审计与内部控制系列

Auditing and Internal Control

商业银行内部控制评价

蒋建华 编著

复旦大学出版社

审计与内部控制系列

商业银行内部控制评价

蒋建华　编著

复旦大学出版社

图书在版编目(CIP)数据

商业银行内部控制评价/蒋建华编著. —上海:复旦大学出版社,2012.5
(审计与内部控制系列)
ISBN 978-7-309-08669-0

Ⅰ. 商… Ⅱ. 蒋… Ⅲ. 商业银行-内部审计-中国 Ⅳ. F239.65

中国版本图书馆 CIP 数据核字(2011)第 273830 号

商业银行内部控制评价
蒋建华 编著
责任编辑/王联合 张咏梅

复旦大学出版社有限公司出版发行
上海市国权路 579 号 邮编:200433
网址:fupnet@fudanpress.com http://www.fudanpress.com
门市零售:86-21-65642857 团体订购:86-21-65118853
外埠邮购:86-21-65109143
上海春秋印刷厂

开本 787×1092 1/16 印张 16.5 字数 391 千
2012 年 5 月第 1 版第 1 次印刷
印数 1—4 100

ISBN 978-7-309-08669-0/F·1792
定价:32.00 元

前言

PREFACE

国际上凭借技术进步，金融创新与资本市场加速发展，使金融业动荡不定，金融事件不断爆发，金融监管已受到各国广泛的重视。1992 年美国 COSO 委员会颁布了内部控制综合框架公告，就是有名的 COSO 报告，并且很快得到了广泛的认可。很多国家及各专业团体仿效 COSO 报告对内部控制的框架内容进行了重新研究，采纳其新的理念，发布了自己的文告，形成了自己的内部控制及其评价标准体系。

1995 年 2 月，具有 230 多年历史的英国巴林银行宣布倒闭，在国际上引起了强烈的震动。1997 年的东南亚金融危机，以及一系列金融事件的爆发，使国际上对商业银行内部控制的重要性更加重视，对商业银行内部控制的内容也有了新的认识。1997 年，巴塞尔委员会发布了《有效银行监管核心原则》，提出了有效监管体系必备的 25 条基本原则，以后随金融环境与业务的变化进行了几次修正。1998 年，又发布了《商业银行内部控制框架》，提出了商业银行内部控制的 13 项监管原则，从而构建了“良好的公司治理结构和内控制度是防范风险的第一道防线，市场约束机制、社会公众和专业机构的监督是防范风险的第二道防线，政府监管则是第三道防线”的国际银行监管理念。

1997 年 5 月，中国人民银行颁布了《加强金融机构内部控制的指导原则》，使我国商业银行的组织结构、业务种类、经营模式等方面发生了很大的变化，商业银行抵御风险的能力也逐渐加强。为了适应国际上内部控制的发展与变化情况，中国人民银行于 2002 年 9 月颁布了《商业银行内部控制指引》，对我国商业银行内部控制提出了指导性意见。

我国加入 WTO 后，中国金融业也将融入国际金融体系中，银行业的经营风险也将增加，商业银行的经营与管理的方式与内容发生了巨大的变化，银行监管也必须遵循国际银行业监管的游戏规则。

2004 年 8 月，中国银行业监督管理委员会通过了《商业银行内部控制评价试行办法》，自 2005 年 2 月 1 日起施行。该《办法》充分体现了对我国商业银行“管法人，管风险，管内控，提高透明度”的监管理念。

本书借鉴国际商业银行内部控制的经验，结合我国商业银行的实际，阐述了商业银行内部控制的基本原理、商业银行所特有的内部控制系统的风险控制点、控制措施，又详细介绍了对其主要业务内部控制进行测试评价的技术与方法、测试程序与具体操作示例。本著作具有下列特点：第一，以全面风险管理为导向，详细介绍了商业银行主要业务环节的内部控制风险点及其评价要点。第二，理论与业务相结合，在对商业银行经营与业务管理的各个环节做一定阐述的基础

