

平安银行股份有限公司
2016年度内部控制自我评价报告

二〇一六年度

目 录

前 言	2
一、董事会声明.....	2
二、内部控制有效性的结论.....	3
三、内部控制自我评价工作的总体情况.....	4
四、内部控制自我评价的依据和目标.....	5
五、内部控制基本框架和自我评价范围.....	6
（一）内部控制的基本框架.....	6
1、内部环境	6
2、风险评估	8
3、控制活动	12
4、信息与沟通	13
5、内部监督	14
（二）内部控制自我评价范围.....	15
六、内部控制自我评价的程序和方法.....	16
七、内部控制缺陷认定标准.....	17
（一）财务报告内部控制缺陷认定标准.....	18
（二）非财务报告内部控制缺陷认定标准.....	18
八、内部控制缺陷认定及整改情况.....	19
（一）内部控制缺陷的认定情况.....	19
1、财务报告内部控制缺陷认定及整改情况	19
2、非财务报告内部控制缺陷认定及整改情况	19
3、内部控制存在的缺陷、面临的主要风险及其影响	19
（二）对内控缺陷拟采取的整改措施及风险应对方案.....	20

前言

根据《企业内部控制基本规范》及其配套指引、《商业银行内部控制指引》的规定和其他内部控制监管要求（以下简称“企业内部控制规范体系”），结合平安银行股份有限公司（以下简称“本行”）内部控制制度和评价办法，在内部控制日常监督和专项监督的基础上，我们对本行2016年度内部控制有效性进行了自我评价。

一、董事会声明

按照企业内部控制规范体系，建立健全和有效实施内部控制，评价内部控制有效性，并如实披露内部控制评价报告是本行董事会的责任。监事会对董事会和高级管理层建立和实施内部控制进行监督。高级管理层负责执行董事会决策，组织领导本行内部控制的日常运行。

本行董事会、监事会及董事、监事、高级管理人员保证本报告内容不存在任何虚假记载、误导性陈述或重大遗漏，并对报告内容的真实性、准确性和完整性承担个别及连带法律责任。

本行内部控制的目标是促进银行各项经营管理活动合法合规，合理保证发展战略和经营目标实现，持续改进和完善内部控制管理体系和运行机制，建立“以防范风险和控制舞弊为中心、以控制标准和评价标准为主体”的风险管理和内部控制规范体系，提高风险管理水平，促进业务、财务、会计及其他管理信息的真实、准确、完整和及时。

由于内部控制存在的固有局限性，故仅能为实现上述目标提供合理保证。此外，由于情况的变化可能导致内部控制变得不恰当，或对控制政策和程序遵循的程度降低，根据内部控制评价结果推测未来内部控制的有效性具有一定的风险。

二、内部控制有效性的结论

根据企业内部控制规范体系，结合本行内部控制制度和评价办法，在内部控制日常监督和专项监督的基础上，通过对本行截至2016年12月31日的内部控制设计与运行有效性的评价，我们认为，报告期内本行纳入评价范围的业务与事项均已建立了内部控制，达到了本行内部控制的目标。

根据本行财务报告内部控制重大缺陷的认定情况，于内部控制评价报告基准日，本行不存在财务报告内部控制重大缺陷，董事会认为，本行已按照企业内部控制规范体系和相关规定的要求在所有重大方面保持了有效的财务报告内部控制。

根据本行非财务报告内部控制重大缺陷的认定情况，于内部控制评价报告基准日，本行未发现非财务报告内部控制重大缺陷。

自内部控制评价报告基准日至内部控制评价报告发出日之间未发生影响内部控制有效性评价结论的因素。

我们注意到，内部控制应当与本行经营规模、业务范围、竞争状况和风险水平等相适应，并随着情况的变化及时加以调整。未来期间，本行将匹配发展战略、结合业务流程的变化，继续完善内部控制制度体系，规范内部控制制度执行，不断优化内部控制评价方法，加强内部控制监督检查，促进本行有效益、可持续地健康发展。

本报告已于2017年3月16日经第十届董事会第五次会议审议通过。

三、内部控制自我评价工作的总体情况

本行按照法律法规、监管规定和内部制度的要求，建立了组织架构完整、制度健全、分工明确、人员具备专业素质的内部控制体系。内控管理委员会作为本行内部控制管理工作的议事与监督管理机构，负责监督、决策及协调涉及全行内部控制方面的重要事务。

总、分行法律合规部、风险管理部为内部控制管理的职能部门，负责牵头全行内部控制的统筹规划，与监管部门衔接内部控制的监管和评价要求，定期检视内部控制管理的执行情况。通过实施内控绩效考评改进内部控制管理，跟踪报告全行内部控制及管理情况。

