类和索引；如需供应商提供支持服务或技术援助，应向相关人员提供所需的合同和相关信息，并将过程记录在案；对完成紧急恢复起至关重要作用的任务和指令集，应有清晰的描述和说明，并通知相关人员；
b) 商业银行应充分识别、分析、评估重要应用系统投产风险，包括系统功能缺陷、客户信息泄露、业务中断、交易缓慢或其他因素可能造成的操作风险、法律风险和声誉风险，并形成风险评估报告；
c) 商业银行应用系统的投产计划需经管理部门正式批准。系统投产前应进行充分的测试并验收，对版本进行控制，保证只有经过测试验收的版本才能用于投产。重要应用系统投产前测试结果应经过信息科技部门和相关业务部门确认，形成测试验收报告，确保系统上线后的正常稳定运行以及系统功能与业务目标的一致性。在确认测试完成后，正式批准并发布投产通知，投产交付资料必须齐全详细，如测试报告、投产方案、版本说明书和正式印发的系统投产通知（如有数据移行，应包含数据移行测试结果）。投产前完成对运行操作人员、技术支持人员、业务人员的相关培训。重要应用系统投产过程中，严格执行投产方案，加强监督与复核，避免操作失误和非法操作。所有的利益相关方能及时了解应用系统的整个投产过程，与投产相关的文档资料应由具体人员负责完整保存；

d) 商业银行应当制定信息系统推广计划，并经归口管理部门和用户部门审核批准。推广计划一般包括人员培训、数据准备、进度安排、应急预案等内容。系统上线涉及新旧系统切换的，银行应当在推广计划中明确应急预案，保证新系统失效时能够顺利切换回旧系统。

7.5.8 项目后评价

主要风险点：

a) 缺乏对版本质量的后评价；

b) 项目后评价没有相关业务人员的参与。

控制要求：

a) 商业银行在应用类版本投产后，应对版本质量情况进行总结评价，以便于持续跟踪和改进版本质量；

b) 商业银行应确保有业务人员参与项目后评价工作，以及时发现交付的新系统在运行中暴露的新问题或与需求之间的偏差，从而确保系统的实际使用效率和效果。

7.6 信息科技运行管理

7.6.1 总体管理

主要风险点：

a) 未设置清晰的运行岗位；

b) 未制定详尽的运行操作手册；

c) 运行人员缺乏操作技能；

d) 运行与开发和维护职责未有效分离；

e) 未严格控制外来人员进入生产区域；

f) 未对应用系统进行日常维护和升级；

g) 对硬件设备缺少定期巡检。

控制要求：

a) 商业银行应制定信息科技运行管理办法，设置运行管理部门及相关岗位，各岗位人员应明确岗位职责和相应的规章制度。如设置操作管理部门、作业调度部门、操作实施部门和技术支持部门等，部门职责应清晰明确；

b) 商业银行应制定详尽的信息科技运行操作手册。如在运行操作手册中说明运行人员的任务、工作日程、执行步骤，以及生产与开发环境中数据、软件的现场及非现场备份流程和要求（即备份的频率、范围和保留周期）。当业务运行发生变化时，运行操作手册做出相应调整，变化的部分及时通知运行人员；

c) 商业银行应对运行人员进行上岗培训和考试，并定期对运行人员进行考核；

d) 商业银行应将信息科技运行与系统开发和维护分离，确保信息科技部门内部的岗位制约，特别是对数据中心的岗位和职责应做出明确规定；

e) 商业银行应严格控制外来人员进入生产安全区域，如确需进入应得到适当的批准，其活动也应受到监控；针对长期或临时聘用的技术人员和承包商，尤其是从事敏感性技术相关工作的人员，应制定严格的审查程序，包括身份验证和背景调查；

f) 商业银行应制定相关制度和流程，及时对应用系统进行维护和适当的升级，控制系统升级过程，以确保与技术相关业务的连续可用性，并完整保存记录，包括疑似和实际的故障、预防性和补救性维护记录；

g) 商业银行应对硬件设备，包括计算机设备、网络设备、动力设备等进行定期巡检。根据生产系统的服务水平目标制定硬件维护计划、编制维护手册，对生产信息系统进行健康检查，根据检查结果提出改进措施和建议。为防备有突发的硬件容量性能需求，应建立相关的储备和应急响应机制。

7.6.2 机房环境及设施管理

主要风险点：

a) 选择数据中心物理位置时未充分考虑环境威胁；
b) 生产机房缺乏必要的环境控制和预防性维护；
c) 生产机房无持续稳定的电源供应；
d) 生产机房没有安全撤离计划和疏散通道。

控制要求：

a) 商业银行在选择数据中心的地理位置时应充分考虑环境威胁，如是否接近自然灾害多发区、危险或有害设施、繁忙或主要公路等，采取物理控制措施监控对信息系统运行构成威胁的环境状况；
b) 商业银行应制定信息系统环境控制和预防性维护应对方案，包括：物理环境适宜度控制（温度、灰尘、湿度等）、计算机连线、消防、防渗水、内部和服务商日常预防性维护的管理等。机房应配备防火、防水、防磁等设施，并由专人对机房环境设备进行监控；
c) 商业银行必须对生产机房设备提供持续且稳定的电源供应。重要生产机房应配备双路电源、发电机、电压稳定器和不间断电源（UPS），不间断电源（UPS）应在全负载情况下至少保证30 分钟以上的持续供电，并由专人对电源装置进行定期检查；
d) 商业银行应制定生产机房人员安全手册，生产机房有专门的疏散通道和疏散线路图，指导机房人员在发生灾难时疏散，并定期进行演练。

7.6.3 批处理管理

主要风险点：

a) 没有建立批量数据处理机制；
b) 没有根据业务变动情况及时调整批处理计划；
c) 运行人员没有按照要求严格执行批处理操作。

控制要求：

a) 商业银行应按照有关法律法规要求保存交易记录，制定批量数据处理机制，采取必要的程序和技术，确保数据处理的完整性、及时性，满足安全保存和恢复要求。对于新投产应用系统的批量数据迁移，应根据新系统的设置及迁移要求，制定详细的批量数据迁移计划，包括移行准备、移行处理、移行后的工作事项、工作内容、负责部门和起止时间。数据迁移后，对数据的完整性、一致性进行检查，由业务部门确认验收，数据迁移的相关工作记录由专人保管；
b) 商业银行应根据业务变动情况及时更新批处理作业计划，确保批处理作业计划与业务需求相符，每次作业计划和编排的调整以正式变更方式执行；
c) 商业银行应要求运行人员必须按照规定进行操作，规范批处理作业的建立和维护细则，对各个系统的批处理作业操作做出规定。管理层对批处理作业的新增、修改以及批处理作业计划的编排等操作进行审批授权。运行操作人员应了解各类业务的交接情况，及时查看通知、邮件，按规定处理各类业务。在批处理开始前，对批处理数据进行检查，停止所有相关进程和

交易，对数据进行保护。保留批处理日志，对批处理日志进行检查，对发现的问题及时跟踪和处理。

7.6.4 服务管理

主要风险点：

a) 未建立服务水平管理程序；
b) 没有建立连续监控的信息系统；
c) 未建立事故处置响应机制。

控制要求：

a) 在科技部门和业务部门之间定义正式的服务水平管理程序。科技部门根据服务实施情况，以及定量和定性评价结果，定期进行服务质量评估，编写服务水平执行情况报告和运营水平执行情况报告。业务部门定期对科技部门的服务质量进行评价。上级管理部门定期对服务水平和运营水平执行情况进行考核；
b) 商业银行应建立连续监控信息系统性能的相关程序，及时、完整地报告例外情况；程序应提供预警功能，在例外情况对系统性能造成影响前对其进行识别和修正；
c) 商业银行应建立事故管理及处置机制，及时响应信息系统运行事故，逐级向相关的信息科技管理人员报告事故的发生，并进行记录、分析和跟踪，直到完成彻底的处置和根本原因分析。商业银行应建立服务帮助平台，提供相关技术问题的在线支持，并将问题提交给相关信息科技部门进行调查和解决。

7.6.5 性能容量管理

主要风险点：

a) 没有针对重要设备定义关键可用性指标；
b) 未对性能容量进行规划、评估和审批；
c) 对信息系统性能容量缺乏全面监控；
d) 未对信息系统监控指标进行有效分析。

控制要求：

a) 商业银行应对重要设备，如应用系统服务器、网络、动力、空调等设备制定可用性（性能、容量）管理办法，定义可用性指标，包括单项可用性指标和综合可用性指标；
b) 商业银行应制定信息系统容量规划，以适应由于外部环境变化产生的业务发展和交易量增长。容量规划应涵盖生产和备份系统的相关设备，评价目前系统、网络的性能容量及负载能力，以此为依据对后续扩容进行评估，并提交管理部门审批；
c) 商业银行应制定对性能容量监控的管理手册和技术文档。运行操作人员应按照要求监控信息系统的性能容量指标，记录相关数据，包括：对系统响应时间和处理量、系统承载能力、任务处理失败的次数、比例、类型和原因、系统使用的峰值和均值、系统使用趋向和容量等；
d) 商业银行应定期对信息系统的可用性和性能容量进行分析，对照可用性及性能容量的实施计划，找出实际指标与标准指标之间的差距查明原因，结合业务发展趋势，制定改进计划提交相关管理部门。

7.6.6 配置管理

主要风险点：

a) 未建立和维护配置信息库；
b) 没有识别和收集配置信息；

c) 未对已录入的配置信息进行控制和维护；
d) 没有对已录入的配置信息进行验证和检查。

控制要求：

a) 商业银行应建立包含配置项中相关信息的配置库，监控和记录所有配置项的变更，保留系统和服务的配置项基线作为变动后返回的检查点；
b) 商业银行应收集和验证纳入配置管理的配置信息，为配置信息放入配置管理数据库做好准备，保证即将被纳入配置管理数据库的数据与现实的配置保持一致；
c) 商业银行应录入配置项信息，并确保配置项得到有效控制和及时维护；
d) 商业银行应周期性地验证与检查，保证配置项记录数据的准确性。

7.6.7 事件、问题和变更管理

主要风险点：

a) 没有对事件有效识别和分类；
b) 没有对问题及时处理；
c) 未制定严格的变更管理流程；
d) 未对紧急变更进行严格控制。

控制要求：

a) 商业银行应对信息系统运行中发生的事件按影响程度、影响范围、影响时段和涉及系统类别、紧急程度进行分级。建立规范的事件处理流程（报告、受理、处理、反馈）和系统帮助平台，及时通知利益相关部门。根据事件管理的内容制定全面衡量管理水平的指标体系，对数据采集、指标计算和对各项指标进行评价，并根据指标发展趋势，制定事件管理的改进计划；
b) 商业银行应加强信息系统的问题管理，规范问题处理流程，深入分析各类问题发生的根本原因，落实防范和解决措施。定期组织相关部门对生产系统进行健康检查，主动发现问题及时解决并提交问题分析报告；
c) 商业银行应制定严格的变更管理流程，设置相应的职能部门，各变更职能部门和岗位人员应清楚各自职责，对变更进行管理和控制。变更申请须经主管部门审批，审批要素包括变更实施计划、风险评估、验证、应急和回退方案，对业务有可能造成影响的变更，在变更实施前通知相关业务部门。对于一般变更、重大变更、紧急变更、特殊时期变更等有对应的处理流程。所有变更应统一管理，变更的申请、受理、方案、审批等要素填写必须符合要求。所有变更都应记录日志，并事先进行备份。严格监控整个变更实施过程，根据计划的执行时间、环境、顺序、条件等要求并保证双人操作。变更实施完成后，根据变更验证方案对变更的准确性、完整性和授权性情况进行验证，对例外情况进行记录和跟踪，将变更实施结果及时反馈；
d) 建立、定义、升级、评估和授权紧急变更的流程，应尽量减少紧急变更，通过正常的验收测试和变更管理流程，采用恰当的修正以取代紧急变更。

7.7 业务连续性管理

7.7.1 备份管理

主要风险点：

a) 没有制定完善的备份管理策略；
b) 未对备份数据进行恢复测试。

控制要求：

a) 商业银行应根据本行应用系统的重要性，建立规范、完善的备份管理政策，建立合理的数据和程序备份流程、备份保存周期和备份介质存储、借用、运输交接和销毁等管理规定，对备份介质进行本地和异地保存，对备份介质实施严格的访问控制。在紧急情况发生时，备份数据和程序有良好的权限访问控制，由专责部门或人员负责业务持续性规划中涉及的各类文档和资料；
b) 商业银行应对系统程序和数据的备份情况进行定期检查，对备份介质定期进行恢复测试，对恢复测试中出现的问题，记录并及时解决。

7.7.2 业务影响性分析

主要风险点：
a) 在突发事件情况下不能满足应急要求；
b) 缺少业务连续性管理的组织架构；
c) 未对业务进行影响性分析和风险评估。

控制要求：
a) 商业银行应采取负载均衡、系统恢复和双机冷热备等措施降低突发事件下关键业务中断的可能性，并通过应急安排和保险等方式降低事件影响。备份中心及辅助设施的建设、配置、组织机构和操作机制应满足突发事件下关键业务持续运行的容量和运行能力需求。定期对备份中心进行检测、维护和更新，使其性能容量与实际生产环境保持一致，确保突发事件下备份中心的可用性；
b) 商业银行应设立关于连续性管理的组织架构，包括内、外部服务提供者的角色、任务、职责，以及制定、测试和执行灾难恢复和应急计划的规定；
c) 商业银行应评估因意外事件导致其业务运行中断的可能性及其影响性，包括评估可能由下述原因导致的破坏：1）内外部资源的故障或缺失，如人员、系统或其他资产；2）信息丢失或受损；3）外部事件，如战争、地震或台风等。商业银行的业务影响性分析和风险评估应覆盖银行所有部门、系统，通过业务影响分析建立分级文档，排定恢复关键数据和系统的优先顺序，合理地确定每项业务职能容许恢复的最长时间和可接受的损失水平。风险评估还应考虑到信息系统、人员、设备、服务提供商等事项风险发生的可能性。业务影响分析和风险评估最终结果应经过高级管理层审批。

7.7.3 业务连续性计划

主要风险点：
a) 没有制定业务连续性计划和应急预案；
b) 未及时更新和发布业务连续计划；
c) 对业务连续性计划没有进行定期的测试和演练。

控制要求：
a) 商业银行应根据自身业务的性质、规模和复杂程度制定适当的业务连续性计划，以确保在出现无法预见的中断时，系统仍能持续运行并提供服务；连续性框架要与银行的业务发展策略保持一致性，连续性计划覆盖的范围应该包括银行关键应用系统和网络，计划应包括关键资源的识别、关键资源可用性的监控和报告、可替代的处理设施以及备份和恢复原则。成立专门的应对突发事件的管理组织架构，制定应急工作计划和有关制度，针对可能出现的情况制定相应的应急操作手册，经过评审后进行归档；
b) 商业银行应定期对业务连续性计划进行更新，保证其有效性，并根据演练情况对应急操作手册进行修订，制定业务连续性计划发布的策略以确保计划能正确和安全地下发给授权的相关

人员。对应急人员进行培训，使其了解突发事件发生时他们的角色和责任以及应该执行的流程；

c) 商业银行应对业务连续性计划进行定期测试和演练，保证紧急情况下业务连续性计划得以正确有效实施。商业银行的业务连续性计划和年度应急演练结果应由信息科技风险管理部门或信息科技管理委员会确认。

7.8 外包服务管理

7.8.1 外包组织架构管理

主要风险点：

a) 未针对外包建立管理组织架构；

b) 没有严格落实信息科技外包管理职责。

控制要求：

a) 商业银行的董事会及高级管理层应当严格落实信息科技外包风险管理的相关职责，制定并审批信息科技外包战略，审议信息科技外包管理流程及制定，督促并监控信息科技外包风险管理效果；

b) 商业银行的董事会及高级管理层应明确信息科技外包管理的主管部门。商业银行的信息科技管理部门或信息科技外包活动执行部门应建立信息科技外包管理执行团队，并配备足够人员。

7.8.2 外包战略风险管理

主要风险点：

a) 未制定信息科技外包战略；

b) 未在信息科技战略中明确不能外包的领域；

c) 对外包服务范围缺乏全面的风险评估；

d) 没有对机构集中度和非驻场外包进行风险管理。

控制要求：

a) 商业银行应基于信息科技战略、外包市场环境、自身风险控制能力和风险偏好制定其信息科技外包战略，包括不能外包的职能、资源能力建设方案、供应商关系管理策略和外包分级管理策略；

b) 商业银行实施重要外包（如数据中心和信息科技基础设施等）应格外谨慎，在准备实施重要外包时应以书面材料正式报告银监会或其派出机构，商业银行不得将信息科技管理责任外包；

c) 商业银行应至少每年开展一次全面的外包风险管理评估，三年内覆盖所有重要的服务提供商。评估内容包括信息科技外包战略执行情况、外包信息安全、机构集中度、服务连续性、服务质量、政策及市场变化对外包服务的影响分析等，并将评估报告提交管理层审批。内部审计部门应每三年对重要外包服务提供商进行一次全面审计；

d) 商业银行应积极采用分散信息科技外包活动、提高自主研发运行能力，降低机构集中度，减少对外包服务提供商的依赖。

7.8.3 外包服务实施管理

主要风险点：

a) 未对外包服务提供商资质进行有效审核；

b) 外包服务合同没有进行严格审查；

c) 没有对外包服务的执行进行监督和评价，未对违规情况进行处理；

d) 在信息安全领域未对外包服务提供商提出明确要求；
e) 没有与外包服务提供商及时签署维护服务协议。

控制要求：

a) 商业银行应充分审查外包服务提供商的财务稳定性和专业经验，对外包服务提供商进行风险评估，考查其设施和能力是否足以承担相应的责任，对外包服务提供商的引入和过程管理按照相关采购文件进行规范操作。关注可能存在的集中度风险，如多家商业银行共用同一外包服务提供商带来的潜在业务连续性风险。评估外包服务提供商提供的业务连续性保障水平，以及提供相关专属资源的承诺，如出现问题时，保证软、硬件持续可用的相关措施。考虑与外包服务提供商意外终止合同的情况，商业银行应建立恰当的应急措施，应对外包服务提供商在服务中可能出现的重大缺失，尤其需要考虑外包服务提供商的重大资源损失、重大财务损失和重要人员的变动；
b) 商业银行所有信息科技外包服务合同应由信息科技风险管理部门、法律部门和信息科技管理委员会审核通过，合同应该包括以下内容：服务水平、售后维护、保密条款、双方权利责任、违约处理等，对合同进行定期审阅更新，并使用统一的合同文本；
c) 商业银行应对外包服务提供商提出定性和定量的服务评价指标，审阅和修订服务水平协议，定期评估外包服务提供商为商业银行提供服务的充分性。通过服务水平报告、定期自我评估、内部或外部独立审计对外包服务提供商进行考核。对监督、评估过程中发现的各项问题进行反映和解决，针对考核不达标的情况采取整改措施，调整选择外包服务提供商流程，评估结果作为下一次选择外包服务提供商的重要依据；
d) 商业银行应与外包服务提供商界定信息所有权、签署保密协议和采取技术防护等措施保护客户信息和其他信息，对本银行客户资料与外包服务提供商其他客户资料做必要权限管理。按照“必需知道”和“最小授权”原则对外包服务提供商相关人员授权，同时合同中要求外包服务提供商保证其相关人员遵守保密规定。商业银行应将涉及本银行客户资料的外包作为重要外包告知相关客户，同时严格控制外包服务提供商再次对外转包，在中止外包协议时收回或销毁外包服务提供商保存的所有客户资料，采取足够措施确保商业银行相关信息的安全；
e) 商业银行针对关键生产设备、技术复杂度高或技术相对封闭的专用计算机系统设备，应与外包服务提供商签署维护协议，购买软、硬件维护服务，使应用系统和设备可以得到及时维护，提供持续供应能力的承诺。

附 录 A
（资料性附录）
内控评价工作底稿

A.1 概述

本附录表A.1给出了第5章公司层面内部控制评价、第6章流程层面内部控制评价、第7章信息技术层面内部控制评价所对应的工作底稿。

A.2 公司层面内控评价工作底稿

表 A.1 公司层面内控评价工作底稿

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
5.2 内部环境	5.2.1	组织架构	健全公司治理机制，加强内部机构制衡	a）商业银行公司治理机制不健全；	a）商业银行应设立股东大会、董事会、监事会和高级管理层，并履行相应职责。公司治理结构方面，股东大会作为权力机构，依法行使对商业银行重大事项的决定权；董事会作为决策机构，负责内部控制的建立健全，监督其有效实施并评价内部控制的有效性；监事会作为监督机构，对内部控制的建设与执行情况进行监督检查；高级管理层作为执行机构，负责组织实施董事会决议事项，组织开展内部控制的日常运行。商业银行还应建立独立董事制度，对董事会讨论事项发表客观、公正的意见；	财政部等五部委《企业内部控制基本规范》及《企业内部控制应用指引第1号》--组织架构 银监会《商业银行内部控制指引》	访谈董事会办公室，访谈董事、监事及高级管理人员，确定其对公司治理结构的效率和效果的评价。调阅《公司章程》，确定公司章程的对公司治理层面相关机构和人员的职能、职责的约束性。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
				b）董事会及专门委员会议事规则不完善；	b）商业银行根据国家有关法律法规和公司章程制定详细的股东大会、董事会、监事会的议事、决策规则，以及高级管理层的工作细则和规程。对内部控制的重大事项应采用集体决策机制，依照法律法规和监管要求以及公司章程在董事会和管理层下设置相应委员会：董事会下设审计委员会，按公司章程履行内部控制相关职责；总行组织制定内控建设规划，研究分析内控管理中存在的重大缺陷，监督重大问题落实整改等；	财政部等五部委《企业内部控制基本规范》及《企业内部控制应用指引第1号》--组织架构 银监会《商业银行内部控制指引》	调阅《公司章程》、《董事会议事规则》，确定董事会下设专门委员会的职责权限议事规则等完善性；抽查董事会各专门委员会会议纪要，确定董事会各专门委员会的履职情况。
				c）组织架构、内部机构设置缺乏制衡；	c）根据经营管理需要和内部控制要求，建立健全授权和分工合理、职责明确、制约平衡、报告关系清晰的内部控制组织架构。在确定职权和岗位分工过程中，应当体现不相容职务相互分离的要求。不相容职务通常包括：可行性研究与决策审批；决策审批与执行；执行与监督检查等；	财政部等五部委《企业内部控制基本规范》及《企业内部控制应用指引第1号》--组织架构 银监会《商业银行内部控制指引》	调阅公司组织架构图及内设机构职能，访谈确定职责设置分工，确定职责权限分工的合理性。抽查重要岗位职责分工，确定不相容职务分离的有效性。
				d）缺乏对子公司（子行）投资的管理和控制。	d）通过外派董事、监事，并监督其履职情况，加强对子公司（子行）的管控，建立科学的投资管控制度，通过合法有效的形式履行出资人职责、维护出资人权益，重点关注子公司特别是异地、境外子公司的发展战略、年度财务预决算、重大投融资、重大担保、大额资金使用、主要资产处置、重要人事任免、内部控制体系建设等重要事项。	财政部等五部委《企业内部控制基本规范》及《企业内部控制应用指引第1号》--组织架构 银监会《商业银行内部控制指引》	调阅《公司章程》、对子公司管理的相关制度等，确定公司对子公司管理的职责分工权限；抽查子公司发展战略、年度财务预决算、重大投融资等，确定公司派出董监事的履职情况。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
	5.2.2	发展战略	制定并有效实现发展战略	a）商业银行缺乏明确的发展战略规划；	a）商业银行建立明确的发展战略规划，在公司层面健全战略决策的组织架构，在董事会下设立战略委员会，对战略发展规划进行审议，商业银行发展战略规划经董事会审议通过后，应当报经股东（大）会批准后实施；	财政部等五部委《企业内部控制基本规范》及《企业内部控制应用指引第2号》--发展战略 银监会《商业银行内部控制指引》	调阅《公司章程》、战略委员会议事规则、公司发展战略计划等，确定公司发展战略制定和审议组织机构建设的健全性，相关部门职责分工是否明确；抽查公司发展战略规划，战略委员会工作会议纪要，确定战略委员会履职情况和战略的审批程序的有效性。
				b）商业银行未在充分调查研究、科学分析预测和广泛征求意见的基础上制定发展战略目标。	b)商业银行在制定发展战略目标过程中，应进行充分调查研究、科学分析预测并广泛征求意见，综合考虑宏观经济政策、国内外市场需求变化、技术发展趋势、行业及竞争对手状况、可利用资源水平和自身优势与劣势等影响因素。	财政部等五部委《企业内部控制基本规范》及《企业内部控制应用指引第2号》--发展战略 银监会《商业银行内部控制指引》	访谈了解商业银行发展目标的制定过程，调阅支持性文档，确认商业银行发展战略目标的制定过程中，综合考虑了宏观经济政策、国内外市场需求变化、技术发展趋势、行业及竞争对手状况、可利用资源水平和自身优势与劣势等影响因素，进行了充分的调查研究和科学分析预测并广泛征求了意见。
				c）战略规划执行、落实不力。	c）商业银行发展战略应保持一定的稳定性，将发展战略进行分解和落实，制定落实发展战略的工作方案，按照部门、机构等管理维度将战略规划进行落实。	财政部等五部委《企业内部控制基本规范》及《企业内部控制应用指引第2号》--发展战略 银监会《商业银行内部控制指引》	调阅战略执行方案，确定战略规划的分解落实情况是否细化的相关部门机构；抽查战略执行情况的报告，确定公司战略执行效果，是否按照职责分工在制定具体政策制度过程中有效执行和贯彻公司发展战略。调阅公司战略执行情况的定期报告，确定对公司战略执行效果监控的有效性。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
	5.2.3	企业文化	培育企业核心价值观，推广企业文化建设	a）未培育全体员工认同的核心价值观，未形成企业文化；	a）商业银行应培育健康的企业文化，对企业文化的内涵及其策划、渗透、评估与改进做出明确的规定，增强员工和社会公众对企业文化的理解和认可，提升商业银行竞争力和品牌价值。特别应向员工传达诚实守信、遵守法律法规和实施内部控制的重要性，引导员工树立合规意识和风险意识，提高员工职业道德水准，规范员工职业行为；	财政部等五部委《企业内部控制基本规范》及《企业内部控制应用指引第5号》--企业文化 银监会《商业银行内部控制指引》	在银行内部各层面开展问卷调查，抽查企业规章制度和操作流程，评价是否将企业核心价值理念贯穿到各项制度建设过程中。
				b）并购重组中存在文化冲突；	b）加强并购中的文化整合，尤其是跨国并购或跨境并购，应对并购双方的文化差异进行识别和有效管理，以指导银行以吸纳式或渗透式对双方企业文化进行有效整合；	财政部等五部委《企业内部控制基本规范》及《企业内部控制应用指引第5号》--企业文化 银监会《商业银行内部控制指引》	抽查企业并购中对企业文化建设方面采取的措施，制定的企业文化整合方案，评价企业对并购双方文化的整合效率和效果。
				c）未落实企业文化。	c）企业文化的传播采用高层推动与基层实践相结合。高层管理者成为企业文化建设的倡导者、组织者和实践者。商业银行应当促进文化建设在内部各层级的有效沟通，加强企业文化的宣传贯彻。	财政部等五部委《企业内部控制基本规范》及《企业内部控制应用指引第5号》--企业文化 银监会《商业银行内部控制指引》	访谈高管层，评价企业文化的传播是否自上而下，在公司治理层面得到重视；抽查员工对企业文化理念的知晓程度和范围，评价员工诉求和意愿的反馈渠道是否畅通。
				d）未建立企业文化评估制度，企业文化建设流于形式。	d）商业银行应当建立企业文化评估制度，明确评估的内容、程序和方法，落实评估责任制，避免企业文化建设流于形式。	财政部等五部委《企业内部控制基本规范》及《企业内部控制应用指引第5号》--企业文化 银监会《商业银行内部控制指引》	了解商业银行企业文化评估制度的建立情况，确认是否明确了评估内容、程序和方法，落实评估责任制。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
	5.2.4	内部审计	建立垂直独立的内部审计体系，合理保证企业经营管理合法合规	a）未建立垂直独立的内部审计组织体系；	a）商业银行设立垂直管理、具有充分独立性的内部审计部门，向董事会负责并报告工作，履行集团层面内部控制评价工作的牵头职责，协助完成内部控制评价报告的对外披露；	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》、《银行业金融机构内部审计指引》	调阅《公司章程》、《内审章程》、内控相关制度等，确定银行内部审计部门机构的独立性、报告路径的独立性等；抽查审计报告及向董事会的定期汇报，确定内审部门履职情况。
				b）内部审计权限不明确；	b）商业银行应当以制度形式明确赋予内部审计部门履行职责所必需的权限。内部审计部门应有权及时、全面了解经营管理信息，并就有关问题向审计对象和人员进行调查、质询、举证；	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》、《银行业金融机构内部审计指引》	调阅《内审章程》、内控相关制度等，确定银行内部审计部门职责权限等；抽查审计报告及向董事会的定期汇报，确定内审部门履职情况。
				c）审计质量缺乏监控。	c）内部审计部门应建立审计回避制度，确保内部审计的客观性，内部审计部门应对审计发现与恰当的管理层沟通，监督整改活动的进行并执行后续审计，有权将发现的内部控制重大缺陷直接向董事会及其审计委员会、监事会报告。	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》、《银行业金融机构内部审计指引》	调阅审计报告整改报告，抽查审计报告及向董事会的定期汇报，确定内审部门履职情况。
	5.2.5	人力资源	实现人力资源合理配置，建立人力资源薪酬与激励机制	a）人力资源政策及开发机制不健全；	a）商业银行根据战略发展规划，结合人力资源现状和未来需求预测，建立人力资源发展目标，制定人力资源总体规划和能力框架体系，优化人力资源整体布局，明确人力资源的引进、开发、使用、培养、考核、激励、退出等管理要求，健全关键岗位员工强制休假和定期岗位轮换，掌握国家秘密、重要商业秘密或知识产权员工脱密安排、竞业限制等管理机制；	财政部等五部委《企业内部控制基本规范》及《企业内部控制应用指引第3号》--人力资源 银监会《商业银行内部控制指引》	调阅人力资源发展战略和年度计划，确认人力资源计划对银行战略目标的遵循性和落实情况。抽查人力资源的相关规章制度、工作总结和报告，验证人力资源工作流程的健全性和有效性。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
				b）缺乏人力资源选聘标准；	b）将职业道德修养和专业胜任能力作为选拔和聘用员工的重要标准，健全相关业务从业人员的资格认定与考核制度，保证从业人员具备必要的专业资格和从业经验。切实加强员工培训和继续教育，确保员工熟知相应岗位的业务操作流程、内控要求和经办业务的主要风险点，充分了解相关的规章制度、奖惩规定，以及在内部控制中的权利和责任；	财政部等五部委《企业内部控制基本规范》及《企业内部控制应用指引第3号》--人力资源 银监会《商业银行内部控制指引》	调阅人员招聘制度和流程，验证人员招聘程序的健全性，招聘考核指标是否有效覆盖职业道德、业务能力等重要方面。抽查招聘结果，对录用人员的专业能力、资质证书等进行有效考察与检查，评价招聘录用程序的规范性。
				c）人力资源薪酬与考核激励机制缺失。	c）董事会下的薪酬委员会负责审议全行薪酬管理制度和政策，拟订董事和高级管理层的薪酬方案，并向董事会提出薪酬方案建议，监督方案实施。薪酬制度应与人力资源考核结果相挂钩，建立健全内部控制激励约束机制，将各机构、各部门和全体员工实施内部控制的情况纳入绩效考评体系，在绩效分配中予以体现；	财政部等五部委《企业内部控制基本规范》及《企业内部控制应用指引第3号》--人力资源 银监会《商业银行内部控制指引》	调阅薪酬管理制度，评价薪酬制度及人力资源考核制度的健全性；抽查人力资源考核结果，评价考核结果是否建立与员工薪酬的联动机制。调阅薪酬标准和发放程序，评价相关程序的合规性。
				d）未对年度人力资源计划执行情况进行定期评估。	d）商业银行应当定期对年度人力资源计划执行情况进行评估，总结人力资源管理经验，分析存在的主要缺陷和不足，完善人力资源政策，促进企业整体团队充满生机和活力。	财政部等五部委《企业内部控制基本规范》及《企业内部控制应用指引第3号》--人力资源 银监会《商业银行内部控制指引》	调阅人力资源计划执行情况评估报告，评价相关程序有效性。
	5.2.6	社会责任	有效履行企业社会责任，保护	a）商业银行未履行社会责任；	a）商业银行应该切实履行社会责任，追求经济效益与社会效益、短期利益与长远利益、自身发展与社会发展相互协调，实现企业与员工、企业与社会、企业与环境的健康和谐发展；	财政部等五部委《企业内部控制基本规范》及《企业内部控制应用指引第4号》--社会责任 银监会《商业银行内部控制指引》	调阅《企业社会责任报告》，全面确定商业银行社会责任履行情况的有效性。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
			员工合法利益	b）危害、侵犯员工合法权益。	b）银行与员工签订并履行劳动合同，遵循按劳分配、同工同酬的原则，建立科学的员工薪酬制度和激励机制，不得克扣或无故拖欠员工薪酬。建立高级管理人员与员工薪酬的正常增长机制，切实保持合理水平，维护社会公平。银行及时办理员工社会保险，足额缴纳社会保险费，保障员工依法享受社会保险待遇。避免在正常经营情况下批量辞退员工，增加社会负担。	财政部等五部委《企业内部控制基本规范》及《企业内部控制应用指引第4号》--社会责任 银监会《商业银行内部控制指引》	抽查劳动合同制度及签订的劳动合同，评价是否建立员工薪酬的正常增长机制。抽查员工各项福利费的列支情况，抽查员工休假情况、加班情况等统计表，确定员工合法权益的落实情况。
5.3 风险评估	5.3.1	风险管理体系	健全全面风险架构，设定风险管理目标	a）风险管理架构不健全；	a）商业银行应建立健全的风险管理组织体系，董事会下设立风险管理委员会，设立专门的风险管理部门牵头负责全面风险管理工作，商业银行能够预见、识别因经营环境、组织结构的变化等因素导致的风险；	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	调阅公司章程等有关文件，了解董事会、监事会、高级管理层在内部控制和风险管理中的职责规定以及履职情况；了解风险管理委员会的建立、职责规定及履职情况；调阅业务部门的风险管理流程和职责文件,了解前台风险自我管理和控制能力；调阅年度风险管理相关资料，以评价该工作的有效性。
				b）风险管理目标不明确。	b）商业银行根据外部形势和内在发展要求，制定风险管理战略和目标，确定风险承受度，包括整体风险承受能力和业务层面的可接受风险水平。	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	调阅风险管理战略规划及目标，确认银行是否明确了风险承受度，以及在确定风险承受度时是否考虑了整体风险承受能力和业务层面的可接受风险水平；调阅相关风险管理报告，确认银行是否对风险偏好的情况进行了监测、报告；