前言

PREFACE

上提出内部控制与评价内容、方式与方法。第三，对商业银行的主要业务内部控制及其评价进行了比较详细、具体的阐述，特别是第三篇，是一个完整的内部控制评价案例，具有很强的可操作性。因此，在编写过程中，作者力求做到观点前瞻，内容翔实，通俗易懂，并能用于实战。

本书的完稿主要是下列成果的总结：第一，以作者2002年出版的《商业银行内部控制与稽核》为理论基础。第二，结合作者在有关企业和各金融机构所作内部控制与内部审计几十轮培训班讲座的内容。第三，是作者及其团队应某商业银行之邀，前后花费了三年多的时间，为该行完成了对其及其分支机构进行内部控制评价的体系与指标设计的成果的凝练。第四，是作者参加某银监局对地方性商业银行进行内部控制评价实务操作的实战成果整理。第五，是作者长期蹲点在银监局、中国国家审计署等相关部门学习与研究的成果。第六，作者参考和引用了一些国内外有关文献资料，借鉴了有关银行的经验和做法。

在此，本人对本书的正式出版给予关心、支持与帮助的有关单位和个人深表谢忱。特别是复旦大学出版社经管分社的王联合总编与张咏梅编辑，他们为本书的出版提供了不遗余力的支持，付出了细致艰辛的劳动，在此一并表示感谢。

本书适用于从事商业银行内部控制评价的注册会计师、银行内部审计人员和各级管理人员、商业银行监管官员、高等院校金融和审计专业的师生等读者群。

由于我国商业银行内部控制及其评价的理论和实践尚在成熟过程中，加之作者水平有限，书中难免存有不当和疏漏之处，欢迎读者多提宝贵意见。

蒋建华

2011年8月

目录

CONTENTS

第一篇　商业银行内部控制理论篇

第二篇　商业银行主要业务内部控制与评价

目录

CONTENTS

目录

CONTENTS

第三篇　商业银行内部控制评价实践

第一篇 商业银行内部控制理论篇

第一章 商业银行内部控制概述

第一节 商业银行内部控制的定义

内部控制是商业银行为实现经营目标，通过制定和实施一系列制度、程序和方法，对风险进行事前防范、事中控制、事后监督和纠正的动态过程和机制①。

第二节 商业银行内部控制的目标

巴塞尔银行监管委员会把内控的三大目标分解为操作性目标、信息性目标和合规性目标。操作性目标不只针对经营活动，而且包括其他各种活动。信息性目标包括管理信息，明确要求实现财务和管理信息的可靠性、完整性和及时性。

(1) 操作性目标(O)。各种活动的效果和效率。

(2) 信息性目标(F)。财务和管理信息的可靠性、完整性和及时性。

(3) 遵从性目标(C)。遵从现行法律和规章制度②。

这三大目标满足不同的需要，又相互交叉。首先，内部控制是保证各种活动发展的，而不是妨碍其发展的。其次，银行不能为实现经营性目标而不遵从法规，更不能为实现遵从性目标或操作性目标而违反财务和管理信息的可靠性、完整性和及时性。