稽核监察部为内部审计部门，履行内部控制监督职能，负责对内部控制的充分性和有效性进行审计，及时报告并监督整改审计发现问题。

总、分行各业务/职能部门/事业部对本机构的内部控制负首要责任，负责贯彻执行内控制度并推动落实本部门各项内控措施和内控保障；制定并落实与自身职责相关的业务制度和操作流程；梳理流程，识别、评估风险点及影响，定期组织开展监督检查，并建立有效的信息沟通机制；负责组织开展内控监督和检查，强化内控文化建设，提高员工内控意识。

本行持续推进内部控制管理建设工作，并根据银监会发布的《商业银行内部控制指引》、《商业银行内部控制评价试行办法》，以及财政部、银监会等五部委发布的《企业内部控制规范》及其配套应用指引及人民银行印发的《商业银行内部控制评级指南》等政策制度相关要求，结合银行自身管理需要，持续整合工具、优化流程，提升内控管理。2016年，本行操作风险与内部控制自我评估（以下简称“RCSA-CSOX”）进一步围绕“加强日常监测、关注重点流程、提升内控自我完善能力”的工作思路，采用“日常监测、重点领域专项分析及年度评估”模式开展自评，强化重点领域监测建立预警及提示机制，提升自评工作的质量和效果。

稽核监察部继续围绕全面风险管理发展战略和目标，充分运用审计资源，整合审计项目与内部控制稽核独立评价工作，将内部控制与风险管理、专项检视与常规测试有机结合，不断追求审计效能的最大化，持续推动提升各层级机构内控管理水平，助力经营效率和效果的提高。2016年，稽核监察部将内控评价工作嵌入审计规划项目中，通过“常规/专项+内控评价”模式开展审计项目，完成内部控制稽核独立评价测试，并在整合审计项目审计发现，对照人民银行《商业银行内部控制评价指南》内部控制缺陷认定标准，认定业务管理和流程操作中存在的内控缺陷的基础上，通过扩大测评范围，补充测试对象，推动重大、重要缺陷及时、有效整改，达成对截至2016年12月31日本行内部控制设计与运行的充分性和有效性的评价。

四、内部控制自我评价的依据和目标

根据《中华人民共和国商业银行法》、《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》、《商业银行内部控制指引》及《深圳证券交易所主板上市公司规范运作指引》、《公开发行证券的公司信息披露编报规则第21号——年度内部控制评价报告的一般规定》等相关要求，本行应当对内部控制的有效性进行自我评价，并编制内部控制自我评价报告，同时应当聘请会计师事务所对财务报告内部控制的有效性进行审计并出具审计报告。

本行根据上述规范要求及中国银行业监督管理委员会《商业银行资本管理办法（试行）》、《商业银行操作风险管理指引》、《商业银行内部控制评价试行办法》，中国人民银行《商业银行内部控制评价指南》以及新资本协议操作风险标准法监管达标各项要求，制定了《平安银行操作风险与内部控制自我评估管理办法》等制度，同时结合本行实际情况，建立完善了本行RCSA-CSOX体系，在内部控制日常监督和专项监督的基础上，对本行截至2016年12月31日内部控制设计与运行的有效性进行自我评价。

本行内部控制自我评价的目标是促进本行依法合规经营，建立“以防范风险和控制舞弊为中心、以控制标准和评价标准为主体”的风险管理及内部控制规范体

系，为银行案件防控提供工具方法和技术支持，持续优化和完善管理体系及业务流程，建立良好的内控文化，保障内控有效运行。

五、内部控制基本框架和自我评价范围

（一）内部控制的基本框架

1、内部环境

（1）公司治理

根据《民法通则》、《中华人民共和国公司法》、《中华人民共和国证券法》、《中华人民共和国商业银行法》等有关法律、法规和规范性文件，本行致力于不断健全公司治理机制，完善公司治理结构。

本行建立了《平安银行股份有限公司章程》、《平安银行股份有限公司股东大会议事规则》、《平安银行股份有限公司董事会议事规则》，并针对董事会下属的战略发展委员会、审计委员会、风险管理委员会、关联交易控制委员会、提名委员会、薪酬与考核委员会制定了相关的议事规则，以及信息披露事务管理制度、投资者关系工作制度、董事监事和高级管理人员所持本行股份及其变动管理办法、内幕信息及知情人管理制度、年报信息披露重大差错责任追究制度、防范大股东及其关联方资金占用制度、董监事履职评价办法等多项公司治理制度。《平安银行股份有限公司董事会审计委员工作细则》对审计委员会在内部控制方面的职责做了明确说明。