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
				c)风险管理制度体系不完善；	c)商业银行应当制定识别、计量、监测和控制风险的制度、程序和方法，以确保风险管理和经营目标的实现；	银监会《商业银行内部控制指引》	调阅风险管理制度，确认银行制定了识别、计量、监测和控制风险的制度、程序和方法，且这些制度、程序和方法能对实现风险管理和经营目标提供合理保证；
				d)风险管理信息系统不完备。	d)商业银行应当建立涵盖各项业务、全行范围的风险管理系统，开发和运用风险量化评估的方法和模型，对信用风险、市场风险、流动性风险、操作风险等各类风险进行持续的监控。	银监会《商业银行内部控制指引》	检查银行风险管理系统对主要业务的覆盖面，评价信息系统建设是否满足风险管理需求。
	5.3.2	风险识别	有效识别主要风险	a) 风险识别范围不明确；	a) 商业银行持续对各类风险进行有效的识别与评估。主要风险包括信用风险、市场风险（含利率风险）、操作风险、国家风险、流动性风险、法律风险以及声誉风险等；特别应考虑计算机系统的运用可能带来的风险；	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	调阅信用风险、市场风险（含利率风险）、操作风险、国家风险、流动性风险、法律风险以及声誉风险等管理制度建设情况及风险识别管理办法，确认政策和制度对风险识别的业务覆盖和机构覆盖等情况是否明确，风险识别范围是否全面。
				b) 风险识别要素不明确；	b) 商业银行对各类风险进行识别时应充分考虑内部和外部因素。当环境和条件发生变化时，应及时对风险进行再识别和再评估，以确保任何新的和以前未曾予以控制的风险得到识别和控制。若涉及到组织结构、流程、计算机系统等方面的重大变更，应考虑可能产生的新风险；	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	调阅内外部市场情况发生变化时相关风险评估报告，检查相关风险评估工作是否根据情况变化进行适当的修正。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
				c）各类风险识别重点不明确。	c）在信用风险识别方面，重点关注但不限于国家、地区、行业、客户、交易方式、集中度等因素。在市场风险识别方面，重点关注但不限于利率、汇率（包括黄金）、股票价格和商品价格等因素。在操作风险识别方面，重点关注但不限于人员、内部程序、系统、外部事件等因素。在流动性风险识别方面，重点关注但不限于存款客户支取、贷款客户提款、债务人延期支付、资产负债结构不匹配、资产变现困难、经营损失和衍生品交易风险等因素。对影响银行经营管理的声誉风险、战略风险、国别风险等其他各类风险，均应根据外部环境、监管要求和经营状况，开展风险识别工作。	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	调阅风险识别办法及评估报告，检查对信用风险、市场风险、流动性风险等相关风险识别的重点是否包括银行面临的主要风险因素。
	5.3.3	风险评估	建立有效的风险评估程序，确定风险评估重点	a）未建立风险评估程序、标准、方法；	a）商业银行应根据风险管理战略和目标，建立健全风险评估的程序、标准和方法，采用有效的工具和方法，对经营管理活动中的风险进行主动识别与准确评估，并采用定性与定量相结合的方法，按照风险发生的可能性及其影响程度等，对识别的风险进行分析和排序，确定关注重点和优先控制的风险。在风险评估过程中，各商业银行应根据监管规定和自身的实际情况选择风险计量方法；	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	调阅牵头管理部门的相关风险评估报告，对照监管规定的要求，评价是否符合监管规定要求的内容；评价内容包括风险识别与评估是否依据业务范围、性质和时限主动进行；评估风险的后果、概率和风险级别；风险量化评估的方法和模型，对识别的风险进行分析和排序，确定关注重点和优先控制的风险。
				b）风险评估重点不准确。	b）商业银行合理分析、准确掌握董事、行长及其他高管人员、关键员工的风险偏好，采取适当的控制措施，避免因个人风险偏好给企业经营带来重大损失。	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	调阅风险评估办法，确认风险评估的重点是否围绕银行面临的主要风险。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
	5.3.4	风险应对	制定合理的风险应对策略	a）未制定风险应对策略；	a）商业银行应根据风险评估结果，结合风险承受度，权衡风险与收益，综合运用风险规避、风险降低、风险分担和风险承受等应对策略，实现对风险的有效控制，避免给本行经营带来重大损失。	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	调阅风险管理报告，访谈相关人员，检查对识别的各类风险是否制定有效的风险应对策略。
				b）风险报告程序不健全。	b）商业银行应根据风险管理的需求，编制不同层次和种类的风险报告，并按照制度规定的范围、程序和频率发送报告，以满足各机构、各部门对风险状况的多样性需求。	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	调阅风险管理报告，确定报告范围、程序和频率的有效性和全面性。
5.4 控制活动	5.4.1	政策与流程	建立贯穿经营管理全过程的有效控制流程	a）控制活动措施不明确；	a）商业银行应根据内部控制目标，结合风险应对策略，通过手工控制与系统控制、预防性控制与发现性控制相结合的方法，综合运用控制措施，对各种业务和事项实施有效控制，控制活动应覆盖各项经营管理的全过程；	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	调阅内部控制目标及制定的相关策略，确认银行制定并实施的各项控制活动的全面性和有效性。
				b）未制定政策制度明确业务处理流程。	b）商业银行制定政策制度，明确业务流程，各项业务应结合实际建立全面、系统、成文的政策、制度和程序，编制业务操作指南，保持统一的业务标准和操作要求，并保证其连续性和稳定性。	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	抽查业务流程和操作指南等，确定业务处理的标准性和统一性。
	5.4.2	不相容职务分离	实施不相容职务分离及轮岗制度	a）未建立全面的不相容职务分离控制制度；	a）商业银行全面系统地分析、梳理业务流程中所涉及的不相容职务，实施相应的分离措施，形成各司其职、各负其责、相互制约的工作机制，明确关键岗位、特殊岗位、不相容岗位及其控制要求；	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	调阅业务部门的业务流程和岗位职责，检查是否全面系统地梳理了业务流程中的不相容职务；调阅《内部控制规定》，审阅其中关于不相容岗位的制度规定；抽查相关业务，检查是否对关键岗位、特殊岗位、不相容职务设置了相互分离的岗位。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
		控制		b）未建立关键岗位人员轮换和强制休假制度。	b）建立关键岗位员工定期或不定期轮换和强制休假制度，明确轮岗范围、轮岗周期、轮岗方式等。	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	调阅《关键岗位人员岗位轮岗和强制休假办法》，检查关键岗位是否设置了轮岗、强制休假制度及是否有关键岗位离岗的限制性规定。
	5.4.3	授权审批控制	建立完善的授权体系及集体决策制度	a）授权管理制度、体系不完善；	a）根据各分支机构和业务部门的经营管理水平、内部控制和风险管理能力、地区经济和业务发展需要，建立相应的授权体系，实行统一法人管理和法人授权。明确各岗位办理业务和事项的权限范围、审批程序和相应责任。授权应适当、明确，并采取书面形式；	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	调阅授权管理的制度规定，检查其关于岗位办理业务和事项的权限范围、审批程序和相应责任的内容是否适当。调阅授权管理的制度规定，检查其关于特别授权的权限范围、层次、审批程序和相应责任的内容是否适当。
				b）重大业务和事项未实行集体决策审批。	b）各机构、各部门管理人员在授权范围内行使职权和承担责任，对须经集体决策审批的重大业务和事项，任何个人不得单独决策或者擅自改变集体决策的意见。确需调整集体决策意见且此调整可能导致风险敞口扩大的，须提请集体决策机构再议；风险没有扩大，无须提请集体决策的，应事先取得相应授权。	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	调阅相关制度规定，检查其关于集体决策审批内容是否适当； 抽查商业银行重大的业务或事项，检查其是否执行了集体决策审批，是否存在越权现象。
	5.4.4	会计系统控制	制定会计制度与规范，财务报告及相关信息	a）未制定会计制度与规范；	a）商业银行严格执行国家统一的会计准则制度，配备具有相应从业资格和资质的人员，加强会计基础工作，明确会计凭证、会计账簿和财务会计报告的处理程序，保证会计资料真实完整；	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	调阅有关会计制度，确定商业银行会计制度的内容是否严格遵守国家统一的最新的会计准则制度；询问有关人员跟踪外部监管机构、会计准则等相关会计政策变化并采取应对措施的程序及流程。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
			真实完整	b）会计岗位设置未实行责任分离、相互制约的原则；	b）会计岗位设置应当实行责任分离、相互制约的原则，严禁一人兼任非相容的岗位或独自完成会计全过程的业务操作。明确会计部门、会计人员的权限，各级会计部门、会计人员应当在各自的权限内行事，凡超越权限的，须经授权后，方可办理；	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	调阅授权的基本规定，确定会计核算业务是否遵循“逐级授权、逐级上报、逐级审批”的原则；调阅会计部门关于会计岗位设置的规定，确定会计岗位设置是否实行责任分离；检查关键岗位人员的规定，检查会计核算业务人员轮岗和强制休假规定。
				c）未配备足够的会计从业人员。	c）银行应该依法设置会计机构，配备会计从业人员。	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	调阅银行会计基本规范，检查其会计机构的设置要求。
	5.4.5	财产保护控制	建立财产保护制度，保证资产安全	a）未建立财产日常管理制度和定期清查制度；	a）建立财产日常管理制度和定期清查制度，采取财产记录、实物保管、定期盘点、账实核对等措施，确保财产安全；	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	调阅固定资产管理、基建项目管理的相关规定，确认其是否建立了财产的日常管理制度和定期清查制度；抽查固定资产的日常管理制度，检查其固定资产台账管理、日常的使用和维护管理以及处置流程、会计记录、账实核对情况等。
				b）未明确规范职责分工、权限范围和审批程序。	b）银行对财产保护的职责分工、权限范围和审批程序进行明确的规范，机构设置和人员配备科学合理，严格限制未经授权的人员接触和处置财产。	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	调阅固定资产管理、基建项目管理的相关规定，确定职责分工审批程序是否合理有效。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
				C）安全工作机制不健全、安防设施建设不完备；	C）提高安全管理的认识，切实加强对安全的保卫工作的组织领导，建立健全安全工作机制；加强对员工的安全意识教育，严格按照业务流程操作；加强安防设施建设。对全辖营业网点全面推行安防设施达标建设，保证所有营业场所有灵敏可靠、严密完善的技防、物防设施；	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	调阅安全管理方面的制度，确认是否建立了健全的安全工作机制；调阅员工安全保卫培训记录，确认定期开展安全保卫培训；现场检查营业网点的技防、物防措施安全有效。
				d）金库、营业网点安全存在风险隐患；款箱交接、ATM加钞、款箱及运行环节存在风险隐患；	d）加强营业网点日常安全管理，严格落实营业网点安全防范工作的相关操作规程；加强制度执行力度，款箱交接环节必须严格按照操作规程流程进行，加强对ATM的运行管理；	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	调阅营业网点安全防范工作的工作规程，确定流程设计是否合理。调阅款项交接记录，确认款项交接手续是否严格执行工作规程；调阅ATM运行记录和检查记录，评价ATM运行是否安全合规。
	5.4.6	预算控制	建立全面预算管理、考核、约束机制	a）未实施全面预算管理制度；	a）实施全面预算管理制度，明确各责任单位在预算管理中的职责权限，规范预算的编制、审定、下达和执行程序，强化预算约束；	财政部等五部委《企业内部控制基本规范》及《企业内部控制应用指引第15号》--全面预算 银监会《商业银行内部控制指引》	调阅全面预算管理的相关规定； 调阅年度预算计划，检查其是否对当年的预算项目、标准和程序都做了很好的规划；抽查本年预算的某个部分，审阅在该项目中，各预算的责任部门是否职责权限清晰。
				b）未建立有效的预算考核、约束机制；	b）银行建立严格的预算执行考核制度，对各预算单位和个人进行考核，切实做到有奖有惩、奖惩分明；	财政部等五部委《企业内部控制基本规范》及《企业内部控制应用指引第15号》--全面预算 银监会《商业银行内部控制指引》	调阅预算管理办法，检查其是否建立了预算业绩考核体系；询问预算责任部门相关人员并分析历年预算-结果的符合性，了解预算业绩考核体系的合理性。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
				c）预算方案及变更未经过适当的审批。	c）银行董事会审核全面预算方案，银行下达的预算应当保持稳定，不得随意调整。由于市场环境、国家政策或不可抗力等客观因素，导致预算执行发生重大差异确需调整预算的，应当履行严格的审批程序。	财政部等五部委《企业内部控制基本规范》及《企业内部控制应用指引第15号》--全面预算 银监会《商业银行内部控制指引》	调阅年度综合经营计划，审阅并确认是否根据战略规划制定预算；调阅最新的发展规划，确认是否定期更新和调整整体和部门的预算计划。
	5.4.7	运营分析控制	建立运营分析制度，促进企业实现发展战略	a）未建立经营管理情况分析制度；	a）建立经营管理情况分析制度，管理层综合运用各方面信息，通过因素分析、对比分析、趋势分析等方法，定期开展经营管理情况分析；	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	调阅各部门管理职责，是否定期进行运营分析；调阅财务运营分析报告、风险管理分析报告、经营情况分析报告、投融资管理分析报告等，确认其运营分析的结果处理程序，确认管理层获得运营分析报告的途径、频率等，并考察其分析方法的科学性和合理性。
				b）未对运营分析中发现的存在问题加以改进。	b）对运营分析中发现的存在问题，及时查明原因并加以改进。	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	抽查运营分析报告，确认报告是否分析并确认问题，提出改进建议。
	5.4.8	绩效考评控制	建立绩效考评制度，有效利用考评结果	a）未建立和实施绩效考评制度；	a）建立和实施绩效考评制度，科学设置考核指标体系，对内部各责任单位和全体员工的业绩进行定期考核和客观评价；	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	调阅考核规定，审阅是否根据本行的战略目标设置业绩指标体系；调阅考评结果，了解考评程序。
				b）绩效考评结果未能得到有效利用；	b）银行将考评结果作为确定员工薪酬以及职务晋升、评优、降级、调岗、辞退等的依据；	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	抽查绩效考核结果的落实情况，确定银行是否将绩效考评结果作为确定员工薪酬以及职务晋升、评优、降级、调岗、辞退等的依据。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
				c）绩效考评指标体系修订不及时。	c）银行应该定期审核关键业绩指标，将其与战略目标进行比较，及时修改和改进银行关键业绩指标体系。	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	调阅银行绩效考评管理办法，将其与银行战略目标比较，确定是否能及时修改和改进关键业绩指标体系。
	5.4.9	重大风险预警控制	建立重大风险预警机制，妥善处理突发事件	未建立重大风险预警机制。	建立重大风险预警机制和突发事件应急处理机制，明确风险预警标准，对可能发生的重大风险或突发事件，制定应急预案、明确责任人员、规范处置程序，确保突发事件得到及时妥善处理。	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	调阅银行应急及突发事件的处理办法，确定是否建立了有效的重大风险预警机制和突发事件应急处理机制，是否明确了预警指标的标准，是否明确了应急方案中的人员职责、处理程序等。抽查应急处理结果，确定相关制度的执行效果。
	5.4.10	并表管理控制	有效管理并表机构，实施风险隔离措施	a）未制定并表管理制度；	a）银行应制定并表管理制度，明确并表管理的机构确认原则与标准、相关组织架构、各相关单位工作责任、以及具体管理要求；母行应与附属机构，以及附属机构之间建立健全防火墙制度，实现风险隔离；	银监会《商业银行内部控制指引》、《银行并表监管指引（试行）》	调阅并表管理办法，确定并表管理组织分工、制度是否健全；抽查并表管理的流程和范围，确定是否建立了附属机构的隔离机制。
				b）并表管理责任未落实；	b）董事会应承担并表管理最终责任，并负责制定银行集团并表管理的总体战略方针，审批和监督并表管理具体实施计划的制定与落实，以及建立定期审查和评价机制。高级管理层应对并表管理体系的充分性和有效性进行监测和评估；	银监会《商业银行内部控制指引》、《银行并表监管指引（试行）》	访谈董事会相关成员，调阅董事履职报告，确定董事会相关成员是否在并表管理中履行最终责任。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
				c）未建立大额风险暴露的管理政策和内控制度；	c）应建立大额风险暴露的管理政策和内控制度。明确相关的政策、程序来识别、计量、监测和控制集团层面的风险暴露。明确大额风险暴露的预警报告制度，以及与风险限额相匹配的风险分散措施等。应实时监控大额风险暴露。	银监会《商业银行内部控制指引》、《银行并表监管指引（试行）》	调阅大额风险暴露的管理政策和内控制度，调阅监控记录，确定大额风险暴露管理的有效性。
				d）未建立监测、报告、控制和处理内部交易的政策与程序。	d）建立监测、报告、控制和处理内部交易的政策与程序。集团内部交易条件不得优于独立第三方。制定相应措施有效控制附属机构所产生信用、市场、流动性、操作、声誉等其他风险和损失对母行所带来的风险。	银监会《商业银行内部控制指引》、《银行并表监管指引（试行）》	调阅内部交易管理制度，抽查检测结果，确定是否制定相应措施有效控制附属机构产生市场、流动性等风险对母行的风险。
	5.4.11	反洗钱控制	建立反洗钱制度，合理保证企业经营管理合法合规	a）未建立反洗钱制度；	a)制定集团层面反洗钱标准、反洗钱合规管理制度、业务部门将反洗钱合规要求嵌入业务制度和操作流程；	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	调阅反洗钱制度，反洗钱操作规定和控制措施，确定制度的有效性。
				b)未明确各部门、各岗位的反洗钱工作职责；	b)设立反洗钱专门机构或指定内设机构负责反洗钱工作；明晰各条线（部门）和各类人员的反洗钱职责；	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	调阅反洗钱专门机构、岗位设置的情况，判断是否设立反洗钱专门机构或指定内设机构负责反洗钱工作，是否明确各条线（部门）和各类人员的反洗钱职责；
				c)未建立反洗钱监测系统；	c)应建立与本行业务规模相适应的反洗钱监测系统，包括建立反洗钱风险名单监控系统、大额交易监控系统和可疑交易监测分析系统，为反洗钱岗位人员提供技术支持；	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	检查银行反洗钱监测系统，是否包含了反洗钱风险名单监控系统、大额交易监控系统和可疑交易监测分析系统，是否为反洗钱岗位人员提供技术支持；

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
				d)未建立洗钱风险评估体系；	d)应从全流程的角度对各项金融业务及产品、系统进行洗钱风险评估，强化高风险领域的反洗钱合规管理措施；建立客户洗钱风险评级系统，对所有客户的洗钱风险等级进行评定，并根据客户风险等级采取相应的风险控制措施；	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	调阅反洗钱风险评估报告，评价银行是否对各项金融业务及产品、系统进行了洗钱风险评估；检查银行客户洗钱风险评级系统，是否对全部客户的洗钱风险等级进行了评定，是否根据客户风险等级采取了相应的风险控制措施；
				e)未开展员工培训；	e)应制定反洗钱培训计划，持续地开展反洗钱培训；	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	调阅反洗钱培训计划和培训记录，确认银行定期制定反洗钱培训计划并持续开展反洗钱培训。
				f)未按规定执行客户身份识别制度、大额和可疑交易报告制度和客户身份资料及交易记录保存制度。	f)应全面履行客户身份识别制度、客户身份资料及交易记录保存制度、大额和可疑交易报告/反恐融资和反扩散融资报告制度等。	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	调阅识别客户身份的相关资料，评价银行客户身份识别制度的执行情况；调阅大额和可疑交易报告，评价银行大额和可疑交易报告制度的执行情况；现场查看银行客户身份资料及交易记录的保存情况。
	5.4.12	关联交易控制	有效管理并及时披露管理交易信息	a) 未建立关联交易制度；	a) 银行应建立健全满足监管部门要求的关联交易制度。管理层应合理界定关联方和关联交易的范围、关联交易的定价和授权等；	银监会《商业银行内部控制指引》及《商业银行与内部人和股东关联交易管理办法》	调阅董事会关联交易控制委员会会议记录，确认该制度是否有效满足外部监管规定。审阅关联交易配套管理制度,确认是否根据外部监管的要求进行了规范和完善。抽查制度与流程，确认是否对关联方交易的范围、定价、授权等控制环节进行了适当规定。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
				b）未明确各部门、各岗位的职责权限；	b）合理设置职能部门和工作岗位，明确各部门、各岗位的职责权限，形成各司其职、各负其责、便于考核、相互制约的关联交易工作机制；	银监会《商业银行内部控制指引》及《商业银行与内部人和股东关联交易管理办法》	调阅公司章程，确认是否对重大关联交易和特别重大关联交易的标准做出规定，关联交易管理控制是否明确部门分工和职责。
				c）未建立关联交易管理体系；	c）银行应建立有效的关联交易管理体系，相关部门、各分支机构、并表机构应按照授权规范开展关联交易；	银监会《商业银行内部控制指引》及《商业银行与内部人和股东关联交易管理办法》	抽查关联交易信息管理和运作情况，检查关联交易信息统计、报送情况是否符合相关规定。
				d）未进行关联交易信息的统计、报告与披露。	d）银行应当通过建立关联交易档案台账等多项措施，确保关联交易数据的真实性、准确性和完整性，满足对关联交易数据采集统计、事后检查、报告与披露的需要。	银监会《商业银行内部控制指引》及《商业银行与内部人和股东关联交易管理办法》	检查关联交易统计信息的具体方法和内容，确认信息统计工作的数据来源、报表报送频率等是否能够有效保证统计信息的完整性。
	5.4.13	业务外包控制	建立外包活动管理框架，有效管理外包风险。	a）未建立董事会高管层承担最终责任的外包组织架构；	a）银行的董事会和高管层承担外包业务的最终责任，董事会审议批准外包战略发展规划、外包风险管理制度、外包范围、外包报告、外包审计等，高管层制定外包战略发展规划、外包风险管理政策和内控制度、确定外包范围、实施监督职责等，外包管理团队执行外包风险管理政策、操作流程和内控制度，并向高管层报告；	《银行业金融机构外包风险管理指引》	调阅外包战略发展规划、外包风险管理制度等，确认外包业务组织架构的合规性和有效性，检查外包团队的履职情况。
				b）不宜外包的核心管理职能进行外包；	b）银行的战略管理、核心管理以及内部审计等职能不宜外包；	《银行业金融机构外包风险管理指引》	调阅全行战略、核心管理业务、内部审计等资料，检查不宜外包的战略管理、核心管理以及内部审计等职能是否外包。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
				c）未有效开展外包活动的风险管理和控制；	c）银行应评估外包活动的战略风险、法律风险、声誉风险、合规风险等，对外包服务提供商进行尽职调查，签订书面合同，确保客户信息安全；	《银行业金融机构外包风险管理指引》	调阅外包活动形成的风险评估报告、尽职调查报告、合同等，确定外包活动风险管理措施和控制执行的有效性。
				d）未对外包活动开展监督检查。	d）银行定期对外包活动进行全面审计与评价，向银监会报送评估报告和重大影响事件。	《银行业金融机构外包风险管理指引》	调阅外包活动审计报告及重大影响事件的报告，确定外包活动监督检查的有效性。
	5.4.14	业务连续性控制	有效识别和评估业务中断风险，建立业务连续性管理体系。	a）未制定业务连续性管理战略并建立组织架构；	a）银行根据业务发展总体目标、经营规模以及风险控制的基本策略和风险偏好，确定适当的业务连续性管理战略，建立业务连续性管理的组织架构，制定业务连续性计划，有效处置运营中断事件，董事会是决策机构，对业务连续性管理承担最终责任，高管层制定业务连续性管理政策，连续性管理委员会落实管理职责，主管部门、执行部门负责业务条线和信息技术的应急响应和恢复；	《商业银行业务连续性监管指引》	调阅业务连续性管理战略、组织架构、管理制度等，确定董事会作为决策机构、高管层作为管理机构、部门作为执行机构，在业务连续性管理中的履职情况。
				b）业务连续性管理未纳入全面风险管理体系；	b）银行应将业务连续性管理纳入全面风险管理体系，建立与全行战略目标相适应的业务连续性管理体系；	《商业银行业务连续性监管指引》	调阅全面风险管理体系，检查业务连续性管理该是否纳入全面风险管理。
				c）未识别和评估业务中断的影响和损失；	c）银行通过业务影响分析识别和评估业务运营中断所造成的影响和损失，根据业务重要程度实现差异化管理，至少每三年开展一次全面业务影响分析并形成报告；	《商业银行业务连续性监管指引》	调阅业务连续性影响分析报告，确定是否识别和评估业务中断的影响和损失。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
				d）未开展业务连续性资源建设和演练。	d）银行开展业务连续性计划所需的资源建设，满足业务恢复目标和重要业务持续运营的要求，建立统一的运营中断事件指挥中心，建立灾备中心、关键岗位备份人员等，开展业务连续性演练和应急处置机制。	《商业银行业务连续性监管指引》	检查业务连续性资源建设、灾备中心、关键岗位备份人员等设置情况，调阅业务连续性演练和应急处置报告，确定业务连续性的资源建设和演练等应急处置机制的有效性。
5.5 信息与沟通	5.5.1	信息指标体系	建立信息指标管理体系，提高经营效率	a）未构建信息数据平台；	a）构建信息数据平台，实现管理信息集中处理，信息体系不仅是数据的集中，而是生产经营管理信息的集中,为经营管理信息的沟通与交流提供基础保障。银行各机构、各管理部门定期开展数据分析工作，为市场营销、风险管理等各项经营管理活动提供数据分析平台，为管理层精细化决策提供系统支持；	财政部等五部委《企业内部控制基本规范》及《企业内部控制应用指引第17号》--内部信息传递 银监会《商业银行内部控制指引》	调阅信息系统管理制度办法，确认银行信息指标体系的建立是否满足内部控制目标；抽查信息系统平台的建设情况，评价是否满足为各项生产活动提供信息分析、处理的平台。
				b）未建立内、外部信息指标体系。	b）全面分析外部经济金融环境，同业信息以及国内外监管法规制度的最新变化情况，全面梳理影响银行发展的重要外部信息来源，完善外部信息资料指标体系，根据发展战略执行情况建立内部信息报告体系，为管理层定期提供内部信息报告。	财政部等五部委《企业内部控制基本规范》及《企业内部控制应用指引第17号》--内部信息传递 银监会《商业银行内部控制指引》	抽查银行外部信息沟通和传递渠道，调阅外部信息指标体系，评价外部信息获取渠道的全面性和充分性。
	5.5.2	信息系统	健全信息管理平台，提高信息	a）未开发信息系统；	a）根据各级管理层对信息数据的需求，有针对性地开发信息系统，提升系统数据质量，根据管理需要建立识别、管理大量数据的工作机制，有力地支持管理需求；	财政部等五部委《企业内部控制基本规范》及《企业内部控制应用指引第17号》--内部信息传递 银监会《商业银行内部控制指引》	检查信息系统的建设情况，对主要业务的覆盖面，评价信息系统建设是否满足管理需求。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
		建设	质量	b）缺乏数据质量考核；	b）定期考核银行数据质量情况，将数据质量纳入到内控管理及银行经营绩效综合考核，逐步建立较为完善的数据质量激励约束机制；	财政部等五部委《企业内部控制基本规范》及《企业内部控制应用指引第17号》—内部信息传递 银监会《商业银行内部控制指引》	检查数据质量管理流程，评价数据质量，是否建立数据质量激励约束机制。
				c）客户端安全控制不健全。	c）商业银行应加强客户端安全控制，明确客户端安全管理要求，防范客户端信息安全风险，严格执行客户端网络准入、软硬件使用控制、互联网访问以及客户端操作行为等方面的安全管理要求，做好客户端安全使用管理。	财政部等五部委《企业内部控制基本规范》及《企业内部控制应用指引第17号》—内部信息传递 银监会《商业银行内部控制指引》	调阅数据客户端安全管理制度，抽查数据管理各环节安全管理措施的有效性，确认客户端数据安全管理体系的健全性。
	5.5.3	信息安全控制	合理设置权限，保障信息安全	a）信息系统安全管理缺失；	a）银行加强对信息系统开发与维护、访问与变更、数据输入与输出、文件储存与保管、网络安全等方面的控制，保证信息系统安全稳定运行。确定信息及信息系统的安全等级，明确应用系统中各类信息使用的安全管理要求，实施分等级安全管理；	财政部等五部委《企业内部控制基本规范》及《企业内部控制应用指引第17号》—内部信息传递 银监会《商业银行内部控制指引》	调阅数据质量的安全管理制度，抽查数据管理各环节安全管理措施的有效性，确认数据安全管理体系的健全性。
				b）信息使用缺乏权限管理。	b）严禁员工之间擅自转让信息系统的用户密码信息，人员调离时，应移交全部技术资料及有关密钥资源的介质，停止其使用、维护和管理的权限，及时更换密码信息，必要时执行有关脱密期的规定。	财政部等五部委《企业内部控制基本规范》及《企业内部控制应用指引第17号》—内部信息传递 银监会《商业银行内部控制指引》	调阅员工名册及离职人员名册，确认员工调离是否及时销户并取消权限，是否执行脱密的规定。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
	5.5.4	信息交流机制	加强信息沟通与交流，提高信息使用效率	a）内部交流机制不健全；	a）信息自上而下传递顺畅，要确保各项信息能够按照内部控制路线准确、快捷地传递到相关机构、部门和员工，促使全体员工及时了解经营管理理念和内部控制要求。信息自下而上传递顺畅，要确保各级机构经营情况、各部门和员工履职情况、发现的内部控制隐患和缺陷、各类突发事件和重大事件等信息能够顺畅反馈，重要信息能够真实、及时传递给董事会、监事会和高级管理层。信息交流与共享，各机构之间和各部门之间应按信息管理权限，加强各类信息资源的共享，确保信息横向交流和互通，促进提升信息使用效率；	财政部等五部委《企业内部控制基本规范》及《企业内部控制应用指引第17号》—内部信息传递 银监会《商业银行内部控制指引》	抽查内部信息的收集和传递程序，明确信息传递的时效性和全面性。
				b）外部交流机制不健全；	b）通过行业协会、业务合作机构、客户、市场调查、来信来访、媒体网络以及有关监管部门等多方有效获取外部信息，对外部信息尤其是客户信息及时进行筛选、核对、整合和分析，及时跟进管理措施，强化内部控制，有效防范和化解经营风险。	财政部等五部委《企业内部控制基本规范》及《企业内部控制应用指引第17号》—内部信息传递 银监会《商业银行内部控制指引》	抽查外部信息的收集和传递程序，明确信息传递的时效性和全面性。
				c）未建立重大信息报告制度。	c）规范信息传递的工作机制，按照真实、准确、完整、及时的原则，将重大信息及时传递给董事会、监事会和经理层。建立重大信息报告联系人制度，保证重大信息在银行内部的顺畅传递；在完善内部信息搜集机制的基础上，规范与监管机构信息传递的途径和方式。	财政部等五部委《企业内部控制基本规范》及《企业内部控制应用指引第17号》—内部信息传递 银监会《商业银行内部控制指引》	调阅信息处理和沟通渠道的制度规定，明确员工获得相关信息的渠道和方法以及频率；抽查相关人员对重要业务信息、战略规划等的掌握程度，判断信息传递渠道的畅通性。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
	5.5.5	信息披露机制	建立信息披露流程与重大信息报告制度	信息披露制度和流程不完善；	商业银行应按照诚实尽职履行信息披露义务，提高信息披露质量和效率，完善信息披露的风险控制机制，确保信息披露的稳健性与透明性。完善信息披露流程、内涵及风险控制机制。理顺信息披露内部流程，按照监管要求定期做好强制性信息披露工作；建立信息反馈机制，主动了解投资者信息需求，逐步增加主动信息披露内容，拓展信息披露的广度和深度，建立多样化信息披露途径，明确信息披露参与各方的职责，建立全面的信息披露风险控制体系和应急反应措施；	财政部等五部委《企业内部控制基本规范》及《企业内部控制应用指引第17号》—内部信息传递 银监会《商业银行内部控制指引》	调阅重大信息报告制度，抽查公告及临时公告，评价银行是否根据监管规定确定对外公开披露的重要信息，并及时传递给董事会、监事会和经理层。
	5.5.6	反舞弊机制	建立反舞弊机制，纳入经营绩效考核体系	a）反舞弊工作的重点不突出；	a）银行确定反舞弊工作的重点，明确舞弊行为的类型，包括未经授权或者采取其他不法方式侵占、挪用银行资产，牟取不当利益；在财务报告和信息披露等方面存在的虚假记载、误导性陈述或者重大遗漏等；董事、监事、经理及其他高级管理人员滥用职权；相关机构或人员串通舞弊；	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	调阅反舞弊制度，检查相关制度的执行情况，是否有效控制案件高发风险点和风险环节；抽查反舞弊工作报告，检查反舞弊工作重点是否集中在财务报告和信息披露等重要方面。
				b）案件举报处理工作不落实；	b）建立举报处理制度，对举报的案件线索和瞒案不报问题进行核查处理。制定反舞弊工作责任制量化检查办法，对各级机构负责人和部门负责人履行反舞弊职责检查的可操作性，并将检查结果纳入经营绩效考核；查处违法违纪案件，治理商业贿赂，提高执纪办案水平，发挥查处案件的综合效应；	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	调阅违法违纪案件举报处理制度，确定对举报人是否建立保护制度，是否建立银行负责人案防职责； 抽查举报案件的落实情况，是否对案件及举报的处理，做到事实清楚、证据确凿、定性准确、程序合法。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
				c）未建立举报投诉制度和举报人保护制度。	c）设置举报专线，明确举报投诉处理程序、办理时限和办结要求，确保举报、投诉成为银行有效掌握反舞弊信息的重要途径。建立举报投诉制度和举报人保护制度，举报途径应当及时传达至全体员工。	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	抽查举报专线的设置情况和员工知晓情况，评价举报制度和举报人保护制度的健全性，评价举报制度的执行效果。
5.6 内部监督	5.6.1	内部监督组织架构	明确内部监督机构及职责权限	a）未建立内部监督组织架构；	a）建立并完善监督组织架构。从公司治理层面建立监事会、董事会审计委员会、内部审计部门和其他内部机构在内部监督中的职责权限。明确内部审计机构和其他内部机构在内部监督中的职责权限，规范内部监督的程序、方法和要求；	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	调阅监事会、审计委员会、内部审计等相关监督部门的组织架构和职责权限等相关制度，确定相关制度建设的健全性；抽查审计报告、监事会、审计委员会工作报告、会议纪要等，确定银行监督体系内相关部门和机构履职的有效性。
				b）内部监督职责权限不明确。	b）商业银行应指定不同的机构或部门分别负责内部控制的建设、执行和内部控制的监督、评价，内部控制建设与内部控制评价部门进行分离。	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	调阅内控制度和部门机构的职能分工，确定内部控制建设执行部门与内控监督评价部门职责分离情况。
	5.6.2	内部监督制度	建立有效的内部监督制度体系，合理保证企业经营	a）检查监督办法缺失；	a）商业银行应制定内部控制检查监督办法，该办法至少包括如下内容：董事会或相关机构对内部控制检查监督的授权；各部门及下属机构对内部控制检查监督的配合义务；内部控制检查监督的项目、时间、程序及方法；内部控制检查监督工作报告的方式；内部控制检查监督工作相关责任的划分；内部控制检查监督工作的激励制度；	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	调阅内部控制相关的检查监督办法，确定内控制度建设的健全性；抽查监督检查报告，确定相关检查监督制度履行的效果。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
			管理合法合规	b）未妥善保存内部控制资料。	b）商业银行应以书面或者其他适当的形式，妥善保存内部控制建立与实施过程中的相关记录或者资料，确保内部控制建立与实施过程的可验证性。	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	抽查内控检查记录，确定工作底稿的完整性及内控制度的可验证性。
	5.6.3	内部监督工作	内部监督范围全面，监督实施效果显著	a）内部监督工作流于形式；	a）建立健全银行日常监督检查工作机制与流程，制定日常监督检查管理制度，明确各级机构、各部门在日常监督检查工作中的职责定位，规范检查流程、报告路线及作业标准等方面要求；开展专项监督，根据风险评估结果及日常监督有效性确定专项监督工作重点；	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	抽查日常监督报告，检查监督管理制度，确定检查监督职责分工定位的明确性，管理制度的健全性。
				b）内部审计工作覆盖范围不全面；	b）内部审计重点关注董事会所关注的重要风险领域，建立健全内部审计监督范围，对内部控制、风险管理和治理过程三大领域开展审计监督检查，开展内部控制评价工作；	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	抽查内部审计工作规划、工作计划、工作总结及审计报告，确定审计工作范围的全面性和有效性。
				c）未开展内部控制评价工作。	c）董事会开展内控评价。董事会开展内控评价应依据上交所、深交所的要求，至少按照年度进行一次内控评价。完善内控评价指标体系，根据业务发展需要，适时修订完善内控评价指标体系，强化指标内涵的深度和覆盖的广度，督促内控管理持续改进和提高。	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	抽查监督检查报告，内控评价报告，确定监督检查工作的有效性。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
	5.6.4	整改机制	完善内部监督整改机制，落实责任	a）未建立内部控制缺陷标准体系；	a）建立内部控制缺陷标准体系，明确内部控制设计缺陷与运行缺陷的认定标准，结合影响程度确定内部控制缺陷轻重等级，确保各类监督检查成果统一可比。制定内部控制缺陷的认定标准，按重要性划分内部控制缺陷等级。根据缺陷影响银行整体控制目标的严重程度，将内部控制缺陷分为重大缺陷、重要缺陷和一般缺陷三个等级；	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	调阅内部控制缺陷标准体系，确定缺陷的认定标准、分级是否有效。
				b）内控缺陷报告机制不健全；	b）对于检查中发现的内部控制缺陷及实施中存在的问题，应在内部控制检查监督工作报告中据实反映，应采取适当的形式及时向董事会、监事会或者经理层报告，并在报告后进行追踪，以确定相关部门已及时采取适当的改进措施；	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	抽查内控检查整改报告，确定对内控缺陷进行整改机制的健全性。
				c）重大缺陷缺乏整改跟踪机制。	c）跟踪内部控制缺陷整改情况，并就内部监督中发现的重大缺陷，追究相关责任单位或者责任人的责任。根据内部控制制度，对各级机构、部门的内部控制状况定期做出评价，并将评价结果作为经营绩效考核的重要依据。	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	抽查重大内控缺陷的整改措施及对相关责任人的责任追究和处罚机制，确定内控发现问题整改的效果和效率。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
	5.6.5	内部控制评价	有效实施内控评价	a）未定期开展内部控制评价工作；	a）商业银行应结合内部监督情况，董事会定期对内部控制的有效性进行评价，出具内部控制评价报告。内部控制评价的方式、范围、程序和频率，应根据经营业务调整、经营环境变化、业务发展状况、实际风险水平等自行确定。内控评价的覆盖面完整性，评价范围应覆盖内部控制活动的全过程及所有的系统、部门和岗位。内控评价时间的及时性，评价应按照规定的时间间隔持续进行，当经营管理环境发生重大变化时，应及时重新评价。内控评价方法的合理性，评价应依据风险和控制的重要性确定重点，关注重点区域和重点业务；	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	抽查内控评价报告，确定内控评价工作的及时性和有效性。
				b）内控评价报告披露风险。	b）上市商业银行董事会应在年度报告披露的同时，披露年度内部控制评价报告，并披露会计师事务所对内部控制评价报告的审计意见。	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	调阅内控自我评价披露报告，评价内控评估报告的内容是否符合监管规定。

A.3　流程层面内控评价工作底稿

表 A.2　流程层面内控评价工作底稿

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
6.2 公司贷款	6.2.1	客户评级与统一授信	健全客户风险评价机制和风险限额管理制度，合理评价客户偿债能力和意愿，控制融资风险总量	a）客户不符合国家法律法规认定的借款人条件或不符合银行准入要求；	a）客户经理应通过实地调查与间接调查相结合的方式，收集整理客户基本资料和业务所需资料，建立客户档案，提出业务受理建议。	《贷款通则》《商业银行授信工作尽职指引》《流动资金贷款管理暂行办法》《固定资产贷款管理暂行办法》《银行开展小企业授信工作指导意见》	查阅银行信贷政策制度及各类信贷产品管理办法，检查对借款人资格的要求及其与国家法律法规的一致性；检查信贷档案资料是否齐全，是否包含营业执照、贷款卡等基本资料；检查信贷档案资料是否及时更新，信贷档案资料是否存在不符合准入条件的情况；
				b）客户评级未按照规定的时限和规定的流程完成或评级信息与借款人实际情况不符；	b）客户经理应对有融资余额的客户和拟办理融资的客户定期进行信用等级评定，选择适当的客户评级模型，采集评级相关信息使用银行评级系统发起评级流程，评级流程应由独立于评级发起人的评级认定人员进行认定，应当保留评级过程和结果信息。	《商业银行信用风险内部评级体系监管指引》 《流动资金贷款管理暂行办法》	查阅银行法人客户评级政策制度及各类评级办法，检查评级系统、数据保持情况；检查是否根据借款人和保证人的经营情况和财务状况开展信用等级评定，是否存在无信用等级而办理融资的情况，是否设置更新条件并及时完成更新，是否存在符合客户评级更新条件但未评级和未及时完成评级的情况；检查评级使用的模型是否符合办法规定，评级数据输入是否准确完整，评级推翻是否符合推翻政策；检查评级发起和认定是否相互独立，认定人是否经过适当的授权。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
				c）未按照规定的方法合理测算客户最高授信额度；	c）应根据不同企业规模和类型选择相适应的授信额度测算模型，在对客户资信情况及融资风险进行综合分析与评价的基础上核定银行对客户愿意和能够承受的风险限额，包括承担客户信用风险的表内外业务、本外币业务、流动资金和固定资产业务。	《贷款通则》《商业银行授信工作尽职指引》《流动资金贷款管理暂行办法》《固定资产贷款管理暂行办法》《银行开展小企业授信工作指导意见》	查阅银行法人客户统一授信/限额管理政策制度及具体测算方法，检查授信/限额管理系统的存在性和数据保持的完整性；检查授信数据的录入情况，分析授信客户概况信息录入的完整性、正确性，银行融资情况录入内容是否符合企业客观实际；查看客户总授信额度、客户各项融资业务余额，分析是否存在部分业务未纳入授信范围的情况。
				d）未能有效识别集团、关联客户，未纳入集团、关联客户授信管理	d）应关注和搜集集团客户及关联客户的有关信息，有效识别授信集中风险及关联客户授信风险。	《贷款通则》《商业银行授信工作尽职指引》《流动资金贷款管理暂行办法》《固定资产贷款管理暂行办法》《银行开展小企业授信工作指导意见》	查阅银行法人客户集团、关联管理的政策制度，是否明了纳入集团关联管理的范围，制度是否明确集团关联授信/限额管理办法及具体测算方法；检查集团关联客户授信相关资料，关注此类客户授信尽职调查是否包括关联关系、股权结构等进信息，调查审查是否分析合并报表、关联融资、关联担保，并据此对集团整体和关联体融资风险进行综合分析评价，并核定对该集团和关联体进行融资风险限额的控制；检查信贷管理系统是否对集体关联客户进行规范明确的标识，是否存在有关联关系而未标识最终影响了融资总量控制。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
	6.2.2	调查和审查审批	确保银行遵循贷审分离、分级审批原则，开展尽职调查和合规审查	a）调查内容不完全或调查失实，风险评估不充分；对于流动资金贷款，未按监管要求测算流动资金需求或测算值偏高，对固定资产贷款，未对项目主体进行综合风险评估；	a）客户经理应通过实地调查与间接调查相结合的方式，按照客户申请的业务品种进行准入条件的初步分析或向客户推荐更适当的融资产品，收集整理该产品所需各类资料和信息，提出业务受理建议，并录入信贷管理系统。对于流动资金贷款应根据授信客户的经营和风险特点，结合其经营周期、上下游客户情况、结算方式等信息，合理分析借款人真实的借款原因和融资需求，准确测算和确定流动资金贷款需求。对固定资产贷款，应结合项目主体的法律性质和经营方式，分析借款人的风险特征和综合偿债能力。	《贷款通则》《商业银行授信工作尽职指引》《流动资金贷款管理暂行办法》《固定资产贷款管理暂行办法》	查阅银行各类信贷产品管理办法，是否针对产品风险特征制定不同的准入条件，是否明确客户经理尽职调查的职责和流程；查阅借款人基本信息资料、营业执照、组织机构代码证、税务登记证、特许经营许可证（如需）、贷款卡，外商投资企业批准证书及外商投资企业外汇管理登记证等资料，分析客户是否及时年检、相关证件是否已过有效期，客户主体资格是否合法；查阅人民银行征信系统、行内相关信息系统保留查询记录、客户征信报告，检查借款申请人和担保人信用状况，分析是否有不良记录；结合具体信贷产品，查阅业务所需资料是否齐全，客户经理是否对资料来源进行确认和标注；查询信贷管理系统，客户经理是否出具调查报告并明确调查意见，系统内信息是否与档案信息保持一致。对流动资金贷款应对借款人资料和信息审查分析，分析借款人真实的借款原因和融资需求，使用监管的测算模型准确测算流动资金贷款需求，避免超额授信情况的发生。对固定资产贷款，应对项目主体的背景、

