前　言

信息科技已经成为银行业金融机构实现经营战略和业务运营的基础平台以及金融创新的重要手段。银行业对信息科技的高度依赖，决定了信息系统的安全性、可靠性和有效性对维系整个银行业的安全和金融体系的稳定具有至关重要的作用。

银监会党委对信息科技风险监管工作高度重视，刘明康主席多次召开专项工作会议并做出重要批示和指示，明确要求着力推进信息科技风险监管。银监会坚持贯彻“管法人、管风险、管内控、提高透明度”的监管理念，把信息科技风险纳入银行总体风险监管框架，切实加强制度建设和风险监控，确保银行业信息系统安全稳定。

在目前信息技术革新日新月异、金融业务不断创新、银行对信息科技依赖性越来越大的新形势下，银监会坚持“风险为本”的监管原则，提出了信息科技风险功能性监管的新思路，突出“制度先行”，完善监管框架，借鉴和吸收国际先进标准及业界最佳实践，不断丰富信息科技风险监管方式方法，制定了一系列的监管规范，结合奥运保障开展现场检查，并针对性地发出有关风险提示，建立非现场监管体系和监管评级体系，从而构建了信息科技风险监管的基础框架，全面展开信息科技风险的监管工作。

按照郭利根副主席提出的“集成资源，形成信息科技风险监管合力”和“搞好规划，全面加强信息科技风险监管制度建设”要求，银监会强化机制建设、优化资源配置，整合科技人力资源，集中全国银监会系统科技骨干力量，在北京成立了信息科技监管“专项工作组”，又在上海、深圳两地分别成立信息科技风险监管工作室，按照统一调度、统一指挥、统一培训的工作原则，制度建设、奥运保障、现场检查、非现场监管及监管评级五线并举，形成了矩阵式的监管工作模式，快速锻炼了一支能战会战、能够担当重任的信息科技风险专业化监管队伍。

《手册》的编写得到了各方的大力支持。上海、湖北、安徽、山东、山西、江苏、江西、河南、内蒙古、黑龙江、青岛、福建、河北、宁夏、辽宁、吉林、浙江、四川、深圳、广东、

天津、重庆、大连、云南、贵州银监局派出精锐技术骨干，参加《手册》编写工作；银监会各部门与各银监局提出了许多宝贵意见；上海银监局为编写工作提供了大量支持和保障工作。整个《手册》内容融合了银监系统内信息科技人员的经验和智慧，汇聚了银监会各部门与各银监局的宝贵意见和建议，应属于银监会系统及科技人员共同努力的成果和结晶。在此，向所有参与工作的单位和个人致以诚挚的谢意!

编写人员

林　丽　朱永扬　徐卫飞　李　丹　骆絮飞　邹　伟　房世晖
崔维琪　朱　斌　冯业伟　叶　照　乔昱瑞　纪奕武　齐兴利
吴瑞麟　张　伟　张惠芳　李晓东　陆　阳　陆　翔　陈云龙
陈宏宇　周嘉弘　郝海峰　杨中华　崔　晨　盛于南　游　琨
谭　杨　史文明　何　禹　靖雪晶　徐美东　徐殿南　刘　楠
李　鹏　李海波　包　龙　殷有超

目 录

第一部分·概述

第一部分 概述

1. 银行信息科技风险及其监管

1.1 银行信息科技风险

定义银行信息科技风险，既要考虑银行的金融特性，也要考虑信息技术本身的特点。银行作为金融机构，其信息科技程度可以直接或间接影响资金融通活动过程，其本身也存在决策问题，也可能因为信息科技某些因素的变化导致银行资金、财产、信誉遭受损失。

银行信息科技风险是指银行在使用信息技术过程中，由于信息技术因素或与信息技术相关因素，导致银行经营不确定、管理不利，并最终导致资金、财产、信誉遭受损失的可能性。其中的信息技术包括计算机硬件、软件、网络通讯设备，各种银行终端设备等。

1.2 银行信息科技风险特点

技术性。银行信息科技本身是利用现代信息技术改造银行经营、管理方式，从而提高生产效率的过程，他涉及现代计算机技术、网络通讯技术、安全技术等多方面技术问题，一旦出现问题，都体现了其技术含量极高的特性。

突发性。信息科技风险的突发性体现在两个方面，一是自然灾害的突发性，导致银行由于信息技术领域的基础设施遭到破坏，造成银行财产损失或业务中断，使银行产生风险；二是由于信息过程的技术性，只要任何一个环节突发故障，都可能造成整个系统无法使用，从而给银行形成风险。

传递性。由于计算机网络快速传递的特点，一旦系统出现故障，可以使金融风险迅速从局部蔓延到整个网络涉及的每一个部分，从而导致风险的进一步加剧。

广阔性。由于金融在经济发展中的核心地位越来越得到大家认可，因此一旦因为信息技

术导致银行产生风险，其影响非常广阔，它不仅涉及千千万万的普通老百姓、大大小小的企事业单位，更是影响社会的方方面面，甚至会对整个社会秩序带来极大的负面影响。

多元性。传统的银行风险，多发生在银行营业场所，通过银行柜台、ATM 等有限的经营场所形成。但在银行信息技术大量运用以后，使得银行风险既可以通过原有渠道形成，也可以通过电话、POS、计算机、电视和手机等任何接入网络的终端设备形成。表现出风险形成的多元性。

多方性。随着银行信息技术的发展，保证银行正常经营不止银行本身，电信部门、电力部门、产品提供商、服务提供商和商家都已成为银行正常经营的一部分。往往银行业务系统一旦出现故障，容易出现责任无法鉴定的情况，也常常给问题的快速解决带来影响。

1.3 风险成因分析

信息科技风险形成原因是多方面的，既有信息科技自身的特点所决定的内部因素，也有自然灾害，人为失误和故意破坏的外部因素，归纳起来主要有以下几种：

信息技术的缺陷，使风险不可避免。现代信息技术虽然取得了长足的进步，对社会经济发展、对银行业的发展做出了很大贡献，但现代信息技术也不是完美无缺的，其本身也经历发展和完善交替进行的过程。大致来说，信息技术诱发风险表现在以下几方面：一是由于网络设备生产技术不过关、网络通讯技术不够先进、或者网络设备管理水平不到位等因素，使得一些不可预见的原因导致网络出现故障，从而影响到银行业务的正常进行给银行带来损失；二是由于操作系统或者数据库管理系统漏洞原因，导致数据损坏、系统受到攻击或者应用系统无法正常运行等问题，从而给银行带来风险；三是由于各类应用系统设计的不科学、不合理，或者隐藏未发现的瑕疵，致使业务运行中断、或者数据错误导致出现风险；四是安全技术运用不当，或者安全技术不过关也是诱发风险发生的一个主要原因；五是由于认证技术不过关，导致出现资金丢失或被骗取等问题，给银行和银行客户造成损失。

信息科技的广阔性，使风险面扩大。一方面，银行几乎所有的业务都使用了信息技术，使得信息技术在银行经营中无处不在；另一方面，银行由于信息技术的使用，使得银行业务延伸的广度和深度发生了很大变化，特别是网络技术的应用，电子银行的发展，使得银行的

业务操作不再仅仅局限于银行内部员工，银行业务的操作已成为全社会的行为。正是由于这些特性，使得银行出现了一些新的风险因素：一是由于客户的误操作造成诸如信息泄露等问题，导致银行或客户财产损失；二是攻击由于网络和银行的各类终端面向全社会，使得不法分子利用网络漏洞进行攻击，盗取银行资金或者进行恶意破坏，给银行造成损失；三是容易受到计算机病毒的攻击和破坏，从而造成损失。

自然灾害客观存在，使风险难免出现。自然灾害的破坏力往往是惊人的，它可以破坏银行信息科技过程中的一些关键场所和关键设备，如机房、各类设备、通讯设施，以及关键的银行业务数据等，从而导致银行无法正常经营，财产受到直接和间接损失等风险。

制度措施不到位，形成风险隐患。制度因素体现在以下四个方面。一是外部法律法规不健全。信息技术的发展往往先于法律法规，当银行使用一项新的信息技术时，如果没有相关法律法规的及时跟进，就会在行为出现争议时没有法律依据，从而导致银行面临诉讼、赔偿和合同失效等法律风险，特别是目前电子银行的快速发展，这一问题显得更加突出；二是内部管理措施不到位。银行大量使用信息技术以后，其业务流程发生很大变化，如果银行管理方式不跟着改变，内部管理制度不及时跟进，就会出现因为内部人员钻制度漏洞而作案的风险；三是安全措施风险。安全技术不到位会给银行造成风险，但如果与之配套的安全管理规章制度能够到位，同样会给银行带来损失，如果相应制度到位，可以大大减少此类风险；四是因技术外包导致风险。随着银行信息科技的发展，银行出于技术人员短缺和降低经营成本两方面的考虑，会将技术外包给专业的信息技术服务商，通过付给一定的费用，由其代为开发、维护和管理等，但这样的做法同样会导致信息系统失控、服务不能满足需要和商业信息泄露给竞争对手的风险。

1.4 信息科技风险监管意义

在银行业高度依赖信息技术的今天，因信息技术诱导金融风险的不确定因素增多，复杂性加大，信息科技风险上升。开展银行信息科技风险监管，将在一定程度上减少或杜绝银行因信息科技而给自身或客户带来损失。其意义在于：

第一，督促银行业信息科技健康稳定的发展。我国银行信息科技发展最大的一个弱点是

规划性不强，没有一套统一的标准来规范和引导银行信息科技发展的道路。开展银行信息科技风险监管，银监会将会陆续出台相关的监管标准和评级标准，相信这些措施将是我国银行业信息科技过程中重要的参考依据，这也将必然引导我国银行业信息科技发展的道路更加规范。

第二，促进银行业金融机构内控能力的提高。开展银行信息科技风险监管，对银行业金融机构加强信息科技管理水平、开展内部信息审计提出了很高的要求，银行业金融机构必然采取措施，避免风险的出现，这将在一定程度上促使银行加强内部管理，对银行提高内控水平是一次促进和提高。

第三，维护金融体系的安全运行。由于信息科技本身的特点决定，一旦信息科技风险出现，影响面将非常大，特别是由于网络普遍运用，风险不仅涉及自己，也会涉及其他银行，甚至有可能是银行以外的证券、保险机构。因此开展银行信息科技风险监管，将有利于维护整个金融体系得安全运行。

第四，保证银行客户的合法利益。银行金融机构是高负债的行业，一旦出现风险，将直接影响到其客户的利益，因此确保银行在信息科技背景下安全运行，也是对其客户利益的最大保护。

2. 现场检查一般流程

现场检查程序包括现场检查准备、现场检查实施、检查后续工作三个阶段。

2.1 现场检查准备阶段

对一个现场检查项目，现场检查前准备工作应包括以下内容：

一、确定现场检查对象。一般情况下，应在每年初制定年度现场检查计划，并确定现场检查对象。确定检查对象的依据：一是银监会的指导意见、工作安排，二是对被监管机构进行检查的时间间隔情况，根据分类监管原则，对不同风险的机构检查频次应不同，但建议至少每 2 年对一家机构应进行一次全面现场检查，三是被监管机构的动态情况。如果某机构出现异常情况，可随时安排对该家机构的专项或全面检查。

二、制定现场检查草案。确定检查对象后，应根据该机构情况制定检查草案，检查草案应包括检查目的、检查类别（全面或专项）、检查范围（单家机构、某类机构、总部、分支机构）、检查内容（全面检查，应包括系统各个方面，专项检查，可只查某一方面或几个方面）、检查重点（应根据检查目的确定检查重点）、检查期间等。

三、确定现场检查人员。银监会组织的现场检查，由银监会从银监局统一抽调人员参加检查；银监局自行安排的检查，由银监局自行组织人员检查，必要时可以提请银监会在系统内集中抽调人员开展检查。检查人数应根据被检查银行信息科技发展情况确定，不得少于 2 人。检查人员一般应具有信息科技背景，必要时可以适当补充部分业务人员参加。

四、发送并回收现场检查前问卷。确定检查对象后，应在正式进点前向被检查银行发送检查前问卷。问卷要使用统一格式。发送问卷一定要明确填报要求，包括填报资料的截止日期、回收问卷的时间等等。为保证检查人员有充足时间阅读、分析问卷，应在进点前 10 天以上回收问卷，并对错报漏报的项目立即要求被检查银行重报或补报。

五、收集其他与被检查银行有关的信息。除向被检查银行发出现场检查前问卷外，还应收集与本次检查有关的文件及其他资料，如有关的政策法规文件、被检查银行以往报送的资料及监管部门对该机构历次检查材料以及群众举报材料等。

六、对所有资料进行分析研究。检查组成员应对回收的检查前问卷、收集的其他资料进行整理、研究和分析，熟悉有关法规及被检查银行情况，找出可能发现的问题线索，为正式进点检查做准备。必要时应于检查前将所有检查人员集中一段时间专门阅读检查前问卷和其他有关资料。

七、确定现场检查方案及人员分工。根据对有关资料的分析研究，检查组织者应在检查草案在基础上，制定检查方案，并明确人员分工和具体检查进度。一般一个检查组应设组长 1 名（必要时可设副组长 1 名），主查人 1 名（必要时可设副主查人 1—2 名）。组长全面负责现场检查项目的组织协调和实施工作，包括审定检查方案，组织进点、离点会谈，与被检查银行就有关问题进行协调，修改审定现场检查报告，提出处罚意见和建议等。主查人负责检查方案的拟订、检查进度的安排、人员分工、各小组之间的协调、事实确认书的审核、检查事实与评价的起草、汇总检查报告、拟定现场检查意见书及行政处罚意见书等工作。一个大

的检查组还应根据工作量情况分为若干工作小组，对不同的检查内容分别进行检查。

八、发送现场检查通知书。在确定现场检查方案后，应向被检查银行发送现场检查通知书，并最好在进点前 5 天送达被检查银行（突击性现场检查可在进点检查时当场出示检查通知书除外）。原则上，谁组织检查谁出具现场检查通知书。

2.2 现场检查实施阶段

现场检查实施阶段包括进点会谈、分工检查和离点会谈。

一、进点会谈

进点会谈标志着现场检查的正式开始。进点会谈应要求被检查银行管理层相关成员及检查组所有成员共同参加。进点会谈的目的，一是通报现场检查的目的、内容、初步计划和安排，介绍检查组成员；二是向被检查银行提出配合检查的有关要求（如提供工作场地、及时提供资料等）；三是请被检查银行介绍有关情况，并对检查组需重点了解的问题进行交流。进点会谈的时间长短可视会谈情况灵活掌握。

二、分工检查

（一）对每项业务检查，都应形成工作底稿。工作底稿是对检查过程的记录，既是对工作量的统计，更是对检查事实的描述，是形成检查事实与评价及汇总报告的来源和基础。因此，工作底稿既要记录问题，也要记录其他客观情况。一般工作底稿应包括检查日期、检查人、检查项目、客观描述、发现问题、分析评价、初步定性等内容（见工作底稿格式）。必要时在要对检查过程中内容定期进行小结。

（二）对检查发现的每项问题，都应该及时取证。如通过谈话发现的问题，应要求被谈话人在谈话记录上签字；对查阅文档发现的问题，应复印有关资料，并在资料及检查人员工作底稿上由被检查单位加盖公章。

（三）每日小结。每天检查结束后，组长或主查人应召集所有检查组成员开碰头会，一是各小组交流当日检查情况及发现问题；二是根据检查情况确定次日的检查重点和内容，并对检查进度进行必要调整；三是提出需与被检查银行进行沟通的事项。

（四）分组检查结束后，主查人应指派检查人员分项整理汇总工作底稿，形成事实确认

书，对检查中存在问题的事实进行列举和描述（只记录事实，不做任何评价）。事实确认书要及时送被查银行签字确认。

三、离点会谈。所有检查项目结束后，应与被检查银行举行离点会谈。参加离点会谈的人员与参加进点会谈的人员应一致，由组长或主查人通报现场检查事实与评价，并听取被检查银行的意见。

2.3 现场检查后续阶段

现场检查后续阶段包括向被检查银行发送《检查事实与评价》、撰写现场检查报告、下达现场检查意见书、下达行政处罚告知书（需要时）、下达行政处罚决定书（需要时）、后续跟进检查和检查资料归档等。

一、发送《检查事实与评价》。根据离点会谈沟通情况，修改检查事实与评价，由现场检查项目的组织机构向被检查银行发送《检查事实与评价》，并要求被检查银行在5个工作日内反馈书面意见。

二、撰写检查报告。根据《检查事实与评价》反馈意见，形成现场检查报告。检查报告应包括以下几部分：1、检查开展情况；2、被检查银行基本情况；3、检查事实与评价；4、检查组与被检查银行存在的主要分歧；5、对检查中发现问题的处理意见；6、对监管工作的建议；7、其他需说明的问题。

五、下达行政处罚意见告知书。如需对被检查单位违规问题进行行政处罚，应向其下达《行政处罚意见告知书》，告知做出处罚决定的事实和依据，同时告知被检查单位有权在收到《行政处罚意见告知书》5 个工作日内进行陈述和申辩，或对重大行政处罚决定要求举行听证会。

六、下达行政处罚决定书。如被检查银行在规定时间内未提出陈述和申辩，或监管部门认定被检查银行提出的申辩理由不充分，应根据原处罚意见予以处罚，并向被检查银行下达《行政处罚决定书》。《行政处罚决定书》的内容包括：违反法律、行政法规和金融规章的事实和证据，行政处罚的种类和依据，行政处罚的履行方式和期限，申请行政复议或提请行政诉讼的途径和期限等。

七、后续检查。收到被检查银行的整改计划后，检查组一方面应跟踪整改计划的落实情况，另一方面应在适当时间（一般为现场检查意见书中规定的所有整改项完成时间）对其整改情况进行检查验收，即后续跟进检查，并对后续检查情况做出评价和报告。如后续检查发现被检查银行对上次检查发现的问题没有彻底纠正或又有新问题发生，应从严处理。涉及行政处罚的要加重处罚，不涉及处罚的可从审慎监管角度对其业务及机构准入进行适当限制。

八、检查资料归档。所有检查及处理过程结束后，检查组应对检查资料进行整理并归档。归档资料应包括：检查方案、检查前问卷的反馈材料、检查通知书、工作底稿、证明材料、检查事实确认书、检查事实与评价及反馈意见、现场检查报告、《现场检查意见书》、《行政处罚意见告知书》、《行政处罚决定书》、后续检查所有有关资料等。原则上，检查档案应由被检查银行的属地监管局留存，检查组有权调阅。

3. 常用检查方法

询问：向适合的人员询问有关控制运作的资料。

交叉/确证询问：除实施适当测试手段外，通过询问企业内其它人员 ，验证控制的执行情况。这个过程的目的在于确认控制使用的有效性及一致性。

观察：观察控制运行的实际情况。

审阅：检查控制生成的记录和文件，作为控制设计和执行情况的证据。

重新运行：重新履行某些控制程序，以证明其运行是正确的。

能力评估：综合运用询问、文件检查、重新履行等手段，可以测试某个管理人员在某一领域的知识及其实施某项控制程序的胜任能力。

系统验证：测试信息系统中的自动化控制是否按设计要求运行。

穿行性测试：追踪交易在信息系统/业务流程中的处理过程，以证实所了解的流程与控制。一般可与询问方法一起执行。

分析性复核：分析重要的比率或趋势，调查这些比率或趋势的异常变动及其与预期数额和相关信息的差异。

数据验证：直接抽取数据进行完整性与准确性的验证。

第二部分·科技管理

第二部分　科技管理

4. 科技治理

中国银行业监督管理委员会颁布的《银行业金融机构信息系统风险管理指引》明确指出了银行业金融机构的科技治理的目标，银行业金融机构的董事会和高级管理层要根据本银行的发展战略，运用先进管理理念进行 IT 治理。通过 IT 治理，加强银行业金融机构日益赖以生存和发展的信息科技实力和信息科技安全，提高信息技术使用效益，推动银行业金融机构的业务创新，增强核心竞争力和可持续发展能力。

4.1 董事会及高管层

检查项 1 ：董事会和高级管理层

基本要求：1、董事会和高级管理层必须要有分管信息科技的领导；应该建立负责全行信息科技工作的管理机构：负责制定全行信息科技工作的总体策略、统筹信息科技系统项目建设、组织和领导全行的信息科技工作。2、董事会和高级管理层要定期审查全行的信息科技战略规划，确保科技战略与银行总体发展战略相一致；提供信息科技建设所需的经费；检查和监督信息科技战略规划的完成情况。3、董事会和高级管理层要定期审查全行的信息科技风险管理政策和框架的建设情况，了解信息科技风险状况，建立覆盖全行信息科技风险的三道防线。4、董事会和高级管理层要对 IT 审计报告进行审查，研究决定确实可行的整改计划，落实整改措施。5、董事会和高级管理层每年要组织进行全行总体信息科技风险审计评估，经过董事会或其他决策机构审查后，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。6、董事会和高级管理层应该及时向银监会及其派出机构报告本机构发生的重大信息科技事故、突发事件，并按预案快速响应。7、董事会和高级管理层应该认真贯彻执行国家有关信息科技的法律法规以及技术标准，切实落实银监会有关办法要求。

检查方法、步骤：

调阅:1、向银监会报送的信息科技风险管理年度报告。2、向银监会报送的重大信息科技事故、突发事件的报告。3、银行的信息科技发展规划。4、董事会高级管理层关于信息科技工作的会议记录。5、风险管理部门制定的信息科技风险管理政策。6、董事会高级管理层决定的审计问题的整改计划。

访谈董事会高级管理层中分管 IT 工作的领导，重点关注：1、董事会或高级领导层对信息科技工作的情况介绍，包括董事会或高级领导层提出了哪些 IT 建设项目，IT 建设的经费投入，了解董事会或高级领导层如何重视 IT 的规划和建设 2、董事会或高级领导层对信息科技风险认识，在建设信息科技风险的三道防线方面采取了哪些措施 3、董事会或高级领导层对有关的信息科技风险报告、信息科技事故报告、信息科技现场检查报告、信息科技审计报告采取了哪些有效的整改措施。

4.2 信息科技工作的管理机构

检查项 1 ：全行信息科技工作的管理机构

基本要求：1、银行业金融机构要建立负责全行信息科技工作的管理机构（对中小型银行可以和 IT 开发部门、IT 运维部门合为同一个部门；对大中型银行，信息科技工作的管理机构可以与 IT 开发部门、IT 运维部门分开，并为在其之上的管理领导部门），负责制定全行信息科技工作的总体策略、统筹信息科技系统项目建设、组织和监督全行的信息科技工作（大中型银行的董事会下面可以设置信息科技管理委员会，作为董事会的咨询、考核机构）。2、信息科技工作的管理机构除了负责组织和领导 IT 部门的开发、运维、安全工作，还负责协调全行各个部门与 IT 有关的事宜。3、信息科技工作的管理机构应该配合风险管理部门，制订出覆盖全行的 IT 风险管理政策，并制定出包括但不限于—需求分析、项目立项、开发测试、上线运行、维护变更、数据安全、业务操作手册、访问安全控制、业务连续性、应急预案—各个 IT 环节的风险控制策略，作为各个 IT 部门和业务部门制定本部门的 IT 风险管理程序的指导方针。4、信息科技工作的管理机构应该配合审计部门，做好全行的 IT 审计和审计问题整

改工作。5、信息科技工作的管理机构应该协助业务部门制定出相关的 IT 业务程序操作手册和安全控制方法，做好业务人员的 IT 操作技能培训和 IT 风险意识教育，协助做好业务环节的 IT 风险控制。6、信息科技工作的管理机构应该根据银行的总体发展规划，制定出全行的 IT 发展规划，提出科技项目预算，并报董事会或高级领导层审核后组织实施。7、信息科技工作的管理机构应该根据 IT 风险控制策略，组织 IT 开发部门、IT 运维部门制定出各项具体的控制流程和管理制度，从安全性、业务连续性、外包服务、应急管理等各个方面控制 IT 风险。8、信息科技工作的管理机构应该定期向董事会或高级领导层汇报信息科技发展规划的执行状况、信息科技预算和支出、信息科技的工作状况，以及信息科技风险整体状况。9、信息科技工作的管理机构应该积极配合银监会及其派出机构做好信息科技风险现场检查和非现场监管工作，并按照监管意见做好整改工作。

检查方法、步骤：

调阅：1、信息科技管理部门的章程文件。2、信息科技工作的管理框架和管理制度清单。3、信息科技工作的管理机构的工作计划和计划完成情况 4、信息科技方面发生的重大问题事件清单和处理方式；

访谈信息科技管理机构负责人，重点关注：1、了解信息科技条线的组织结构和工作分工，了解信息科技管理部门的组织结构。2、了解信息科技工作的管理框架和管理制度结构，了解信息科技管理部门如何从组织和人员上履行上述职责的。3、了解信息科技管理部门的工作计划完成情况，了解有哪些难点，从中查找问题和原因。4、了解重大问题事件发生的原因。5、了解信息科技管理部门制定的 IT 风险政策是否全面和有效？6、了解信息科技管理部门针对审计出来问题采取的整改措施。

4.3 信息科技部门

检查项 1 ：信息科技部门

基本要求：1、建立与银行业务相适应的信息科技部门，负责 IT 业务产品的开发、外包、测试、上线、变更，负责相应 IT 系统的运行、维护、安全，为银行提供 IT 业务产品。2、信息科技部门应该根据工作内容，制定出部门内部完整的工作流程和内控制度，在各个信息科

技部门之间制定出协调配合机制，保证信息科技工作有序高效。3、信息科技部门应该分析评估 IT 生命周期的各个环节的 IT 风险，制定出各个环节的 IT 风险控制策略；根据策略制定出每个 IT 产品和每个 IT 系统的风险控制措施；并且制定出相应的工作流程和制度执行情况的检查流程，确实做好 IT 风险控制。4、信息科技部门应该根据相应 IT 规模和技术要求，配置适当数量和水平的信息科技人员，保证各个 IT 系统和各项 IT 工作能够安全持续地正常运转。信息科技部门要做好科技人员管理：信息科技人员要有良好的个人品德和良好的职业道德，有良好的信用记录，有相应的知识技能；应该注重科技人员科技教育、风险安全教育。5、信息科技部门应该建设一支与银行 IT 业务产品开发战略相适应的 IT 开发队伍，要做好 IT 开发管理，以及相关的外包服务管理、知识产权管理，要做好 IT 开发环节的风险管理，为银行提供安全的 IT 业务产品。6、信息科技部门要建设好银行 IT 系统安全连续运行的环境（包括场地环境、设备环境、网络环境、系统环境、数据安全环境、访问控制环境、管理制度环境），做好各种环境的监测控制，做好事件、问题管理和变更管理，做好紧急事件应急预案。7、信息科技部门要严格遵守国家的各项安全管理制度，配合风险管理部门、合规部门、业务部门编制好各项 IT 业务产品的操作手册和访问控制制度，协助做好全行业务部门的 IT 风险控制和 IT 风险的安全教育。

检查方法、步骤:

调阅：1、信息科技部门的各项工作流程和相应的规章制度。2、信息科技部门制定的信息科技风险管理策略。

访谈信息科技部门负责人、信息科技部门内部各条线的负责人、信息科技部门的 IT 风险管理人员，重点关注：信息科技部门的设置是否完善合理，职责分明？了解 IT 各个部门、各个条线之间存在哪些矛盾？查找问题原因；

(1) 信息科技部门内部设置了哪些条线？各条线有无明确的业务流程？各条线是否配置了合适的科技人员？各条线是否都能正常地运转？

(2) 信息科技部门内部有无专职的 IT 风险管理岗位和人员？

(3) 信息科技部门内部有无 IT 风险管理策略？各个业务流程、各个运行环境、各个控制环节有无明确的控制制度？

(4) 信息科技部门有无针对科技人员的管理机制?

4.4 信息科技战略规划

检查项 1 ：信息科技战略规划

基本要求：1、信息科技战略规划是指导信息科技工作的大纲。应该高度重视制定信息科技战略规划，要在充分的市场和技术调查分析基础上，由银行的高级管理层、市场部门、管理部门、科技部门共同讨论制定，并且经过董事会和高级管理层审查和批准。2、信息科技战略规划应该以企业的发展战略为中心，以银行产品战略为着手、以业务流程为导向，以实现信息科技设施和信息的安全、实现对信息科技风险的识别评价控制为基础，组织开展 IT 治理，为实现银行发展战略提供紧密的 IT 支持。3、信息科技战略规划应该包含但不限于：IT 产品的开发规划、IT 基础架构规划、IT 服务水平建设规划、信息科技的管理组织和管理制度建设规划、信息科技风险管理政策和企业文化建设规划。4、信息科技战略规划应该包含详细实施方案、工作进度计划、考核指标、费用计划。

检查方法、步骤:

调阅：1、信息科技发展战略规划或其他中长期发展规划。2、信息科技发展战略规划所包含工作的完成情况。

访谈信息科技部门管理部门负责人和相关工作人员，重点关注：1、了解信息科技发展战略规划的制定过程，是否有各方面的人员参与，是否经过高级管理层的审批？2、了解信息科技发展战略规划的内容，是否包含了 IT 工作的各个方面？3、了解信息科技发展战略规划工作的完成情况，了解 IT 工作的总体状况，查找 IT 工作的薄弱点和问题原因。

4.5 信息科技风险管理部门

检查项 1 ：信息科技风险管理部门

基本要求：1、必须建立或明确全行信息科技风险的管理部门：配置足够的专职 IT 风险管理人员，负责建设全行 IT 风险管理框架，牵头组织、协调、检查全行的 IT 风险管理工作。

2、应该把 IT 风险管理纳入全行总体风险管理框架，制定全行的信息科技风险管理大纲。管理大纲应该描述信息系统的风险，信息系统风险的识别和评估流程，描述持续的信息系统风险控制政策、风险和事件的报告处理机制。3、必须建立覆盖全行范围的 IT 风险控制策略，IT 风险控制策略应该包含但不限于：需求分析、IT 项目立项、开发测试、上线运行、访问控制、数据安全、维护变更、业务使用操作、业务的连续性、外包服务、紧急事件应急预案等各个环节的风险控制策略，作为各个 IT 部门、业务部门制定具体 IT 风险控制流程和管理手册的指导方针。

4、在 IT 部门或重要的 IT 工作环节，应该配置 IT 风险管理岗位和 IT 风险管理人员，负责识别评估 IT 风险、制定风险控制流程和管理制度、检查和上报 IT 风险控制状况。5、要定期审查各个部门、各个环节的 IT 风险控制流程和管理制度，定期组织检查制度的执行情况，防止出现无控制的环节、控制失效的环节和管理制度老化的情况。6、应该对全行进行持续不断的 IT 风险教育。

检查方法、步骤:

调阅：1、信息科技风险管理大纲。2、各项 IT 风险控制策略。3、IT 风险管理部门的组织结构和 IT 风险管理人员的配置情况。4、金融机构的信息科技风险年度报告。

访谈 IT 风险管理部门负责人和 IT 风险管理工作人员,重点关注：1、了解银行 IT 风险管理框架和控制策略，检查是否存在无控制或控制薄弱环节？2、了解 IT 风险管理部门所做的工作（包括对 IT 风险制度执行情况是否有记录，有检查），了解 IT 风险管理机制是否有效？

4.6 信息科技风险审计

检查项 1 ：信息科技风险审计机制

基本要求：1、应该设立或明确负责信息科技风险审计的部门，建立信息科技风险审计制度，配备适量专业 IT 审计人员，开展信息科技风险审计。2、应该有重点、有计划地开展 IT 总体风险审计、IT 系统审阅和 IT 专项审计。3、审计报告要及时向董事会或高级管理层报告。4、在内部审计和外部审计中发现的重大风险隐患要及时向银监会及其派出机构报告。

检查方法、步骤：

调阅：1、调阅 IT 风险审计制度、专业 IT 审计人员清单。2、调阅金融机构的审计计划，审计工作清单、审计报告。

访谈 IT 审计的负责人和 IT 审计工作人员，重点关注：1、是否有 IT 审计部门和专职的 IT 审计人员。2、是否有 IT 审计制度，IT 审计工作的开展情况。3、IT 审计报告是否向董事会和高级管理层报告？董事会和高级管理层对IT审计出来的问题决定采取什么整改措施？这些整改措施的进展落实情况。4、了解 IT 审计部门和审计报告对银行 IT 组织机构、IT 工作流程、IT 项目开发、IT 系统运行环节、银行总体 IT 风险的评价，从中发现和查找问题。5、询问 IT 审计工作中遇到的困难，了解第三道防线的有效性。

4.7 知识产权保护

检查项 1 ：知识产权制度

基本要求：1、银行业金融机构应该按照有关的知识产权法律，制订知识产权保护策略和程序，并且使得所有员工充分理解并遵照执行。2、应该建立相关制度来规范合法软件的购买和使用，禁止使用盗版软件，并且保护银行自身开发的信息科技产品的知识产权。

检查方法、步骤：1、调阅银行相关遵守知识产权法律的制度；2、查阅银行的软件清单，检查是否拥有产权或授权。3、抽查在有关外包服务协议和类似相关文件中是否有知识产权的保护条款。

4.8 信息披露

检查项 1 ：信息披露

基本要求：

银行业金融机构应该依据有关法律法规的要求，按照银监会规定的格式和时间，及时规范地披露信息科技风险评估结果和其他信息。

检查方法、步骤：1、调阅银行相关披露信息科技风险评估结果的制度。2、查阅银行披

露信息科技风险评估结果的记录。 3、**重点**关注，信息披露是否符合有关法律法规、是否按照银监会规定的格式和时间，及时规范地发布。

5. 连续性管理

信息系统业务连续性的现场检查主要包括银行业金融机构信息系统连续性管理的完备性；制定、管理、执行的组织架构、工作人员管理的健全性；信息系统连续性计划制定的完善性；信息系统连续性计划测试、更新的管理；对相关业务人员的培训；对信息系统连续性计划的审计以及管理工作的合规性等方面。

银行业金融机构应充分研究自身信息系统潜在的危机和相关影响，考虑由于内部或外部资源故障、信息丢失或遭到破坏和外部事件（如战争、地震和台风等）等意外事件，导致信息系统连续性遭到中断的可能性及其影响，高度重视和加强信息系统连续性管理，提高信息系统的风险防范与抗打击能力，有效地响应非计划的业务破坏事件并降低不良影响。

银行业金融机构应建立自身信息系统连续性管理的责任架构和日常管理制度，提高自身的风险防范能力，以降低突发灾难的破坏并降低不良影响。银行业金融机构应根据其业务的性质、规模和复杂性进行妥善规划，以确保在出现无法预见的干扰时，该机构仍能持续运行，应定期对这些计划进行更新和测试，以确保其有效性。

5.1 信息系统连续性组织

检查项 1：系统连续性管理组织

基本要求：1、银行业金融机构应综合考虑其业务和系统规模，建立信息系统连续性管理组织机构，负责本机构信息系统连续性管理工作。2、银行业金融机构信息系统连续性管理组织机构应包含但不限于董事会、高级管理层、信息系统风险管理部门、业务牵头管理部门、信息系统管理部门。

检查方法、步骤：1、调阅银行业金融机构信息系统连续性管理相关规章制度、文件以及人员名单，检查其是否制定了信息系统连续性管理组织及明确其职责。2、与信息系统连续性

管理组织相关人员进行座谈，包括银行业金融机构董事会、高级管理层、信息系统风险管理部门、业务牵头管理部门、信息系统管理部门人员，询问系统连续性管理情况，对相关规章制度、文件的内容进行证实，检查其对自身职责是否明确了解。

检查项 2：系统连续性管理组织职责

基本要求：1、董事会和高级管理层应领导监督本机构信息系统连续性管理体系建设，审核表决信息系统连续性管理重大决策和指导意见，审核批准信息系统连续性管理策略和计划，保障信息系统连续性管理所需资源，批准和组织信息系统连续性计划的测试和演练，定期听取信息系统风险状况分析、重大信息系统突发事件、现有信息系统连续性管理战略和政策重大修改或特例事项等的汇报等。2、信息系统风险管理部门应根据董事会和高级管理层审定的信息系统连续性管理战略、政策、基本管理制度和信息系统连续性管理相关决定等，统一组织、协调、指导、检查本机构信息系统连续性管理工作，定期分析总结信息系统风险状况，对信息系统连续性管理工作进行审计评估，履行向董事会和高级管理层的报告职责，经董事会和高级管理层授权后履行向银监会信息系统风险监管部门的报告职责等。3、业务牵头管理部门和信息系统管理部门负责本机构信息系统连续性管理工作的具体落实，制定信息系统突发事件业务和技术层面的预防措施、预警标准和信息系统连续性管理策略，做好信息系统营运监测和维护，实施信息系统连续性管理处置，评估总结信息系统突发事件及信息系统连续性管理中暴露的问题，完成症结问题的整改，履行向信息系统风险管理部门的报告职责，定期开展信息系统连续性演练，持续改进本机构信息系统连续性管理计划等。4、系统连续性管理组织应统一规划信息系统连续性的组织形式，统一规范信息系统连续性的管理制度，当发生业务连续性风险时，统一指挥、协调有关部门展开业务连续性的恢复。

检查方法、步骤：1、调阅银行业金融机构信息系统连续性管理相关规章制度、文件，检查其是否明确制定了其组织职责，分析职责制定是否合理、完整。2、调阅信息系统连续性管理组织相关会议纪要、领导讲话等资料，检查其是否展开信息系统连续性管理工作。3、与信息系统连续性管理组织相关人员进行座谈，包括银行业金融机构董事会、高级管理层、信息系统风险管理部门、业务牵头管理部门、信息系统管理部门人员，询问系统连续性管理情况，

对相关规章制度、文件的内容进行证实，检查其对自身职责是否明确了解。

检查项 3：系统连续性计划编制、维护

基本要求：1、银行业金融机构应明确负责编制和维护信息系统连续性计划相关人员。2、成员应能充分代表各个关键业务部门及相关的支持部门。3、系统连续性计划编制、维护人员应包含但不限于信息系统风险管理部门、主要业务部门、信息系统科技部门、支持保障部门。

检查方法、步骤：1、调阅银行业金融机构信息系统连续性计划编制、维护相关规章制度规定以及人员名单，检查其建立健全情况。2、与系统连续性计划编制、维护相关人员进行座谈，对相关规章制度、文件的内容进行证实，检查其对自身职责是否明确了解。

检查项 4：系统连续性计划编制、维护职责

基本要求：负责编制和维护信息系统连续性计划的人员职责应包括:1、识别关键业务和/或产品；2、识别可能发生的灾难事件；3、审阅业务影响分析的标准；4、评估风险及测算对业务的影响；5、统筹落实部门级别的危机管理制度及流程；6、更新业务恢复计划；7、更新业务持续计划的演练方案；8、对员工进行业务持续计划的培训。

检查方法、步骤：1、调阅银行业金融机构信息系统连续性计划编制、维护组织相关规章制度、文件，检查其是否明确制定了其职责，分析职责制定是否合理、完整。2、与信息系统连续性计划编制、维护相关人员进行座谈，询问系统连续性计划编制、维护情况，对相关规章制度、文件的内容进行证实，检查其对自身职责是否明确了解。

检查项 5：系统连续性计划执行组织

基本要求：1、银行业金融机构应组建信息系统连续性计划执行团队，在发生信息系统突发事件时，相关职能部门联动，统一指挥，各负其责，协调配合，启动和执行相应的信息系统连续性计划。2、信息系统连续性执行团队应包括但不限于信息系统连续性计划执行领导小组、专家小组、执行小组、支持保障小组。3、领导小组由董事会和高级管理层授权，负责信息系统突发事件应急处置工作，信息系统风险管理部门负责人任领导小组总指挥，信息系统

涉及相关职能部门（包括但不限于业务牵头管理部门、信息系统管理部门、系统开发部门、系统营运部门、客户部门和支持保障部门等）和一级分支机构的负责人为银行业金融机构应充分研究自身信息系统潜在的危机和相关影响，高度重视和加强信息科技信息系统连续性管理，提高信息系统的风险防范与抗打击能力，有效地响应非计划的业务破坏并降低不良影响。4、专家小组由信息系统相关业务和技术专家组成。5、执行小组由业务牵头管理部门、信息系统管理部门、信息系统开发部门、信息系统营运部门等派员组成。6、支持保障小组由客户部门和支持部门（包括但不限于法律事务部门、公共关系部门、安全保卫部门、人力资源部门、计划财务部门、资产负债管理部门、总务部门等）派员组成。

检查方法、步骤：1、调阅银行业金融机构信息系统连续性计划执行方面相关规章制度、文件以及人员名单，检查其是否制定了系统连续性计划执行组织及明确其职责，检查其建立健全情况。2、与系统连续性计划执行组织相关人员进行座谈，包括信息系统连续性计划执行领导小组、专家小组、执行小组、支持保障小组等人员，对相关规章制度、文件的内容进行证实，检查其对自身职责是否明确了解。

检查项 6：系统连续性计划执行组织职责

基本要求：信息系统连续性计划执行组织职责应包括： 1、领导小组主要职责是：（1）负责信息系统突发事件的指挥、组织协调和过程控制等；（2）明确责任报告人，授权其在突发事件处置过程中履行向银监会信息系统风险监管部门的报告职责；（3）明确新闻发布人，授权其在信息系统突发事件处置过程中统一口径对外信息发布；（4）信息系统突发事件影响重大或事态发展难以控制时，向董事会和高级管理层报告，由董事会和高级管理层决策应对措施；（5）宣布重大信息系统突发事件响应状态的降级或解除；（6）信息系统突发事件处置过程中向董事会和高级管理层报告处置进展情况，信息系统突发事件处置结束后向董事会和高级管理层报送总结报告；（7）其他信息系统突发事件处置过程中需领导和指挥的事项。2、专家小组职责是：（1）对信息系统重大突发事件的发展趋势、救治措施、处置办法、影响损失和恢复方案等进行研究和评估；（2）为董事会和高级管理层、领导小组提供科学有效的决策咨询；（3）必要时现场参加具体信息系统突发事件处置工作；（4）其他需专家小组参与解决的事项。3、执行小组职责是：（1）按照本机构信息系统专项业务和技术应急预案，实施信

息系统突发事件的问题排查、抢修和调整等具体信息系统突发事件处置工作；（2）对信息系统突发事件业务影响情况进行分析和判断；（3）收集分析信息系统突发事件处置过程中的数据信息和日志；（4）向领导小组报告信息系统突发事件处置进展情况和事态变化情况；（5）其他需执行小组参与处置的事项。4、支持保障小组职责是：（1）为执行小组应急处置提供信息系统突发事件处置过程中所需人力和物资等资源保障；（2）做好对受影响客户的解释和安抚工作，引导其做好相关应对工作；（3）做好秩序维护、安全保障、法律咨询和支援等工作；（4）其他为降低信息系统突发事件负面影响或损失提供的支持保障等。