监事会根据《平安银行股份有限公司监事会议事规则》召开监事会会议，通过列席董事会及其专门委员会会议对董事会进行监督。

截至2016年12月31日，本行董事会由14名董事组成，其中独立董事5名；监事会由7名监事组成，其中职工代表监事3名，外部监事3名，股东监事1名。

（2）组织架构

本行管理决策部门主要包括股东大会、董事会、监事会、高级管理层。股东大会、董事会、监事会分别按照职责行使表决权、决策权和监督权。

董事会负责保证建立并实施充分有效的内部控制体系，明确设定可接受的风险水平，监督高级管理层采取必要的风险控制措施；董事会下设的审计委员会具体负责确定本行的内控管理方向，制定内控政策，审查、监督内部控制的有效实施。监事会负责监督董事会、高级管理层完善内部控制体系，履行内部控制职责。高级管理层负责建立系统化的制度体系，完善内部管理组织架构，组织、协调、监督内部控制管理工作有效运行。

2016年12月本行根据深化转型、提质增效、调整业务机构、优化经营模式的要求，对总行组织架构进行了优化调整。截至2016年12月31日，全行按照大公司、大零售、大内控及大行政四大组织板块共设置41个总行业务/职能部门（含8大行业事业部），60家分行、650家传统支行（其中小微支行23家）、357家社区支行、4家专营机构。

（3）发展战略

本行董事会下设战略发展委员会，负责对本行中长期发展进行战略规划。《平安银行五年发展战略规划（2013-2017年）》明确了各阶段、各业务发展的目标、指标和行动举措，并将其细化为各条线、事业部、部门和分行的战略规划图和平衡计分卡，构建了上下承接、横向协同的战略执行管理体系。同时，通过制订《平安银行战略管理办法》，建立健全了战略执行过程的持续监督纠偏机制，进一步完善了战略规划体系。

2016年本行结合战略规划检视和发展环境变化，编制了《平安银行三年战略规划（2016-2018年）》，以合理保证战略规划得到有效实施。

（4）人力资源

本行继续落实可持续发展的人力资源政策，持续优化能力评估方法及工具，细化能力评估标准，对每一能力层级及发展趋势进行更为清晰、客观、明确的界定；同时强化对直线主管的宣导和培训，统一评估人对能力评估标准的理解；设置多位评估人，为决策人提供多维度的评价参考，避免个人评估误差。

本行致力于建立科学、系统的绩效考核体系，不断提升绩效管理工作的科学性和规范性，客观、公平、准确考核评价工作成效。根据董事会制定的战略规划和业务指标，结合各业务条线特点制定相应的绩效计划和考核指标体系，包括业务指标、资产质量指标、合规内控指标、管理效益指标等。经营机构的考核以利润为中心，与“两率”（即利润工资率和利润变动率）挂钩，并利用平衡计分卡进行调整。全员制定个人绩效目标，由被考核人上级定期对员工绩效目标完成情况进行考核，考核结果与员工的奖金、薪资调整、晋升等挂钩。

2016年12月，为配合总行组织架构调整，对新架构下总行各部门、各事业部的高、中级管理人员进行了重新选拔任命，确保了新架构下全行经营管理工作的正常开展。

（5）社会责任

本行根据中国银监会《中国银行业金融机构企业社会责任指引（2009）》要求，制订了《平安银行履行企业社会责任信息报告制度》，由办公室专门策划并搜集整理社会责任方面的工作内容，包括股东责任、客户责任、员工责任、环境和社会责任以及合作伙伴责任五大部分。

2、风险评估

（1）信用风险

本行建立了集中、垂直、独立的全面风险管理架构，建成“派驻制风险管理、

矩阵式双线汇报”的风险管理模式。总行风险管理委员会统筹全行风险管理，总行各专业风险管理部门负责全行信用风险管理工作，并由总行风险管理委员会向各分行/事业部派驻主管风险副行长/风险总监，负责所在单位的信用风险管理工作。同时，制定了一整套规范的信贷管理流程，完善了内部控制机制，对信贷业务实行全流程管理。

（2）市场风险

本行建立了有效的市场风险治理架构。董事会是市场风险管理的最高决策机构，承担市场风险管理的最终责任；高级管理层及其下设委员会在董事会授权范围内履行市场风险管理职责；总行风险管理部是全行市场风险管理的牵头部门，与前台业务部门保持独立。