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
				b）固定资产贷款未进行充分的项目风险评估；	b）应落实具体的责任部门和岗位，对固定资产贷款进行全面的风险评价，并形成风险评价报告。应建立完善的固定资产贷款风险评价制度，设置定量或定性的指标和标准，从借款人、项目发起人、项目合规性、项目技术和财务可行性、项目产品市场、项目融资方案、还款来源可靠性、担保等角度进行贷款风险评价。	《贷款通则》《商业银行授信工作尽职指引》《项目融资业务指引》《固定资产贷款管理暂行办法》	查阅银行固定资产贷款业务的管理办法，检查固定资产贷款风险评估制度和流程是否存在，岗位设置和人员配备是否合理；检查是否独立进行固定资产贷款的风险评估，评估流程和参与评估人员是否符合评估制度和授权制度；检查评估报告内容是否完整，方法是否科学，结果是否合理。
				c）商业银行已实行债项评级的，债项评级的依据不充分，结果不准确；	c）商业银行已实行债项评级的，客户经理应根据银行债项评级的具体要求，将债项相关信息准确输入系统并开展债项等级评价。	《贷款通则》《商业银行授信工作尽职指引》《流动资金贷款管理暂行办法》《固定资产贷款管理暂行办法》《商业银行信用风险内部评级体系监管指引》	查阅银行债项评级政策制度和具体办法，检查债项评级制度和流程、债项评级系统、数据保存是否存在且完整；检查样本客户档案资料、影像资料中的营业执照、验资报告、财务报表、审计报告等客户基本信息，与系统中的客户基本信息台账及评级信息采集中的基本信息进行比较核对，核查信息输入是否准确；调阅样本调查、审查报告、项目评估报告、人行征信系统信息等资料，对债项合同要素信息、抵（质）押担保合同信息及押品价值评估流程和结果、保证合同信息及保证人担保能力、债项相关风险调整因素信息录入准确性进行判断，核查评级结果是否合理。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
				d）审查不严格，未对业务风险进行识别评估并拟定适当的控制防控措施；	d）审查人员应根据融资业务品种不同，对客户提交的资料进行核对，并分析客户融资需求的合理性，揭示存在的主要风险并提出防范措施要求，对融资额度、期限、担保方式、还款方式、利率等要素进行风险和收益的评估。	《贷款通则》《商业银行授信工作尽职指引》《流动资金贷款管理暂行办法》《固定资产贷款管理暂行办法》《商业银行信用风险内部评级体系监管指引》	查阅银行各类信贷产品管理办法，是否针对产品风险特征设定不同的融资条件，是否明确审查人员的审查内容和和流程；查阅贷款资料和审查报告或审查审批表，是否存在审查所需资料不完整的情况；检查抽样样本中审查人是否对融资业务的风险进行提示，是否拟定了相应的风险应对措施，是否对融资业务提出明确的审查意见，融资额度、期限、担保方式、还款方式、利率等要素是否符合该客户所属行业的行业政策规定，是否符合该信贷产品管理办法的具体要求。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
				e）调查、审查、审批未有效分离，审批人未经授权或超授权审批；	e）应根据贷审分离、分级审批的原则，建立规范的贷款评审制度和流程，确保风险评价和信贷审批的独立性。应建立健全内部审批授权与转授权机制，审批人员应在授权范围内按规定流程审批贷款，不得越权审批。	《贷款通则》《商业银行授信工作尽职指引》《流动资金贷款管理暂行办法》《固定资产贷款管理暂行办法》《银行开展小企业授信工作指导意见》	查阅银行信贷业务政策制度，是否明确调查、审查、审批岗位相互分离，是否对业务审批制定规范明确的授权和转授权制度，并对照授权文件查阅信贷管理系统对业务审批授权和转授权的记录；查阅业务调查、审查、审批记录，核实岗位是否相互分离，是否均独立发表意见并记录于审批表或审批系统内；对照审批人的授权文件，查看该业务是否在其授权范围内，若超过授权是否有特别授权文件；符合集体审议条件的，是否按照制度规定进行集体审议，并保留审议结论。
	6.2.3	发放和支付管理	严格按照审批意见签署贷款合同文本，发放贷款前要落实	a)未经贷款有权人审批即与借款人签订借款合同；	a）应根据有权审批人签署的审批意见书，与借款人及其他相关当事人签订书面借款合同、担保合同和其他相关协议，合同要素应当明确，且与审批意见书一致，并应明确贷款发放的前提条件和资金支付条款，且与审批意见书一致。	《贷款通则》《商业银行授信工作尽职指引》《流动资金贷款管理暂行办法》《固定资产贷款管理暂行办法》《银行开展小企业授信工作指导意见》	查阅银行信贷贷款合同签订流程；检查借款合同的签订时间与审批意见书的出具时间，分析是否存在审批前已经签订合同的情况；检查借款合同及其他相关协议，是否存在要素不一致；检查借款合同内是否按照审批意见书增加了或落实了贷款发放的前提条件和支付管理条款。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
			前提条件并按约定进行支付管理	b)未采用融资产品对应的格式化的合同文本，或使用非格式文本但未经法律部门审查同意；	b）应根据融资产品选择银行统一制定的合同文本，包括借款合同、担保合同及其他协议文本，如需使用非格式文本或增加其他条款应当经过法律部门审查同意	《贷款通则》《商业银行授信工作尽职指引》《流动资金贷款管理暂行办法》《固定资产贷款管理暂行办法》《银行开展小企业授信工作指导意见》《合同法》	检查贷款合同文本管理制度是否完善；检查借款合同、担保合同和其他协议文本是否使用该融资产品对应的统一格式文本，若非统一格式文本，是否有法律部门审查同意的意见书。
				c）未落实审批前提条件即向借款人发放贷款，或超过授信限额发放贷款，会计核算不准确；	c）应设立独立的部门或岗位负责贷款发放和支付审核，发放贷款前应确认借款人满足合同约定的提款条件。应确保贷款发放额度在客户、集团或其他维度的统一授信/限额管理的额度之内。应按照银行统一规定进行贷款业务的会计核算。	《贷款通则》《商业银行授信工作尽职指引》《流动资金贷款管理暂行办法》《固定资产贷款管理暂行办法》《银行开展小企业授信工作指导意见》	查阅贷款发放和支付岗位（部门）的职责；检查贷款发放和支付审核人员是否独立；检查贷款发放前是否落实审批意见书设定的贷款前提条件；检查贷款发放后客户的风险融资总量是否超过客户统一授信额度、集团关联企业统一授信额度、地区或行业限额；检查贷款科目选择、还款方式、计息设定等是否符合会计核算规范。
				d）未执行支付管理相关规定，符合受托支付条件的未执行受托支付；	d）应设立独立的部门或岗位负责贷款发放和支付审核，应按照合同约定通过贷款人受托支付或借款人自主支付的方式对贷款资金的支付进行管理与控制，监督贷款资金按约定用途使用。采用受托支付方式的，应审核支付用途的证明材料和具体支付对象，检查借款借据和支付凭证是否与其保持一致，支付是否及时。	《贷款通则》《商业银行授信工作尽职指引》《流动资金贷款管理暂行办法》《固定资产贷款管理暂行办法》《银行开展小企业授信工作指导意见》	查阅贷款发放和支付岗位（部门）的职责；检查贷款发放和支付审核人员是否独立；符合受托支付条件的贷款资金支付是否执行受托支付，分析是否存在化整为零等规避受托支付的情况；检查贷款资金支付所提供的用途证明材料是否与客户申请贷款时一致，与支付凭证上的对象、金额、用途吻合；检查贷款资金实际流向是否与审核同意的受托支付相一致。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
	6.2.4	贷后管理	有效开展贷后检查识别风险隐患，准确开展质量分类并提取拨备，落实还本付息管理	a）未按规定进行资金用途检查、贷后检查、风险监测，检查发现风险隐患未采取应对措施	a）贷款发放后，贷款人应当对借款人执行借款合同情况及借款人的经营情况、融资担保情况进行追踪调查和检查。对于自主支付的借款人应核查贷款支付是否符合约定用途。对于受托支付的借款人也应关注资金的最终流向是否异常。应定期或不定期通过现场检查与非现场监测，分析借款人经营、财务、融资情况的变化，监测担保保障能力的变化，掌握各种影响借款人及其债务偿还能力和意愿的风险因素。应通过非现场和现场检查，及时发现潜在风险并发出预警风险提示，及时采取提前收贷、追加担保等有效措施防范化解贷款风险。	《贷款通则》《商业银行授信工作尽职指引》《流动资金贷款管理暂行办法》《固定资产贷款管理暂行办法》《银行开展小企业授信工作指导意见》	查阅贷后管理制度和流程；检查资金流向跟踪报告，通过账户分析、凭证查验或现场调查等方式核查自主支付是否符合约定用途、核查受托支付的实际流向是否存在异常；检查贷后检查报告是否按照规定间隔期限开展，检查内容是否包括借款人的经营、财务风险，债项风险以及担保风险等，是否及时发现潜在风险并预警，采取适当的风险应对措施；检查定期贷后风险监测报告，是否对贷款业务总量、增量、质量和结构进行动态分析，是否对公司客户的财务风险、资金流向风险、经营管理风险、资信风险、关联及担保风险以及突发风险等进行监测。
				b）未按规定进行贷款风险分类或分类结果不准确	b)应至少每季对全部贷款进行一次分类，根据银监会的贷款分类类别和标准或银行自定的贷款分类类别和标准进行分类，并及时调整分类结果。	《贷款风险分类指引》《小企业贷款风险分类办法（试行）	查阅银行信贷资产质量分类管理制度、流程、系统；查阅信贷资产质量分类结果及相关分类资料，分析是否至少按季进行分类、分类资料是否完整、分类标准和结果是否合理。
				c）风险拨备计提不合规；	c）应当按照谨慎会计原则，合理估计贷款可能发生的损失，及时计提贷款损失准备。	《银行贷款损失准备计提指引》	查阅银行的风险拨备政策制度；检查贷款风险拨备的计算方法是否符合制度规定；检查贷款风险拨备的计提、转回、冲销等核算是否符合制度规定。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
				d）还本付息管理不到位；	d）应当提示借款人按照合同约定按时足额还本付息。对逾期的贷款和欠息要及时催收。对借款人申请提前还款的，应及时给予回复。	《贷款通则》《商业银行授信工作尽职指引》《流动资金贷款管理暂行办法》《固定资产贷款管理暂行办法》《银行开展小企业授信工作指导意见》	查阅银行信贷管理的贷款回收流程；检查贷款到期前是否及时向借款人进行提示；检查贷款逾期和发生欠息后是否及时发出催收通知书；检查客户提出提前还款申请的，是否予以回复，同意的是否按时进行会计核算。
	6.2.5	不良贷款管理	及时采取资产保全措施；以物抵债符合相关政策；债务重组依法合规；严格审查核销贷款项目。	a)现金清收不力；	a）根据不良贷款到期、逾期及计息情况，及时向借款人、担保人等还款义务人催收不良贷款本息，密切关注不良贷款诉讼时效、保证及抵（质）押担保期间、申请执行期限、资产查封与续封期限等，及时主张权利，确保主债权及担保权利受法律保护；	《贷款通则》银监发【2007】66号《中国银监会关于加强大额不良贷款监管工作的通知》	查阅银行不良贷款管理制度和流程；检查不良贷款风险分析报告、贷款催收记录，分析是否及时对借款人及保证人进行催收；诉讼时效内是否及时采取诉讼、处置抵押物等保全措施。
				b)以物抵债政策执行存在偏差；	b）贷款到期后，贷款行应积极采取有效措施进行清收，包括依法变卖抵（质）押物或债务人、保证人，第三人的合法财产，以现金形式收回贷款本息。只有在债务人确实难以以现金形式偿还贷款本息的情况下，方可实施以物抵贷。信贷员在进行借款人申请以物抵债时，采用双人现场勘查制，并且出具现场勘查报告；	《贷款通则》银监发【2007】66号《中国银监会关于加强大额不良贷款监管工作的通知》	查阅银行不良贷款管理制度和流程；检查不良贷款风险分析报告、以物抵债现场勘查报告，分析债务人是否确实无法用现金偿还债务，以物抵债方式是否合规，检查是否采用双人现场勘查制。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
				c）债务重组不符合条件；	c）对不良贷款进行重组应符合相关条件，在实施改制前须将客户改制方案按规定报批。债务重组对借款人减免部分本息，应满足借款人无力按期足额偿还贷款本息，经与借款人、担保人及其他还款义务人协商一致，确保减免和重组后能如期偿还剩余债务的条件。	《贷款通则》银监发【2007】66 号《中国银监会关于加强大额不良贷款监管工作的通知》	查阅不良贷款重组转化管理制度和流程；检查不良贷款风险分析报告、债务重组审查报告，分析债务重组是否按规定报批，重组削债是否符合条件。
				d)呆账核销不合规；	d) 审查审批部门要严格审查核销数据，核销材料要件要求规范、完整。加强对不良贷款处置预案的指导和管理，控制和预防不符合核销认定条件的项目。	《贷款通则》《银行贷款损失准备计提指引》 银监发【2007】66 号《中国银监会关于加强大额不良贷款监管工作的通知》	查阅贷款核销管理制度和流程；检查不良贷款核销报告，分析数据或内容是否真实，贷款是否符合核销认定条件，是否进行了责任认定，核销是否进行了逐级审查、集体审核，是否存在越权行为。
6.3 公司存款	6.3.1	开户	商业银行结算账户开立管理的合规性。	a)申请人开户资料或身份证明不真实，外汇账户不符合外管政策；	a)严格审核存款人身份和账户资料（营业执照、组织机构代码证、法人代表身份证等等）的真实性、完整性和合法性，外汇账户开户时需审核其提供的资料与国家外汇管理局相关管理要求一致。	《中国人民银行关于进一步加强人民币银行结算账户、转账、现金支取业务管理的通知》银发[2011]116 号银监会《商业银行内部控制指引》	调阅客户开户申请书和相关的开户资料复印件，核对客户的营业执照、组织机构代码证、法人代表授权书、法人身份证、预留印鉴、开户申请书、单位银行结算账户管理协议、税务登记证等,检查银行经办人员是否认真进行审核签章，相关资料是否在有效期内；外汇账户如资本金账户开户资料是否符合外管政策规定。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
				b)代理人身份不合规；	b) 对公客户经理不可为其服务的客户代办开户业务；营业网点员工不可直接代理客户办理任何金融业务；授权人必须审核申请人（代理人）的证件类型、证件号码等相关资料，对于客户授权委托书需明确被授权人及授权经办的业务种类，确认申请人（代理人）在业务办理现场，柜员须审核开户凭单或账户协议书上的客户签名盖章正确无误。	《中国人民银行关于进一步加强人民币银行结算账户、转账、现金支取业务管理的通知》银发[2011]116号	调阅客户开户申请书和相关的开户资料，核对代理人身份证件，是否经开户单位适当授权办理开户业务，是否存在银行员工代理开户情况；现场观察网点开户流程是否按规定流程与要求操作。
				c)开户凭证、协议上无客户签名盖章或签名不正确；	c)柜员须审核开户凭单或账户协议书上的客户签名盖章正确无误；	《中国人民银行关于进一步加强人民币银行结算账户、转账、现金支取业务管理的通知》银发[2011]116号	调阅客户开户申请书和相关协议、凭证，核对客户的签名盖章是否完整、准确。
				d)开户风险提示不充分。	d)柜员须主动向客户进行风险提示，包括：客户与银行间的风险责任；客户要妥善保管账户预留印鉴、支付密码及U盾等支付介质；对于大额取款业务须提前预约，并携带身份证件等。	《中国人民银行关于进一步加强人民币银行结算账户、转账、现金支取业务管理的通知》银发[2011]116号	调阅客户开户协议，查看是否有风险提示条款内容，客户是否有签字确认；实地观察，网点开户时，柜员是否向客户进行风险提示。
	6.3.2	存取款	商业银行结算账户转账、现金支取管理的合规性。	a)支付凭证上无客户预留印鉴或印鉴、支付密码错误；	a)柜员须审核支付凭证、记载事项、预留签章等的真实性、完整性、合规性，约定使用支付密码时须校验支付密码，核对无误后方可支付。	《中国人民银行关于进一步加强人民币银行结算账户、转账、现金支取业务管理的通知》银发[2011]116号 银监会《商业银行内部控制指引》	调阅客户结算账户取款、支付凭证，查看经办行是否核对凭证的有效性、支付的合规性，是否进行客户预留印鉴（支付密码）核对。
				b)未核实取款人（代理人）身份，或员工为客户代办存取款业务；	b)严格审核存取款人及代理人身份。对大额存款支取实行分级授权和双签制度。客户经理不可为其服务的客户代办存取款业务。	《中国人民银行关于进一步加强人民币银行结算账户、转账、现金支取业务管理的通知》银发[2011]116号 银监会《商业银行内部控制指引》	实时观察营业网点是否存在客户经理、员工代理客户办理存取款业务的情况；抽查客户大额取款凭证，查看是否摘录代理人和存款人的身份信息。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
				c)客户存取款金额与凭证打印记录不一致。	c)柜员须审核凭证打印输出的内容正确无误。若为大额现金业务，授权人须审核现金及交易输入金额与客户凭证填写金额相符；若为大额转账业务，授权人须审核转出账户及款项合规性。	《中国人民银行关于进一步加强人民币银行结算账户、转账、现金支取业务管理的通知》银发[2011]116号	调阅大额公到私转账业务或取款业务资料，核对是否经有权人审核业务的合规性，并做记录；查看差错登记薄，是否存在客户存取款金额与记账金额不相符的情况。
	6.3.3	账户变更	商业银行结算账户变更的合规性。	账户更改名称、印鉴、支付密码或法定代表人等其他开户资料未提供相关证明；	开户行需严格审核银行账户变更申请，核对预留印鉴、授权书等，对于重大开户资料的变更需核对营业执照等相关证明文件，并及时报备人民银行。	《人民币银行结算账户管理办法》	检查客户账户变更申请书或印鉴变更申请书，核对账户变更信息是否提供相应的资料，账户变更后是否及时上报监管并留有记录。
	6.3.4	挂失冻结	商业银行结算账户挂失、冻结管理的合规性。	a)无挂失申请或者申请书内容不完整；	a)柜员受理挂失申请时，须认真审核申请人（挂失人或代理人）的挂失申请书内容的真实性、完整性，核对客户提供的挂失公函、账户信息的准确性，核查确认申请人的身份，确认无误后及时办理挂失止付手续；	《人民币银行结算账户管理办法》中国人民银行令[2003]第5号	调阅挂失登记薄，核对挂失申请书内容的填写是否完整，经办人员是否认真核对客户申请挂失的公函及相关资料；查看系统设置，核对客户挂失止付信息在系统中的设置是否正确。
				b)未实施换人复核，擅自冻结或解冻客户账户。	b)建立复核制度，确保交易的记录完整和可追溯。专人复核柜员操作结果，同时确认柜员登记的挂失、冻结登记簿无误。有权冻结部门持有关公函，文件，通知等来银行办理冻结或解冻账户或账户余额业务时，需经银行业务主管人员审核，涉及有关账户余额确实未被冻结或已被冻结的情况下，办理冻结或解冻手续并打印相关记录。银行业务主管人员据此登记协助有权机关查询、冻结、扣划登记簿，并在执行通知书等文件回执上签字，加盖业务公章后交执法人员。	《人民币银行结算账户管理办法》中国人民银行令[2003]第5号 银监会《商业银行内部控制指引》	调阅挂失/冻结登记薄，核对操作是否双人办理。冻结或解冻客户账户是否有充分的理由并符合监管规定；调阅档案资料，看网点是否按规定保留相关材料。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
	6.3.5	对账	商业银行结算账户管理的合规性。	未与客户进行对账或对账结果不符时未及时核实。	建立和完善对账制度，对对账频率、对账对象、可参与对账人员等做出明确规定并确保对账的实时有效。对纳入余额对账单对账的单位，应定期与单位进行对账。对账人员收到企业反馈对账信息后，对“银企余额对账单”中不符的，开户行应及时与企业逐笔核查未达账项，确认未达原因。发现异常情况应及时采取有效措施。	《商业内部控制指引》银监会令[2007]第6号	调阅银行制定的客户对账制度，并实地抽查银企对账单及客户回执，评价对账制度执行的有效性。
	6.3.6	销户	商业银行结算账户撤销管理的合规性。	a)客户未正确填写撤销银行结算账户申请书，办理销户前未清理核对在途票据并交回未用票据。	a)柜员须审核客户撤销银行结算账户申请书，确保填写完整、准确；通过系统审核该账户是否有未归还的记账费用，是否有未归还的贷款、欠息，以及在途票据，确保未用票据空白凭证已全部交回或清理。	《人民币银行结算账户管理办法》中国人民银行令[2003]第5号	调阅已销户的账户档案，查看客户撤销银行结算账户申请书填写是否完整、准确；检查经办行是否存在客户未清偿开户银行债务，或未按规定交回各类重要空白票据及结算凭证，提前撤销账户的情况。
				b)授权人未核实申请人（代理人）身份；	b)授权人须确认销户申请人（代理人）身份；	《人民币银行结算账户管理办法》中国人民银行令[2003]第5号	调阅客户销户资料，判断代理人（申请人）是否已获得客户的授权；访谈了解网点销户的操作流程，评价其执行情况是否符合规定。
				c)销户信息未输入系统。	c)账户结清撤销后，须及时将销户信息录入系统，并按规定上报人行账户系统。	《人民币银行结算账户管理办法》中国人民银行令[2003]第5号	调阅已销户的账户档案，检查银行是否按监管规定及时销户并通知其基本户银行。查看人民银行账户管理系统，检查已销账户是否于银行销账户之日起2个工作日内向人民银行上报。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
6.4 票据融资	6.4.1	业务受理	对客户资信、贸易背景、交易行为的调查，控制票据欺诈风险和套用银行信用风险	a)汇票承兑人不具备承兑资格或贴现申请人/转贴现申请行不具备业务资格；	a)应对承兑人范围、贴现申请人和转贴现卖出行范围进行明确界定。客户经理收到贴现、转贴现申请后，应对承兑人、贴现申请人或转贴现申请行开展资信调查、授信调查、贸易真实性调查并收集相关资料；	人行《票据管理实施办法》、《中国人民银行关于完善票据业务制度有关问题的通知》；银监会《银行业监督管理委员会办公厅关于银行承兑汇票业务案件风险提示的通知》（银监办发[2011]206号）	查阅票据融资制度和流程，检查是否明确界定贴现申请人、转贴现申请行、汇票承兑人的范围；核对票据融资的贴现申请人、转贴现申请行、汇票承兑人是否在票据融资制度规定的范围内；检查汇票承兑人是否有充足可用的授信额度。
				b)申请资料不完整或不真实；	b)应对票据融资的申请人和贸易背景进行调查，收集客户基本资料和证明贸易背景的交易合同、增值税发票或普通发票。	《中国人民银行关于完善票据业务制度有关问题的通知》	检查客户资料是否齐全，证明贸易背景的交易合同和发票是否齐全，金额是否匹配，发票真实性是否进行查询核实并保留记录。
	6.4.2	审查审批	遵循审贷分离、分级审批原则，确保票据真实有效	a)票据不真实或有瑕疵	a) 票据应提交会计柜面，通过现场核查和人行系统等核查票面要素是否真实相符，他行是否已办理查询和贴现，是否办理了挂失止付和公司催告，核实票据背书是否连续。	《中国人民银行关于加强票据业务管理的通知》（讨论稿）；《中国人民银行关于完善票据业务制度有关问题的通知》（银发[2005]235号）	调阅查询查复记录，是否落实票据真实性的核查要求，并保留查询结果记录；检查大额银行承兑汇票是否采用双人实地查询。对回复“有他行查询”或有疑点的票据，是否采用实地查询、传真查询等多种方式进一步核查；检查票据背书是否连续；
				b)业务未经过适当审查、审批，或审批人超授权审批	b) 应制定票据融资审批流程、标准和授权机制，由专人开展独立性初复审，有条件的银行可以开发票据业务系统，采用系统审批方式；	《中国人民银行关于加强票据业务管理的通知》（讨论稿）	调阅审查记录，查看审查人是否独立开展票据融资的审查，并记录；调阅审批记录，查看审批人是否具有权限，是否按规定开展审批。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
	6.4.3	资金核算	严格控制资金划转，规范账户核算	a)资金核算不规范	a)贴现资金应划付至贴现申请人账户，贴现利息应准确计算并在贴现时扣收。	《银行业监督管理委员会办公厅关于银行承兑汇票业务案件风险提示的通知》（银监办发[2011]206号）《中国银监会办公厅切实加强票据业务监管的通知》（银监办发[2011]197号）	核查会计记账凭证，查看入账账户是否为贴现申请人；重新计算贴现利息，利息扣收是否正确。
	6.4.4	票据出入库	确保票据安全，避免票据遗失或毁损行为	a)票据出库、移存、入库过程中票据遗失或毁损	a)应对票据进行出入库管理，应定期对库存票据进行盘点，与账户信息进行核对。	《中国人民银行关于完善票据业务制度有关问题的通知》（银发[2005]235号）	查看票据的出入库记录，是否有交接记录；随机调阅监控录像，观察交接人员是否双人会同，是否办理当面交接，实物是否当日进入库房保管；查阅票据盘点记录，是否账实相符。
	6.4.5	票据托收（贴现或转贴现买	及时进行票据托收并正确进行账务处理	a）托收不及时；	a） 由专人负责查询票据到期日，匡算托收日程，与邮局等收件人员办理交接手续；	《中国人民银行关于完善票据业务制度有关问题的通知》（银发[2005]235号）	查看票据托收的交接记录，是否及时办理到期票据托收。
				b）收款销账出现错误；	b）收款凭证到达后，及时制作表内外凭证，由会计人员进行账务处理。	《中国人民银行关于加强票据业务管理的通知》（讨论稿）	调阅记账凭证，看是否在收款当日及时记账，完成票据贴现的到期收回处理。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
		入流程适用）					
	6.4.6	票据保全（贴现或转贴现买入流程适用）	及时采取票据保全措施，控制法律风险	a）挂失止付通知书发出不及时	a）一旦发生贴现票据的灭失，应立即通知承兑人挂失止付；	《中国人民银行关于加强票据业务管理的通知》（讨论稿）	核查票据灭失时出具的挂失止付通知书，或其他通知方式的记录文件。
				b）未及时向票据支付地法院申请公示催告。	b）在挂失止付3日内依法向票据支付地人民法院申请公示催告，或提起诉讼。	《中国人民银行关于加强票据业务管理的通知》（讨论稿）	核查票据灭失后的公示催告记录，是否在挂失止付后3日内完成。
				c)发生拒付时未采取追索等保全措施	c)收到拒付证明时，应对拒付事由进行审查，并及时向前手背书人追索或采取其他保全措施。	《中国人民银行关于加强票据业务管理的通知》（讨论稿）	检查发生拒付时是否保留拒付证明材料，拒付理由不成立是否与承兑行协商解决，拒付理由成立是否采取向前手背书人追索或采取其他保全措施。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
6.5 国际结算	6.5.1	业务受理	客户和业务准入条件符合国家政策、监管规定和银行内部管理制度。	a）客户准入及业务办理条件不符合国家政策、监管规定和银行内部管理制度。	a）严格按照国家政策及外部监管和银行内部管理制度开展尽职调查和业务审查审批。	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	调阅客户的营业执照、进出口权证明、业务委托书等申请资料及相关业务凭证，调阅经办银行的授权文件、尽职调查报告和审查审批等资料，查看是否按照规定进行尽职调查和审查审批，是否严格执行银行内部授权制度办理业务，客户和业务的准入条件是否符合国家政策、监管规定和银行内部管理制度。
				b)客户申请资料凭证不完整、不准确。	b）审核客户申请资料凭证，确保客户提交的业务申请资料和凭证完整准确。	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	调阅客户业务委托书、营业执照、进出口权证明等申请资料及相关业务凭证，审核相关申请资料和凭证的完整性和准确性。
	6.5.2	单证处理	遵循国际惯例和监管规定，避免因业务纠纷导致银	a）单证审查不严，与国际惯例和监管规定不符。	a)业务具有真实的贸易背景；符合单证相符等国际惯例；单证处理符合反洗钱、反恐等外部监管规定；严格执行有关业务金额和期限的银行内部授权管理和系统控制；业务部门出具单证审查意见。	《跟单信用证统一惯例》、《跟单托收统一惯例》、《关于审核跟单信用证项下单据的国际标准银行实务》等最新版国际惯例；监管规定和银行内部管理制度。	调阅留存单证、银行技术审查审批、银行间往来电传、客户投诉记录等资料，检查业务是否具有真实贸易背景，单证处理是否存在错误或瑕疵，是否符合国际惯例、监管规定和银行内部管理规定，业务风险事件处理是否妥当。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
			行资金损失或声誉风险。	b)单据保管或传递失误导致银行出现资金损失或声誉风险。	b)建立并执行严密的单据保管和交接制度。	《跟单信用证统一惯例》、《跟单托收统一惯例》、《关于审核跟单信用证项下单据的国际标准银行实务》等最新版国际惯例；监管规定和银行内部管理制度。	调阅并清点银行保管的正本单据以及有关单据签收记录，查看单据交接手续是否符合制度规定。
				c)业务处理缺乏依据导致纠纷。	c)涉及单据处置、往来函电、资金收付等业务处理均应获得客户或交易对手的书面指令或授权，指令不明确或授权不完整的应要求澄清后再进行业务处理。	《跟单信用证统一惯例》、《跟单托收统一惯例》、《关于审核跟单信用证项下单据的国际标准银行实务》等最新版国际惯例；监管规定和银行内部管理制度。	调阅全流程业务资料，了解所有业务流程中银行操作是否均符合规定并获得客户或交易对手的授权或指令。
	6.5.3	收付汇	资金收付准确及时，收付汇手续符合监管规定。	出口收汇延误、解付错误或不及时。	确保收汇指令汇路清晰、业务要素准确无误；建立和执行查询查复催收制度，确保客户收汇及时解付准确；对已办理融资的收汇应先行归还银行融资本息；	《跟单信用证统一惯例》、《跟单托收统一惯例》、《关于审核跟单信用证项下单据的国际标准银行实务》等最新版国际惯例；监管规定和银行内部管理制度。	调阅客户申请书、银行间往来报文、面函等业务留底资料，以及差错登记本和客户投诉记录，查看具体收汇业务涉及的汇路、金额、币种、账号、起息日、业务编号等要素是否准确，收汇和催收是否及时，已办理融资的收汇是否先行归还银行融资本息，客户投诉及业务纠纷是否妥善处理。
				进口承付（付汇/承兑/拒付）差错或延误。	提前落实付汇资金或办妥承兑/拒付手续，及时回复国外催收报文，确保承付报文准确及时发送。	《跟单信用证统一惯例》、《跟单托收统一惯例》、《关于审核跟单信用证项下单据的国际标准银行实务》等最新版国际惯例；监管规定和银行内部管理制度。	调阅客户申请书、银行间往来报文、面函等业务留底资料，以及差错登记本和客户投诉记录，查看具体付汇业务涉及的汇路、金额、币种、账号、起息日、业务编号等要素是否准确，进口承付是否及时，客户投诉及业务纠纷是否妥善处理。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
				收付汇（含预收付）手续不符合监管要求。	严格执行收付汇（含预收付）审核要求以及国际收支申报、结售汇、信息统计等相关监管规定。	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	调阅相关收付汇(含预收付)审核资料、国际收支申报、结售汇、信息统计等资料，登陆国际收支申报等相关监管系统，查看国际收支申报、结售汇、信息统计等相关手续是否符合监管规定，是否完备、准确、及时。
	6.5.4	资金清算及会计核算	清算准确及时、资金安全、会计核算准确和合规。	未严格执行有关资金清算的审查审批授权规定，清算操作失误和保全措施不力导致银行资金损失、业务纠纷等不良后果。	建立和执行清算授权制度并从严审核，操作环节减少人工干预，确保资金清算准确及时；发生清算失误时及时采取保全措施。	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	调阅资金算审查审批授权文件，查看业务处理系统的权限设置并观察操作环节是否存在过多或不必要的人工干预，是否严格执行授权规定办理清算业务；调阅银行间往来报文，查看资金清算是否准确、及时，发生清算失误后是否及时采取妥当的保全措施。
				会计核算和账务处理差错。	会计处理严格遵循有关会计准则，通过系统自动进行会计核算和账务处理；定期对账并及时纠错，确保账账相符、账实相符。	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	调阅会计凭证、银行间往来报文；查看业务系统、会计系统等系统数据和实物单证，检查是否账账一致、账实一致；调阅与账户行、客户、银行内部的对账记录，查看是否定期开展对账，并及时纠错。
				费用收取不符合规定。	严格执行监管规定和银行内部规定收取相关费用。	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	调阅相关业务资料和收费凭证，调阅费用减免授权文件和审查审批资料，对照制度规定和授权文件，查看是否按照规定或批复的项目、费率和收费时机进行收费。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
6.6 贸易融资	6.6.1	业务受理	确保业务资料齐全，协议文本规范	a)借款人不具备主体资格；	a)严格审核借款人主体资格，确保营业执照、贷款卡等有效，视具体业务还应取得必要的许可和批复，借款人主体还需满足行内管理制度相关要求；	《贷款通则》《商业银行授信工作尽职指引》《流动资金贷款管理暂行办法》《商业银行表外业务风险管理指引》	调阅融资业务档案，检查借款人的营业执照、贷款卡等证明其主体资格的文件，确认其真实有效性。
				b)业务资料不全、协议条款文本不规范；	b)根据统一的操作规程受理业务，确保业务办理前资料齐全；使用统一的业务申请书和协议文本，非格式文本经法律部门审定后使用。	《贷款通则》《商业银行授信工作尽职指引》《流动资金贷款管理暂行办法》《商业银行表外业务风险管理指引》	查阅各类贸易融资业务管理办法，调阅融资业务档案，核对业务所需资料是否齐全；检查协议文本是否按规定格式签署，非格式文本是否经法律部门审查。
	6.6.2	审查审批	遵循审贷分离、分级审批原则，确保交易背景真实，有效控制风险	a)贸易背景不真实或存在交易未履约记录；	a)严格审查客户提供的合同等贸易资料，综合研判过往履约记录和交易习惯	《贷款通则》《商业银行授信工作尽职指引》《流动资金贷款管理暂行办法》《商业银行表外业务风险管理指引》	调阅融资业务档案，查阅各类贸易融资业务管理办法和流程；了解银行核实贸易背景和履约情况的标准和方法；查阅证实贸易背景的资料，通过审核运输单据、报关单、增值税发票等资料佐证贸易背景的真实性，查阅申请人以往交易记录，核实实际履约情况；查阅审查报告对贸易背景是否发表审查意见。
				b）信用审查不严；	b）应从政策风险、行业风险、企业经营风险、担保能力等角度对贸易融资业务的信用风险进行审查，出具审查意见。	《贷款通则》《商业银行授信工作尽职指引》《流动资金贷款管理暂行办法》《商业银行表外业务风险管理指引》	调阅融资业务档案，查阅各类贸易融资业务管理办法和流程，了解融资比例控制要求；调阅审查报告，检查是否全面分析评价融资业务风险，授信额度的使用是否合理，担保是否足值有效。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
				c)融资额度、期限、利率费率等设定与贸易背景不匹配；	c)应根据贸易合同以及融资产品特点、信用审查结论等，合理设定融资金额、期限以及利率、费率等要素	《贷款通则》《商业银行授信工作尽职指引》《流动资金贷款管理暂行办法》《商业银行表外业务风险管理指引》	查阅融资产品管理办法，调阅融资协议和对应贸易合同；查看融资额度是否超过规定比例甚至合同金额，查看融资期限是否超过规定时间，是否和贸易背景相匹配，融资利率和费率是否在规定范围内，减免是否合规。
				d）调查、审查、审批未有效分离，审批人未经授权或超授权审批；	d）应根据贷审分离、分级审批的原则，建立规范的贷款评审制度和流程，确保风险评价和信贷审批的独立性。应建立健全内部审批授权与转授权机制，审批人员应在授权范围内按规定流程审批贷款，不得越权审批。	《贷款通则》《商业银行授信工作尽职指引》《流动资金贷款管理暂行办法》《商业银行表外业务风险管理指引》	查阅贸易融资制度、流程和岗位职责，查阅业务调查、审查、审批记录，核实岗位是否相互分离，是否均独立发表意见并记录于审批表或审批系统内；对照审批人的授权文件，查看该业务是否在其授权范围内，若超过授权是否有特别授权文件；符合集体审议条件的，是否按照制度规定进行集体审议，并保留审议结论。
	6.6.3	贷后管理	有效开展融资后检查，控制风险隐患	a)实际融资用途与约定不符；	a)严格执行受托支付有关规定发放贷款后，持续跟踪贷款资金流向，防止贷款资金被挪用；	《贷款通则》《商业银行授信工作尽职指引》《流动资金贷款管理暂行办法》《商业银行表外业务风险管理指引》	调阅借款合同等融资协议、贷后检查报告和同期资金往来明细，检查借款人实际使用贷款资金的合规性，是否符合协议约定。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
				b）未定期开展融资跟踪监控；	b)应关注客户经营活动和交易进展情况，加强对物流、单据流、资金流的跟踪监控，对融资担保情况进行追踪调查和检查。	《贷款通则》《商业银行授信工作尽职指引》《流动资金贷款管理暂行办法》《商业银行表外业务风险管理指引》	查阅各贸易融资产品的管理办法和流程，是否对贸易融资还款来源有控制要求；查阅贷后检查报告，是否定期开展跟踪监控，是否关注客户经营活动及风险，是否关注交易进展并控制资金回笼，是否关注贸易背景相关的汇率、商品价格波动，对于风险或潜在风险是否及时预警并采取有效控制措施。
6.7 投资银行	6.7.1	银团贷款	全面有效审查、审批银团贷款风险	a）银团贷款审批超授权；	a）投资银行业务部门根据申请对项目进行审批，各级审批权限在审批系统中严格设定。项目评审委员会的主要职能是负责评价、审议需协调或审批的投资银行项目；	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	抽查银团贷款审批程序及授权书，检查授权制度执行情况，确认是否有超授权现象。
				b）未履行信用风险审批职责；	b）对于承担声誉风险和信用风险的业务，应按规定履行审查审批程序。投资银行业务与关联的融资业务应分别按照各自的业务流程独立地进行审批；	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	抽查银团贷款审批程序及授信情况，检查信用风险制度执行情况，确认是否有超授信现象。
				c）银团贷款档案管理不规范。	c）银团贷款协议签署后，融资顾问工作及银团贷款筹组过程中的各项有效文件统一管理，具体文件包括：基础资料类、协议类、报批类、服务类。	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	抽查银团贷款档案，检查档案的完整性。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
	6.7.2	信贷资产转让	授权、授信额度内审批信贷资产转让业务	a）信贷资产转让申请要件要件不齐备；	a）信贷资产转让申请项目审核时要提供以下要件：申请中应说明拟办理的业务类型、交易对手、交易方式、收益分配等问题，拟签署的资产转让与交易协议及法律意见，拟交易资产的原贷款调查报告，对买断型银团资产转让与交易业务，须提供拟买入资产的信用审批文件；	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	抽查信贷资产转让业务档案，检查档案的完整性。
				b）未履行信用风险审批职责；	b）信贷资产转让业务需开展信用风险审批，与关联的融资业务应分别按照各自的业务流程独立地进行审批；	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	抽查信贷资产转让业务审批程序及授信情况，检查信用风险制度执行情况，确认是否有超授信现象。
				c）信贷资产转让审批超授权。	c）分支机构拟交易的资产转让与交易项目逐级报送，并在授权范围内审批，要按照投资银行业务授权将协议复印件（签署本）、资金往来的会计凭证复印件、系统操作方式等材料上报备案。	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	抽查信贷资产转让业务审批程序及授权书，检查授权制度执行情况，确认是否有超授权现象。
	6.7.3	重组并购	重组并购业务开展有效的立项论证及审批	a）项目未开展立项审查；	a）重组并购项目实施前必须立项审查，建立严密的内部审核工作规则，认真核查各类文件的真实性、准确性和完整性，加强对重大业务的合同与法律文书的审查；	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	抽查重组并购项目的审查审批资料，确认程序的完整性和有效性。
				b）评估人不具备并购交易主评估人及分析员资格；	b）配备符合要求的并购业务从业经验人员，主评估人要具有3年以上并购从业经验。	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	抽查重组并购评估人资质，确认符合监管要求。
				c）项目未经过投资银行项目评审委员会评审。	c）项目评审委员会负责评价、审议需协调或审批的重组并购类投资银行项目。	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	抽查重组并购项目评审记录，确认程序的有效性。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
	6.7.4	常年财务顾问	常年财务顾问执行授权管理，建立监督检查机制	a) 业务审批时越权审批；	a) 商业银行各级机构严格按照审批权限进行审批，对于协议金额超出权限范围的常年财务顾问业务，报有权审批机构审查批准；	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	抽查常年财务顾问业务授权审批情况，确认是否有超授权现象。
				b) 常年财务顾问业务监督检查机制不完善。	b) 商业银行定期开展常年财务顾问业务检查，检查内容包括审批制度执行情况、业务流程规范性、档案管理情况等。	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	抽查常年财务顾问业务档案资料，确认资料的完整性。
6.8 个人存款	6.8.1	开户	商业银行个人结算账户开立管理的合规性。	a)申请人开户资料或身份证明不真实；	a)严格审核个人客户身份和开户资料的准确性真实性、和完整性和合法性，按规定进行身份证件联网核查；	《中国人民银行关于进一步加强人民币银行结算账户、转账、现金支取业务管理的通知》银发[2011]116号 银监会《商业银行内部控制指引》	实地观察个人客户开户时，网点经办人员是否核对存款人身份证件，是否联网核查公民信息；抽查个人开户凭证，检查是否准确记录客户实名制身份信息。
				b)代理人身份不合规；	b)个人客户经理不可为其服务的客户代办业务；营业网点员工不可直接代理客户办理任何金融业务，柜员亦不可为自己办理任何业务。授权人必须审核申请人（代理人）的证件类型、证件号码等相关资料；	《中国人民银行关于进一步加强人民币银行结算账户、转账、现金支取业务管理的通知》银发[2011]116号	调阅客户开户申请书和相关的开户资料，是否记录存款人、代理人身份证件，是否存在银行员工代理开户情况；现场观察网点开户审核是否核对并联网核查存款人、代理人的身份。
				c)开户凭证上无客户签名或签名不正确；	c)柜员须审核开户凭单上的客户签名正确无误；	《中国人民银行关于进一步加强人民币银行结算账户、转账、现金支取业务管理的通知》银发[2011]116号	调阅客户开户申请书或相关协议、凭证，核对客户的签名是否完整、准确。
				d)开户风险提示不充分。	d)柜员须主动向客户进行风险提示，包括：客户与银行间的风险责任；客户要妥善保管个人信息、介质及密码。对大额支取业务应审核客户及代理人身份证件，应按监管要求上报大额交易。	《中国人民银行关于进一步加强人民币银行结算账户、转账、现金支取业务管理的通知》银发[2011]116号	调阅客户开户协议，检查是否有风险提示条款内容，客户是否有签字确认；观察网点开户时，是否向客户进行风险提示，并对大额取款进行身份审核及上报监管。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
	6.8.2	存取款	商业银行个人结算账户转账、现金支取管理的合规性。	a)未能识别假币和伪造的存单、国债、存折等；	a)柜员须提高对现金和存单（折）、国债真伪的甄别能力，对其真实性开展审核；	《中国人民银行关于进一步加强人民币银行结算账户、转账、现金支取业务管理的通知》银发[2011]116号 银监会《商业银行内部控制指引》	实地观察网点人员业务操作是否按规定对现金、存单折进行真实性识别，是否具备反假币证书等上岗必须的资质。
				b)银行打印凭证内容与客户交易内容不一致；	b)业务操作完成后，柜员（授权人）须审核凭证打印输出内容与客户交易内容一致，并在凭单上签章确认；	《中国人民银行关于进一步加强人民币银行结算账户、转账、现金支取业务管理的通知》银发[2011]116号	实地观察网点对个人客户大额存、取款业务的操作，经办人员是否按规定进行账务核对并签章确认。
				c)大额存取款业务未经授权办理。	c)柜员须按权限规定办理存取款业务，大额交易须经授权；授权人须审核申请人（代理人）的证件类型、证件号码等相关资料，同时确认申请人（代理人）在业务办理现场。	《中国人民银行关于进一步加强人民币银行结算账户、转账、现金支取业务管理的通知》银发[2011]116号	调阅大额取款业务凭证，核对是否经有权人审核业务的合规性，是否摘录存款人（代理人）的身份信息。
	6.8.3	挂失	商业银行个人结算账户挂失管理的	a）挂失申请缺失或者挂失申请书内容不完整。	a)柜员受理挂失申请时，须认真审核挂失申请人（代理人）的挂失申请书内容的真实性、完整性，核对客户提供的个人信息、账户信息的准确性，联网核查申请人的身份，确认无误后及时办理挂失手续。	《储蓄管理条例》国务院令第107号	调阅个人业务挂失登记薄，查看挂失申请书内容填写是否完整性，有无客户签章；实地察看挂失办理时，经办人员是否联网核对申请人身份信息；检查系统对挂失账户止付的正确性。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
			合规性。				
				b)未实施换人复核，擅自冻结或解冻客户账户	b)建立复核制度，确保交易的记录完整和可追溯。有权冻结部门持有关公函，文件，通知来银行办理冻结或解冻账户或账户余额业务时，需经银行业务主管人员审核，涉及有关账户余额确实未被冻结或已被冻结的情况下，办理冻结或解冻手续并打印相关记录，专人复核柜员操作结果，同时确认柜员登记的冻结登记簿无误。银行业务主管人员据此在执行通知书等文件回执上签字，加盖业务公章后交执法人员。	《储蓄管理条例》国务院令第107号	调阅冻结登记薄，核对操作是否双人办理。冻结或解冻客户账户是否有充分的理由并符合监管规定；调阅档案资料，看网点是否按规定保留相关材料。
6.9 个人贷款	6.9.1	调查和审查审批	确保银行遵循贷审分离、分级审批原则，开展尽职调	a）个人贷款借款人不符合法律法规或银行规定的资格	a）借款人应具有民事行为能力，借款人应具有还款能力，无不良信用记录；	《个人贷款管理暂行办法》《贷款通则》	查阅个人贷款政策制度和流程，检查制度对借款人资质的要求是否明确；核对借款人是否具有民事行为能力符合法律法规和行内制度规定；核对相关收入证明能否说明借款人还款来源的稳定性；检查借款申请人和担保人的征信报告等是否反映有不良记录。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
			查和合规审查	b）贷款申请资料提供不完整或不真实；	b）应执行面谈制度，调查借款人身份、诚信状况、借款用途、还款来源、担保方式的真实性，收集相关调查资料，应同时调查按揭贷款的开发商、汽车贷款的经销商、消费贷款的收款方等的资格和资信情况；	《个人贷款管理暂行办法》《贷款通则》	检查面谈记录核实是否执行面谈制度；检查客户贷款申请资料，比照具体贷款品种核实调查资料是否完整，是否包括开发商、汽车经销商等证照资料；查阅调查报告或申请审查表，检查调查人员是否对资料完整性真实性进行调查，出具调查意见。
				c）信用审查不严；	c）应对贷款调查内容进行风险审查，关注借款人偿还能力、诚信状况、担保情况、风险程度，全面动态地进行风险评估。	《个人贷款管理暂行办法》《贷款通则》	调阅审查报告或申请审批书，检查审查内容是否包括借款人偿还能力、诚信状况、担保情况、风险程度等，是否明确出具审查意见。
				d)调查、审查、审批未有效分离，审批人未经授权或超授权审批；	d）应根据贷审分离、分级审批的原则，完善授权管理制度，规范审批操作流程，明确贷款审批权限，审批人员应在授权范围内按规定流程审批贷款，不得越权审批。	《个人贷款管理暂行办法》《贷款通则》	查阅个人贷款政策制度和流程与岗位职责，检查业务调查、审查、审批记录，核实岗位是否相互分离，是否均独立发表意见并记录于审批表或审批系统内；对照审批人的授权文件，查看该业务是否在其授权范围内，若超过授权是否有特别授权文件。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
	6.9.2	发放和支付管理	确保贷款发放及时准确，支付用途符合实际	a）个人贷款未经贷款有权人审批即与借款人签订借款合同；	a）应根据有权审批人签署的审批意见书，与借款人及其他相关当事人签订书面借款合同、担保合同和其他相关协议，应采用统一格式文本，合同要素应当明确，且与审批意见书一致。	《个人贷款管理暂行办法》《贷款通则》《合同法》	检查借款合同的签订时间与审批意见书的出具时间，分析是否存在审批前已经签订合同的情况；检查借款合同及其他相关协议，是否为统一格式文本，是否存在要素不一致；检查借款合同内是否按照审批意见书增加了或落实了贷款发放的前提条件和支付管理条款。
				b)未落实抵押担保等前提条件即发放贷款，会计核算不准确；	a）应落实独立的放款部门或岗位，负责落实放款条件。应规范担保流程，加强对抵押或保证的核保。应按照银行统一规定进行贷款业务的会计核算。	《个人贷款管理暂行办法》《贷款通则》	查阅放款部门或岗位的职责，检查是否设立独立的放款部门或岗位；检查个人贷款档案，分析是否在放款前落实担保等放款条件；检查担保手续是否齐全有效。检查贷款科目选择、还款方式、计息设定等是否符合会计核算规范。
				c)未执行个人贷款支付管理要求；	c）个人贷款资金采取受托支付方式的，应审核支付用途的证明材料和具体支付对象，检查借款借据和支付凭证是否与其保持一致。采取借款人自主支付方式的，必须符合银监办法规定的条件，并要求贷款人定期报告或提供贷款资金使用情况。	《个人贷款管理暂行办法》《贷款通则》	检查个人贷款受托支付管理制度和流程；查看借款合同、放款凭证及贷后管理资料，核对个人贷款是否执行受托支付，支付对象和金额是否准确，未执行受托支付是否符合自主支付条件，是否补充提供资金支付凭证或使用报告。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
	6.9.3	贷后管理	全面及时开展贷后检查，确保资金安全	a)贷后检查未按要求进行；	a） 应采取有效方式对贷款资金的使用、借款人的信用及担保情况变化等进行跟踪检查和监控分析	《个人贷款管理暂行办法》《贷款通则》	查阅检查监测报告，是否对借款人资信状况、履约情况、担保情况、按揭项目的进展情况等相关内容进行定期监测和检查；发现风险是否进行预警并采取风险控制措施。
				b）未执行贷款风险分类并足额 计提拨备；	b)对零售贷款如自然人主要依据贷款逾期时间长短直接划分风险类别。应当按照谨慎会计原则，合理估计贷款可能发生的损失，及时计提贷款损失准备。	《贷款风险分类指引》《银行贷款损失准备计提指引》	查阅个人贷款分类制度和风险拨备制度；检查个人贷款风险分类划分标准和结果是否合规；检查风险拨备的计算方法是否符合制度规定；检查贷款风险拨备的计提、转回、冲销等核算是否符合制度规定。
	6.9.4	不良贷款管理	确保不良贷款及时催收；贷款核销流程合规	a)对个人贷款不良贷款未按要求管理；	a） 应根据风险分类结果制定逾期催收、违约清收、不良贷款转化处置等管理措施，仍未归还的应通过诉讼、抵押物拍卖、以物抵债等方式进行资产保全；	《个人贷款管理暂行办法》《贷款通则》	检查个人不良贷款管理制度和流程；检查不良贷款的催收记录，分析是否按规定对借款人及保证人进行催收；对于催收无效仍未收回的贷款，是否在规定时限内进行诉讼、处置抵押物、以物抵贷等其他保全措施。