检查方法、步骤：1、调阅银行业金融机构信息系统连续性计划执行组织相关规章制度、文件，检查其是否明确制定了其职责，分析职责制定是否合理、完整。2、调阅信息系统连续性计划组织相关会议纪要等资料，检查其工作开展情况。3、与信息系统连续性计划执行组织相关人员进行座谈，包括信息系统连续性计划执行领导小组、专家小组、执行小组、支持保障小组等人员，询问系统连续性计划执行情况，对相关规章制度、文件的内容进行证实，检查其对自身职责是否明确了解。

检查项 7：人员变动管理

基本要求：1、银行业金融机构信息科技部门应当制定信息科技连续性管理的岗位人员的流动、流失的应对措施,加强关键流程的后备人员培养，防范因人员变动造成岗位连续性问题。

检查方法、步骤：1、调阅信息系统连续性管理中有关人员流动管理的规章制度，检查其是否制定人员流动应对措施及岗位连续性建设。2、调阅相关培训或以往人员流动应对措施记录，检查其工作开展情况。3、与信息系统连续性管理的岗位人员、后备人员进行座谈，了解人员流动管理情况，检查其是否能有效的防范因人员变动造成岗位连续性问题。

5.2 信息系统连续性计划

检查项 1：系统连续性计划

基本要求：银行业金融机构制定信息系统连续性计划应包括但不限于以下方面：1、银行业金融机构应在该机构统一的业务连续性计划框架下制定信息系统连续性计划。2、银行业金

融机构应制定明确的信息系统连续性控制的总体目标及风险的底线。3、银行业金融机构应规定在统一的信息系统连续性计划框架下制定不同事件的信息系统连续性计划。4、信息系统连续性计划应涵盖所有业务部门的重要应用系统。5、信息系统连续性计划应明确启动信息系统连续性计划的条件，信息系统连续性管理处理流程，降低短期、中期和长期中断所造成影响的措施，系统恢复流程，事后教育和培训等内容。6、银行业金融机构应对信息系统连续性计划进行业务影响分析。（1）银行业金融机构制定信息系统连续性计划,必须基于业务影响分析的结果, 确定考虑了不可控的和非特定的灾难事件对银行业金融机构业务流程的潜在影响。潜在的灾难事件至少应包括:环境灾难；有组织的、或蓄意的破坏；公共设施服务中断；设备或系统故障；严重的信息安全事件；其他紧急事态。（2）针对潜在的高风险或中等风险的灾难事件，银行业金融机构应采取必要的危机应对和业务恢复措施，使中断的关键业务或服务在设定的恢复时间目标内，恢复到可接受的水平。7、银行业金融机构应根据业务影响分析规定业务运行恢复的优先顺序，制定合理的业务恢复策略。8、信息系统连续性计划应规定在限定时间内恢复核心业务的运行；根据业务部门的需求制订恢复点目标(RPO)和恢复时间目标(RTO)。9、信息系统连续性计划至少应强调以下事项：关键计算机处理的地点；关键业务处理的应用系统与用户要求；关键业务处理的终端用户的活动；电信和网络；关键的数据库、信息仓库(information warehouses)等；人力资源；员工及其他人员的安全。10、应建立健全突发事件应急管理体系和重要业务的灾难恢复策略。(详见突发事件应急管理、灾难恢复策略）11、应确定银行业金融机构在最差情况下持续营业需要提供的最低服务标准。12、应制定银行业金融机构在使用海外机构支持的情况下，解决法律和合规问题的方案。13、应制定遇长时间中断情况时，关键人员的岗位后备安排。14、应规定从人力、设备、技术和财务等方面确保信息系统连续性计划的执行有足够的资源保障。15、应采用清晰的结构，对资源进行清楚的描述，工作内容和步骤应具体，每项工作应有明确的责任人。16、应规定建立与相关管理部门、新闻媒体、设备及服务提供商、电信和电力部门等通畅联络渠道，确保在灾难发生时能及时通报准确情况和获得适当支持。17、银行业金融机构应关注供应商、外包商本身是否拥有业务连续性，对关键服务供应商、外包商对突发状况的应对能力进行评估。

检查方法、步骤：1、调阅银行业金融业务连续性计划，检查其是否包括信息系统业务连

续性计划。2、调阅银行业金融机构信息系统连续性计划，查看其内容、要点是否具备以上相关基本要求。3、调阅信息系统连续性计划业务影响分析报告，检查其分析是否全面、合理，符合要求。4、调阅突发事件应急管理预案和灾难恢复策略，检查其制定是否合理、完善。（详见突发事件应急管理、灾难恢复策略）5、与信息系统连续性计划负责人、相关工作人员进行座谈。询问是否制定不同事件的信息系统连续性计划，是否定期对信息系统连续性计划进行测试，测试周期多长，是否对信息系统连续性计划定期进行审查并更新，目前的预案文档为第几版，了解其对信息系统连续性计划的掌握程度。6、与信息系统连续性计划负责人、相关工作人员进行座谈，询问是否具备应急设备并能正常工作，信息系统连续性计划执行所需资金是否做过预算并能够落实。

检查项 2：测试及持续更新

基本要求：1、银行业金融机构应规定定期对信息系统连续性计划进行测试。2、应根据不同的应急恢复内容，确定合理的测试的周期，保证信息系统连续性计划在特殊情况下能有效的发挥作用。3、测试前应预先制订测试计划，测试内容应包含基本单元测试、关联测试和整体测试。4、测试的整个过程应有详细的记录，并形成测试报告。5、测试结果和报告应由董事会和高级管理层、信息科技风险管理部门、内部信息科技审计师、信息管理委员会签字确认，以确定有关的信息系统连续性计划的适用性。6、应根据测试的记录和报告，对信息系统连续性计划进一步完善。7、应规定定期评估、审查信息系统连续性计划，以确保信息系统连续性计划的有效性。8、应规定随着信息系统的变更定期对原有的信息系统连续性计划重新评估，修订完善，并按照执行。

检查方法、步骤：1、调阅信息系统连续性计划测试记录和更新记录，检查与相关支持部门的联系方式和记录，测试联系渠道是否保持畅通；检查业务流程、信息系统、人员变更是否在信息系统连续性计划中及时反映和修订。2、调阅检查信息系统连续性计划测试、更新记录，检查其在测试、演练和灾难发生后实际执行时，其过程均是否有详细的记录，是否有对测试、演练和执行的效果进行评估，是否对信息系统连续性计划进行相应的修订。3、调阅检查信息系统连续性计划测试记录，检查信息系统连续性计划是否定期测试、评审和修订；检查信息系统连续性计划的修订和年度测试结果是否经过董事会和高级管理层、信息科技风险

管理部门、内审部门、信息管理委员会的审核签字。

检查项 3：信息系统连续性计划管理

基本要求：1、信息系统连续性计划应统一编号，由专人负责保存与分发，要确保至少有二份以上的完整拷贝异地保存。2、每次修订后的新版本计划应及时按类分发给参与信息系统连续性工作的相关人员。3、原分发的旧版本除档案管理规定要求保留的，其他均应及时收回销毁。

检查方法、步骤：1、调阅有关信息系统连续性计划管理的规章制度，检查是否对其管理做出相关规定。2、调阅信息系统连续性计划，检查其是否符合保管要求。3、调阅相关登记簿，与工作人员座谈，检查是否在每次修订后所有拷贝统一更新；原分发的旧版本方案是否销毁。4、与有关工作人员座谈，询问信息系统连续性计划管理情况，包括是否由专人负责保存与分发；是否有拷贝在不同的地点保存。5、与有关工作人员座谈，询问信息系统连续性计划是否分发给参与信息系统连续性工作的所有人员。

检查项 4：系统连续性计划培训

基本要求：1、银行业金融机构应对相关工作人员进行信息系统连续性计划的培训。2、应对培训的情况和结果进行记录并归档保存。

检查方法、步骤：1、调阅信息系统连续行计划培训资料、培训指南、培训讲义等相关资料，检查是否开展了培训。2、与负责培训人员、信息系统连续性计划负责人、相关工作人员进行座谈，询问信息系统连续性计划培训情况，比如是否对系统相关人员进行信息系统连续性计划培训，培训内容，培训频率等。

检查项 5：系统连续性计划审计

基本要求：1、银行业金融机构应聘请具备信息系统风险审计资质的外部审计部门对信息系统连续性计划按有关规定进行审计，并报银监会信息系统风险监管部门备案。2、银行业金融机构内审部门对信息系统连续性计划风险、筹备所需资源、详细任务及时间表、监督和管理规划活动、跟踪和报告应进行审计。3、银行业金融机构每年应至少组织一次信息系统连续

性计划全面评审。

检查方法、步骤：1、调阅银行业金融机构有关审计的规章制度、计划等资料，检查其是否制定系统连续行计划的审计计划，分析其制定的内容是否合理。2、调阅有关信息系统连续性计划内部、外部审计报告，检查银行业金融机构对信息系统连续性计划的审计是否合规，审计频率是否合乎标准尤其关注外部审计部门是否具备审计资质。3、调阅有关信息系统连续性计划的审计整改报告，检查其整改措施是否合理、有效、及时。4、与内审人员、信息系统连续性计划有关工作人员进行座谈,具体检查其对信息系统连续性计划审计工作的开展情况。

6. 应急管理

信息系统突发事件应急管理是银行业金融机构开展风险防范和风险处置工作的一项重要工作，是银行业金融机构预防信息系统突发事件发生、处置信息系统突发事件、避免和降低信息系统突发事件风险和确保业务连续性的重要保障。

6.1 应急组织

检查项 1：应急管理团队

基本要求：应建立应急管理团队，团队至少包括应急管理领导小组、应急管理执行小组和应急管理保障小组。应急管理领导小组由管理层成员担任组长，并得到管理层授权实施应急管理，其成员由相关职能部门负责人组成。应急管理执行小组由相关业务部门和科技部门共同组成。应急管理保障小组由人力资源、财务、法律、公共关系、安全保卫和后勤部门组成。

检查方法、步骤：查阅有关文件或规章制度，确认是否制定相关规章制度。在银监会相关规定没有出台之前，银行业金融机构可以只设置一个突发事件应急管理小组，但在小组内至少要明确有关领导、执行和保障的岗位；银行业金融机构也可以设置多于上述要求设置的突发事件应急管理各小组数量，但至少包括负责领导、执行和保障的具体小组。在相关小组建立的前提下，要分析相关组成人员的合理性，是否能够确保突发事件应急处置工作的开展。

在查阅有关文件或规章制度的基础上，可以通过与相关人员交谈，对有关文件或规章制

度的内容进行证实，同时要注意突发事件应急管理小组成立时间，以掌握其时效性。

检查项 2：应急管理职责

基本要求：应急管理领导小组职责：指挥、协调和控制应急事件处置，指定应急事件报告责任人并授权向银监会系统报告，指定新闻发布人并授权其对外发布信息，建立应急处置预授权制度，宣布应急事件状态，向管理层报告应急处置进展和总结报告。应急管理执行小组职责：实施具体应急处置工作，对突发应急事件影响做出分析和评估，收集应急事件处置过程中的相关信息，向应急管理领导小组报告应急事件处置情况和发展情况，提出应急预案修订意见。应急管理保障小组职责：提供做好应急管理的人力物力保障，做好对外宣传工作，做好秩序维护、安全保障、法律咨询和其他支援工作。

检查方法、步骤：查阅有关文件或规章制度，看有没有相关的规定。重点关注职责划分是否清晰，是否将突发事件应急管理各个环节都考虑在内。进一步可以通过抽查访谈有关成员，确认是否明确其应急管理职责。

检查项 3：应急管理制度

基本要求：应该建立一套有效的应急管理制度，明确相关职责，对应急管理、应急准备、应急处置、应急保障，以及有关奖惩措施等做出明确规定。

检查方法、步骤：查阅有关文件或规章制度，检查是否制订相关的规章制度，也可以与相关工作人员交谈，求证是否建立有关规定。如已建立相关规定，则应关注相关规章制度内容，分析其合理性。

6.2 应急预案

检查项 1：应急预案制订

基本要求：各银行业金融机构应根据业务要求，制订总体应急预案和分类应急预案，分类应急预案至少包括基础设施、网络通讯、信息系统和业务流程等。

检查方法、步骤：查阅相关资料，了解银行业金融机构是否制订总体应急预案和 IT 应急

预案，二者是否衔接一致。IT 应急预案的每个分项是否涵盖关键基础设施、网络通讯、信息系统和业务流程等内容，预案是否科学、合理。应急预案是否得到了管理层的审核和批准。

检查项 2：应急预案内容

基本要求：应急预案应包含内容：1、明确有关各方的分工和责任；2、说明重要信息系统的业务影响范围、恢复时间目标、恢复点目标、以及信息系统包括的系统资源，明确资源的物理位置、设备型号、软件资源、网络配置等关键信息；3、明确各类故障的诊断方法和流程；应急场景应至少覆盖电力故障、通信线路故障、火情水灾、治安、病毒爆发、网络攻击、人为破坏、不可抗力、计算机硬件故障、网络操作系统故障、漏洞、应用系统故障以及其他各类与信息系统相关的故障；4、制定系统恢复流程和应急处置操作手册，应尽可能将操作代码化、自动化，降低应急处置过程中产生的操作风险；5、明确应急恢复过程中的关键状态，并明确不同状态的沟通和报告内容及等级；6、明确应急相关人员的协调内容和沟通方式；7、明确系统重建步骤，确保信息系统恢复正常业务处理能力。

检查方法、步骤：查阅相关资料，走访相关人员，确定应急预案是否建立，是否清楚考虑每一个可能出现问题的环节，对不可预见事件考虑是否周全，IT 应急预案与业务整体应急预案内容的衔接性，应急预案对突发事件的定级是否清楚，应急预案关于应急流程的描述是否简单清晰，对 RTO 和 RPO 的描述是否清晰和准确。

一般突发事件分三个等级：

1、特别重大突发事件(1 级)。（1）单家银行业金融机构在主要业务服务时段，导致 50%(含)以上的客户无法办理业务的信息系统突发事件；（2）两家(含)以上银行业金融机构同时发生Ⅱ级信息系统突发事件。

2、重大突发事件(Ⅱ级)。（1）单家银行业金融机构在主要业务服务时段，导致 10%(含)以上、50%以下的客户无法办理业务的信息系统突发事件；（2）单家银行业金融机构在主要业务服务时段，导致 3%(含)以上、10%以下的客户在 30 分钟(含)以上无法办理业务的信息系统突发事件。

3、较大突发事件(Ⅲ级)。单家银行业金融机构在主要业务服务时段，导致 3%(含)以上、

10％以下的客户在 30 分钟以内无法办理业务的信息系统突发事件。

检查项 3：应急预案更新

基本要求：银行业金融机构应对应急预案进行测试和演练，并根据测试和演练情况对应急预案进行修订，当信息系统发生软件升级、系统补丁安装、配置参数调整、网络改造等变更时应及时更新应急预案，并适时实施演练。

检查方法、步骤：查阅相关资料，约谈相关人员，确认是否具备应急预案更新机制，更新频率是否满足实际需要，过程是否合理，是否根据应急演练进行了更新，是否根据业务发展变化、系统变化进行了应急预案的更新。

检查项 4：外包服务应急

基本要求：银行业金融机构应将支撑信息系统运行的重要外包服务的应急管理纳入预案范围，建立重要外包服务的专项应急预案，对于重要基础设施、重要设备、网络、系统集成以及其他外包服务商的技术与产品政策、服务水平、服务能力制定风险应对措施，外包服务的应急预案应能够保障银行业信息系统恢复时间目标和恢复点目标的要求。

检查方法、步骤：查阅有关资料，约谈相关人员，检查：1、应急预案中是否充分考虑了外包服务应急的问题，是否明确了外包供应商的职责；2、外包服务协议是否包含了应急响应的条款；3、是否对应急管理外包服务商进行评估；4、是否定期对服务外包商进行定期考核。

检查项 5：应急培训

基本要求：应专门组织对技术人员和业务人员进行应急预案有关培训，以达到明确应急预案内容，清楚角色职责的目的。

检查方法、步骤：是否建立培训机制，培训程度是否确保相关人员明确应急预案内容，清楚其角色职责。

6.3 应急演练

检查项 1：应急演练前

基本要求：银行业金融机构应制订应急演练计划，明确应急演练时间、内容、依据、目的、负责人和相关部门，演练对应应急预案进行，要验证应急预案各个环节是否有效，应急资源是否完备，应急人员是否胜任，应急演练是否包括全面演练和专项演练，全面演练至少每年进行一次。

检查方法、步骤：调阅相关资料及演练报告确认是否建立总体应急演练计划和 IT 应急演练计划，分析应急演练是否全面、合理，任务是否明确清晰，全面应急演练和专项演练是否满足需求。

检查项 2：应急演练过程

基本要求：银行业金融机构应严格按照应急演练计划实施应急演练，并确保做到：1、以应急预案为基础，制定应急演练总体方案，并进行风险再评估，制定相应的保障措施；2、应急演练内容应全面完整，涵盖信息系统的各类应急场景；3、严格控制应急演练引起的信息系统变更风险，避免因演练导致服务中断；4、应急演练应选择在非主要业务时段进行；5、应急演练完成后，应保证实施应急预案所需的各项资源恢复正常；6、定期对应急演练相关人员进行培训。

检查方法、步骤：查阅有关应急演练过程记录和应急演练报告，并约谈相关人员，确认：1、应急演练是否能够按照一定的时间间隔进行，是否严格按照应急预案进行；2、应急演练过程是否真实，是否达到演练目的；3、应急演练保障措施是否得到很好执行，时间段选择是否合理；4、应急演练培训工作落实情况。

检查项 3：应急演练后

基本要求：应急演练结束后，银行业金融机构应撰写应急演练总结报告，大型或重要的应急演练总结报告应提交管理层。总结报告包括但不限于：内容和目的、总体方案、参与人员、准备工作、主要过程和关键时间点记录、存在的问题、后续改进措施及实施计划、演练

结论。根据演练总结报告提出改进措施进行整改，并及时修订相应的应急预案。组织审计部门对整改情况进行监督和检查。根据审计要求以及监管部门检查要求，将应急演练计划、过程记录和结果分析等归档留存。

检查方法、步骤：调阅应急演练报告和应急演练记录资料，约谈相关工作人员，确认：1、应急演练过程记录详细、真实；2、应急演练报告内容全面、客观，有过程描述、问题分析和改进建议等内容；3、演练报告是否及时报告管理层并得到了管理层的认可；4、根据应急演练情况及时对应急演练方案进行了修改，并整理归档。

6.4 应急响应

检查项 1：应急响应流程

基本要求：1、突发事件发生后，应急执行小组应根据既定的应急预案，启动授权的应急操作，并及时报告应急领导小组。应急处置应集中于建立临时业务处理能力、修复原系统损害、在原系统或新设施中恢复运行业务能力等应急措施；2、对于应急预案没有覆盖的突发事件，应立即报告应急领导小组进行应急决策；3、应急领导小组应立即启动本机构应急组织，组织协调机构内部进行应急处置，并负责向监管部门报告应急响应情况；4、支持保障小组做好各项应急保障工作，为应急处置提供场地、交通、通讯及其他后勤保障。

检查方法、步骤：关注银行业金融机构是否按照挽救生命、控制受损程度、对外界及时发布信息、启动应急响应预案原则处理问题，评估其应急响应流程，应急响应流程一般包括：宣布应急事件的发生，启动应急响应流程，联系相关人员（员工、危机处理专家等），执行评估和抢救生命，控制所受损失，对外界及时发布信息，评估损失以索赔，调查根本原因并采取预防措施。查阅银行应急流程是否包含了上述步骤，其中控制所受损失部分的进一步细分步骤是否科学也作为重点予以关注。

检查项 2：全程记录处置过程

基本要求：应急处置中所有相关的信息和处理过程都要进行严格记录，外部供应商的处理过程应有专门的记录文件，如果设计保险理赔，中间过程和场景可用相机和录像机进行记录。所有相关资料都应有专人存档保管。

检查方法、步骤：查阅应急处理记录，查看应急流程是否被得到很好的执行以及流程是否合理，重点关注应急预案失效时的处理流程。

检查项 3：应急事件报告

基本要求：突发事件发生后，应急领导小组应根据事件严重程度，及时将情况报告管理层，必要时报告监管部门。报告内容应包括突发事件时间、地点、现象、影响范围、原因分析、后果初步判断、已采取的措施、后续拟采取的措施建议、报告单位、报告人以及其他与事件有关的内容。

检查方法、步骤：查阅相关资料，确认是否建立应急事件报告制度，关注相关事件是否报告了管理层和监管部门，关注对事件严重程度划分依据是否合理。

检查项 4：与第三方沟通

基本要求：突发事件发生后，银行业金融机构应将相关信息及时通报给受到影响的外部机构以及重要客户，并将相关信息准确通报给相关设备及服务提供商、电信、电力等外部组织，以获得适当的应急响应支持。

检查方法、步骤：是否具备第三方沟通清单及联系方式，是否指定联系人员，何种情况下与何机构何人联系是否清晰。

检查项 5 ：向新闻媒体通报制度

基本要求：根据突发事件严重程度，应急领导小组应及时向新闻媒体发布相关信息，信息发布严格按照行业、机构相关规定和要求进行，机构内其他部门和个人不得随意接受新闻媒体采访或对外发表个人看法。

检查方法、步骤：查阅突发事件应急管理制度，了解是否有关于向新闻媒体通报相关规定，查阅有关新闻稿，分析是否按照有关新闻通报制度规定操作。

检查项 6：应急处置总结

基本要求：应急终止后，应针对应急工作进行评估和总结，总结报告应包括信息系统突发事件评估、处置工作总结以及症结分析和相应建议等内容。突发事件评估应包括现象、影响范围、处理时间和过程以及造成的损失；处置工作总结应评价应急预案的可用性，分析处置工作中存在的问题，总结处置工作的整体过程；症结分析和相应建议应分析突发事件的深层次原因，明确存在的困难和问题，提出改进措施、计划及相关建议。

检查方法、步骤：查阅评估报告和建议书，确认是否进行了应急处置总结，进一步分析总计是否深刻，建议是否合理，相关建议是否得到了改进。

6.5 应急保障

检查项 1：人员保障

基本要求：应急人员具备必要的资质，并定期组织应急培训；确保重要岗位建立主、备角色机制，并能够定期互换。

检查方法、步骤：查阅应急人员清单和联系方式，确认应急人员是否真实存在。查阅有关培训资料，包括培训指南、培训讲义等确认是否进行了培训，约谈相关人员，通过提问方式了解培训工作是否到位。

检查项 2：物质保障

基本要求：确保应急处置不会因为物资保障问题而中断。应储备一定数量的应急设备和应急物资，保证物资供应渠道畅通。应建立应急响应专项资金审批制度，保证急需物资的采购。

检查方法、步骤：查阅保障物资清单，并抽查核实主要保障物资的真实性，了解供应渠道是否畅通，存放位置是否合理，性能是否良好。了解银行对应急物资是否有定期的检查盘点机制。调阅应急专项资金审批制度，分析是否能够满足应急工作需要。

检查项 3：技术保障

基本要求：确保应急处置不会因为技术问题而导致应急响应中断或延长应急处置时间。建立预警平台确保应急事件及时被发现并及时传达相关人员。掌握第三方技术水平并保证第三方能够提供及时有效的技术保障。

检查方法、步骤：调阅应急预案有关资料，了解每一个环节对技术的要求，并据此了解负责次环节工作人员背景，分析其有没有相应的技术水平和能力，同时关注 B 角人员的技术水平，了解银行对技术人员的绩效考核机制；对需要第三方技术支持的环节要重点关注，同时关注其实际可用性，是否与其签订有关保障协议。

检查项 4：沟通保障

基本要求：应该有明确的应急管理各部门、各岗位的联系方式和联系电话，尤其是第三方联系方式和联系电话，并做到及时更新，联系方式不能单一，要有多种渠道。

检查方法、步骤：询问有关人员是否有应急管理相关人员联系方式一览表，如有，参照应急管理相关规定，分析是否全面，是否考虑了第二种联系方式，重点要关注第三方单位、人员联系方式是否包含在内。必要时根据联系方式一览表，抽查部分人员的联系方式，验证是否畅通。

6.6 持续改进

检查项 1：应急事件评估、改进

基本要求：银行金融机构应每年至少对各种突发事件进行一次评估，评估内容包括：风险识别、措施的有效性、预案的完备性、演练的完备性和及时性等。

检查方法、步骤：询问有关人员是否开展了应急事件评估和持续改进工作，查阅有关底稿或会议记录，对比前后风险预案的变化是否有改进。

检查项 2：应急响应评估

基本要求：每年至少开展一次对应急响应工作的全面评估和审计，评估重点包括：响应的有效性，资源的充分性，报告的及时性。

检查方法、步骤：询问有关工作人员，求证是否进行有关应急响应评估，查阅资料求证是否针对年度应急演练或出现的突发事件应急响应进行过评估，评估是否细致、到位。

检查项 3：应急管理评估

基本要求：根据发展情况和实际应急管理的经验，至少每年对应急管理策略、机制、方法和流程进行持续改进。

检查方法、步骤：询问相关人员，查阅有关底稿或会议记录（纪要），求证是否对本单位应急管理工作进行整体评估，并提出改进措施，重点关注信息技术应急管理评估是否到位。

检查项 4：纳入全面风险管理机制

基本要求：董事会和高管层将应急管理纳入全面风险防范工作当中，建立长效机制，保证应急管理持续性和有效性

检查方法、步骤：查阅有关全面风险管理制度中是否有应急管理内容，并求证是否落实。

7. 信息系统安全管理

保证信息系统的安全是银行业金融机构的一项重要任务，银行业金融机构应成立信息系统安全的内部组织保障部门，应重视对信息系统安全的管理，采取足够的措施，保护信息系统安全。用管理和制度手段，保证客户资料、交易信息以及金融机构各种信息的安全，防止以上重要信息被窃取、非法复制、泄露和丢失。该项检查内容包括组织建设、内部管理、制度建设和执行。

7.1 安全管理组织

检查项 1：管理目标

基本要求：信息系统安全管理部门应依据信息系统安全管理战略目标制定信息系统安全管理规定，安全管理规定应涉及安全计划、身份管理、用户管理、风险评估、信息资产管理、网络安全、病毒防护、敏感数据交换等内容；管理规定应达到银监会提出的按银行规模、按风险等分类监管的要求。

检查方法、步骤：1、调阅银行文件，查看是否制定信息系统安全管理规定。2、对制定的信息系统安全规定进行核实，是否涉及上述几方面。3、调阅信息系统安全管理规定，对规定的各方面是否明确、是否具有相应的实施要求和细则。4、调阅信息系统安全管理部门的管理规定，看是否符合银监会提出的按银行规模、按风险等分类监管的要求。

检查项 2：人员风险

基本要求：信息科技的岗位设置应合理；信息科技人员应无不良记录；信息科技人员的专业知识和业务水平应达到本行要求；应对正式信息科技人员、临时聘用或合同制信息科技人员及顾问采取不同的管理措施；应对信息科技人员权限进行分级管理，关键岗位应有 AB 角；应配备专职安全管理员，关键区域或部位的安全管理员应符合机要人员管理要求，对涉密人员应签订保密协议；信息科技人员薪酬应该合理；信息科技人员管理要全面，应包括背景调查、人员招聘、上岗培训、安全培训、人员离岗审查、强制休假等方面。

检查方法、步骤：1、调阅银行人事制度，了解银行的信息科技岗位设置情况，是否配备了专门的安全管理岗位或部门。2、与信息科技管理人员和普通员工进行座谈，听取其对信息科技岗位设置的意见，看岗位设置是否合理。3、调阅银行人事档案，查看是否建立了信息科技人员的绩效考核制度，查看信息科技人员是否有不良记录。4、调阅银行人事档案和与信息科技从业人员进行座谈，了解信息科技人员的专业知识和业务水平，看是否达到人事要求。5、调阅银行人事管理制度或部门人事管理制度，看是否有针对正式信息科技人员、临时聘用或合同制信息科技人员及顾问制定不同的人事管理制度。6、调阅信息系统安全管理的相关制度，

看是否对不同信息科技岗位进行了权限划分和分级管理，并能贯彻落实上述制度和要求。7、调阅银行人事档案和与信息科技人员座谈，看信息科技从业人员的薪酬是否合理。

7.2 安全管理制度

检查项 1：规章制度

基本要求：银行应对信息系统安全风险进行分析、评估；应对信息安全管理工作建立相应的管理制度；应要求管理人员或操作人员严格执行管理制度，各项操作符合制度要求；有密级的安全管理制度，应注明安全管理制度密级程度，并进行密级管理；信息系统安全制度建设应与信息系统安全风险相结合；信息系统安全制度建设应全面涵盖信息系统安全的风险点，如：策略、制度、机房、软件、硬件、网络、数据、文档等方面；信息系统安全制度应包含违规处罚条款；信息系统安全制度应经过内外审计部门审计评估，相关制度依据审计报告进行了修改；重要工作和岗位应单独制订详尽的管理办法和工作职责；信息系统安全制度中应包括对外包商、服务商的职责和义务要求；信息系统安全事件报告制度和处理流程应清晰和明确；信息安全管理制度应注明发布范围，有发文编号和相关部门的收文记录；信息系统安全制度应能及时发布和修订。

检查方法、步骤：1、调阅银行信息系统安全方面的会议记录，看是否对安全风险进行过分析、评估。2、调阅信息系统安全相关的制度，看是否围绕着风险分析、评估报告开展制度建设，各项制度能否有效规避风险。3、调阅信息系统安全制度，看已有制度是否涵盖信息系统安全的各项风险点，如：策略、制度、机房、软件、硬件、网络、数据、文档等方面。4、调阅内、外审计资料，看是否对信息系统安全制度建设进行过审查。5、调阅信息系统安全制度，看是否包含违规的处罚条款。6、调阅信息系统安全管理部门职责和工作计划，看是否对重要的信息系统安全管理岗位制定了单独的管理办法和工作职责。7、调阅信息系统安全制度，看已有信息系统安全制度中是否包括针对外包商、服务商的管理要求，或者职责和义务。8、调阅信息系统安全制度，看是否建立信息系统安全事件报告制度和处理流程，制度和流程是否清晰和明确。9、调阅信息系统安全制度和与信息系统安全管理部门负责人座谈，了解近期

信息系统安全方面的重大（管理、安全、人事等方面）事件，查明是否已经针对上述事件对信息系统安全制度进行了及时修订和颁布实施。

检查项 2：制度合规

基本要求：信息系统安全制度应符合国家有关信息科技管理的法律法规；应符合国家有关信息科技管理的技术标准；应符合银监会有关办法要求；应按照《信息系统安全等级保护实施指南》要求，对信息系统进行分级保护；对于拥有境外机构的银行，其制度也应符合境外监管机构的要求。

检查方法、步骤：1、调阅信息系统安全制度和与信息系统安全管理部门负责人座谈，审查制度编写参照文件是否违反国家有关信息科技管理的法律法规。2、对技术性比较强的信息系统安全制度，查明其是否低于国家相关标准规定。3、调阅信息系统安全制度，审查制度是否与银监会相关办法、要求相冲突。4、与信息系统安全管理负责人座谈，看其是否了解《信息系统安全等级保护实施指南》，是否依据《信息系统安全等级保护实施指南》对信息系统进行了分级，是否制定了相应的信息系统安全分级保护规定，分级保护规定是否落实到位。5、与信息系统安全管理负责人座谈，了解该银行是否在境外设立分支机构，境外分支机构信息系统安全制度是否符合所在国、地区监管机构的要求。

查项 3：制度执行

风险点基本包括：工作中应严格遵从信息系统安全制度规定；对违规操作的应根据相应处罚条款进行处罚；被处罚管理部门或个人是否对违规操作进行了整改；内外审计部门是否对信息系统安全制度执行情况进行过审计。

检查方法、步骤：1、调阅信息系统安全制度中涉及到的相关档案、日志和视频等记录，核对工作人员是否按照相关要求进行了操作。2、调阅银行或部门会议记录，查看银行或部门是否对日志、视频等记录中出现的违规操作行为进行过认定，并对违规人员或部门进行过处罚。3、调阅银行或部门会议记录，查看是否对违规操作进行过整改，整改的后继情况如何。对于因制度漏洞造成的风险，是否及时对相关制度进行了修改。4、调阅内、外部审计资料，

看是否有关于信息系统安全制度执行情况的审计报告。5、调阅审计文件，查看信息系统安全制度执行情况审计频度和审计内容是否符合银行要求。6、调阅银行或部门文件，看是否对审计报告进行过整改落实，后续的整改落实情况是否符合审计要求。

检查项 4：宣传和教育培训

基本要求：高管层、信息系统安全部门负责人应知晓信息系统安全制度；银行应加强对客户的信息安全风险宣传教育工作；银行应定期组织员工接受信息系统风险性和安全性教育；银行应组织员工学习基本的信息系统安全管理制度；信息科技人员应掌握所从事岗位的信息系统安全管理制度。

检查方法、步骤：1、与高管层、信息系统安全部门负责人座谈，了解是否知晓本银行的信息系统安全制度。2、与高管层座谈，了解银行是否对客户进行过信息系统安全方面的宣传教育，其内容、力度和频度如何。3、与普通员工座谈，了解是否接受过有关信息系统风险性和安全性教育。4、抽查银行内部部门的学习记录，看是否组织过信息系统安全防范知识方面的学习培训。5、与普通员工座谈，看是否知晓本银行基本的信息系统安全制度。6、调阅信息科技部门的学习记录，看是否对信息科技人员进行过信息系统安全制度的传达，是否组织过信息系统安全制度的学习培训。7、与信息科技人员座谈，看是否掌握所从事岗位的信息系统安全管理制度。

检查项 5：事件响应和处理

基本要求：信息系统安全事件报告制度和处理流程应清晰、明确和完善；信息系统安全事件报告制度和处理流程应遵从银行制定的信息系统安全制度；信息系统安全事件应进行分级管理；信息系统安全事件响应流程应定期进行演练；内外审计部门应对演练过程进行审计；对演练中存在的问题应及时进行整改；信息系统安全事件制度中应包括信息披露的相关要求，对披露对象和内容应进行明确的规定。

检查方法、步骤：1、调阅银行或信息安全管理部门文件，看是否对信息系统安全事件报告和处理流程进行过规定。2、调阅信息系统安全事件报告制度和处理流程规定，看是否对信

息系统安全管理部门和信息科技人员进行过职责划分，职责划分是否清晰。3、内外审计部门是否对信息系统安全事件报告制度和处理流程进行过审计。银行或信息系统安全管理部门是否对审计过程中发现的问题进行过整改。4、调阅信息系统安全事件报告制度和处理流程规定，看是否包括信息系统安全事件披露制度。5、调阅信息系统安全事件报告制度和处理流程规定，与信息系统安全制度比对，看是否存在互相违背的条款。6、调阅信息系统安全事件报告制度和处理流程规定，看规定中是否对信息系统安全事件进行了分类、分级，并对不同类别、级别的安全事件制定了相应的处理流程。7、与信息系统安全管理人员座谈，了解是否进行过信息系统安全事件响应流程演练，是否知晓演练内容和要求。8、调阅信息系统安全事件报告制度和处理流程规定，看信息系统安全部门组织的演练内容和流程是否涵盖核心的信息系统和流程。9、调阅信息系统安全事件报告制度和处理流程规定，看信息系统安全管理部门组织的演练内容、流程和频度是否符合信息系统安全制度的要求。10、在信息系统安全事件响应演练过程中，是否有内外审计部门参与。审计部门是否对演练过程进行过审计评估。信息系统安全管理部门是否根据审计结果进行过整改和完善。

8. 外包管理

服务外包管理检查主要针对银行业金融机构在进行信息系统外包时是否根据风险控制和实际需要，合理确定外包的原则和范围，认真分析和评估外包存在的潜在风险，建立健全有关规章制度，制定相应风险防范措施。

8.1 服务外包管理制度

检查项 1：服务外包管理制度

基本要求：1、银行业金融机构应建立服务外包管理制度、服务外包协议；2、银行业金融机构应建立服务外包管理框架，明确界定允许服务外包的内容、范围和活动；3、银行业金融机构应建立外包审查审批机制，对服务外包进行监督管理。

检查方法、步骤：1、调阅服务外包管理制度、各类服务外包协议和审查审批制度及服务

外包框架；2、与相关人员进行监管谈话，询问目前有哪些业务是通过服务外包支持的，确立服务外包的原则是什么;3、调阅服务外包商的资质认定资料。4、与相关人员进行监管谈话，了解信息科技风险管理部门、内部审计部门在审查审批流程中的职责；

检查项 2：对重要外包项目评估

基本要求：1、银行业金融机构应定期对重要项目的外包进行风险评估；2、银行业金融机构应制定服务外包相应的风险防范措施，并将其纳入总体安全策略和风险控制之中。

检查方法、步骤：调阅风险评估报告、外包风险管理资料、IT 治理安全策略及风险控制框架相关文档。

检查项 3：外包安全保密措施

基本要求：1、银行业金融机构将敏感的信息系统，以及其他涉密数据的管理与传输等内容进行外包时，应遵守国家有关法律法规，符合相关规定；2、银行业金融机构应与服务外包商签署相应安全管理保密合同。

检查方法、步骤：调阅安全管理保密合同，审查是否违背国家有关法律法规和相关规定，是否建立了对外包人员的安全管理规定。

8.2 服务外包管理风险评估

检查项 1：对服务外包商评估

基本要求：银行业金融机构应建立对服务外包商的评估机制，充分审查、评估其经营状况、财务实力、诚信历史、安全资质、技术服务能力和实际风险控制与责任承担水平。

检查方法、步骤：1、调阅银行业金融机构对服务外包商的评估管理制度;2、调阅服务外

包商的经营状况、财务实力、诚信历史、安全资质、技术服务能力和实际风险控制与责任承担水平等证明文件。

检查项 2：对服务外包商审查

基本要求：1、银行业金融机构应对服务外包商提交的服务报告进行评审；2、对于涉及银行机密数据的外包服务商，应定期对其安全管理进行检查；3、银行业金融机构应建立服务外包不足的应急管理办法。

检查方法、步骤：1、调阅银行业金融机构对服务外包商服务报告的评审报告；2、调阅银行业金融机构对于涉及银行机密数据的外包服务商，应定期对其安全管理进行检查的相关文档；3、调阅银行业金融机构针对服务外包不足建立的应急管理办法。

8.3 服务外包审批

检查项 1：服务外包审批流程

基本要求：1、银行业金融机构应制定服务外包审批制度；2、银行业金融机构对服务外包商的访问要求，应经过相应的申报和审批程序。

检查方法、步骤：1、调阅服务外包审批制度;2、调阅相关服务外包会议纪要；3、检查相关部门的审查、审批记录。

8.4 服务外包应急响应

检查项 1：服务外包应急计划

基本要求：1、银行业金融机构应建立针对服务外包的应急计划，以应对服务外包商在服务中可能出现的重大缺失，包括资源的重大损失、服务外包商的财务失败，以及外包协议的意外中止；2、银行业金融机构应对每个外包合同都制订专门的应急计划。

检查方法、步骤：1、抽样查阅服务外包管理应急计划，核实是否制定了对应每个外包合同专门的应急计划;2、与相关人员进行监管谈话，了解在制定服务外包风险应急方案时，考虑了哪些风险因素，这些风险因素对银行业务影响程度。

检查项 2：服务外包商联络机制

基本要求：1、银行业金融机构应与服务外包商建立有效的联络、沟通和信息交流机制，并制定在意外情况下能够实现服务商的顺利变更，保证服务外包不间断的应急预案；2、银行业金融机构应协调双方的应急计划、制定服务商未履约情况下银行业金融机构的应急计划。

检查方法、步骤：1、调阅服务外包管理应急计划，核实与服务外包商建立联络、沟通和信息交流机制落实情况，是否有在意外情况下能够实现服务商的顺利变更，保证服务外包不间断的应急预案；2、与相关人员进行监管谈话，了解并掌握服务外包商制订的应急计划，服务外包商制订的应急计划与本机构制订的服务外包应急计划是如何协调实施的，如果服务外包商不能履约，有否相应的应急计划。

检查项 3：服务外包应急演练

基本要求：1、银行业金融机构服务外包应急响应计划要定期组织演练；2、银行业金融机构必要时要和外包服务商进行联合演练。

检查方法、步骤：1、调阅应急计划文件和应急演练报告;2、与相关人员进行监管谈话，了解服务外包应急演练情况，对演练结果是否进行了整改。

8.5 外包合同

检查项 1：外包合同

基本要求：1、银行业金融机构应当与服务外包商签订书面合同，明确双方的权利、义务，并规定服务外包商在安全、保密、知识产权等方面的义务，外包关系受此书面合同制约；2、

银行业金融机构与服务外包商签订的合同要对服务外包合同各方的安全责任有明确的界定，应确保外包合同中参与方（包括转包商）都了解各自的安全责任。

检查方法、步骤：1、调阅银行与服务外包商签订的合同，核实合同在双方的权利、义务，安全、保密、知识产权方面有否明确的界定；2、与相关人员进行监管谈话，核实服务外包合同中有否关于双方安全责任的界定，安全责任划分的区域是否能够足以防范潜在的风险，是否让服务外包商充分了解了安全责任范围，合同审查和正式批准的流程是否存在，他们是如何遵从的。

检查项 2：服务外包商访问权限

基本要求：1、银行业金融机构与服务外包商签订的合同应包括限制授权用户对敏感业务信息访问，以及为外包出去的设备提供何种级别的物理安全保护；2、银行业金融机构与服务外包商签订的合同应包括服务外包发生风险时应采取的措施，以维护服务的可用性；3、银行业金融机构与服务外包商签订的合同应包括服务外包的期限、中止的条件和善后处理的事宜以及服务外包商应承担的责任。

检查方法、步骤：1、调阅银行与服务外包商签订的合同;2、与相关人员进行监管谈话，了解在合同中采用什么样的物理和逻辑控制对敏感的业务信息访问限制的，对外包的硬件设备制定了什么样的物理安全保护规则,了解在服务外包合同到期、中止情况下，对服务外包商需要承担的责任是如何定义的，服务外包商在发生风险时应采取哪些必要的措施是否在合同中明确界定。

检查项 3：外包服务法律风险

基本要求：1、银行业金融机构与服务外包商签订的合同要符合法律要求和监管要求；2、银行业金融机构与境外服务外包商签订服务合同要符合服务外包商所在国的法律法规和监管要求。