本行不断完善市场风险管理制度体系，优化市场风险计量模型和数据质量，加快市场风险管理信息系统建设，搭建涵盖市场风险基本制度、一般管理办法、操作流程的市场风险管理制度体系，覆盖了市场风险识别、计量、监测报告和控制的全流程。

（3）流动性风险

本行不断完善流动性风险管理框架和管理策略，加强流动性风险管理。董事会承担流动性风险管理的最终责任，资产负债管理委员会是最高管理机构，资产负债管理部在资产负债管理委员会指导下负责日常管理，根据本行流动性风险容忍度及经营策略制定基础政策和程序，并对业务或经营单位专项流动性风险管理政策进行审议。

本行建立健全流动性风险管理机制，明确了流动性风险管理的职责分工，以保证有效识别、计量、监测和控制风险；定期开展流动性风险压力测试，审慎评估未来流动性需求；完善和细化流动性风险应急计划，针对特定事件制定具体的解决方案；加强各相关部门之间的沟通和协同，提高流动性风险应对效率。

（4）操作风险

本行遵循操作风险管理监管要求，建立并不断完善与本行业务性质、规模和复杂程度相适应的操作风险管理体系。法律合规部作为操作风险统筹管理部门，负责建立健全全行操作风险管理组织体系，制定本行操作风险管理政策、制度以及操作风险识别、评估、监测、控制及缓释、报告的标准工具，完善操作风险信息系统，组织实施操作风险监控分析及资本计量并开展新产品上市前的操作风险评估等。

本行通过优化升级操作风险管理架构、制度、系统、考评标准，加大操作风险管理整合、推广力度，完善全行操作风险管理体系；通过提升操作风险管理三大工具“操作风险与控制自我评估(RCSA)、关键风险指标(KRI)、损失数据收集(LDC)”的运用深度、覆盖广度及实施效果，提高操作风险识别、评估、监测、预警、整改能力；同时，强化操作风险管理工作监督和评价，持续开展操作风险文化建设。

（5）国别风险

本行按照监管要求制定了《平安银行国别风险管理办法》，明确规定国别风险管理职责、管理手段和工作流程，建立规范的国别风险管理体系。本行动态监测国别风险变化，认真做好国别风险评级、限额管理、监测预警和国别风险准备金计提工作。

（6）银行账户利率风险

本行董事会承担对利率风险管理实施控制的最终责任，资产负债管理委员会在董事会授权下履行利率风险管理职责，总行资产负债管理部经资产负债管理委员会授权，独立于其他管理和经营机构行使利率管理职责并向资产负债管理委员会负责。各业务条线、经营机构是利率风险的责任承担部门，在既定的利率风险管理目标、政策和限额体系内开展各项经营活动。总行风险管理部负责拟定交易账户与银行账户划分的相关政策，并对市场风险所辖部分银行账户利率风险设定限额并进行

监控管理。

本行不断建立和完善利率风险计量、监测和报告体系，基于合理性和审慎性原则，采取多种方法对利率风险进行计量和评估，定期监测人民币生息资产和付息负债在各期限重定价缺口水平，并通过资产负债管理系统对利率风险进行情景分析和压力测试。

（7）声誉风险

本行行长及其他高管层是声誉风险管理的日常管理负责人和执行决策人，在董事会授权范围内制定并落实声誉风险管理的各项政策。总行办公室为全行声誉风险归口管理部门，牵头组织制定声誉风险管理办法体系，建立声誉风险的识别、评估、控制、监测和报告机制。本行对声誉风险实行分类分级管理并明确了管理权限、职责和报告路径。

本行持续完善声誉风险管理制度，加大声誉风险考核力度；开展声誉风险事前排查，加强声誉风险前置管理；持续优化舆情监测机制，强化危机应对系统，提升声誉风险管理的主动性；提升全行声誉风险意识，构建自媒体关系网络，不断夯实声誉风险管理基础。

（8）其他风险

本行面临的其他风险还包括法律风险、合规风险等。

本行法律风险管理工作重点围绕事前风险防范，事中风险控制，事后风险化解三个层次展开，并在主要领域建立制度化、规范化、系统化的管理机制，持续提升本行业务的法律风险管理成效。

本行强化与创新相适应的合规评审管理，加大对重点业务监管文件的解读、分析与传导，及时识别合规风险，提升合规风险防御能力。同时，积极开展合规文化建设，强化全行员工合规意识，营造良好的合规文化氛围。

3、控制活动

本行建立健全内部控制制度体系，围绕制度管理、风险监控、系统控制、职责权限和人员管理以及各专业领域控制活动，落实内外部管理要求，检视内部控制措施的合理性和充分性，完善和强化内部控制保障体系，为业务持续、健康发展奠定基础。