				b)个人贷款核销未按规定办理；	b） 个人贷款呆账核销须限定核销范围、保证手续要件齐备，贷款经办行申报核销前，必须查清贷款损失形成原因、明确责任认定与追究。个人贷款呆账核销按“尽职追索、逐户组卷、逐级审查、集体审核、授权审批”的程序进行。核销完成后，还需账销案存，继续追收，最大限度减少损失。	《个人贷款管理暂行办法》《贷款通则》	检查个人贷款核销制度和流程；检查不良贷款核销报告，分析是否进行了责任认定，核销是否进行了逐级审查、集体审核，是否存在越权行为。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
6.10 信用卡	6.10.1	审批与开户	商业银行规范银行卡发卡行为，落实银行卡账户实名制，有效控制信用卡发卡风险。	a)申请人身份不真实或提供资料不实；	a)经办人员对申请办卡资料进行审核。个人申请办卡的，需提供身份证件复印件影像材料及其及其他相关证明材料；企业申请办卡的，需提供《开户许可证》、组织机构代码证书、经过年检的营业执照副本的复印件，并加盖公章；审核开卡申请的其他资料的真实性	《中国人民银行中国银行业监督管理委员会公安部国家工商总局关于加强银行卡安全管理预防和打击银行卡犯罪的通知》银发[2009]142号	调阅客户开卡申请书和相关的资料复印件，核对经办人员是否联网核查个人客户的公民身份信息并留有记录；对于代理开卡的，检查是否同时核对代理人的真实身份并记录，单位卡的相关资料是否有经办人员的审核签章。
				b)申请人存在信用不良或其它不良记录；	b)银行应建立资信调查与资信审查制度，对信用卡申请材料出现疑点信息或系统审核记录缺失等情况的，不得核发信用卡。	《中国人民银行中国银行业监督管理委员会公安部国家工商总局关于加强银行卡安全管理预防和打击银行卡犯罪的通知》银发[2009]142号 《商业银行信用卡业务监督管理办法》银监会令2011年第2号	调阅发卡机构的资信调查记录，检查其是否逐户查询人民银行征信系统、中国银联银行卡风险信息共享系统等，分析申请人的资信状况；检查是否存在向具有不良信用记录的申请人发卡的现象。
				c)未经本人或本单位同意申办信用卡；	c)申请材料必须由申请人本人亲自签名，不得在客户不知情或违背客户意愿的情况下发卡。发卡银行受理的信用卡附属卡申请材料必须由主卡持卡人以亲自签名、客户服务电话录音、电子签名或持卡人和发卡银行双方均认可的方式确认。	《中国人民银行中国银行业监督管理委员会公安部国家工商总局关于加强银行卡安全管理预防和打击银行卡犯罪的通知》银发[2009]142号 《商业银行信用卡业务监督管理办法》银监会令2011年第2号	调阅发卡机构的发卡前资信调查记录，检查是否执行新发卡的亲访亲签并留有记录。访谈了解发卡机构是否存在信用卡发卡营销业务外包的现象。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
				d)对高风险人群发卡。	d)银行设立独立审批人，根据开卡人的综合资信状况，职业，收入水平等因素对个人资信进行审查，授予信用额度。超过审批人批准限额部分报上一级分管领导审批。对符合高风险特征的人群，审慎发卡。	《银行卡业务管理办法》银发[1999]17号 《中国人民银行中国银行业监督管理委员会公安部国家工商总局关于加强银行卡安全管理预防和打击银行卡犯罪的通知》银发[2009]142号	调阅发卡机构的银行卡授信审批制度，检查是否按不同层级进行设置不同的的授权权限和授权限额。调阅大额授信、高风险人群的开卡审批记录，检查开卡机构是否按监管要求谨慎发展无稳定工作、收入的客户群体，从严授信。
	6.10.2	卡片管理	商业银行规范银行卡内部制卡和客户卡片启用流程，有效防范操作风险。	a)空白卡保管不严；	a)坚持定期、不定期查库，定期轮岗。严密领用、使用过程交接手续；	《银行卡业务管理办法》银发[1999]17号	调阅发卡机构的银行卡卡片的交接登记、查库记录等，调阅银行卡制卡点人员的轮岗记录，检查是否定期查库与轮岗。
				b)制卡岗位未做到岗位分离，制卡过程存在操作风险；	b)制卡员应保持相对稳定，与密码信封管理岗、空白卡保管岗岗位分离。设立专用机房，制卡在监控下进行，专人负责，人离上锁；打卡机应加密上锁；微机应设置密码；设立打卡机登记簿和运行日志；	《商业银行信用卡业务监督管理办法》银发[2011]2号	调阅银行卡发卡机构人员的岗位设置及职责，检查是否做到关键岗位相分离；实地观察制卡工作现场，检查是否存在兼岗、混岗、串岗的情况，评价发卡机构的制卡环境和人员操作是否符合内控要求。
				c)打卡、打密数据信息泄露；	c)制卡员、打密员应在制卡和打印密码信封后立即删除制卡、打密信息；制卡数据的保留时间不得过长。商业银行经营信用卡业务，应当依法保护客户合法权益和相关信息安全。未经客户授权，不得将相关信息用于本行信用卡业务以外的其他用途。	《银行卡业务管理办法》银发[1999]17号	实地观察制卡工作现场，制卡、打密人员是否在工作完成后及时删除相关信息，调阅系统记录，检查是否遗留未及时删除的客户制卡信息、密码数据；系统是否有外接设备（USB等）向外转移客户相关信息的痕迹。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
				d)非本人启用信用卡。	d)建立信用卡激活操作规程，激活前应当对信用卡持卡人身份信息进行核对。不得激活领用合同（协议）未经申请人签名确认、未经激活程序确认持卡人身份的信用卡。	《银行卡业务管理办法》银发[1999]17号 《商业银行信用卡业务监督管理办法》银监会令2011年第2号	访谈了解营业网点对客户新卡启用的核对流程，检查是否允许代理启用信用卡；实地观察电话银行客服对客户电话启用信用卡的审核过程，并调取部分系统记录或业务的电话录音，检查是否认真核对客户信息后启用新卡。
	6.10.3	交易监控	商业银行落实银行卡交易监测，强化特约商户管理，有效防范套现的信用风险。	a)未对信用卡异常交易进行监测并采取适当措施；	a)银行应建立持续监测记录和追踪预警异常业务行为（含入侵事故或系统漏洞）的流程并认真执行。对信用卡日常交易开展系统监测，对异常交易开展实时调查，必要情况下采取止付、降额等处理措施；	《中国人民银行中国银行业监督管理委员会公安部国家工商总局关于加强银行卡安全管理预防和打击银行卡犯罪的通知》银发[2009]142号 《商业银行信用卡业务监督管理办法》银监会令2011年第2号	查看发卡机构建立的银行卡交易监测系统和持卡人主体交易信息数据库，检查是否实施风险防控。检查发卡机构是否建立大额、可疑交易信息监测和报送制度，是否对相关记录的信用卡、持卡人跟踪，后期发卡机构是否采取了与持卡人联系确认、调整授信额度、紧急止付等措施。
				b)未对信用卡套现交易进行监测并采取适当措施。	b)强化日常交易监控力度，规范用卡行为，严禁持卡人参与信用卡套现或为他人提供套现便利。采取切实措施防范收单风险，严格执行特约商户的准入条件，认真审核查访商户的资信状况，并落实特约商户的巡查巡访制度。加强特约商户的日常管理，关注商户的交易行为，对存在疑似套现或确有受理伪卡、盗录信息、欺诈交易等的特约商户，及时采取切实有效的处置措施。	《中国人民银行中国银行业监督管理委员会公安部国家工商总局关于加强银行卡安全管理预防和打击银行卡犯罪的通知》银发[2009]142号	调阅商业银行建立的特约商户现场检查和非现场监控制度，检查收单机构是否落实对特约商户的准入机制和定期现场检查制度；调阅银行对特约商户的监测、检查记录，检查是否对相关套现人员或商户进行停止银行卡业务等对应处置，并及时将信息报告银联银行卡风险信息共享系统。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
	6.10.4	透支管理	商业银行建立并有效执行信用卡业务风险管理制度，合理催收。	a)对透支款逾期的客户未能及时提醒、催收；	a)对于逾期客户，按照透支逾期期限的长短采取短信提醒、电话提醒、信函催收、上门催收、司法催收等不同催收措施；	《商业银行信用卡业务监督管理办法》银监会令2011年第2号	调阅发卡机构的信用卡欠款催收管理制度，检查信用卡透支逾期的客户记录，是否建立对应的催收记录，是否按催收政策和客户的逾期天数，采取相应的催收措施。
				b)合作催收管理不规范，客户信息外泄。	b)信用卡合作催收单位应符合准入条件，按照监管机构外包风险管理指引，做好日常检查辅导工作，与外包方签订客户信息保密合同，并跟踪验证合作催收效果。	《商业银行信用卡业务监督管理办法》银监会令2011年第2号	调阅信用卡合作催收的合约，检查发卡银行是否对催收人员采用以欠款回收金额提成的考核方式；检查合作方的风险管理条款是否涵盖对催收过程中获取的银行客户信息进行保密的内容和违约责任。实地观察双方来往数据的交接过程是否符合保密规定。
	6.10.5	额度调整	商业银行建立并有效执行信用卡的额度管理。	a)对不符合调额信用条件的客户调整信用额度，或调额不符合信用政策规定；	a)审批人员根据客户的历史用卡情况、其他资信状况及其所申请的额度综合考虑调额比例，并对客户调额目的进行联系确认后开展调额。发卡银行应当建立信用卡授信管理制度，根据持卡人资信状况、用卡情况和风险信息对信用卡授信额度进行动态管理。	《商业银行信用卡业务监督管理办法》银监会令2011年第2号	调阅发卡机构信用卡授信管理制度和调整信用卡额度的记录，检查是否存在不符合调额要求而放大授信的情况。
				b)超权限调额。	b)银行设定调额条件、调额标准和调额权限，由独立审批人审批。超过调额权限的要报上一级审批人员审批。	《商业银行信用卡业务监督管理办法》银监会令2011年第2号	调阅发卡机构调整信用卡额度的记录，检查是否存在超出既定权限的放大授信的情况，检查已调整信用额度的记录中，是否有审批人员的签批意见。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
	6.10.6	交易清算	商业银行遵循信用卡的清算规则并有效执行。	a)垫款业务未经过审批；	a)如出现业务垫款，按金额大小逐级审批后方可办理；	《银行卡业务管理办法》银发[1999]17号	检查收单机构的其他应收款或垫款账户，检查是否存在业务垫款，已发生的垫款审批是否经有权人签字。
				b)清算不规范不不准确。	b) 记账人员认真审核凭证，记账后有专人开展事后监督。	《银行卡业务管理办法》银发[1999]17号	访谈银行卡清算业务处理人员，了解其日常操作的流程，检查对清算中差错的处理方式是否规范。调阅事后监督记录，检查银行卡交易记录是否纳入监督范围。
	6.10.7	卡片挂失	商业银行银行卡挂失处理的有效性、合规性。	a)申请挂失的客户证件无效，签名不符或未签名。	a)柜员必须严格审查客户提交的身份证件，确保证件的真实、有效。个人代办挂失业务时，代办人须持本人和持卡人身份证原件办理。《业务申请书》内容填写正确、完整；必须有客户签名，代办业务还需登记代办人和持卡人身份证件类型、号码、发证机关；对于通过核实的持卡人信息，应注明已核实内容。持卡人的证件丢失，本人提供相关证明办理挂失，如代办挂失，则注明相关情况办理。	《商业银行信用卡业务监督管理办法》银监会2011年2号	调阅发卡机构的挂失记录，检查资料是否填写要素完整、准确，客户签字是否正确，是否及时止付挂失银行卡；需要核证的，是否有银行人员的核实记录。
				b)持卡人未委托代办挂失。	b) 卡片挂失时，代办人须持本人和持卡人身份证原件办理挂失。密码挂失及补换卡业务必须确认为本人办理。	《商业银行信用卡业务监督管理办法》银监会2011年2号	调阅发卡机构的挂失记录，检查资料填写是否完整、准确，代理人身份是否有效，是否由银行人员核实客户身份后办理挂失新开银行卡。
	6.10.8	拒付调单	正确处理调单业务。	a)拒付调单未在规定时间内查询答复。	a)业务主管不定期检查，对查询查复业务存在的不足及时纠正，防范因拖延时间超过拒付期限而形成损失。	《银行卡业务管理办法》银发[1999]17号	调阅银行卡查询查复记录，检查目前未处理的记录中最早的日期是否合理；调阅客户投诉记录，检查是否存在超出拒付查付期限，造成损失的情况。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
				b)外卡调单业务未及时、准确处理。	b)外卡调单时，清算部门审核客服部门提交的客户拒付申请，查询交易明细后判断处理方式。不需要调单的申请，直接进入一次拒付。需要调单的申请，调阅并审核单据，获取持卡人答复。如单据不复核要求或持卡人否认，则向国际组织提出争议；如单据复核要求，且持卡人确认，则进行清算。	《银行卡业务管理办法》银发[1999]17号	调阅银行卡查询查复记录，检查相关处理是否及时；调阅客户投诉记录中是否存在超出拒付查付期限，造成损失的情况。
	6.10.9	坏账核销	严格坏账核销处置，控制操作风险。	a)坏账核销未经过适当审批。	a)坏账款项的核销需要经过逐级审批，按一定条件实行核销。	《银行卡业务管理办法》银发[1999]17号	调阅已核销的信用卡坏账，检查已提供的核销资料是否符合核销政策，核销金额是否经有权人审批。
				b)核销客户信息未录入黑名单系统，或未进行账销案存管理。	b)应将客户信息录入黑名单系统，应实行账销案存、继续追索。	《银行卡业务管理办法》银发[1999]17号	调阅已核销的信用卡坏账，检查是否按账销案存的要求进行管理。
6.11 私人银行		私人银行	私人银行客户准入标准明确，产品信	a) 私人银行客户准入、交易委托未经过适当权限审批；	a) 客户准入需经过适当的审批，金融资产符合准入标准，对暂不符合准入标准，但客户的金融资产丰富、资质良好的客户可以发展为私人银行客户，但需要报有权人审批并备案，客户委托交易需进行客户有效授权并经有权人审批；	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	调阅私人银行管理制度，抽查私人银行客户准入审批表，检查是否有相关权限人签字审批。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
			息披露充分	b）未将私人银行销售产品信息及风险充分告知客户；	b）客户经理、财富顾问和投资顾问根据客户风险等级向客户推介与其风险属性相匹配的理财产品，并全面准确地揭示产品风险。对于非保证收益型私人银行产品，严禁做出任何形式的收益承诺。对于市场风险较大特别是与衍生交易相关的投资产品，客户经理、财富顾问和投资顾问不应主动向无相关交易经验或经评估不适宜购买该产品的客户推介或销售。风险评估结果显示客户不适宜购买某产品但客户仍坚持要求购买的，须要求客户在产品说明书或其他销售文件上完整抄录风险提示并签字；	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	抽查产品销售流程、相关合同等，查看客户风险评估相关资料，检查客户风险揭示资料及风险披露是否充分有效。
				c）未对产品基础信息开展尽职调查并经过独立风险评估。	c)私人银行客户投资项目在授权范围内审查审批，对私人银行销售的产品开展现场调查、文件资料的审查、当事人的访谈、第三方调查、关联情况分析评价等尽职调查，对产品的风险、收益进行综合评价，做出独立的风险评估。	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	调阅私人银行产品的风险评估报告，检查是否对产品基础信息尽职调查并经过独立风险评估。
6.12 资产托管	6.12.1	托管账户开立	托管账户独立建账，分账管理	a）账户设置不符合监管部门要求及协议规定；	a）办理托管业务应开展合规检查，严格按照制度规定审核开户资料，严格按授权规定签订托管协议，规范开立和管理托管账户，按规定使用和保管托管业务印鉴，监督投资运作；	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	调阅开户的相关资料，检查是否对托管资产的开户开展尽职调查，并签订开户协议。
				b）托管资产不独立。	b）受托托管资产应与自有资产及托管的其他资产相互独立，对不同委托人的资产、同一委托人托管的不同产品分别建账、独立核算、分账管理（委托人有特殊要求的除外），确保不同托管资产的相互独立。	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	调阅开户资料，检查是否按照托管资产单独开立托管专户，确保不同托管资产的相互独立。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
	6.12.2	托管账户监控	监督托管账户投资范围	未监控托管资产的投资范围、投资比例、投资限制。	通过在系统中设置监督指标对交易进行监督控制，通过交易监督系统和手工相结合的方式对法规和托管合同约定的比例和非比例方面的要求进行全面监控。	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	调阅托管账户监控记录，确认监控内容是否涵盖了托管资产的投资范围、投资比例和投资限制，查看相关监控的违规情况是否向委托人提交提示函，并执行监管规定。
	6.12.3	托管账户资金清算	资金清算与核算岗位分离	a）托管业务资金清算不规范；	a）资产托管业务资金清算应按照托管协议和相关制度办理，未经托管承办行授权批准，任何机构和个人不得动用托管账户资金；	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	调阅托管协议及资金清算记录，检查是否按照协议规定有效执行清算。
				b）清算与核算岗位未有效分离。	b）负责办理资金清算的人员与负责估值核算的人员实行岗位分离；资金清算应遵循时效性、合规性、保密性、托管人不垫款原则；建立定期对账制度，确保账账、账证、账实相符。	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	调阅托管业务清算与核算人员清单，确定不相容岗位分离制度执行情况。
6.13 养老金	6.13	养老金	养老金业务不相职务分离，有效防范违约风险	a）受托人与托管人、托管人与投资管理人未有效分离；	a）同一企业年金计划中，受托人与托管人、托管人与投资管理人不得为同一人；建立企业年金计划的企业成立企业年金理事会作为受托人的，该企业与托管人不得为同一人；受托人与托管人、托管人与投资管理人、投资管理人与其他投资管理人的总经理和企业年金从业人员，不得相互兼任。建立养老金业务授权管理制度，对超授权业务逐级进行审批管理，制定规章制度和操作流程，明确岗位职责，对从业人员进行职业道德教育，防止养老金信息错误、损失或泄露等风险；	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	调阅养老金计划及协议，确定受托人与托管人、托管人与投资管理人分离控制的执行情况。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
				b）未防范受托管理的违约风险。	b）办理受托管理业务要防范其他管理人的违约风险，在业务实际运营中，严格监督其他管理人的履约情况；办理账户管理业务要确保按签订的备忘录或合同约定的业务处理时效进行各项业务操作和信息传递。	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	调阅养老金管理的管理人违约记录，访谈相关业务人员，检查违约风险的控制情况。
6.14 贵金属	6.14.1	实物贵金属	有效控制实物贵金属借贷的市场风险	a）实物贵金属原料准备存在市场风险；	a）品牌金的原料的准备主要采用向境外商业银行借贷的方式，而对于从金交所买入的黄金原料，则采用境外账户黄金对冲的方式锁定黄金原料的价格，避免黄金原料因市场价格变动而遭受损失；	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	调阅实物贵金属借金台账，查看贵金属借贷中市场风险暴露情况及防范措施，检查相关风险控制情况。
				b）实物贵金属运输、库存管理不规范。	b）实物类贵金属应双人封装入库（箱）、双人保管，调拨手续严密，定期盘点，确保账实相符；应与客户当面核验实物，双方签章、交接手续明晰；建立严密的贵金属运输管理流程和制度。	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	调阅实物贵金属交接登记簿，查看贵金属库存管理、封箱管理情况，检查贵金属实物交接、库存管理的有效性。
	6.14.2	交易类贵金属	提高交易保证金比例，有效控制信用风险	a）客户拒绝提供所承诺的保证金或无力按时和全额偿还所欠的保证金；	a）适度提高客户贵金属延期交易业务保证金比例，并且在节假日期间适用更高的保证金比例；	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	调阅贵金属延期交易保证金收取、垫款明细账，抽查保证金的追缴及信用风险措施是否及时有效。
				b）贵金属报价存在异常；	b）完善金交所系统和网银等交易系统的衔接，加强交易报价的监控；	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	调阅贵金属报价登记簿，抽查贵金属报价的准确性。
				c）自营业务超授权或超过市场风险限额。	c）制定贵金属自营投资业务市场风险限额：投资敞口限额、年度止损限额等，制定交易员授权制度，并监测执行情况，严禁超授权或超市场风险限额。	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	调阅贵金属市场风险限额管理制度及授权管理制度，抽查交易明细，确定自营贵金属交易业务是否有效执行限额管理及授权管理制度。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
	6.14.3	融资类贵金属	加强融资类贵金属信用风险审查审批及监督检查	a）融资类贵金属未开展信用风险审批；	a）建立融资类贵金属信用管理机制，客户需通过系统内的信用等级评定和授信额度核定，单笔业务均需比照流动资金贷款进行审批，应严格抵押手续，核验贵金属实物的权属、规格、成色、重量等；	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	调阅融资类贵金属信用管理制度，抽查融资类贵金属业务授信、抵押等相关程序的执行情况是否执行制度规定。
				b）缺乏贷后检查监督；	b）加强贷后检查监督，比照流动资金贷款要求明确信贷作业监督岗位职责，贷款资金不得用于证券、期货和金融衍生品交易以及其他违反国家有关规定的用途；	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	抽查融资类贵金属贷后的检查监督报告及相关措施落实情况，是否有效监督了资金流向，是否违反相关制度规定。
				c）贵金属价格变动造成抵押率不足。	c）持续监控贵金属价格，规范处置并适时增加抵押物等。	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	抽查抵押物的抵押是否随贵金属价格变动及时增加，避免抵押不足。
6.15 理财	6.15.1	资金募集	理财产品销售环节充分揭示风险	a）理财产品宣传和销售风险揭示的不足；	a）商业银行总行统一管理和授权理财产品宣传销售文本，全面、客观反映理财产品的重要特性和与产品有关的重要事实，不得虚假记载、误导性陈述或者重大遗漏。理财产品宣传销售文本中出现表达收益率或收益区间字样的，应当在销售文件中提供科学、合理的测算依据和测算方式。理财产品销售文件应当包含专页风险揭示书；	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》 《商业银行理财产品销售管理办法》（银监发[2011]5号）	抽取理财产品，调阅理财产品宣传资料，确认是否有歧意性、误导性描述；风险提示是否到位；收益率及测算的相关说明是否合规。检查理财产品实际投资范围、投资资产种类和各投资资产种类的投资比例是否与销售文件相符。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
				b）产品客户适合度评估机制不完善；	b）商业银行销售理财产品，应当遵循风险匹配原则，禁止误导客户购买与其风险承受能力不相符合的理财产品，销售人员除应当具备理财产品销售资格。商业银行应当根据风险匹配原则在理财产品风险评级与客户风险承受能力评估之间建立对应关系；应当在理财产品销售文件中明确提示产品适合销售的客户范围，并在销售系统中设置销售限制措施。商业银行应当在客户首次购买理财产品前在本行网点进行风险承受能力评估；	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》 《商业银行理财产品销售管理办法》（银监发[2011]5号）	调阅客户适合度评估管理办法，检查产品适合度评估机制是否完善，访谈客户经理，检查是否按照风险匹配原则向客户推荐理财产品。调阅理财产品购买交易相关档案资料及客户评估报告，检查客户风险类型与所购买理财产品风险类型是否匹配。
				c）客户投诉处理机制不健全。	c）商业银行应当建立全面、透明、快捷和有效的客户投诉处理体系，有专门的部门受理和处理客户投诉。客户投诉处理机制至少包括处理投诉的流程、回复的安排，调查的程序集补偿或赔偿机制。商业银行应为客户提供合理的投诉途径、确保客户了解投诉的途经、方法及程序，采用统一的标准，公平和公正的处理投诉。商业银行应配备足够的资源，确保客户投诉处理机制有效执行。	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》 《商业银行理财产品销售管理办法》（银监发[2011]5号）	调阅理财产品投诉处理相关制度，了解是否明确部门和专人负责客户投诉处理，是否配备足够的资源确保客户投诉处理机制的有效执行。抽查投诉记录资料，对有关理财业务责任人处罚、处分记录资料等，确认客户投诉机制是否得到有效执行，客户投诉得到有效的处理，声誉风险得到有效控制。
	6.15.2	投资运作	理财产品投资运作与自营业	a）未实行岗位分离控制；	a）理财业务与自营业务分离。理财业务应遵循前台销售、中台投资与风控、后台核算估值的三分离原则。负责投资管理的部门也应实行投资交易、运行风控等岗位分离；	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	调阅理财业务职责分工，访谈理财业务销售、投资运作和核算估值相关的业务部门，抽查交易明细，了解理财业务前、中、后台的分离执行情况。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
			务有效分离，实施投资比例管理	b）未遵循投资比例管理；	b）对信托公司融资类银信理财合作业务实行余额比例管理，理财产品资金投资于高流动性、本金安全程度高的存款、债券等产品实行比例管理。理财资金用于向单一借款人及其关联企业发放融资的总额实行比例管理；	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	调阅投资明细，访谈相关部门，确定理财产品余额占银信理财合作业务比例情况，判断合规性。
				c）投资超越监管范围，缺乏投资品管理机制；	c）理财资金投资范围符合监管规定，建立相应的风险管理体系和内部控制制度，严格实行授权管理制度，建立投资品的审核、审查机制；	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	调阅产品成立及到期报告、投资组合运作报告和投资品管理报告，确定投资范围的合规性。
				d）未遵循公允价格交易以及价格验证工作缺失。	d）理财业务与银行自营业务之间要建立防火墙，实行风险隔离，采取公允价格交易，避免产生利益输送的交易行为。理财产品之间的交易应依法合规，采取公允价格交易，避免产生不同产品之间利益输送的交易行为。	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	分析投资品价格变动情况，并与同期市场价格进行对比，确定资金池之间投资品交易价格的公允性，判断是否存在资金池间进行利益输送的情况。
	6.15.3	会计核算与	独立核算理财产品，资金清算及时准	a）理财产品未独立核算；	a）商业银行应对每个理财计划单独核算，覆盖资金募集、投资过程、各类标的资产的明细、到期清算的全过程。每个理财计划建立托管明细账。计划终止计算每个理财计划单独兑现的收益；	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	调阅理财产品明细账，查看是否以理财产品为主体，单独建账、独立核算；募集资金划入托管账户后，是否及时建立投资组合，不同的投资组合要严格进行分账管理，独立核算。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
		托管	确	b）理财产品收入核算、资金清算不及时准确；	b）投资管理人要根据按照产品说明书约定的方式支付理财产品承担的销售手续费、托管费、投资管理费、业绩报酬等费用，公允地进行资产管理业务中间业务收入的分配工作。各项手续费应按规定的范围、标准和费率严格收费，并纳入账内核算，防止收费流失。产品募集成立后，销售部门应最晚于产品起息日将募集资金划入指定的理财产品托管账户。投资管理人必须在理财产品申购、赎回、付息及到期的资金兑付日前将兑付款项足额划至清算账户，确保履约；	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	检查理财产品发行结束后，清算后台是否由理财资金清算专户及时准确划至理财资金托管专户，到期清算时间是否及时完成清算，是否实现对投资人赎回日的先期承诺。检查理财产品赎回、付息及到期、提前终止后，清算后台是否由理财资金托管专户划至理财资金清算专户。开户行收到清算后台划来的到期兑付资金（本金及收益）后，是否将资金及时准确划付给投资人。调阅抽样的理财产品的投资明细，检查清算后台对交易对手的资金汇划是否及时准确。
				c）理财产品资金未进行托管管理。	c）理财产品资金必须进行托管，托管机构与运行管理部门定期开展会计核算和估值结果等对账。	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	抽查理财产品托管明细核算记录，确认托管人职责履行情况。
	6.15.4	项目管理	理财项目管理实施信用风险限额控	a）项目管理未实现前中后台分离；	a)理财项目管理应做到前、中、后台相分离，即项目营销、风险审批、投资审批与投资后管理相分离；	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	查阅项目管理相关制度文件，在制度规范层面看项目管理是否实现了前中后台分离；访谈相关部门，并结合现场审计情况，判断项目管理的前中后台管理是否实现分离。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
			制，落实前中后台分离制度	b）项目前提条件不落实或不符合准入标准；	b）理财项目前提条件必须在投资前全部落实和审核完毕。投资监管机构确定风险权重不为零的金融机构债券（不包括次级债券）、非金融企业债务融资工具，信用评级须达到投资级以上。股权投资数额和投资项目应当与现有生产经营规模、财务状况、技术水平和管理能力等相适应，不得用于与主营业务无关的高风险投资；	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	调阅项目档案资料，对照有权部门对项目做出的审查批复，检查项目投资前是否落实了批复中提出的前提条件。
				c）项目未纳入信用风险限额管理。	c）商业银行的董事会或高级管理层应当根据理财计划及其所包含的投资产品的性质、销售规模和投资的复杂程度，针对理财计划面临的各类风险，制定清晰、全面的风险限额管理制度，建立相应的管理体系。理财计划涉及的有关交易工具的风险限额，同时应纳入相应的交易工具的总体风险限额管理。商业银行对信用风险限额的管理，应当包括结算前信用风险限额和结算信用风险限额。商业银行的各相关部门都应当在规定的限额内进行交易，任何突破限额的交易都应当按照有关内部管理规定事先审批。	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	通过查阅理财业务相关制度文件，看针对理财产品建立相应的风险限额管理要求。抽样项目管理情况，理财产品投资金额与信贷融资余额之和是否纳入统一的信用风险限额管理体系。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
6.16 债券投资与交易	6.16	债券投资与交易	债券投资执行授权、授信、限额管理制度	a）债券投资与交易未按规定审批；	a）交易人员根据债券投资决策会议的决议，对债券投资方案进行修订和完善，按照授权权限审批，审批内容主要包括：信用风险审查、投资额度审查、投资策略审查等。制定债券投资与交易的授权规定，明确允许交易的业务品种和单笔最大交易额度等交易权限。未经上级机构批准，下级机构不得开展任何资金交易；	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	调阅债券投资与交易明细账，调阅年度投资计划，授权、授信额度，与债券投资明细相比照，访谈相关项目投资管理情况，检查债券投资与交易的信用风险审查审批、授权制度的执行情况。
				b）未执行市场风险限额管理；	b）银行市场风险限额包括名义限额、止损限额、敏感度限额和 VaR 限额等，根据银行账户和交易账户的划分管理要求，针对不同账户的业务和交易组合，采用不同种类的市场风险限额指标进行管理；	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	访谈了解债券交易策略的制定情况。调阅市场风险限额管理及执行情况，抽查交易系统报价清单，核查报价权重、期限、价格、权限等执行情况。调阅交易系统操作系统日志，抽查交易报价权限系统控制情况。
				c）债券发行体的授信管理不落实；	c）对债券发行主体实行授信管理，开展授信尽职调查并在授信额度内开展债券投资，对金融债券、企业债等涉及信用风险的债券投资，实施信用风险限额管理，开展债券投资后信用风险管理检查；	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	调阅信用风险评估分析报告和尽职调查报告，检查发行主体的信用评级是否符合准入条件，债券投资是否在发行体授信额度内并逐级审批。
				d）债券投资分类不准确。	d）交易人员在进行债券买入时，应根据持有意图确定债券资产的账户分类。交易人员在持有债券期间，根据业务需要或持有意图变化等情况可根据不同的资产账户对已持有的券资产进行账户重分类，并报送资产负债管理委员会审议。	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	查看债券投资交易明细，筛选持有至到期债券出售的交易样本；调阅可供出售债券、持有至到期债券和应收款项类债券的重分类的审批资料及披露资料，确认重分类的审查审批制度执行情况。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
6.17 外汇交易	6.17	外汇交易	外汇交易业务有效执行交易限额、授权授信及不相容职责分离制度	a）外汇交易前、中、后台未分离；	a）开展外汇交易业务应遵循职责分离原则，前台交易或营销、中台价格验证和限额管理等风险控制和后台账务核算、证券结算及资金清算需相互分离，不得由同一部门承担；	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	访谈交易前台、风险管理中台及核算后台，调阅交易明细，了解中台对前台交易的授权交易限额、交易对手的授信额度和交易价格的是否实施了有效监控。抽样复核相关价格验证的客观性、准确性。抽样检查后台核算与清算的执行情况。
				b）办理外汇交易业务的客户未落实信用风险缓释措施；	b）对于按“T+1”“T+2”方式交割的即期、远期外汇交易业务，经办行应落实信用风险管理措施，采取占用客户授信、收取风险保证金等低风险担保措施控制信用风险；	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	与相关部门人员开展访谈，了解对客户的尽职调查程序及步骤，客户专项授信情况和保证金扣收制度。抽查外汇交易业务是否占用客户授信、收取风险保证金或其他担保措施，有效控制业务的信用风险。
				c）未对交易限额、交易对手授信进行有效监控。	c）商业银行应当建立资金交易中台和后台部门对前台交易的反映和监督机制。中台监控部门应当核对前台交易的授权交易限额、交易对手的授信额度和交易价格等，对超出授权范围内的交易应当及时向有关部门报告。	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	询问并抽样验证中台能否对前台交易的授权交易限额、交易对手的授信额度和交易价格的有效监控，能否实现对前台交易的授权交易限额、交易对手的授信额度的实时监控，并对交易价格的公允性进行验证。
6.18 货币市场业务	6.18	货币市场	融资业务处理规范，流动性风	a）融资超授信或超融资额度；	a）审查交易对手信用风险，对单一交易对手的拆出余额不得超过商业银行对其核定的融资专项授信额度，运用系统进行控制；	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	调阅同业拆入、拆出交易明细账，检查交易对手授信及执行情况，判断拆出余额是否超过对其核定的融资专项授信额度。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
		业务	险管理有效	b）未实行流动性风险限额管理；	b）通过明确设定货币市场业务的流动性风险限额或主要账户余额来确保资金流动性；	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	调阅流动性风险的相关管理办法，抽查发生账户透支的明细，检查融资业务流动性限额的执行情况。
				c）融资业务处理不规范。	c）在授权范围内开展货币市场业务，规范操作融资业务的申请受理、审批、协议签署、资金汇划及清算、后续管理等，并纳入系统管理，任何同业融资清算均不得使用现金支付，不得滥用会计科目核算，业务办理后要及时建立从审查至收回全过程的融资情况档案。	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	调阅融资业务受理、审批、协议签署、资金汇划及清算、后续管理的档案，查看授权执行情况及业务处理的合规性。
6.19 衍生品交易	6.19	衍生产品交易	衍生产品交易授权及止损制度完善，有效控制客户及交易对手信用风险	a）申请衍生产品交易客户风险评估不到位；	a）客户首次办理衍生产品交易前，商业银行营业机构应对代客衍生产品交易适合度进行评估。按照评级授信的相关要求对客户履行尽职调查程序，评定客户信用等级并核定衍生产品交易专项授信额度，同时明确专项授信使用条件；	《银行业金融机构衍生产品交易业务管理办法》银监令[2011]第1号	调阅衍生产品交易档案，查看是否有对客户进行风险提示函、风险评估表等相关文件资料，客户是否有书面的签字确认已了解并愿意承担衍生产品的业务风险。抽查衍生产品协议书，检查客户授信及执行情况。
				b）交易授权和止损管理制度不完善；	b）商业银行建立并严格执行授权和止损制度，制定并定期审查更新各类衍生产品交易的风险敞口限额、止损限额、应急计划和压力测试的制度和指标，制定限额监控和超限额处理程序，在因市场变化或决策失误出现账面浮亏时，应当严格执行止损制度；	《银行业金融机构衍生产品交易业务管理办法》银监令[2011]第1号	调阅止损限额及止损制度，以及衍生产品垫款情况，调阅衍生产品公允价值变动清单，检查是否存在超止损限额情况。抽查金融衍生业务代客交易组合限额指标的制定及执行情况。
				c）交易对手信用风险控制缺失；	c）商业银行制定完善的衍生产品交易对手信用风险管理制度，选择适当的方法和模型对交易对手信用风险进行评估，并采取适当的风险缓释措施；	《银行业金融机构衍生产品交易业务管理办法》银监令[2011]第1号	调阅衍生产品信用风险管理制度及执行情况，检查银行对交易对手及客户的信用风险敞口控制及风险控制措施的有效性。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
				d）未定期对未到期金融衍生合约进行公允价值评估。	d）风险管理人员应定期对未到期金融衍生合约进行公允价值的评估，并建立有效的风险监督、控制和报告制度。	《银行业金融机构衍生产品交易业务管理办法》银监令[2011]第1号	访谈了解金融衍生产品的公允价值定期评估流程，包括评估的频率、参考的市场价值、参数的调整等。 抽取部分合约样本测试其在初始确认、后续计量公允价值计量及财务计量的准确性。
6.20 债券承销发行	6.20	债券承销发行	承销发行业务授权审批，有效监测交易情况	a）超授权办理主承销项目；	a）建立承销发行业务授权审批制度，在完成主承销协议本文的法律审查后，对于超出权限范围的主承销项目逐级上报有权人审批；	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	调阅债券投资专项授信审批资料，调阅主承销项目的信用审批文件、授权书，是否存在超授权现象。
				b）债券承销持有比例违反监管规定；	b)债券承销持有比例符合监管规定，承销人员应在缴款日前督促各缴款机构尽快按照指定要求及时缴款，对于行外机构在缴款日未能按时划付募集款的，有权人审批后进行资金垫付。承销人员应按承销协议及相关协议约定向违约机构追索；	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	调阅债券承销发行的申报材料和债券承销余额明细表，判断本行持有比例是否超过监管规定。
				c）未对二级市场交易情况监测。	c）承销人员负责收集并监测承销债券的信用风险情况，并关注预警信息：客户已发行金融债券二级市场交易是否出现重大异常波动，客户信用风险影响已发行的金融债券本息的偿付。	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	调阅监测报告，核实银行是否对承销的债券的二级市场交易情况进行了有效监测。
6.21 运行管理	6.21.1	账户管理	规范人民币银行结算账户管	a)存款人出租出借账户或利用存款账户从事违法欺诈活动；	a)按照操作流程开立账户，严格执行账户开立操作与审批管理相分离的制度，保证新开立账户资料的真实性、完整性和合规性；	人民银行《人民币结算账户管理办法实施细则》、人民银行《支付结算管理办法》、银监会《商业银行内部控制指引》	访谈运行管理部，了解结算账户开立流程的执行情况。调阅结算账户档案，查看相关资料是否符合要求。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
			理业务，加强对银行结算账户的监督管理，确保银行结算账户、内部账户的核算安全。	b)利用签章、票据进行诈骗或从事违法活动；	b) 加强客户预留印鉴管理，严格客户预留印鉴建立、启用和变更环节的审核，加强对预留印鉴的保管，认真核对预留印鉴；	人民银行《支付结算管理办法》、银监会《商业银行内部控制指引》；	访谈运行管理部，了解客户预留印鉴建立情况。查看业务办理现场，对预留印鉴的审核情况。
				c) 利用内部账户、通过内部特种转账业务从事违法活动。	c)加强内部账户和内部特种转账业务管理，内部账户的开立、使用、变更和撤销应遵循统一管理、明晰核算、防范风险、降低成本的原则，对内部特种转账业务实行授权审批管理，加强对内部账户核对和监督检查，确保内部账户管理合规安全。	银监会《商业银行内部控制指引》	访谈运行管理部，理解内部账户的建立和使用情况。调阅相关文件及要求，调阅内部账户的凭证，查看相关内部账户业务的办理是否符合要求。
	6.21.2	会计核算要素管	严格执行“印、押、证”三分管制度，工作人员的名章、	a)冒领、冒用他人权限卡实施从事违规、违法活动；	a) 加强权限卡的申请、审批、使用、变更管理。权限卡密码应不定期更换，严禁随意放置权限卡或转交他人使用；	人民银行《中国人民银行会计基本制度》；银监会《商业银行内部控制指引》	访谈运行管理部，了解权限卡的启用和使用情况，调阅权限卡相关登记簿进行核对。现场访谈查看权限卡的保管和使用是否符合业务管理要求。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
		理	操作密码、权限卡应实行个人负责制，妥善保管，按章使用。	b)利用空白重要凭证与其共同构成支付要件的会计印章、密押机具等从事内、外部违 规、违法欺诈活动。	b)加强对空白重要凭证、会计核算专用印章、密押机具的管理：1) 空白重要凭证及与其共同构成支付要件的会计印章、密押机具等实行分人使用、分开管理；空白重要凭证上不得预先加盖印章备用，内部员工不得为客户代购、保管和传送各类空白重要凭证，重要空白凭证应按规定定期盘点,重要空白凭证的领取、使用要做好登记手续；2) 会计核算专用印章实行“统一管理、分级刻制”的原则，会计核算专用印章领取时做到双人签收、双人领取，使用时做到专人使用、专人负责，保管时做到专匣保管、固定存放、临时离岗、人离章收。3) 密押机具按照重要物品机具进行管理，坚持专人保管、专人负责的原则。	《中国人民银行会计基本制度》附件《中国人民银行有价单证及重要空白凭证管理规定》、《中国人民银行会计基本制度》、银监会《商业银行内部控制指引》	访谈运行管理部，了解“印、押、证”三分管制度执行情况，现场检查会计要素相关登记薄与实际执行情况是否一致。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
	6.21.3	账务组织管理	账务处理及时、准确、安全。	a)业务核算人员未按照记账规则进行操作，引发操作风险；	a) 业务核算人员须严格按记账规则进行操作：1)业务核算人员应严格按照规定的记账规则，正确使用会计科目和会计凭证进行业务核算，发生核算差错应经有权人授权或审批后进行更正；2) 业务核算必须有账有据，及时记账，当日结账，做到账账、账款、账实、账表、账据、账簿、账卡（折）和内外账务等全部相符。	《中国人民银行会计基本制度》	访谈运行管理部，了解账务组织管理情况，查阅相关业务凭证及会计账簿及报表。
				b)未按规定程序办理查询查复业务，引发客户资金风险和商业银行声誉风险。	a)受理司法机关等有权部门查询应符合规定程序；查询查复应做到有疑速查，查必彻底，有查速复，复必详尽。	《中国人民银行会计基本制度》	访谈运行管理部，了解受理司法机关等有权部门查询业务的组织开展情况，调阅相关留存档案资料，查看查询查复相关操作是否符合要求。
	6.21.4	现金业务管理	强化现金业务管理，规避业务风险。	a)现金业务岗位混乱，职责不清；	a) 落实现金业务岗位分离制度，坚持现金业务管库员、记账柜员和授权柜员等岗位分离，做到各司其职，互相制约；	《中国人民银行会计基本制度》《商业银行内部控制指引》	访谈运行管理部，调阅相关文件、岗位职责和管理办法，查看相关岗位设置和人员职责界定是否符合要求。
				b) 现金出入库交接手续不清、现金收付核算不正确，造成现金损失或引发截留案件；	b)加强网点钱箱及现金收付管理，现金收付款应凭合法、有效的凭证办理，坚持先收款后记账、先记账后付款原则，按券别操作，当面清讫，一笔一清，日清日结，现金、实物交接应责任分明、有据可查；	《中国人民银行会计基本制度》《商业银行内部控制指引》	访谈运行管理部，了解现金业务的开展情况。调阅相关文件，现场查看相关现金业务操作是否符合要求。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
				c)金库和自动柜员机（ATM机）管理不当，引发操作风险和道德风险。	c)加强金库和自动柜员机（ATM机）管理。金库管理应坚持金库主任负责制，严格执行业务操作规程，加强金库门锁（密码）管理，现金、实物出入库遵循先入库后记账、先记账后出库的原则，日结日清，确保账账、账实、账款相符，有效控制金库管理风险。加强自动柜员机（ATM机）控制，严格按规定执行业务操作，加强密码和钥匙或其他密钥管理，有效防范操作风险。	《中国人民银行会计基本制度》《中国人民银行会计核算监督办法》《商业银行内部控制指引》	访谈运行管理部，了解金库管理及ATM管理运行情况，现场查看现金出入库及ATM款箱操作是否符合制度要求。
	6.21.5	支付结算管理	加强支付结算管理，防范有由虚假凭证和支付结算错误引发的风险，确保支付结	a)使用虚假凭证引发交易风险，导致客户及商业银行资金损失；	a) 认真审核支付凭证、记载事项、签章等的真实性、完整性、合规性，约定使用支付密码时须校验支付密码；	人民银行《支付结算管理办法》、《中华人民共和国票据法》	现场访谈，查看工作人员对支付凭证的审核要求情况是否符合要求。
				b)违反支付结算原则办理支付结算业务引发客户资金风险和商业银行的声誉风险；	b)办理支付结算应准确、及时、安全，并做到恪守信用，履约付款；谁的钱进谁的账，由谁支配；银行不垫款；	人民银行《支付结算管理办法》、银监会《商业银行内部控制指引》	访谈运行管理部，了解相关业务的开展情况。现场查看账务处理是否及时。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
			算的安全、及时、准确。	c)延迟支付结算，截留挪用客户资金。	c)不得以任何理由压票、任意退票、截留挪用客户资金，不得无理拒绝支付应由银行支付的票据款项，不得拒绝受理代理他行正常结算业务。	《中华人民共和国票据法》、银监会《商业银行内部控制指引》	现场查看账务处理是否正确及时，调阅退票登记薄，检查退票理由是否充分、合理。
	6.21.6	清算管理	建立资金清算事前、事中、事后监督管理体系，确保资金清算安全、及时、准确。	a)资金清算事前、事中、事后的全程管理不到位，未建立清算风险准备金的筹集及使用规则，引发流动性风险；	a)建立清算的风险准备金筹集及使用规则；	《中华人民共和国商业银行法》《商业银行市场风险管理指引》	访谈运行管理部，了解资金清算业务的开展情况。调阅资金清算相关制度和文件，了解业务办理情况是否符合要求。
				b)资金清算过程中人工干预动作过多，引发操作风险；	b)对有疑问的报文按查询查复管理要求进行处理，按照清算对账管理要求进行系统内各级清算机构之间、相关部室之间以及与人民银行、同业机构之间的账务核对，及时处理清算差错；	《中国人民银行关于加强大额支付系统清算管理的通知》；《商业银行市场风险管理指引》	访谈运行管理部，了解资金清算系统功能设置情况。调阅查询、查复登记薄及对账登记薄，检查清算业务处理流程是否符合制度要求。
				c)关键性操作缺乏必要的复核及授权，引发操作风险。	c) 资金清算须在规定的清算时间内统一进行，并实行清算业务录入、复核、授权、对账的分离制度，本外币资金调拨业务应凭资金管理部门及相关前台部门的支付指令办理。	《中国人民银行关于改革联行清算制度的通知》；《商业银行市场风险管理指引》	现场访谈相关业务人员，了解复核、授权制度的建立及业务办理流程，现场查看实际操作是否符合制度要求。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
	6.21.7	参数管理	参数设置及时准确，确保业务顺利开展。	a)参数维护权限责任权限不清晰，维护权限管理、监控不当，造成业务数据非法修改，产生舞弊风险；	a) 参数管理实行统一设计、集中管理原则，健全参数管理制度，按职责分离的方式落实参数变更申请审批，将参数维护、数据录入、监督控制的职能分开。	《商业银行内部控制指引》	访谈运行管理部，了解业务参数设置的情况。调阅相关业务参数岗位设置登记薄，并与实际执行情况进行核对。
				b)系统参数控制变量的设置、维护错误、功能测试不充分，引发系统逻辑风险和商业银行的声誉风险。	b)参数设置应准确完整、安全合规，参数维护应依据有效的业务需求凭据，履行必要的审批手续，严格按岗位流程进行。参数监控应遵循重点监控原则，对参数管理的重要环节和重要参数表进行监控和检查。	《商业银行内部控制指引》	调阅相关业务参数设置的资料及档案，查看参数设置情况。现场访谈参数设置工作人员，检查参数的相关制度执行情况是否符合要求。
6.22 电子银行	6.22	电子银行	加强电子银行业务的风险管理，保障客户及银行的	a) 未对电子银行系统、数据库和应用程序建立授权控制和进入特权制度；未在电子银行系统、数据库和应用程序中采取适当措施保证	a) 商业银行应规范电子银行业务岗位人员设置，按照“事权划分、岗位牵制、权限可控”的原则，为电子银行相关业务系统、数据库和应用程序的用户设置操作权限，并有效实施不相容职责的分解。商业银行应明确电子银行管理、运营等各个环节的主要权限、职责和相互监督方式，有效隔离电子银行应用系统、验证系统、业务处理系统和数据库管	巴塞尔委员会《电子银行业务的风险管理》；银监会《电子银行业务管理办法》	调阅电子银行业务岗位设置及人员分工；检查电子银行业务相关系统、数据库及应用程序的用户设置及相关登记簿或申请表；检查相关业务处理凭证,是否做到关键岗位的职责分离，是否实现重要数据库的有效授权，防范