检查方法、步骤：与相关人员进行监管谈话，服务外包合同签署前是否经过法律部门的审核，是否已经消除了可能违法的风险，银行与境外服务外包商签订的合同是否关注到服务

外包商所在国的法律法规和监管要求。

8.6 服务外包文档的完备性

检查项 1：服务外包文档

基本要求：1、完善外包管理制度，对外包过程中产生的各类文档依据其重要程度制定保存年限，并妥善保存服务外包所产生的所有文档;2、外包管理中所产生的相关日志和记录保存时间应当满足内部和外部审计的需要。

检查方法、步骤：1、审查外包服务保存环境;2、查阅全部服务外包项目文档清单，核实服务外包文档的完备性；3、查阅服务外包管理的日志和记录文档，核实服务外包日常管理制度的遵从情况。

9. 审计监督

审计是指针对银行业金融机构信息科技的独立客观的监督和评价活动，它通过审查和评价信息科技活动及内部控制的适当性、合法性和有效性来促进组织目标的实现。

内部审计是银行业金融机构内部发起的，由内部审计部门或由外部审计机构执行的信息科技审计。

外部审计是指银监会及其派出机构必要时指定具备相应资质的审计服务供应商对银行业金融机构执行的信息科技审计或相关检查。

9.1 内部审计

检查项 1：信息科技审计制度

基本要求：1、银行业金融机构应建立内部审计制度，明确审计策略、程序和内部审计部门履行职责所必需的权限。2、内部审计工作应当独立于经营管理，以风险为导向，确保客观公正。3、专人负责组织实施内部审计规划，并对内部审计的整体质量负责。4、配备足够的资源和具有专业能力的人员独立于银行业金融机构的日常活动。 5 、内部审计部门可将内部

审计项目外包，但必须对外包机构进行资质审查。

检查方法、步骤：1、调阅审计制度和规划，审查是否明确了信息科技审计的策略、程序、方法、范围、角色、职责权限和独立性，是否建立了有效的质量控制制度并定义了对外包审计的管理要求，审计章程和委托书是否足够详细，能否表达信息科技审计功能或审计任务的目的、责任和限制。2、与相关人员进行监管谈话，了解其内部审计工作的独立性、内部审计部门职责权限、内部审计规划、内部审计项目外包、内部审计程序和方法等情况。

检查项 2：内部审计的范围、频率

基本要求：1、内部审计部门应对信息科技的安全事故进行评估。2、审计内容应包括信息科技治理、信息科技风险管理、信息安全、系统开发与维护、信息科技运行、业务连续性管理、外包管理等。3、内部审计部门应参与大规模或大范围的项目开发。4、应定期进行信息科技审计。

检查方法、步骤：1、调阅相关资料，了解是否根据信息科技环境确定适当的审计覆盖，是否进行了必要的风险评估。2、与相关人员进行监管谈话，了解确定内部审计范围和频率的依据。3、调阅审计规划，了解审计范围是否以 IT 风险控制为对象，涵盖全行 IT，包括对总行 IT 和分支机构 IT 的审计，审计内容是否包括对银行信息科技合规性的审计、对各类工作参与人资质是否合乎要求的审计、对各类信息产品的准入、对服务供应商的服务质量的审计等。4、调阅审计部门参与大规模或大范围项目开发的记录。

检查项 3：审计质量控制

基本要求：1、审计部门应获取前期审计报告中的审计发现、审计结论和意见等信息，在此基础上进行评估，并制定相应的审计方案。2、内部审计人员在实施审计前，应向被审计单位送达内部审计通知书。3、审计人员应当有针对性地收集与审计事项相关的审计证据。4、审计组应当按照审计档案管理要求收集与审计项目有关的材料，建立审计档案。5、内部审计人员应在实施必要的审计程序后，出具审计报告。6、银行业金融机构应建立完善与监管部门沟通和报告的制度。7、内部审计行为必须严格按照审计程序和审计方法实施。

检查方法、步骤：1、调阅审计计划或方案，审查审计计划或方案是否合理，是否进行了必要的风险评估，是否合理分配审计资源。2、调阅内部审计通知书。3、调阅审计工作底稿，调阅审查审计程序的执行过程及收集和评价的审计证据记录。4、调阅审计档案，审查审计过程和结果的完整性。主要包括以下内容：（1）内部审计通知书、项目审计计划、审计方案及其调整的记录。（2）审计程序执行过程和结果的记录。（3）获取的各种类型审计证据的记录。（4）其他与审计事项有关的记录。5、调阅与监管部门的沟通和报告制度,以及相关文字性材料。

检查项 4：审计结果的有效性和持续性

基本要求：1、审计报告应说明审计目的、范围，提出结论和建议，并应当包括被审计单位的反馈意见。2、银行业金融机构应确保内部审计成果得以充分利用。3、银行业金融机构应要求被审计单位在规定的期限内落实纠正措施。4、内部审计人员应进行后续审计，促进被审计单位对审计发现的问题及时采取合理、有效的纠正措施。

检查方法、步骤：1、调阅审计报告，是否以经过核实的审计证据为依据，做到客观、完整、清晰、及时、具有建设性，有无被审计单位的反馈意见，有无董事会或高管层的审批意见。2、与相关人员进行监管谈话，了解审计意见落实执行情况。3、调阅相关资料，审查被审计单位是否在规定的时间内按照审计意见要求实施整改。4、调阅相关资料，了解审计部门是否对前期审计整改要求的落实进行监督和后续审计，并评价其采取的纠正措施是否合理、有效、及时。

9.2 外部审计

检查项 1：内部审计与外部审计的协调

基本要求：1、银行业金融机构应要求审计服务供应商出示委托授权书，并拒绝委托授权书上规定的范围以外的审计。2、被审计的银行业金融机构应根据该审计报告提出整改计划，并在规定的时间内实施整改。

检查方法、步骤：1、与相关人员进行监管谈话，了解是否认真查看委托授权书并明确委托授权书上规定的审计范围，是否按授权书规定的范围配合外部审计，是否定期评价外部审计工作质量并充分利用外部审计工作成果。2、审查整改计划和报告。

10. 开发变更管理

10.1 开发管理

良好的系统开发管理是一个系统能否稳健运行的必要前提，因此应加强对银行业金融机构系统开发管理工作的检查力度，从而准确评估各运行系统以及即将上线系统的稳定性和可靠性。通过对银行业金融机构的相关制度、规定、流程、指引以及记录的检查和分析，可以了解其管理层是否统筹考虑系统开发与信息科技战略规划及业务发展目标的一致性，是否对系统开发的可行性、必要性、成本效益性以及存在的风险等方面进行全面评估，是否组织建设了合理的管理组织框架，是否对开发过程进行了全面的风险管控，以确保系统开发过程的合理、高效和安全。

检查项 1：制度建设

基本要求：银行业金融机构应制定全面的信息系统开发管理制度、流程和指引，包括但不限于：系统的开发流程和组织管理、参与部门的职责划分、时间进度和财务预算管理、质量检测和风险评估等。银行业金融机构制定的制度、流程和指引，应涵盖系统开发的全周期，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。银行业金融机构制定的制度、流程和指引，应经过高级管理层和所有相关部门的认可，明确相关部门和人员的职责并定期进行重审和更新。

检查方法、步骤：1、调阅银行业金融机构系统开发相关的制度、流程和指引，检查其是否制定了明确的管理组织及其职责，是否对开发流程管理进行全面的管控，是否有完整的时间进度管理和财务预算管理，是否建立了质量检测和风险评估机制等；2、询问相关人员，是否有高级管理层和所有有关部门认可这些制度、流程和指引的说明，如相关会议纪要、相

关文件的传阅痕迹等；3、检查系统开发过程中，相关制度、流程和指引是否得到有效的实施，如是否制定了明确的部门和人员职责，职责划分是否合理等。

检查项 2：管理架构

基本要求：银行业金融机构高级管理层在审批前应要求相关部门提供系统开发充分性的研究结果，以控制与信息科技系统有关的风险；重大信息系统项目开发应经过高级管理层的批准，符合该机构的 IT 战略规划和业务发展目标；开发过程中应定期向高级管理层上报该项目实施状况的更新报告；银行业金融机构应组成独立的部门并配备足够的具备相关知识和技能的专业人员对信息系统项目开发进行集中管理。

检查方法、步骤：1、检查银行业金融机构是否有系统开发的可行性研究、成本效益分析、风险评估、影响分析等报告，查看是否对项目的可行性、成本效益性以及可能出现的各种操作风险、财务损失、无效系统规划等进行了深入的分析；2、调阅系统开发相关会议纪要，查看相关分析结果是否得到高级管理层的认可，分析高级管理层是否对系统开发的可行性、必要性以及与 IT 战略规化和业务发展目标是否一致有充分的认识；3、查看是否有银行高级管理层同意实施系统开发的记录；4、查看是否有定期向银行高级管理层报告的系统开发进展报告；5、查看银行业金融机构是否建立了独立部门负责系统开发，调阅部门人员的清单及简介（含资质），判断该部门人员的数量和技术水平相对于系统开发方式是否充分。

检查项 3：项目控制体系

基本要求：银行业金融机构应制定合理的项目生命周期，加强项目生命周期管理；同时应开展对系统需求和技术架构的管理，使系统需求与业务目标保持一致；应当建立一套符合质量管理标准的质量控制体系，有效控制开发质量；应根据项目风险评估，在系统开发过程中落实主要风险点的风险控制措施；系统开发环境与运行环境应当分离，防止开发活动对业务运行环境造成风险。

检查方法、步骤：1、检查银行是否有生命周期管理制度，是否有生命周期管理流程和记录；2、检查系统需求和技术架构的评估文档，看系统需求与业务目标是否保持一致；3、询

问系统开发部门负责人，银行是否建立了系统开发质量控制体系，调阅其项目质量控制标准、代码编写规范（软件）以及质量控制检查和监督的记录；4、检查是否有项目需求和计划的风险评估和业务的风险点分析,是否有对业务操作环境（如人员素质、操作场所等环境）的相关风险分析，是否有对项目延期的风险、项目进程中发现的风险、项目外包的风险等关键控制点制定风险控制措施，是否有风险控制措施的落实记录和监督记录；5、检查系统开发环境和运行环境是否分离，开发过程中是否使用了生产数据,使用的生产数据是否得到高级管理层的批准并经过脱敏或相关限制。

检查项 4：系统开发的操作风险

基本要求：银行业金融机构应当加强对开发队伍的管理，合理选择具备相当知识和水平的项目经理，并要对技术人员，尤其是外来技术人员的开发行为加强管理，对于外包开发与合作开发的开发方应进行充分调研分析，以保证系统的可靠性；应当加强信息科技项目文档管理和文档版本控制；银行信息科技开发部门应当加强对开发过程的检查，确保开发目标的实现。

检查方法、步骤：1、询问银行业金融机构对项目开发经理的知识水平要求，查看部分项目开发经理的资信历史、资格证书、从业经历的调查记录，查看其权限范围是否设置合理，查看是否规定了开发人员的权限范围并进行了监控，对涉及敏感信息的开发行为是否有详细的控制记录；2、对于外包开发与合作开发的项目，询问项目管理成员，开发方是否在业内有过针对客户的不良纪录,银行业金融机构是否有对开发方技术实力与人力资源充分性进行分析；3、检查是否制定了文档管理规范制度，查看项目开发设计、源代码、技术使用和运维说明书、用户使用手册，风险评估报告等项目文档管理是否符合规范，是否进行了文档的版本控制；4、检查银行是否有系统开发过程的检查记录，是否对系统完整性、恶意代码和后门程序进行了检查。

10.2 系统测试与上线

充分的系统测试和周密的上线程序是保障系统正常稳定运行的重要因素，银行业金融机

构应该加强对系统测试充分性和系统上线程序完善性的管理，以确保系统的测试结果是可信的，上线流程是完善的。通过对相关制度、流程和程序的检查，分析银行业金融机构在系统测试和上线过程是否存在缺陷，从而对各系统做出合理的评估，避免系统测试不充分上线，或上线程序不周密，导致系统风险，造成损失。

检查项 1：系统测试

基本要求：银行业金融机构应建立完善的测试团队，并确保测试工作的公正性和独立性；应当确保系统测试的充分性，完整性；测试环境应与生产环境相隔离；应当对信息系统功能进行充分测试，保障系统功能与业务目标一致；应当对信息系统进行非功能测试，防范在信息系统性能峰值情况下发生的问题。

检查方法、步骤：1、调阅测试团队人员清单，分析测试团队人员角色、知识水平等是否充分，询问相关负责人通过哪些措施保证测试团队的公正性和独立性；2、调阅测试方案、测试用例、测试记录等，分析银行的测试方案是否完善，测试计划是否完整，测试环境是否与生产环境相隔离，测试用例是否充分，测试用例是否有生产数据，当使用生产数据测试时是否得到高级管理层的审批并采取相关限制及进行脱敏处理，测试执行情况记录是否完整，查看是否有测试充分性的审核报告；3、调阅功能测试记录，查看系统功能测试结果是否与业务目标一致；4、调阅非功能性测试报告或记录（非功能测试技术主要包括：配置和安装测试、兼容性和互操作性测试、文档和帮助测试、错误恢复测试、性能测试、可靠性测试、保密性测试、压力测试、可用性测试、容量测试），分析测试用例是否充分和测试报告是否完整。

检查项 2：系统验收

基本要求：银行业金融机构应当在系统发布前对测试过程进行充分审查，防止未经充分测试的系统上线运行；应当在系统发布前对系统的完整性进行检查，以及对代码进行检验；对打包销售的系统，应要求其提供充分可靠的测试证明，并进行代码审查；应当对系统进行一段时间的试运行，及时发现试运行中存在的问题，改正后方可正式上线

检查方法、步骤：1、调阅系统验收记录和测试质量的评估报告，检查系统发布前银行业

金融机构是否对测试的过程和充分性进行了审查并对测试质量进行了评估； 2、查看验收记录中是否对系统的完整性进行了检查，检查的内容还应该包括软件发布计划、操作手册和应急预案等文档；3、检查打包销售的软件是否有完整的、充分的和可靠的测试报告，是否有对软件代码的审查记录，特别是对秘密信道及特洛伊木马程序审查；4、检查是否有完整的试运行报告、试运行记录、系统错误修正记录等，查看系统的试运行是否通过。

检查项 3：系统上线

基本要求：银行业金融机构应当对软件分发的过程加强管理，特别对通过人工进行软件传递的行为进行监督和记录，确保分发过程的安全；应有健全的软件发布程序，确保系统安装上线过程的顺利实施。

检查方法、步骤：1、检查银行的系统分发登记；2、检查是否有系统上线过程的相关记录和操作人员名单，检查是否有应急恢复措施以保证出现问题时对生产系统的影响降到最低。

10.3 系统升级变更

及时可靠的系统变更增加了系统对各类风险的防范能力，健全的系统升级变更流程为系统持续稳健运行提供了保障，银行业金融机构应建立健全变更管理流程，加强对系统变更措施的管控，对于重大系统变更和升级的控制应视为新系统开发处置，防止正常的升级变更对系统运行产生不良影响。通过检查银行业金融机构是否建立了健全的变更制度和组织、是否有良好的变更管理团队、是否对系统变更进行了充分的测试，是否对紧急变更作了良好的规范等，正确评估系统变更的可行性、必要性和充分性，从而加强对系统运行风险的防范。

检查项 1：制度建设

基本要求：银行业金融机构应制定充分的信息系统变更制度、流程和指引，应从性质、规模、重要性等方面预先设定变更等级标准及与之相适应的具体操作程序。银行业金融机构制定的制度、流程和指引，应经过高级管理层和所有有关部门的认可，明确有关部门和人员的职责并定期进行重审和更新。

检查方法、步骤：1、调阅银行业金融机构系统变更相关的制度、流程和指引，检查其是否覆盖变更管理的全过程；2、询问相关人员，是否有高级管理层和所有有关部门认可这些制度、流程和指引的说明，如相关会议纪要、相关文件的传阅痕迹等； 3、检查相关制度、流程和指引的执行记录，看其是否得到有效的实施。

检查项 2：管理架构

基本要求：重大和大规模的信息系统变更应向银行业金融机构高级管理层提供充分的审批前研究结果；所有主要的信息系统变更都应经过高级管理层的批准，符合该机构的 IT 战略规划和业务发展目标；所有主要的信息系统变更，应定期向高级管理层上报该变更实施进度报告；银行业金融机构应明确部门负责管理变更流程。

检查方法、步骤：1、检查银行业金融机构是否有重大和大规模的信息系统变更的可行性研究、成本效益分析、风险评估、影响分析等报告，查看是否对变更的可行性、成本效益性以及可能出现的各种风险等进行了深入的分析；2、询问相关人员该分析结果是否得到高级管理层的认可，调阅相关审批记录或会议纪要；3、查看是否有高级管理层同意实施系统变更的相关记录；4、查看是否有定期向高级管理层报告的系统变更进展报告；5、询问银行业金融机构是否有明确的部门负责系统变更，调阅重大变更记录，分析该部门是否严格按照变更流程对变更过程进行监督、记录和管控。

检查项 3：测试体系

基本要求：银行业金融机构应为所有的主要变更设立充分的测试体系（如：系统单元测试、系统集成测试、系统验收测试、用户测试、预演、数据转换的验证、平行测试等）保证系统测试的完整性和充分性；测试过程中要对测试的情况进行规范的记录，最终形成测试文档并进行分析；测试用例与测试环境应与开发测试等同要求；对于在生产环境中实施的重要和大规模的变更，应采取措施尽量减小影响的生产环境区域，将对客户的影响降低到最小；系统变更应建立回滚变更的程序，以便能在发生问题的情况下可以恢复到原始的程序、系统配置和数据，在变更迁徙到生产环境前应进行回滚程序的试运行，以保证回滚程序是有效、

可靠的。

检查方法、步骤：1、检查系统变更的测试报告，分析测试报告是否完整，测试过程是否完整，测试用例是否充分；2、调阅检查用例，看是否存在生产数据，是否得到高级管理层的批准以及采取了哪些手段进行了脱敏处理；3、查看系统变更测试的环境，看是否与生产环境严格分离，检查是否有对变更人员、日期、目的、内容、影响等的审核，是否按照银行设立的审批流程对系统变更进行审核；4、检查是否建立系统变更的回滚程序，是否有回滚程序的测试或试运行成功的记录，

检查项 4：紧急变更控制措施

基本要求：银行业金融机构应确保所有的紧急变更请求的来源可信，应维持适当的控制机制对紧急变更进行授权，应确保所有紧急变更都完全地记录在相关文档上并由相关负责人进行补签批准，应保持适当的文档记录，详述紧急变更的性质、为解决问题采取的紧急措施，以及为永久更正问题而采取的后续行动，应对执行紧急变更的原因的合理性进行评估。

检查方法、步骤：1、调阅银行业金融机构系统紧急变更相关的制度、流程，查看是否有明确的紧急变更发起来源，检查采取了哪些紧急变更授权的控制措施；2、检查是否有紧急变更后相关负责人的补签记录；3、检查是否有对紧急变更合理性的评估。

10.4 系统下线

银行业金融机构应对系统下线按规范流程妥善处理，确保下线系统敏感数据的安全性和完整性。

检查项 1： 制度和流程建设

基本要求： 银行业金融机构应制定合理、安全、可靠的系统下线的制度和流程，应明确部门负责系统下线过程操作。

检查方法、步骤： 调阅系统下线相关的制度和流程，看是否有对下线系统中数据的安全性和完整性进行了有效的规定，是否有详细、可行的系统下线操作。

检查项 2： 操作管理

基本要求： 银行业金融机构应严格执行系统下线相关制度，按照规定的流程进行系统下线。

检查方法、步骤： 调阅系统下线记录，看系统下线的操作流程是否符合系统下线相关制度，是否对数据的安全性和完整性作了有效的保护。

11. 系统运行管理

11.1 日常运行管理

运行管理部门应制定详细的操作规程，以保证运行管理工作有序开展。操作规程应当明确说明信息系统、信息资产与具体业务的关联关系，数据在业务系统间流转的过程，工作安排以及操作细则，并确保能被正确的理解和使用。

检查项 1：运行部门和岗位设置

基本要求：银行负责信息科技运行的职能部门，应当合理设置运行的各个岗位，对岗位职责、权限进行明确划分，保持岗位职责与岗位权限保持一致，并对岗位的最小权限进行限定及不兼容岗位进行不兼岗限定，同时重要岗位、重要系统管理人员应该有双人备份机制。

检查方法、步骤：1、调阅有关岗位职责及权限的说明书，人员清单，不兼容岗位清单等资料；2、询问两个不兼容岗位的人员，了解同一个人是否存在不兼容岗位。

检查项 2：信息科技部门人员管理

基本要求：对 IT 业务从业人员有严格的管理制度，并能够按照制度要求实行定期轮岗，同时保证一人不会存在两个有危险交叉的岗位上实行轮换，保证重要岗位执行强制休假制度，。

检查方法、步骤：1、调阅 IT 部门相关人员管理制度、岗位职责等相关文件；2、调阅 IT 部门岗位交接相关制度文件；3、调阅有人员调离或换岗时的登记记录，并对调离人员签署相

应的安全协议；4 询问重要岗位备份人员相关情况，检查是否满足人员备份要求；5、调阅重要岗位强制休假记录。

检查项 3：信息科技部门人员培训

基本要求：信息科技部门人员须定期进行培训，并保证操作人员已掌握了新业务的操作，并对新业务带来的风险有防范意识。

检查方法、步骤： 1、调阅业务培训计划和以往培训记录等相关资料；2、询问 IT 部门业务主管，是否对相关业务人员根据业务发展制定相关的培训计划。

检查项 4：系统用户的管理

基本要求：银行信息科技运行部门应当加强应用系统、主机系统、数据库系统等系统的授权管理。

检查方法、步骤：1、询问系统管理员是否严格按照系统授权管理制度进行了用户管理，并定期检查系统用户账号，确保每个账号有唯一的、合规的使用人员；2、询问系统管理员在使用超级用户职权时，是否采取了如双人管理等制约措施并留有操作记录；3、调阅授权管理制度，各类系统用户清单，定期检查记录，访问日志，用户设置、变更、删除的审批记录等相关；4、参考人员换岗、离职清单，检查其权限变更、删除情况

检查项 5：系统性能的监控

基本要求：银行应当建立重要信息系统的性能监控系统，尤其是加强对系统重要性能参数的监控，并合理设置监控系统的预警值。

检查方法、步骤：1、询问 IT 部门主管，是否建立了系统性能的监控系统，并设定了系统重要核心参数监控清单和合理的预警值（至少包含：CPU 利用率、网络利用率、存储容量、系统状态等）；2、调阅性能状况、趋势的分析报告；3、调阅峰值记录的分析。4、调阅系统设计文档等资料。

检查项 6：信息系统配置的管理

基本要求：银行信息科技部门应当对运行环境的系统配置进行严格的控制，并与备份配置保持一致，绝对禁止任何非授权的修改配置行为。

检查方法、步骤：1、询问 IT 部门主管，是否建立了有效的配置管理措施。2、调阅配置管理机制或系统，配置管理记录，检查安全配置策略等。

检查项 7：系统设置参数的更改

基本要求：各类系统的管理人员更改系统的设置参数时，必须提出书面申请并经信息科技管理部门负责人签字确认，特别重要的系统，如：主机操作系统和数据库系统,需经 CIO 签字确认,其执行情况应在《操作日志》中记录。

检查方法、步骤：1、调阅资料：检查管理员更改系统的设置参数时，是否提出书面申请，并经过科技部门负责人的签字确认；检查对主要系统主机操作系统和数据库的更改是否经过 CIO 的签字确认；2、检查更改的执行情况是否在《操作日志》中留有记录。

检查项 8：设备和介质的生命周期管理

基本要求：银行应当按照设备和介质的安全等级，制定生命周期全流程的管理措施，尤其是加强报废期的安全管理。硬件设备主要包括：主机、小型机、服务器、网络和拨号设备、网络安全设备、通讯设备、PC 等终端设备和外来的特定用途设备等。介质包括：文档、磁带、磁盘、远程存储器、光盘、移动存储器等。

检查方法、步骤：1、询问 IT 部门主管，是否按照设备和介质的安全等级，制定了生命周期的管理措施；2、调阅管理措施，监控或检查记录等相关资料；3、查看相关资料，查看有无报废控制的要求；

检查项 9：日志管理

基本要求：银行信息科技运行部门应当加强日志管理，对日志实行分级管理，确保重要

的运行行为被记录和分析，对重要日志实行定期备份，保证当发生安全事件时做到有据可查。

检查方法、步骤：1、询问 IT 部门主管，是否有专人负责日志管理和定期分析的记录；2、调阅日志，定期分析记录等资料。

检查项 10：问题管理

基本要求：银行应当建立有效的问题管理机制，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汇报事故的发生，记录、分析和跟踪所有事故，直到对事故进行彻底的改正并完成根本原因的分析。

检查方法、步骤：1、询问 IT 部门主管，是否建立了问题管理机制；2、是否有问题管理处理过程记录文档;3、调阅问题管理机制，问题管理处理过程记录文档等资料。

检查项 11：服务台管理

基本要求：银行信息科技应当建立服务台，为行内用户提供所有技术相关问题的在线支持，并将问题提交给相关信息科技职能部门进行调查核实解决。

检查方法、步骤：1、询问相关人员，是否建立了服务台及管理制度；2、是否保有服务台服务过程记录文档；3、调阅服务台管理制度，服务台服务过程记录文档等资料。

检查项 12：呼叫中心

基本要求：银行信息科技部门应为呼叫中心提供给技术支持，对信息科技事件做出迅速响应，制定问题与事件管理机制，记录、分析与追踪所有问题及事件的发展，直至问题和事件解决为止。

检查方法、步骤：

访谈负责系统维护管理的主管，调阅相关制度和文档，了解以下要点：1、是否为呼叫中心提供技术支持；2、是否建立问题与事件管理机制，记录、分析与追踪所有这些问题及事件的发展。

检查项 13：桌面管理

基本要求：信息科技运行部门应当对系统运行部门桌面进行有效管理，建立桌面管理制度。

检查方法、步骤：1、调阅相应的桌面管理制度；2、查看是否有离开时间使用屏幕保护的要求；3、是否有定期更改密码的要求及相应得记录；4、调阅定期修改密码的检查记录等资料。

11.2 日常运行的监督

运行管理部门应定期通过自我评估或独立的审计活动，结合业务系统间的关联关系，识别运行中的风险因素，并完善风险控制措施。对各类管理人员的履行职责情况进行定期检查、核对，并及时纠正其错误。

检查项 1：规章制度及信息安全控制执行情况的检查

基本要求：银行信息科技部门应当对规章制度执行情况进行检查，确保规章制定得到有效落实；对信息安全策略、标准及制度的执行情况进行检查，及时发现制度执行过程存在的问题。

检查方法、步骤：1、调阅检查制度；2、调阅按照规章制度要求对执行情况进行检查的记录；3、调阅对安全策略和标准的执行进行跟踪和检查的记录；4、调阅对制度执行过程存在问题的原因进行分析的相关记录；5、调阅审计部门出具的评估报告等。

检查项 2：运行报告

基本要求：信息科技运行部门应当定期将重要信息系统的运行报告提交管理层。

检查方法、步骤：1、调阅重要信息系统运行报告；2、检查管理层是否阅读了运行分析报告并签字确认。

11.3 可靠性运行管理

运行管理部门应制定详细的业务连续性计划，以保障业务系统的稳定运行，并能在业务中断以及灾难情况下，快速的恢复。

检查项 1：单点故障的排查

基本要求：银行信息科技部门应当定期排查单点故障问题。

检查方法、步骤：1、调阅资料，检查是否有完整的定期关键单点故障排查的记录；2、调阅排查机制，排查记录等相关资料。3、询问 IT 部门主管，是否对故障采取了有效的措施。

检查项 2：信息系统漏洞导致业务失控的风险排查

基本要求：银行信息科技部门应当及时对偶然发生的因信息系统漏洞导致业务失控的风险进行排查，并采取相应的控制措施。如：ATM 偶然出现超大额现金支取权限等。

检查方法、步骤：调阅资料，查看是否保留案例故障原因排查的记录等。

检查项 3：数据的管理

基本要求：银行应当建立了足够的数据管理措施，保证重要的业务信息和客户信息在采集、传输、使用、存储、备份、恢复、查询、销毁等过程中得到保护。

检查方法、步骤：询问 IT 部门主管，调阅相关资料，了解是否制定了数据管理各环节的严格控制制度，并保留相关的管理记录；

11.4 安全运行管理

银行业金融机构应建立完善的信息安全组织体系，清晰、明确地阐明各层组织机构、信息技术管理各相关部门及岗位的安全职责，确保信息安全的决策、管理、指导、执行、监督、审查等各环节工作的有效落实、改进和不断完善。

检查项 1：对已获知的外部安全问题信息的反应

基本要求：银行信息科技运行部门对已获知的外部安全问题信息应该引起重视，研究自身是否有同样的问题隐患，及时采取安全防范措施。

检查方法、步骤：1、调阅资料，检查是否有外部信息系统安全事件，本部门研究记录；2、询问 IT 部门主管，是否对已获知的外部事件针对本行采取向应的应对措施

检查项 2：信息安全事件的响应

基本要求：银行应当建立信息安全事件的响应机制。

检查方法、步骤：1、调阅资料，检查是否建立了信息安全事件的响应机制和流程；2、查看信息安全事件的响应过程是否符合响应机制和流程的要求。

检查项 3：信息安全设备的完备性

基本要求：银行应当配备足够网络安全设备，并符合信息系统安全保护的等级要求。安全设备主要包括：边界控制设备（如防火墙、网关等）、身份识别设备（如门禁、证书系统、用户登录系统等）、加密设备（如加密机、加密卡等）、病毒和黑客防范设备（如防病毒系统、防篡改系统、防病毒网关等）等。

检查方法、步骤：1、询问 IT 部门主管，信息系统是否达到信息系统安全保护的等级要求；2、在系统投入生产前是否有生产前测试 3、有无防攻击演练记录； 3、调阅设备配置清单，网络拓扑图，攻击演练记录，系统设计文档等相关资料。

检查项 4：信息安全的管理工具

基本要求：银行应当合理配置信息安全管理工具，并经授权后使用管理工具进行分析和报告。信息安全管理工具包括但不限于：入侵检查管理工具、性能检测管理工具、网络管理工具、配置管理工具。

检查方法、步骤：1、询问 IT 部门主管，是否留有使用管理工具进行有效分析的记录和

报告；2、是否配置入侵检测管理工具；3、有无防攻击演练记录；4、调阅管理工具清单，分析记录或报告，攻击演练记录等相关资料。

检查项 5：病毒的检测和预防

基本要求：银行应当制定病毒检测和预防的措施，预防病毒的大规模爆发。

检查方法、步骤：1、询问 IT 部门主管，病毒检测系统能否覆盖全部的信息科技设备和终端；2、是否对病毒检测系统及时升级和维护；3、询问是否发生过大规模的病毒爆发，如果出现过，是怎么样进行处理的 4、调阅资料，查看处理记录；5、查看病毒定义版本。

11.5 保密运行管理

银行要对数字签名、认证和口令进行严格管理，达到国家有关密码管理要求，根据交易的重要性和安全程度建立必要的交易验证机制，尤其是对高风险业务。

检查项 1：数字签名和认证的安全性

基本要求：银行建立的数字签名和认证系统应当符合国家法律法规的要求，并有国家权威部门的认证。

检查方法、步骤：1、数字签名和认证系统符合国家相关法律的要求；2、数字签名和认证系统获得国家权威部门的销售许可和安全监测；3、使用第三方的数字签名和认证系统，服务提供方获得了相关法律许可，使用的数字签名和认证系统进行过充分测试；4、调阅资料，查看产品说明书，产品认证证书，测试记录，数字签名和认证安全等资料等。

检查项 2：口令的管理

基本要求：银行口令管理应达到口令和密码安全策略的要求，并制定了口令和安全策略。

检查方法、步骤：1、询问 IT 部门主管，询问口令设置符合口令和密码安全策略，对弱口令进行了屏蔽；2、调阅审计部门的或 IT 部门根据相关制度文件，对于口令管理的现场检查记录等。

检查项 3：交易的验证

基本要求：银行应当根据交易的重要性和安全程度建立必要的交易验证机制，尤其是对高风险业务。

检查方法、步骤：1、询问 IT 部门主管，是否有对交易的重要性和安全程度进行验证、分类的机制；2、对于高风险业务是否采取了符合法律法规要求的多重验证机制；3、调阅验证机制分类，验证方法，高风险业务的验证方法等相关资料。

检查项 4：数据的加密

基本要求：银行应当对信息系统的各种敏感数据进行加密，并能够合法保护。（如：客户信息）

检查方法、步骤：1、询问 IT 部门主管，是否对敏感数据按照信息资产的最低保护要求，采取经过权威部门认证或通过充分的反破解测试的加密措施；2、是否对数据的采集、加工、存储、传输、检索的授权使用等保护及保密措施；2、调阅客户信息保护和保密制度，保护措施，加密措施，认证证书，测试记录或报告等。

12. 灾难备份管理

灾难备份（以下简称灾备）是指为了灾难恢复而对数据、数据处理系统、网络系统、基础设施、专业支持能力和运行管理能力进行备份的过程。灾难备份和恢复系统（以下简称灾备系统）是以灾备为目的的数据备份系统、备用数据处理系统和备用网络系统组成的信息系统。灾备系统的检查是根据《中国银行业监督管理委员会关于印发〈银行业金融机构信息系统风险管理指引〉的通知》（银监发〔2006〕63 号）文件的要求，检查银行业金融机构根据自身情况建立备份机制的合规性，同时确认银行业金融机构灾备系统整体管控策略、项目实施过程，运行维护、监控评估过程的适当性。

12.1 灾难恢复的总体控制

检查项 1：灾难恢复的规划

基本要求：省级以下数据中心实现备份异地保存，省域数据中心建立异地实时备份，全国中心应实现异地灾备。银行业金融机构应该有完备的、正式的针对灾难恢复的规划。

检查方法、步骤：1、面谈或现场查看，根据银行业金融机构的情况，检查是否建立了相应的备份恢复机制。2、与信息科技主管人员会谈，了解是否明确定义了为减少灾难带来的损失和保持信息系统所支持的关键业务灾难后迅速恢复和继续运行的总体安排和计划。3、与信息科技主管人员会谈，调阅相关资料，查看灾难恢复工作的范围定义的完整性。包括了灾难恢复规划和灾难备份中心的日常运行、关键业务功能在灾难备份中心的恢复和重续运行，主系统的灾后重建和回退工作，突发事件的响应。4、确定灾难恢复规划的生命周期是否完整，检查这些过程中的文档和正式审批过程。主要包括灾难恢复需求的确定过程、灾难恢复策略的制定过程、灾难恢复策略的实现过程，灾难恢复预案的制定、落实和管理。

12.2 灾难恢复的组织机构

检查项 1：灾难恢复的组织机构

基本要求：银行业金融机构应根据其具体情况建立相应的负责灾难恢复的组织机构。

检查方法、步骤：1、是否建立了负责灾难恢复的组织机构及其完整性。一般可分为灾难恢复领导小组，灾难恢复实施小组和灾难恢复日常运行小组。如果没有以上组织构，是否有相应的机制来保证灾难恢复过程的实施。2、灾难恢复组织机构人员组成是否合理。组织机构内人员的职责是否明确，并指定相同职责的人员代替顺序。灾难恢复的组织机构人员的组成应包括管理、业务、技术和后勤方面的人员。

检查项 2：灾难恢复领导小组职责

基本要求：灾难恢复领导小组是信息系统灾难恢复工作的组织领导机构，组长应由银行

业金融机构最高管理层成员担任，领导和决策信息系统灾难恢复的重大事宜。

检查方法、步骤：1、是否有明确的正式文件来规定灾难恢复领导小组的职责和分工。2、是否由银行业金融机构最高管理层成员担任组长，并能够切实在灾难发生时迅速响应，同时建立了相应的人员备份机制。3、职责定位的准确性。是否明确了包括审核并批准经费预算、审核并批准灾难恢复策略、审核并批准灾难恢复预案和批准灾难恢复预案的执行在内的职责范围，或以正式文件明确的类似的职责权限。

检查项 3：灾难恢复规划实施小组职责

基本要求：建立正式的文档，明确定义灾难恢复规划实施小组的人员组成和职责定位。

检查方法、步骤：1、是否有明确的正式文件来规定灾难恢复实施小组的职责和分工，并明确了各重要职责的人员备份策略。2、是否明确规定了灾难恢复规划实施小组的职责为：灾难恢复需求分析、提出灾难恢复策略和等划分、灾难恢复策略的实现、制定灾难恢复预案、组织灾难恢复预案的测试和演练。或者有相类似的职责定义完成以上工作。

检查项 4：灾难恢复日常运行小组职责

基本要求：建立正式的文档，明确定义灾难恢复日常运行小组的人员组成和职责定位。

检查方法、步骤：1、是否有明确的正式文件来规定灾难恢复日常运行小组的职责和分工，并明确了各重要职责的人员备份策略。2、是否明确定义了如下职责：协助灾难恢复系统实施，备份中心的日常管理，灾难恢复运行维护，参与和协助灾难恢复预案的教育、培训和演练，维护和管理灾难恢复预案，突发事件发生时的损失控制和损害评估，灾难发生后信息系统和业务功能的恢复，灾难发生后的外部协作。

12.3 灾难恢复的规划过程

检查项 1：业务影响分析

基本要求：在灾难恢复的规划过程中，标识信息系统的资产价值，识别信息系统面临的

自然和人为的威胁，识别其脆弱性，分析威胁发生的可能性并定量或定性描述可能造成的损失，识别现有的风险防范和控制措施。分析各项业务功能及各项业务功能之间的相关性，确定支持各种业务功能和相关资源。采用定量或定性的方法，对业务功能中断造成的影响进行评估。灾难恢复的规划过程中应根据风险分析和业务影响性分析的结果，确定灾难恢复的目标。

检查方法、步骤：1、调阅灾难恢复策略制定开发过程的风险分析文档，确认是否对自身信息系统的风险进行了全面分析，确保覆盖了所有关键业务系统。2、检查是否根据风险分析结果确定了风险防范和风险接受的程度，并出具正式的分析文档做为灾备系统开发的重要依据，该文档是否经过管理层的正式审批。3、调阅灾难恢复策略制定开发过程的相关文档，确认银行业金融机构在灾难恢复策略制定过程中实施了全面的业务影响性分析，确保覆盖了所有关键业务系统，并明确相关信息的保密性、完整性和可用性要求。4、调阅灾难恢复策略制定开发过程的相关文档，确认灾难恢复策略制定开发过程中是否实施了中断影响的评估。确定是否利用量化或定性分析的方法，评估业务功能中断可能给组织带来的非经济损失，及由此带来的风险。并形成正式的、经管理层审批的业务影响性分析文档。5、调阅灾难恢复策略制定开发过程的相关文档，检查是否明确定义了关键业务功能及恢复的优先顺序。确认该优先恢复顺序的确认过程中是由业务部门发起，并经高级管理层的审批。6、调阅灾难恢复策略制定开发过程的相关文档，确认明确定义了灾难恢复时间范围（RTO 和 RPO 的范围）。确认该优先恢复顺序的确认过程中是由业务部门发起，并经高级管理层的审批。7、调阅 RTO/RPO 与灾难恢复能力等级关系的相关文档。查看 RTO/RPO 时间定义是否附合银行业金融机构业务连续性的要求。

检查项 2：联络与通讯

基本要求：灾难恢复策略中所涉及的关键岗位的联系与通讯地址应该详细记录并持续更新，建立完备的通讯和报告机制。

检查方法、步骤：1、检查灾难恢复策略是否记录了涉及的关键岗位的详细通讯方式。包括：建议所有相关人员的姓名、地址，家庭、办公的电话号码、移动电话号码，及其他可

以迅速取得联系的方式。以及灾难发生的时候可用的备份联系方式。2、根据灾难恢复策略中的记录，确认关键岗位通讯方式的可用性，确保灾难恢复策略中记录的有效性。3、同灾难恢复策略中涉及的人员会谈，确认所有人都已经得到该通讯记录，并在异地进行了备份存储，并可以及时取得。

检查项 3：灾备系统中的外包风险

基本要求：充分考虑灾备系统建设中外部力量的使用策略，可以聘请相应资质的外部专家，或委托具有相应资质的外部机构承担实施和运行的部分或全部工作。

检查方法、步骤：1、查看是否聘请相应资质的外部专家参于灾备系统的建设和运维过程，根据确定外部专家过程中的相关会议纪要或备忘录，确认外部专家的资质有足够的能力提供相应的服务。2、查看聘用外部专家的相关文件，确认其工作职责、范围是否明确规定，并制定了正式的安全保密措施。3、委托相应资质的外部机构进行灾备系统建设时，应查看与外部机构之间的服务水平协议（SLA），确认其中安全保密措施是适当的。4、考察灾难恢复策略中涉及到的电信运营商、电力供应商、设备及技术支持供应商之间的服务水平协议（SLA），确保灾难发生时可以得到及时的服务。（参考“外包服务部分”）

12.4 灾难恢复的实施过程

检查项 1：灾难恢复策略的制定

基本要求：灾难恢复策略的制定过程中，应根据自身情况进行灾难恢复等级划分，并根据等级需求明确定义灾难恢复资源（数据备份系统、备用数据处理系统、备用网络系统、备用基础设施、专业技术支持能力、运行维护管理能力和灾难恢复预案），同时，根据成本风险平衡的原则确定每项关键业务功能的灾难恢复策略。

检查方法、步骤：1、审阅灾难恢复策略制定过程中产生的文档，确认银行业金融机构全面分析了灾难恢复资源的成本与风险可能造成的损失之间取得平衡的原则确定每项关键业务功能的不同灾难恢复策略。2、确认灾难恢复策略内容的完整性，是否完全包括了灾难恢复资