(1) 制度管理。本行内部控制管理制度分为基本制度、一般制度、操作规范三个层次。通过完善制度体系，规范了内部控制管理工具、管理要求，明确了内部控制管理具体标准、方法论和操作指引。同时，本行还建立了内控制度定期检视机制，确保内部控制制度的适用性与有效性。

(2) 风险监控。本行运用操作风险与内部控制先进技术和三大工具（RCSA-CSOX、LDC、KRI），不断提升识别、评估业务和管理活动中风险的能力，并通过持续更新、日常监测、重点领域专项分析、评估，达成对主要风险及控制活动的持续监控。

(3) 系统控制。2016年，本行完成了新核心系统建设，为业务发展和管理提升奠定了基础，以适应互联网发展和本行战略转型的需求，新型应用架构体系建设正在按计划推进。同时，本行持续完善IT运维管理体系和灾备体系，不断提升IT服务能力和质量。

(4) 职责权限和人员管理。通过明确职责和权限，形成规范的部门、岗位职责说明及报告路线，并建立动态更新和调整的授权体系；界定关键岗位和轮岗规则，确保不相容岗位分离与制衡，并实行重要岗位轮岗和强制休假制度；对员工行为进行全面规范，将诚实守信的经营理念融入日常生产经营过程，从工作表现、经济往来、社会交往、家庭状况等方面协助员工识别禁止的行为，加强对员工异常行为的排查。

(5) 专业领域控制活动。制定《平安银行基本会计制度》及财务管理、费用管

理、业务会计核算等制度和操作流程，规范会计确认、计量和报告行为，定期对财务政策执行情况进行检查，确保财务会计信息真实、可靠、完整；建立账务核对、监控制度，定期对各种账证、报表进行核对，对现金、有价证券等有形资产和重要凭据进行盘点；明确新机构建设流程和要求、新产品评审职责权限和程序规则等，规范全行产品风险管理，落实风险管理前移的要求，有效支持产品创新；完善客户投诉管理办法和渠道，明确投诉处理的职责和流程，并定期汇总分析投诉反映事项，改进客户服务和管理；修订了《平安银行外包风险管理办法》，重点梳理了外包风险管理职责分工，明确了高级管理层、总行各条线、各职能部门的职责，规定了外包风险管理组织架构、职责分工、管理规则和要求等内容；建立了业务连续性管理制度体系，各部门按职责分工完善了业务连续性及应急恢复预案；建立由安全策略、方针、标准、基线和流程等构成的信息安全制度体系，对各类信息实施分等级安全管理，对信息系统访问实施权限管理，覆盖了物理、网络、应用、数据、终端、访问控制、电子银行安全等各方面的安全控制需求。

4、信息与沟通

本行董事长、行长是公司信息披露的责任人，董事会秘书负责具体协调和组织信息披露事务。本行通过制定信息披露事务管理制度，明确信息披露职责、程序及管理措施，完善信息披露的风险控制机制，为合法合规地开展信息披露工作提供了制度保障，确保披露的信息真实、准确、完整、及时、公平。本行建立了重大事项及突发事件报告制度，规范了案件（风险）信息的报告报送。

为及时掌握监管信息动态、加强管理，修订发布《平安银行监管信息管理办法（4.0版，2016年）》，重新梳理报送流程，对监管信息事项进行风险分类，分类别明确报送范围，促进监管信息传达的准确性和传送效率。稽核监察部检视规范各分行监管信息录入呈报情况，对迟漏报重大监管信息的典型案例通报全行、进行问责；开展培训，帮助提高机构重视度和报送质量。同时，加强与监管机构的信息传递，确保按照监管要求如实报告相关信息。

本行建立了内部信息沟通机制，明确了信息报送职责，规范了信息传递要求，制定了公文流转程序，会议制度和内部信息报送制度，并采取多种信息沟通渠道确保重要的信息得到及时沟通和汇报。本行通过公文流转、会议、办公自动化系统、行刊等多种渠道收集信息并在银行内部各管理级次、责任单位、业务环节之间进行沟通和反馈。组织利于内部沟通的活动如行业动态分析、员工动态等。办公室在总行各部室、各管理部门和各事业部设立了公务邮箱，要求指派专员管理邮箱，及时收发本部门公务邮件，确保办公信息高效流转。本行还建立了个人工作台（PWS系统），将内部报告信息集成和共享，对公司内外部重要的新闻进行报导。