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
			合法权益，促进电子银行业务的健康有序发展。	不相容职责的分离。	理系统之间的风险。		被篡改或毁损。
				b）开展电子银行服务未采取适当措施对客户身份和授权情况进行认证；未对客户作业权限、资金转移或交易限额实施有效管理。	b）客户注册、变更、注销电子银行服务，商业银行应对客户身份进行审核；个人电子银行注册、变更业务应由客户本人办理，企业电子银行业务应由企业授权办理相应电子银行业务的人员办理；为客户提供电子银行服务，应使用个人身份号码、密码、智能卡、生物测量技术和数字证书等方法对客户身份进行认证。客户使用的身份认证方式应与其办理业务的风险程度相适应，对使用不同身份认证方式的客户设置不同的交易权限和额度权限。	巴塞尔委员会《电子银行业务的风险管理》；银监会《电子银行业务管理办法》	调阅电子银行相关业务政策与流程，检查是否建立客户身份与授权的认证机制；查看客户注册、变更、注销、交易等业务凭证及附件，检查是否对客户作业权限、资金转移或交易限额实施有效管理。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
				c）未对电子银行客户证书实施有效管理，不能促进交易的不可否认性和明确电子银行交易责任；	c）向客户发放的客户证书应作为重要物品管理，商业银行应对其保管、传递、交接、发放等进行准确、及时记载，并进行定期清理；已制作未发放的客户证书在商业银行内部应严格保管和交接，严禁由具有证书解冻权限的柜员保管；证书解冻必须在确认客户已领取证书后才能办理。商业银行应采用适当的加密技术和措施，保证电子交易数据传输的安全性与保密性，以及所传输交易数据的完整性、真实性和不可否认性。	巴塞尔委员会《电子银行业务的风险管理》；银监会《电子银行业务管理办法》；行业领先实践	调阅电子银行业务政策与流程，调阅电子银行物品相关登记簿和空白客户证书实物，客户证书领取单等，检查是否对客户证书的保管、传递、交接、发放建立有效的管理措施并有效实施；询问并查看柜员操作，查看柜员操作日志，了解柜员办理证书冻结、解冻的手续是否合规。评估商业银行采用的数据加密技术是否符合国家有关规定，是否定期开展自查和自评估所使用的加密技术和算法的强度，对加密方式进行适时调整。
				d）未建立业务连续性计划、应急计划和事故处理预案，不能确保电子银行系统和服务的连续可用性；	d）商业银行应制定电子银行业务连续性计划，应充分考虑第三方服务供应商对业务连续性的影响并采取适当预防措施；应制定电子银行应急计划和事故处理预案，并定期进行测试与演练；	巴塞尔委员会《电子银行业务的风险管理》；银监会《电子银行业务管理办法》	调阅电子银行业务连续性计划、应急计划和事故处理预案；调阅相关测试与演练方案及记录，检查是否有效地建立业务连续性计划和应急计划。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
				e）未实施数据交换与转移的有效管理，未采取适当措施确保客户信息与隐私安全；	e）商业银行应控制客户信息的知悉范围，避免无关人员获取客户信息，客户数据的使用不能超越客户允许的范围；不应向无业务往来的机构转移电子银行客户信息；由于业务发展需要向其他机构转移电子银行客户信息应在法律法规或客户许可范围内，并与信息接收机构签订书面保密合同，指定专人监督有关数据使用、保管、传递和销毁；为电子商务提供网上支付平台，应严格审查合作对象，签订书面合作及保密协议，建立有效监督机制；	巴塞尔委员会《电子银行业务的风险管理》；银监会《电子银行业务管理办法》	调阅电子银行业务相关政策与流程，检查是否建立数据交换与转移的控制；访谈电子银行业务人员与外部转移信息情况，调阅电子银行客户信息接收机构签订的保密合同，调阅电子商务合作对象审查相关资料、合作协议及监督管理相关文档，检查是否采取措施保护客户信息与隐私安全。
6.23 代理业务	6.23	代理业务	业务开办符合准入和授权，操作有规可循，资金实现专户管理，资金支付严格管理、	a）开办代理业务未满足相关准入要求，未取得有关主管部门核准的机构资质、业务人员从业资格及商业银行内部的业务授权；未建立对合作方的准入管理制度，未对拟合作方的资质进行审慎调查。	a）商业银行开展代理业务应履行相关审批程序，确保取得合法的机构资质、人员从业资格和内部授权许可；建立合作方准入管理制度，并对代理业务拟合作方的资质进行审慎调查；	银监会《商业银行内部控制指引》	调阅有关主管部门下发的机构资质核准文件、商业银行内部授权文件；调阅对合作方准入管理相关制度及调查报告；检查业务人员从业资格。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
			业务收入正确核算、代理资产独立核算。	b）未建立代理业务相关的规章制度和操作规程，未对代理合同或协议实施统一管理，导致合法有效性问题。	b）建立代理业务相关规章制度和操作规程，统一代理合同及相关协议管理；	银监会《商业银行内部控制指引》	调阅代理业务相关规章制度及操作规程；调阅各代理合同或协议，并查看法律部门出具的审查意见书。
				c）未为代理资金设立核算专户，代理资金的拨付、回收、核对等手续不完善，未做到专款专用。	c）商业银行办理代理业务，应当设立专户核算代理资金，完善代理资金的拨付、回收、核对等手续，防止代理资金被挤占挪用；	行业领先实践	检查是否设立核算专户；调阅代理资金的拨付、回收、核对凭证及相关资料，检查相关手续是否完备。
				d）未对代理资金支付进行审查和管理，未按照代理协议进行资金划转；未遵循银行不垫款原则，介入委托人与其他人交易纠纷。	d）应建立和遵循代理资金支付的审查和管理流程，按照代理合同或协议约定办理资金划转手续；遵循银行不垫款的原则，不介入委托人与其他人的交易纠纷；	银监会《商业银行内部控制指引》	调阅代理合同和协议，同代理资金支付审查和管理流程相对照；调阅资金划转凭证，检查是否按协议约定划转资金，是否出现银行垫款。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
				e)未按照会计制度正确核算和确认代理业务收入；未对代理业务实行收支两条线管理，出现代理业务收入被截留或挪用的情况。	e）商业银行应当完善代理业务收入核算和确认的会计制度，并严格按照会计制度进行收支核算与管理；	银监会《商业银行内部控制指引》	调阅代理业务收入核算制度，检查是否符合企业会计制度；调阅代理收入核算凭证，检查是否与已建立的内部核算制度相符合。
				f）开展代保管业务时场地、设备等未符合国家标准，未对客户身份进行有效验证。	f）商业银行开办保管箱业务，应当在场地、设备和处理软件等方面符合国家安全标准，对用户身份进行核验确认。对进入保管场地和开启保管箱，应当制定相应的操作规范，明确要求租用人不得在保管箱内存放违禁或危险物品。	银监会《商业银行内部控制指引》	实地查看保管箱业务的场所设置，调阅安全部门对其的验收报告，查看与客户签订的保管箱协议是否明示租用人不得存入违禁品的条款。实地观察保管库现场的出入库情况，检查是否核对客户身份并适当记录。
6.24 财务会计管理	6.24.1	经营发展规划及计划	计划编制合理	a）缺少中长期发展规划和年度经营计划，或规划和计划不健全，导致经营缺乏约束；	a)制定计划编制制度，明确计划框架、指标口径、编制内容和流程；	财政部《金融企业财务规则》第一章第三条“金融企业应当根据本规则的规定，综合运用规划、预测、计划、预算等方法,反映经营状况、防范和化解财务风险，实现持续经营和价值最大化。”	调阅中长期发展规划和年度经营计划，审阅其健全性。
				b)经营目标设计不合理，与发展战略目标不统一，或违背监管政策和宏观政策；	b)建立科学的计划编制指引，明确编制依据、程序和方法，确保经营计划和发展规划具有预见性、先进性和可操作性；	财政部《金融企业财务规则》第一章第三条“金融企业应当根据本规则的规定，综合运用规划、预测、计划、预算等方法,反映经营状况、防范和化解财务风险，实现持续经营和价值最大化。”	调阅中长期发展规划和年度经营计划，评价其可行性。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
				c)计划执行不力，经营计划流于形式。	c)建立计划执行监督考核制度，加强监测、监督，明确相应奖惩措施。	财政部《金融企业财务规则》第一章第三条“金融企业应当根据本规则的规定，综合运用规划、预测、计划、预算等方法,反映经营状况、防范和化解财务风险，实现持续经营和价值最大化。”	调阅年度经营计划完成情况和计划执行监测、监督、考核文件，审查其执行情况。
	6.24.2	会计科目管理	会计科目准确设置、正确使用	a)未制定统一的会计科目政策，会计科目设置不够完整准确，存在随意设置会计科目、随意改变会计科目核算内容，任意增加、取消、合并会计科目、分户账现象；	a)严格遵循统一规划、集中管理、规范使用、定期监控的原则，加强会计科目的设置、调整、编号及核算标准的控制；	财政部《金融企业会计制度》第一章（六）“金融企业应按本制度规定，设置和使用会计科目。”	调阅内部会计科目管理政策和余额表，访谈了解会计科目管理。
				b)会计科目使用不正确，使用已停用、撤销的会计科目，乱用、串用、混用会计科目，混淆科目的使用币种、级次以及科目对应关系。	b)规范会计科目的使用，定期开展定性定量的监控分析，提高会计信息质量。	财政部《金融企业会计制度》第一章（六）“金融企业应按本制度规定，设置和使用会计科目。”	调阅内部会计科目管理政策和余额表，访谈了解会计科目使用和检查监督情况。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
	6.24.3	财务收支	财务收支依法合规	a)超越权限的财务事项未上报审批，存在分拆财务事项绕开权限管理的情况，未对财务权限实行刚性控制，未对财务授权审批情况实施有效监控；	a)建立财务授权和转授权制度，各级机构、部门和人员要在授权范围内实施财务管理活动、审批决策财务事项并对财务结果负责，严禁越权审批或超绕授权指标办理业务；	财政部《会计基础工作规范》第九十五条“各单位应当建立财务收支审批制度。”	调阅财务授权和转授权制度，抽查财务支付记录及相应财务审批相关文件，评价其财务授权制度执行情况。
				b)财务收入不真实，收入确认不符合权责发生制原则，不属于本期的收入未按规定进行分期确认；	b)各项收入要按照会计核算制度及时、完整、准确确认，不得截留或以任何理由坐支，严禁提前或延迟确认收入。任何机构、部门及个人都不得少计、少收、转移、挪用、截留收入；	财政部《会计基础工作规范》第七十九条“会计机构、会计人员应当对财务收支进行监督，对违反国家统一的财政、财务、会计制度规定的财务收支，不予办理。”	调阅营业收入明细账及相关财务凭证、协议，评价其收入核算的真实性、完整性。
				c)支出确认不符合权责发生制原则，虚列成本支出，存在违反规定列支财务费用、营业外支出等情况；	c)严格区分本期成本和下期成本、收益性支出和资本性支出、成本性支出和营业外支出的界限；	财政部《会计基础工作规范》第七十九条“会计机构、会计人员应当对财务收支进行监督，对违反国家统一的财政、财务、会计制度规定的财务收支，不予办理。”	调阅营业费用明细账及相关财务凭证，评价支出核算的规范性。
				d)资产减值准备计提范围不完整，计提方法不符合新财务会计制度要求，计提金额与预计损失金额不一致；	d)按规定提取和使用各项准备金，确保风险拨备完整和准确；	财政部《金融企业会计制度》第一章第七条（十）“金融企业各项财产如果发生减值，应当按照本制度规定计提相应的减值准备。”	查看资产分类明细，抽查贷款减值损失记账凭证与列账依据，核查是否存在少提或多提的减值准备的情况。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
				e)存款应付利息计提范围不完整，计提利率不准确，未按规定比例计提职工教育经费、工会经费；	e)对应计、应提、应列、应摊、应并的财务收支应按规定进行核算，确保损益真实、准确、完整，严禁隐瞒、虚造损益，严禁截留利润；	财政部《会计基础工作规范》第七十九条“会计机构、会计人员应当对财务收支进行监督，对违反国家统一的财政、财务、会计制度规定的财务收支，不予办理。”	调阅应付利息计提清单、损益表等资料，评价存款应付利息、职工福利费、职工教育经费、工会经费等核算是否准确。
				f)重大支出没有经过财务审查委员会审议。	f)严格贯彻执行财务审查委员会工作规则，财务审查委员会对固定资产、无形资产和费用投入等财务资源配置的必要性、合理性、合规性进行审议，对审议项目执行情况进行检查、监督。	财政部《会计基础工作规范》第九十五条“各单位应当建立财务收支审批制度。”	调阅重大财务支付记录及相应的财务审查委员会会议纪要，抽查是否严格执行财审会制度。
	6.24.4	财务集中业务	财务集中核算，防范风险	a)未建立适应财务集中核算要求的内部控制措施；	a)建立统一的财务集中制度，制定财务集中办法，明确组织机构、核算管理模式、财务集中事项和主要核算流程，制定机构岗位责任制文件，财务核算中心内部制定并实行定期或不定期的岗位轮换制度和人员强制休假制度，推行离岗审计制度；	银监会《商业银行内部控制指引》	了解财务核算管理模式，是否建立相适应的控制措施。
				b)财务集中处理流程各环节衔接不紧密，未对报账机构备用金账户进行定期对账等有效管理，备用金账户收支范围不符合规定；	b)严格执行财务集中业务操作规程等制度办法，规范备用金账户和集中支付账户的使用，通过财务管理综合系统进行财务管理、控制、核算、支付等各项工作，规范操作程序，加强财务集中数据的日常核对与监测控制，实施有效的过程与事后控制；	银监会《商业银行内部控制指引》第二十三条“商业银行应当实现业务操作和管理的电子化，做到业务数据的集中处理。”	调阅财务集中业务操作规程等制度办法，抽查备用金账户明细、凭证，评价其收支范围是否合规。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
				c) 未对财务中心进行定期检查和持续监督。	c)对财务中心进行定期检查和持续监督，建立一套满足本行财务集中风险控制要求的监测分析指标体系，开展对各项监测指标的监测分析，对财务核算中心进行全面审计，建立规范的风险控制责任认定和严格的责任追究制度。	银监会《商业银行内部控制指引》	调阅对财务部门检查报告，了解是否对财务中心进行定期检查和持续监督。
	6.24.5	固定资产控制	规范固定资产管理	a)购建需求不符合实际，重大项目购建没有进行可行性论证，投入产出达不到预期成效；	a)建立健全固定资产管理制度，科学编制固定资产投资预算，科学编制网点建设预算，优化固定资产配置资源，固定资产配置实行统一规划、授权管理；	财政部《金融企业财务规则》第二十九条“购建主要固定资产、实施重大技术改造，应当进行可行性论证，并落实决策和执行责任。”	调阅固定资产管理制度和固定资产预算、决算报告，评价固定资产购建需求是否符合实际，投入效果如何。
				b) 核算内容不真实、不准确，虚列固定资产；	b)规范固定资产的核算管理，严格按照固定资产的确认条件和价值标准，对固定资产进行分类和初始计量、后续计量，及时对固定资产增减变动进行会计处理；	财政部《金融企业会计制度》	调阅固定资产核算科目明细账，抽查列账凭证，评价核算内容不真实、不准确。
				c)固定资产未定期进行实物盘点造成账实不符，固定资产长期闲置，或被无偿占用，或丢失。	c)加强固定资产日常管理，严格固定资产权属管理，确保资产完整；建立固定资产实物维修、保养、定期清查制度，明确使用部门、实物管理部门和价值管理部门的职责权限；固定资产的处置应按照规定权限和处置方案执行，通过分类整合和专业化处置，实现资产回收价值最大化。	财政部《金融企业财务规则》	调阅固定资产明细卡片账，抽查实物资产，是否与账务记载相符。
	6.24.6	集中采	严格执行集中采购制	a) 集中采购制度体系不健全、不适用或制度维护不及时；	a) 建立健全集中采购管理制度，严格划分职责权限，执行使用人、主管人、审批人、采购人和监督人分离的管理模式；	财政部《关于加强国有金融企业集中采购管理的若干规定》	调阅集中采购制度和实施细则，了解其制度的健全性。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
		购管理	度	b)采购申请审批流程不合规，或集中采购审查委员会和专家小组未依据有关规定对集中采购项目有效履行职责，存在超权限实施集中采购；	b)规范采购申请审批流程，严格按照所授权限实施集中采购，严禁越权、擅权审批；	财政部《关于加强国有金融企业集中采购管理的若干规定》	调阅集中采购项目档案，审查采购申请审批流程是否合规。
				c)采购合同文本使用和签署不规范，未按合同验收采购项目，财会部门未对付款事项进行审核。	c)严格采购合同文本和签署程序，严格按照合同条款验收付款；	财政部《关于加强国有金融企业集中采购管理的若干规定》	调阅集中采购项目档案，抽查是否严格采购合同文本和签署程序，并按照合同条款验收付款。
				d)供应商推荐方式不符合规定，未定期开展供应商的综合评价，建立健全供应商退出机制；	d)建立供应商评估和准入管理，健全集中采购工作后评价工作机制；	财政部《关于加强国有金融企业集中采购管理的若干规定》	调阅集中采购项目档案和供应商管理文件
				e)未建立集中采购考核办法，或集中采购考核办法不能有效提高集中采购的质量和效果。	e) 完善集中采购考核管理。	财政部《关于加强国有金融企业集中采购管理的若干规定》	调阅集中采购考核办法，访谈了解执行的效果。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
	6.24.7	应税事务管理	依法合规纳税	对税收法规理解不到位，未严格执行税收政策，造成应纳税额计算差错，未按时申报纳税，申报资料不全，或未及时支付税款或税款支付数额出现差错。	加强税收政策培训，明确分加强税收政策培训，明确分工管理，落实责任，建立并完善涉税台账，按税法落实对不同申报事项的具体要求，规范对各类涉税证明、发票、凭证资料及涉税台账的复核与监测工作，精确计算，严格申报，准确计缴。	财政部《金融企业财务规则》	调阅纳税申报资料，评价执行税收政策情况。
6.25 资产负债管理	6.25.1	人民币资金管理	合理保障业务经营合法合规，提高风险管理水平，提高全辖资金使用的效	a）利率管理制度不健全、利率政策执行不到位造成利率风险或经营决策风险；	a）加强利率管理： 1） 认真执行国家利率政策，健全利率管理制度，加强利率定价议价管理，按照利率政策、规章制度与合同约定规范利率执行； 2） 加强利率风险监测、报告和监督检查工作。	《人民币利率管理规定》、《商业银行流动性风险管理指引》、《商业银行资本充足率管理办法》	访谈资产负债部门，询问、检查系统参数设定、维护、变更情况，检查头寸调拨表及监测报告。
				b）资金内部转移价格制定不合理或执行不到位，造成资金使用效果不佳或经营风险；	b）根据全行资产负债管理要求、市场利率情况综合确定，并根据外部市场环境变化和全行经营策略定期或不定期调整，完善内部资金转移价格管理；	《商业银行流动性风险管理指引》	调阅调整内部资金转移价格有关文件。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
			率、效果。	c）审批不严格、操作行为不规范，造成流动性支付风险及操作风险。	c）严格资金运营审批和监督： 1） 按照事权划分和岗位分离要求，加强对资金运营的审查和监督，包括利率设定、额度限制及其对全行资金头寸的影响等。编写资金运营分析报告，对全行的利率风险、流动性风险，资金配置状况等进行分析并报资产负债管理部门负责人审阅； 2） 加强系统参数管理，对参数设置、维护的进行权限控制。	《商业银行流动性风险管理指引》、《商业银行资本充足率管理办法》	检查资金调拨授权、审批文件及相关手续。
	6.25.2	外汇资金管理	合理保障业务经营合法合规，防范经营风险。	a）汇率使用不准确或由于外汇买卖业务所导致资产负债的错配所引发的汇率风险；	a）所有外汇业务的汇率均由总行统一规定，同时利用系统对汇率进行硬控制；建立对汇率波动的实时监测制度，防范汇率波动所产生的损失风险；	《中华人民共和国外汇管理条例》	检查汇率参数设置、维护、更新情况