源的获取方式和灾难恢复能力等级（灾难恢复资源各要素的具体要求）。3、数据备份系统。审阅灾难恢复策略制定过程中产生的文档，确认是否根据成本风险平衡，明确定义了数据备份的范围、时间间隔、技术及介质、数据备份线路的速率及相关通信设备的规格和要求，采用定性的方式确认其保证 RTO 和 RPO 的要求的能力。4、备用数据处理系统的获取方式。审阅灾难恢复策略制定过程中产生的文档，确认备用数据处理系统的数据处理能力、与主系统的兼容性要求，日常运维过程就绪或运行状态的情况，结合恢复的时间性要求，确认备用数据处理系统取得方式能够满足业务连续性的要求。（三种方式：事前的紧急供货协议；灾备中心或设备仓库储备的数据处理设备；外包服务提供的兼容设备）5、备用网络系统。审阅灾难恢复策略制定过程中产生的文档及灾备中心制定的相关操作规程和管理制度，确认备用数据通信线路的可用性（可参考“网络”部分进行实质性测试，审核数据通信的技术和线路带宽，网络通信设备的功能和容量，确认其可用性）。6、备用基础设施。审阅灾难恢复策略制定过程中产生的文档，是否按照成本风险平衡原则，考虑与主中心的距离要求，场地和环境要求（参考“物理环境/计算机机房”），运行维护和管理要求三个方面的内容，确认备用基础设施的可用性。租用的商业化灾难备份中心的基础设施，应考虑“外包服务”内容确认其服务水平协议的有效性，或根据公允的第三方提供的安全评估报告来确认其可靠性。7、专业技术支持能力。审阅灾难恢复策略制定过程中产生的文档，审核灾难备份中心设置专职技术支持人员的技术能力，以及相应职质。由主中心技术支持人员兼任灾备中心的技术支持时，审核灾难发生时由于交通和通讯不正常时的备用技术支持方案。外包方面的技术支持应根据“外包服务”相关内容进行复核其可用性。8、运行维护管理能力。审阅灾难恢复策略制定过程中产生的文档，确认是否按照成本风险平衡的原则确定灾难备份中心在软件、硬件和网络等方面的技术支持要求。进一步调阅灾备中心运行维护的相关制度、流程和相关审批和操作记录，确认其技术支持的组织架构、技术支持人员数据和素质是否满足灾备中心的运维能力的需要。委托外包方运行维护的需要根据“外包服务”内容确认其可用性或根据公允第三方评估报告确认其可用性。

检查项 2：灾难恢复策略实现

基本要求：银行业金融机构应根据灾难备份策略制定相应的技术方案，经过严格的确认、验证的开发过程，并根据验证的技术方案进行完整的安装和测试。

检查方法、步骤：1、技术方案的设计。查看灾难备份系统技术方案的相关文档，查看是否包含了数据备份系统、备用数据处理系统和备用的网络系统。确认方案中明确考虑了备用系统获得同主系统相当的安全保护策略，充分考虑了冗余度和可扩展性，并考虑了备用系统对主系统可用性和性能的影响。2、查看备份系统技术方案得到相关部门正式的确认和验证的结果性文档证明材料，确认该方案得到正式审批。3、查看备份系统技术方案实施过程的相关实施及测试计划的完备性，确保灾难恢复规划实施组按审核过的技术方案制定相应的安装测试计划。查看最终用户参与各关键业务功能系统的测试的相关记录，保证计划得到了严格的实施。查看测试的结果，确保数据备份及数据恢复功能的有效性，规定时间内恢复各项关键业务功能的有效性和客户端与备用数据处理系统通信的有效性。3、灾难备份中心的选择和建设。审阅灾难恢复策略，确认根据风险分析的结果，避免了灾难备份中心与主中心同时受到同类风险。根据银行业金融机构类型，确认其选择同城和异地灾备的适当性。根据“物理环境/计算机机房”检查要点，确认灾难备份中的物理环境的安全性，确认灾备相关通讯、电力资源和交通条件得到保障的可靠性。4、灾难备份中心的运维管理。调阅灾备中心制定的相关操作规程和管理制度，及运维过程中产生的相关的档案和审核记录，确认数据备份的及时性和有效性；确认备用数据处理系统和备用网络系统处于正常状态，并与主系统的参数保持一致；有效的应急响应和处理能力。

检查项 3：灾难恢复预案的实现

基本要求：定义信息系统灾难恢复过程中所需的任务、行动、数据和资源，指导相关人员在预定的灾难恢复目标、按灾难恢复手册的要求，恢复信息系统支持的关键业务功能。

检查方法、步骤：1、审阅灾难恢复预案，检查是否涵盖了灾难恢复的整个过程，以及灾难恢复所需的尽可全面的数据和资料，明确定义了恢复的启动过程、启动条件及启动流程。2、审阅灾难恢复预案，检查其使用的语言和图表的易于理解程序，其结构的清晰程度，资源描

述的清楚程度，工作内容和步骤的具体程度和相应的责任人员定义的明晰程度，确保灾难恢复的易用性和明确性。3、与负责应急系统管理和灾备系统管理的主管人员进行会谈，了解灾难恢复预案与其他应急体系的结合程度，确保其兼容性。4、审阅灾难恢复预案制定过程产生的文档记录，确保灾难恢复预案在制定过程，经过了起草、评审、测试、完善、审核和批准的全过程。查看评审流程，确保对预案的完整、易用、明确、有效和兼容性进行了严格评审。查看测试报告，确保测试包含了单元测试、关联测试和整体测试。查看预案的审批稿，确保评审和测试过程中发现的问题和缺陷得到有效整改。查看预案的执行稿，确保灾难恢复领导小组对审批稿进行了正式的审核和批准。

12.5 灾难恢复的维护更新过程

检查项 1：教育、培训和演练

基本要求：为了使相关人员了解灾难备份恢复的目标和过程，确保灾难备份恢复系统的有效性，需要对相关人员进行持续的教育和培训，并实施灾难恢复演练。

检查方法、步骤：1、与灾备相关的人员进行会谈，确认银行业金融机构从灾难恢复规划的初期就开始了灾难恢复观念的宣传教育，并不断进行灾难恢复观念或相关知识的宣传教育活动。2、检查已经实施培训记录和未实施的培训计划，并与灾备相关的技术支持人员进行会谈，确认银行业金融机构持续提供关于灾备、应急、专业技术、业务系统方面的培训，提高专业技术支持能力的提升。3、检查已经实施的演练计划所形成的报告，根据演练的类型（桌面演练，模拟演练，真实演练，混合演练）和结果，确认其演练过程的有效性。每年应至少完成一次有最终用户参与的完整演练。

检查项 2：灾难恢复的管理和持续更新

基本要求：经过审核和批准的灾难恢复预案应实施严格的管理流程，并对预案进行严格和持续性的维护和变更管理。

检查方法、步骤：1、与灾难恢复预案的管理人员进行会谈，调阅相关的管理制度。了解

其保存和分发的流程，确定其在如下几个方面的合理性：专人负责；多份拷贝异地保存；分发给所有参与灾难恢复工作的人员；每次修订后的所有拷贝统一更新，并保留一套备查；旧版本按规定销毁。2、检查灾难恢复预案的维护和变更记录及审核文档，确保业务流程的变化、信息系统的变更、人员的变更都在灾难恢复预案中及时反映。3、调阅测试、演练和执行的效果评估结果，以及预案相应的修订记录，确保灾难恢复预案进行了相应的修订。4、调阅针对灾难恢复预案进行的评审或内部 IT 审计的相关报告，确认灾难恢复预案进行了相应的修订。所有的修订都应执行严格的起草、评审、测试、完善、审核和批准的全过程。注：灾难恢复能力等级划分表见《信息系统灾难恢复规范 GB20988-2007-T》附件 A。

13. 数据管理

13.1 数据管理制度和岗位

信息系统处理的各种数据（用户数据、系统数据、业务数据等）在维持系统正常运行上起着至关重要的作用。一旦数据遭到破坏，都在不同程度上影响银行业金融机构的业务连续性和安全性，甚至带来巨大的声誉风险或造成经济损失。由于信息系统的各个层面（网络、主机、应用等）都对各类数据进行传输、存储和处理等，因此，对数据的保护需要物理环境、网络、数据库和操作系统、应用程序等提供支持。银行业金融机构应严格业务数据的采集、传输、使用、存储、备份、恢复、查询、销毁等各个环节，确保数据的机密性、完整性、可用性。

检查项 1：数据管理的制度

基本要求：银行业金融机构应制定严格的指导意见，对业务数据的使用、存储、备份、恢复、销毁等各个环节进行严格管理。

检查方法、步骤：1、获取银行业金融机构数据管理方面的制度，查看是否有数据安全管理方面的管控措施，在用户私密信息保护措施是否符合国家相关法律法规的要求。2、获取银行业金融机构数据管理方面的制度，查看其是否对业务数据的保护进行了适当分级，并对高

保护等级数据进行相应的数据管理。3、与银行业金融机构安全管理人员会谈，了解是否指定或授权专门的人员负责安全管理制度的制定；与数据安全管理维护人员会谈，了解是否将安全管理制度完整的发布到相关人员手中的方式，并确认其适当性。4、获取银行业金融机构数据管理方面的制度，确认其制定和发布过程得到有效控制，并经过高层管理部门的审核和批准。检查数据备份和恢复策略文档，查看其内容是否覆盖数据的存放场所、文件命名规则、介质替换频率、数据离站传输方法等方面内容。

检查项 2 ：数据管理的岗位

基本要求：银行业金融机构应针对数据管理的内容和等级，以及数据产生、存储、分发、备份、恢复和销毁的过程，建立完整的岗位责任制度，责任落实到人。

检查方法、步骤：1、检查岗位划分相关的文档，确认是否已经设立系统管理员、安全管理员等岗位，并明确各岗位之间在数据的产生、存储、分发、备份、恢复和销毁过程中的职责和权限划分。2、与数据安全管理负责人员进行会谈，了解各个工作岗位在数据安全管理方面的人员数据，并确认人员的相关资质是否符合数据安全管理的要求。3、获取银行业金融机构数据管理方面的制度，确认与机密数据相关的工作岗位人员都签订了相关的安全保密协定。可进一步与相关人员进行会谈，确认其对安全保密协议的了解程度及遵守情况。4、获取银行业金融机构数据管理方面的制度，分析各岗位职责之间的职责分离的遵循程度，确认其划分的适当性，确保关键岗位的职责分离。如安全管理员不得兼任其他岗位。5、获取银行业金融机构数据管理方面的制度，确认各岗位之间相互监督和牵制的适当性，确保对关键业务数据的访问和操作经过严格的审批流程和日志记录，操作过程由双人在场，防止舞弊发生。相关记录应长期保存备查。

13.2 数据备份、恢复的策略

检查项 1：数据备份策略

基本要求：银行业金融机构应根据业务的需求及数据安全保护等的要求，制定相应的数据备份和恢复策略，以保持数据可访问性和可用性。

检查方法、步骤：1、与银行业金融机构负责安全管理方面的人员进行会谈，确认银行业

金融机构已经建立了完整的数据备份策略。并在策略中识别了需要定期备份的重要业务信息、系统数据及软件系统。2、检查备份与恢复策略。确认其包括了备份与恢复管理相关的安全管理制度，对备份信息的备份方式、备份频度、存储介质和保存期等进行规定。并指明备份数据的放置场所、文件命名规则、介质替换频率和将数据离站运输的方法。3、检查相关的数据备份策略，确认其建立了控制数据备份和恢复过程的程序，记录备份过程，所有文件和记录应妥善保存。查阅相关的数据备份和恢复的历史记录，确保可以提供本地数据备份与恢复功能，完全数据备份至少每天一次，备份介质场外存放。查阅异地数据备份相关的记录或日志，确认利用通信网络将关键数据定时批量传送至备用场地的时间频度和完整性。4、检查相关的数据备份策略，确认其根据业务变更、软件变更或硬件变更的过程进行了相应的修订，其修订过程有严格的流程控制，并得到领导层的审核和批准。

检查项 2：数据恢复、抽检策略

基本要求：应定期执行恢复程序，检查和测试备份介质的有效性，确保可以在恢复程序规定的时间内完成备份的恢复。

检查方法、步骤：1、与安全管理人员进行会谈，确认是否有制度化的数据恢复和抽检测试策略。2、根据数据恢复和抽检策略，查阅恢复和抽检的相关记录，确认该计划得到了严格的实施。3、检查数据恢复测试的执行记录，确认数据恢复过程得到管理层的正式审批，机密数据的操作过程应由两人同时在场。操作步骤和日志记录应妥善保管。4、根据数据恢复、抽检测试策略，检查执行记录，确认数据恢复过程在时间要求方面和正确程度方面符合业务的需求。其衡量标准为数据成功恢复的百分比。5、根据数据恢复、抽检测试策略，查看相关的操作记录，确认恢复、抽检中存在的问题得到有效整改，其整改过程经过严格的审核和批准过程。

13.3 数据存储介质及文档的管理

检查项 1：介质管理

基本要求：加强存储介质的管理，防止对存储介质的非授权访问、变更、删除和破坏，而带来的业务持续性和安全性的影响。

检查方法、步骤：1、与安全管理人员进行会谈，确认银行业金融机构制定了关于可移动存储介质（磁带、磁盘、闪存、可移动硬盘、DVD、VCD、及打印出的介质）的正式的、文档化的管理流程，并经管理层进行了审核和批准。2、检查存储介质的管理流程，确认可重用存储介质中不需要的内容应该及时删除，并确保其删除是不可恢复的。3、检查存储介质的管理流程，确认所有存储介质都按照厂商要求的存放条件进行存放。确认存放的物理环境在基本的防磁、防水及温湿度要求在合规的范围内。（参考“物理环境”相关标准）。4、根据信息的保存期，检查各类存储介质的保存周期，确保由于存储介质过期损坏带来的信息丢失。5、查看是否对可移动介质进行了严格的登记管理，确认只有在业务需求的时候才使用移动介质，并实施相应的管控过程。

检查项 2：介质的清理和销毁

基本要求：银行业金融机构对存储介质的清理和销毁过程进行严格的管控，并制定相应的流程确保敏感信息对非授权人员泄露的风险。

检查方法、步骤：1、与安全管理人员进行会谈，确认建立了相应的存储介质的清理和销毁的流程，确保敏感信息与其保密等级适应。2、检查存储介质的清理和销毁过程产生的相关记录，确认机密数据得到了安全的处理过程。主要包括焚烧、粉碎或内部进行的清除数据的操作。3、检查存储介质的清理和销毁过程产生的相关记录，确认介质的清理和销毁流程中包括了对需要安全处理的数据项的识别过程。4、检查存储介质的清理和销毁过程产生的相关记录，确认对弃置的纸张、设备和介质的收购者进行了合理的管控，防止信息泄密。5、检查存储介质的清理和销毁过程产生的相关记录，确认在对敏感信息进行处理的过程中进行了全面登记，并保留相关记录备查，同时经过严格的审批。

检查项 3：系统文档管理

基本要求：系统文档可能包含一系列敏感信息，如应用系统的描述 、相关的流程办法、数据结构和授权程序，因此，应该适当的管理，并防止非授权的访问。**检查方法、步骤：**1、与系统安全管理人员进行会谈，确认银行业金融机构对相关的文档进行了全面的管理和保护，并安全存放。。2、与系统安全管理人员进行会谈，通过开放式的网络应用维护和提供的系统文档，是否经过了适当的授权访问保护策略，并对访问进行了记录。。3、检查系统文档访问的记录列表 (文本或电子) ，确认这些访问都经过应用所有者的授权，并坚持了“最小授权”的原则。

第三部分・支持平台

第三部分　支持平台

14. 机房管理

14.1 物理环境/计算机机房业务连续性

物理环境/计算机机房业务连续性检查主要是对银行业金融机构的计算机机房及计算机机房所在建筑物的选址、基础设施、功能分区、管理、维护、应急体系和外包服务的合规性、真实性的检查。通过现场检查督促银行业金融机构规范计算机机房的维护、监控和应急响应等相关操作、加强计算机机房管理、规避业务停顿风险，从物理环境/计算机机房层面确保银行业金融机构的业务连续运做。

物理环境/计算机机房业务连续性检查采取调阅资料、实地勘测和询问谈话的形式。

检查项 1：计算机机房运行管理

基本要求：1、运行管理体系架构是否合理。物理环境/计算机机房管理岗位的设置是否全面，是否与实际管理需求相符合。2、管理制度是否全面有效、制度执行情况如何。管理制度是否覆盖物理环境/计算机机房的运维的各方面，是否定期更新，是否切合实际。了解相关人员的制度执行情况。3、岗位职责设置是否合理，人员职责是否明确，人员资质与能力是否胜任相应的岗位。4、是否执行相关培训计划。5、人员的录用、离岗和考核制度执行情况。

检查方法、步骤：1、通过座谈了解：计算机机房运行管理的体系架构、岗位设置和职责的分工。业务流程和制度的制订和执行情况。 2、通过分析业务流程判断制度和岗位等的设定是否合理、全面。3、约谈一般员工特别是关键岗位员工，判断其对岗位职责、各项制度的理解和执行情况。3、人员的录用、考核等管理情况。

检查项 2：计算机机房选址

基本要求：1、物理建筑应避开易发生火灾和危险程度高的地区，如油库和其他易燃物附近的区域；避开尘埃、有毒气体、腐蚀性气体、盐雾腐蚀等环境污染的区域；避开低洼、潮湿及落雷区域；避开强震动源和强噪声源区域；避开强电场和强磁场区域；避开有地震和水灾危害的区域。2、机房和办公场地应选择在具有防震、防风和防雨等能力的建筑内；3、机房场地应避免设在建筑物的高层或地下室，以及用水设备的下层或隔壁，一般在建筑物的二到三层。应根据设备的外形尺寸、所需工作场地的大小确定主机房面积。主机房净高应为 2.5 到 3.2 米。

检查方法、步骤：1、实地勘察建筑物和计算机机房周围的环境。2、调阅建筑物和机房权威性的检测、验收报告，了解相关情况。

检查项 3：计算机机房基础设施有效性

基本要求：1、供电系统及其负载的冗余性。机房供电应与其它市电供电分开；供电设备的容量应留有余量；应在机房供电线路上配置稳压器和过电压防护设备；提供短期的备用电力供应（如 UPS 设备、UPS 设备是否双回路互备），至少满足设备在断电情况下的正常运行要求（至少 2 小时）；应设置冗余或并行的电力电缆线路为机房设备供电（来自不同变电站的双回路市电供电）；应建立备用供电系统（如备用发电机、备用发电机燃料应充足），备用供电系统应能够自动启动。2、空调系统的有效性和冗余性。计算机机房应采用专用精密空调设备，空调系统的主要设备应有备份，空调设备在能量上应有一定的余量；应尽量采用风冷式空调设备，空调设备的室外部分应安装在便于维修和安全的地方；采用水冷式空调设备时，应设置漏水报警装置，并设置防水小堤，还应注意冷却塔、泵、水箱等供水设备的防冻、防火措施。3、安装在活动地板及吊顶上的送、回风口应采用难燃材料或非燃材料；新风系统应安装空气过滤器，新风设备主体部分应采用难燃材料或非燃材料；机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料。4、消防系统的有效性。机房应设置火灾报警装置，在机房内、基本工作房间内、活动地板下、吊顶里、主要空调管道中及易燃物附近部位应设

置、烟、温感探测器自动检测火情，自动报警，并自动灭火；设置卤代烷 1211、1301 自动消防系统，并备有卤代烷 1211、1301 灭火器；除纸介质等易燃物质外，禁止使用水、干粉或泡沫等易产生二次破坏的灭火剂；机房应采取区域隔离防火措施，将重要设备与其他设备隔离；定期检测消防系统，确保灭火器和灭火剂有效；严禁挤占消防通道的。4、通信及布线系统的有效性。定期维护检修建筑物及机房内的通讯设备，保持通信系统的畅通；机房内值班电话保持畅通；机房线缆应有序部署，线缆标签完整、清晰，标签编码规则应便于保密与内部维护；所有的配线电缆、连接硬件、跳线、连接线等类别必须相一致；机房内所有线缆预先布放至机架内配线架，并在配线架端口上标明对应机架编号；布缆裁剪整齐、美观，所有线缆应标明型号及连接方向；严禁悬空或飞线。5、防盗窃系统有效性。应将主要设备放置在机房内；应将设备或主要部件进行固定，并设置明显的不易除去的标记；应将通信线缆铺设在隐蔽处，可铺设在地下或管道中；应对介质分类标识，存储在介质库或档案室中；应利用光、电等技术设置机房防盗报警系统、监控报警系统。6、防雷系统的有效性。机房建筑应设置避雷装置；应设置防雷保安器，防止感应雷；应设置交流电源地线。7、防水、防潮系统的有效性。水管安装不得穿过机房屋顶和活动地板下；应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透；应采取措施防止机房内水蒸气结露和地下积水的转移与渗透；应安装对水敏感的检测仪表或元件，对机房进行防水检测和报警。8、防静电的有效性。设备应采用必要的接地防静电措施；机房应采用防静电地板；采用静电消除器等装置，减少静电的产生。9、温湿度控制的有效性。机房应设置温湿度自动调节设施，使机房温、湿度的变化在设备运行所允许的范围之内。机房温度变化范围为 18－28℃，湿度变化范围为 40－70%。10、电磁防护系统的有效性。应采用接地方式防止外界电磁干扰和设备寄生耦合干扰，交流工作接地、安全保护接地，接地电阻不应大于 4 欧姆；电源线和通信线缆应隔离铺设，避免互相干扰。电磁场干扰环境场强应满足 GB2887 中的有关要求。11、 在易受鼠害的场所，机房内的电缆和电线上应涂敷驱鼠药剂或设置捕鼠或驱鼠装置。

检查方法、步骤：1、调阅建筑物和机房权威性的检测、验收报告，判断相关指标是否符合国家标准的规定。2、实地勘察计算机机房各项设施的设置、维护和管理是否达标，检查其维护日志中温湿度控制情况（以上所列指标为 A 类机房级别设定，指标详细设定和测量方法

请参照《电子计算机场地通用规范》（GB/T2887-2000），《计算站场地安全要求》GB 9361-88，B 类、C 类机房请参照相关标准）。

检查项 4：计算机机房日常维护

基本要求：1、应对机房的供电系统、空调系统、消防系统 、通信系统、防雷系统、环境检测系统、电磁防护等系统定期检测，实时监控相关设备的运行状况，及时处理设备运行中出现的问题。2、应规范机房存储介质管理，存储介质应存放在上锁的柜子或其他形式的安全器具中；磁介质采取电磁保护。3、应确保机房技术文档、操作档案、操作手册与日志的规范性、完备性和有效性；定期对维护日志、系统监控日志进行分析，发现问题；机房维护变更后，应及时更新技术文档、操作档案、操作手册，并及时告知和培训相关人员；负责人和运维人员通讯录（包括服务商和外部协作单位）应该放置在重要位置；确保关键人员有两种以上有效联系方式，并定期更新。

检查方法、步骤：1、检查计算机机房的日常维护日志、系统监控日志、值班日志、检测报告、技术文档和操作档案，判断其真实性、完备性和有效性。2、实地查看各系统的运行状况，存储介质、日志、文档的保管和使用情况。

检查项 5：机房功能分区

基本要求：1、计算机机房的组成应按计算机设备运行的特点及具体要求确定，一般分为主机房、基本工作间、第一辅助房间、第二辅助房间等；主机房又分为核心设备区，操作区，供电区（UPS 间、电池间、油机间、高压间、变压器间、低压间），钢瓶间，监控间等。2、机房内主要走道宽度≥1.5m，次要走道宽度不小于 0.8m，机架列间间距≥1.0m，两相对机柜正面距离≥1.5m，机柜侧面距墙≥0.5m，当需要维修测试时墙≥1.2m。

检查方法、步骤：1、实地查看机房的功能分区，判断其划分是否合理，是否满足机构实际业务需要。2、实地测量相关距离。

检查项 6：应急预案及演练

基本要求：1、应评估各类事件（如各种报警等）、事故（如供电、消防、UPS、空调发生故障等）和灾害对机房运行的影响，并制定有效的应急处置方案。2、机房应设置应急照明和应急指示系统，并有设有明显标志的疏散出口。3、机房内应明确标识关键部位和系统位置，以便应急时快速定位。4、根据应急预案和应急操作手册对相关人员进行培训，并定期演练。5、定期评估和更新应急预案和应急操作手册。6、机房发生重大事故或案件，机房主管部门应立即向公安机关和银监会或其派出机构报告，并保护现场。

检查方法、步骤：1、调阅应急预案资料，结合业务流程等实际情况，判断应急预案覆盖范围是否足够，业务影响分析是否到位，应急小组的设置、应急预案的启动，应急流程、恢复计划和报告路径是否有效。2、约谈相关人员，确认应急培训是否到位，人员职责是否明晰，第三方服务商是否及时提供应急服务。3、查看应急演练的记录和资料，判断应急演练覆盖的范围是否足够，是否定期进行演练，预案是否定期更新。3、实地勘察应急照明、应急指示系统和疏散出口的设置，并判断其可用性。

14.2 物理环境/计算机机房安全

物理环境/计算机机房安全检查主要是对银行业金融机构的计算机机房及计算机机房所在建筑物的安全管理、物理环境、集中监控、安全区域、消防报警系统、设备安全以及相关安全控制措施的合规性、真实性的检查。通过现场检查及时发现、查处、纠正银行业金融机构在物理环境/计算机机房安全方面存在的问题，督促银行业金融机构规范计算机机房安全管理，防范风险，实现银行业金融机构的物理环境/计算机机房安全运作的目标。

物理环境/计算机机房安全检查采取调阅资料、实地勘察、询问谈话、抽样评估、测试（实质性测试和符合性测试）的形式。

检查项 1：物理环境/计算机机房安全管理

基本要求：1、 应制定机房安全工作的总体方针和安全策略，说明安全工作的总体目标、

范围、原则和安全框架等；应对安全管理活动中的各类管理内容建立安全管理制度；应要求管理人员或操作人员执行的日常管理操作建立操作规程；应指定或授权专门的部门或人员负责安全管理制度的制定；安全管理制度应具有统一的格式，并进行版本控制；应组织相关人员对制定的安全管理制度进行论证和审定；安全管理制度应通过正式、有效的方式发布并定期评估、更新；安全管理制度应注明发布范围，并对收发文进行登记；有密级的安全管理制度，应注明安全管理制度密级，并进行密级管理。2、应设立机房安全管理工作的职能部门，设立安全主管、安全管理各方面的责任人岗位，并定义各责任人的职责。3、应对各类人员进行安全意识教育、岗位技能培训和相关安全技术培训；应对安全责任和惩戒措施进行书面规定并告知相关人员，对违反违背安全策略和规定的人员进行惩戒； 应对定期安全教育和培训进行书面规定；应对安全教育和培训的情况和结果进行记录并归档保存。

检查方法、步骤：1、通过座谈和调阅相关资料，了解机房安全工作的总体方针和安全策略、安全组织架构，操作规程，人员职责以及安全管理制度的相关情况。2、约谈相关人员了解其职责履行、教育培训、安全意识和制度执行情况，判断相关安全工作落实情况。3、检查安全教育和培训情况的记录。

检查项 2：计算机机房的环境安全管理

基本要求：1、建筑物应设置外部边界的保护系统和入侵检测系统 。如运动探测器、振动探测器、光束探测器等；2、包含建筑物和计算机机房的周边在物理上应是安全的（即，在周边或区域内不应存在可能易于闯入的任何缺口）；场地的外墙应是坚固结构，所有外部门要有适当保护以防止未授权进入，例如，控制机制、门闩、报警器、锁等等。3、控制物理访问场地、建筑物的手段要到位，进入场地或建筑物应仅限于已授权人员。4、安全边界的所有防火门应可发出报警信号、被监视并经过检验，应紧闭。它和墙一起按照合适的地方、国内和国际标准建立所需的抵抗程度。5、如果需要，物理屏障应从计算机机房真正的地板（包括地板和地板下的空间）扩展到真正的天花板（包括天花板和天花板上的空间），以防止未授权进入和由诸如火灾和水灾所引起的环境污染。6、应指定专门的部门或人员定期对机房供配电、空调、温湿度控制等设施进行维护管理。7、应指定部门负责机房安全，并配备机房安全管理

人员，对机房的出入、服务器的开机或关机等工作进行管理。8、应建立机房安全管理制度，对有关机房物理访问，物品带进、带出机房和机房环境安全等方面的管理作出规定。9、应加强对办公环境的保密性管理，规范办公环境人员行为，包括工作人员调离办公室应立即交还该办公室钥匙、不在办公区接待来访人员、工作人员离开座位确保终端计算机退出登录状态和桌面上没有包含敏感信息的纸档文件等。10、应对机房和办公环境实行统一策略的安全管理，对出入人员进行相应级别的授权，对进入重要安全区域的活动行为实时监视和记录。11、应采用清理桌面和清空屏幕策略。12、标识敏感信息处理设施位置的目录和内部电话簿不要轻易被公众得到。

检查方法、步骤：1、实地检查建筑物的保安情况、保安设施和保安措施是否到位，是否符合标准。检查人员访问授权情况。2、实地检查建筑物和机房的安全周边是否符合标准要求。查看安全周边系统定期维护记录和检修记录。3、通过实地查看、约谈和调阅相关资料（日志记录等），检查计算机机房、相关设施、存储介质和相关敏感信息的安全维护和管理是否到位。

检查项 3：计算机机房集中监控系统

基本要求：1、应通过值班等制度，确保通信线路、环境监控系统、防盗监控系统等 7*24 小时有效运做，形成记录并妥善保存。实时监控的监控内容的内容至少保存 3 个月,非定时监控至少 3 年；有实时交易服务的数据中心应实行 24 小时值班，值班人员至少有二名工作人员。2、应组织相关人员定期对监测和报警记录进行分析和评审，发现可疑行为，形成分析报告，并采取必要的应对措施；3、应制定监控系统报警后事件处理程序与流程，并对相关人员进行培训。

检查方法、步骤：1、查看计算机机房监控和值班的记录和日志，检查计算机机房监控和值班的相关制度落实情况。2、就监测和报警记录分析情况约谈相关人员，判断其做法是否有效。3、查看监控系统报警后事件处理程序与流程是否合理有效，并检查相关人员的执行情况。

检查项 4：计算机机房安全区域访问控制

基本要求：1、关键和敏感的业务信息处理设施要放置在安全区域内，并受到一种已定义

的安全周边和适合的安全屏障和入口控制的保护。这些设施要在物理上避免未授权访问、损坏和干扰。2、安全区域访问用户和权限的管理应由专门部门执行。对安全区域的访问者要予以监督或办理进入手续，并记录他们进入和离开的日期和时间。只能允许他们访问特定的、已授权的目标，并要向他们宣布关于该区域安全要求和必要的应急规程的说明。访问敏感信息和信息处理设施要受到控制，并且仅限于已授权的人员。鉴别控制(插卡加个人识别号)应用于授权和确认所有访问。所有访问的审核踪迹要安全地加以维护。要求所有人员佩带某种形式的可视标识，并且鼓励他们询问无人护送的陌生人和未佩带可视标识的任何人。对安全区域的访问权利要定期地予以评审和更新。3、机房应具有独立的出入口。机房出入口应安排专人值守并配置电子门禁系统，控制、鉴别和记录进入的人员；需进入机房的来访人员应经过申请和审批流程，并限制和监控其活动范围；应对机房划分区域进行管理，区域和区域之间设置物理隔离装置，在重要区域前设置交付或安装等过渡区域；重要区域应配置第二道电子门禁系统，控制、鉴别和记录进入的人员。4、交付或安装等过渡区域应设计成：即在无需交货人员获得进入本建筑物其他部分的情况下就能卸下物资。当内部的门打开时，交接区域的外部的门应紧闭。在进来的物资从交接区域运到使用地点之前，要检查有潜在危险的进来物资。如果合适，进来的物资应在场地的入口处进行登记。由建筑物外进入交接区限于已标识的和已授权的人员。

检查方法、步骤：1、判断计算机机房安全区域的划分、交付或安装等过渡区域设置是否合理，各区域是否有效运做。2、了解计算机机房访问人员授权的情况，检查有无过期和无效的授权。3、通过实地检查和查看日志记录，检查安全区域的物理防护和访问控制是否有效防御非授权物理访问、破坏和干扰。4、是否根据所运行业务重要性将机柜分类管理，保障访问合法性。5、外来设备（如电信设备）与内部设备是否分区放置，确保维护安全。

检查项 5：机房设备安全

基本要求：1、设备应进行合理安置，以尽量减少不必要的工作区域访问。2、对设备有专门登录、维护和操作记录，记录应实现自动化，对记录应妥善保管。3、在未经授权的情况下，不应让设备、信息或软件离开安全区域。若需要并合适，要对设备作出外挪的记录，当

返回时，要作出送回的记录。为了检测未授权的财产移动，要进行抽查。要让每个人都知道将进行抽查。4、离开建筑物的设备和存储介质在公共场所应派人值守。5、制造商保护设备用的说明要始终加以遵守。6、进入机房的电源和电信线路宜在地下。计算机系统的各设备走线不得与空调设备、电源设备的无电磁屏蔽的走线平行。交叉时，应尽量以接近于垂直的角度交叉。为了防止干扰，电源电缆要与通信电缆分开。7、网络布缆要免受未授权窃听或损坏。

检查方法、步骤：1、通过约谈相关工作人员和检查设备维护日志，检查设备维护流程和维护情况是否满足安全要求。2、查看设备的安置情况、维护和操作记录情况，检查放置区域，用电环境、布线，值守情况是否满足安全要求。3、查看有无设备外挪的管理记录，有无抽查记录。抽样检查外挪设备的管理。

15. 网络通信

网络及通讯技术是银行业金融机构 IT 架构的基础部分，也是确保其业务正常运营的关键因素，在网络规划、建设、运行、维护、监控及退出过程中由于技术和管理缺陷都有可能产生操作、法律和声誉方面的风险，给银行业金融机构利益带来一定的损失。

15.1 内控管理

检查项 1：内控制度

基本要求：银行业金融机构应建立健全网络管理相关的内部控制规章制度、技术规范、操作规程等，加强对网络的管理和控制，拥有对硬件、应用系统、网络和通讯系统的获取、开发或维护进行指引的正式的方法或流程。

检查方法、步骤：1、面谈：包括银行业金融机构信息科技主管领导和内控合规部门及内部审计部门对于网络安全的内控制度制定情况，内部控制监督、完善程序，相关绩效考核目标，对谈话中的一些关键内容记入工作底稿；2、调阅银行业金融机构文件汇编，调阅信息科技方面的管理制度，查阅被查单位的网络拓扑图，了解对网络安全管控的内控制度情况；

检查项 2：人员管理

基本要求：相关工作的人员应符合以下要求：1、具备良好的职业道德，掌握履行网络系统相关岗位职责所需的专业知识和技能；2、未经岗前培训或培训不合格者不得上岗,经考核不适宜的工作人员，应及时进行调整。

检查方法、步骤：1、调阅人力资源部门相关网络管理人员的信息，查阅相关的人员信息和培训记录以及绩效考核记录；2、调阅统一授权管理的相关文档资料，查阅网络管理人员的角色、分工和授权情况；3、查看相关设备的操作日志；4、调阅值班记录进行查看。

检查项 3：授权管理

基本要求：1、应明确网络通信管理部门的职责，根据制度设置相应的岗位职责并配备相关的管理人员。如设置网络基础设施管理、网络监控、网络应用管理、网络用户管理、网络安全保密管理、网络机房管理等岗位，明确岗位职责权限； 2、重要的网络管理岗位应试行 A/B 角色制，对要害岗位的人员，至少有两名人员备用、替换，确保在任何情况下，都不会因人员的缺岗而影响整个系统的正常运行； 3、应能够落实重要岗位人员强制休假制度。

检查方法、步骤：调阅统一授权管理的相关文档资料，查阅网络管理人员的角色、分工和授权情况，对于建立了统一认证登录管理系统的机构，登录服务器查看相关的权限分配信息。

检查项 4：口令管理

基本要求：1、网络管理人员的操作口令的管理策略是否执行；2、应及时更改网络设备或相关网络管理系统缺省口令；3、口令应该定期更换；4、应对口令周期、存储、长度、加密强度做出明确要求并通过一定的技术手段实现，应避免使用弱口令（注：弱口令是设置过于简单并且非常容易被破解的口令或密码）。

检查方法、步骤：检查口令策略是否执行。

检查项 5：第三方管理

基本要求：1、应对第三方服务供应商订立服务合同，对参数配置等信息保密做出约束；2、应确保在外部人员访问受控网络区域前先提出书面申请，批准后由专人全程陪同或监督，并登记备案；3、对外部人员允许访问的区域、网络设备等内容应进行书面的规定，并按照规定执行。例如外来人员对网络的检查，厂商人员对网络设备维护、更换等行为都要有良好的管理办法。

检查方法、步骤：检查第三方管理办法，订立的合同。

检查项 6：服务外包

基本要求：1、外包方评估和资质。对外包承包方评估机制，充分审查、评估承包方的经营状况、财务实力、诚信历史、安全资质、技术服务能力和实际风险控制与责任承担水平，并进行必要的尽职调查；2、外包合同。与承包方签订书面合同，明确双方的权利、义务，并规定承包方在安全、保密、知识产权方面的义务和责任；3、服务外包的信息保密要求。 银行业金融机构将敏感的信息系统，以及其他涉及国家秘密、商业秘密和客户隐私数据的管理与传递等内容进行外包时，应遵守国家有关法律法规，符合银监会的有关规定，经过董事会或其他决策机构批准，并在实施外包前报银监会及其派出机构和法律法规规定需要报告的机构备案。

检查方法、步骤：检查外包合同，第三方协议或互惠协议，获得使用的网络软件列表和使用许可，关注其中的条款。检查敏感数据的加密传输控制策略，检查网络工程的外包合同，关注风险点基本要求，具体可参照手册服务外包管理部分。

检查项 7：文档管理

基本要求：1、识别是否对硬件、应用系统、网络和通讯系统的获取、开发或维护采用了正式的文档化的策略，评估策略的适当性；2、检查拓扑结构图、各项操作文档、配置文档、及备份文档是否完备、齐全；3、文档是否放置在安全的场地；4、文档管理是否考虑到灾难

备份的要求，重要的操作手册、配置文档、变更文档应该在灾备中心得到妥善的管理。

检查方法、步骤：检查网络通信系统各项文档是否完备，包括故障处理手册、应急手册、配置手册、配置文档等，检查文档是否及时更新，检查文档的保管情况。

检查项 8：审计和检查

基本要求： 1、首先要建立审核规定，明确审核的周期和时间，每次审核前需要制定审核的计划和内容，针对技术和管理两大方面的具体要求，制定审核项目的检查列表，方便审核工作的开展，每次审核结束后要生成审核报告； 2、安全管理员应负责定期进行安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况； 3、应由内部审计人员或聘请外部机构定期进行网络风险进行审计，审计或检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等； 4、应汇总安全检查数据，形成安全检查报告，并对安全检查结果进行通报； 5、应制定安全审核和安全检查制度规范安全审核和安全检查工作，定期按照程序进行安全审核和安全检查活动。

检查方法、步骤： 1、应调阅安全检查制度，安全检查报告，安全检查过程记录，安全检查表格。应访谈安全管理员，询问是否定期进行全面安全检查，检查周期多长，安全检查包含哪些内容，检查人员有哪些，检查程序是否按照系统相关策略和要求进行，是否制定安全检查表格实施安全检查，检查结果如何，是否对检查结果进行通报，通报形式、范围如何；2、应检查安全检查制度文档，查看文档是否规定检查内容、检查程序和检查周期等，检查内容是否包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等，内容是否包括系统日常运行、系统漏洞和数据备份等情况；3、应检查安全检查报告，查看报告日期与检查周期是否一致，报告中是否有检查内容、检查人员、检查数据汇总表、检查结果等的描述；4、应检查安全检查过程记录，查看记录的检查程序与文件要求是否一致；5、应检查审计分析报告，查看报告日期与检查周期是否一致，报告中是否有分析人员、异常问题和分析结果等的描述，是否对发现的问题提出相应的措施；6、应检查是否具有安全检查表格。

检查项 9：风险评估

基本要求：银行业金融机构应该定期地对网络的安全脆弱性进行评估。

检查方法、步骤：询问管理人员是否定期进行安全评估，了解评估机构的资质和评估的范围，调阅相关的安全评估报告进行查看。

检查项 10：剩余风险控制

基本要求：1、虽然实施了 IT 安全控制措施，但应定期对剩余的风险进行评估；2、银行业金融机构 IT 管理部门应对内部或外部审计的提出问题或风险根据风险管理目标进行改进，减少剩余风险，对于改进情况应有文档记录，对未进行改进的风险应说明原因并给出改进的计划；3、内部审计部门应进行必要的后续跟踪，降低剩余风险。

检查方法、步骤：1、确认被查单位是否定期进行内部审计，确认中介机构和内部审计部门的对网络审计的频率和范围及相关评估报告，调阅中介机构和内审部门出具的审计报告和评估报告，关注其中的风险点；2、对网络事件或问题的管理是否按照相关制度执行，是否按照被查机构的业务流程进行，有无违章操作，查看被查单位对于违章操作的处理措施，分析可能存在的风险；3、被查单位按照内外部审计要求进行整改的措施，相关文字记录、文档。对于已经整改的问题查看是否有相关的文字记录，对于未整改的问题，向被查机构了解原因，分析存在的剩余风险；4、对内控制度落实不到位的处理措施，查阅相关责任处理记录。

15.2 运行维护

检查项 1：运行监控

基本要求： 1、应建立网络运行情况集中管理监控平台； 2、应合理地配置交换机、路由器、IDS、防火墙等网络设备监控策略。网管系统管理的设备应正确的配置了网管协议，网管系统能够监测到网络设备的信息，记录相关网络设备的拓扑，提示故障； 3、网络监控工具应该被合理的使用，设备监控是否经过有权人的审批，防止监控工具的滥用； 4、运行监控应能够按照常见的攻击特点侦测异常的网络活动。

检查方法、步骤：1、实地进入运行监控中心，查看网络运行监控的情况，调阅相关运行日志进行查看；2、了解监控阀值的定义，监控的有效性，查看监控平台，调阅监控日志文件；3、了解对网络监听、诊断工具的使用策略，查看网络监听、诊断工具的使用日志，使用范围。

检查项 2：性能监控

基本要求：1、应能够对网络的性能进行监控，监控平台包括设备运行情况的监控，定义阀值，能够统计 CPU 占有率，内存占有率，数据转发等参数性能监控参数，数据中心核心设备与各分区汇聚设备链接链路总流量及各业务流量的监测；2、网络及备份设施是否满足高可用性要求，包括硬件、软件的高可用性的要求；

检查方法、步骤：查看性能监控平台和性能监控的统计报告。

检查项 3：流量监控

基本要求：是否能够对网络流量进行持续的监控，应能够对异常流量进行识别、分析并采取相应的应对措施，如异常流量的源头分析、清洗等措施。

检查方法、步骤：从现有网络中获取更为详细的网络管理报表，如：协议的流量分布等。可以透视企业内部网络运作情况，对网络流量可以做到一目了然。

检查项 4：性能调优

基本要求：是否针对网络监控的情况对网络系统进行性能优化，确保网络运行的稳定和效率，包括线路升级、软硬件参数优化调整等。对于设备调优等操作应该制定指导方案，指定软件版本，对设备配置参数进行指导，同时制定割接方案，重大调整、割接时刻应能够进行外部的现场支持。