5、内部监督

本行建立了独立、垂直的内审架构和管理体系，能够保证在首席审计官的直接领导下，独立、客观地履行内部监督职责。本年度内审部门坚持求变、求新、求实，调整稽核架构适配银行转型，形成首席审计官直接领导下的稽核监察条线新架构。深化审计思维和方法转型，强化授信业务尽职尽责、未尽职问责的责任追究机制，严格处罚和整改监督；深化审计技术/手段转型，增强预警监控能力，完善审计系统平台，提升审计工作效能。担负总行处罚委秘书处、党风廉政组织教育专项活动办公室和履职排查等新职责，以守护公司资产质量/安全为主线，以反舞弊反欺诈和防控案件为重点，为内控和全面风险管理保驾护航。

本行监事会根据内控职责履行监督职能，负责监督董事会、高级管理层完善内部控制体系，履行内部控制职责。内控管理委员会作为本行内部控制管理工作的议事与监督管理机构，负责监督、决策及协调涉及全行内部控制方面的重要事务。

本行建立健全了内部控制检查监督、报告和信息反馈以及问题整改机制，稽核监察部、法律合规部及各业务部门根据分工协调配合，建立并组织开展覆盖各级机构、各个产品、各个业务流程的内部控制监督检查。法律合规部围绕“加强日常监测、关注重点流程、提升内控自我完善能力”的工作思路，组织各业务部门采用“日常监测、重点领域专项分析及年度评估”模式开展自评，强化重点领域监测，

建立预警及提示机制。稽核监察部将内控评价嵌入审计规划项目中，并整合审计项目审计发现，认定业务管理和流程操作中存在的稽核问题/内控缺陷，推动重大、重要缺陷及时、有效整改；同时，强化整改监督，落实问责，从加强内控角度制定更为合理的整改验证标准，促进提高问题整改的真实性、有效性。

（二）内部控制自我评价范围

2016年本行RCSA-CSOX范围涵盖银监会要求的八大业务条线、覆盖本行所有业务/管理流程，包括25个一级流程、177个二级流程。经梳理，确定主要风险点958个，关键控制活动1261个，涵盖公司层面、流程层面和信息技术层面内容。总行39个部门/事业部及34家分行参加了对控制活动执行情况的抽样评估，自评范围涉及25个一级流程、1261个关键控制活动。内控稽核独立评价共完成对256个风险点、344个关键控制活动的测试，覆盖23个一级流程、78个二级流程，涉及总行部门/事业部及深圳、北京、广州、成都、佛山、杭州、天津、宁波、沈阳、珠海、武汉、大连、东莞、太原、昆明、石家庄、重庆、青岛、中山、济南、西安、郑州、长沙、海口24家分行。纳入独立评价范围单位资产总和占本行合并财务报表资产总额的56%，营业收入合计占本行财务报表营业收入的48%¹。具体评价范围如表1所示。

表 1 2016 年度内部控制评价范围

流程	RCSA-CSOX自评		稽核独立评价	
	风险点	控制活动	风险点	控制活动
财务报告	20	39	3	6
电子银行	26	31	12	15
对公贷款	67	79	41	48
费用管理	10	13	4	5
个人存款	21	30	8	10
公司层面	44	64	12	21
公司存款	27	52	18	28
固定资产、无形资产管理	17	19	6	6
离岸业务	25	37	8	11
理财产品	31	40	10	15

¹ 根据 2015 年公司年报数据统计计算

零售贷款	61	108	25	36
贸易结算	43	60	4	8
贸易融资	32	57	1	1
票据业务	59	69	13	16
汽车金融	72	92	22	30
人力资源	23	24	1	1
税务管理	16	19	0	0
投融资管理	27	27	4	4
投资银行	47	50	10	10
小微企业业务	37	45	8	13
信息科技管理	55	74	20	28
信用卡	46	60	0	0
运营管理	46	56	17	23
资产托管	34	37	6	6
资金和同业业务	72	79	3	3
合计	958	1261	256	344

上述纳入评价范围的单位、业务和事项以及高风险领域涵盖了本行经营管理的主要方面，不存在重大遗漏。

六、内部控制自我评价的程序和方法

2016 年度本行遵循全面性、重要性、客观性和成本效益原则开展内部控制评价工作。根据内部控制整体目标和职能分工，由法律合规部组织实施全行 RCSA-CSOX，由稽核监察部组织实施内部控制稽核独立评价，相关责任部门根据内控缺陷整改建议制定并执行整改计划。