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
				b）市场利率波动，导致外币业务遭受损失的风险；	b）执行人民银行关于外币存款的利率政策，执行询价、报批制度，及时平盘，确保利率风险净敞口为零；	《中华人民共和国外汇管理条例》	检查外汇资金利率使用情况。
				c）由于资产负债期限不匹配、突发的大额支取或结汇而导致的流动性风险。	c）加强对资金运营的审查和监督，保持合理头寸。	《中华人民共和国外汇管理条例》	检查外汇资金平盘情况。
	6.25.3	本外币	合理保障业务经营合	a）未按规定缴纳法定存款准备金及备付金；	a）严格按照规定统一调缴法定存款准备金，合理安排超额存款准备金比例，提高资金头寸周转效率，减少低息资金占用；	人民银行存款准备金制度；	询问准备金缴存情况，调阅缴存凭证。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
		资金运营	法合规，保证资金安全，防范经营风险，提高全辖资金使用的效率、效果。	b）头寸匡算不准确，出现资金缺口或流动性支付风险；	b）强化资金头寸管理：加强资金头寸管理，实时监控本级和下级行的资金来源和运用情况，准确匡算资金头寸；建立覆盖各级机构的大额资金预测预报管理体系，加强上下级行之间、部门之间的信息交流和协调配合，对大额资金变动进行及时、准确的预测预报，做好对账及跟踪监测，减少资金在途损失，保证支付与清算，严防支付风险。	银监会《商业银行内部控制指引》、《商业银行操作风险管理指引》	调资金调拨相关凭证及审批资料。
				c）超权限进行资金调拨，调拨金额与实际匡算金额不一致。	c）强化资金调拨清算控制，严格按照前后台分离要求设置资金调拨岗位权限，在严格授权管理下进行资金调拨。	银监会《商业银行内部控制指引》	调资金调拨相关凭证及审批资料。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
	6.25.4	经济资本管理	达到监管要求，提高全辖资金使用的效率、效果。	a）资本充足率未达到监管部门的要求；	a）每年年初总行对全行的资本充足率进行预算，编制当年的经济资本限额指标，资本充足计划和经济资本配置计划，按季向人行报送其各项资本充足率指标，确保资本充足率达到监管部门的要求；	《巴塞尔协议（III）》、《商业银行资本管理办法（试行）》、《商业银行资本充足率管理办法》	检查向监管部门报送的各项资本充足率指标。
				b）经济资本的目标不合理，不能对银行的业务起到指导作用；	b）按国家宏观经济政策和企业经营发展战略，及时优化调整各项业务经济资本配置系数，鼓励发展低经济资本占用、较高收益的业务，控制风险资产盲目扩张；	《巴塞尔协议（III）》、《商业银行资本管理办法（试行）》	检查全行各项业务经济资本占用情况，年初总行对全行的资本充足率进行预算情况，包括编制经济资本限额指标，资本充足计划和经济资本配置计划情况。
				c）经济资本的计量方法不统一或未经有效性验证。	c）经济资本计量原则和计量模型由总行统一制定并定期进行合理性评估，计量方法实行系统硬控制。	《巴塞尔协议（III）》、《商业银行资本管理办法（试行）》	询问经济资本管理员，现场调阅经济资本计量模型，了解分行经济资本计量方法是否与总行一致，计量参数修改是否上报总行批准。
	6.25.5	国债业务	正确代理发行、兑付国债	a）超计划发行、串档或串期发行；	a）准确完成相关参数设定，建立双人复核制度，防止超计划发行、串档或串期发行；	《中国人民银行关于印发储蓄国债（电子式）管理办法（试行）的通知》、《财政部 中国我民银行关于印发凭证式承销团成员考评办法（试行）的通知》、人民银行《凭证式承销团成员考核实施细则（试行）》	检查国债参数的设定、维护及变更情况，调阅各期国债发行、兑付文件。
				b）缴存国债的路径、缴存款项错误，收取的兑付本金或代理手续费错误。	b）及时与财政部核对缴款路径和款项，根据代销量与国债公司核对兑付本金及手续费。	《中国人民银行关于印发储蓄国债（电子式）管理办法（试行）的通知》、《财政部 中国我民银行关于印发凭证式承销团成员考评办法（试行）的通知》、人民银行《凭证式承销团成员考核实施细则（试行）》	检查国债款项划的相关记账凭证及与各相关方的对账清单。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
6.26 产品创新管理	6.26	产品创新管理	促进企业实现发展战略	a）新产品的开发管理混乱，存在重复开发等资源浪费情况。	a）对新产品开发立项实行统一管理，加强新产品在全行的推广和运用。	《企业内部控制审计指引》	了解项目审批流程，查看相关审批资料。
				b）未根据市场、客户需求，同类产品情况等综合比较后进行新产品研发，所开发的新产品不适销对路或不符合监管机构的规定；	b）建立执行立项审批制度，及时按规定向监管机构报备；	《企业内部控制审计指引》	查看项目立项制度及相关的立项审批报告及分析报告。
6.27 租赁	6.27.1	业务审查与授信管理	租赁业务资产评估准确，有效开展授信授权控制	a）客户经理尽职调查内容不完备、不真实、缺乏有效性；	a）前台业务部门对客户的相关情况进行尽职调查，加强对企业股东方及偿债能力的调查和分析；	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》 银监会《金融租赁公司管理办法》(中国银行业监督管理委员会令（2007年第1号）	抽样尽职调查报告，对相关信息进行核查，确定尽职调查的有效性。
				b）授信环节未按照业务规定进行严格审查。	b）风险管理部门受理授信业务后，对前台业务部门提交的授信预案提出审查意见，项目评审委员会对授信方案进审议。	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》 银监会《金融租赁公司管理办法》(中国银行业监督管理委员会令（2007年第2号）	调阅授信预案的审批资料，核查审批过程是否符合规定。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
	6.27.2	业务审批	合规办理租赁业务	a）未对租赁物的价值、所有权属和抵押物价值和权属进行评估；	a）前台业务部门应对租赁物进行调查评估，评估内容包括租赁物的价值、所有权属和抵押物的价值和权属；	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》 银监会《金融租赁公司管理办法》(中国银行业监督管理委员会令（2007年第3号）	调阅租赁物和抵押物的价值评估报告，判断其是否偏离市场价格
				b）未对调查评估报告进行有效审查；	b）风险管理部门受理租赁业务后，审查岗位人员遵循客观、独立、公正的原则，对前台业务部门提交的调查报告及相关资料提出审查意见，项目评审委员会集体审议；	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》 银监会《金融租赁公司管理办法》(中国银行业监督管理委员会令（2007年第4号）	调阅相关会议纪要等文档资料，确认租赁业务方案得到有效审批
				c）未按照授权规定审批租赁业务方案。	c)租赁业务方案须经决策层审议通过。	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》 银监会《金融租赁公司管理办法》(中国银行业监督管理委员会令（2007年第5号）	调阅转让应收租赁款的审查资料，检查其审查审批手续的完善性。
	6.27.3	业务办理	合规办理租赁业务	a）未按审批要求落实前提条件；	a）前台业务部门落实租赁前提条件，风险管理部审核岗位人员核准；	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》 银监会《金融租赁公司管理办法》(中国银行业监督管理委员会令（2007年第6号）	调阅租赁项目档案资料，对照有权部门对项目做出的审查批复，检查是否落实了批复中提出的前提条件。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
				b）未对租赁资产进行投保，或购买的保险不符合规定；	b）租赁业务应执行对项目租赁物保险的要求；	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》 银监会《金融租赁公司管理办法》(中国银行业监督管理委员会令（2007年第7号）	调阅保险合同，确认租赁资产已投保且或购买的保险符合相关规定；
				c）未按规定办理租赁标的物所有权转移的手续。	c） 前台业务部门完成租赁物所有权转移手续。	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》 银监会《金融租赁公司管理办法》(中国银行业监督管理委员会令（2007年第8号）	调阅相应产权证书，确认租赁标的物已办理所有权转移；
	6.27.4	后续管理	合规办理租赁业务	a)未按规定对承租人进行监测；	a）前台业务部门定期编制租后检查表与分析报告；	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》 银监会《金融租赁公司管理办法》(中国银行业监督管理委员会令（2007年第9号）	调阅租后检查表、分析报告等资料，验证是否定期对承租人的经营状况、偿债能力等进行了监测
				b）未按照规定检查租后情况；	b）租后检查表与分析报告应交风险管理部审查岗位人员进行风险分析；	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》 银监会《金融租赁公司管理办法》(中国银行业监督管理委员会令（2007年第10号）	查阅贷后检查报告，分析是否对承租人经营状况进行跟踪，是否及时反应了承租人经营状况的变化；是否按规定的频率和内容进行了租后检查。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
				c)未提示客户按时支付租赁本金和租赁利息。	c）在租赁业务存续期内，提示客户按时给付租赁本金和租赁利息，进行租金催收，催收未果的按照不良租赁资产管理的相关规定进行处理。	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》 银监会《金融租赁公司管理办法》(中国银行业监督管理委员会令（2007年第11号）	调阅客户通知书等相关文档，确认银行提示了客户按时支付租赁本金和租赁利息。
6.28 基金	6.28.1	公募基金	公募基金开展客户风险评估，投资管理独立建账、独立核算	a）基金产品开发未经逐级授权审批；	a）公募基金产品研发后，按照授权管理规定逐级审核批准，并审批产品定价方案；	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》 证监会《证券投资基金销售管理办法》	调阅公募基金产品审查审批资料，确认授权制度的执行情况。
				b）基金产品发行未履行信息披露审批流程；	b）招募说明书、发售公告、发行文件（基金合同、托管协议、招募说明书及发售公告）、基金净值履行信息披露审批流程，定期披露；	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》 证监会《证券投资基金销售管理办法》	调阅基金产品的披露报告及审批记录，确认相关披露审批手续的有效性。
				c）基金销售未开展客户风险能力测试；	c）基金销售人员应取得基金销售业务资格，建立基金销售适用性管理制度，对基金投资人开展风险能力测试，投资人应购买与其风险承受能力相适合的基金产品。对于购买基金产品与个人风险承受能力不相匹配的投资人，要求投资人签订投资人意愿声明书；	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》 证监会《证券投资基金销售管理办法》	抽查基金投资人的风险评估测试报告，检查基金销售中产品与客户的风险匹配程度。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
				d）基金投资管理未执行授权制度；	d）基金公司明确投资决策委员会、分管投资的高管人员、基金经理等各投资决策主体的职责权限划分，合理确定各基金经理的投资权限。基金经理在授权范围内可以自主决策，超过投资权限的操作需要经过严格的审批程序；	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	抽查基金投资交易明细记录，调阅授权及转授权文件，检查投资管理中是否有效执行授权管理制度。
				e）基金公司未按不同基金设立账户进行核算。	e）基金公司对所管理的基金应当以基金为会计核算主体，独立建账、独立核算，保证不同基金之间在名册登记、账户设置、资金划拨、账簿记录等方面相互独立。基金会计核算应当独立于公司会计核算。	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	抽查基金账户管理的明细账，检查基金分户管理、独立建账的制度执行情况。
	6.28.2	专户理财	专户理财与自营资产有效分离，投资经理与基金经理不得兼任	a）专户理财产品未授权审批；	a）专户理财产品研发完成后，按照授权逐级审核批准，对专户理财产品进行审核，评估表决形成决议，同拟任基金经理人选上报有权人进行审批；	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	调阅专户理财产品的审批记录，检查授权制度的执行情况。
				b）基金管理公司固有财产与委托财产未有效分离；	b）基金管理公司从事特定资产管理业务，委托财产独立于资产管理人和资产托管人的固有财产，并独立于资产管理人管理的和资产托管人托管的其他财产。资产管理人、资产托管人不得将委托财产归入其固有财产；	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	抽查基金公司自有资产及委托资产的管理明细账，确定自有资产与委托资产是否有效分离。
				c）专户理财业务投资经理与基金经理相互兼任。	c）基金管理公司办理特定资产管理业务的投资经理与证券投资基金的基金经理不得互相兼任。	财政部等五部委《企业内部控制基本规范》 银监会《商业银行内部控制指引》	调阅基金公司职责分工明细，确定专户理财与开放式基金管理人的分离情况。