检查方法、步骤：调阅性能调优的指导方案，查看相关性能调优操作的日志记录。

检查项 5：监控预警

基本要求：网络管理监控平台应该能够自动响应网络安全事件，包括控制台报警，记录

网络安全事件的详细信息，并提示系统安全管理员采取一定的安全措施。

检查方法、步骤：实地查看监控预警平台的工作情况，调阅监控预警的记录文档。

检查项 6：事件管理

基本要求：1、应建立对网络设备或通信中出现的事件、问题的发现和响应机制，健全管理制度，定义事件响应的流程，对于事件或问题应被完整记录；2、应该对紧急事件提供紧急响应服务，并按流程和操作手册进行处理，如黑客入侵、病毒救治、灾难恢复、设备抢修和通信故障等紧急情况的相应。其中黑客入侵响应包括追踪黑客踪迹，分析入侵记录，总结入侵报告，紧急修复引起入侵的漏洞。病毒救治应分析造成病毒施虐的系统原因，挽救由于病毒损坏的数据。灾难恢复应分析灾难引发的原因，挽救灾难带来的数据丢失，进一步实现系统恢复，总结灾难报告。设备抢修包括现场检查故障设备，调试解决由于软件引起的故障，返回厂家检修，重新实施替代设备，加强安全性管理等。通信故障包括 现场检查通信线路故障，采用电信级故障检测仪分析解决由于软件或硬件引起的故障所在，及时书面报告客户；3、应该能够对运行问题、变更问题、历史故障等进行分析。

检查方法、步骤：查阅值班日志和调阅网络事件或问题的记录，查阅记录是否完整，查阅处理的措施是否合规，是否按照被查机构的业务流程进行，有无违章操作，是否按照报告路线向上报告。

检查项 7：运行检查

基本要求：1、是否定期通过对网络中运行的路由器和交换机设备使用专业工具进行设备状态信息的收集，然后对收集到的数据进行汇总分析来检查网络设备中主要硬件的运行情况、软件运行和配置情况、以及设备的负载情况；2、检查内容分为网络设备硬件运行情况检查，网络设备的软件运行情况检查，网络设备负载情况检查三个部分。对于硬件的检查应该涉及到单板的状态检查、电源模块状态检查、风扇状态的检查、整机指示灯状态检查、机框防尘网检查、机房温湿度以及设备地线的检查。软件运行及设备负载情况的检查应该涉及到设备运行情况的检查、路由运行情况检查、网络报文分析、流量分析、设备对接运行状况检查等

方面；3、检查结果应该具备相关的文档记录。

检查方法、步骤：查阅相关运行检查文档记录。

15.3 网络变更管理

检查项 1：变更计划

基本要求：1、应制订严密的变更处理流程和计划，明确变更控制中各岗位的职责，并遵循流程实施控制和管理；2、变更前应明确应急和回退方案；3、应确保网络通信设备的配置变更操作的安全。查看变更流程是否有申请、审批、双人操作、失败回滚和测试等保障措施。

检查方法、步骤：调阅相关变更的日志记录等资料，访谈网络管理员，了解变更管理方案和流程，了解变更操作对业务持续的影响分析；

检查项 2：变更审批

基本要求：1、用户和其他对网络基础架构和通讯软件进行变更的请求由管理层进行了审批，包括升级和厂商提供的修正版本。实施过程应与信息系统计划和管理的意图相符。以下审批是适用的：变更请求、业务/IT 审批、测试计划审批、测试结果/用户接收度的正式批准、迁移审批、实施审批、实施完工情况的审批；2、根据变更需求、变更方案、变更内容核实清单等相关文档审核变更的正确性、安全性和合法性；3、网络管理人员无授权不得进行变更操作。

检查方法、步骤：确认客户的网络变更管理流程。如，以下审批是适用的：变更请求;业务/IT 审批;测试计划审批;测试结果/用户接收度的正式批准;迁移审批;实施审批; 实施完工情况的审批;评估变更文档以证明其变更及时实施。

检查项 3：配置和策略变更

基本要求：是否定期对漏洞扫描系统知识库和检验规则和防火墙系统策略进行定期升级，集中监控和网络设备（交换机、防火墙、路由器、负载均衡器等）配置策略的变更，应保证

网络安全策略和规章制度一致。

检查方法、步骤：检查配置和策略的变更是否和业务目标相一致。

检查项 4：设备变更

基本要求：1、网络设备操作系统软件和网络管理软件版本变更前应保留一定期限的备份版本，保留所有历史的变更内容核实清单和记录；2、网络通信设备软件的变更是否覆盖到了备份网络设备系统；3、网络硬件设备替换后应得到妥善保管，防止网络配置信息的泄漏。

检查方法、步骤：查看相关设备硬件和软件的变更记录，包括网络设备硬件的增加，替换，移除是否经过了管理人员批准，网络设备操作系统软件升级是否经过测试，是否经过审核，备份设备的软硬件是否进行了相应的升级变更，升级完成后是否有升级前的软件备份版本。查阅并比较相同设备主设备和备用设备的软件版本。

检查项 5：变更测试

基本要求：现有网络和通讯软件在正式实施之前在测试环境中进行了初始安装和评估。

检查方法、步骤：确认网络变更流程和一个网络变更的例子，以及变更迁移到生产环境中之前已经在独立的测试环境中进行了测试。

15.4 网络服务连续性

检查项 1：连续性计划

基本要求：1、应明确网络连续性计划中组织结构、人员、岗位职责分工和事件处置流程及报告路线；2、 检查是否制定网络系统的应急预案，并定期演练、评审和修订。应根据信息系统总体规划，制定明确、持续的网络风险管理策略，按照信息系统的敏感程度对各个集成要素进行分析和评估，并实施有效控制；3、银行业金融机构应采取措施防范自然灾害、运行环境变化等产生的安全威胁，防止各类突发事故和恶意攻击。

检查方法、步骤：1、调阅被查机构的 BCP 文档，关注计算机通信网络的连续性计划，

详见业务连续性计划检查手册部分；2、查阅被查机构应对突发事件的处置策略文档，查阅相关处置日志或记录。

检查项 2：业务影响分析

基本要求：是否根据网络服务情况对重要业务保障程度进行分析和评估，评估网络对业务的影响程度并确定保障的优先顺序。

检查方法、步骤：检查是否进行业务影响分析，业务影响是否充分考虑到网络服务的要求，参看业务连续性检查手册。

检查项 3：应急管理

基本要求：1、应制定网络系统管理的应急预案；2、应急管理中应按照信息资产重要程度、业务重要性等要求制定应急保障顺序；

检查方法、步骤：查阅网络应急预案。

检查项 4：容量管理

基本要求：1、应保证主要网络设备的业务处理能力具备冗余空间，满足业务高峰期需要；2、应保证网络各个部分的带宽具备冗余空间，满足业务高峰期需要；

检查方法、步骤：查看重要网络设备的流量统计报告，对带宽的 QOS 保障策略，是否按照业务和交易流量要求保证传输带宽，对突发高峰流量的监测预警措施和应对措施。

检查项 5：冗余管理

基本要求：1、重要的网络设备和通讯线路应采取冗余备份措施，防止因单点故障而影响整个网络的正常运行，提高网络的可靠性。应与通讯线路供应商签订严格的线路租用合同，保证网络系统和生产业务能够持续不间断地运行。通讯线路和备份线路尽量选用不同通讯公司的线路；2、重要网络管理人员冗余，备份人员是否经过培训，具备同样的运维管理能力；

3、相关网络配置应有备份，备份配置被严格管理，网络设备的操作手册及配置异地备份，使用得到严格的控制；4、对生产网络设备的漏洞更新和软件升级是否覆盖到备份网络设备，对于热备份网络设备和冷备份设备以及不同型号的备份设备的软件更新管理；5、网络系统是否考虑到第三方的支持，包括网络通信运营商和设备厂商的支持，第三方互惠协议。

检查方法、步骤：1、检查网络设备或备件和线路是否冗余备份，查阅运营商线路租用合同，通讯线路和备份线路尽量选用不同通讯公司的线路，对于同一运营商要关注冗余线路是否来自于不同的接入局；2、网络安全管理人员的冗余情况，关注备份网络安全管理人员的资质及培训记录；3、建立完善的网管中心，监测和管理通信线路及网络设备，保障网络安全稳定运行；4、查阅被查机构应对突发事件的应急处置策略文档（应急预案），查阅相关处置日志或记录；5、查阅备份冗余设备切换的演练记录；6、查看重要网络设备的流量统计报告，对带宽的 QOS 保障策略，按照业务和交易流量要求保证传输带宽；7、查看相关备份设备、文档、配置文件的保管情况，使用及变更记录；8、了解被查机构制定的业务恢复的 RTO 和 RPO 指标，查看相关故障记录。详细的检查方法可以参照手册中业务连续性和灾备的检查部分。

检查项 6：带外管理

基本要求：1、对灾备中心和无人值守的网络设备是否能够进行集中带外管理；2、带外管理应该满足安全性、可靠性等要求。

检查方法、步骤：调阅网络拓扑结构图，查看网络管理区域的拓扑结构，访谈网络管理员，是否能够进行带外管理，检查带外管理登录认证服务器日志，检查带外管理服务器的相关安全配置。

检查项 7：压力测试

基本要求：应能够定期对网络系统的压力进行测试。

检查方法、步骤：检查压力测试报告，检查是否进行压力测试，调阅相关压力测试报告，确认压力测试的结果，测试报告的权威性。

检查项 8：应急演练

基本要求：应定期对应急计划进行测试和确认。

检查方法、步骤：查阅相关培训记录和业务连续性管理的演练记录。

检查项 9：灾备要求

基本要求：1、应建立异地灾备中心，制定网络系统的灾难备份方案；2、对网络设备、线路进行异地应备份满足灾备的要求；3、应制定在发生紧急情况下，网络的替代措施和切换方案；4、灾难发生时，第三方服务商是否准备就绪。

检查方法、步骤：检查灾备方案，确认灾备实施情况。

检查项 10：服务中断的管理

基本要求：计算机网络通信系统的中断可能影响客户服务时，应由相关部门以适当方式告知客户。

检查方法、步骤：访谈管理员，询问网络服务服务中断，是否由相关部门通知客户。

15.5 网络安全

检查项 1：结构安全

基本要求：1、应按照不同部门、不同业务需求以及信息系统的类别和重要性，评估应用程序和用户组的关键程度，将网络划分为不同的逻辑安全域，合理划分虚拟网络（V-LAN），有效隔离生产业务网络与开发测试网络、生产业务网络与办公网络、内部网络与外部网络等，以便采取不同的安全策略和保护措施。应对接入国际互联网采取可靠的隔离手段，实施有效的安全管理；2、应在业务终端与业务服务器之间进行路由控制建立安全的访问路径；3、网

络拓扑结构规划是否合理，路由协议规划是否合理，网络容量规划是否满足需要；4、IP 地址规划是否合理，应根据各部门的工作职能、重要性和所涉及信息的重要程度等因素，划分不同的子网或网段，并按照方便管理和控制的原则为各子网、网段分配地址段；5、是否进行网络安全规划，应避免将重要网段部署在网络边界处且直接连接外部信息系统，重要网段与其他网段之间采取可靠的技术隔离手段；6、Qos 规划是否合理，应按照对业务服务的重要次序来指定带宽分配优先级别，保证在网络发生拥堵的时候优先保护重要主机；7、是否进行网络管理的规划，网络是否具有带外管理的能力。

检查方法、步骤：1、调阅文件资料，具体包括银行业金融机构董事会等高级管理层对 IT 的战略规划，包括网络建设的规划、预算、工程建设的决议和文件，可以在被查单位的文件汇编、高管层关于 IT 系统的决议文件、会议纪要及 OA 中进行查阅；2、查阅被查单位的网络拓扑图，包括网络逻辑拓扑和数据拓扑，对网络架构、数据架构、应用架构进行分析，并要求被查单位对网络拓扑进行介绍说明；3、访谈安全管理人员，了解组织对安全的整体构想和规划。访谈信息系统技术维护人员，从技术维护角度出发，了解他们对安全需求的看法。访谈信息系统业务使用人员，从应用的角度出发，了解他们对安全需求的看法；4、根据网络拓扑图，查看被查机构是否按照结构化层次设计的要求进行各功能分区的设置，对各功能分区进行隔离，查阅网络协议的规划情况，了解网络协议的选择，查看网络 IP 地址段的划分情况，IP 地址的分配策略和控制要求；5、了解网络协议的选择要求，生产网和办公网等的网络协议选择，对于可靠的传输和不可靠传输的协议需求，判断网络协议的选择覆盖是否足够；6、检查被查机构对网络带宽的控制，是否进行了压力测试，压力测试的流程和工具，是否按照业务的优先程度网络进行 Qos 保障，Qos 的保障策略情况；7、查阅核心业务区防火墙的设置策略，了解核心和骨干路由器对业务流量的保障程度，必要时要求被查单位提供 Qos 的配置进行查阅；8、检查是否有采取虚拟网关冗余等技术，是否配置了路由热备份协议，保证线路的冗余。

检查项 2：物理安全

基本要求：确保网络通信机房物理安全，网络机房所有警报和监视保安设备是充分地可

使用和充分地维护。应确保通信线路的安全，是否电磁屏蔽，网络布线是否合理，线路防监听防电磁泄漏的措施，应对无线网络环境进行管理控制。

检查方法、步骤：1、通信机房的检查,详见手册物理环境的检查部分（包括电力供应、电源、空调湿度、防尘、防火、防水及其他威胁），应确认以下事项：温湿度是否在允许范围；静电保护是否到位；防火设施是否充足可用；是否存在把饮料等液体带入机房的情况；是否存在在机房内吸烟的情况；2、调阅被查机构网络布线图，实地查看网络布线是否合理，线路标记是否清晰，重要线路光缆/电缆布设、加密传输情况，无线网络有无屏蔽干扰设备；3、调阅被查机构对于无线网络的使用策略文件，在这种情况下，应执行风险评估识别控制措施(例如，强认证、密码手段和频率选择)，以维持网络隔离；4、调阅相关的监控录像资料。

检查项 3：传输安全

基本要求：1、保证通信链路的可用性，可靠性，通讯双方的链路机制一样；网络链路的数据传输应满足数据完整性、可靠性和抗抵赖性等要求，关键链路是否进行加密传输；2、敏感数据传输必须采用加密技术（链路加密、PPTP、IPSec、VPN 等）；3、重要的 E-mail 应采取加密；4、应根据数据的敏感标记允许或拒绝数据通过；5、应不开放远程拨号访问功能，开放网络带外拨号访问管理应采取严格的访问控制措施。

检查方法、步骤：1、询问管理人员，了解广域网和局域网重要传输链路采用的通信协议，如广域网重要的 HDLC 或 ATM 链路是否采用加密机进行加密传输，对于重要的应用服务，应避免使用 UDP 协议等不可靠连接的传输协议；2、询问管理人员对银行 POS、ATM 自助机具、网上银行的等敏感数据的加密技术；3、查阅互联网 E-mail 和内网 E-mail 的相关规定，了解重要的信息是否通过 E-mail 进行，信息是否经过加密处理。

检查项 4：访问控制

基本要求：1、应在网络边界对公共网络出口、与第三方机构网络联接出口、DMZ 区域部署防火墙等访问控制设备，启用访问控制功能；应合理配置防火墙等网络安全设备，根据实际业务需求，制定合理的安全策略；应对不同逻辑安全域之间的互相访问进行有效控制，

合理配置访问控制列表（ACL）。应采取 MAC 地址、交换机端口、IP 地址绑定等方式，严格管理跨不同逻辑安全域的主机或设备。应在会话处于非活跃一定时间或会话结束后终止网络连接；重要网段应采取技术手段防止地址欺骗；2、应不允许数据带通用协议通过；3、应根据数据的敏感标记允许或拒绝数据通过；

检查方法、步骤：1、访谈安全管理员，检查，测试边界网络设备。应访谈安全管理员，询问网络访问控制的措施有哪些；询问访问控制策略的设计原则；询问访问控制策略是否做过调整，以及调整后和调整前的情况如何；应检查边界网络设备，查看是否有相应的访问控制措施来实现禁止数据带通用协议通过；应测试边界网络设备，可通过发送带通用协议的数据（如使用 http 隧道工具），测试访问控制措施是否有效阻断这种连接。2、抽查为主要业务应用所开放的端口和配置的访问路径，查看业务应用所使用网络服务是否进行最小授权；3、查看网络服务访问许可的审批文档和操作记录，如要求被查机构网络管理人员进入相关边界网络的防火墙日志系统，查阅相关访问日志，要求管理员调阅设备的访问控制策略，查看策略是否与审批文档一致；4、检查是否有对重要核心应用的网络访问控制策略，如对核心主机以及相关存储网络的保护策略；5、查阅网络交换机的配置策略，接入层、汇聚层、骨干及核心交换机的配置，检查是否进行 VLAN 的划分，VLAN 的划分是否覆盖重要业务需要，划分是否合理；6、询问管理人员是否对不同逻辑安全域之间的互相访问进行有效控制（如访问控制列表(ACL)）；7、了解被查机构网络路由控制策略是否与业务应用系统的访问控制策略相符；8、检查交换机路由器的口令是否启用了加密功能，重要的网络路由表更新是否启用加密；9、询问网络管理员是否配置了路由器远程拨号登录，拨号网络是否在拓扑图中标识。

检查项 5：接入安全

基本要求：应进行网络核证，以确保网络设备及基础设施的增补或变动，不会导致网络其它部分容易出现问题。组织边界的网络，应限制用户联接的能力，并与业务应用系统的访问控制策略和要求一致。

检查方法、步骤：调阅被查机构针对网络接入管理的制度办法，访谈网络管理员针对网络接入采取的管理措施，是否能够对非授权设备私自联到内部网络和不允许外联的设备联接到外部网络的行为进行监测并采取相应的管控措施。如，对于不开放远程拨号访问的检查，可以检查电话线路是否能够进行拨号，检查是否有相关的内部网络外联检测设备，对外联检查系统的规则设定进行排查。

检查项 6：网络边界安全

基本要求：1、应采取但不限于接入边界控制、防火墙、恶意代码过滤等技术方式，控制对不同逻辑安全域的网络接入和访问。防火墙包括但不限于包过滤防火墙、状态检查防火墙、代理服务器防火墙和应用层防火墙等。应合理配置防火墙，制订合理的安全策略；2、应在网络边界处监视以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP 碎片攻击和网络蠕虫攻击等；3、跨境网络应采用必要的安全措施，如增加防火墙，增加访问控制等。

检查方法、步骤：1、访谈网络管理员，了解网络边界控制策略，防火墙、恶意代码过滤等技术方式，控制对不同逻辑安全域的网络接入和访问。防火墙包括但不限于包过滤防火墙、状态检查防火墙、代理服务器防火墙和应用层防火墙等。应合理配置防火墙，制订合理的安全策略。2、应在网络边界处监视以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP 碎片攻击和网络蠕虫攻击等；3、跨境网络应采用必要的安全措施，如增加防火墙，增加访问控制等。

检查项 7：入侵检测防范

基本要求：1、重要业务网段应当部署入侵检测和防御系统以保证在第一时间检测到攻击的发生，可能的情况下与防火墙联动实时阻断攻击；2、当检测到攻击行为时，应记录攻击源 IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警，网络管理人员应采取相应防御动作。

检查方法、步骤：1、应访谈安全管理员，询问网络入侵防范措施有哪些；是否有专门设备对网络入侵进行防范；询问网络入侵防范规则库的升级方式；2、应检查网络入侵防范设备，查看是否能检测以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP 碎片攻击、网络蠕虫攻击等入侵事件；3、应检查网络入侵防范设备，查看入侵事件记录中是否包括入侵的源 IP、攻击的类型、攻击的目的、攻击的时间等；查看是否设置了安全警告方式（如采取屏幕实时提示、E-mail 告警、声音告警等）；4、应检查网络入侵防范设备，查看其规则库是否为最新；5、应测试网络入侵防范设备，验证其监控策略是否有效（如模拟产生攻击动作，查看网络入侵防范设备的反应）；6、应测试网络入侵防范设备，验证其报警策略是否有效（如模拟产生攻击动作，查看网络入侵防范设备是否能实时报警）。7、检查被查机构是否配备了网络故障诊断工具，查看监控工具的使用日志。

检查项 8：恶意代码防范

基本要求：1、应在网络边界处对恶意代码进行检测和清除；2、应维护恶意代码库的升级和检测系统的更新。

检查方法、步骤：1、访谈安全管理员，了解被查机构采用防恶意代码产品，询问网络恶意代码防范措施是什么，询问恶意代码库的更新策略；2、应检查网络设计/验收文档，查看其是否有在网络边界及核心业务网段处对恶意代码采取相关措施的描述（如是否有防病毒网关），防恶意代码产品是否有实时更新功能的描述；3、应检查在网络边界及核心业务网段处是否有相应的防恶意代码措施；4、应检查防恶意代码产品，查看其运行是否正常，恶意代码库是否为最新版本。5、检查是否运用网络防病毒进行病毒的防范，网络防病毒的措施，是否对影响网络使用效率的事件进行分析。

检查项 9：网络设备防护

基本要求：1、应对登录网络设备的用户进行身份鉴别；2、应对网络设备的管理员登录地址进行限制；3、主要网络设备应对同一用户选择两种或两种以上组合的鉴别技术来进行身份鉴别；4、身份鉴别信息应具有不易被冒用的特点，口令应有复杂度要求并定期更换；5、

网络设备用户的身份鉴别信息至少应有一种是不可伪造的；6、应具有登录失败处理功能，可采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施；7、当对网络设备进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听；8、应实现设备特权用户的权限分离。9、网络设备用户的标识应唯一；10、重要安全设备如加密机、防火墙等产品还应符合国家信息安全的相关规定。作为安全设备，防火墙具有其本身的敏感性。所选择的防火墙产品，必须经过国家相关权威部门的认证和销售许可，这些认证包括公安部和信息产业部的销售许可，国家测评中心的认证等。

检查方法、步骤：1、访谈网络管理员，应访谈网络管理员，询问对网络设备的防护措施有哪些，询问对网络设备的登录和验证方式做过何种特定配置；询问对网络特权用户的权限如何进行分配；应访谈网络管理员，询问网络设备的口令策略是什么；2、访谈被查机构对网络设备的技术要求，相关的电子设备的选型、购置、是否经过技术论证，性能是否符合国家有关安全标准（相关权威的证明文件）；3、网络设备 Lan Console 和广域网 Console 地址是否置于安全的网络区域内，对这些 IP 地址的终端的操作行为是否有记录，查看相关的日志记录。4、检查，测试边界和网络设备.应检查边界和主要网络设备，查看是否配置了登录用户身份鉴别功能或采用相应的登录统一认证设备对操作行为进行记录，口令设置是否有复杂度要求；查看是否对同一用户选择两种或两种以上组合的鉴别技术来进行身份鉴别，其中一种是不可伪造的；5、应检查边界和网络设备，查看是否配置了鉴别失败处理功能（如是否有鉴别失败后锁定帐号等措施）；6、应检查边界和网络设备，查看是否配置了对设备远程管理所产生的鉴别信息进行保护的功能；7、应检查边界和网络设备，查看是否对网络设备的管理员登录地址进行限制；查看是否设置网络登录连接超时，并自动退出；查看是否实现设备特权用户的权限分离；8、调阅网络设备的登录日志，调阅网络管理用户的权限分配文档资料，设备日志（审计）管理权限是否与维护权限有效隔离；9、实地查看相关的网络设备，查看的保管、备件管理是否有详细的记录，设备标记。设备的或与设备连接的标识符能用于指示此设备是否允许连接网络。如果存在多个网络，尤其是如果这些网络有不同的敏感度，这些标识符应清晰的指明设备允许连接到哪个网络。可能需要考虑设备的物理保护以维持设备标识符的安全。

检查项 10：网络安全测试

基本要求：为保障系统安全，对网络通信的安全采取一些测试方法进行以下测试：通信线路和网络基础设施安全性测试与优化，网络加密设施测试，通信加密软件测试，身份鉴别机制测试，测试安全通道，测试各项网络协议运行漏洞，测试防火墙等安全设备的策略等。

检查方法、步骤：访谈网络管理员是否进行过网络安全方面的测试，访谈测试的内容，并要求提供测试报告，检查测试内容覆盖检查内容。 应对边界和网络设备进行渗透测试，通过使用各种渗透测试技术（如口令猜解等）对网络设备进行渗透测试，验证网络设备防护能力是否符合要求。

检查项 11：安全检查

基本要求：为使网络长期保持较高的安全水平，网络管理员应当用网络安全检测工具对网络系统进行安全性分析，及时发现并修正存在的安全漏洞。网络管理员在系统检测完成后，应编写检测报告，需详细记叙检测的对象、手段、结果、建议和实施的补救措施与安全策略。检测报告存入系统档案。

检查方法、步骤：检查网络安全检查和测试报告，确认网络安全测试内容。

检查项 12：安全审计日志

基本要求：1、应具备网络安全审计日志功能，至少应对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录，日志数据完整、连续；2、审计记录应包括：事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；3、应能够根据记录数据进行分析，并生成审计报表。网络日志的分析工具的使用应限定于特定的人员，对于审计报表应该定期进行审核；4、应对审计日志进行保护，避免受到未预期的删除、修改或覆盖等，拥有网络日志访问权限的用户应该是特定的网络管理人员或审计人员；5、应定义网络审计日志跟踪极限的阈值，当存储空间接近极限时，能采取必要的措施，当存储空间被耗尽时，终止可审计事件的发生；6、应根据信息系统的统一安全策略，实现审计日志集中。

检查方法、步骤：1、访谈网络审计人员，询问对边界和网络设备是否实现集中安全审计，审计内容包括哪些项；询问审计记录的主要内容有哪些；对审计记录的处理方式有哪些；2、应检查边界和网络设备，查看审计策略是否对网络设备运行状况、网络流量、用户行为等进行全面的监测、记录；3、应检查边界和网络设备，查看事件审计策略是否包括：事件的日期和时间、用户、事件类型、事件成功情况，及其他与审计相关的信息；4、应检查边界和网络设备，查看其是否为授权用户浏览和分析审计数据提供专门的审计工具（如对审计记录进行分类、排序、查询、统计、分析和组合查询等），并能根据需要生成审计报表；5、应检查边界和网络设备，查看其审计跟踪设置是否定义了审计跟踪极限的阈值，当存储空间被耗尽时，能否采取必要的保护措施，例如，报警并导出、丢弃未记录的审计信息、暂停审计或覆盖以前的审计记录等；6、应检查边界和主要网络设备，查看时钟是否保持一致；7、应测试边界和网络设备，可通过以某个系统用户试图删除、修改或覆盖审计记录，验证安全审计的保护情况与要求是否一致。

16. 主机设备

核心（主机）设备系指为银行业金融机构业务系统运行提供特定应用服务的大（小）型机及服务器等计算机设备，由硬件系统（如处理器、存储设备、网络连接设备等）和软件系统（如操作系统、数据库管理系统、应用系统等）组成。核心设备是银行业金融机构信息系统运行的中枢，为确保银行业金融机构的平稳运行，必须加强对系统核心设备的安全管理。核心设备安全检查的目的主要是为了防止财产的丢失、损害和危险；降低系统未授权访问的风险；防止数据的丢失和破坏；防止业务中断等。

16.1 设备安全

检查项 1：实体和环境安全

基本要求：1、设备标签。系统核心设备应在显著位置设置标签（如编号、用途、负责人等），以方便查找和明确责任；根据安全等级的要求应在部分核心设备的关键部件（包括硬盘、

主板、内存、处理器、网卡等）设置标签，以防止随意更换或取走。2、设备安置。系统核心设备应放置在计算机机房的安全区域内。3、访问管理。对主机设备应实行严格的授权访问制度。访问情况应进行严格登记，登记内容应包括访问时间、离开时间、陪同人员、访问理由及批准人等事项。4、安全监控。对主机设备应实施 24 小时录像监控并保存记录。

检查方法、步骤：1、检查系统核心设备及其关键部件是否设置标签。2、检查主机设备放置的区域。3、抽查监控录像和记录，检查主机的访问情况。4、检查监控的有效性。

检查项 2：可靠性及状态监控（硬件维护协议、版本升级、硬件的备件）

基本要求：1、系统核心设备关键部件应具有容错、冗余或热插拔等安全功能。2、对设备硬件应实施监控。设备的关键部件，包括 CPU、内存、硬盘、电源、风扇等，应具备管理接口，通过该接口或其他措施收集硬件的运行状态，并对其进行实施监控，当所监测数值超过预先设定的阀值时，提供报警、状态恢复等处理。

检查方法、步骤：1、了解系统核心设备的品牌、型号及配置情况。2、了解设备部件的容错、冗余、热插拔等功能的情况。3、了解是否有对设备硬件运行情况实施监控，采用何种监控措施。4、现场查看并核实以上情况。

检查项 3：设备电磁防护

基本要求：根据电磁防护强度与设备安全保护等级相匹配的原则，系统核心设备应按国家有关部门的规定实施电磁防护。

检查方法、步骤：调查了解对于系统核心设备是否采用了电磁防护措施、防护级别及防护效果。

16.2 运行安全

检查项 1：安全监控（主动防护，定期检测）

基本要求：1、应制定对核心（主机）设备及其运行的网络情况实施监控的制度和措施。

2、主机运行安全监控。应对核心（主机）设备运行情况实施安全监控，根据安全保护等级安全监控分为：（1）提供服务器硬件、软件运行状态的远程监控功能；（2）对命令执行、进程调用、文件使用等进行实时监控，在必要时应提供监控数据分析功能。3、网络安全监控。应在核心（主机）设备网络接口处对进出的网络数据流进行实时监控。根据不同安全等级对网络安全监控的不同要求，网络安全监控应：（1）不依赖于核心设备操作系统，且不因核心设备出现非断电异常情况而不可用。（2）对进出核心设备的网络数据流，按既定的安全策略和规则进行检测。（3）支持用户自定义的网络安全监控的安全策略和规则。（4）具有对网络应用行为分类监控的功能，并根据安全策略提供报警和阻断能力；（5）提供集中管理功能，以便接收网络安全监控集中管理平台下发的安全策略和规则，以及向网络安全监控集中管理平台提供审计数据源。4、对核心（主机）设备及网络情况应实行 7*24 小时监控，监控中出现的异常情况应进行记录。

检查方法、步骤：1、调阅对核心（主机）设备及其运行的网络进行监控的相关制度规定措施。2、现场查看监控软件的运行情况，了解监控的有效性。3、调阅监控记录，了解监控记录的真实和完整性。

检查项 2：操作及维护

基本要求：1、设备操作。对于设备开关机、参数设置和调整等操作应进行严格管理，只有经授权的人员才能进行相关操作。各项操作必须在有效监控情况下进行。对业务影响重大的核心参数调整，建议至少由双人负责及双重认证后才能获得修改权。应严格记录参数变更的情况、结果、操作人、责任人、时间等。2、设备维护。应按照供应商推荐的服务时间间隔和指标对设备进行维护和保养，以确保其连续使用和完整性。只有已授权的维护人员才可对设备实施修理和服务。维护过程应记录所有可能的和实际的故障，以及所有预防性的、正确的维护。

检查方法、步骤：1、询问是否有核心设备操作及维护相关管理制度，如果有则调阅相关管理制度，审查其是否满足安全管理的要求。2、检查制度的执行情况。要求被查单位提供管理制度中所涉及申请、审批、操作或参数调整记录等文档资料，检查制度执行情况。3、调阅

设备维护记录，检查是否按要求对设备进行维护。

检查项 3：恶意代码防护

基本要求：应在核心主机中设置防恶意代码软件，对所有进入核心设备的恶意代码采取相应的防范措施，并与防恶意代码集中管理平台协调一致，进行整体防护，及时发现和清除进入系统内部的恶意代码。

检查步骤、方法：询问并检查采取了何种措施进行恶意代码防护及取得的实际效果，在确保安全的情况下由被查单位操作人员对防护软件进行操作，查看防护软件其是否根据安全情况定期进行升级更新。

检查项 4：时钟同步

基本要求：核心设备的时钟应被设定在一个统一的标准上，应建立检查和修正这些偏差的程序。

检查步骤、方法：询问核心设备的时钟设定标准，询问是否有时钟管理方面的相关规定，如果有则进行调阅，审查规定内容的是否满足安全要求。可对部分设备的时钟情况进行实际查看，以验证其有效性。

检查项 5：电缆安全

基本要求：对于核心设备的电源和传送数据的或支持信息服务的通信电缆应加以保护，防止窃听和破坏。应考虑如下内容：1、电源和进入核心设备的通信线路应埋入地下，可能的情况下，应建立备用通道。2、网络电缆应避免窃听和损坏，如，使用地下管道，或避免经过公共区域。3、电力电缆应与通信电缆进行隔离，防止串扰。4、根据安全保护等级，还应考虑更多的控制如下：（1）安装具有防护的管道和上锁的检查点和端点；（2）采用可选路由或传输介质；（3）使用光缆；（4）清除与电缆相连的无关设备。

检查方法、步骤：询问设备负责人设备的电力电缆和通信电缆的布设方式及采取了何种安全保护方式，是否对电缆情况进行安全检查，对检查情况和结果是否有相关记录。

检查项 6：备份与故障恢复

基本要求：为实现核心设备的安全运行，银行业金融机构核心（主机）设备应采用紧耦合集群结构进行备份与故障恢复，确保其中一台主机发生故障中断运行时，业务应用系统能在其余的主机上不间断运行。另外，根据业务连续性的不同要求，应设置异地备份与恢复功能，确保主机因灾难性故障中断运行时，业务应用系统能在要求的时间范围内恢复运行。

检查步骤、方法：实际检查是否制定了对核心设备实施有效的备份和恢复策略；采用何种方式备份和策略；是否定期对备份和恢复策略的有效性进行测试（即是否进行实际的演练）。

17. 操作系统

操作系统是控制和管理计算机系统内的各种硬件和软件资源并有效组织应用程序运行的系统软件，是用户与计算机的唯一接口。目前，商业银行使用较多的操作系统有：MVS、OS390、AIX、HP－UX、Solaris、UNIX、WINDOWS NT 等。

17.1 操作系统日常维护

检查项 1：日常维护管理

基本要求：应对操作系统进行定期维护、升级、备份

检查方法、步骤：

1、OS 等系统软件是否升过级 [*有/无*]

若*有*则提供书面记录 [*好/一般/差*]

2、 OS 等系统软件是否做过重要维护 [*有/无*]

若*有* [*自己维护/开发商维护/其他*]

书面记录 [*有/无*]

3、主机 OS 等定期备份 [*有/无*]

若*有*查看备份 [*好/一般/差*]

4、主机硬件系统是否做过扩充/升级等 [*有/无*]

若*有* [*自己维护/开发商维护/其他*]

书面记录 [*有/无*]

5、主机等硬件设备定期测试 [*有/无*]

若*有*查看书面记录 [*好/一般/差*]

6、主机等硬件设备定期维护 [*有/无*]

若*有*查看记录 [*好/一般/差*]

7、主机上有无开发环境 [*有/无*]

8、主机上有无源程序等 [*有/无*]

9、OS 的系统补丁是否经过测试 [*有/无*]

10、OS 的系统补丁是否经过批准 [*有/无*]

11、银行是否建立日常管理制度文件 [*有/无*]

17.2 用户、密码设置及根系统管理

检查项 1： root 用户及密码管理

基本要求：应对登录操作系统用户进行身份标识和鉴别；操作系统管理用户身份标识应具有不易被冒用的特点，口令应有复杂度要求并定期更换。应对 root 密码双人分段管理并封存保管。

检查方法、步骤：

1、按规定掌握 root 密码的人数及密码设置情况：

主机_____[ ]人，岗位[ ]

分段保管 [*是/否*]

封存保管 [*是/否*]

封存情况 [*好/否*]

2、其他知道 root 密码的人 [*有/无*]

若*有*则 [*主机名*] *岗位* | *职称* | *其他*]

3、银行是否建立 root 用户资格管理机制 [有/无]

4、银行是否建立 root 密码保管制度 [有/无]

检查项 2： root 用户及密码设置

基本要求：应严格限制默认帐户的访问权限，重命名系统默认帐户，修改这些帐户的默认口令。应保证 root 用户的密码达到一定的复杂度。

检查方法、步骤：查看/etc/default/security 文件，确认配置了比较健壮的密码策略：

-密码长度 6 到 8 位

-密码是否是字母和数字的组合

-是否启用了密码历史，并且至少比 6 要大

-是否最少每 90 天修改一次密码

【备注】

/etc/default/security 文件规定了密码标准的参数及其值，每行一组参数和值。请使用系统管理员的帐号登陆系统，使用命令"more /etc/default/security"查看文件的内容：

-禁止空密码 ALLOW_NULL_PASSWORD=0

-密码长度检测 MIN_PASSWORD_LENGTH=6（或更大）

-为保证字母和数字的组合，请确认下列参数都不为 0

- PASSWORD_MIN_UPPER_CASE_CHARS
- PASSWORD_MIN_LOWER_CASE_CHARS
- PASSWORD_MIN_DIGIT_CHARS
- PASSWORD_MIN_SPECIAL_CHARS

-密码历史 PASSWORD_HISTORY_DEPTH=6（或更大）

-密码更改日期 PASSWORD_MAXDAYS=90（或更小）

检查项 3： root 登录失败记录管理

基本要求：应启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施。审计内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件。审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等。

检查方法、步骤：查看 root 登录失败日志，从中分析是否有可疑记录。

【备注】

1、检查有无 root 登录失败日志定期检查、分析机制，有无问题报告上报机制。

2、可使用命令 more var/adm/loginlog，分析使用 root 用户登录失败的情况。

检查项 4： su 命令失败记录管理

基本要求：审计范围应覆盖到服务器和重要客户端上的每个操作系统用户。审计内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件。审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等。操作系统应详细记录使用 su 命令的记录。

检查方法、步骤：调阅使用 su 命令的日志，从中分析是否有可疑记录。

【备注】

1、检查有无 su 命令日志定期检查、分析机制，有无问题报告上报机制。

2、使用命令 more /etc/security/failedlogin 调阅 su 命令日志。

检查项 5： 定时保护管理

基本要求：应根据安全策略设置登录终端的操作超时锁定

检查方法、步骤：查阅/etc/default/login 文件是否包含 TIMEOUT 参数的设置（按秒）。

检查项 6： root 是否只能在某设备上注册

基本要求：当对服务器进行远程管理时，应采取必要措施，防止鉴别信息在网络传输过程中被窃听，root 只能在固定的设备上注册。

检查方法、步骤：（1）与系统管理员进行会谈，以了解 root 用户登录策略；（2）使用#more /etc/default/login 查看：CONSOLE= 设备描述。

检查项 7： 根文件系统自动清理设置管理

基本要求：应保证操作系统用户的鉴别信息所在的存储空间，被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中。应确保系统内的文件、目录和数据库记录等资源所在的存储空间，被释放或重新分配给其他用户前得到完全清除。

检查方法、步骤：

使用命令#more /etc/default/boot

正确值： AUTOBOOT=YES 实际值： AUTOBOOT=_____

FSCKFIX=YES FSCKFIX=_____

检查项 8： 其他特权用户管理

基本要求：应根据管理用户的角色分配权限，实现管理用户的权限分离，仅授予管理用户所需的最小权限。确认无关的系统帐号已被禁用。

检查方法、步骤：

1、与系统管理员进行会谈：

- 软件安装过程中，与设置用户访问权限和禁用默认用户帐号有关的步骤
- 与用户名管理有关的策略、流程、标准和指南
- 用户名管理的责任

2、默认用户帐户的状态

查看/etc/passwd 文件，确认厂家默认的用户 ID 已被禁用。

【备注】如果密码区域含有*号，表示这个帐户的密码不起作用。要想查看/etc/passwd 中列出的用户帐户的状态，请以系统管理员的帐号登陆，敲入如下命令："userstat -a"。检查下列系统默认帐户的状态：root (0), daemon (1), bin (2), sys (3), adm (4), uucp (5), lp (9), nuucp (11), hpdb (27), www (30), webadmin (40), smbnull (101)。确认除 root 外，UID 小于 100 的用户都已经被禁用，除非业务特殊需要。

检查项 9： 用户 UID 管理情况

基本要求：应为操作系统的不同用户分配不同的用户名，确保用户名具有唯一性。应采用两种或两种以上组合的鉴别技术对管理用户进行身份鉴别。应及时删除多余的、过期的帐户，避免共享帐户的存在，严格管理多个用户使用一个 UID 的情况。

检查方法、步骤：

1、检查/etc/passwd 文件检查（系统用户情况，重点检查 uid 重复的用户）

系统用户（伪用户）异常情况：

[用户名|uid|gid|group|home-dir|shell]

系统普通用户设置情况：

[用户名|uid|gid|group|home-dir|用途]

2、检查/etc/security/passwd 文件（password 的属性值）

系统用户（伪用户）异常情况：

[用户名|uid|gid|group|home-dir|shell]

系统普通用户设置异常情况：

[用户名|uid|gid|group|home-dir|用途]

3、/etc/user、/etc/security/user 文件检查（有无重复用户、应删除而没删除的用户）

4、调阅银行一段时间内离职人员清单，检查是否存在用户还存在的情况。

检查项 10：配置文件管理

基本要求：应对重要信息资源设置敏感标记。应依据安全策略严格控制用户对有敏感标

记重要信息资源的操作。相关系统文件的权限应根据业务需求进行设置。

检查方法、步骤：

1、与系统管理员进行会谈以取得用户配置文件策略以及银行是否建立相关策略制度。

2、分别取得/etc/security/limits 、 /etc/environments 、 /etc/security/environ 、 /etc/security/lastlog、/etc/security/.ids、/etc/security/.profile 等配置文件，检查是否符合配置文件策略。

检查项 11：用户目录管理

基本要求：应严格限制用户目录下的文件，以防止恶意代码侵入系统。用户目录不应存在非正常文件。

检查方法、步骤：1、与系统管理员进行会谈以取得用户目录管理策略；2、抽查部分用户的/home 目录逐个检查。

17.3 主机文件系统安全

检查项 1：文件系统目录权限配置管理

基本要求：应依据安全策略严格控制用户对有敏感标记重要信息资源的操作。根据实际需求配置核心文件系统目录权限。

检查方法、步骤：

1、与信息安全管理员或技术支持人员进行会谈以了解：

- 银行是否建立与系统文件和文件夹访问控制相关的信息安全策略和流程
- 系统文件和文件夹管理的角色和责任
- 系统文件和文件夹访问控制权限与银行标准背离，其原因何在
- 相关系统处理平台实现的系统文件和文件夹访问控制方法
- 对修改系统文件和文件夹、修改其访问权限进行的监控过程