法律合规部作为内控管理职能部门，负责牵头组织全行开展 RCSA-CSOX 工作，自评流程包括确定自评范围、固有风险识别评估、风险控制矩阵（RCD）更新、内控测试与校验、缺陷整改等六个工作环节。本年度本行 RCSA-CSOX 在创新整合的基础上，围绕“关注重点流程、加强日常监测，提升内控自我完善能力”工作思路，建立“动态更新与日常监测相结合”的模式，多场景动态触发流程梳理及矩阵更新机制，采用“常规+重点流程+重点机构”模式开展多角度内控自评及监测，强化重点领域监测预警及提示机制，具体体现为：各业务部门按照不同的测试

频率定期对控制活动执行情况进行抽样评估，实现以风险为导向的差异化管理，并对高风险领域及关键控制活动实施日常化监测，形成动态量化的风险评估监测体系；法律合规部结合日常监测及内外部典型案件、事件，开展热点、重点风险领域的风险检视、预警和整改推动，并对全行 RCSA-CSOX 工作进行实时监督，评估自评工作质量。同时，通过组织全行就稽核问题/内控缺陷制定整改计划，汇总自我评估情况及缺陷整改执行情况，最终形成全行性的操作风险与内部控制自我评估工作报告。

稽核监察部组织实施内部控制稽核独立评价，对 RCSA-CSOX 工作成果进行审阅，检视自评风险点及相应控制活动识别的完整性、准确性；通过对 2015 年度内部控制自我评价结果的分析，结合监管规定和同业实践以及 2016 年本行经营发展目标，分析判断各业务条线系统性风险隐患和制度缺失，制订年度内部控制测试计划；通过“常规/专项+内控评价”项目执行内控测试计划，同时整合项目审计发现中影响内部控制的事项，认定内控缺陷并跟进整改。按照计划准备、嵌入项目测试、整合审计发现及落实整改、补充测试及报告五个阶段开展内部控制稽核独立评价。突出了以风险为导向，强化对重点业务、重点风险领域的关注，加大了对关键风险控制环节测试的覆盖面，提高了内部控制稽核独立评价的全面性和准确性。

本行持续完善 RCSA-CSOX 和内控稽核独立评价流程，不断加强内控评价工作过程管理、质量复核，优化内控评价方法，规范评价工作的开展，实现对工作任务、测试进度、测试复核、底稿审批、整改追踪、汇总分析全过程管理。

七、内部控制缺陷认定标准

本行根据企业内部控制规范体系对内部控制缺陷的认定要求，采用人民银行《商业银行内部控制评价指南》内部控制缺陷认定标准，从定性和定量两个维度，结合内部控制缺陷对整体控制目标实现影响的严重程度，将内部控制缺陷分为一般缺陷、重要缺陷和重大缺陷。重大缺陷是指一个或多个控制缺陷的组合，可能导致本行严重偏离控制目标；重要缺陷是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，但仍有可能导致本行偏离控制目标；除重大缺陷、重要缺陷之外的其他控制缺陷为一般缺陷。

（一）财务报告内部控制缺陷认定标准

1、财务报告内部控制缺陷评价的定量标准

表 2 财务报告内部控制缺陷评价定量标准

重大缺陷	重要缺陷	一般缺陷
1.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 $\geq 0.25\%$ ； 2.财务错报金额占当年度利润总额的比例 $\geq 5\%$ 。	1.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 $[0.0125\%, 0.25\%)$ ； 2.财务错报金额占当年度利润总额的比例区间为 $[0.25\%, 5\%)$ 。	1.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 $< 0.0125\%$ ； 2.财务错报金额占当年度利润总额的比例 $< 0.25\%$ 。

2、财务报告内部控制缺陷评价的定性标准

重大缺陷是指可能产生或者已经造成重大金额财务报告的错报；重要缺陷是指可能产生或者已经造成较大金额财务报告的错报；一般缺陷为可能产生或者已经造成较小金额财务报告的错报。

（二）非财务报告内部控制缺陷认定标准

非财务报告内部控制是指针对除财务报告目标之外的其他目标的内部控制。

1、非财务报告内部控制缺陷评价的定量标准

表 3 非财务报告内部控制缺陷评价定量标准

重大缺陷	重要缺陷	一般缺陷
财务损失按照损失金额占当年度集团营业收入的比例 $\geq 1\%$ 。	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 $[0.05\%-1\%)$ 。	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、非财务报告内部控制缺陷评价的定性标准

表 4 非财务报告内部控制缺陷评价定性标准

重大缺陷	重要缺陷	一般缺陷
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； 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。	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； 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。	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； 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。