我国银监会颁布的《商业银行内部控制指引》认为商业银行内部控制目标为：

(1) 确保国家法律规定和商业银行内部规章制度的贯彻执行。

(2) 确保商业银行发展战略和经营目标的全面实施和充分实现。

---

① 《商业银行内部控制指引》，中国银行业监督管理委员会令(2007 年第 6 号)。

② 三大目标在以后叙述中分别用“O”、“F”、“C”代表。

（3）确保风险管理体系的有效性。

（4）确保业务记录、财务信息和其他管理信息的及时、真实和完整。

第三节　商业银行内部控制的原则

商业银行内部控制应当贯彻全面、审慎、有效、独立的原则，包括以下方面：

（1）内部控制应当渗透商业银行的各项业务过程和各个操作环节，覆盖所有的部门和岗位，并由全体人员参与，任何决策或操作均应当有案可查。

（2）内部控制应当以防范风险、审慎经营为出发点，商业银行的经营管理，尤其是设立新的机构或开办新的业务，均应当体现“内控优先”的要求。

（3）内部控制应当具有高度的权威性，任何人不得拥有不受内部控制约束的权力，内部控制存在的问题应当能够得到及时反馈和纠正。

（4）内部控制的监督、评价部门应当独立于内部控制的建设、执行部门，并有直接向董事会、监事会和高级管理层报告的渠道。

内部控制应当与商业银行的经营规模、业务范围和风险特点相适应，以合理的成本实现内部控制的目标。

第四节　商业银行内部控制的组成要素

COSO 委员会认为，内部控制包括控制环境、风险评估、控制活动、信息与交流和监督评审五大要素。银监会印发的《商业银行内部控制指引》、《商业银行内部控制评价试行办法操作说明》也将内部控制分为这五大组成部分，并根据巴塞尔委员会颁发的适用于银行一切表内外业务的《内部控制系统评估框架》以及中国的国情，具体规定了商业银行内部控制的组成要素。

一、控制环境

控制环境是推动控制工作的发动机，是所有内控组成部分的基础，它奠定组织的风尚和结构，涉及所有活动的核心——人。“以人为本”的管理思想的核心是强调人是发展的动力，是一切事物的基础。控制环境塑造企业文化，影响企业员工的控制意识。商业银行内部审计部门应根据控制环境的每一要素，判定银行是否存在积极的控制环境。内控环境主要包括以下因素：

1. 商业银行公司治理

（1）是否建立以股东大会、董事会、监事会、高级管理层等为主体的公司治理组织架构？

（2）是否设立了提名委员会、风险管理委员会、人事和薪酬委员会、审计委员会、关联交易控制委员会等其他专门委员会？

(3) 是否定期或不定期召开股东大会年会和临时会议，是否向全体股东汇报？股东大会是否实行律师见证制度？是否制定内容完备的股东大会议事规则并由股东大会审议通过，包括通知、文件准备、召开方式、表决形式、会议记录及签署、关联股东的回避制度等？

(4) 董事会是否建立了议事规则和决策程序？议事规则是否完备，包括通知、文件准备、召开方式、表决形式、会议记录及签署、董事会的授权规则等？董事会是否定期(每季一次)或不定期召开例会和临时会议？

(5) 监事会是否建立了议事规则和决策程序？议事规则是否完备，包括通知、文件准备、召开方式、表决形式、会议记录及其签署等？是否定期(每季一次)或不定期召开例会和临时会议？

(6) 是否建立了独立董事和外部监事制度并设立了 2 名(含)以上独立董事和 2 名(含)以上外部监事？

(7) 董事会审计委员会负责人是否由独立董事担任？是否要求银行报送内部审计报告并进行评价？独立董事是否对董事会讨论的有关商业银行内部控制事项发表客观、公正的独立意见？是否对董事会决议中违反法律、法规或商业银行章程的条款提出反对意见？

(8) 审计委员会负责人是否由外部监事担任？外部监事是否根据监事会决议组织开展商业银行内部控制相关审计工作？是否及时向外部监管部门报告监督检查中发现的问题？

(9) 采取何种措施确保商业银行根据内部审计、外部审计和外部监管部门改进内部控制的意见和建议实施有效的整改？

2. 董事会、监事会和高级管理层责任

(1) 董事会是否审批了商业银行整体经营战略和重大政策并定期检查、评价执行情况？

(2) 董事会是否设定了商业银行可接受的风险程度，并审批管理层所制定的风险防范措施及额度设置？是否确保商业银行充分了解资本充足、风险集中度、关联交易、不良资产管控和处置的有关规定，并指导和监督具体政策、程序的产生和实施？

(3) 董事会是否及时审查银行内部审计机构和外部监管部门对银行内部控制的评价报告，并督促管理层落实整改措施？

(4) 监事会是否通过适当的方式对银行内部控制进行监督？

(5) 监事会是否组织对银行内部控制相关检查？是否对董事会及董事、管理层及高级管理人员履行内部控制职责情况进行检查？

(6) 监事会是否在发现董事、董事长及高级管理人员有损害商业银行利益的行为时要求其纠正？

(7) 高级管理人员是否明确其在内控体系方面的职责？在各项业务和管理活动中是否制定了明确的内部控制政策？

(8) 是否定期评审内部控制状况的充分性和有效性？是否及时审查外部监管部门、内部和外部审计部门对内部控制体系的评价报告？是否及时听取了审计部门和外部监管部门有关内部控制体系缺失的建议与意见，并部署采取纠正整改措施？