2、查看/etc、/bin、/usr、/var、/home 等文件目录权限设置是否违背上述策略。

检查项 2： 参数“umask”配置管理

基本要求：默认 umask 参数：默认 umask 参数设置在/etc/profile 目录下。Root 用户的“umask”参数应该被设为 027 以移除其他用户对 root 用户所创建文件的权限。检查其他特权用户例如 admin、dba 的”umask”参数是否根据需求合理的设置。对于非特权用户，“umask”设置为 022 通常是合适的，因为它可以阻止其他用户写文件的权限，从而限制更新文件的权限。抽查任意一个非特权用户，检查其用户目录下的”umask”参数是否被设置为 022。

检查方法、步骤：

1、通过与系统管理员访谈以了解：

－定义系统参数和系统策略的步骤；

－执行和评估系统安全的责任。

2、查看是否违背上述策略。

检查项 3： 应用目录权限配置管理

基本要求：应启用访问控制功能，依据安全策略控制用户对资源的访问。

检查方法、步骤：

1、通过与系统管理员访谈以了解应用目录权限参数和目录下应有的文件；

2、抽查部分应用目录进行核实。

17.4 主机系统访问控制

检查项 1： 登录失败日志管理

基本要求：审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等；应能够根据记录数据进行分析，并生成审计报表；应保护审计进程，避免受到未预期的中断；应保护审计记录，避免受到未预期的删除、修改或覆盖等。日志应当记录信息安全策略中所定义的登录失败情况，应当定期查看系统生成的报告并采取措施。

检查方法、步骤：1、查看银行是否建立日志定时审阅、分析机制，有无相关制度，有无

清晰的报告路线；2、通过查阅银行诸如系统配置和安全报告等方面的文档，搜集相关证据证实银行就询问所提供答案的真实性，看是否根据已建立的制度和流程实施了控制活动。

【备注】

通过以下途径检查登陆失败日志是否有效记录：

- 在 HP-UX 系统中失败的登陆记录可通过命令“lastb”查看。

- 在 AIX 系统中失败的登陆记录可通过命令“who -a/etc/security/failedlogin”查看。

- 在 Sun Solaris 系统中失败的登陆记录可通过命令“more/var/adm/messages”查看。

- 命令“more /var/adm/sulog”显示使用命令“su 用户名 密码”在用户间切换的所有成功和失败的操作

检查项 2： UNIX 通信服务管理

基本要求：应依据安全策略严格控制用户对有敏感标记重要信息资源的操作。应当在业务需求的基础上启动 UNIX 通信服务。

检查方法、步骤：1、与系统管理员访谈以了解允许启动的网络服务清单，有无相关策略制度；2、检查“inetd.conf”文件，识别所有已启动的网络服务。使用系统管理员帐号在命令行运行 netstat-a 命令（查看开启了那些端口），识别所有正在运行的网络服务，并通过具体的“侦听”识别服务的类型；3、使用管理员帐号检查所有网络服务的必要性，关注高风险的服务，如 ftp,telnet 和 finger。

检查项 3： NFS 目录共享管理

基本要求：应依据安全策略严格控制用户对有敏感标记重要信息资源的操作。应通过设定终端接入方式、网络地址范围等条件限制终端登录。应当只在必要时提供 NFS 目录共享，并进行合理的限制。

检查方法、步骤：

1、与系统管理员访谈以了解允许启动的 NFS 目录共享；

2、通过以下方法检查当前的 NFS 配置：

--AIX 和 HP-UX: 执行“more /etc/exports”命令，查看 NFS 服务器上所提供的目录共享配置。执行“showmount -a”命令，显示当前所有挂载到服务器共享目录上的客户端系统。

--SOLARIS: 执行 dfshares 命令，查看/etc/exports 文件

检查项 4： HTTP 服务管理

基本要求：应依据安全策略严格控制用户对有敏感标记重要信息资源的操作。操作系统应遵循最小安装的原则，仅安装需要的组件和应用程序，并通过设置升级服务器等方式保持系统补丁及时得到更新。web 服务（HTTP）的访问是基于必要的业务需求，并进行了适当的限制。应通过设定终端接入方式、网络地址范围等条件限制终端登录。

检查方法、步骤：

1、与系统管理员进行会谈：

-确定检查范围内的服务器是否有服务器启用了 HTTP 服务

-用来支持 HTTP 服务器正常工作的物理地点和文档

-讨论对 HTTP 服务的监控和 HTTP 相关的进程

-HTTP 服务器采用的安全配置和安全报告机制

2、HTTP 服务器

如果检查范围内的服务器没有需要被用作 HTTP 服务器的，请确认的确如此。/etc/inetd.conf 文件列出了所有已启动的服务，请检查 HTTP 服务是否在列。如果的确因为业务需要，启用了 HTTP 服务，请看下一步。

3、Web 服务器安全

如果因业务需要启用了 HTTP 服务，请检查 ip 过滤是否已经建立，用于控制远程的访问。/etc/opt/ipf/ipf.conf 文件用来设定 IP 过滤规则。要查看当前的 IP 过滤规则，请用系统管理员账号登陆，敲入"more /etc/opt/ip/ipf.conf"命令。查看是否建立了对 HTTP 流量的控制（以'port www'标识），并且这些规则与规定的策略一致。执行"ps -ef"命令，查看 HTTP 后台进程不是以”root”用户运行的。

检查项 5： FTP 对主机的访问管理

基本要求：应依据安全策略严格控制用户对有敏感标记重要信息资源的操作。操作系统应遵循最小安装的原则，仅安装需要的组件和应用程序，并通过设置升级服务器等方式保持系统补丁及时得到更新。通过 FTP 对主机的访问应基于业务需要并得到有效控制。

检查方法、步骤：

1、与系统和安全管理员进行会谈：

-FTP 服务的配置、管理策略和流程（包括匿名用户、TFTP）

-使用 FTP 进行文件传输所采取安全措施

-对 FTP 活动的监控，包括对 FTP 用户主文件夹文件访问权限的检查

2、检查 FTP 用户列表

HP-UX 使用/etc/ftpusers 或 /etc/ftpd/ftpusers 文件来限制 FTP 用户。文件中所列用户是不允许通过 FTP 访问系统的。请确认除了合法的用户外，其他任何用户都不在该文件中。系统级别的用户帐户如果没有重要原因，也不应当通过 FTP 来传输信息，因此 root 帐户通常也不应该被允许使用 FTP。

3、检查匿名 FTP

请检查系统是否建立了 FTP 匿名帐户，方法是看“/etc/passwd”是否有一个条目用户名为“ftp”，密码为*，所属用户组为 guest，并且登陆的 shell 为“/usr/bin/false”。举个例子（假设 guest 组的 ID 为 10）：“ftp:*:500:10:anonymous ftp:/home/ftp:/usr/bin/false”。进入 FTP 主目录，执行命令-laR，获取该文件夹的内容列表。除了 public 目录外，所有其他目录的访问权限都应该是 555，文件的访问权是 444。Public 目录一般的访问权限为 777。

检查项 6： Telnet 网络服务管理

基本要求：应依据安全策略严格控制用户对有敏感标记重要信息资源的操作。应能够检测到对重要服务器进行入侵的行为，能够记录入侵的源 IP、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时提供报警。应根据业务需要决定是否屏蔽 telnet 网络服务。

检查方法、步骤：

1、与系统和安全管理员进行会谈：

-Telnet 服务的配置、管理策略和流程

-使用 Telnet 进行访问所采取安全措施

-对 Telnet 活动的监控

2、使用命令#more /etc/inetd.conf 核实是否与上述策略相匹配

检查项 7： 远程访问控制策略管理

基本要求：应能够检测到对重要服务器进行入侵的行为，能够记录入侵的源 IP、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时提供报警。应通过设定终端接入方式、网络地址范围等条件限制终端登录；

检查方法、步骤：

1、与系统管理员进行会谈：

- 银行是否制定远程访问控制方面制度
- 评估系统管理员在远程访问管理方面的认知水平
- 业务需要开启哪些远程访问
- 在 Internet 服务中，提供了哪些默认的远程访问服务
- 用户主目录的管理情况，特别是主目录中的远程访问配置文件

2、参照风险点 1、风险点 2、风险点 3、风险点 4、风险点 5、风险点 6 的检查情况进行综合判断。

【备注】

1、检查保障 HP-UX 系统远程访问安全的策略和流程。确定策略和流程中规定了哪些网络是被信任的。

2、远程访问相关服务

使用命令"more /etc/inetd.conf"，列出 HP-UX 服务器上的所有服务。确定一些相对不安全的服务如：telnet、rlogin、rsh、rcp 和基于 rpc 的服务 NIS 是没有启动的。确定只有当业

务实际需要时，这些服务才被启动。

3、检查是否启用了系统间的信赖机制

查看” hosts.equiv”文件，确定是否建立了信任网络。注意到，如果 SSH/Telnet 功能开启，具有 shell 访问权限的系统用户在远程访问时也同样具有这样的权限，这是很危险的。使用系统管理员账号登陆，敲入"more /etc/hosts.equiv"命令以查看信任网络是否是严格按照策略进行建立的。

4、rhosts 支持

.rhost 文件提供了用户级远程访问的方法。.rhost 文件基于远程计算机的网络地址或用户名，实现了一种不太安全的认证机制。请确认 rhost 功能是关闭的。如果根据业务需要启用了 rhost 功能，确认强匹配符’+’没有使用，因为.rhosts 中的条目应当始终是确定的主机和用户（举个例子”trustedhost alice”而不是”trustedhost”）。

17.5 主机系统工作情况

检查项 1： 系统进程数量管理

基本要求：应限制单个用户对系统资源的最大或最小使用限度。系统进程数量应控制在正常值以内。

检查方法、步骤：1、与系统管理员进行会谈以了解系统中正常的进程数量；2、查看系统中实际的进程数量，看是否超出正常值。

检查项 2： 系统容量管理

基本要求：银行应定期检查容量规划并进行定期检查。应对重要服务器进行监视，包括监视服务器的 CPU、硬盘、内存、网络等资源的使用情况。应能够对系统的服务水平降低到预先规定的最小值进行检测和报警。

检查方法、步骤：1、检查银行是否制定有主机容量规划，是否针对主机容量进行定期检测；2、uptime 显示，系统综合处理能力判断（系统负载） [富裕很大/可用/有潜在问题]；3、

top 显示，系统综合处理能力判断 [富裕很大/可用/有潜在问题]（提供运行在系统上的与 CPU 关系最密切的进程列表，以及负载平均、进程数量、使用的存储器和页面空间数量）；4、sar 显示，系统综合处理能力判断 [富裕很大/可用/有潜在问题]（系统资源的使用情况，特别是内存和 CPU 的使用情况）；5、vmstat 显示，系统内存/虚存情况判断 [富裕很大/可用/有潜在问题]；6、iostat 显示，系统设备处理能力判断 [富裕很大/可用/有潜在问题]；7、df iv 显示电脑硬盘空闲空间是否大于 15%，以保证系统性能的稳定

检查项 3： 定时进程设置情况管理

基本要求：应安装防恶意代码软件，并及时更新防恶意代码软件版本和恶意代码库。定时进程设置情况（批处理情况）应根据业务需求设定。

检查方法、步骤：

1、与系统管理员进行会谈以了解系统定时处理的程序的情况以及银行创建、修改、终止定时程序的相关制度文件及审批流程。

2、查看系统中 cron 进程的状态 [*启动 / 无*]

3、/var/adm/cron/cron.deny 和 allow 文件情况

/var/adm/cron/cron.deny 文件 [*正常/异常*]

/var/adm/cron/cron.allow 文件 [*正常/异常*]

【备注】:

1、同负责 AIX 管理的系统管理员和主管人员进行会谈：

- 怎样在 cron table 和“at”命令中处理进行中的交易和用户请求.
- 怎样确保“cron” 和 “at”作业被完成
- 是否有任何第三方软件用于调度批处理
- 在 cron table 添加和删除条目的步骤以及谁有权进行这样的操作
- 在 cron table 中修改已有的条目的位置以及谁有权进行这样的操作
- cron table 的文件权限和存取权限
- 在这些文件中使用 cron.allow, cron.deny, at.allow, 和 at.deny 条目

- 限制未经授权用户进入“cron” 和 “at”的方法。
- cron 的登陆特征和 cron table 的配置
- 日志审查/错误警报机制到位

2、查看相关配置文件

cron.allow 和 at.allow 文件中列出了被允许使用 Crontab 程序和 at 命令进行任务调度的用户列表。cron.deny 和 at.deny 文件正好相反。检查 /var/adm/cron/at.allow，/var/adm/cron/at.deny，/var/adm/cron/cron.allow，/var/adm/cron/cron.deny 这四个文件，确认只有授权的用户才能进行任务调度。当同时存在.allow 和.deny 文件时，.deny 文件将被系统忽略。使用管理员帐号登陆，使用如下命令查看文件的内容：

"more /var/adm/cron/cron.allow"和"more /var/adm/cron/at.allow"

检查项 4： 定时进程 Cron 日志管理

基本要求：审计内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件。审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等。定时进程 Cron 日志应当完整，提供足够的可供审计的资料。

检查方法、步骤：Cron 日志通常存放在/var/adm/cron/log file 目录。 要检查当前日志的内容，使用以下命令，当以管理员登入帐户的系统： “more/var/adm/cron/log”。 检查 /etc/cronlog.conf 并且发现日志记录间隔时间。 证实日志记录间隔时间被设置是根据政策或程序或者根据银行需要。并且证实记录文件的权限使用“ls”命令并且保证未批准的用户不可能删除日志。

17.6 HACMP 设置情况

检查项 1： HACMP 维护切换管理

基本要求：对重要主机设备应采取双机热备方式以保障业务连续性，对双击热备设备应定时检查并定时切换演练。

检查方法、步骤：

（1）群集、资源等配置和维护情况

查看安装上机时书面记录 [有/无]

日常维护记录 [有/无]

若有，记录情况[*好/一般/差*]

（2）检查切换情况

定期切换规定 [*有/无*]，切换记录 [*有/无*]，情况 [*好/一般/差*]

故障切换次数 [ ]，切换情况 [*正常/异常*]

检查项 2：其他高可靠性方案管理

基本要求：对重要主机设备应采取措施以保障业务连续性，对保障业务连续性的设备应定时检查并定时切换演练。

检查方法、步骤：

（1）高可靠性技术方案名称

名称 [ ]，实现方式 [ ]

技术特点 [ ]

主机间备份方式 [ ]

（2）群集、资源等配置和维护情况

查看安装上机时书面记录 [有/无]

日常维护记录 [有/无]

若有，记录情况 [好/一般/差]

（3）检查切换情况

定期切换规定 [有/无]，切换记录 [有/无]，情况 [好/一般/差]

故障切换次数 [ ]，切换情况 [正常/异常]

17.7 Windows 系统安全策略设置是否合理

检查项 1： 信息安全政策管理

基本要求：应严格限制默认帐户的访问权限，重命名系统默认帐户，修改这些帐户的默认口令。

检查方法、步骤：与管理员访谈并获取可用的信息安全政策和程序，讨论其规则;工具和程序用来防止未经许可存取信息、以及用户的安全策略信息。了解其组管理、用户管理、用户策略、用户权限、文件和目录权限、网络服务、审计和 Windows 远程存取。

检查项 2： 安全选项设置管理

基本要求：操作系统管理用户身份标识应具有不易被冒用的特点，口令应有复杂度要求并定期更换。

检查方法、步骤：通过与管理员访谈取得安全策略，和推荐安全策略进行比较：

允许服务器操作员在特定的时间或以特定的时间间隔计划执行特定的任务	禁用
允许在不登录的情况下关闭系统	禁用
当系统被关闭时，清除虚拟内存的页文件	启用
禁止登录时按 CTRL+ALT+DEL	禁用
登录时不显示最后登录的用户名	启用
防止系统维护计算机帐户密码	禁用
恢复控制台: 允许管理员自动登录	禁用
恢复控制台: 允许从所有驱动器文件夹中复制文件	禁用
允许第三方 服务器消息块（Server message block）服务器使用未加密的密码进行身份验证	禁用
为对象指定默认自由访问控制列表	启用

检查项 3： 日志策略设置管理

基本要求：审计范围应覆盖到服务器和重要客户端上的每个操作系统用户；审计内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件；审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等； 应能够根据记录数据进行分析，并生成审计报表；应保护审计进程，避免受到未预期的中断；应保护审计记录，避免受到未预期的删除、修改或覆盖等。

检查方法、步骤：通过与管理员访谈取得日志策略，和推荐日志策略进行比较，至少反映以下事件日志：

帐户登录事件	成功, 失败
帐户管理	成功, 失败
访问目录服务	成功, 失败
登录事件	失败
对象访问	成功, 失败
变更策略	成功, 失败
使用特权	失败
全过程跟踪	失败
系统事件	成功, 失败
最大的应用日志大小	>10 MB
最大的安全日志大小	>10 MB
最大的系统日志大小	>10 MB
限制访客访问应用日志	必须
限制访客访问安全日志	必须
限制访客访问系统日志	必须
保留应用日志	>14 天
保留安全日志	>14 天

保留系统日志	>14 天
应用日志保留方法	按天
安全日志保留方法	按天
系统日志保留方法	按天
安全日志满关闭计算机	关闭

检查项 4： 硬盘分区格式管理

基本要求：硬盘分区应尽量使用 NTFS 文件系统

检查方法、步骤：NTFS 允许管理员以用户和/或用户组指定文件和目录许可。FAT 格式不具备这个特点，所以在 FAT 卷难以实现文件和目录许可。

17.8 Windows 日常管理

检查项 1：版本管理

基本要求：银行应统一操作系统版本

检查方法、步骤：查看各桌面电脑 windows 操作系统版本是否统一。

检查项 2：补丁管理

基本要求：应及时检查操作系统安全补丁发布情况，发现有新的补丁发布，应及时升级。生产业务系统应首先在模拟环境下进行升级测试，通过后，经过审批，再对生产环境操作系统进行升级，并定期向主管负责人员汇报打补丁状态。

检查方法、步骤：检查有无补丁管理制度，查看各桌面电脑 windows 操作系统是否统一升级补丁。

检查项 3：软件管理

基本要求：银行业金融机构应禁止从事业务生产的计算机安装来历不明的软件，或私自

从互联网下载的软件。外来软件在安装前，应查杀病毒，确保安全后才可安装上线。

检查方法、步骤：查看各桌面电脑 windows 操作系统有无安装与办公无关的软件及有无游戏软件或盗版软件。

检查项 4： 登录密码、屏幕保护密码管理

基本要求：服务器和终端应通过设置屏幕保护密码或即时锁屏等方式进行访问控制。

检查方法、步骤：查看各桌面电脑 windows 操作系统是否设置了登录密码、屏幕保护密码。

检查项 5： 机器命名、工作组设置管理

基本要求：应根据安全策略设置登录终端的操作超时锁定。机器命名、工作组设置应根据银行同一策略设置。

检查方法、步骤：与管理员访谈并获取机器命名、工作组设置规则，并查看各桌面设置是否符合规则。

检查项 6： IP 地址管理

基本要求：应根据全行同一的 IP 管理策略设置 IP 地址。

检查方法、步骤：与管理员访谈并获取 IP 地址设置规则，并查看各桌面设置是否符合规则。

18. 数据库管理系统

银行机构常用的数据库产品有 informix、oracle、sybase 和 SQL server 等关系型数据库管理系统。数据库系统检查的基本要点包括：访问控制、身份认证、数据安全、网络安全、审计策略、备份及恢复和性能管理。检查过程中主要审阅和分析数据库日常管理和维护、安全策略、应急演练、备份策略、数据维护和获取、变更管理、压力测试等方面的文档和操作手册，在必要时采取进一步调查取证措施。

检查项 1：访问控制

基本要求：应制定和严格执行数据库的访问控制策略，通过严格的用户和角色授权，对用户有权在特定的数据库对象（表、视图、存储过程、数据库连接等）上使用哪些特权或执行哪些操作进行限制，降低数据库非法访问的风险。

检查方法、步骤：1、检查数据库管理员的岗位设置情况。数据库管理权限的使用，须经过信息科技管理部门负责人的签字批准。一般情况下，数据库管理员不得由业务系统开发和应用人员兼任，数据库重要变更应实行双人操作。数据库管理员使用特权账户进行管理工作，应在操作日志中记录有关情况；2、检查是否定义了基本的用户访问控制策略。调阅数据库用户清单，询问用户的权限设置情况，检查是否设置了必要的权限分离，至少应设置查看用户与操作用户的分离。数据库用户包括人工登录用户和程序配置用户，检查是否存在系统用户保留了默认密码的情况，检查测试用户和其他无用帐号是否及时清理。3、检查是否针对终端用户制定了安全策略，如是否对所有用户进行了合理的授权、是否对终端用户登陆数据库的 IP 地址进行限定；4、检查系统的安全性策略。对重要的数据库对象、数据库管理工具(如 PL/SQL、OEM)和程序包的授权进行有效的控制；5、当数据库管理须通过堡垒机或其他统一登录系统进行访问时，检查堡垒机或相应软件的访问控制和用户授权，如 IP 地址限制、帐号管理、密码策略、登录日志等。

检查项 2：身份认证

基本要求：应对本地和远程数据库用户的登录进行安全控制，采用可靠的认证机制加强对特权用户登录的约束，使用有效的密码策略，避免使用弱口令登录。

检查方法、步骤： 1、检查数据库是否修改了拥有管理权限的数据库用户的默认密码。检查非法的管理员用户的登录情况（包含定期执行）； 2、检查数据库连接是否采用了安全的身份认证机制；3、检查密码策略设置。包括：最大错误登录次数、密码复杂性校验、口令有效期、口令历史功能等。

检查项 3：数据安全

基本要求：应建立并实施对敏感数据进行管理的机制。对敏感信息进行分类，并采取相应的保护措施；对来自于主机、网络的访问进行监控；以防止发生数据被非法篡改、破坏和泄露的事件发生。

检查方法、步骤： 1、调阅有关数据库和应用维护记录，检查是否存在直接修改数据库数据的记录。直接获取数据和修改数据参数的需求多数由业务部门发起或由未知应用错误引起，并使用脚本进行操作，询问维护脚本的编写和测试过程中采取了哪些控制措施（某些脚本中可能嵌入了应用程序用户的密码）。较好的做法是为此类数据库维护操作开发专用的用户界面进行控制。2、检查对文件系统的访问控制策略（攻击者可利用一些数据库程序包（如 UTL_FILE）或 Java 程序绕过访问控制获得数据的存取权限）。检查是否对数据库工具的使用进行严格的授权；检查对重要数据库文件如控制文件、密码文件的访问授权；3、检查对数据库结构的修改是否进行了详细的记录，并由管理人员进行审核。

检查项 4：网络安全

基本要求：数据库应建立对远程管理、远程访问的安全控制机制，对敏感的网络通信进行加密，识别并限制用户进程中的非法数据库访问活动。

检查方法、步骤： 1、检查是否设置了网络上的 DBA 权限控制，以降低数据库在网络中的风险。可以通过下列两种方式对网络上的 DBA 权限进行控制： 设置成拒绝远程 DBA 访问；通过密码文件给 DBA 设置密码；2、检查是否允许数据库的远程访问；检查远程数据库用户访问的合法性；检查远程连接的安全机制和其提供的安全服务；3、检查是否对连接到数据库的网络通信进行加密，采用何种加密算法，密钥是多少位；4、针对 SQL 注入攻击、后门数据窃取等攻击手段，检查是否安装了入侵检测系统，检测网络中流入和流出的数据包，是否进行深入数据包检测，检查应用代码中执行的 SQL 调用，入侵检测系统是否可以通过设定规则在异常情况下触发报警器。

检查项 5：审计策略

基本要求:应当对重要信息系统的数据库开启和配置审计功能，监控数据库访问的行为，分析非法访问行为和潜在的风险。

检查方法、步骤：检查是否启用了数据库审计功能或使用外部审计系统，重点审计那些数据库活动和用户，由谁负责审计日志的查看和分析，采用何种审计分析工具。审计是否覆盖了高权限用户的数据库操作，是否存在日常维护中绕过审计进行操作的情况（如使用非审计覆盖的帐号）。

检查项 6：备份和恢复

基本要求：通过制定有效的备份和恢复机制，采用一定的数据库备份和恢复技术，对数据库中的数据、表空间、数据库结构和参数等重要信息进行本地或远程备份，确保在数据库系统死机、介质损坏或用户误操作时，数据库信息不至于丢失。

检查方法、步骤：对数据库备份与恢复的检查内容包括：1、是否针对不同数据库系统制定了可行的数据库备份和恢复方案，方案有无文档记录，以备故障发生时有案可查。2、调阅信息系统配分策略文档，内容应包括：策略名称、执行脚本、保存时间、发起时间/方式、备份方式、备份内容等信息；3、是否由专人负责定期查看数据库备份日志，就数据库备份的完整性和一致性进行检查和测试，如检查备份介质或磁带驱动器、使用备份介质进行恢复测试等；4、针对具体的 RPO 目标，采用何种数据库备份技术，用来保证备份的一致性程度。如：数据库备份和日志归档、磁盘镜像。5、是否在修改数据库结构之前和之后，备份所影响的数据文件、日志文件和控制文件。6、调阅异地备份磁带交接记录，检查其完整性。

检查项 7：性能管理

基本要求：数据库管理员应当在数据库建立时，根据应用的需要合理设计分配表空间以及存储参数、内存初始化参数；在数据库运行过程中，数据库管理员应当使用一定的工具对数据库性能进行监控。通过分析和解决数据库运行过程当中出现的各种性能问题，保证 Oracle

数据库高效可靠运行。

检查方法、步骤：1、检查相关制度和维护手册中是否对数据库性能管理内容进行了明确规定，包括：性能检测的范围、频度、注意事项、处理措施、负责人和注意事项；2、检查是否使用了自动化统计量收集工具对数据库性能进行监控，是否设定了各种数据库性能指标的阈值；3、调阅数据库定期性能报告，如数据库运行报告、厂家巡检报告：检查性能检测指标的完备性以及是否覆盖了业务高峰期的采集数据、是否进行了必要的趋势分析；检查是否存在性能下降的情况，以及是否实施了出现问题时的反馈和处理机制。主要的性能指标包括：（1）informix 数据库：数据库磁盘读写命中率、逻辑日志备份情况、数据库空间使用率、表 I/O、表空间使用率、表扩展块使用率、索引层、索引唯一性、大表顺序扫描情况等；（2）oracle 数据库：oracle 初始化参数、表空间使用率、对象的数据量、无效的约束、无效的 trigger、无主键的表、job 信息、异常等待的事件、当前磁盘活动状态、undo 使用情况。

检查项 8：连续性和应急管理

基本要求：重要信息系统数据库应实行双机热备并开展相应的切换演练，建有同城或异地灾备的应开展灾备演练。重大 IT 事件应急预案中应针对不同系统的数据库制定具体、可操作的故障恢复措施，包括问题诊断、厂商支持流程和数据恢复步骤等；应用系统的应急演练中，应针对紧急情况下数据库不可用的各种可能情况，设计具体的故障场景，并对具体的恢复步骤进行描述。

检查方法、步骤：1、检查是否拟定并实施了保证数据库双机配置一致性的策略，如生产数据库变更时是否同时考虑灾备系统，调阅数据库主机双机切换手册和切换记录，确认其可操作性；2、调阅信息系统应急预案中数据库故障排除和恢复的具体内容，检查其是否设计了数据库故障的各种场景并提供具体的操作说明。可能的场景包括：数据库服务器崩溃、数据库启动失败、数据无法插入、逻辑日志满导致数据库挂起等。3、询问是否进行过数据库全库恢复测试，使用哪种恢复方式（本地带库、异地备份带、灾备数据库），有无描述或记录数据库恢复的具体步骤。

19. 第三方中间件产品

19.1 产品管理

检查项 1：中间件产品准入

基本要求：中间件产品的准入程序应当满足软件产品准入规则；中间件产品应当进行必要的安全检查；中间件产品的性能应当经过必要的测试程序。

检查方法、步骤：通过查阅银行中间产品的采购程序，重点是查看中间件产品的相关安全检查和测试记录，是否符合既定的产品准入要求。调阅材料：产品采购文档、测试记录、产品安全检测记录及产品所提供的权威认证证书。

检查项 2：中间件软件管理目录

基本要求：是否建立了中间件产品使用清单；中间件产品清单中是否有与应用系统的关联标识；其对业务的影响进行了分级分类；并始终保证中间件产品目录及时得到了更新。

检查方法、步骤：通过查阅银行中间产品目录清单和应用系统设计文档，判断目录清单的完整性，和更新的及时性。调阅材料：产品清单、应用系统设计文档。

检查项 3：中间件产品与业务系统架构

基本要求：中间件产品的使用应当满足业务架构总体规划中的应用逻辑；中间件产品的类型和配置应当满足业务架构规划中的相关性能要求；被检查行能够提供清晰的中间件产品运用的逻辑拓扑。

检查方法、步骤：通过查阅银行业务系统架构设计文档和中间件产品清单、逻辑拓扑以及各类应用系统设计文档，搜集相关证据证实银行就询问所提供答案的真实性，分析中间件的运用现状与业务架构设计的一致性。调阅材料：业务系统架构设计文档、中间件产品清单、应用系统设计文档。

19.2 运行管理

检查项 1：维护流程和操作手册

基本要求：中间件产品的运行操作应当建立书面的维护流程和操作手册，重要的中间件系统的维护应当建立适当的审批流程。

检查方法、步骤：查阅维护流程和操作手册。调阅材料：维护流程、操作手册

检查项 2：中间件产品配置管理

基本要求：中间件产品的配置应当符合配置管理的程序；中间件产品的配置参数应当得到严格的版本控制，保证配置的正确性，并在故障发生时被及时的恢复；中间件产品的版本和配置应当始终保持 C/S 两端的匹配和一致。

检查方法、步骤：通过查阅中间件产品配置管理记录、版本控制记录和相关配置文档，分析配置管理流程的落实情况和配置的一致性。调阅材料：中间件产品配置管理记录，版本记录，相关配置文档和拷贝。

检查项 3：中间件产品日志管理的程序

基本要求：中间件产品的日志应当纳入日志管理的程序；中间件产品的日志是否对危险的操作进行了记录；中间件管理工具访问日志是否有非授权的访问。

检查方法、步骤：通过查阅中间件产品的日志、日志保存的时间、日志分析记录，分析日志是否符合日志管理要求，其中交易日志是否满足监管当局要求的保存时间，是否有非授权访问。调阅材料：中间件产品日志，日志分析报告。

检查项 4：中间件产品的性能监控

基本要求：中间件产品的性能应当进行监控；性能监控应当包括承载中间件产品的硬件设备性能和容量的监控；软件处理能力应当根据业务需求和实际业务量合理设定预警阀值，并得到监控。

检查方法、步骤：通过查阅中间件产品性能监控记录，预警阀值设置情况，应用系统设计的业务处理能力；分析监控记录和相关阀值设定是否能达到预警的要求。调阅材料：性能监控记录，阀值设定记录，应用系统设计文档。

检查项 5：中间件产品产生的事件和问题管理

基本要求：中间件产品产生的事件和问题应当纳入事件管理的程序；中间件产生的事件和问题应当得到有效分析，并识别事件和问题的风险等级，高等级的事件和问题应当按照既定的报告路线进行了报告。

检查方法、步骤：通过查阅中间件产品产生的日志、事件和问题记录，分析事件管理流程是否符合既定要求；是否对事件和问题的风险进行了分析并得到了有效处理；事件和问题是否及时的进行了报告。调阅材料：事件和问题记录，事件和问题报告，事件和问题的处理记录。

检查项 6：中间件产品的变更

基本要求：中间件产品产生的变更应当纳入变更管理的程序；变更经过了适当的审批，变更前变更方案应当进行了严格测试，变更前应当建立了应急恢复措施。

检查方法、步骤：通过查阅中间件产品变更记录、分析变更管理程序是否得到有效执行。调阅材料：中间件产品变更记录，中间件产品的配置管理记录，应急恢复计划。

19.3 安全管理

检查项 1：中间件产品安全措施和认证

基本要求：中间件产品应当能够保证通信的保密性、完整性和不可抵赖性，应当具有权威机构的安全认证证书。

检查方法、步骤：通过查阅中间件产品的安全认证证书、提供确保通信的保密性、完整性和不可抵赖性的机制说明，查看为提供安全机制部署的安全设施；在技术条件允许的情况

下，截取部分报文或相关控制信息，分析安全机制是否有效。调阅材料：中间件产品安全认证证书，中间件产品的安全保障机制说明，电子报文。

检查项 2：中间件产品的访问认证机制

基本要求：中间件产品应当能够保证对系统和应用访问控制满足系统访问控制的要求，帐户和口令应当符合密码管理要求。

检查方法、步骤：通过查阅中间件产品的访问控制列表、中间件中数据访问组件的参数配置；测试用非法用户尝试访问的结果和产生的相关日志；涉及帐户和密码的参数是否用明文存储，且配置文件没有进行有效的访问控制。调阅材料：应用系统访问控制列表，中间件产品访问控制列表，配置参数。

检查项 3：中间件产品的管理控制台

基本要求：中间件产品的管理控制台应当得到有效控制，避免非授权用户的访问；应当避免通过管理控制台使用非授权帐户对系统和应用进行访问。

检查方法、步骤：查阅是否有限制管理控制台安装和使用的制度；测试管理控制台是否能直接使用非授权帐户对系统和应用进行访问。调阅材料：管理控制台使用限制规定，管理控制台使用手册。

检查项 4：单点故障问题和负载均衡

基本要求：中间件产品的是否存在单点故障问题，重要业务系统的中间件产品是否进行了必要的负载均衡机制，避免系统瓶颈的产生。

检查方法、步骤：查看中间件的系统设计文档和承载中间件的设备；重要业务系统中间件产品关于高可用性的设计说明。调阅材料：系统设计文档，设备。

19.4 灾备系统

检查项 1：中间件产品应急处理预案

基本要求：中间件产品应当建立明确清晰的应急处理预案和应急操作规程；并根据应用重要程度确定，应急恢复等级，确保重要业务的可靠运行。

检查方法、步骤：查看灾备系统中中间件的应急处理预案和操作规程；应用系统分级。调阅材料：应急预案，操作规程，系统分类。

检查项 2：中间件产品灾备系统

基本要求：灾备系统的中间件产品应当始终保持与生产系统版本和配置的一致；应当定期检查灾备系统中间件产品的健康状态。

检查方法、步骤：查看灾备系统中中间件产品的版本配置比较与生产系统的差异；灾备系统中间件产品的日常维护和检查记录。调阅材料：灾备系统中间件产品配置，日常维护记录，设备状态。

19.5 多应用中间件产品风险

检查项 1：业务流程管理

基本要求：多应用中间件产品的应用逻辑应当与业务流程建立清晰明确的匹配关系；并确保与业务匹配的组件、部件、应用工具、代码和技术支援方式被有效标识和关联。

检查方法、步骤：通过查阅银行业务系统逻辑和流程清单；组件、部件和应用工具及代码与业务系统的关系表。分析业务是否被有效管理，并在紧急情况下，是否能迅速获得相关支持。调阅材料：业务系统架构设计文档、中间件产品清单、应用系统设计文档。

检查项 2：应用关联管理

基本要求：多应用中间件产品的应用逻辑应当反应业务关联关系，以及业务依赖程度；

并对应用的风险转移和可能的衍生次生风险进行了有效识别。

检查方法、步骤：通过查阅银行应用逻辑和风险评估和分析文档，分析风险识别的有效性。调阅材料：应用逻辑、风险评估分析文档。

检查项 3：压力测试

基本要求：多应用中间件产品在多业务峰值情况下的压力测试，和业务冲击影响分析。

检查方法、步骤：通过查阅银行中间件压力测试报告。调阅材料：压力测试报告。

19.6 数据库中间件产品风险

检查项 1：数据库访问控制信息的保护

基本要求：中间件产品对数据库访问控制列表及相关帐户和密码信息应当得到有效控制，储存与终端设备的数据库连接信息应当使用密文存储，文件型的数据连接文档应当设置访问控制措施。

检查方法、步骤：通过查阅银行客户段和服务器段数据连接配置信息和参数配置工具，查看数据库帐户和密码控制的有效性。调阅材料：客户端数据库访问配置信息。

第四部分 · 应用系统

第四部分　应用系统

20. 应用系统

20.1 应用系统管理

检查项 1：应用系统管理制度

基本要求：银行业金融机构要加强应用系统的管理，建立相关规章制度。有条件的要指定负责应用系统管理的部门，确保每一个应用系统在系统生命周期内安全、稳健运行。

检查方法、步骤：1、查阅与应用系统相关规章制度，确认银行业金融机构是否建有有关应用系统管理的制度，并进一步分析制度是否能够满足工作需要；2、约谈应用系统管理部门负责人或负责应用系统管理的具体人员，分析应用系统管理制度是否得到实施，实施是否充分；3、查阅应用系统管理过程中的相关工作底稿，分析应用系统管理制度落实情况。

检查项 2：应用系统分类保护

基本要求：1、银行业金融机构应建立应用系统分类和保护体系，保证该体系在银行内部的贯彻落实；2、银行业金融机构应制定应用系统分类管理制度，对应用系统实施分类保护；3、银行业金融机构应对不同的应用系统进行安全评估，制定不同的防范措施，切实保护好各项应用系统，要按照《信息安全等级保护管理办法》的要求，对应用系统按照重要程度实行等级保护。对于安全等级确定为二级以上的应用系统，必须向公安等部门备案。

检查方法、步骤：1、约谈有关人员，了解是否建立了应用系统分级保护机制；2、调阅应用系统分级保护制度，了解是否已经建立次制度，对应用系统实施了分级保护机制；3、查阅有关工作底稿和应用系统评估报告，了解是否对应用系统进行了分级，并按照《信息安全等级保护管理办法》的要求对应用系统实施了响应的保护措施。重点关注二级以上的应用系

统是否按照规定落实了分级保护要求。

检查项 3：重要应用系统应具有审计功能

基本要求：银行业金融机构应建立应用系统安全审计机制，特别是重要的生产业务应用软件，要进行严格的安全审计。具体包括：1、应提供覆盖到每个用户的安全审计功能，对应用系统重要安全事件进行审计，要在关键的控制点或风险点进行输入验证和输出核对；2、应保证无法单独中断审计进程，无法删除、修改或覆盖审计记录；3、应用系统应具有可追溯性，应以书面或电子格式保存操作记录、交易流水等审计内容。审计记录的内容至少应包括事件的日期、时间、发起者信息、类型、描述和结果等；4、用户管理员应监控和审查未成功登录情况，和用户账户修改等异常情况，并随时记录和上报。

检查方法、步骤：1、查阅有关应用系统开发过程中有关设计文档，分析系统有无安全审计功能，必要时可以直接查阅系统源代码进行确认；2、约谈系统开发人员和系统操作人员应用系统是否有上述审计机制；3、有操作人员在终端登陆应用系统，观察是否有审计记录存在。

检查项 4：应用系统版本管理

基本要求：银行业金融机构应建立完善的应用系统变更管理制度和审批流程，并建立针对应用软件安全性、功能性的定期评估机制，根据评估结果实施软件版本变更。软件版本变更前应制定完善的测试方案，并保证测试过程的完整性（单元测试、集成测试、验收测试和试运行阶段）和测试内容的全面性（功能性测试和非功能性测试），并形成完整的测试文档。测试中如需使用生产数据，必须对相应数据进行脱敏、变形处理。

检查方法、步骤：1、与相关系统负责人进行访谈，以了解银行软件版本变更情况；2、调阅银行软件变更管理制度、相关评估机制，检查银行相关方面制度的完善性；3、查阅银行软件变更登记表及测试记录，验证版本更新前是否执行了相关操作；4、询问登记表中参与测试的人员，验证是否真正、负责的参与了软件测试；5、验证测试中使用的生产数据是否经过了脱敏、变形处理。

检查项 5：应用系统培训教育

基本要求：银行应根据应用软件需求举办相应培训，确保运行人员具有履行其角色所需的知识和技能，并定期进行考核。培训中应保证同一名员工不同时掌握应用软件安全机制、后台控制、前台操作的全过程。

检查方法、步骤：1、调阅银行与员工培训相关的制度，验证是否能够做到根据版本的更新进行跟踪培训；2、查阅培训记录并与软件版本升级记录进行对比，验证是否能够做到根据版本的更新进行跟踪培训；3、询问软件操作人员，验证其是否掌握应用软件安全机制、后台控制、前台操作的全过程。

20.2 应用系统安全

检查项 1：终端用户管理

基本要求：银行业金融机构应采取必要的措施，建立相应的安全制度，保证所有应用系统终端用户设备的安全，这些设备包括个人台式计算机（PC）、便携式计算机、柜员终端、自动柜员机（ATM）、存折打印机、借记卡或信用卡读卡机、销售终端机（POS）、个人数字助理（PDA）、移动存储介质等，定期对所有设备进行安全检查。

检查方法、步骤：１、调阅相关制度文件，是否已建立对于终端用户安全管理的制度；２、对于终端用户是否已经进行了分类，并依据分类采取不同的管控策略；３、机构是否已制定严密的权限控制措施，限制终端用户能够访问的各种资源；４、机构是否已采取对应得技术手段、配置合适的安全设备与软件，以控制终端用户私自更改系统配置，私自更改网络接口，私自安装监听软件、扫描软件、攻击软件、反编译软件和其它不安全软件；５、机构在终端用户所使用的软件应为授权许可的；６、对于离线式终端用户如便携式计算机、个人数字助理（PDA）、移动存储介质等是否建立接入前监测措施，同时按信息敏感度进行分级；７、是否对于终端用户建立了详实的档案登记，并按登记分级确定不同的巡检频率；８、调阅相关规范文件，对于有具体安全标准的要求的终端设备，机构是否已按安全标准与规范实施，并经过安全部门的认证。

检查项 2：访问控制

基本要求：根据不同的业务种类，不同安全系统等级，不同的网络边界，不同的操作权限，机构应制定一整套访问控制策略，该策略应可有效地区分不同的用户访问请求。机构应建立对应的访问监测系统，通过实时监测系统访问用户数量，保证系统访问可控，机构应根据被访问信息的类别选择相匹配的用户认证机制。