A.4 信息科技层面内控评价工作底稿

表 A.3 信息科技层面内控评价工作底稿

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
7.2 信息科技治理	7.2.1	治理架构	IT 战略计划符合业务目标。	a)未制定符合全行整体发展战略的IT发展战略规划，没有考虑利益相关方的要求，系统战略规划与运行管理能力不能适应商业银行发展战略要求。	a)商业银行在制定信息科技战略计划的过程中，应从业务发展战略出发，充分考虑业务部门内部和外部利益相关者的监管要求，使信息科技战略计划符合业务目标。	《商业银行信息科技风险管理指引》第八条	访谈相关部门的负责人，了解管理层在制定IT战略计划的过程中，是否从业务发展战略出发，并使受其影响的内部和外部利益相关者进行参与，充分考虑他们的意见。
			形成分工合理、职责明确、相互制衡、报告关系清晰的信息科技治理组织结构。	b)未建立清晰的信息科技组织治理结构，部门分工不合理、职责不明确,缺少制衡制约,汇报渠道不明确。	b)在建立良好的公司治理的基础上进行信息科技治理，形成分工合理、职责明确、相互制衡、报告关系清晰的信息科技治理组织结构。	1.《企业内部控制基本规范》第十四条 2.《企业内部控制基本规范》第二九条 3.《商业银行信息科技风险管理指引》第七条	调阅信息科技治理组织架构图，检查组织架构图中各成员相应履职情况。
			确保董事会与银行的总体业务战略和重大策略相一致。	c)董事会职责中未包括审查批准信息科技战略。	c)董事会应负责审查批准信息科技战略，确保其与银行的总体业务战略和重大策略相一致。评估信息科技及其风险管理工作的总体效果和效率。	《商业银行信息科技风险管理指引》第七条	调阅信息科技管理委员会会议纪要，抽样检查是否有董事会对重大信息科技战略的审查批准意见。
			确保信息科技风险管理的年度报告经董事会审阅。	d)董事会每年未审阅信息科技风险管理的年度报告。	d)董事会应每年审阅并向银监会及其派出机构报送信息科技风险管理的年度报告。	《商业银行信息科技风险管理指引》第七条	调阅有关信息科技风险管理报告经董事会审阅的有关会议纪要。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
			确保信息科技管理委员会有效履职。	e)未建立来自高级管理层、信息科技部门和主要业务部门的代表组成的专门信息科技管理委员会。	e)商业银行应设立一个由来自高级管理层、信息科技部门和主要业务部门的代表组成的专门信息科技管理委员会，负责监督各项职责的落实，定期向董事会和高级管理层汇报信息科技战略规划的执行、信息科技预算和实际支出、信息科技的整体状况。	《商业银行信息科技风险管理指引》第七条	调阅信息科技管理委员会具体职责，抽样检查会议纪要。
			商业银行应设立直接向行长汇报的首席信息官。	f)未设立首席信息官。	f)商业银行应设立首席信息官，直接向行长汇报，并参与决策。首席信息官的职责包括：直接参与本银行与信息科技运用有关的业务发展决策；确保信息科技战略，尤其是信息系统开发战略，符合本银行的总体业务战略和信息科技风险管理策略；负责建立一个切实有效的信息科技部门，承担本银行的信息科技职责；确保信息科技风险管理措施落实到相关的每一个内设机构和分支机构等。	《商业银行信息科技风险管理指引》第八条	调阅有关首席信息官职责，抽样检查首席信息官主持召开的信息科技管理委员会会议纪要。
	7.2.2	控制环境	应建立组织结构清晰、部门职能明确的IT部门。	a)未建立一个切实有效的信息科技部门，承担本银行的信息科技职责。	a)商业银行应建立组织结构清晰、部门职能明确的IT部门，确保其履行：信息科技预算和支出、信息科技策略、标准和流程、信息科技内部控制、专业化研发、信息科技项目发起和管理、信息系统和信息科技基础设施的运行、维护和升级、信息安全管理、灾难恢复计划、信息科技外包和信息系统退出等职责。	《商业银行信息科技风险管理指引》第八条	调阅本行信息科技部门职责。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
			建立完善的信息科技制度体系。	b)未建立科学的信息科技制度、规范、标准和管理流程，未形成规范的信息科技制度体系。	b)商业银行应建立完善的信息科技制度体系，包括管理程序和操作流程，并保证其得以严格执行。	《商业银行信息科技风险管理指引》第三条	调阅信息科技管理制度总体框架及具体制度。
			确保当前的 IT 人力资源满足信息科技发展需要。	c)未定期开展人力资源评估，不及时掌握人力资源实际状况，不清楚员工的真实履职能力。	c)商业银行的信息科技管理层应定期对信息科技人力资源状况进行评估，科学配置人力资源，为信息科技战略目标的实现提供资源保障。评估内容主要包括当前的信息科技人力资源能否满足信息科技发展需要，信息科技人员能否胜任当前的工作岗位等。	1、商业银行信息科技风险管理指引》第十四条 2.、COBIT 控制框架 PO7	1、访谈了解综合部门如何对人力资源进行评估的。 2、审阅人力资源管理文档，了解是否对人力资源充分性进行评估，并做相应的要求。 3、调阅相关文档，检查是否开展人力资源评估。
			IT 部门应明确 IT 关键岗位。	d)信息科技部门职能和岗位职责定义及描述不够清晰，未明确不相容岗位和信息科技关键岗位，难以实现不相容岗位的职责分离。	d)商业银行的信息科技部门应明确关键岗位，并在岗位设计上实现了职责分离。此外，定期或不定期的对职责划分的合理性进行评价，以符合组织发展变化的要求。	1、《商业银行信息科技风险管理指引》第九条 2、《企业内部控制基本规范》第十四条、第二十九条	调阅本行信息科技部门有关关键岗位的定义与人员对照关系，检查是否在岗位设计上实现了职责分离。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
			在信息科技部门员工入职前进行人员背景调查。	e)未对信息科技部门员工在其入职前进行背景调查。	e)商业银行应在信息科技部门员工入职前进行人员背景调查（内容主要包括：核验有效身份证件、学历证明、工作经历和专业资格证书等信息）。	1、《商业银行信息科技风险管理指引》第九条 2、COBIT 控制框架 PO7	1、访谈了解如何对信息科技部门员工背景调查。 2、审阅人力资源管理文档，是否就招聘，对雇佣人员开展背景调查做出具体明确的要求。 3、抽样最近一年新雇佣人员为样本总量，按照抽样原则进行抽样，检查： ——获取雇佣人员背景调查记录，是否开展背景调查（内容包括：有无从业人员的身份和资格；工作经历和背景；离开原单位的原因；犯罪记录和其他评价）； ——是否签订了安全保密协议。
			建立相应的人员调动、离职机制。	f)未针对员工工作岗位变化制定响应机制。	f)商业银行应建立相应的人员调动、离职机制，确保员工调动到新的工作岗位或离开商业银行时，及时变更相关信息,系统及时检查、更新或注销用户身份；评估关键岗位信息科技员工流失带来的风险，做好安排候补员工和岗位接替计划等防范措施。	1、《商业银行信息科技风险管理指引》第九条 2、《企业内部控制基本规范》第十六条、第四十四条	1、访谈了解是否存在员工岗位变动及离职管理流程。 2、调阅人力资源管理等制度等，检查具体的响应机制。 3、获取岗位变动及离职人员清单，并以此为样本总量，按照抽样原则进行抽样，检查相应系统用户权限是否得到了调整。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
			信息科技资产的所有者必须对其负责的资产承担维护以及安全保护的责任。	g)未建立信息科技资产清单和指定相关责任人。	g)商业银行应对所有关键信息科技资产（固定资产、重要系统、软件产品和数据）编制清单，并为其指定所有者。资产的所有者必须对其负责的资产承担维护以及安全保护的责任。	《商业银行信息科技风险管理指引》第十二条	1、访谈了解是否通过手工台账或信息系统方式建立并维护信息科技固定资产、重要系统、软件产品和数据的清单，是否指定所有者。 2、调阅查看IT资产管理的制度，是否对各项资源的管理流程进行了说明。 3、抽样调阅固定资产、数据（生产数据）、软件产品清单，是否IT资产进行了记录。 4、分别以为固定资产、软件产品清单为样本总量，按照抽样原则，分别对固定资产、软件产品开展随机抽样，检查相关资产清单是否对固定资产、数据或软件产品进行了记录，并记录完整。
			确保信息科技重要资源安全。	h)没有对信息科技资产的物理环境进行保护与控制。	h)商业银行应建立信息系统物理安全管理制度，保证重要资源安全。	《商业银行信息科技风险管理指引》第十二条	1、了解如何对IT资产进行物理安全管理的。 2、抽样检查机房及其他基础设施中对IT资产的物理安全管理情况。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
	7.2.3	信息与沟通	持续关注与IT管理相关的法律、规章等外部监管要求及检查结果	a)未持续关注外部监管和审计的要求，并配合外部检查。	a)商业银行应持续关注与信息科技管理相关的法律、规章等外部监管要求，及时采取相应的措施；配合外部监管和审计对本行的检查，并将检查结果及时报告董事会、高管层和内审等有关方。	《商业银行信息科技风险管理指引》第七条	访谈相关部门的负责人，了解： 1、科技部门如何会监控与IT的活动和控制相关的法律、规章以及其他外部需求是否发生了变化，并保证IT活动与变化一致。 2、科技部门如何配合外部监管对本行的科技检查并做好检查结果在本行内部的报告。
			确保信息科技风险状况及时对外披露。	b)商业银行未及时披露信息科技风险状况。	b)商业银行应依据有关法律法规的要求，规范和及时披露信息科技风险状况。	《商业银行信息科技风险管理指引》第十三条	调阅本行最近年度对外正式披露的信息科技风险管理报告。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
			确保员工职业道德和行为规范、内部控制和安全管理意识方面的培训定期开展。	c)缺乏针对员工职业道德和行为规范的教育。	c)商业银行应定期对员工开展有关职业道德和行为规范、内部控制和安全管理意识方面的培训。	1、《商业银行信息科技风险管理指引》第九条 2、COBIT 控制框架 PO7，DS7 3、《企业内部控制基本规范》第九条	1、访谈相关部门的负责人，了解： —内部控制、安全教育宣传； —知识技能共享； —技能、能力方面的培训； —内部控制和安全意识方面的培训； —培训执行效果的保证措施。 2、观察员工如何及时了解内部控制和安全管理方面的要求， 3、审阅相关文档，例如培训的规定和培训计划： —是否就关键技能、能力、内部控制和安全管理意识的培训进行了规定。 —是否建立培训计划，计划中是否包含了人员技能、能力及内部控制和安全意识方面的培训。 —抽样检查员工参加培训的记录。
			确保员工对信息科技风险管理制度和流程的了解。	d)未使员工了解、遵守信息科技策略、信息保密、信息科技风险管理制度和流程等要求。	d)商业银行应确保员工（包括正式员工、临时员工和其它相关外来人员）充分理解和遵守经董事会批准的信息科技风险管理制度和流程，通过同员工签订相关协议的方式，授权使用信息系统、了解信息科技管理制度和流程等。	《商业银行信息科技风险管理指引》第九条	调阅科技部门对于正式、临时、外来人员如何了解并遵守本行信息科技策略、保密制度、管理流程要求等方面的文档。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
	7.2.4	监督与评价	确保董事会和高管层对于IT战略计划的执行情况进行监督。	a)董事会和高管层对信息科技管理缺少适当的监督。	a)商业银行的董事会和高管层对于信息科技战略计划的执行情况进行监督，并使其满足业务发展需要，促进信息科技战略目标的实现。	《商业银行信息科技风险管理指引》第七条	调阅信息科技管理委员会纪要，抽样检查是否包括董事会和高管层对IT战略执行情况的监督记录。
			商业银行应建立信息科技风险管理三道防线。	b)商业银行未建立信息科技风险管理三道防线。	b)商业银行应建立由信息科技部门、内控和风险管理部门、内部审计部门组成的信息科技风险管理三道防线机制，并在该机制下各相关部门分别承担对信息科技风险的日常管理、内控监督以及审计评价。	《商业银行信息科技风险管理指引》第七条	1、从信息科技部调阅本行有关信息科技风险管理三道防线建立情况的文档。 2、分别访谈信息科技部、内控合规部、内部审计局相关岗位人员，了解各部门在信息科技风险管理三道防线的相应履职情况。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
			信息科技部应对IT日常运营管理开展持续的检查。	c)作为第一道防线的信息科技部门没有对信息科技日常运营管理开展持续的检查，未对外部监管和内部检查发现的问题进行跟进且未及时采取相应的措施。	c)商业银行的信息科技部门应基于风险评估结果，制定信息科技管理检查计划；开展的信息科技检查能够发现问题和潜在风险，并将检查结果及时报告董事会、高管层和内部审计部门等有关方；对检查发现的问题及时跟进，及时制定整改措施，并及时将整改结果报告董事会、高管层和内部审计部门等相关方。	《商业银行信息科技风险管理指引》第七条、第八条	1、访谈信息科技部门的负责人，了解总行如何开展IT日常运营管理持续检查； 2、抽样检查相关文档，检查IT检查的内容、报告。 3、访谈信息科技部制度管理处负责人，了解我行针对问题跟踪整改相关的制度规定，了解有关问题跟进流程； 4、调阅上述相关制度办法，确认我行对IT控制中发现的问题的具体跟进流程； 5、抽样检查相关文档（如，后续跟踪报告、问题整改报告、问题整改跟踪表等），检查具体的跟进流程执行落实情况。
			内控合规、风险管理部门应监控与评估信息科技部门为业务部门提供服务的效果，对信息科技部门合规运营、风险管理效果进行监督评价。	d)作为第二道防线的内控合规、风险管理部门未监控与评估信息科技部门为业务部门提供服务的效果，未对信息科技部门合规运营、风险管理效果进行监督评价。	d)商业银行应设定或指派内控或风险管理部门承担信息科技风险管理职责，为业务部门和信息科技部门提供合规建议，监控信息安全威胁和不合规事件的发生，监控信息科技部、各中心、各分行为业务部门提供的服务，并将检查结果及时报告高管层，并抄送内部审计部门。	《商业银行信息科技风险管理指引》第七条、第八条	1、访谈内控部门的负责人，了解如何开展对信息科技日常运营管理的内控监督检查； 2、抽样检查相关文档，检查IT内控检查的内容、报告。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
			商业银行应在内部审计部门设立专门的信息科技风险审计岗位。	e)商业银行未在内部审计部门设立专门的信息科技风险审计岗位。	e)商业银行内部审计部门应配备足够的资源和具有专业能力的信息科技审计人员，负责信息科技审计制度和流程的实施，制定、实施和调整信息科技审计计划，检查和评估信息科技系统和内控机制的充分性和有效性，对信息科技整个生命周期和重大事件等进行审计。	《商业银行信息科技风险管理指引》第十一条	调阅本行内部审计部门职责，检查是否设立专门的信息科技审计处室或岗位，及其相关履职情况。（即信息科技风险的第三道防线）
			商业银行内部审计部门应对信息科技风险开展有效的监督与评价。	f)商业银行内部审计部门未对信息科技风险开展有效的监督与评价。	f)商业银行内部审计部门根据业务性质、规模和复杂程度，信息科技应用情况，以及信息科技风险评估结果，决定信息科技内部审计范围和频率，但至少每三年实现审计范围的全面覆盖。	《商业银行信息科技风险管理指引》第十一条	1、访谈内部审计部门负责人，了解第三道防线在信息科技审计方面的履职情况。 2、调阅审计时限内内部审计计划，IT审计项目方案和报告，了解有关IT审计项目制定与开展情况。
7.3 信息科技风险管理	7.3.1	风险管理策略	确保全面的信息科技风险管理策略的建立。	a)未制定全面的信息科技风险管理策略。	a)针对信息分级与保护、信息系统开发、测试、运行和维护，以及访问控制、物理安全、人员安全、业务连续性计划与应急处置建立风险识别与评估流程。	《商业银行信息科技风险管理指引》第十五条	调阅科技部门有关全面信息科技风险管理策略的制度文档，访谈了解具体执行情况。
			根据信息科技风险管理策略，制定明确的信息科技风险管理制度。	b)未依据信息科技风险管理策略实施全面的风险防范措施。	b)商业银行应依据信息科技风险管理策略，制定明确的信息科技风险管理制度、技术标准和操作规程等，定期进行更新和公示。	《商业银行信息科技风险管理指引》第十七条	通过访谈了解科技部门风险管理的具体制度： 1、是否建立了全面的信息科技风险管理制度，覆盖了信息系统开发、测试和维护，以及访问控制、物理安全、人员安全、应急安全等方面。 2、是否定期更新和公示。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
			确保遵守境内外监管要求。	c)商业银行在境外设立的机构未遵守境内外监管要求。	c)商业银行在境外设立的机构及境内的外资商业银行，应当遵守境内外监管机构关于信息科技风险管理的要求，并防范因监管差异所造成的风险。	《商业银行信息科技风险管理指引》第十九条	通过访谈科技部门了解，本行境外机构的信息科技风险管理是否发生过违反当地监管要求的生产事件，并调阅相关文档。
	7.3.2	风险识别和评估	确保风险识别和评估流程是持续的。	a)未制定持续的风险识别和评估流程，无法确定信息科技中存在隐患的区域。	a)商业银行应制定持续的风险识别和评估流程，确定信息科技中存在隐患的区域，评价风险对其业务的潜在影响，对风险进行排序，并确定风险防范措施及所需资源的优先级别（包括外包供应商、产品供应商和服务商）。	《商业银行信息科技风险管理指引》第十六条	1、访谈了解风险评估是否是持续的，并是内部控制、IT 策略及监控评价机制的一部分。 2、审阅《中国工商银行信息系统安全体系规范》等文档，检查风险评估的方式，风险评估与内部控制、IT 策略及监控评价机制的关系。 3、抽样检查未识别风险的事例。
			确定信息科技风险的潜在区域。	b)未依据信息科技风险评估结果确定应该关注的主要风险。	b)商业银行应依据信息科技风险评估结果，确定应该关注的主要风险，并对这些区域进行详细和独立的监控，实现风险最小化。	《商业银行信息科技风险管理指引》第十七条	调阅信息科技风险评估报告，了解是否根据结果确定潜在风险区域，并对这些区域进行独立监控。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
	7.3.3	风险应对和监测	建立持续的信息科技风险计量和监测机制。	a)未建立持续的信息科技风险计量和监测机制。	a)商业银行应建立持续的信息科技风险计量和监测机制。包括：建立信息科技项目实施前及实施后的评价机制；建立定期检查系统性能的程序和标准；建立信息科技服务投诉和事故处理的报告机制；建立内部审计、外部审计和监管发现问题的整改处理机制；安排供应商和业务部门对服务水平协议的完成情况进行定期审查；定期评估新技术发展可能造成的影响和已使用软件面临的新威胁；定期进行运行环境下操作风险和管理控制的检查；定期进行信息科技外包项目的风险状况评价。	《商业银行信息科技风险管理指引》第十八条	访谈了解科技部门如何建立持续的信息科技风险计量和监测机制： 1、如何建立信息科技项目实施前及实施后的评价机制； 2、如何建立定期检查系统性能的程序和标准； 3、如何建立信息科技服务投诉和事故处理的报告机制； 4、如何建立内外审及监管发现问题的整改机制； 5、如何安排供应商和业务部门对服务水平协议完成情况进行定期审查； 6、如何定期对信息科技外包项目风险状况开展评价。
			确保清晰的风险评估管理流程和报告路线。	b)风险评估没有清晰的管理流程和报告路线。	b)商业银行应根据实际情况明确制定风险评估管理流程的负责部门，并制定风险评估管理流程和风险评估报告制定路线。	《商业银行信息科技风险管理指引》第十八条	1、访谈相关部门的负责人，了解分行及数据中心如何将风险评估的结果与总行进行报告。 2、审阅相关文档，检查分行和数据中心风险评估的上报结果和总行反馈意见。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
7.4 信息安全	7.4.1	总体管理	建立完善的信息安全管理制度。	a）缺乏完善的信息安全管理制度；	a） 商业银行应负责建立和实施信息分类和保护体系，并负责建立信息安全管理机制，包括信息安全标准、策略、实施计划和持续维护计划，并定期更新。商业银行应建立全行统一的信息分类标准，应对各类信息都有合理的安全级别及控制措施，定期对安全级别进行评估和相应的修改，并应建立对重要数据和信息的使用、审批制度。商业银行应建立详细完整的信息安全管理制度，经管理层审批后发布，并应定期对信息安全管理制度进行复核，如果环境发生了变化，必须做出相应的修订。	《银行业金融机构信息科技风险评价审计要点》1.1.2 《银行业金融机构信息系统风险管理指引》第十五条、第十九条	1、访谈相关部门负责人，了解有哪些安全制度和细则。 2、查阅相关制度及细则，确认其是否涵盖了操作系统安全、数据库安全、应用系统安全、网络安全、物理安全等方面。
			建立健全信息安全组织架构，落实信息安全管理工作。	b）未落实信息安全管理职能和组织架构；	b）商业银行应建立信息安全管理组织框架，落实管理职能，以启动和控制信息安全的实施，并在部门和岗位职责分工中定义并分配信息安全的关键职责。	《商业银行信息科技风险管理指引》第二十一条	访谈相关部门负责人，了解安全制度和细则的落实情况。审阅相关的信息安全工作职责文档。
			对员工进行必要的信息安全培训，提高信息安全意思，了解其职责范围内的信息保护工作流程。	c）员工缺乏必要的信息安全培训；	c） 商业银行应使所有员工都了解信息安全的重要性，并组织提供必要的培训，让员工充分了解其职责范围内的信息科技安全管理制度和信息保护流程,提高全体员工的信息安全意识，以达到信息安全控制的要求。	银监会《2006 年度银行业金融机构信息科技风险评价审计指引》第二部分信息安全管理 《商业银行信息科技风险管理指引》第二十条	1、访谈相关部门负责人，了解通过何种途径，将安全制度和流程下发给各个相关部室和员工，并对相关人员进行信息安全方面的培训。 2、抽样查阅培训记录，了解培训情况和内容；抽查制度下发记录。 3、抽样访谈员工是否了解已发布的安全制度和流程，验证培训效果。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
			建立有效的用户管理机制和访问控制流程。	d）未建立用户管理机制和访问控制流程。	d)商业银行应建立有效的用户认证管理机制和访问控制的流程，建立完整的用户管理流程，包括各类应用系统、安全系统、网络系统、数据库和操作系统的用户的开立、变更和销户。同时应明确定义终端用户和信息科技技术人员在各信息系统安全中的角色和职责。对用户权限的授予应遵循岗位职责分离和知所必须的最小授权原则。	《商业银行信息科技风险管理指引》》第二十一条、第二十二条	1、访谈相关部门负责人，了解有哪些用户安全制度和细则。 2、查阅相关制度及细则，确认其是否涵盖了操作系统安全、数据库安全、应用系统安全、网络安全、物理安全等方面。
			制定相关策略和流程，管理所有生产系统的活动日志，以支持有效的审核、安全取证分析和预防欺诈。	e）未建立生产系统活动日志管理策略和流程。	e）商业银行应制定相关策略和流程，管理所有生产系统的活动日志，以支持有效的审核、安全取证分析和预防欺诈。活动日志应包括交易日志和系统日志，其中交易日志由应用软件和数据库管理系统产生，内容包括用户登录尝试、数据修改、错误信息等，交易日志应按照国家会计准则要求予以保存；系统日志由操作系统、数据库管理系统、防火墙、入侵检测系统和路由器等生成，内容包括管理登录尝试、系统事件、网络事件、错误信息等，系统日志保存期限按系统的风险等级确定，日志保存期限不能少于一年。	《商业银行信息科技风险管理指引》》第二十七条	1、访谈相关部门负责人，了解有哪些日志相关安全制度和策略。 2、查阅相关日志，确认其是否涵盖了操作系统、数据库、应用系统、网络等方面，检查日志的保存时间是否超过1年。
	7.4.2	物理访问控制	建立完善的信息系统物理安全管理制度。	a）物理安全管理制度不完善。	a)商业银行应建立完善的信息系统物理安全管理制度，保证重要资源安全。	《商业银行信息科技风险管理指引》第二十一条、第二十三条	访谈相关部门负责人，了解有哪些物理安全制度和细则。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
			设立物理安全保护区域，实现对重要信息科技设备的区域的防护。	b）未能有效实施对重要信息科技设备的保护。	b）商业银行应确保设立物理安全保护区域，包括计算机中心或数据中心、存储机密信息或放置网络设备等重要信息科技设备的区域，明确相应的职责，采取必要的预防、检测和恢复控制措施。应根据职能和安全等级不同划分不同安全区域，并且根据员工工作岗位和职责不同开放相应区域，对安全区域进行保护。	《商业银行信息科技风险管理指引》第二十一条	1、访谈保卫部负责人，了解门禁卡相关的制度和流程。 2、查阅《保卫工作手册》，确认是否对门禁卡的管理做出了完善的规定。查阅相关的文档，确认各部门的访问区域划分合理。
			制定重要信息安全区域的访问控制制度和流程。	c）重要信息安全区域的出入访问控制措施不完善。	c）商业银行应制定人员登记管理制度和流程，对需要访问重要信息科技设备环境（如机房）的人员进行审批和详细记录，确保只有经授权人员才能访问。商业银行应使用电子门禁系统对不同安全区域人员出入进行管理，制定相关门禁系统管理办法。对于外来人员（如第三方技术支持人员或服务商等），特别是从事敏感性技术相关工作的人员，应制定更为严格的审查程序，包括身份验证和背景调查。	《商业银行信息科技风险管理指引》第二十一条	1、访谈保卫部负责人，了解对机房访问管理的制度和流程。 2、查阅《保卫工作手册》，确认是否对机房的访问管理做出了完善的规定。 3、抽样检查外来人员进入生产楼审批表，确认外来人员对机房的访问是否都经过相关管理人员的审批。 4、查阅员工门禁卡权限列表，抽样检查门禁卡访问权限是否与该员工其工作职责相符。 5、从办公室人力资源人员得到审计期间内离职人员名单，抽样检查其门禁卡是否被停用并收回。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
			对重要安全区域视频监控和录像。	d）重要信息安全区域和关键位置缺乏视频监控和录像，出入口应配备保卫人员，并安装警报系统保证保卫人员及时到达现场。	d）商业银行应该对重要安全区域（如核心机房及其出入口）进行不间断的视频监控和录像，出入口应配备保卫人员，并安装警报系统保证保卫人员及时到达现场。	《商业银行信息科技风险管理指引》第二十一条 银监会《2006年度银行业金融机构信息科技风险评价审计指引》第二部分信息安全管理中，物理访问的风险与控制。	1、访谈保卫部负责人，了解24小时视频监控点的布置情况。确认是否有保卫对重要区域进行实时监控。 2、了解视频录像的存放情况，确认录像资料是否都得到妥善保存。
	7.4.3	网络安全管理	制定网络安全管理制度，划分安全区域，实现相关访问控制和边界控制。	a）网络设计不合理。	a）商业银行应制定网络安全管理制度，将内部网络划分为相对独立的安全域，制定和维护相关访问控制和边界控制策略。网络设计须从服务商的选择、网络设备和网络链路的规划等多方面充分考虑到业务连续性要求。	《商业银行信息科技风险管理指引》第二十四条	访谈网络部和安全部负责人，了解网络安全区域划分原则和各安全区域间的边界保护方式，查看与网络服务商、设备供应商签订的合同、服务协议、保密协议。登录网管服务器查看实际网络拓扑图，检查所有外网接入是否符合设计规范，并充分考虑到业务连续性要求，查看应急演练相关文档。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
			对网络变更进行有效管理。	b）对网络结构和配置的变更没有完善的控制措施。	b)商业银行应对网络结构和配置的变更进行管理，建立相应的管理制度和变更流程，对变更情况进行记录。	《商业银行信息科技风险管理指引》第二十四条	访谈网络部负责人，了解网络变更流程和审计期间网络变更情况和变更次数。抽样检查网络变更申请和审批记录，确定是否按照流程规定经过审批，变更操作步骤和回退方案是否描述清楚。变更后是否对网络设备的配置信息进行备份，对备份信息的访问权限是否进行了控制。
			对网络进行实时监控，定期检查日志。	c）缺乏对网络的监控。	c)商业银行应对内部网络进行实时监控和网络设备日志定期检查，并应建立自动报警机制和紧急事件响应流程，保证及时发现异常事件和安全隐患。	《商业银行信息科技风险管理指引》第二十四条	访谈网络部了解网络监控流程，抽样检查网管监控日志，确认异常事件是否进行了跟踪和后续处理。了解网络设备日志管理情况，确定网络设备日志是否开启，是否指定服务器保存和保存期限，是否安排人员定期审核。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
			实现对生产环境网络和办公网络的有效隔离。	d）网络隔离和访问控制手段不足。	d)商业银行的生产环境网络和办公网络应逻辑或物理隔离。对于生产网的接入应有相应的管理办法和控制措施；对远程访问应进行严格控制，并建立相应的管理制度，控制远程访问的方式与范围，远程访问应该经过授权和审批；对远程访问活动应该进行记录，以便进行跟踪查询，并且对记录进行定期的检查；防火墙、入侵检测机制应合理布局，配置遵循安全原则，定期进行漏洞扫描及时发现并处理安全漏洞；应对网络设备特权用户进行管理。	《商业银行信息科技风险管理指引》第二十四条	确定生产环境和办公环境网络是否隔离（测试无线网络是否能与生产环境相通）。访谈ACS系统管理员，了解对网络设备的AAA管理，检查用户权限设置是否与实际的工作职责一致。了解防火墙、入侵检测设备数量和分布情况，确定是否对防火墙策略定期进行审核，了解防火墙系统日志、异常事件、安全事件日志和入侵检测日志进行了审阅，并记录了审阅结果。了解防火墙特权用户的管理、了解ACS静态用户密码设置的管理。
			对所有网络设备配置相关安全参数。	e）未对网络设备进行安全参数配置。未对网络设备划分等级实施保护。	e)商业银行应根据业界标准对网络设备配置安全参数。商业银行应按照人民银行《金融行业信息系统信息安全等级保护实施指引JR/T 0071-2012》标准对网络设备实施等级保护。	《商业银行信息科技风险管理指引》第二十四条、《金融行业信息系统信息安全等级保护实施指引 JR/T 0071-2012》	对网络设备（防火墙、路由器、交换机、负载均衡设备）检查是否配置相关安全参数（远程访问安全、认证授权安全要求、密码加密设置安全要求、接口设置安全要求、网络服务设置安全要求、包过滤安全要求、路由协议安全配置要求、SNMP安全配置要求、日志审计安全配置要求）。
	7.4.4	操作系统及数据库	针对操作系统和数据库系统制定基本安全管理基线。	a）未针对各类操作系统和数据库制定最低安全管理基线。	a)商业银行应制定每种类型操作系统和数据库系统的基本安全管理基线，确保所有系统满足基本安全要求。	《商业银行信息科技风险管理指引》第二十一条	访谈安全部门负责人，了解是否对各操作系统和数据库制定了相应的基本安全要求。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
		安全	对操作系统用和数据库用户权限配置合理的访问权限。	b）操作系统用和数据库用户权限配置不合理。	b）商业银行应明确定义包括终端用户、系统开发人员、系统测试人员、计算机操作人员、系统管理员和用户管理员等不同用户组的访问权限。对用户的授权应符合岗位职责分离和最小授权原则，应定期检查操作系统和数据库的用户权限，如发现与用户岗位职责不符的情况，及时进行调整。	《商业银行信息科技风险管理指引》第二十一条 银监会《2006年度银行业金融机构信息科技风险评价审计指引》第二部分信息安全管理中，逻辑访问的风险与控制	1、访谈安全部门相关负责人，了解各操作系统和数据库用户访问权限的管理办法及实施情况，并查看检查管理办法。 2、对安全部的定期检查记录进行抽样检查，同时查看对那些发现的问题，各系统部门是否做了相关的整改。
			对高权限用户的操作进行管理。	c）未对高权限用户的操作进行管理。	c）商业银行应制定最高权限系统账户的审批、验证和监控流程，并确保最高权限用户的操作日志被记录和监察。	《商业银行信息科技风险管理指引》第二十一条、第二十五条	抽样验证高权限的系统账户的授权审批以及是否有对其日志的审计。
			对关键的高风险操作系统漏洞进行完善管理。	d）未对关键的高风险操作系统漏洞进行修复。	d)商业银行应要求技术人员定期检查操作系统可用的安全补丁，并报告补丁管理状态，及时修复关键的高风险漏洞。	《商业银行信息科技风险管理指引》第二十一条、第二十五条	检查操作系统的补丁安装机制，抽样检查操作系统补丁的安装情况。
			建立操作系统用户账户的访问权限控制制度和设置流程。	e）缺少对操作系统权限变更的有效控制。	e)商业银行应当建立操作系统访问权限的批准程序，操作系统中所有用户账号以及权限的变更需经过正确的授权。	《商业银行信息科技风险管理指引》第二十一条、第二十五条	访谈了解是否有对系统日志的检查机制，检查检查记录。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
			对操作系统和数据库的日志进行适当管理。	f）未对操作系统和数据库活动日志进行定期的检查。	f)商业银行应在操作系统和数据库的交易日志和活动日志进行定期的检查，审阅系统出现的任何异常事件，定期汇报监控情况。	《商业银行信息科技风险管理指引》第二十一条、第二十五条	抽样验证高权限的系统账户的授权审批和变更审批情况。
			实现对操作系统的防病毒安全管理。	g）没有安装防病毒软件，或未及时更新、分发病毒库，未定期开展病毒扫描。	g）商业银行应在操作系统上安装防病毒软件，并确保防病毒软件均更新到最新病毒码。商业银行应部署扫描软件，及时发现未安装授权防病毒的计算机，应定期生成防病毒报告，提交给相应负责人。	《商业银行信息科技风险管理指引》第二十一条、第二十五条	1、访谈相关人员，并查看相关管理规定，了解与防病毒相关的管理制度。 2、查看防病毒服务器上的防病毒软件及其版本号、更新日期确认其进行了及时更新。 3、抽查客户端的防病毒软件版本号、升级日期是否符合相关管理规定。
	7.4.5	数据安全管理	制定信息安全方面的数据分类标准和级别定义，以及相应的安控措施。	a）缺乏对数据的分类标准、安全级别定义和安全控制措施。	a)商业银行应根据安全及保密政策对信息资产进行分类，并采取相应的安全处理措施。	《商业银行信息科技风险管理指引》第二十一条	1、访谈相关部门的负责人，了解是否存在数据分类制度流程。 2、审阅相关文档，检查具体的数据分类情况。
			制定对客户相关信息的全方位的信息安全保护制度和流程。	b）未制定对客户信息的保护制度和流程。	b）商业银行应制定相关制度和流程，严格规范客户关键和敏感信息的采集、处理、存贮、传输、分发、备份、恢复、清理和销毁等环节的管理。	《商业银行信息科技风险管理指引》第二十一条	1、访谈相关部门的负责人，了解是否客户数据相关管理制度。 2、审阅项目相关文档，检查具体的数据管理情况。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
			建立存储介质的存放、借用、运输交接和销毁等管理规定。	c）存储介质的访问控制措施不完善。	c）商业银行应建立存储介质的存放、借用、运输交接和销毁等管理规定，包含敏感信息的存储介质应该有专责部门或人员负责保管，调阅、复制这些存储介质等操作应该得到适当的授权。	《商业银行信息科技风险管理指引》第二十一条	1、访谈运维部、系统部负责人，查阅相关的制度，确认对存储介质的存放、借用、销毁等做出了完善的规定。 2、查看放置存储介质的库房。抽样检查相关记录，确认存储介质的存放、借用、销毁等是否都有专人监控和相应管理人员的授权。
			对包含有商业秘密、敏感信息、信息资产等重要数据文档进行适当的安全管理。	d）未能对重要文档进行安全管理。	d)商业银行应对包含有商业秘密、敏感信息、信息资产等重要数据文档的存放和使用进行管理，从而保证重要文档的安全。	《商业银行信息科技风险管理指引》第二十一条	1、调阅相关工作手册，确定数据中心是否建立完善的文档保存制度。 2、对于纸质文档是否进行标识、分类，存放的地点等情况进行现场检查。 3、对保存电子文档的文档服务器安全情况进行检查，确认对文档服务器的访问权限进行控制，访问需要得到相应的授权与审批。
			使用符合国家要求的加密技术和加密设备对涉密信息进行加密，防范在传输、处理、存储过程中出现泄露或被篡改的风险。	e）未使用适当的加密技术对涉密信息进行加密。	e)商业银行应使用符合国家要求的加密技术和加密设备，防范涉密信息在传输、处理、存储过程中出现泄露或被篡改的风险。应对管理、使用密码设备的员工进行严格审查和专业培训。应确保加密强度满足信息机密性的要求。应建立密码设备管理制度，制定并落实有效的管理流程，尤其是密钥和证书生命周期管理。	《商业银行信息科技风险管理指引》第二十一条	1、访谈安全相关部门负责人，了解有哪些加密相关的安全制度和细则；了解有哪些具体的加密解密设备和技术。 2、了解是否对涉密员工进行审查和培训，检查培训记录，了解加密机制，评估加密强度是否满足信息机密性的要求，了解密码设备的管理制度，抽样密钥的使用和管理记录，检查使用和保管情况。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
			建立完善的密钥管理制度。	f）缺乏完善的密钥管理制度流程。	f）商业银行应建立完善的密钥管理制度流程，以支持组织使用密码技术。	《商业银行信息科技风险管理指引》第二十一条	访谈相关人员了解密钥管理制度，以及密钥产生、变更、撤销、销毁、分发、认证、存储、登记、使用和归档流程。
			根据的密钥管理制度对密钥的生命全过程进行适当管控。	g）密钥管理不符合制度要求。	g）商业银行应根据密钥管理制度，对密钥的产生、变更、撤销、销毁、分发、认证、存储、登记、使用和归档流程进行适当稳妥的管控，以免密钥遭到修改或泄露。	《商业银行信息科技风险管理指引》第二十一条	抽样检查密钥产生、变更、撤销、销毁、分发、认证、存储、登记、使用和归档的记录，检查流程是否符合制度要求。
	7.4.6	应用系统访问控制管理	建立有效的用户认证管理和访问控制的流程，并对用户进合理授权。	a）用户对数据和系统的访问权限设置不正确。	a)商业银行应建立有效的用户认证管理和访问控制的流程。用户对数据和系统的访问必须选择与信息访问级别相匹配的认证机制，并且对用户的授权应符合岗位职责分离和最小授权原则，对关键或敏感岗位进行双重控制。用户调动到新的工作岗位或离开商业银行时，应在系统中及时检查、更新或注销用户身份。明确定义终端用户和信息科技技术人员在信息系统安全中的角色和职责。	《商业银行信息科技风险管理指引》第二十一条、第二十二条	访谈安全部门负责人，了解用户认证管理和访问控制的机制和操作流程。是否有统一的用户管理系统，检查是否对用户的变动情况及时更新到各个系统。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
			对保存的特权用户的日志进行定期审核。	b）未对应用系统中用户的访问权限定期进行审核。	b)商业银行应保留应用系统管理员和其他超级用户的系统日志，指定专人定期对系统用户权限和日志进行审核，监控和审查未成功的登录和用户账户的修改。	《商业银行信息科技风险管理指引》第二十一条、第二十二条	访谈安全部门负责人，了解是否有对系统管理员和其他超级用户的日志的定期审核机制和审核记录，检查相关的审核记录。
			对系统的输入和输出进行合理的安全控制设计。	c）未对系统的输入输出进行安全控制。	c)商业银行在关键的接合点进行输入验证或输出核对，采取安全的方式处理保密信息的输入和输出，防止信息泄露或被盗取、篡改。系统按预先定义的方式处理例外情况，确保系统被迫终止时，能够向用户提供必要信息。	《商业银行信息科技风险管理指引》第二十一条、第二十二条 银监会《2006年度银行业金融机构信息科技风险评价审计指引》第二部分信息安全管理中，网络安全控制。	1、访谈项目开发人员，了解是否对关键的输入输出有安全相关控制。 2、抽样项目开发文档，检查系统例外的输出控制。
			对应用软件和数据库管理系统的日志妥善保存并定期审阅。	d）未对交易操作日志进行妥善保存和定期审阅，但不得少于三年。	d)商业银行应对应用软件和数据库管理系统产生的交易日志按照国家会计准则要求予以保存并定期审阅。	《商业银行信息科技风险管理指引》第二十一条、第二十二条	1、访谈安全部门负责人，并查阅制度手册，了解日志审阅流程。 2、抽样检查日志分析报告，确定是否对系统日志、异常事件和安全事件日志进行了审阅，并记录了审阅结果。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
	7.4.7	终端设备安全管理	实现对各类终端设备信息安全的有效控制	商业银行对重要终端设备缺少安全保护措施。	商业银行应配备切实有效的系统，确保所有终端用户设备（如：台式个人计算机（PC）、便携式计算机、柜员终端、自动柜员机(ATM)、存折打印机、读卡器、销售终端（POS）和个人数字助理（PDA）等）的安全，并定期对终端设备进行安全检查，及时发现控制漏洞并进行整改。	《商业银行信息科技风险管理指引》第二十九条	访谈安全部门负责人，了解用终端安全相关的规章制度。是否有定期的安全检查记录，抽样安全检查记录和相关的问题发现及整改记录。
7.5 信息系统开发、测试和投产	7.5.1	总体管理	制定了完善的项目管理相关制度和规定。	a）未建立信息系统开发、测试和维护管理制度，相关流程缺乏规范。	a）商业银行应制定相关制度，规范信息系统需求分析、规划、采购、开发、测试、部署、维护、升级和报废等流程，管理信息科技项目的优先排序、立项、审批和控制。	《商业银行信息科技风险管理指引》第三十二条	1、与开发部门负责人访谈，查阅目前已经制定与系统开发相关的制度和规范。 2、确认这些制度中，包括了对项目的审批流程、参与部门的职责划分、时间进度和财务预算管理、质量检测、风险评估等内容。确认这些制度涵盖了项目全周期的各个过程，包括立项、可行性分析、制定需求、方案设计、程序开发、系统测试、系统验收、使用培训、实施操作和维护等方面。
			实现对项目开发生命周期的全过程的管理。	b）未采取适当的系统开发方法，控制信息科技项目生命周期。	b）商业银行应结合自身实际情况，根据信息科技项目的规模、性质和复杂度，采取适当的系统开发方法，控制信息科技项目的生命周期。项目生命周期包括可行性研究、需求定义、系统分析、设计、开发或外购、测试、试运行、部署和维护。	《商业银行信息科技风险管理指引》第三十二条	1、访谈开发部门负责人，了解项目生命周期各阶段的管理相关制度。 2、检查重要项目的开发方法以及各阶段的管理是否符合制度要求。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
			在信息科技项目管理各环节中及时控制项目相关风险。	c）对信息科技项目相关风险缺少认识和管理。	c）商业银行应在信息科技项目管理各环节中，及时识别并跟踪信息科技项目相关的风险（包括潜在的各种操作风险、财务损失风险和因无效项目规划或不适当的项目管理控制产生的机会成本），并报告利益相关方，及时采取适当的项目管理方法，控制信息科技项目相关的风险。	《商业银行信息科技风险管理指引》第三十二条、第三十三条	1、访谈项目架构负责人，了解对项目的风险控制制度和流程； 2、按照抽样原则，随机选取开发项目样本，检查项目抽取开发项目样本，调阅评审会议纪要检查是否有相关风险评估记录。
			对不同平台下的数据库、存储、中间件、操作系统、性能容量、灾备和自动化等方面，以及信息系统的架构设计、参数设计、日志设计、风险防范设计等方面制定正式的技术规范。	d）未针对不同的技术平台、技术架构、信息系统建立适用的技术规范。	d）商业银行应制定并印发正式的技术规范，对不同平台下的数据库、存储、中间件、操作系统、性能容量、灾备和自动化等方面，以及信息系统的架构设计、参数设计、日志设计、风险防范设计等方面做出具体规定，确保信息系统的正常运行以及数据的完整性、保密性和可用性。	《商业银行信息科技风险管理指引》第三十二条	1、访谈项目负责人，了解并调阅项目开发技术规范。 2、按照抽样原则，随机选取开发项目样本，检查项目开发技术规范的符合情况。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
			建立完善的项目质量控制机制，监督项目全过程质量。	e）缺乏对项目全过程的质量控制。	e）商业银行应建立项目质量控制机制，监督项目全过程质量，对发现的问题（含不符合项）进行跟踪处理，确保项目符合开发规范，并对项目过程的实际执行情况进行客观评价。	《商业银行信息科技风险管理指引》第三十六条	1、访谈质量管理人员，了解项目开发过程中的质量监督工作的开展情况； 2、按照抽样原则，随机抽取开发项目样本，检查 在项目时间里是否有定期提交质量报告。 3、按照抽样原则，以抽查的开发项目所有质量报告为样本总量，随机抽取并检查报告内容是否完整。
			建立项目进度控制机制，对项目进度进行跟踪和监督。	f）未能按计划完成项目各关键时间节点的进度任务。	f）商业银行应按照各任务时间节点的要求，按时完成各节点工作任务。应确保对项目进度的监督，及时沟通项目进程中遇到的问题，对项目进度进行有效的控制，以避免影响项目目标的实现。	《商业银行信息科技风险管理指引》第三十四条	按照抽样原则，随机选取开发项目样本，检查项目概算与决算： - 项目概算表的内容及其时效性；
			建立项目文档质量管理制度，确保文档的编写质量，以及对文档实行适当保存。	g）缺乏对信息系统相关文档的编写质量控制和统一管理。	g）商业银行应参照《GB8567-88 计算机软件产品开发文件编制指南》等相关国家标准和行业标准，提高项目开发计划、软件需求说明书、系统设计说明书等系统开发相关文档的编写质量，并应建立相应的文档管理制度，集中存放和保管信息系统相关文档。	《商业银行信息科技风险管理指引》第三十二条、第三十七条 《GB8567-88 计算机软件产品开发文件编制指南》	1、访谈项目负责人，了解并调阅项目开发文档编写规范。 2、按照抽样原则，随机选取开发项目样本，检查项目开发文档及其内容与规范的符合情况。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
	7.5.2	立项管理	对项目进行技术、经济和社会等全方面的可行性分析，并审核通过。	a）未对项目进行全面的可行性分析。	a）商业银行应对项目进行技术、经济和社会方面的可行性分析，并出具可行性分析报告，确定项目立项的可行性，保证资源的合理使用，避免浪费。应制定立项审批流程，由技术和业务人员共同对项目的成本、安全、风险、技术可行性、投入产出比等方面进行审核，审核通过后方可进入研发流程。	《商业银行信息科技风险管理指引》第三十二条	按照抽样原则，随机选取开发项目样本，检查项目抽取开发项目样本，调阅评审会议纪要，确认是否有《可行性分析报告》，是否经评审会评审
			制定项目合理有效的实施计划，以应明确各阶段的工作内容和相关管理措施。	b）未建立项目计划或计划不完整。	b）商业银行应根据信息系统开发项目的重要性、紧急程度、规模等要素，建立信息科技项目实施的优先级原则，并据此确定项目的先后次序。并应依据项目的规模和重要程度，选择适当的项目计划的审批流程。在项目实施之前，需制定实施计划，以应明确各阶段（如需求定义、系统分析、设计、开发或外购、测试、试运行、部署等）的主要任务、执行顺序与优先级，任务工期、成本和预算，所需资源、人员分工与职责等内容。	《商业银行信息科技风险管理指引》第三十二条、第三十三条	1、访谈项目负责人，了解《项目计划》的上报流程及其内容； 2、按照抽样原则，随机选取开发项目样本，检查项目计划情况： -《项目计划》的内容是否完整 - 查看是否明确了业务需求的提交时间、业务需求的确认时间等重要里程碑时间点以及各阶段人员安排
	7.5.3	需求管理	业务部门必须提出明确需求。	a）业务需求模糊、范围界定和目标不明确。	a）商业银行应由需求部门提出具体的业务需求，明确描述业务目标与范围，详细列出业务对系统的要求，包括功能和风险控制要求。	《商业银行信息科技风险管理指引》第三十二条； 银监会《银行业金融机构信息系统风险管理指引》第三十六条	抽取开发项目样本，查看《业务需求书》，确认业务需求是否详尽，描述是否清晰。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
			必须组织项目相关人员对需求进行全面完整的分析。	b）对业务需求缺少全面的分析。	b)商业银行应组织需求提出相关业务人员和科技人员共同对业务需求进行分析，将用户需求转化为系统需求，确定系统效率、效果、保密性、完整性、可用性、符合性和可靠性等非功能性需求，同时确定需求实现方式是采用自行开发或者购买现成的商品化软件。	《商业银行信息科技风险管理指引》第三十二条	1、访谈项目负责人，了解项目需求的分析过程 2、抽取开发项目样本，查看《需求分析书》，确认需求分析是否完整，描述是否清晰明确，是否包含了非功能性需求的内容。
			对业务需求的分析结果经过业务人员、开发人员，以及利益相关方的共同确认。	c）开发人员需求分析结果没有经过利益相关方的确认。	c)商业银行应确保最终交付开发人员的需求分析结果经过业务人员、开发人员，以及利益相关方的共同确认，并经过业务主管人员的审核，以避免项目后期再调整需求造成的成本增加和资源浪费，同时避免开发人员对业务需求的理解产生偏差，影响系统开发的效用。	银监会《银行业金融机构信息系统风险管理指引》第三十六条；《商业银行信息科技风险管理指引》第三十二条	抽取开发项目样本，查看《业务需求分析说明书》和评审会纪要，确认其是否经评审，并经业务牵头部门确认；查看有无业务部门回复的《业务需求分析说明书确认函》。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
			建立完善的需求变更申请、审批流程。	d）未建立完善的需求变更流程。	d）商业银行应建立完善的需求变更流程。应由需求牵头部门发起需求变更，向项目承担部门提供详细的需求变更材料。项目承担部门应组织相关人员对需求变更进行分析评估，对项目规模的变化、工作量、项目进度、项目质量等方面的影响进行评估，并将变更评估意见反馈需求牵头部门。	《商业银行信息科技风险管理指引》第三十二条，第三十五条（四）	检查《需求变更明细清单》，随机抽查发生需求变更的开发项目： - 确认对应需求变更是否经由业务部门向承担部门以正式渠道提出。 - 确认对应需求变更是否存在对应的《需求变更处理意见反馈表》。确认对应需求变更处理是否符合本行实际操作流程。 - 确定项目开发过程中的需求变更都有相应的《项目变更申请表》。 - 检查《项目变更申请表》的内容确定其包含变更影响的内容。 - 检查《项目变更申请表》变更评审会议纪要,确认变更是否经审核。
			建立对项目规模的合理评估计量方法，对项目的人力和物力投入进行计算。	e）未建立对项目规模进行评估。	e)商业银行应针对大型或关键信息科技项目的规模建立评估和计量方法，用以确定项目资源、成本与预算。	《商业银行信息科技风险管理指引》第三十二条	按照抽样原则，随机选取开发项目样本，检查项目概算与决算： - 项目概算表的内容及其时效性；

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
			建立与项目相应的项目工作组，以保证信息系统研发质量和进度。	f）项目工作组成员缺乏相关业务知识和技术经验。	f)商业银行应针对项目指定项目经理和相关专业经理，并建立项目工作组。项目工作组由业务人员、技术人员和管理人员组成，具体负责整个项目的开发工作。项目工作组人员应具备与项目要求相适应的业务经验与专业技术知识，小组负责人需具备组织领导能力,保证信息系统研发质量和进度。	银监会《银行业金融机构信息系统风险管理指引》第三十三条、三十四条；《商业银行信息科技风险管理指引》第三十二条	1、抽取开发项目样本，查看项目计划书中列示的项目组人员，确认是否包含业务、技术、管理人员。 2、访谈技管办和项目经理，了解项目组人员是否具备与项目要求相适应的业务经验与专业技术知识。 3、抽取项目组成员的资质证明、培训记录以及工作考核记录或履历表等信息。
	7.5.4	系统设计	对系统开发的关键内容进行分析和审核。	a）未确定系统关键内容并对其进行评审；	a）商业银行应确定系统总体架构设计、技术实现手段、系统与其他外部系统的接口定义及逻辑关系、系统内部的关键数据结构、界面及模块流程、系统错误处理和资源要求等内容，并对这些重要内容进行正式评审，评审必须有产品使用部门的有关人员参与。	《商业银行信息科技风险管理指引》第三十二条、第三十四条	1、访谈项目负责人，了解系统的开发方法是否与项目的具体规模和复杂度相一致。 2、抽取开发项目样本，查看其《总体方案》，确认是否包括了系统的技术实现手段；与其他外部系统的逻辑关系；系统内部的关键逻辑结构等。 查看相关项目评审会的会议纪要，确认是否对《总体方案》进行了审核。 3、抽取开发项目样本,查看相关项目评审会的会议纪要，查看其《项目目标定义书》是否得到技术部门管理层的审批。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
			编制对系统性能安全和环境需求等方面内容的分析文档，文档应通过评审。	b）系统性能安全分析、环境需求分析不详尽。	b)商业银行应由项目承担部门根据项目实际需要组织编制针对系统性能安全和环境需求等方面内容的分析文档，并组织召开项目运行部门参加的评审会。项目运行部门应分析研究上述内容对生产系统的影响，并结合生产运行维护要求提出有关建议。	银监会《银行业金融机构信息系统风险管理指引》第三十六条；《商业银行信息科技风险管理指引》第三十二条	抽取开发项目样本，查看《非功能性需求说明书确认函》和《非功能性需求说明书》和评审会议纪要，确认是否经评审。
	7.5.5	编码及自测	建立系统编码方法和代码规范，从而确保编码的质量和一致性。	a）缺乏规范的编程方法和编码规范。	a)商业银行应确立统一的编码方法和代码规范，从而确保编码的质量和一致性，以便于独立审核和软件维护。	《商业银行信息科技风险管理指引》第三十二条	1、查看是否存在关于代码编写的政策或规定。 2、访谈相关技术开发人员，了解目前采取了何种标准的编程方法和编码规范。 3、查看该编码规范的相关内容。 4、抽取开发项目样本，检查是否按照软件开发部门的编码规范进行代码检查。 5、查看对于外部资源编写代码是否进行覆盖率为100%的代码安全检查。
			根据项目的实际情况制定相应的代码检查计划和代码检查内容。	b）未及时制定代码检查计划或代码检查方式。	b)商业银行应按项目计划要求及时制定代码检查计划，同时根据每个程序特点确定不同的检查点。项目组根据项目自身特点，编制合适的代码检查表，检查点的内容必须详细、准确。编码完成后，开发人员和负责代码检查人员应进行程序代码检查，登记代码检查表，跟踪问题的解决。	《商业银行信息科技风险管理指引》第三十二条	1、访谈项目负责人，了解项目检查计划的相关制度。 2、检查重要项目开发过程中的质量监督工作的开展情况；抽取开发项目样本，检查是否存在代码检查计划，检查是否按照软件开发部门的编码规范进行代码检查。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
			建立项目版本控制管理制度，包括配备版本管理人员对版本的制作和交付进行有效的检查和管理。	c）缺乏项目版本管理。	c）商业银行应建立项目版本控制管理制度。应对项目配备版本管理人员，在进行程序开发时，确保每次在最新的代码基础上进行更改；当多名程序员同时进行更改工作时，能够做好相互协调；在交付版本制作过程中，版本管理员应对程序包内容与版本说明书中的程序内容进行检查比对，确保程序包内容与版本说明书程序内容一致。	《商业银行信息科技风险管理指引》第三十二条	按照抽样原则，抽样检查具体项目，检查： -版本更新过程中，实际提交的程序包内容与版本说明书中的程序内容是否一致。 -版本提供单位是否存在重复发布相同版本的现象。
	7.5.6	项目测试	对项目测试人员进行相关内容的培训，以确保项目测试的质量。	a）测试人员未经过项目测试相关内容的培训。	a）商业银行应针对项目组织测试培训，确保测试人员能很好地掌握版本的基本要求，以保障测试质量和测试进度。	《商业银行信息科技风险管理指引》第三十二条	1、检查培训计划及实施记录； 2、抽查培训教材。
			项目测试和验收应有业务相关人员的参与。	b）业务相关部门人员未参与测试。	b)商业银行应组织需求提出部门和相关业务人员参与版本测试及验收。	《银行业金融机构信息系统风险管理指引》第三十三条;《商业银行信息科技风险管理指引》第三十二条	抽样检查《测试方案》，调阅是否有业务部门会签投产意见。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
			项目测试前应编制有测试方案和测试计划。	c）测试方案、测试计划等文档缺失。	c）商业银行应编制测试方案、测试计划等文档。应按照项目计划的要求确定测试目标、测试范围、测试软硬件配置、测试规模分析等内容，具体文档包括《测试计划》、《测试方案》和《测试案例》等。	《银行业金融机构信息系统风险管理指引》第三十八条。《商业银行信息科技风险管理指引》第三十二条	1、抽取开发项目样本，确认项目组是否制定了单元、集成和系统测试的《测试计划》、《测试方案》和《测试案例》，确认测试计划和方案是否包括各种测试的时间安排，是否对各种测试制定出明确的测试步骤，是否列明各种测试需要的系统设置要求等内容。 2、查阅评审会议纪要，确认计划和方案是否经评审。
			测试内容应于业务需求相一致，并包含非功能性需求。	d）测试与业务需求不一致或测试内容不完整。	d）测试内容应依据业务需求进行，具体应包括用户功能、业务流程、安装测试、备份恢复等方面的测试。测试内容应该尽量全面和完整，还须包括性能容量、系统兼容性、业务特殊时间点（计利和年终结算）等，如有非功能性需求也必须包含在内。	《商业银行信息科技风险管理指引》第三十二条	抽样检查验收测试的《测试计划》及测试文档,确定是否包括用户功能、业务流程、安装测试、备份恢复等方面的测试。
			项目测试应按测试计划进行，应控制测试的进度和质量。	e）未能有效按测试计划实施测试方案。	e)商业银行应根据测试计划组织实施验收测试及适应性测试工作并全面监控测试质量，控制测试整体进度。应根据测试发现问题轻重缓急程度进行分类，实施相应的分级报告和处理。	《商业银行信息科技风险管理指引》第三十二条	1、抽样检查验收测试及适应性测试样本，抽取《测试周报》确认是否包括相关版本测试的测试质量监控及测试整体进度信息。 2、检查是否有测试管理平台，抽取测试版本样本,从中抽取测试问题,看是否分级报告或补报。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
			测试结束后应有科技和业务部门共同确认的报告。	f）测试结束未见测试验收报告。	f）商业银行在适应性测试完毕及验收后，编写《验收测试报告》或《投产确认书》，并经业务主管部门审批。	《商业银行信息科技风险管理指引》第三十二条	1、抽取测试版本样本，确认是否有《投产确认书》和《验收测试报告》； 2、《投产确认书》和《验收测试报告》是否经主管总经理审批。
	7.5.7	投产与推广	建立完善有效的投产问题管理流程，确保问题的记录、跟踪和解决流程符合流程规范。	a）缺乏有效的投产问题管理制度流程。	a)商业银行应建立并完善有效的投产问题管理流程，以确保全面地追踪、分析和解决信息系统问题，并对问题进行记录、分类和索引；如需供应商提供支持服务或技术援助，应向相关人员提供所需的合同和相关信息，并将过程记录在案；对完成紧急恢复起至关重要作用的任务和指令集，应有清晰的描述和说明，并通知相关人员。	《商业银行信息科技风险管理指引》第三十七条、第三十二条	1、访谈推广部门负责人，了解推广部作为开发中心对外服务的窗口的作用。 2、查看《技术支持管理手册》，了解技术支持管理的流程。 3、抽样检查事件记录，检查开发中心答复的时效性是否符合要求。
			评估对系统投产的风险，形成风险评估报告。	b）对应用系统的投产没有进行风险评估。	b）商业银行应充分识别、分析、评估重要应用系统投产风险，包括系统功能缺陷、客户信息泄露、业务中断、交易缓慢或其他因素可能造成的操作风险、法律风险和声誉风险，并形成风险评估报告。	《商业银行信息科技风险管理指引》第三十二条	1、访谈项目负责人，了解系统投产风险评估相关制度。 2、检查对重要信息系统的投产评估是否有风险评估报告。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
			建立完善的项目投产制度和流程，投产过程符合流程规范。	c）未制定完善的应用系统投产流程。	c）商业银行应用系统的投产计划需经管理部门正式批准。系统投产前应进行充分的测试并验收，对版本进行控制，保证只有经过测试验收的版本才能用于投产。重要应用系统投产前测试结果应经过信息科技部门和相关业务部门确认，形成测试验收报告，确保系统上线后的正常稳定运行以及系统功能与业务目标的一致性。在确认测试完成后，正式批准并发布投产通知，投产交付资料必须齐全详细，如测试报告、投产方案、版本说明书和正式印发的系统投产通知（如有数据移行，应包含数据移行测试结果）。投产前完成对运行操作人员、技术支持人员、业务人员的相关培训。重要应用系统投产过程中，严格执行投产方案，加强监督与复核，避免操作失误和非法操作。所有的利益相关方能及时了解应用系统的整个投产过程，与投产相关的文档资料应由具体人员负责完整保存。	《商业银行信息科技风险管理指引》第三十二条	1、访谈项目负责人，了解系统投产的相关的制度和管理办法。 2、查看项目投产前、中、后的相关文档是否缺失，是否符合相关制度对项目投产必须文档的要求，查看文档内容是否完整。 3、查看是否有投产相关人员培训的记录。 4、查看投产方案的具体执行情况，检查重要应用系统是否有操作的监督和复核记录。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
			制定信息系统推广计划，并经归口管理部门和用户部门审核批准。	d）系统推广缺乏完整可行的推广计划。	d）商业银行应当制定信息系统推广计划，并经归口管理部门和用户部门审核批准。推广计划一般包括人员培训、数据准备、进度安排、应急预案等内容。系统推广涉及新旧系统切换的，银行应当在推广计划中明确应急预案，保证新系统失效时能够顺利切换回旧系统。	《商业银行信息科技风险管理指引》第三十二条	1、访谈推广部门负责人，了解推广部具体的项目推广计划安排。 2、查看具体的推广计划文档，检查推广计划内容是否完整。
	7.5.8	项目后评价	项目投产后需进行总结和评价。	a）缺乏对版本质量的总结评价。	a）商业银行在应用类版本投产后，应对版本质量情况进行总结评价，以便于持续跟踪和改进版本质量。	《商业银行信息科技风险管理指引》第三十二条	1、抽取投产的应用类版本样本，确认是否有对版本质量情况进行总结，并形成报告。
			业务人员参与项目后评价工作有利于问题的发现和解决。	b）项目后评价没有相关业务人员的参与。	b）商业银行应确保有业务人员参与项目后评价工作，以及时发现交付的新系统在运行中暴露的新问题或与需求之间的偏差，从而确保系统的实际使用效率和效果。	《商业银行信息科技风险管理指引》第三十二条	抽取投产的应用类版本样本，确认是否有业务人员参与相关的项目后评价工作。
7.6 信息科技运行管理	7.6.1	总体管理	制定信息科技运行管理办法，设置运行管理部门及相关岗位。	a)未设置清晰的运行岗位。	a)商业银行应制定信息科技运行管理办法，设置运行管理部门及相关岗位，各岗位人员应明确岗位职责和相应的规章制度。如设置操作管理部门、作业调度部门、操作实施部门和技术支持部门等，部门职责应清晰明确。	《商业银行信息科技风险管理指引》第四十三条	1、调阅相关管理办法，查看是否设置运行部门及相关岗位； 2、访谈运行和变更岗的相关人员，了解运行和变更申请、受理、管理、实施和审批部门和岗位的设置情况，并询问对岗位职责的理解。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
			制定信息科技运行操作手册，明确步骤和要求。	b)未制定详尽的运行操作手册。	b)商业银行应制定详尽的信息科技运行操作手册。如在运行操作手册中说明运行人员的任务、工作日程、执行步骤，以及生产与开发环境中数据、软件的现场及非现场备份流程和要求(即备份的频率、范围和保留周期)。当业务运行发生变化时，运行操作手册做出相应调整，变化的部分及时通知运行人员。	《商业银行信息科技风险管理指引》第四十三条	1、调阅运行操作手册，查看是否包括操作任务、工作日程、执行步骤和数据备份流程等； 2、访谈运行操作人员，了解手册是否根据业务运行发生变化时及时更新并接收到通知。
			运行人员具备熟练的操作技能。	c)运行人员缺乏操作技能。	c)商业银行应对运行人员进行上岗培训和考试，并定期对运行人员进行考核。	《商业银行信息科技风险管理指引》第四十三条	1、访谈相关管理人员，了解是否对运行人员进行操作培训和考核； 2、调阅培训记录和考核记录。
			确保运行与系统开发和维护有效分离。	d)运行与开发和维护职责未有效分离。	d)商业银行应将信息科技运行与系统开发和维护分离，确保信息科技部门内部的岗位制约，特别是对数据中心的岗位和职责应做出明确规定。	《商业银行信息科技风险管理指引》第四十一条	1、通过查看相关的文档和与相关管理人员访谈，确定对各技术岗的职责定义完整、准确； 2、访谈操作管理部门、作业调度部门、操作实施部门和技术支持部门的负责人或岗位人员了解部门设置情况和工作内容，检查与制度规定是否匹配。
			严格控制外来人员进入生产安全区域。	e)未严格控制外来人员进入生产区域。	e)商业银行应严格控制外来人员进入生产安全区域，如确需进入应得到适当的批准，其活动也应受到监控；针对长期或临时聘用的技术人员和承包商，尤其是从事敏感性技术相关工作的人员，应制定严格的审查程序，包括身份验证和背景调查。	《商业银行信息科技风险管理指引》第四十条	1、抽样检查外来人员进入生产区域登记表、变更单、门禁记录，了解外来人员背景、进出时间、原因和所携带设备等； 2、抽样检查监控录像确认外来人员是否直接对重要生产设备进行操作。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
			对应用系统进行维护和升级，确保业务的连续可用性。	f)未对应用系统进行日常维护和升级。	f)商业银行应制定相关制度和流程,及时对应用系统进行维护和适当的升级，控制系统升级过程，以确保与技术相关业务的连续可用性，并完整保存记录，包括疑似和实际的故障、预防性和补救性维护记录。	《商业银行信息科技风险管理指引》第四十八条	1、访谈维护部门相关人员，了解系统维护和升级的情况，并查看维护部门的生产维护计划； 2、对于抽取的项目样本，查看软件分发和投产版本出入库记录、升级记录，抽样检查对应用系统的健康检查报告。
			制定硬件维护计划和编制维护手册，对硬件设备定期巡检。	g)对硬件设备缺少定期巡检。	g)商业银行应对硬件设备，包括计算机设备、网络设备、动力设备等进行定期巡检。根据生产系统的服务水平目标制定硬件维护计划、编制维护手册，对生产信息系统进行健康检查，根据检查结果提出改进措施和建议。为防备有突发的硬件容量性能需求，应建立相关的储备和应急响应机制。	《商业银行信息科技风险管理指引》第四十八条	1、访谈数据中心负责人，了解管理层是否制定了设备管理工作手册，对硬件设备维护流程进行了规定； 2、抽样检查相关管理部门是否定期对硬件设备进行维护，并填写日常巡检表。
	7.6.2	机房环境及设施管理	数据中心选址时应充分考虑环境威胁。	a)选择数据中心物理位置时未充分考虑环境威胁。	a)商业银行在选择数据中心的地理位置时应充分考虑环境威胁，如是否接近自然灾害多发区、危险或有害设施、繁忙或主要公路等，采取物理控制措施监控对信息系统运行构成威胁的环境状况。	《商业银行信息科技风险管理指引》第三十九条	1、访谈数据中心负责人，了解在选择数据中心的地理位置时是否充分考虑环境因素； 2、现场观察数据中心物理位置是否接近自然灾害多发区、危险或有害设施、繁忙或主要公路等； 3、现场查看数据中心园区是否有7*24小时监控全覆盖，安全保卫部门是否有应急处理机制等。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
			制定信息系统环境控制和预防性维护应对方案。	b)生产机房缺乏必要的环境控制和预防性维护。	b)商业银行应制定信息系统环境控制和预防性维护应对方案，包括：物理环境适宜度控制（温度、灰尘、湿度等）、计算机连线、消防、防渗水、内部和服务商日常预防性维护的管理等。机房应配备防火、防水、防磁等设施，并由专人对机房环境设备进行监控。	《商业银行信息科技风险管理指引》第三十九条	1、访谈生产机房相关人员，了解与信息系统环境安全有关的制度和机房各种安全设施的情况； 2、查看机房的安全配套设施，具体包括：门禁设备、防火设施、监控设备、空调、温度计、湿度计、通风设备等。 3、查看机房安全设施的巡检和维护记录，确认这些设施被定期巡检和维护。
			生产机房必须拥有持续且稳定的电源供应。	c)生产机房无持续稳定的电源供应。	c)商业银行必须对生产机房设备提供持续且稳定的电源供应。重要生产机房应配备双路电源、发电机、电压稳定器和不间断电源（UPS），不间断电源（UPS）应在全负载情况下至少保证30分钟以上的持续供电，并由专人对电源装置进行定期检查。	《商业银行信息科技风险管理指引》第三十九条	1、与相关部门职员进行访谈，了解并查看相关制度办法，确定其包含了UPS需要定期维护的内容； 2、查看UPS的配置，确定其在全负载的情况下可以提供30分钟以上的持续供电； 3、抽样检查UPS定期维护单，确定有专人对UPS进行定期维护。
			生产机房必须拥有安全撤离计划和疏散通道。	d)生产机房没有安全撤离计划和疏散通道。	d)商业银行应制定生产机房人员安全手册，生产机房有专门的疏散通道和疏散线路图，指导机房人员在发生灾难时疏散，并定期进行演练。	《商业银行信息科技风险管理指引》第三十九条	1、与相关部门的管理人员访谈，了解对机房人员的安全所制定的计划。查看相应的手册内容，确定其对机房人员安全有规定； 2、查看人员疏散计划、疏散通道和疏散线路图，确定灾难发生时，机房人员能及时疏散。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
	7.6.3	批处理管理	制定批量数据处理机制，确保数据处理的完整性、及时性，满足安全保存和恢复要求。	a)没有建立批量数据处理机制。	a)商业银行应按照有关法律法规要求保存交易记录，制定批量数据处理机制，采取必要的程序和技术，确保数据处理的完整性、及时性，满足安全保存和恢复要求。对于新投产应用系统的批量数据迁移，应根据新系统的设置及迁移要求，制定详细的批量数据迁移计划，包括移行准备、移行处理、移行后的工作事项、工作内容、负责部门和起止时间。数据迁移后，对数据的完整性、一致性进行检查，由业务部门确认验收，数据迁移的相关工作记录由专人保管。	《商业银行信息科技风险管理指引》第四十二条	1、通过访谈，确认批处理作业的管理部门及相关部门负责人，了解批处理作业的管理制度和相关业务流程； 2、查看相关制度，了解批处理程序的作业流程，确认数据处理的完整性和及时性； 3、现场查看运行操作人员是否严格按照双人操作、双人复核的要求进行操作与监控，并在日志的操作与复核栏签字；投产新应用时是否制定详细的批量数据迁移计划，包括移行准备、移行处理、移行后的工作事项、工作内容、负责部门和起止时间，投产完成后是否对数据的完整性、一致性进行检查等。
			根据业务变动情况及时更新批处理作业计划。	b)没有根据业务变动情况及时调整批处理计划。	b)商业银行应根据业务变动情况及时更新批处理作业计划，确保批处理作业计划与业务需求相符，每次作业计划和编排的调整以正式变更方式执行。	《商业银行信息科技风险管理指引》第四十二条	1、访谈相关管理人员了解如何制定批处理作业计划，是否根据业务要求调整批处理计划，查看具体变动情况； 2、查看运行操作管理部门是否具备详细的作业编排记录，抽样运行操作日志，确认批处理作业得到调整。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
			制定批处理作业维护手册，要求运行人员必须严格按照手册进行操作。	c)运行人员没有按照要求严格执行批处理操作。	c)商业银行应要求运行人员必须按照规定进行操作，规范批处理作业的建立和维护细则，对各个系统的批处理作业操作做出规定。管理层对批处理作业的新增、修改以及批处理作业计划的编排等操作进行审批授权。运行操作人员应了解各类业务的交接情况，及时查看通知、邮件，按规定处理各类业务。在批处理开始前，对批处理数据进行检查，停止所有相关进程和交易，对数据进行保护。保留批处理日志，对批处理日志进行检查，对发现的问题及时跟踪和处理。	《商业银行信息科技风险管理指引》第四十二条	1、访谈运行操作管理人员，了解如何对批处理操作进行记录和检查。抽样检查排班表、工作交接登记表、操作日志、批处理日志等，检查其是否符合相关流程要求，是否有人进行审核，是否存在审核证据； 2、现场抽样检查运行日志、操作日志、运行日报、交班记录等是否按规定要求进行记录，并进行适当保存； 3、访谈运行操作管理人员，了解在批量处理前是否对数据的完整性、准确性、有效性进行检查，以及检查的具体步骤有哪些，是否有业务部门共同参与； 4、获取批处理程序更新列表，包括数据库、主机系统、开放平台批处理变更日志等，按照抽样原则抽取相关变更，查看其是否符合变更规定；查看数据库、主机系统、开放平台的日志及权限列表，查看都有哪些人员有权对批处理程序进行更改； 5、根据实际情况进行测试，若批处理为手动方式抽查操作日志确认运行人员是否进行了数据检查步骤，关注批处理数据操作日志上是否存在实施证据；若批处理为自动方式，检查批处