(9) 董事会、高级管理层是否能及时了解银行的业务风险和操作业绩？银行内部的信息流动是否通畅(包括信息上报、信息下达及机构内部信息的横向流动)？内部控制政策相关每一项信息是否都传达到每一相关人员？

(10) 是否建立了授权和责任明确、报告关系清晰的组织结构？是否采取措施引导管理人

员和全体员工参与到内部控制活动中，以保证内部控制的各项职责得到有效履行？

3. 内控政策

（1）是否已建立文件化的政策（包括人力资源政策、财务管理政策、信贷总量和信贷结构政策、流动性风险和市场风险政策、信息交流政策等等）？

（2）政策的内容是否：第一，为制定和评审目标提供框架；第二，与商业银行的宗旨和发展战略相一致；第三，符合适用法律法规和监管要求；第四，指导员工实施风险控制；第五，体现持续改进内控体系的要求。

（3）政策是否已为员工所理解？

（4）政策是否可以并已向相关方公开，同时寻求互利合作？

（5）各级各类政策是否定期评审，需要时及时更新？

4. 内部控制目标

（1）商业银行已建立了哪些内部控制目标？是否形成文件？

（2）各个目标是否可测量并分解为指标？是否已展开到相关职能和层次？通过哪些方式传达到相关员工？

（3）内控体系的目标是否能确保与法律法规、监管要求相一致并使之满足？能否确保商业银行的发展战略和经营目标的全面实施与实现？确保风险控制的有效性？确保业务记录、财务信息和其他相关信息的及时、真实和完整？

（4）在建立和评审内控目标时，是否考虑了可供选择的技术方案、财务、运作和经营要求、风险相关方的要求等？

（5）内控目标是否符合内控政策？如何体现对持续改进的承诺？

5. 组织结构

（1）商业银行的组织结构状况如何？包括：部门分工合理性、职责明确程度和报告关系清晰程度。

（2）是否考虑职责分离、相互监督制约？

（3）涉及资产、负债、财务和重要人事变动的事项如何决定？

（4）是否建立关键岗位轮换和强制休假制度？

（5）是否建立统一授权体系？

（6）是否设立了全行系统垂直管理、具有充分独立性的内部审计部门？

（7）内部审计部门是否配备了具有相应资质和能力的审计人员？

（8）是否建立了内部审计风险评级体系？每年是否根据审计风险评级结果确定审计频率，以及对机构和业务的审计覆盖率？

（9）内部审计部门是否有权获得商业银行的所有经营信息和管理信息？

（10）内部审计报告是否及时报董事会或董事会审计委员会？

（11）董事会及高级管理层是否采取有效措施保证审计报告中指出的内部控制的缺失得到及时纠正整改？

（12）总行内部审计负责人的聘任和解聘是否经董事会或监事会同意？

6. 企业文化

（1）商业银行是否培育了健康的企业文化？现有企业文化怎样为内部控制提供适宜的环境？

(2) 如何创立和完善企业文化的环境使全行员工树立预期要求的企业价值观、企业精神及经营理念?

(3) 是否把企业核心价值观、内部控制原则、风险意识、风险控制、风险防范,以及出现险情或损失的对策等作为对员工的教育内容?

(4) 是否制定了员工行为准则或类似规范,并传达到员工?

(5) 员工是否熟悉银行关于职业道德的规范并确知职业道德标准和违规行为界限及后果?

(6) 员工是否明白其职权范围违规违纪行为的表现形式?

(7) 是否建立针对员工违规行为的补救和处罚应急机制?

(8) 管理层对员工的违规行为是否进行严厉的批评和处理?

(9) 管理人员道德水平是否保持高尚,是否以身作则?

7. 人力资源

(1) 是否确定与风险和内控有关的人员所必要的能力要求(含满足法律法规要求及监管机构对人员资质要求)?

(2) 是否建立及健全激励约束机制、员工绩效考评体系,是否充分体现风险管理和内控体系要求?

(3) 是否对高管人员及影响风险和内控人员等重要岗位的招聘、聘用、培训、考核、调整、出国、离岗和离行进行控制?