检查方法、步骤：1、调阅机构在应用系统中的用户列表，查看用户的权限赋予是否与用户的操作需求相一致；2、机构是否依据不同的业务种类、不同安全系统等级、不同的网络边界、不同的操作权限制定一整套访问控制策略，该策略是否以文档留存；3、机构的访问控制策略是否经过安全评估；4、机构是否依据系统等级分类不同，采用不同的物理技术手段对访问用户予以认证；5、机构是否采取合理的安全措施，保证正常访问，避免恶意访问和黑客攻击；6、对于有明确规定的访问控制要求，机构是否已按规定的内容实施，是否达到规定的要求；7、机构是否建立的访问监测体系，对访问进行实时监测；8、机构是否建立了访问控制事件处理流程，及时通过监测到的事件依流程进行处理；9、机构是否建立了访问控制信息的档案，以便在发生事件时查询；10、机构是否对于重要的访问控制日志文件进行备份，并定期进行回看；11、是否每位信息系统用户使用单独的账号进行操作，该用户身份发生变更时，其用户访问设定是否及时更改；12、用户的访问权限是否遵循最小权限原则。

检查项 3：保密机制

基本要求：银行业金融机构应采取可靠的加密技术，防范机密信息在应用系统或传输过程中丢失的风险。

检查步骤、方法：1、与信息安全管理人员会谈，了解各应用系统分级，并了解重要应用系统中敏感数据是否采取了适当的加密机制进行保护，制定并落实了有效的关键管理流程。利用公共网络传输业务数据的主干网络线路，应配备加密机；2、与信息安全管理人员会谈，了解所使用的加密设备应符合国家安全标准或要求，可以进一步调阅加密设备的相关认证资料，确认其符合国家安全标准要求；3、与信息安全管理人员会谈，了解对负责加密设备的员

工进行的培训和审查过程，可进一步调阅培训计划和审查材料，确认员工具备加密设备维护和管理的能力；4、与信息安全管理人员会谈，了解是否对加密的强度、长度、时效进行有效评估，并根据评估结果实施进一步的控制措施。可进一步调阅其审核和评估相关文档，确认审核和评估过程覆盖所有关键业务敏感数据；5、与信息安全管理人员会谈，了解其对加密信息实施加密的密钥管理流程，可调阅密钥管理的相关的制度及实施记录，确认银行业金融机构定期对密钥使用及保管情况进行检查的机制和紧急情况下销毁密钥的措施。调阅密钥生成、分发和销毁的相关记录，确认密钥的生成、分发和销毁经过了严格的批准过程，核心密钥保证至少双人操作；6、与信息安全管理人员会谈，了解是否有相关制度和流程，确保开发、测试和外包公司使用的数据是经过变形或脱敏处理之后的数据，确保数据的安全。

检查项 4：数据完整性

基本要求：银行业金融机构应针对应用系统的安全等级，对敏感数据实施采取适当措施防止敏感数据的泄露，并保证数据在生产、存储和传输过程中的完整性。

检查步骤、方法：1、与安全管理人员进行会谈，确认银行业金融机构是否对重要业务数据和系统管理数据和鉴别信息在传输、存储过程完整性进行了相应的管理。2、根据相应的管理机制和操作记录，确认银行业金融机构对数据完整性的破坏事件进行了识别和检测，并采取了相应的措施。3、与安全管理人员进行会谈，了解其是否对数据输入和修改过程实施了管控措施，确保业务数据记录完整，账务平衡。可进一步调阅数据的输入和修改的相关记录，确认其经过了完善的审批流程，并对输入操作进行安全控制，检测、防止对业务数据的恶意篡改。4、与安全管理人员进行会谈，了解其是否对输出数据进行了适当扫描和检测，以防止隐含的数据泄露和数据完整性被破坏。

检查项 5：数据准确性

基本要求：银行业金融机构对生产业务数据的添加、删除和修改应尽量使用账务冲正等会计手段实现，不得绕过业务操作界面进行后台操作。对于无法用会计手段实现的数据添加、删除和修改，应编制专门的程序对生产业务数据库进行后台操作，不得直接打开数据库进行

操作。

检查步骤、方法：1、与安全管理人员及维护人员进行会谈，了解银行业金融机构是否对生产业务数据的添加、删除和修改过程的控制措施。2、调阅相关生产业务数据添加、删除和修改的记录，确认其过程没有直接打开数据库进行操作。无法用应用系统直接实现的数据添加、删除和修改，应编制专门的程序对生产业务数据库进行后台操作，并经过严格的测试和审批过程。3、调阅相关生产业务数据添加、删除和修改的记录，确认对数据库的后台操作必须保证双人完成，并建立了严格的登记手续。登记表格的保管应等同于会计凭证，不得撕毁，并按照国家会计政策的要求予以保存。4、调阅对数据库进行生产数据变更操作的审批手续，确认经过业务部门和信息系统管理部门严格审批过程。

检查项 6：监督制约分级授权

基本要求：1、应制定严密的管理办法和操作流程，加强对生产业务系统账户，特别是柜员账户的创建、变更、交接、删除等操作的管理；2、应授予不同用户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系。业务应用系统应具有监督制约功能和分级授权功能，明确划分责任，对关键和敏感岗位或职能进行双重控制，做到双人操作，互相监督。对操作人员的权限进行限定，超过操作权限，应设定必要的授权控制。应制定明确的授权管理制度和授权控制列表，满足业务处理的保密性、安全性等要求；3、生产业务系统账户权限的授予一般应根据需要，由扎口业务部门统一向数据中心提出申请，审核后，数据中心指定专门安全管理人员开立账户，并做相应记录。

检查方法、步骤：1、调阅分级授权管理办法、操作流程，了解生产业务系统账户开立情况；2、抽查多个业务系统账户是否符合上述检查要求；3、约谈相关人员核实账户管理情况，并核查相应的开户记录。

检查项 7：日志管理机制

基本要求：1、银行业金融机构应用系统应具备日志功能，记录系统运行情况、系统运行状态、异常事项和人员登录、使用情况。银行业金融机构信息系统电子日志可以划分为两大

类：**交易日志**。交易日志由应用软件和数据库管理系统产生，包括身份认证尝试、数据修改、错误信息、交易内容、交易时间等。交易日志应按照国家会计政策的要求予以保存。**系统日志**。系统日志由操作系统、数据库系统、防火墙、入侵检测系统、交换机、路由器，以及出入口控制设备等生成，包括身份认证尝试、系统事件、网络事件、错误信息等。系统和网络日志保存期限至少应为一年;2、银行业金融机构应重视对电子日志的管理和应用分析;3、银行业金融机构应制定完善的指导意见和操作流程，控制所有生产系统的活动日志，以支持有效的审计、安全论证分析和预防欺诈;4、银行业金融机构应保证在电子日志中包含足够的项目，以便有效地满足内部控制、系统故障解决和审计等需求。应采取适当措施保证所有日志的计时同步;5、交易日志应作为生产系统的重要信息进行保存，每天随同生产业务数据进行备份保存;6、系统日志定期、集中保存，并由专人负责管理。各系统管理员不得接触系统日志;7、应分配充足的硬盘空间以防止日志文件被覆盖。日志应采取合理的格式保存，保证能够满足内部控制、系统故障解决和审计等需要;7、银行业金融机构应定期检查交易日志和系统日志，有任何的例外情况发生都应当复查系统日志。交易日志或数据库日志的复查频率和保留周期应由信息科技部门和有关业务部门共同决定，并报信息管理委员会批准。

检查方法、步骤：1、核查各重要应用系统是否具有日志功能，了解银行业金融机构有无日志管理机制；2、根据日志管理机制抽查多个业务系统的日志，检查其包含的信息，以及利用信息审计情况，判断其在审计中所起的作用；3、约谈相关人员，检查电子日志的维护情况是否符合以上规定。

检查项 8：备份、恢复机制

基本要求：1、应提供应用系统本地备份与恢复功能，应用系统变动（如版本升级）后应完全数据备份至少一次，备份介质场外存放。定期测试系统的备份，确保其处于可用状态，并记录测试情况；2、若异地灾难备份中心采用系统级备份策略，应确保备份中心系统备份及时更新，提供业务应用的无缝切换；应提供异地实时备份功能，利用通信网络将数据实时备份至灾难备份中心；3、关键业务应用系统应采取冗余和热备技术，避免存在应用系统单点故障。

检查方法、步骤：1、了解银行业金融机构应用系统相关的备份策略和制度，检查其制度落实情况；2、约谈相关人员了解应用系统备份以及备份的测试情况，对照记录进行核查；3、抽查业务应用系统结构，检查是否存在单点故障风险。

21. 电子银行

电子银行检查手册的编写依据是银监会颁发的《电子银行业务管理办法》及《电子银行安全评估指引》；手册中的电子银行包括网上银行、电话银行和手机银行，不包括 ATM、POS 等自助设备;手册中调阅的资料都包括网上银行、电话银行和手机银行的资料。

21.1 电子银行业务合规性

检查项 1：电子银行业务合规性

基本要求：1、银行在开办新的电子银行业务或者增加、变更原有的电子银行业务时，要符合《电子银行业务管理办法》的有关要求；2、金融机构应定期对电子银行业务发展与管理情况进行自我评估，并应每年编制《电子银行年度评估报告》报送银监会。

检查方法、步骤：1、按照《电子银行业务管理办法》第十五条的要求，调阅以下资料，检查资料是否齐全：1）由金融机构法定代表人签署的开办电子银行业务的申请报告；2）拟申请的电子银行业务类型及拟开展的业务种类；3）电子银行业务发展规划；4）电子银行业务运营设施与技术系统介绍；5）电子银行业务系统测试报告；6）电子银行安全评估报告；7）电子银行业务运行应急计划和业务连续性计划；8）电子银行业务风险管理体系及相应的规章制度；9）电子银行业务的管理部门、管理职责，以及主要负责人介绍。2、调阅银行目前开办的电子银行业务清单，访谈电子银行业务主管，了解是否增加或变更过电子银行业务类型，如有，按照《电子银行业务管理办法》第二十二条及第二十三条的要求，调阅有关资料，检查增加或变更的电子银行是否经过审批。3、访谈电子银行业务主管，了解电子银行业务运营系统和业务处理服务器的设置地点，如果是中资银行业机构，检查是否设置在中华人民共和国境内，如果是外资金融机构，如设置在境外，检查其在中华人民共和国境内是否设

置了可以记录和保存业务交易数据的设施设备，且能够满足金融监管部门现场检查的要求，在出现法律纠纷时，能够满足中国司法机构调查取证的要求；4、调阅《电子银行年度评估报告》，检查评估报告是否符合《电子银行业务管理办法》的第七十七条及第七十八条的要求。

21.2 电子银行风险管理组织体系及制度体系

检查项 1：组织体系及制度体系

基本要求：1、电子银行风险管理体系和内部控制体系应当具有清晰的管理架构、完善的规章制度和严格的内部授权控制机制。

检查方法、步骤：1、访谈电子银行业务部门主管，了解电子银行业务管理涉及的部门、岗位及其职责分工，检查各个部门、岗位的职责分工是否明确，检查是否建立了电子银行风险管理组织体系。2、调阅有关电子银行管理的内控制度，检查是否建立了电子银行内控体系。

21.3 电子银行安全管理

检查项 1：电子银行安全策略管理

基本要求：1、银行应当针对电子银行制定安全策略，安全策略应符合国家和银监会的有关要求。2、对安全策略应定期检查、测试，并根据实际情况适时调整，保证安全策略的持续有效和及时更新。

检查方法、步骤：1、访谈信息科技部门主管，调阅与电子银行安全策略相关的制度和资料，检查是否制定了统一的电子银行安全策略，电子银行的安全策略是否包括以下内容：1）网络安全策略；2）系统访问策略（操作系统、数据库、中间件、Web Server）；3）网银网站安全保护策略；4）数据传输保密策略；5）用户身份认证策略；6）客户信息（证书、账号、密码）安全保护策略；7）电子银行柜面管理安全策略等内容；2、调阅电子银行系统的网络架构、系统软硬件架构相关资料，检查是否符合安全策略的要求；3、访谈信息科技部门主管，调阅有关资料，了解电子银行安全策略的制定过程，检查安全策略的制定和变更是否经过正式审批；4、访谈信息安全管理部门，检查是否对安全策略的实施情况进行检查。

检查项 2：电子银行安全基础设施

基本要求：1、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；2、银行应采取适当的措施和采用适当的技术，识别与验证使用电子银行服务客户的真实、有效身份；3、银行应建立电子银行入侵侦测与入侵保护系统，实时监控电子银行的运行情况，定期对电子银行系统进行漏洞扫描；4、银行使用第三方认证系统对客户信息和交易信息等使用电子签名或电子认证时，应对第三方认证机构进行定期评估，保证有关认证安全可靠和具有公信力；5、银行应对客户数字证书载体（USB-Key）进行安全性测试，对 USB-Key 供应商资质进行定期评估。

检查方法、步骤：1、调阅电子银行数据加密技术的有关资料，检查是否符合国家有关规定；2、调阅有关电子银行客户的身份识别的有关技术资料，检查是否采取了措施识别与验证客户的真实、有效身份；3、调阅有关电子银行系统架构图，检查是否建立了电子银行入侵侦测与入侵保护系统；4、银行认证系统是否采用第三方认证系统，如果是第三方认证系统，调阅有关第三方认证机构的资质，检查是否具有国家颁发的认证资质；5、调阅有关 USB-Key 供应商的资质审查报告，以及 USB-Key 测试报告，检查 USB-Key 供应商资质是否经过审核，USB-Key 是否经过安全性测试。

检查项 3：电子银行安全监控

基本要求：1、银行应建立电子银行入侵侦测与入侵保护系统，实时监控电子银行的运行情况，定期对电子银行系统进行漏洞扫描，并建立对非法入侵的甄别、处理和报告机制；2、银行应当建立相应的机制，搜索、监测和处理假冒或有意设置类似于金融机构的电话、网站、短信号码等信息骗取客户资料的活动。

检查方法、步骤：1、访谈电子银行业务部门主管，调阅电子银行安全监控制度，检查是否制定了对电子银行非法入侵的甄别、处理和报告机制的相关制度；2、调阅电子银行安全监控相关报表，检查是否定期进行安全分析和处理；3、访谈电子银行业务部门主管，了解是否制定了相关制度或规定，搜索、监测和处理假冒或有意设置类似于金融机构的电话、网站、

短信号码等信息骗取客户资料的活动，是否收集、统计、分析电子银行安全事件（例如客户资金被盗），并采取措施提高系统安全性，同时加强客户宣传，保护客户资金安全。

检查项 4：电子银行安全评估

基本要求：1、银行应根据其电子银行发展和管理的需要，至少每 2 年对电子银行进行一次全面的安全评估；2、金融机构应建立电子银行安全评估的规章制度体系和工作规程，保证电子银行安全评估能够及时、客观地得以实施。

检查方法、步骤：1、访谈电子银行业务部门主管，调阅有关电子银行安全评估的规章制度，检查是否建立了电子银行安全评估的规章制度体系和工作规程；2、调阅电子银行安全评估资料，检查是否至少每 2 年进行一次全面地安全评估；3、调阅电子银行安全评估资料，检查其内容是否符合《电子银行安全评估指引》的要求。

21.4 电子银行可用性管理

检查项 1：电子银行基础设施（网络设备、通讯线路、主机设备、软件平台）

基本要求：1、电子银行基础设施应具备冗余性，消除单点故障；2、电子银行系统基础设施的性能应能满足当前及可预见将来业务发展的需要；3、电子银行系统基础设施能满足应对突发业务高峰的要求。

检查方法、步骤：1、调阅有关电子银行系统的软硬件配置资料、网络带宽及拓扑图，检查是否存在单点故障隐患，检查是否建立了负载均衡机制；2、调阅有关当前系统容量、性能、网络带宽利用率的资料，了解当前系统的运行情况，检查是否存在系统容量、性能不足的情况；3、调阅有关系统压力测试报告或系统性能评估报告，对比当前系统的实际交易量与系统可承受的最大交易量，检查系统是否满足应对突发业务高峰的要求。

检查项 2：电子银行性能容量管理

基本要求：1、银行应对电子银行系统的性能、容量进行监控，定期对电子银行系统进行

健康性检查和性能评估，确保电子银行系统的性能、容量持续地满足业务发展的需要。

检查方法、步骤：1、调阅有关性能及容量管理制度，检查是否建立了对电子银行系统的性能容量监控和评估机制，是否明确了系统评估的周期；2、调阅有关系统性能和容量的监控报表是否对电子银行主机系统、数据库系统的关键参数进行监控；3、调阅有关系统性能和容量的评估报告，检查是否对电子银行主机、数据库、中间件、Web Server 等进行了定期健康性检查和性能评估。

21.5 电子银行应急管理

检查项 1： 电子银行应急预案

基本要求：1、银行应按照《电子银行业务管理办法》的要求制定《电子银行业务运行应急计划和业务连续性计划》，并纳入总体应急预案体系中；2、应急预案应包括具体的检查和恢复操作手册，在操作手册中应明确责任人、责任分工、事件处理标准、操作步骤等。

检查方法、步骤：1、调阅有关电子银行系统的应急预案，检查是否按照《电子银行业务管理办法》的要求制定了《电子银行业务运行应急计划和业务连续性计划》；2、检查是否制定了电子银行系统相关的检查和恢复操作手册，手册是否得到定期的审阅，手册的内容是否具有明确的责任人、责任分工、事件处理标准、操作步骤等。

检查项 2：电子银行应急演练

基本要求：1、银行应定期组织对电子银行系统的应急演练；2、对应急演练的结果应进行总结和改进，完善电子银行应急预案和操作手册；3、应急演练应包含但不限于以下场景：1）网银系统安全事件（例如网站遭受攻击、网页遭篡改等）；2）电子银行系统故障事件（例如电子银行主机系统故障、软件系统故障等）。

检查方法、步骤：1、调阅有关电子银行系统应急演练的记录，检查是否进行应急演练；2、检查应急演练的内容是否包括系统安全事件、系统故障等内容；3、应急演练的内容是否包含上述基本要求第 3 条的内容。

22. 银行卡系统

22.1 银行卡系统管理

银行卡系统管理检查主要是对银行业金融机构涉及银行卡业务的主机（前置机）系统、网络的容量规划、监控和应急机制进行检查，涉及对客户信息、交易信息和技术外包商的管理等方面。银行卡系统包括处理本行信用卡业务的信用卡系统和转发他行卡交易信息的前置机或银联节点机。检查从管理制度、操作规范、连续性计划入手，采取调阅资料、询问责任人员、现场查看等方式进行风险确认和评估。

检查项 1： 银行卡系统容量的合理规划

基本要求：1、定期检查信用卡系统和前置机运行能力及容量，以应付银行卡业务的预期增长，并采取适当措施应对主机或前置机容量不足。2、定期对银行卡系统的网络运行状况，特别是与银行卡组织的外联网络运行状况进行审核分析，并采取适当措施应对网络容量不足。

检查方法、步骤：1、确定备查文件和询问人员。备查文件包括：
主机容量情况历史记录、与银联网络运行情况的历史记录、主机和银联网络扩容的情况记录；询问人员包括：主机和网络监控人员，主机和网络变更人员。2、检查银行业务连续性计划中关于主机和前置机定期检查或监控的工作。3、结合主机容量情况历史记录、网络运行情况历史记录，询问监控人员监控工作的执行情况，重点在发现问题后的报告路径和对外联系的措施以及银联网络质量的监控。4、结合主机和网络扩容的情况记录，询问变更人员变更工作的执行情况，重点在外联系统的变更程序和有效性。5、现场查看主机、前置机和网络运行的监控信息，并了解系统处理的峰值和目前主机利用率。6、了解是否有系统容量扩充的规划。

检查项 2： 银行卡系统物理设备风险和故障处理

基本要求：1、对关键主机和前置机、关键网络设备和线路，特别是与银行卡组织的外联网络设备和线路，须配备冗余，避免有单点故障。2、后备系统和网络设备应定期检测并维护更新。3、确保发卡中心和数据中心的物理安全。

检查方法、步骤：1、确定备查文件和询问人员。备查文件包括：主机和网络设备配备情况、备用设备的维护和更新记录、机房管理制度；询问人员包括：业务连续性计划管理人员、主机和网络管理人员，网络安全部门人员。2、检查关于主机（前置机）和网络的冗余配备有关情况，特别是外联网络设备和线路的冗余配备情况。3、结合备用设备的维护和更新记录，询问主机和网络管理人员关于备用设备和网络的定期检测和维护情况。4、询问主机和网络管理人员关于冗余设备的日常运行和维护、演练情况。5、结合机房管理制度，现场查看制卡机房、主机房和外联网络情况。

检查项 3 ：具有完备的银行卡系统应急预案并实施定期演练

基本要求：1、对银行卡系统的运行情况应具备实时监控能力，并能及时启动应急预案。2、具备银行卡业务安全事故处理应急预案，预案包括但不限于应对解决网络拥塞，服务中断，账户信息、交易数据遭到篡改、泄漏和破坏的安全事故。3、应急预案必须明确责任制，由银行高管层直接领导执行。4、应急预案必须进行定期演练，定期复核流程，并做好书面记录。5、应急预案必须包括外包服务商的应急服务协议。

检查方法、步骤：1、确定备查文件和询问人员。备查文件包括：银行卡业务安全事故处理应急预案、预案复核更新记录、预案演练记录；询问人员包括：业务连续性计划管理人员、银行卡系统监控人员、银行卡系统管理人员、主要外包商代表。2、检查业务连续性计划或银行卡业务安全事故处理应急预案，询问覆盖范围的情况。3、询问银行卡系统监控人员、银行卡系统管理人员关于日常运行监控的内容和启动应急预案的流程。4、调阅预案复核更新记录、预案演练记录，询问银行卡系统管理人员关于复核和演练频度、演练内容等情况。5、检查预案关于外包服务商的应急服务协议，询问外包服务商的相关措施。

检查项 4： 银行卡交易监控

基本要求：1、实施商户风险监控，对商户的交易行为进行事后监控，监控系统包括但不限于交易金额，笔数，退单，授权。2、实施银行卡监控，包括但不限于整数大额交易，商户

营业终了的交易，单笔交易异常增大，短时多笔交易，短时多地点交易。3、具备应对措施和报告机制，应对商户和客户的异常交易状况。

检查方法、步骤：1、确定备查文件和询问人员。备查文件包括：有关商户和客户交易的监控规范，商户监控情况记录、卡交易监控情况记录；询问人员包括：商户监控人员、交易监控人员。2、具备银行卡交易监控系统，检查银行交易监控规范中关于商户和客户异常交易的监控内容、应对措施和报告机制。3、询问商户监控人员关于事后商户监控的执行情况，查看商户监控情况记录。4、询问交易监控人员关于事后商户监控的执行情况，查看交易监控情况记录。

检查项 5： 账户密码和交易数据的存储和传输

基本要求：1、客户账户信息和交易数据必须在具有安全保护措施的主机和网络中存储、传输。2、必须使用硬件加解密设备生成、存储密钥，对个人密码的加解密和鉴别报文。密钥和个人密码的完整明文只能在存储在硬件加密设备中，不能在其他设备中出现。

检查方法、步骤：1、确定备查文件和询问人员。备查文件包括：该银行对银行卡密钥管理的有关规定，制卡业务流程；询问人员包括：网络管理人员，银行卡制卡部门管理人员、密钥管理的执行部门主管人员。2、检查该银行对银行卡密钥管理的有关规定，询问密钥管理的执行部门主管人员有关规定的执行情况。3、询问网络管理人员关加密网络中账户数据和交易数据的存储和流转情况。4、询问制卡部门的管理人员关于制卡业务流程的执行情况，特别是密钥生成和存储情况。5、询问相关人员密钥维护流程是否具有相应的安全控制措施（如双人操作等）。6、结合制卡业务流程，现场查看制卡机房，复核制卡流程。

检查项 6： 技术外包服务商管理

基本要求：1、发卡机构应审慎选择技术外包服务商，满足《银行业金融机构信息科技管理风险指引》关于外包服务商选择的要求，并与技术外包服务商签订安全保密协议。2、技术外包服务商必须满足信用卡组织的安保标准及规定。3、在与技术外包服务商签约前必须对服务商进行安全、保密、制度等方面的培训。4、对技术外包服务商必须定期进行服务质量和响

应时间的评估，并有惩戒性措施。5、应与电信部门和银行卡组织订具服务水平条款（SLA），并定期评价。

检查方法、步骤：1、确定备查文件和询问人员。备查文件包括：该银行技术外包服务商管理的有关规定，最近一次对技术外包服务商的评估文档，技术外包服务商安全保密协议和培训内容，主要技术外包服务商资质文件、与电信部门和银行卡组织的服务水平条款（SLA）及最近一次评价；询问人员包括：外包服务管理部门主管、主要技术外包服务商代表。2、检查该银行技术外包服务商管理的有关规定，询问外包服务管理部门主管关于技术外包服务商选取的标准和流程，了解最主要的三家技术外包服务商的情况。3、调阅与最主要的三家技术外包服务商签订的保密协议。4、调阅对最主要的三家技术外包服务商的安全、制度和保密方面的培训内容。5、调阅最主要的三家技术外包服务商的资质文件，并比对他们实际所从事的工作。6、结合最近一次对技术外包服务商的评估文档，询问外包服务管理部门主管关于评估内容的执行情况，重点是服务质量和响应时间，询问有关惩戒措施的执行情况。7、询问主要外包服务商代表关于资质、服务内容、响应时间和评估的执行情况。8、了解电信部门和银行卡组织的服务水平情况和对其评价情况。

22.2 终端设备

本部分主要针对自助银行设施、机具和 POS 机的软硬件进行检查。包括自助银行机具的物理安全、维护和更新；自助银行机具的安装环境；自助银行机具特别是离行式自助银行机具的通信安全；自助银行机具的保安情况和安全装置；自助银行机具软件的功能设置、维护和变更以及相关的问题处置流程；POS 机的检测和通信安全。

检查项 1：自助银行机具和安装环境的物理安全

基本要求：1、自助银行机具应符合相关的制造标准；2、自助银行机具的安装环境及相关设施应符合相关的标准；3、自助银行机具硬件的维护和更新情况；4、自助银行机具发生问题的处置流程。

检查方法、步骤：1、调阅自助银行机具的制造标准和验收记录；2、调阅自助银行机具

的安装环境标准，包括选址、供电、通讯等对自助银行机具正常使用造成影响的环境设施并进行现场抽查；3、调阅自助银行机具硬件设施的维护和更新记录，包括相关网络通讯设备等；4、调阅问题处置流程和处置记录；5、与自助银行机具的制造、安装和维护部门相关人员谈话了解执行情况。

检查项 2：自助银行机具的通信安全

基本要求：1、自助银行机具是否对交易数据进行了加密；2、自助银行机具通信发生问题的处置流程及其执行情况。

检查方法、步骤：1、询问自助银行机具的信息传输过程，了解自助银行机具交易数据的加密情况，特别是离行式自助银行机具的数据安全问题并进行现场抽查；2、询问是否制定了问题处置流程并落实到了具体的岗位和责任人，调阅相关的资料和执行记录并与相关人员谈话了解执行情况。。

检查项 3：自助银行机具的巡查维护

基本要求:1、自助银行机具的巡查制度是否符合相关的标准及其执行情况；2、自助银行机具维护是否符合相关的标准及其执行情况；3、发生问题的处置流程。

检查方法、步骤:1、调阅自助银行机具巡查记录；2、了解自助银行机具维护相关记录；3、询问是否建立了发生相关问题时的处置流程及其执行情况，并调阅相关的记录。

检查项 4：自助银行机具的安全装置

基本要求：1、自助银行机具是否安装了相关的安全装置来保障客户的使用安全；2、自助银行机具是否针对常发案件类型安装相关的安全设施。

检查方法、步骤：1、询问自助银行机具是否安装了类似密码遮盖、用户安全提示等相关保障客户安全的装置并进行抽查；2、询问是否针对常见案件安装了相关的安全装置，类似防侧录装置和后视镜等。

检查项 5：自助银行业务操作流程（机具软件）

基本要求：1、是否建立了安全机制来保障自助银行机具各项业务操作流程的安全使用；2、自助银行机具的密码显示方式和声音是否采取了安全设置来保证客户的安全使用；3、自助银行机具应根据相应的规定设置每日取款限额和次数；4、自助银行机具应进行吞卡设置并制定相应的后续处置流程。

检查方法、步骤：1、调阅自助银行机具的操作流程图，询问是否采取了例如限时操作等安全设置来保障客户的安全使用并进行现场演示；2、询问是否采取了密码输入掩码显示和不同数字不区分声音等安全设置并进行现场检查；3、询问是否依据有关规定采取了每日取款限额和次数的限制，调阅相关的规定；4、询问自助银行机具吞卡设置和后续处置流程及其执行情况，调阅相关的制度和记录。

检查项 6：自助银行机具软件的维护和更新

基本要求：1、是否制定了相关的制度、流程对自助银行机具软件进行定期的检测和维护；2、是否建立了机具软件发生问题的处置流程 3、是否制定了软件变更的相关制度、审批流程及其执行情况；4、是否制定了软件变更的相应操作流程及其执行情况；5、软件变更所涉及到的相关业务部门是否参与了该变更的审批、测试和执行；6、是否对于比较重大的变更建立了变更的回滚程序并进行了测试；7、进行机具软件维护和更新的相关人员是否具备了相关的资质并进行了培训。

检查方法、步骤：1、询问相关人员了解检修维护、变更和问题处置的流程和执行情况，调阅相关的制度、流程和操作记录；2、了解维护、变更人员的资质能力和业务水平，调阅相关的人员资料和培训记录。

检查项 7：POS 机

基本要求包括：1、对商户的 POS 机使用情况必须进行检查或抽查，检查或抽查内容应包括 POS 机安装环境（安全保卫、侧录风险等）、运行状态和操作情况等；2、是否采取了

相关的安全措施来保障 POS 机的网络通信。

检查方法、步骤：1、调阅 POS 机管理的有关规定， POS 机检查的记录文档，询问商户管理部门人员有关 POS 机管理日常工作，检查或抽查的内容；2、了解 POS 机的网络接入方式，询问是否采取了相关的安全措施来保障网络通信的安全和畅通，调阅相关的记录。

22.3 自助银行监控

本部分主要针对自助银行的监控进行检查。包括自助银行设备日常运行的监控情况；监控中心和监控设备本身的维护、更新和监控；监控发现问题的具体处置流程、人员落实情况；自助银行设施、监控的定期评估情况等。

检查项 1：自助银行设备日常运行的监控情况

基本要求：1、是否建立了相关的监控制度、监控人员管理制度及其执行情况；2、监控的范围是否达到 100％的覆盖率；3、所有的自助银行设备是否都进行了定期的轮巡监控；4、监控的录像和监控记录的保存情况。

检查方法、步骤：1、调阅自助银行相关设备的监控制度、人员管理制度，查看是否都落实到具体岗位和责任人；2、询问监控的覆盖率、轮巡频率等相关参数和监控录像的保存时间是否符合相关的规定和标准，调阅自助银行设备的监控记录和人员管理记录；3、现场了解监控实际情况并对覆盖率等参数进行检查。

检查项 2：监控中心和监控设备

基本要求：1、监控中心的相关设施和监控设备是否符合相关的标准；2、监控设备的运行是否进行了实时监控；3、监控设备出现问题的处置流程；4、监控中心和监控设备的维护制度和更新情况。

检查方法、步骤：1、询问是否建立了监控中心来统一监控所有的自助银行设施，调阅监控中心的各项指标，包括位置、空调、电力等相关指标；2、调阅监控中心设备和监控设备的清单及相关指标，了解各项设备的功能和运行情况；3、询问监控中心和监控设备的监控情况，

发生问题的处置流程。了解设备的维护、更新情况，调阅相关的制度和监控、维护、更新记录以及问题的处置记录。

检查项 3：自助银行监控发现问题的处置情况

基本要求：1、是否建立了监控发现问题的处置流程，是否落实到了具体岗位和责任人；2、监控发现问题的响应、处置的执行情况；3、是否进行相关的培训和演练；4、监控处置流程的修订情况。

检查方法、步骤：1、询问发现问题的处置流程和具体执行情况，调阅相关的文件和制度，相应的工作记录和日志；2、询问问题处置流程相关人员的培训情况，处置流程的演练情况，以及处置流程是否定期进行评估和修订，调阅培训记录，培训资料，演练记录和修订记录等。

检查项 4：自助银行设施安全评估（信息科技方面）

基本要求：1、是否定期召开会议对自助银行设施、自助银行机具及自助银行的监控等方面进行评估；2、是否对自助银行相关的常见案件类型采取相应的应对措施。

检查方法、步骤：1、了解银行是否定期对自助银行相关进行评估，参与的部门，评估的内容以及后续整改意见的落实（信息科技方面）；2、了解银行是否对自助银行相关的常见案件采取相应的应对措施（信息科技方面）。

23. 重要应用系统信息流程及主要风险点

从广义上讲，金融机构的电子化涉及商业银行各项业务操作。传统的金融电子化着重于用信息技术模拟现行手工处理流程来处理银行交易和输出格式化的信息，而忽视了银行内部业务活动和流程的改造，使信息技术很难发挥其在降低经营成本、提高管理效率和质量、吸引客户等方面的应有作用。90 年代初开始，美国商业银行开始进行“业务再造”（Business Reengineering），根据新的管理理论和方法，结合信息技术的特点和功能，重新定义银行的信息流，用信息技术手段更新业务流程，从而直接创造利润。

随着金融电子化的发展，商业银行的业务流程发生了很大改变，过去为保证业务正常运行而制订的各项内控措施很多已不适应，都应相应做出调整和改变。而电子技术对金融业务的改造才刚刚开始，新技术、新产品、新理念日新月异。加之时间短，各商业银行对在电子化业务处理方式这一新形势下如何加强内控，有一个认识和发展的过程，因此规章制度、内部控制措施都有待加强。

23.1 核心（综合）业务系统电子流程

核心（综合）业务系统就是银行进行日常营业使用的，以会计核算为基础，面向银行管理和业务，集中、统一的业务处理系统。银行核心（综合）业务系统作为银行业务运行的最基本的支撑平台，是所有其它银行电子化产品得以应用的前提。可以说，银行的每一笔交易，都离不开综合业务系统。

银行传统的柜台业务，实行双人临柜制度，只有会计、出纳同时在场，才能够正常办理业务，所以各项内部控制规章制度也是根据这一工作方式制订的。随着电子技术的飞速发展，目前各商业银行普遍实行综合柜员制度，一人临柜，处理各项业务，综合业务系统处理业务的模式有了很大变化。在这种工作方式下，内控风险点发生了变化，内控措施也要相应做出改变。

在数据大集中的工作模式下，目前各商业银行综合业务系统电子信息处理流程大体如下页图所示。

从下面的流程图中可以看出，一，综合柜员制下，会计与出纳双重不兼容身份必然集于一身。二，取消了复核这一环节，不再有事中监督。三，会计主管卡与柜员操作卡互相不兼容。四，事后监督存在至少一天的时间差。这几个方面，正是检查中应重点关注的问题。

核心（综合）业务系统的风险点，主要包括以下几个方面。

1、核心业务系统是否具有**身份验证功能**，防止非法用户随意进入系统；**访问控制功能**，防止系统出现越权访问；**故障恢复功能**，能够自动或在人工干预下从故障状态恢复到正常状态而不致造成系统混乱和数据丢失；**安全保护功能**，对信息的交换、传输、存储提供安全保护；**安全审计功能**，便于系统建立用户访问系统资源的审计功能。

2、业务操作是否具有**分权制约功能**。在综合柜员工作模式下，会计和出纳双重不兼容身份由一人担任，如何对柜员进行风险控制呢？目前各商业银行普遍的做法是，小额放开，大额授权。核心业务系统分级设置柜员权限，现金业务 5 万元以下、转账业务 20 万元以下不需要授权，由一般柜员单独即可完成。超过以上限额，则必须由高一级的柜员或会计主管授权。检查时，应查看核心业务系统是否对大额业务设置了授权功能，授权限额是否合理。

查看更改存贷款利息、更改起息日是否需要授权；

查看柜员查询客户账户信息是否需要输入账户密码，如不需要输入密码，是否需要授权；

查看错帐当日冲正、错账隔日冲正是否需要授权；

查看挂失、解挂、冻结、解冻等特权操作是否需要授权。

3、柜员管理情况。首先，金融机构应制订严密的柜员管理办法，对柜员的创建、变更、交接、删除等各个方面进行有效管理，并保证以上各项操作由双人完成。其次，核心业务系统应具备柜员账号管理功能，系统应能够显示或打印分支机构内柜员名单。如果系统无法显示或打印分支机构内柜员名单，则核心业务系统不完善，对柜员管理不严密。

现场查看柜员登记簿，再从系统中打印出该分支机构的柜员清单，互相比较，检查是否存在未登记的隐身柜员。

查看核心业务系统是否对柜员的密码、时效、复杂性进行有效控制。

4、柜员卡的使用情况。柜员应妥善保管自己的柜员卡，不能混用、借用。主管卡或授权卡应由会计主管或相应人员保管，设置密码并定期修改。会计主管卡或授权卡不能操作业务。另外柜员离开工作岗位，应及时从系统中签退。在现场检查中，经常见到营业员将柜员卡随意放在桌子上，或人离开柜台，而没有从系统中及时签退的现象。

5、录像监控状况。按照要求，营业场所应安装录像监控装置，并且监控录像保存期限不能少于三个月。

23.2 ATM（CDM/CDS）业务处理流程及内控关键点

ATM 是英文(Automatic Teller Machine)缩写，中文译为“自动柜员机”，主要具有取现、查询、更改密码（跨行无更改密码功能）等功能。它是利用计算机网络来实现交易信息的高

速传送，并应用自动控制技术来联机适时处理信用卡交易，从而代替银行柜员手工操作的自动化金融设备。

ATM 机基本操作流程为：①按提示插入银行卡；②根据屏幕提示，输入个人密码；③依照屏幕所示，按功能键，如“查询”、“取款”等进行业务操作。④如做“取款”交易，请按键盘上的数字输入所需提款数额，再按“确认键”。操作完毕请取回信用卡及钞票和凭条。⑤如作“查询”交易，屏幕将显示您的存款余额和当日在取款机上的可用余额。操作完毕请按“取消”键，取回卡。

ATM 如遇下列情况之一可能出现“吃卡”：①操作不当；②该银行卡已列入止付名单；③卡过期；④卡磁条损坏。

ATM 如遇下列情况，交易不成功：①发卡行主机因故关机；②通讯线路堵塞；③ATM 机出现机械故障；④ATM 内钞票已使用完毕。

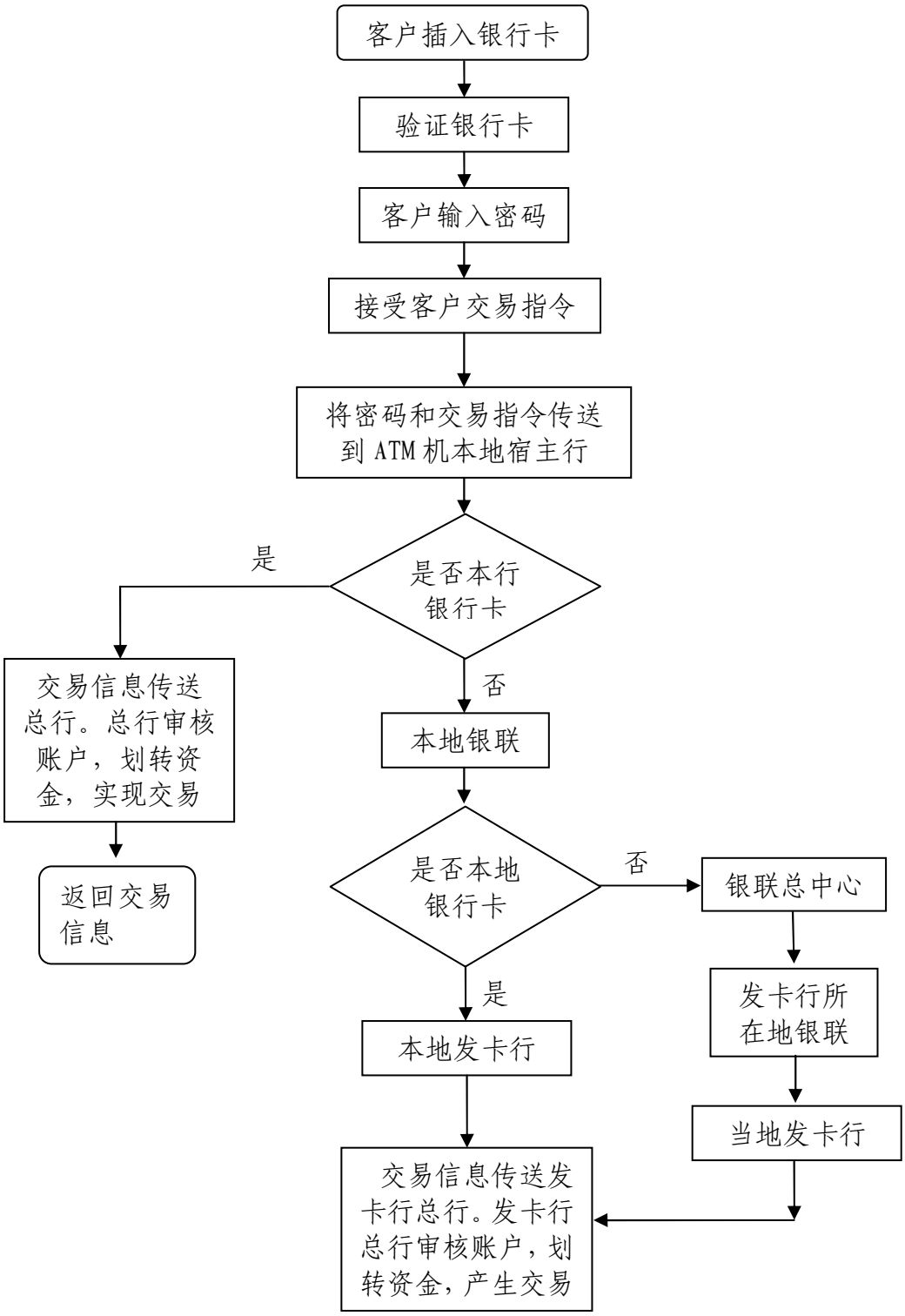
ATM 机直接连接到银行的核心业务系统，且 ATM 机一般设置在公共场所，因此犯罪分子利用 ATM 机作案时有发生。因此，金融机构应加强对 ATM 机的管理。

另外，各金融机构设立了很多自助银行服务网点，网点没有工作人员，或只有一个安全服务人员值班。网点内一般设有自助存款机（CDM）、自助取款机（ATM）、业务查询机等各类电子服务设施，各项银行业务由客户通过电子银行设施自助办理。对自助银行网点的要求比较严格。