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
	7.6.4	服务管理	在科技部门和业务部门之间定义正式的服务水平管理程序。	a)未建立服务水平管理程序。	a)商在科技部门和业务部门之间定义正式的服务水平管理程序，包括定义服务水平协议和运营水平协议。科技部门根据服务实施情况，以及定量和定性评价结果，定期进行服务质量评估，编写服务水平执行情况报告和运营水平执行情况报告。业务部门根据服务水平协议和运营水平协议中的指标体系，定期对科技部门的服务质量进行评价。上级管理部门定期对服务水平和运营水平执行情况进行考核。	《商业银行信息科技风险管理指引》第四十五条	1、访谈相关部门负责人，了解本行是如何监控和考核科技部门为业务部门提供的服务，审阅相关文档检查监控和考核的内容和结果。 2、访谈相关部门负责人，了解服务水平协议的制定及其相关内容，查看服务水平协议确认其包括以下内容：服务要求、衡量服务水平的定量和定性指标、职责分工、对服务水平的持续监督等，确认考虑的因素是否包括：可用性、可靠性、业绩、改进可能性、持续性、安全性等； 3、访谈服务使用部门，了解其如何定期对服务提供部门所提供的服务质量按照服务水平协议所规定的标准进行评估。抽样检查服务使用部门的评估报告，了解是否包含相关的要素。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
			建立连续监控的信息系统，及时、完整地报告例外情况。	b)没有建立连续监控的信息系统。	b)商业银行应建立连续监控信息系统性能的相关程序，及时、完整地报告例外情况；程序应提供预警功能，在例外情况对系统性能造成影响前对其进行识别和修正。	《商业银行信息科技风险管理指引》第四十六条	1、通过访谈运行操作人员了解是否有系统对重要应用和网络性能及负载能力水平进行实时监控； 2、调阅生产操作与监控程序等相关文档，检查监控和处理的内容和方法，抽样检查系统监控和处理的记录和结果，是否包含响应时间、处理业务量、系统承载能力、任务处理失败的次数、比例、类型和原因、系统使用的峰值和均值、系统使用趋向和容量等内容。
			建立事故管理及处置机制。	c)未建立事故处置响应机制。	c)商业银行应建立事故管理及处置机制，及时响应信息系统运行事故，逐级向相关的信息科技管理人员报告事故的发生，并进行记录、分析和跟踪，直到完成彻底的处置和根本原因分析。商业银行应建立服务帮助平台，提供相关技术问题的在线支持，并将问题提交给相关信息科技部门进行调查和解决。	《商业银行信息科技风险管理指引》第四十四条	1、访谈相关部门负责人，了解目前制定了哪些定期的事件或问题的分析机制和报告，并提交到哪些管理层； 2、抽样检查分析报告，其中是否有对问题解决的建议，努力确保不会重复发生类似问题； 3、按时间对问题和事件进行分类统计，分析相似问题和事件是否经常重复发生。
	7.6.5	性能容量管理	对重要设备制定可用性管理办法，定义可用性指标。	a)没有针对重要设备定义关键可用性指标。	a)商业银行应对重要设备，如应用系统服务器、网络、动力、空调等设备制定可用性（性能、容量）管理办法，定义可用性指标，包括单项可用性指标和综合可用性指标。	《商业银行信息科技风险管理指引》第四十七条	1、访谈相关部门的管理人员，了解性能管理方面的制度和流程。 2、查阅可用性及性能管理办法，检查是否清楚定义了重要资源（系统服务器、网络、动力、空调等设备）的可用性指标（性能、容量）。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
			根据业务发展和交易量增长情况，制定信息系统容量规划。	b)未对性能容量进行评估、规划和审批。	b)商业银行应制定信息系统容量规划，以适应由于外部环境变化产生的业务发展和交易量增长。容量规划应涵盖生产和备份系统的相关设备，评价目前系统、网络的性能容量及负载能力，以此为依据对后续扩容进行评估，并提交管理部门审批。	《商业银行信息科技风险管理指引》第四十七条	1、访谈性能容量管理岗人员，查阅优化方案的评估及审批结果； 2、确认是否收集整理监控指标数据，对性能容量异常事件进行分析；是否关注指标变化趋势，进行趋势预测分析；是否定期对生产环境性能容量进行评估，根据评估结果制定性能容量优化方案，实施优化并跟踪确认优化效果；是否综合考虑业务的容量、服务的容量和资源的容量三方面的因素，制定性能容量计划。
			对信息系统性能容量进行全面监控。	c)对信息系统性能容量缺乏全面监控。	c)商业银行应制定对性能容量监控的管理手册和技术文档。运行操作人员应按照要求监控信息系统的性能容量指标，记录相关数据，包括：对系统响应时间和处理量、系统承载能力、任务处理失败的次数、比例、类型和原因、系统使用的峰值和均值、系统使用趋向和容量等。	《商业银行信息科技风险管理指引》第四十六条	1、访谈性能容量监控岗人员，查阅监控手册等技术文档，确认是否建立了性能容量管理程序； 2、现场确认是否根据生产环境各应用系统的性能情况和日常管理需求，设置了系统、网络、应用、设备不同层面的性能容量指标；是否针对每个指标落实了相应的监控手段，突出对重点时段、重点业务的监控。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
			定期对信息系统的可用性和性能容量进行分析。	d)未对信息系统监控指标进行有效分析。	d)商业银行应定期对信息系统的可用性和性能容量进行分析，对照可用性及性能容量的实施计划，找出实际指标与标准指标之间的差距查明原因，结合业务发展趋势，制定改进计划提交相关管理部门。	《商业银行信息科技风险管理指引》第四十六条	1、访谈性能容量管理岗人员，确认是否对信息系统日常监控结果进行记录； 2、对出现异常情况进行分析，找出实际指标与标准指标之间的差距并查明原因。
	7.6.6	配置管理	建立和维护配置信息库。	a)未建立和维护配置信息库。	a)商业银行应建立包含配置项中相关信息的配置库，监控和记录所有配置项的变更，保留系统和服务的配置项基线作为变动后返回的检查点。	COBIT IO07	1、访谈配置管理岗人员，了解配置管理情况； 2、确认是否制定配置管理手册，是否建立配置管理信息系统。
			收集和验证纳入配置管理的IT资源信息。	b)没有识别和收集配置信息。	b)商业银行应收集和验证纳入配置管理的配置信息，为配置信息放入配置管理数据库做好准备，保证即将被纳入配置管理数据库的数据与现实的配置保持一致。	COBIT IO07	访谈配置操作岗人员，了解目前配置管理的处理流程；了解配置管理信息系统实现的机制，是否能确保配置管理数据库的数据与现实配置保持一致。
			控制和维护配置信息。	c)未对已录入的配置信息进行控制和维护。	c)商业银行应录入配置项信息，并确保配置项得到有效控制和及时维护。	COBIT IO07	访谈配置操作岗人员，了解目前配置管理的处理流程；是否能确保系统的配置信息得到有效控制和及时维护。
			对配置信息进行验证和检查。	d)没有对已录入的配置信息进行验证和检查。	d)商业银行应周期性地验证与检查，保证配置项记录数据的准确性。	COBIT IO07	1、访谈配置管理岗人员，了解是否对配置信息进行定期验证与检查； 2、抽样检查配置管理系统的配置信息与现实系统的配置信息进行比对，确保配置项记录数据的准确性。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
	7.6.7	事件、问题和变更管理	建立规范的事件处理流程，并及时通知利益相关部门。	a)没有对事件有效识别和分类。	a)商业银行应对信息系统运行中发生的事件按影响程度、影响范围、影响时段和涉及系统类别、紧急程度进行分级。建立规范的事件处理流程（报告、受理、处理、反馈）和系统帮助平台，及时通知利益相关部门。根据事件管理的内容制定全面衡量管理水平的指标体系，对数据采集、指标计算和对各项指标进行评价，并根据指标发展趋势，制定事件管理的改进计划。	《商业银行信息科技风险管理指引》第四十九条	1、访谈事件管理岗人员，了解生产故障事件、安全事件的相应处理流程，查阅相关制度确定制度中对事件分类的标准； 2、访谈事件受理、分派、处理岗人员，调阅检查生产运行月报、生产运行日报、安全事件报告表、主要生产故障事件统计表、生产邮箱等，确认事件是否全部记录系统内，检查事件补单记录，确认事件单受理、反馈的及时性； 3、登陆系统帮助平台，通过事件单、变更单了解事件与变更之间的对应关系。
			规范问题处理流程，深入分析各类问题发生的根本原因。	b)没有对问题及时处理。	b)商业银行应加强信息系统的问题管理，规范问题处理流程，深入分析各类问题发生的根本原因，落实防范和解决措施。定期组织相关部门对生产系统进行健康检查，主动发现问题及时解决并提交问题分析报告。	《商业银行信息科技风险管理指引》第四十九条	1、访谈问题管理岗人员，如何进行问题的记录萃取； 2、抽查相关部室的萃取的问题和生产系统健康检查报告，登录系统平台抽查是否建立了问题单； 3、抽查问题评价报告和问题根源分析报告。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
			制定严格的变更管理流程。	c)未制定严格的变更管理流程。	c)商业银行应制定严格的变更管理流程，设置相应的职能部门，各变更职能部门和岗位人员应清楚各自职责，对变更进行管理和控制。变更申请须经主管部门审批，审批要素包括变更实施计划、风险评估、验证、应急和回退方案，对业务有可能造成影响的变更，在变更实施前通知相关业务部门。对于一般变更、重大变更、紧急变更、特殊时期变更等有对应的处理流程。所有变更应统一管理，变更的申请、受理、方案、审批等要素填写必须符合要求。所有变更都应记录日志，并事先进行备份。严格监控整个变更实施过程，根据计划的执行时间、环境、顺序、条件等要求并保证双人操作。变更实施完成后，根据变更验证方案对变更的准确性、完整性和授权性情况进行验证，对例外情况进行记录和跟踪，将变更实施结果及时反馈。	《商业银行信息科技风险管理指引》第四十九条	1、访谈数据中心的相关负责人，了解系统变更管理标准，以及在实际中使用的管理工具，了解变更管理及维护阶段角色和岗位职责； 2、查阅变更管理办法及相关实施细则，查看变更管理岗位设置情况和各个岗位的职责描述，确认对变更审批流程进行控制。抽取投产及变更项目样本，检查相关文档是否齐全； 3、访谈变更实施等部门相关人员，了解变更回退策略的相关要求和回退流程。选取变更样本，查看变更实施牵头部门是否组织制定“变更实施计划及回退方案”，有无具体的回退方案或流程，是否提交各相关部门审批。对于变更失败的情况，抽样查看因某种原因导致变更失败的情况的记录，检查实施单位最终审批人决定启动回退方案的授权记录或授权文档。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
			严格控制紧急变更的数量。	d)未对紧急变更进行严格控制。	d)建立、定义、升级、评估和授权紧急变更的流程，应尽量减少紧急变更，通过正常的验收测试和变更管理流程，采用恰当的修正以取代紧急变更。	《商业银行信息科技风险管理指引》第四十九条	1、查阅关于紧急变更管理政策和实施细则中对紧急变更的定义，以及相应的管理流程，是否涵盖如下内容： 紧急变更突发事件定义、分类和优先程度划分、定义授权管理途径，包括人员的角色和责任； 2、访谈相关人员，了解对紧急变更的管理流程。针对抽取的紧急变更样本，确认紧急变更是否经过不同管理职能部门的充分授权，查看授权记录；在紧急变更实施之后是否按照管理制度进行相应的后续测试、记录等工作，并查看相关记录。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
7.7 业务连续性管理	7.7.1	备份管理	根据应用系统的重要性，建立规范和完善的备份管理政策。	a)没有制定完善的备份管理策略。	a)商业银行应根据本行应用系统的重要性，建立规范、完善的备份管理政策，建立合理的数据和程序备份流程、备份保存周期和备份介质存储、借用、运输交接和销毁等管理规定，对备份介质进行本地和异地保存，对备份介质实施严格的访问控制。在紧急情况发生时，备份数据和程序有良好的权限访问控制，由专责部门或人员负责业务持续性规划中涉及的各类文档和资料。	《商业银行信息科技风险管理指引》第五十二条	1、访谈相关部门负责人，了解管理层制定了哪些备份管理政策和流程，以及这些政策和程序是如何有效地与相关员工进行沟通的； 2、查看相关备份制度文件，检查是否包括以下内容：对备份数据和程序清单的更新步骤、备份操作步骤、对数据和程序的备份频率的要求、备份介质保存周期和循环使用、备份介质的标识规则、备份介质的存储规定、备份介质的清理、存储介质借用管理规定等； 3、与相关管理人员访谈，确定对业务连续性计划中涉及的文档和资料进行保管； 4、查看备份介质保存环境是否防水、防电、防火、防磁等； 5、查看备份介质存储场所是否存在有效的访问控制。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
			定期对备份数据进行恢复测试。	b)未对备份数据进行恢复测试。	b)商业银行应对系统程序和数据的备份情况进行定期检查，对备份介质定期进行恢复测试，对恢复测试中出现的问题，记录并及时解决。	《商业银行信息科技风险管理指引》第五十二条	1、访谈相关部门负责人，了解其对备份工作的检查程序，查看数据恢复流程及相关操作手册； 2、抽查数据管理部门对备份介质的恢复测试记录，确保其符合相关规定； 3、抽样检查恢复测试中的问题记录，查看其解决方法是否符合相关规定的要求； 4、抽查相关部门负责人对备份工作的检查记录。
	7.7.2	业务影响性分析	采取必要措施降低突发事件情况下关键业务中断的可能性。	a)在突发事件情况下不能满足应急要求。	a)商业银行应采取负载均衡、系统恢复和双机冷热备等措施降低突发事件下关键业务中断的可能性，并通过应急安排和保险等方式降低事件影响。备份中心及辅助设施的建设、配置、组织机构和操作机制应满足突发事件下关键业务持续运行的容量和运行能力需求。定期对备份中心进行检测、维护和更新，使其性能容量与实际生产环境保持一致，确保突发事件下备份中心的可用性。	《商业银行信息科技风险管理指引》第五十二条	1、与相关的管理人员访谈，了解备份设备与实际生产环境配置是否保持一致，通过发放调查调查问卷的方式，了解备份中心的建设、配置、容量、组织架构和操作机制等情况； 2、调阅近两年来对备份中心的内外部审计报告及整改报告，了解备份中心存在的缺陷及整改情况； 3、查阅相关文档和演习报告，确定数据中心的建设、配置、容量、组织架构和操作机制能满足突发事件下关键业务能持续运行； 4、抽样检查相应的检测、维护报告，确定相关部门是否定期对备份所需的设备定期进行检测、维护。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
			建立针对业务连续性管理的组织架构。	b)缺少业务连续性管理的组织架构。	b)商业银行应设立关于连续性管理的组织架构，包括内、外部服务提供者的角色、任务、职责，以及制定、测试和执行灾难恢复和应急计划的规定。	《商业银行信息科技风险管理指引》第八条	1、查看业务连续性框架，确定是否对相关的管理组织架构、职责作出定义； 2、与相关部门负责人访谈，确认是否成立专门的故障应急处理管理组织；是否制定应急工作计划和有关制度； 3、查看相关计划和制度、判断制度是否健全与合理，是否在上线前在模拟工作状态下，得到过充分的验证。
			评估因意外事件导致业务运行中断的可能性及其影响性。	c)未对业务进行影响性分析和风险评估。	c)商业银行应评估因意外事件导致其业务运行中断的可能性及其影响性，包括评估可能由下述原因导致的破坏：1）内外部资源的故障或缺失，如人员、系统或其他资产；2）信息丢失或受损；3）外部事件，如战争、地震或台风等。商业银行的业务影响性分析和风险评估应覆盖银行所有部门、系统，通过业务影响分析建立分级文档，排定恢复关键数据和系统的优先顺序，合理地确定每项业务职能容许恢复的最长时间和可接受的损失水平。风险评估还应考虑到信息系统、人员、设备、服务提供商等事项风险发生的可能性。业务影响分析和风险评估最终结果应经过高级管理层审批。	《商业银行信息科技风险管理指引》第五十一条	1、与相关部门负责人访谈是否进行业务影响分析和风险评估，查看相应的评估文档是否具备；识别关键业务流程、关键应用、关键信息系统的策略及具体清单等文档； 2、确定业务影响分析和风险评估是否覆盖全部应用系统；调阅中断级别的确认策略，确定各种级别的中断对业务的影响程度的策略，调阅相关评估文档及记录； 3、了解对应用系统业务影响的评估结果，以及各级系统恢复的优先级；相关策略及标准等是否得到管理层批准； 4、确定业务影响分析和风险评估是否满足应用系统灾备需求，调阅业务分析影响所涉及各种资源的清单； 5、与相关部门的管理人员访谈，了解对业务影响分析和风险评估结果的审批流程，确定管理人员是否认可影响分析； 6、查看相关的审批记录，确定上述评估结果都得到管理层的审批。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
	7.7.3	业务连续性计划	根据业务的性质、规模和复杂程度制定适当的业务连续性计划。	a)没有制定业务连续性计划和应急预案。	a)商业银行应根据自身业务的性质、规模和复杂程度制定适当的业务连续性计划，以确保在出现无法预见的中断时，系统仍能持续运行并提供服务；连续性框架要与银行的业务发展策略保持一致性，连续性计划覆盖的范围应该包括银行关键应用系统和网络，计划应包括关键资源的识别、关键资源可用性的监控和报告、可替代的处理设施以及备份和恢复原则。成立专门的应对突发事件的管理组织架构，制定应急工作计划和有关制度，针对可能出现的情况制定相应的应急操作手册，经过评审后进行归档。	《商业银行信息科技风险管理指引》第五十条、第五十三条	1、查看业务连续计划，确定其涵盖了银行的关键业务和关键业务系统，确定是否对关键资源的识别、关键资源可用性的监控和报告、可替代的代理设施、备份和恢复原则作出定义； 2、确定是否对业务连续性计划和应急预案的测试和执行作出规定，确定测试执行计划安排是否合理。
			定期对业务连续性计划进行更新，确保其有效性。	b)未及时更新和发布业务连续计划。	b)商业银行应定期对业务连续性计划进行更新，保证其有效性，并根据演练情况对应急操作手册进行修订，制定业务连续性计划发布的策略以确保计划能正确和安全地下发给授权的相关人员。对应急人员进行培训，使其了解突发事件发生时他们的角色和责任以及应该执行的流程。	《商业银行信息科技风险管理指引》第五十三条	1、与相关管理人员访谈，了解业务连续性计划培训情况并查看是否进行培训，了解培训目标和内容，确定是否涵盖角色和责任的培训； 2、与相关管理人员访谈，了解业务连续计划的更新和下发流程；与运行操作人员访谈，了解他们是否定期收到更新的业务连续性计划。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
			定期对业务连续性计划进行测试和演练，确保紧急情况下业务连续性计划得以有效实施。	c)对业务连续性计划没有进行定期的测试和演练。	c)商业银行应对业务连续性计划进行定期测试和演练，保证紧急情况下业务连续性计划得以正确有效实施。商业银行的业务连续性计划和年度应急演练结果应由信息科技风险管理部门或信息科技管理委员会确认。	《商业银行信息科技风险管理指引》第五十四条	1、与相关的管理人员访谈，并查看相关制度，确认是否建立了业务连续计划定期测试的流程，了解对灾备测试的实施情况； 2、查看灾备测试记录，确定灾备测试涵盖了系统层面、应用层面和业务层面的业务连续性运营需求，确定测试流程满足 IT 连续性计划要求。
7.8 外包服务管理	7.8.1	外包组织架构管理	建立外包管理组织架构。	a)未针对外包建立管理组织架构。	a)商业银行的董事会及高级管理层应当严格落实信息科技外包风险管理的相关职责，制定并审批信息科技外包战略，审议信息科技外包管理流程及制定，督促并监控信息科技外包风险管理效果。	《银行业金融机构信息科技外包风险管理指引》第十三条、第十五条	访谈高级管理层了解是否针对外包建立管理组织架构；确认是否在部门内建立信息科技外包管理执行团队，并配备足够人员履行以下职责：实施信息科技外包战略；制定并执行信息科技外包管理制度与流程；执行供应商准入、评价、退出管理，建立并维护供应商关系管理；制定外包服务连续性应急管理方案，并组织实施定期演练；对外包过程的各项管理活动进行监控分析，定期向信息科技及外包风险管理的主管部门报告外包活动情况。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
			严格落实信息科技外包管理职责。	b)没有严格落实信息科技外包管理职责。	b)商业银行的董事会及高级管理层应明确信息科技外包管理的主管部门。商业银行的信息科技管理部门或信息科技外包活动执行部门应建立信息科技外包管理执行团队，并配备足够人员。	《银行业金融机构信息科技外包风险管理指引》第十四条	访谈高级管理层和信息科技外包管理的主管部门，确认是否包含以下职责：对外包风险进行识别、评估与风险提示；监督、评价外包管理工作，并督促外包风险管理的持续改善；向高级管理层定期汇报信息科技外包活动开展情况；董事会或高级管理层确定的其他信息科技外包风险管理职责。
	7.8.2	外包战略风险管理	制定详细的科技外包战略。	a)未制定信息科技外包战略。	a)商业银行应基于信息科技战略、外包市场环境、自身风险控制能力和风险偏好制定其信息科技外包战略，包括不能外包的职能、资源能力建设方案、供应商关系管理策略和外包分级管理策略。	《银行业金融机构信息科技外包风险管理指引》第十六条、第十七条、第十八条	1、访谈高级管理层了解是否制定信息科技外包战略； 2、访谈信息科技外包执行部门是否了解战略并予以执行。
			在信息科技战略中明确不允许外包的领域。	b)未在信息科技战略中明确不能外包的领域。	b)商业银行实施重要外包（如数据中心和信息科技基础设施等)应格外谨慎，在准备实施重要外包时应以书面材料正式报告银监会或其派出机构，商业银行不得将信息科技管理责任外包。	《商业银行信息科技风险管理指引》第五十五条、第五十六条	1、调阅所有外包服务合同，包括业务外包服务合同和科技外包服务合同； 2、访谈相关管理部门，了解哪些领域已外包和外包的原因； 2、关注外包是否牵涉到本行核心业务和敏感信息安全领域，是否违背监管要求。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
			对外包服务范围进行全面的风险评估。	c)对外包服务范围缺乏全面的风险评估。	c)商业银行应至少每年开展一次全面的外包风险管理评估，三年内覆盖所有重要的服务提供商。评估内容包括信息科技外包战略执行情况、外包信息安全、机构集中度、服务连续性、服务质量、政策及市场变化对外包服务的影响分析等，并将评估报告提交管理层审批。内部审计部门应每三年对重要外包服务提供商进行一次全面审计。	《银行业金融机构信息科技外包风险管理指引》第二十二条、第二十三条、第二十四条、第二十五条	1、访谈信息科技外包执行部门，了解是否对外包服务范围进行全面的风险评估； 2、调阅风险评估报告，查看评估内容是否包含信息科技外包战略执行情况、外包信息安全、机构集中度、服务连续性、服务质量、政策及市场变化对外包服务的影响分析等；风险评估报告是否提交管理层审批。
			对机构集中度和非驻场外包实施风险管理。	d)没有对机构集中度和非驻场外包进行风险管理。	d)商业银行应积极采用分散信息科技外包活动、提高自主研发运行能力，降低机构集中度，减少对外包服务提供商的依赖。商业银行应对不在本机构现场提供的外包服务从信息安全、知识产权保护、质量监控、法律合规等方面进行风险管理，对非驻场外包服务至少一年进行一次现场检查。	《银行业金融机构信息科技外包风险管理指引》第五十二条、第六十条	1、访谈信息科技外包执行部门，了解外包服务内容和服务提供商的具体承接情况，确认外包服务的必要性； 2、调阅风险评估报告和服务评价表，确认执行部门从务从信息安全、知识产权保护、质量监控、法律合规对外包服务商开展了定期检查。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
	7.8.3	外包服务实施管理	对外包服务商进行风险评估，确认其提供的业务连续性保障水平。	a) 未对外包服务商资质进行有效审核。	a)商业银行应充分审查外包服务商的财务稳定性和专业经验，对外包服务商进行风险评估，考查其设施和能力是否足以承担相应的责任，对外包服务商的引入和过程管理按照相关采购文件进行规范操作。关注可能存在的集中度风险，如多家商业银行共用同一外包服务商带来的潜在业务连续性风险。评估外包服务商提供的业务连续性保障水平，以及提供相关专属资源的承诺，如出现问题时，保证软、硬件持续可用的相关措施。考虑与外包服务商意外终止合同的情况，商业银行应建立恰当的应急措施，应对外包服务商在服务中可能出现的重大缺失，尤其需要考虑外包服务商的重大资源损失、重大财务损失和重要人员的变动。	《商业银行信息科技风险管理指引》第五十七条、第五十八条	1、访谈相关部门负责人，并查看相关文件制度，了解科技外包引入管理和科技外包过程管理的相关程序； 2、抽查科技外包商选择文档，检查其是否与相关管理制度相符； 3、查看外包服务商联系方式的记录，并与相关部门管理人员访谈，了解在紧急情况下是否能及时联络上外包服务商，并得到及时有效的服务。
			对外包服务合同进行严格审查。	b)外包服务合同没有进行严格审查。	b)商业银行所有信息科技外包服务合同应由信息科技风险管理部门、法律部门和信息科技管理委员会审核通过，合同应该包括以下内容：服务水平、售后维护、保密条款、双方权利责任、违约处理等，对合同进行定期审阅更新，并使用统一的合同文本。	《商业银行信息科技风险管理指引》第六十二条	1、抽查科技外包服务合同，检查：合同是否在有效期内，是否定期（如：每年）、及时地续签； 2、合同是否包括服务水平、售后维护、保密条款、双方权利责任、违约处理等内容。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
			针对外包服务商的服务质量制定服务评价指标。	c)没有对外包服务的执行进行监督和评价，未对违规情况进行处理。	c)商业银行应对外包服务商提出定性和定量的服务评价指标，审阅和修订服务水平协议，定期评估外包服务商为商业银行提供服务的充分性。通过服务水平报告、定期自我评估、内部或外部独立审计对外包服务商进行考核。对监督、评估过程中发现的各项问题进行反映和解决，针对考核不达标的情况采取整改措施，调整选择外包服务商流程，评估结果作为下一次选择外包服务商的重要依据。	《商业银行信息科技风险管理指引》第五十九条	1、访谈相关部门负责人，了解制定了哪些衡量科技外包服务的指标，以及如何对这些指标进行更新； 2、检查这些指标是否包含了确保外包服务商能满足当前业务的需求、持续性遵守合同和服务水平约定； 3、抽查相关的评价、监督文档，确认对科技外包商所提供的产品和服务定期进行评估，且通过访谈和查看其他相关资料，确认在评估、监督过程中发现的各项问题都已得到反映和解决； 4、了解评价、监督结果是否作为下一次选择外包商的重要依据。

领域/线条	序号	环节	控制目标	主要风险点	控制要求	控制依据	测试步骤及测试方法
			在信息安全领域对外包服务商采取严格的控制措施。	d)在信息安全领域未对外包服务商提出明确要求。	d)商业银行应与外包服务提供商界定信息所有权、签署保密协议和采取技术防护等措施保护客户信息和其他信息，对本银行客户资料与外包服务提供商其他客户资料做必要权限管理。按照“必需知道”和“最小授权”原则对外包服务提供商相关人员授权，同时合同中要求外包服务提供商保证其相关人员遵守保密规定。商业银行应将涉及本银行客户资料的外包作为重要外包告知相关客户，同时严格控制外包服务提供商再次对外转包，在中止外包协议时收回或销毁外包服务提供商保存的所有客户资料，采取足够措施确保商业银行相关信息的安全。	《商业银行信息科技风险管理指引》第五十七条、第五十八条、第六十条	1、访谈相关部门负责人，了解有关外包服务协议中是否包含信息安全领域的相关内容； 2、查看有关外包服务协议，确认包括了保密性、可用性、可靠性、安全性等因素； 3、查看科技和业务外包领域，应用设备的系统和数据库用户名是否由本行人员掌握。
			针对重要生产设备及时与外包服务商签署维护服务协议。	e)没有与外包服务商及时签署维护服务协议。	e)商业银行针对关键生产设备、技术复杂度高或技术相对封闭的专用计算机系统设备，应与外包服务商签署维护协议，购买软、硬件维护服务，使应用系统和设备可以得到及时维护，提供持续供应能力的承诺。	《商业银行信息科技风险管理指引》第六十二条	1、抽样检查设备管理部门是否与第三方硬件供应商签订了服务协议，对服务期限及服务内容、权利和义务、违约责任作出规定。 2、抽样检查设备管理部门是否定期都会对系统设备进行检测，填写日常硬件预防性维护报告。

参 考 文 献

[1] 财政部，证监会，审计署，银监会，保监会.企业内部控制基本规范.[S]. 上海：立信会计出版社，2010.

[2] 财政部会计司.企业内部控制规范讲解 2010. [M]. 北京：经济科学出版社，2010.

[3] 上海证券交易所.上海证券交易所上市公司内部控制指引. [S].上海：上海证券交易所，2006.

[4] 深圳证券交易所. 深圳证券交易所上市公司内部控制指引. [S].深圳：深圳证券交易所，2007.

[5] 中译本，方红星.内部控制——整合框架. [M]. 辽宁：东北财经大学出版社，2008.

[6] 张翌轩，陈汉文.内部控制体系监督指南.[M].辽宁：东北财经大学出版社，2010.

[7] 王希全.商业银行内部审计实务.[M].北京：中国金融出版社，2009.