(4) 是否明确了员工招聘、培训、考核、奖励、处罚、晋升等方面合理的政策和程序? 并得到有效执行?

(5) 是否搜集了员工工作业绩、工作效率及胜任程序等相关信息?

(6) 是否采取适当的措施来降低更换员工或员工缺席所带来的负面影响(交叉培训,工作轮换等)?

(7) 是否确保员工得到了充分的非技术性能力的培训(包括人际关系、口头表达和文字表达能力,客户服务等)?

(8) 是否确保每个员工明确所在行及其所在部门的工作目标?

二、风险识别与评估

有效的内控系统需要识别和不断地评估影响银行实现其目标,或者有可能对银行起负影响的有关风险。这种评估应包括银行的和银行组织集团所面对的全部风险。识别和分析那些妨碍实现各种经营管理目标的风险的活动,构成银行风险管理决策的前提和依据。在风险管理的政策和战略制定中,董事会负有最终的责任。风险识别与评估主要包括以下因素。

1. 经营与管理活动的风险识别与评估

(1) 是否识别和确定了常规和非常规的业务和管理活动? 并识别这些活动的风险?

(2) 对新识别的风险是否已考虑到其产生根源、路径及对商业银行的影响范围? 是否已考虑并识别了本部门的运作过程和活动中因运用计算机系统而带来的风险?

(3) 本部门已识别并确定的主要风险有哪些? 是否有风险点的清单? 是否确定风险点的风险级别及风险可接受程度?

(4) 是否对风险的后果及发生的可能性等进行了评估？评估的结果是否形成文件？文件中所包含的信息是否充分，包括可作为建立内控体系中各项决策的基础？并为改进内控绩效提供衡量的基准？

(5) 是否对可接受风险进行定期监测？对不可接受的风险是否制定了相应的控制方案？

(6) 当内外部环境和条件发生变化时，是否对风险进行再识别和再评估？并及时更新风险评估文件及传达到相关人员？再识别和再评估的结果能否确保新的风险及以前未加控制的风险得到识别和控制？

(7) 在设立新的分支机构或开办新的业务时，是否事先制定有关的政策、制度和程序，是否对潜在的风险进行识别和评估，并提出风险防范措施？

(8) 能否及时发现由于员工的思想道德及业务素质问题所产生的风险，并重视对员工的法制教育和职业道德教育？

2. 法律法规、监管要求和其他要求

(1) 是否已建立了相应的程序，以确保商业银行能及时识别和获取适用的法律法规、监管要求和其他要求？包括明确信息获取的渠道、职责等。

(2) 是否及时更新法律法规、监管要求和其他要求的信息，并将这些信息传达给相关员工和其他风险相关方？

(3) 是否在已制定的商业银行规章体系中充分体现应遵循的所有法律法规要求？

(4) 是否采取有效措施管理全行反洗钱工作？

3. 内部控制方案

(1) 是否为实现内控目标制定了内控方案？内控方案如何运用风险识别与评估结果的信息？确定了哪些控制要点和控制措施？

(2) 内控方案是否包括了各项任务的职责权限和相应的控制策略、方法、资源和时限要求？并形成了文件？

(3) 内控方案是否考虑了由方案自身带来的新的风险？方案是否涉及业务流程、管理活动等重大变化？

三、内部控制措施

为保证银行各种经营管理活动目标的实现，需要指导员工实施管理指令，防范和化解风险，执行相关政策和程序，即各种控制活动。这些活动包括高层检查、直接管理、审批、授权、核实、信息加工、确定指标、会计控制、资产保全、职责分工等。