八、内部控制缺陷认定及整改情况

（一）内部控制缺陷的认定情况

1、财务报告内部控制缺陷认定及整改情况

按照财务报告内部控制缺陷认定标准，报告期内本行不存在财务报告内部控制重大缺陷、重要缺陷。内控评价中发现的2个一般缺陷，截至2016年12月31日已完成整改。

2、非财务报告内部控制缺陷认定及整改情况

按照非财务报告内部控制缺陷的认定标准，报告期内本行不存在非财务报告内部控制重大缺陷、重要缺陷。内控评价中发现的95个一般缺陷，截至2016年12月31日均已完成整改。

3、内部控制存在的缺陷、面临的主要风险及其影响

在本年度内控评价过程中，RCSA-CSOX 认定缺陷 67 个，内控稽核独立评价认定缺陷 30 个，合计共认定缺陷 97 个（如表 5）。其中设计性缺陷 5 个，表现为制度

不完善、流程存在缺陷、系统功能需优化，占内控缺陷的 5.15%；运行性缺陷 92 个，表现为管理制度、控制措施执行不到位、不规范；系统维护及用户管理、外包业务及人员管理、员工行为管理等待加强，占内控缺陷的 94.85%。内控缺陷主要涉及操作层面，包括对公业务、零售业务及小企业业务的贷前调查、审查审批和贷后管理未有效落实相关控制要求；投行业务投前、投后管理制度不健全，操作中存在执行不到位的情况；小企业业务不良资产管理缺失、理财产品宣传销售不规范以及员工行为管理有待进一步加强等。经营管理层对于发现的内部控制缺陷，有重点地制定了整改计划并跟进落实，对设计性缺陷，梳理业务流程，完善管理制度，修正系统缺陷，优化系统功能；对运行性缺陷，对问题事件举一反三，健全管控机制，加强日常检查和监督，加大处罚力度，并通过培训和宣导加深员工对制度的理解，提高合规意识。

通过验证和评价，根据内部控制评价和缺陷认定标准，本行内部控制制度设计合理、运行基本有效，有待改善事项对本行经营管理不构成实质性影响。

表 5 2016 年度内控缺陷情况

一级流程数量	风险点数量	管理层内控自评发现的内控缺陷数	内控稽核独立评价新增发现的缺陷数	截至 20161231 尚未完成整改的内控缺陷数
25	958	67	30	0

（二）对内控缺陷拟采取的整改措施及风险应对方案

2017 年本行将围绕抓经营、抓管理、推转型，实现质量、效益均衡发展。重点工作涵盖精兵简政、零售转型和廉洁教育活动等，为此，本行将以“内控管理前置，提升管理实效”为工作思路，积极应对互联网金融和新型业务的发展，变革现有的内控思维与技术和方法，推动内控管理架构的升级和优化。

1、完善内控管理组织架构，为全行内部控制管理配备适当资源，建立产品部门、市场部门内控管理队伍，专人负责内部控制具体管理工作，推动本部门各项内控措施及内控保障等管理要求的落实，保证内部控制的各项职责得到有效履行。着力内控前置、内控嵌入，在新机构、新业务、新产品、新制度流程上线或有重大变

化时，主动开展内部控制评估工作，对风险点的识别及控制活动的设计进行审查。建立科学的绩效考评体系，合理设定内部控制考评标准，并将考评结果与业务授权等挂钩，根据考评结果改进内部控制管理。同时，将以内部控制系统为依托，根据业务性质及风险级别差异化确定内控测试频率，持续推进内控评价管理工具（CSOX）、操作风险与控制自我评估管理工具（RCSA）及 DCFC 日常检查的有效整合。

2、加大全行业务系统化管理力度，并持续对系统迭代优化，更多采用数据验证和系统控制等技术手段扩大监控的覆盖面，减少人工操作的风险，确保复杂业务和重点业务均纳入系统控制。

3、在持续完善操作风险三大工具运用的同时引入大数据分析技术，内控职能部门将结合数据分析开展流程梳理及矩阵更新，以数据分析的重点流程/风险领域、流程变更、监管政策变动、内部管理需求（如关键流程检视）等多维度动态化触发矩阵更新，持续更新完善风险及控制活动库。

4、内审部门恪守内部控制第三道防线，针对稽核监察项目发现问题，深入分析问题产生的原因，推动相关部门切实提高认识，运用好惩处和纠正机制，并开展“举一反三”的后续整改工作，提高系统性整改效果，杜绝同类问题再次发生，确保整改工作的全面有效落实。稽核监察部还将通过探索和搭建风险监测体系，加强大数据分析运用，从企业和资产、系统权限、员工异常行为、资金交易四个监控维度规划模型，通过模型实现全样本监测，提高审计效率，增强监测预警的精准性和预判力。