1. 运行控制

(1) 董事会与高级管理层是否及时检查商业银行在实现内部控制目标方面的进展？高级管理层是否根据检查情况提出内部控制缺失，督促职能管理部门改进？

(2) 各级职能管理部门是否审查收到的经营管理情况和特别情况专项报表或报告？是否提出问题，并要求采取纠正整改措施？

(3) 对实物控制是否实行实物限制、双重保管和定期盘存？

(4) 是否审查遵循风险限制方面的合规性，并在不合规的情况下继续跟踪检查？

(5) 是否根据若干限制条件对各项业务、管理活动进行审批与授权，明确各级管理责任？

(6) 是否验证各项业务、管理活动，以及所采用的风险管理模型的结果，并定期核实相关情况？是否及时将发现的问题向职能管理部门报告？

(7) 是否实行不兼容岗位的适当分离？

(8) 是否针对已识别的风险和需采取的控制措施，确定其运作过程和活动？

(9) 对已确定的过程和活动如何实施控制？

(10) 对缺乏程序可能导致偏离内控政策和目标运行的情况，建立并保持了哪些程序文件，在程序中是否规定了操作方法和标准？

(11) 在实施和运行中按照程序规定如何实施持续记录和监督检查？

(12) 运用计算机系统采取了哪些内控措施？

(13) 对购置和使用的设施、设备、系统和服务中已识别的风险是否建立并保持控制程序实施有效控制，并以什么方式将有关程序和要求通报供方，使其符合控制要求？

(14) 为从根本上消除或降低风险，针对产品和业务、运行程序和工作组织设计及对人员适任能力要求建立了哪些控制程序？

(15) 是否建立有效的核对、监控制度？对重要业务是否实行双签制度及监控授权、授信执行情况？

(16) 是否建立完整的会计、统计和业务档案？

2. 计算机系统环境下的控制

(1) 是否建立信息安全管理体系？

(2) 是否对计算机信息系统从立项、开发、验收、运行和维护实施全过程管理？例如，项目立项时技术部门是否与业务部门进行了充分论证和良好沟通；程序开发环境是否与程序生产环境严格分离；计算机软件和网络系统从开发环境转入生产环境之前是否进行充分的压力测试？

(3) 对外购计算机软件、硬件设备是否严格审查供应商的资格和资信状况？是否明确其产品在使用期间应当承担的使用、维护和其他责任，在使用前是否严格进行安全性测试确保产品正常使用和有效维护？

(4) 计算机机房建设是否符合国家有关标准？是否加强计算机机房管理，出入按规定审批并保留记录，确保硬件、各种存贮介质的安全？

(5) 是否建立和健全网络管理系统，有效地管理网络的安全、故障、性能、配置等，并对接入国际互联网实施有效的安全管理？

(6) 采取哪些措施确保计算机信息系统的安全(如更新系统、认证、加密、内容过滤、入侵监测、安全设置、防止病毒、黑客攻击、软件补丁程序等以确保计算机信息系统安全)？有关程序和要求是否及时更新？

(7) 网络设备操作系统、数据库系统、应用程序是否设置必要日志，满足内外审计需要？

(8) 对各类数据信息、数据操作、数据备份介质的存放、转移、销毁是否有严格的管理制度？

(9) 计算机处理业务如何确保可复核性和可追溯性？应用程序是否为有关的审计和检查预留接口？

(10) 电子银行服务是否具备确保识别客户身份，安全认证等功能，保证交易安全，防范操作风险？

(11) 计算机操作系统的变更是否有明确的规章制度(对内和外包系统),可靠的技术手段,满足合法性、正确性、安全性、可复核性和可追溯性的系统变更控制要求,并对软件版本进行管理?

(12) 是否建立设备管理系统,对设备验收、入库、配发、维护、变更、损益、报废等环节进行管理?

(13) 是否建立远程备份?

(14) 是否提供对电子银行客户的培训、客户服务和相关支持工作?如何与风险控制方案相结合?

(15) 在制定电子银行业务的准入标准、管理办法和操作规程中,如何考虑风险因素及相应措施?

(16) 如何控制网上银行交易的风险,确保交易安全?

(17) 系统安全运行中的不安全因素是否全面分析和控制?对分中心运行如何监视?

(18) 对计算机系统数据的管理。是否建立接入授权程序并对接入后的操作进行安全控制?是否核对输入数据,对数据的修改进行批准并建立日志?

(19) 计算机系统运行过程中是否配备计算机安全管理人员且明确其职责?是否建立技术部门和业务部门的沟通渠道?

(20) 如何明确用户的创建、变更、删除、用户口令等控制要求;是否明确员工计算机信息系统的用户名或权限卡的使用要求?

3. 应急准备和处置

(1) 是否已建立并保持应急预案和程序,已识别可能发生意外或紧急事件?

应急预案是说明特定紧急情况发生时必须采取的措施,应包括以下方面:

Ⅰ. 识别潜在的事故(风险)和紧急情况。

Ⅱ. 确定紧急情况发生时的负责人。

Ⅲ. 确定紧急情况发生时各类人员的行动计划,包括发生紧急情况的区域内所有外来人员的行动计划。

Ⅳ. 确定紧急情况发生时具有特定作用人员的职责、权限和义务,如柜员、保安、保卫人员等。

Ⅴ. 明确与外部应急机构的接口。

Ⅵ. 与执法部门进行交流。

Ⅶ. 重要记录资料和重要设备的保护。

Ⅷ. 紧急情况发生时可利用的必要资料,如报警设备和联络电话号码等。

(2) 在应急计划中是否对外部机构的参与有明确的规定,是否向其说明他们需参与和可能遇到的情况,并提供相关信息以便其参与?

(3) 如何规定意外或紧急事件发生时,应采取应急响应的措施?措施是否及时、有效?

(4) 是否规定并实施对应急的设施、设备和系统定期检查和维护?是否保证充足提供?

(5) 在可行情况下,是否对应急预案定期进行演习和测试?是否按计划进行应急演练?

(6) 是否对制定的应急预案进行评审?应急准备是否与可能发生的意外或紧急事件的性质(如事故、险情)相适应?

(7) 近年来,是否发生过意外或紧急事件(如挤兑、信息系统崩溃、火灾、地震等)?如发生

过，如何按应急预案及时、有效采取相应措施，并确保业务持续开展？

四、监督评价与纠正

内部控制系统需要监督，监督可确保内部控制能有效运作。它是一个不断评估系统的质量的过程。监督评审是经营管理部门对内部控制的管理监督和审计部门对内部控制的再监督和再评价活动的总称。它通常由管理层自测和由董事会委派内部审计员或外部审计单位审计来完成。审计部门一般在下列方面为机构提供监督服务：评估管理控制的效率和效果；评估资产和风险；针对检查出的问题向管理层提出改进意见。

1. 内部控制绩效监测

(1) 是否建立了内部控制绩效监测程序？

(2) 绩效监测的对象有哪些？

(3) 内控绩效监测的方法有哪些？

(4) 何时进行内控绩效监测(频次)？

(5) 监测结果评价的准则是什么？

(6) 监测结果的信息如何传递和利用？

(7) 对下一级分行的经营、管理是否进行经常性检查？并及时纠正问题？

(8) 如何对全行的经营、内控和风险状况的审计、监督和评价做出安排？审计的频次是怎样决定的？

(9) 如何对全行审计工作执行有关审计政策、审计准则和规章制度情况进行监管和检查？

(10) 是否对审计监督中发现的重大问题和事件的处理结果进行跟踪，以防止问题或事件的再次发生？近年来发现的重大问题和事件是否已采取有效措施？

(11) 如何确保全行的审计部门和审计人员的独立性？

(12) 高级管理人员离职时是否进行离任审计？

(13) 如何对审计效果进行评价？

(14) 如何对高层人员进行监督？是否有监管档案？

2. 事故、险情、违规和纠正与预防措施

(1) 是否已建立和保持了书面程序文件，规定事故、险情、违规发现、报告、处置、原因分析及纠正和预防措施等内容？

(2) 发现事故、险情、违规时，是否及时报告？

(3) 如何处置事故、险情、违规事项？从发现到处置的时效如何？

(4) 针对发现的事故、险情、违规的原因，所采取的措施(纠正或预防措施)是否考虑了问题大小和风险危害程度？

(5) 纠正或预防措施在付诸实施前是否做过风险评估？

(6) 被批准执行的纠正或预防措施是否实施？这些措施的效果是否能防止发生或再发生事故、险情、违规？

(7) 发生事故、险情和重要违规事项时是否追究相关人员责任？

(8) 在内控评价、业务检查和审计中，对发现的问题，如何作责任认定？

(9) 信访、举报、投诉、控告、处分的程序和记录的管理方式如何？