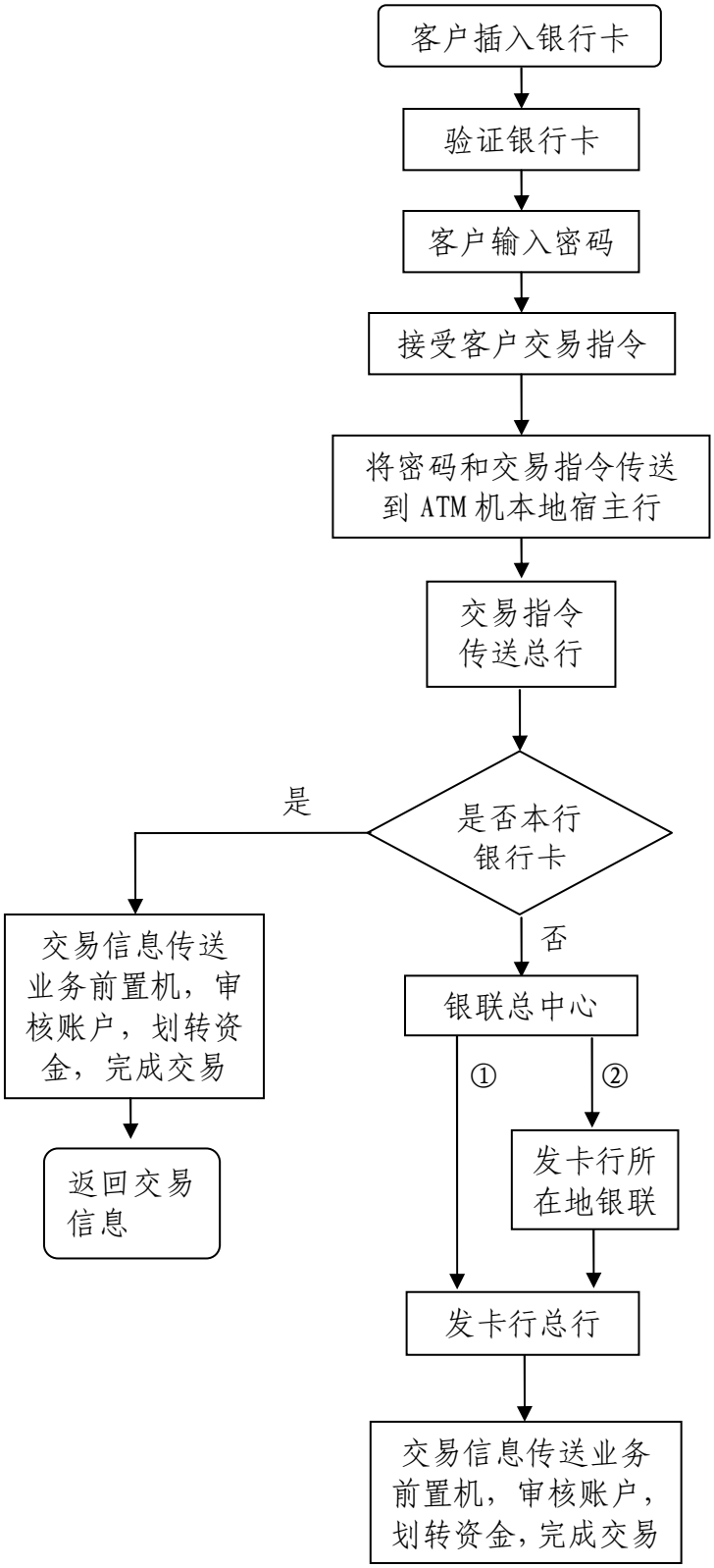
ATM 机业务信息传递流程有多种情况，各家行采取的模式不一样。下页二流程图是目前用得较多的。以前模式一用得较多，称为有区域中心交易模式。现在各行逐步采用模式二，称为无区域中心交易模式。模式二中，当数据包传递到银联总中心后，又有二种交易途径。实行数据大集中的银行一般采用途径①。没有实行数据大集中的行，及城市商业银行等地方法人金融机构一般采用途径②。

ATM 机系统及自助银行网点主要风险包括以下几个方面：

1、是否制订了完善的规章制度和严密的操作流程以对 ATM 机业务进行有效管理。


客户插入银行卡
验证银行卡
客户输入密码
接受客户交易指令
将密码和交易指令传送到 ATM 机本地宿主行
是否本行银行卡
是
否
交易信息传送总行。总行审核账户，划转资金，实现交易
返回交易信息
本地银联
是否本地银行卡
否
银联总中心
发卡行所在地银联
当地发卡行
是
本地发卡行
交易信息传送发卡行总行。发卡行总行审核账户，划转资金，产生交易

ATM 机交易模式一


客户插入银行卡
验证银行卡
客户输入密码
接受客户交易指令
将密码和交易指令传送到 ATM 机本地宿主行
交易指令传送总行
是否本行银行卡
是
否
交易信息传送业务前置机，审核账户，划转资金，完成交易
返回交易信息
银联总中心
①
②
发卡行所在地银联
发卡行总行
交易信息传送业务前置机，审核账户，划转资金，完成交易

ATM 机交易模式二

2、是否建立了 ATM 机运行所必需的各类登记簿，如加钞登记簿、维护登记簿、长短款登记簿、吞卡及返还登记簿、尾箱清查登记簿（清机登记簿）、设备运行日志簿等。

3、ATM 前置机是否有备份，是否有运行日志。是否定期检查 ATM 机监控录像，监控录像是否保存足够时间。运行日志是 ATM 机打印的持卡人交易的原始凭证和自助设备工作过程的完整记录，因此必须保证字迹清晰、内容完整。

4、ATM 机对取款、转账是否有限额，限额是否有自动累加功能。按照相关规定，ATM 机每次取款不能超过一定限额，每天累计取款也有限额。在现场检查中，曾发现某银行 ATM 机虽然对取款、转账设置了限额，但是系统没有自动累加功能，如果换一台 ATM 机，又可以取款和转账。

5、是否建立自助银行服务网点突发事件处置预案；是否有专人负责自助银行相关的监控、报警、消防等系统的安全。

完善的自助银行网点的服务区内应提供自助设备操作使用说明、客户投诉用电话、投诉表、意见薄、报警装置等。自助银行内必须安装性能可靠的防抢、防盗、防火、监控和防非法侵入（门禁）等安全防范设施和报警系统，报警系统要与监控中心、当地公安机关联网，做出声、光提示，并记录有关信息，自助银行必须安装火灾报警和气体消防灭火系统，自助银行必须安装全方位的闭路电视监控系统，实施 24 小时的全景实时监控录像。监控范围应应能完整清晰记录出入口的人员和自助设备操作人员。自助银行网点内应在明显位置张贴便于客户使用的文字说明和操作流程介绍，要建立自助银行安全日志。全面记录自助银行的安全防护设施、报警系统运行情况，日常检查、事故及设备维护等情况。

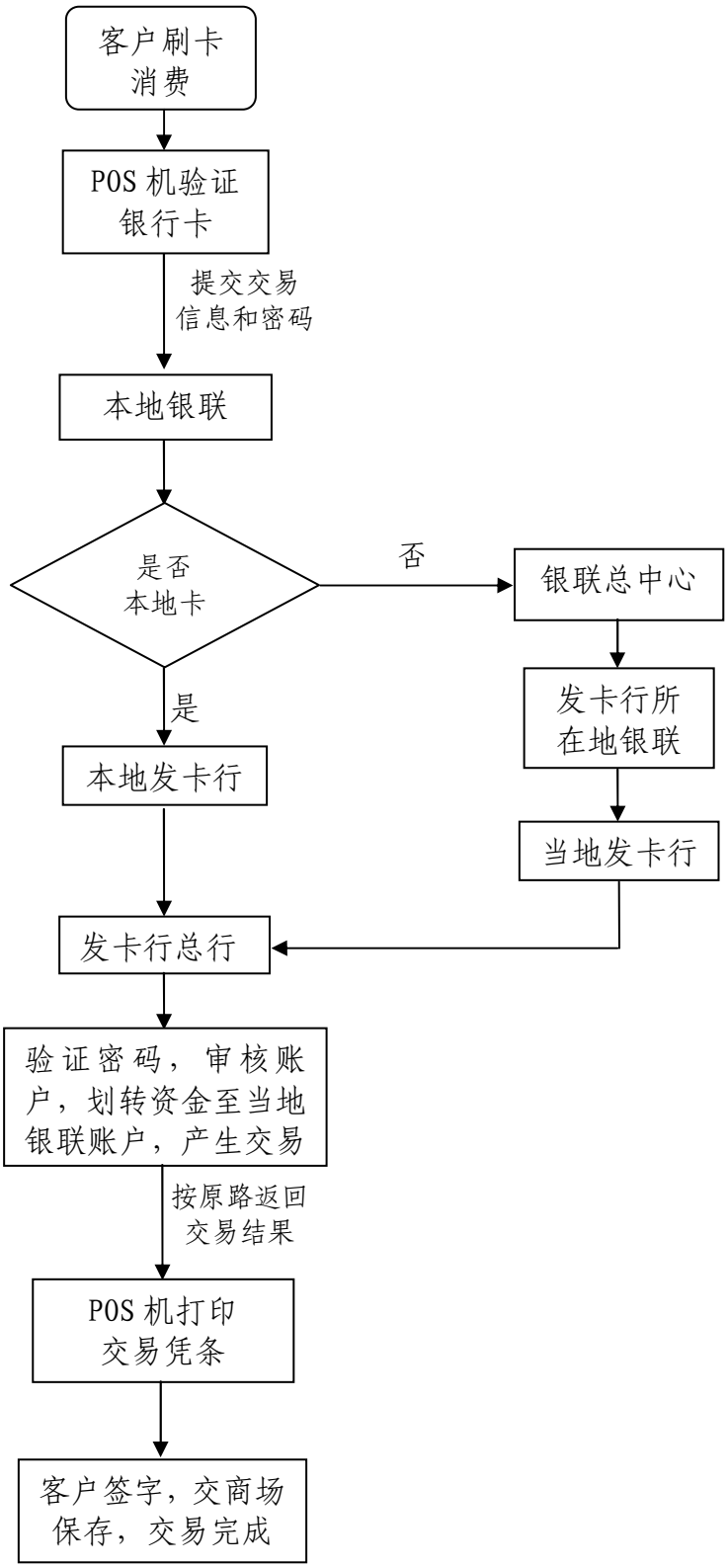
23.3 POS 业务处理流程及内控关键点

POS 机最早是各商业银行与商家为便利客户消费，在商场设立的远程自助结算柜台，POS 机通过网络互联，直接联接到特定银行的数据中心，由商户和银行之间结算。开始，各家银行各自为战，自己发展商户市场，因此人们可以看到在 2002 年以前，各商场的收银台上摆放着多家银行的 POS 机。这既给客户的使用带来了很多麻烦，也带来了安全隐患。进入新世纪，随着金卡工程的实施和完成，各家银行通过银联实现了互联互通，实时结算，POS

机已不再和某一银行通过网络互联，而是直接联接到银联公司，由银联进行资金清算，这类POS 机可以称为直连 POS 机。但在某些特殊的场合，目前仍然有直接连接到金融机构，而不通过银联的 POS 机。如在某些大型宾馆、高速公路收费站等地方设置的 POS 机，一般不通过银联结算，而是直接连接到某一金融机构。这类 POS 机可以称为间连 POS 机。

操作 POS 的基本流程为：刷卡----输入金额----持卡人在密码键盘上输入密码----交易成功，打印签购单，持卡人签名。密码和签名是保证持卡人资金安全的手段。

POS 交易有时不成功，可能有以下几个原因：①发卡行主机因故关闭；②通信线路故障；③POS 设备故障；④密码不对或磁条损坏；⑤操作不当。


客户刷卡
消费
POS 机验证
银行卡
提交交易
信息和密码
本地银联
是否
本地卡
否
银联总中心
是
发卡行所
在地银联
本地发卡行
当地发卡行
发卡行总行
验证密码，审核账户，划转资金至当地银联账户，产生交易
按原路返回
交易结果
POS 机打印
交易凭条
客户签字，交商场保存，交易完成

POS 机业务操作流程

交易如果不成功，可能出现以下问题：①因重复操作发生重复扣帐；②交易不成功扣帐。

下图为 POS 机业务流程图。和 ATM 机一样，POS 机的信息传递流程也有多种，这里不再详细介绍。每日营业终了由发卡行与当地银联进行清算。商场定期凭客户签字的交易凭条与银联进行资金清算。

POS 业务的风险点，应主要包括以下方面：

1、银行是否制订了规章制度和业务流程对 POS 机业务进行管理。

2、POS 机业务前置机是否能够安全管理，是否有流水日志，是否定期与银联进行账务核对，是否将商场提交的客户签字购物凭条与银联提交的交易流水仔细进行事后监督。

3、特约商户 POS 机连接方式是否安全，对特约商户的审查是否严格，是否签订严密的合同。是否定期与特约商户进行账务核对。

4、如果 POS 机交易不成功，处理方式是否合适。如果账务不平，如何处理。

23.4 网上银行业务处理流程及内控关键点

网上银行（Banking online）又称网络银行。按照《电子银行管理办法》第二条的规定，网上银行业务是指利用计算机和互联网开展的银行业务。网上银行业务的主要特点是客户通过互联网访问银行网站，自助办理银行业务。

所有电子银行业务一般不设单独的账务体系，从信息流的角度看，电子银行和柜台业务只是业务渠道的差别，银行内部账务系统是一样的，都是由银行的核心业务系统统一处理的。下面详细介绍网上银行的业务处理过程和方式。

网上银行业务在会计处理上可分为两类，即系统内业务与系统外业务。其中系统内业务又分为分行辖内和总行辖内两种。分行辖内业务以分辖通存通兑方式实现，总行辖内业务及系统外业务以代理行方式实现，即由代理行落地处理。所谓代理行，是指客户在网上通过网上银行发出转账指令后，其指令内容由该行指定某一机构统一打印并提出交换或发出报单，该机构即为代理行。

①、分行辖内业务：由系统自动进行通存通兑处理，会计分录为：

付款行：

借：XX 存款科目（付款账户）

贷：通存通兑往来资金清算　分辖通存通兑

收款行：

借：通存通兑往来资金清算　　分辖通存通兑

贷：XX 存款科目（收款账户）

若收款方与付款方在同一机构开户，会计分录为：

借：XX 存款科目（付款账户）

贷：XX 存款科目（收款账户）

次日营业开始，各机构专门柜员启用“打印网上汇款票据”交易，打印网上汇款清单，加盖业务公章代传票入帐，同时打印“网上银行客户回单”并加盖转讫章，作为客户入帐凭证。

②、总行辖内业务：经总行进行结算，发往代理行做总辖电子联行处理。会计分录为：

代理行：

借：通存通兑往来资金清算

贷：总行辖内往来

付款行：

借：XX 存款科目（付款科目）

贷：通存通兑往来资金清算

收款行：

借：总行辖内往来

贷：XX 存款科目（收款账户）

当日代理行启用联行交易打印报单，加押后发送，并打印“网上汇款清单”核查。次日营业开始，代理行启用联行交易查询是否有未加押报单（一般是客户在银行机构每日日结后，比如晚上 12 点，发出的总辖指令），如果有，则打印后加押发送。然后各机构专门柜员打印出网上汇款清单，加盖业务公章作为传票入帐，同时打印“网上银行客户回单”并加盖“转讫”章，作为客户入帐的凭证。

③、系统外业务：经总行结算，发往代理行通过大、小额支付系统或同城票据交换进行

处理。会计分录为：

代理行：

借：通存通兑往来资金清算

贷：同城票据交换

付款行：

借：XX 存款科目（付款账户）

贷：通存通兑往来资金清算

当日，代理行打印进帐单和电汇凭证，加盖业务公章后提出交换，并打印“网上汇款清单”核查。次日营业开始，代理行打印前一天未提出交换的进帐单和电汇凭证（客户在代理行停止当天交换后发出的票据交换指令），加盖业务公章后提出同城交换。然后各机构打印“网上汇款清单”加盖业务公章后代传票入帐，同时打印“网上银行客户回单”并加盖转讫章，作为客户入帐凭证。

以上我们以转账业务为例，详细介绍了网上银行业务的会计处理方法。其它如代发工资、代交费、扣收代办费用等，会计处理方式类似，这里就不详细介绍了。

网上银行作为新兴的业务方式，除了存在和传统业务一样的风险外，还突出存在技术风险、操作风险、信誉风险和法律风险。

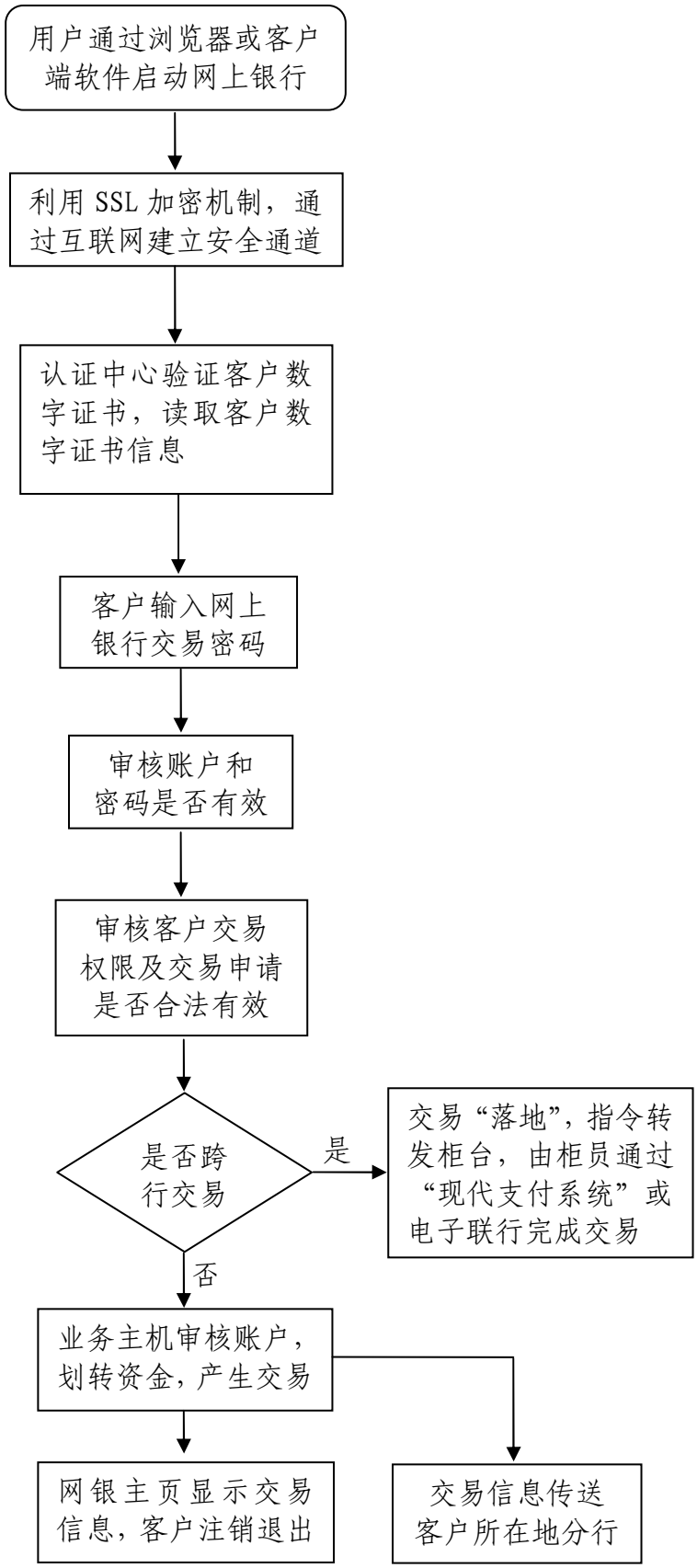
技术风险。由于网络的开放性、匿名性和技术复杂性，电子银行业务面临比传统服务渠道更大的操作风险，如来自外部的非法进入，来自内部的越权使用数据，“黑客”和病毒攻击，系统故障导致的数据丢失等。银行电子系统在客户身份鉴别、数据保护、业务审计、客户隐私保护等方面较容易出现漏洞和延误。

操作风险。企业或个人开办网上银行业务，从另一个角度讲，就是将该企业或个人的账户交给网上银行的申请人自行管理。因此，申请人是否为账户的主人，或是否为账户主人授权操作的人，是至关重要的。银行在审核客户开办网上银行业务的各项操作时，必须制订严格的规章制度，设计严密的操作流程，并审核和保存好各项证明材料，以保证网上银行业务的申请人为账户的主人或其授权的人，防范操作风险，同时也防范法律风险。最近金融机构发生的网上银行案件，有很多是因为开办网上银行业务的申请人，不是账户的主人或账户主

人授权的人，而是犯罪分子，或银行内部员工冒充账户主人开办而产生的。发生的原因是银行员工没有严格执行规章制度，对开办网上银行的资料审查不严格，或没有严格保管好客户的开户资料，或没有将客户的数字证书和网上银行交易口令直接交付到客户手中，而是由客户经理或其他人代收。

信誉风险。电子银行业务使银行面临更大的信誉风险。一个银行开办电子银行业务，如果不能很好控制各类风险，一旦出现问题，可能使银行多年辛苦建立起来的信誉毁于一旦。在目前情况下，因为客户对电子银行业务技术层面的不熟悉，及虚拟交易的不可见性，人们对钢筋水泥构筑实实在在的银行有更多的安全感，对使用电子银行服务渠道多数是尝试性的，一次尝试失败就很可能使客户完全否定这一服务渠道，如果客户在某银行提供的电子银行服务尝试失败，将导致对该银行整个服务的怀疑或否定，该银行的信誉将受到严重损害。

法律风险。对电子银行法律的不熟悉和电子银行相关法律本身的不完善、不确定性使法律风险也显著增大。目前，各国都在积极探索与电子银行相关的法律问题，但到目前为止仍然很不完善，特别是缺乏国际公认的法律规范体系，因而发展电子银行业务面临的是一个正


用户通过浏览器或客户端软件启动网上银行
利用 SSL 加密机制，通过互联网建立安全通道
认证中心验证客户数字证书，读取客户数字证书信息
客户输入网上银行交易密码
审核账户和密码是否有效
审核客户交易权限及交易申请是否合法有效
是否跨行交易
是
交易“落地”，指令转发柜台，由柜员通过“现代支付系统”或电子联行完成交易
否
业务主机审核账户，划转资金，产生交易
网银主页显示交易信息，客户注销退出
交易信息传送客户所在地分行

网上银行业务流程图

在演进中的、带有很大不确定性的法律环境。另外，由于法律的国别差异，开展跨国电子银行业务法律风险更大。

网上银行的业务流程如下页图所示。

网上银行业务的风险点，主要包括以下几个方面：

1、网上银行业务开办过程中，是否建立严格的规章制度和操作流程进行安全控制。

2、银行自身的数字证书是否严格管理，是否有在紧急情况下销毁数字证书的措施。从前面基础知识介绍中，我们知道客户进行网上银行业务操作，交易数据包是用银行的公开密钥加密，通过安全传输通道传输到银行，银行利用自己的私人密钥解密，接受客户的交易请求，因此银行自身的数字证书是该行最核心的机密。如果银行自身的数字证书丢失或被窃取，则所有网上银行业务将没有任何秘密保障和安全保障。银行自身的数字证书应严密保管，并用密码信封封存备份，并有在紧急情况下销毁数字证书的措施。

3、银行开办的网上银行业务是否与申请开办的经营范围一致。查看银行向监管部门申请开办网上银行业务的申请和批复文件，并在
线查看该行的网上银行页面，检查开办的业务与被批准开办的业务范围是否一致，是否超范围经营。

4、银行在网页上对客户声明的协议是否合法有效，是否发布违规广告，是否违法经营。

5、是否采取了有效手段保证网络系统安全。开办网上银行业务，是否经过银监会认可的，具有相关资质的机构进行安全评估。金融机构开办网上银行业务，需要银行内部网络和互联网连接。因此对隔离和防护措施要求严格。银行应使用防火墙、加密机、入侵检测、病毒防护等足够的技术手段来有效隔离内外网，保护数据安全。在电子银行基础设施检查中，将详细介绍检查内容和方法。

6、银行内部网络是否进行有效隔离，是否进行必要的网段划分。网上银行业务面对所有公共网络用户，提供全天的服务，既需要防范来自整个公共网络的风险和攻击，也需要防范来自银行内部的攻击和误操作。银行应有效隔离内部网络，与业务生产无关的计算机和系统不得接入生产业务网段。分支机构也应合理进行网络划分。

7、如果开通支付网关功能，是否和商场或其它机构进行数据交换和转移，数据交换和转

移是否安全，是否合法合规。。

8、电子签名是否满足《电子签名法》的要求，身份验证系统（RA）是否严密有效，网上银行开办手续是否完善、严格，是否验证客户的身份有效证件、企业有效证件、企业营业执照、客户或企业法人代表签名、企业预留印鉴，是否妥善保管与客户签订的网上银行协议书、账户授权申请表、客户签领数字证书证明、数字证书发放记录、发放客户网上银行交易口令记录。要严格审查客户签名是否真实，企业网上银行申请表上的公章是否为企业预留的公章，防止出现未经许可由他人私自代为开办网上银行的情况。

9、银行对数字证书的管理是否严格，系统管理员、应用程序管理员、证书管理员是否由不同人员担任。是否对网上银行管理员登录地址严格保密。

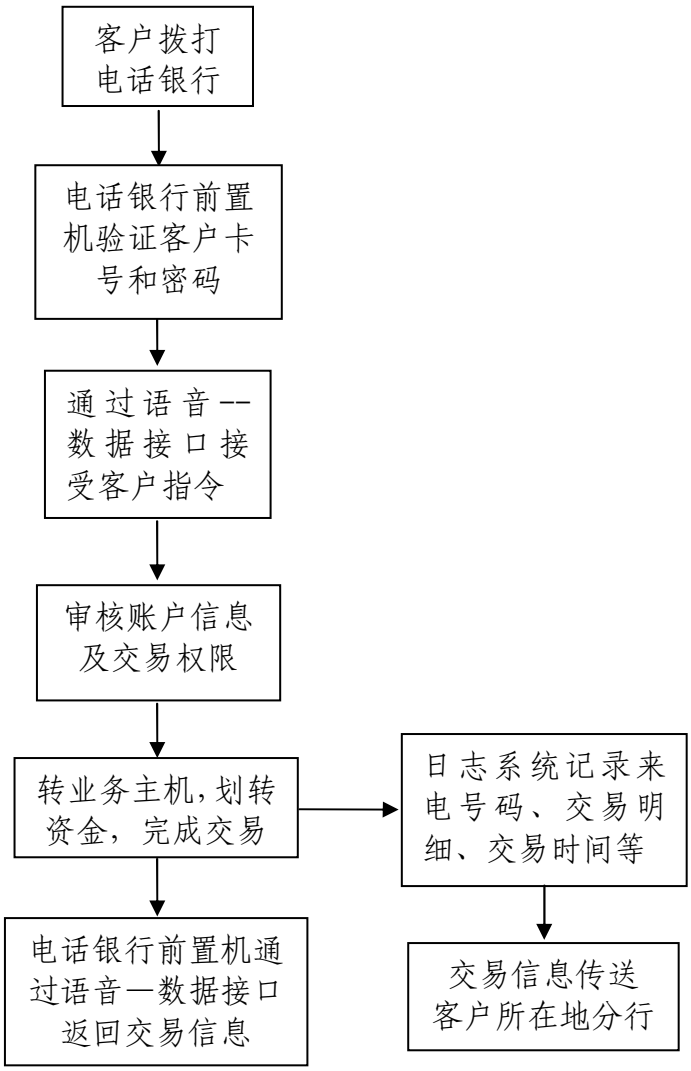
10、开办企业网上银行业务，应对企业的网上银行操作人员进行权限划分，明确操作员、授权员、管理员的不同职责，并保证一个操作员只能拥有经办、复核、授权中的一项，保证一笔业务必须经过至少二人的操作才能完成。

从大的方面来讲，网上银行的风险包括两个方面，一方面是银行内部网络的安全性及数据管理的严密性，另一方面是客户自身使用的电子设备的安全性。目前，各金融机构普遍重视网上银行的安全性，采取了多种措施以保障网络安全。相反，因为计算机病毒的泛滥，客户办理网上银行的终端电子设备成了目前网上银行的主要风险点。因此，客户使用网上银行开办业务，必须保证自身计算机的安全和可靠。

23.5 电话银行业务处理流程及内控关键点

电话银行是客户通过拨打银行提供的固定电话，接入银行内部生产网络，由客户自主进行业务操作。

由于电话系统的局限，电话银行无法象网上银行一样，使用数字证书来对客户进行身份验证，只是通过账户和密码审核客户交易权限。所以通过与客户签署协议保证交易不可抵赖性。同时，电话银行前置机日志系统详细记录客户的来电号码、交易明细、交易时间等内容。



电话银行业务流程图

电话银行的风险，主要包括以下几个方面：

1、电话银行的电子日志系统是否健全。因为电话银行没有数字证书等身份验证机制，只有通过客户账号和密码进行简单身份审核，所以安全性不如网上银行。这就要求银行应详细记录电话银行的各交易事项，如来电号码，来电时间，交易明细等。同时应将日志系统长期备份保存。

2、电话银行硬件设施是否可靠运行，前置机、服务器是否有备份机。电话银行系统接入银行内部网络是否安全可靠。

3、电话银行交易审核机制是否完善。是否经常检查电话银行系统的电子日志，是否查看有否可疑交易，是否设定密码尝试错误次数。

23.6 中间业务处理流程

目前金融机构开办的中间业务以代收费为主，代收电费、水费、煤气费、电话费、有线电视费、网络费、手机费等。

银行开办中间业务，需要和合作单位进行网络连接和数据交换，因此，对代收费业务的检查，主要侧重于这两方面。

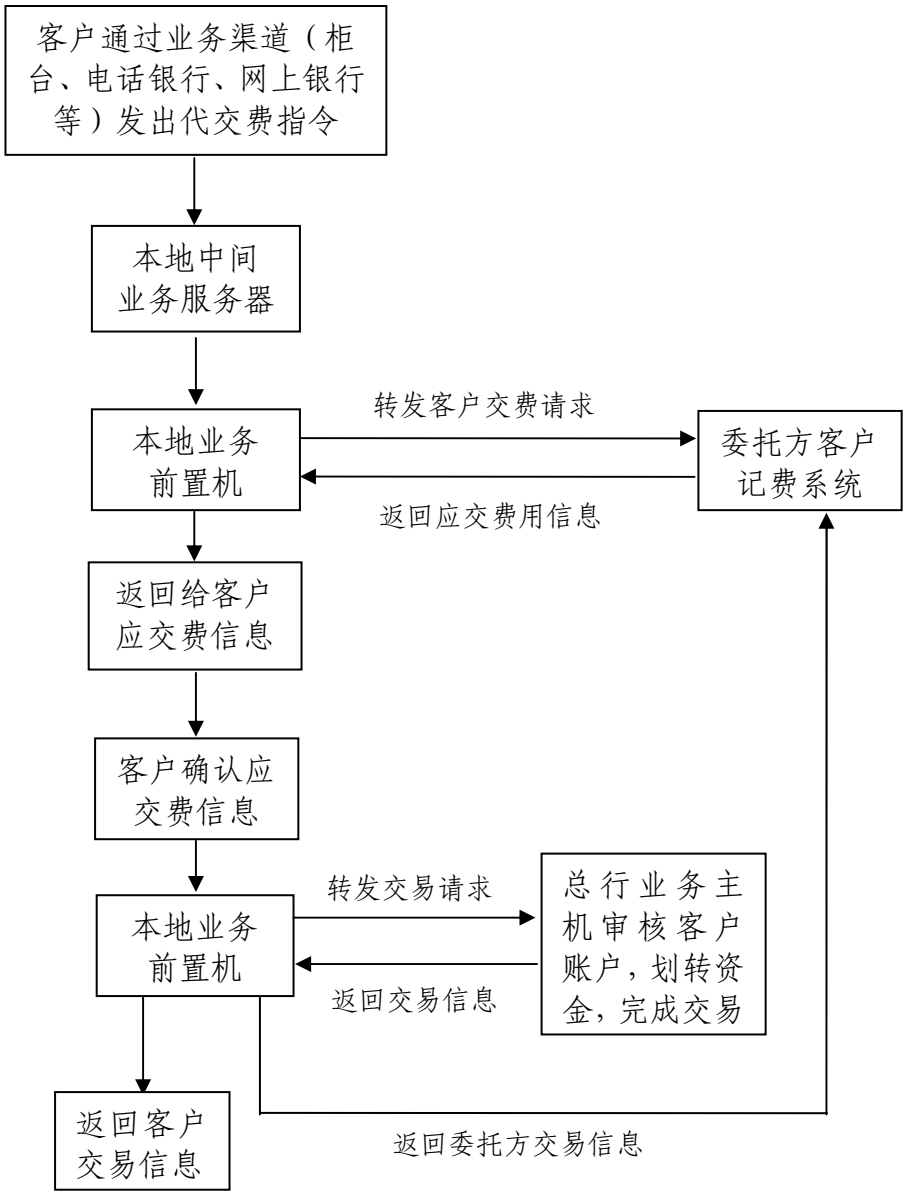
1、是否制订相关的规章制度，并与合作单位签订合同，以保证中间业务安全运行。

2、与合作单位联网，是否安装有防火墙、入侵检测等必需的安全防护措施，是否能够保证网络安全。

3、业务数据是否安全传输和转移，是否保证数据传输过程中的安全和保密。

4、数据转移和交换是否安全。金融机构开展代收费业务如果需要和其它金融机构或非金融机构进行数据交换或转移，应严格执行《电子银行业务管理办法》中的相关规定。

另外，银证转账、第三方存管、代办保险等业务，其流程和主要风险点和其它中间业务基本一样，这里不详细介绍了。

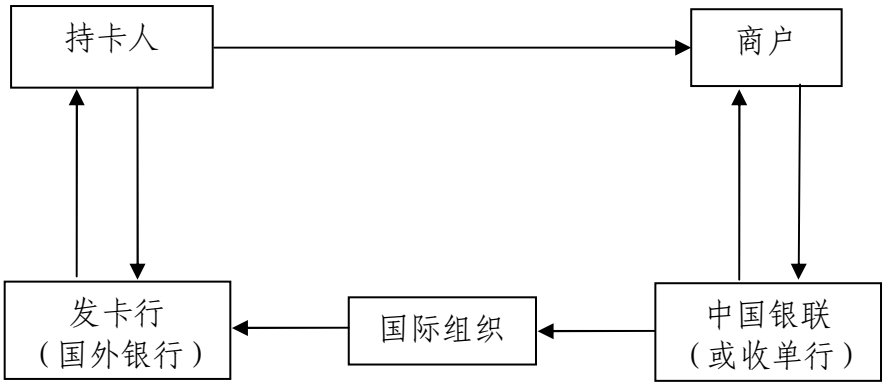

客户通过业务渠道（柜台、电话银行、网上银行等）发出代交费指令
本地中间业务服务器
本地业务前置机
转发客户交费请求
委托方客户记费系统
返回应交费用信息
返回给客户应交费信息
客户确认应交费信息
本地业务前置机
转发交易请求
总行业务主机审核客户账户，划转资金，完成交易
返回交易信息
返回客户交易信息
返回委托方交易信息

代收费业务流程

23.7 外卡业务处理流程

目前我国很多银行都开通了境外支付功能，携带我国发行的信用卡到国外消费或携带国外发行的信用卡到我国消费已经很普遍。外卡消费主要是通过国际结算组织来进行资金清算的。下面以境外信用卡在我国进行 POS 机消费为例加以介绍。

外卡收单业务主要涉及境外发卡行、持卡人、国内收单机构（银联或银行）、国内外卡特约商户和国际信用卡组织等机构和个人。国外信用卡持卡人在国内刷卡消费时，商户通过银联（或收单行）联线境外发卡行，提交交易申请。在获得批准交易的授权后，POS 机自动打印交易单据，并请持卡人签名确认。银联（或收单行）在收到商户 POS 机传送的电子交易数据信息后一定期限内，将扣除收单业务手续费后的交易金额划入商户帐户，同时银联（或收单行）通过国际结算组织从境外发卡行获得结算资金，境外发卡行再根据交易数据向持卡人发送对账单收款。商户打印的原始交易单据，由商户在一定期限内保存。



外卡交易流程

若持卡人在收到对账单后发现交易有问题，将通过其发卡行向国内银联（或发卡行）查询交易，银联（或收单行）将联系商户，要求其提供原始交易单据以回复查询。如果银联（或收单行）不能在信用卡国际结算组织规定期限内回复查询，发卡行有权向银联（或收单行）退单并扣回已付资金。

附件・检查使用格式文件

现场检查通知书

XXX 银行：

依据《中华人民共和国银行业监督管理法》，兹派出检查组对你单位进行现场检查。现将现场检查的有关事项通知如下：

一、检查内容：XXX

二、检查时间：XXXX 年 XX 月 XX 日至 XXXX 年 XX 月 XX 日（必要时可顺延）

三、请你单位按照现场检查前问卷要求，认真填写并提供相关材料。所提供的内容资料必须真实完整，并应承担相应的法律责任。

检查前问卷请于 XXXX 年 XX 月 XX 日前寄（送）我局 XXX 处。联系人：XXX；联系电话：XXXXXXXX。

请你单位积极配合现场检查，并提供必要的工作条件。

检查组组长：XXX

副　组　长：XXX

主　查　员：XXX

其 他成 员：XXXX

附件:现场检查前问卷

中国银行业监督管理委员会
XXX 监管局

现场检查前问卷

被查机构名称：XXX 银行

发出问卷机构名称：中国银监会 XXX 监管局

发出问卷时间：XXXX 年 XX 月 XX 日

填 报 说 明

1、报送数据的起止日期：

2、xxx 指 xxxxx：

3、xxx 范围是 xxxxxx

请你行在收到问卷 1 个工作日内将负责填写问卷的部门和人员报告问卷发出部门，便于沟通与联系。

发出问卷部门：XXX

发出问卷时间：XXXX 年 XX 月 XX 日

问卷上报时间：XXXX 年 XX 月 XX 日

联系人：XXX

联系电话：XXXXXXXX

传真：XXXXXXXX

问题一：

答：

相关材料：

主要责任部门：

问题二：

答：

相关材料：

主要责任部门：

我行承诺提供的内容资料真实完整，并愿意承担相应的法律责任。

负责人签字:

日期:

单位盖章:

中国银行业监督管理委员会 XXX 银监局
现场检查进点会谈记录

年　月　日　　编号：

被查单位（部门）		会谈地点	
被查单位（部门）参加人员			
检查组参加人员			
会谈内容			
被查单位（部门） 负责人签名：		检查组组长/主查员签名：	

国银行业监督管理委员会 XXX 监管局
现场检查资料调阅清单

被查单位：

序号	调阅资料名称	数量	资料日期	调阅日期	调阅人签名	归还日期	收回人签名

注:本表一式两份,一份检查组留存,一份被查单位留存。

中国银行业监督管理委员会 XXX 监管局
现场检查工作底稿

年　月　日　　编号：

被查单位（部门）		项目名称	
检查人		复核人	
检查内容：			
发现的问题：			
评价和意见：			

注：工作底稿主要记录现场检查中工作内容及情况、发现的问题和事实（包括认定的事项、认定事项过程中对有关凭证、报表等资料进行计算、分析、比较的内容及其结果、认定的依据），与问题或事实有关的附件材料应当附例于工作底稿之后。工作底稿应按检查内容分类注明索引

中国银行业监督管理委员会 XXX 监管局
现场检查事实确认书

年　月　日　　编号：

<table>
<tr><td colspan="6">被查单位（部门）：</td></tr>
<tr><td colspan="6">项目名称：</td></tr>
<tr><td colspan="6">检查事实：</td></tr>
<tr><td colspan="6">被查单位（部门）意见：

被查单位（部门）负责人签字：
年　月　日</td></tr>
<tr><td>检查人签字</td><td></td><td>复核人签字</td><td></td><td>主查员签字</td><td></td></tr>
</table>

注：被查单位对“现场检查事实描述”的确认必须有明确的意见。意见分为三种，一是“承认事实”，二是“否认事实及其理由”，三是“承认部分事实并补充相关材料”。

中国银行业监督管理委员会 XXX 监管局
现场检查总结会谈记录

检查机构名称：　　年　月　日　　编号：

<table>
<tr><td>被查单位
（部门）</td><td colspan="2"></td><td>会谈
地点</td><td></td></tr>
<tr><td>被查单位（部门）
参加人员</td><td colspan="4"></td></tr>
<tr><td>检查组
参加人员</td><td colspan="4"></td></tr>
<tr><td>会
谈
内
容</td><td colspan="4">主要记载内容：
一、被查机构负责人对《现场检查事实与评价》的意见
二、存在不同意见的问题
三、双方讨论的情况
四、达成一致、基本一致、存在重大分歧的内容记载
五、对《现场检查事实与评价》的签署情况（当场签署、反馈后签署、不同意签署）。</td></tr>
<tr><td>被查单位
（部门）</td><td colspan="2"></td><td>检查组组长
签名</td><td></td></tr>
<tr><td>负责人
签名：</td><td colspan="2"></td><td>主查员
签名</td><td></td></tr>
</table>

记录员签名：

中国银行业监督管理委员会 XXX 监管局
检查事实与评价

×××××分行(部/处室/支行/办事处/公司):

提示：本现场检查事实与评价系我局依法对你单位实施现场检查后形成的，并向你单位下发。除法律另有强制性规定外，未经我局同意，你单位及其工作人员均不得以任何方式向其他任何机构或个人披露本文件的任何内容。同时，我局及其工作人员依法对本文件内容保密。

根据中国银行业监督管理委员会××××厅/部/局关于《关于开展×××××专项（全面）检查的通知》（银监办通〔200×〕×××号）要求，我局检查组于××××年××月××日至××××年××月××日对你分行或××部/处室/支行/办事处/公司××××年××月××日至××××年××月××日的×××××××××进行了现场检查。现将检查情况反馈如下，请你分行对相关事实予以确认。你分行如对《检查事实与评价》材料无异议，请你分行负责人在《检查事实与评价》上签署无异议意见，签字并加盖公章；如有异议，请你分行于　　年　月　日前书面回复我局，逾期未反馈意见的，视为对《检查事实与评价》无异议。

一、总体评价

略

二、检查中发现的问题

（一）×××××××××问题

拟写要求：1、检查事实评价结论（根据检查事实与违规条款作出客观定性评价）

2、主要事实（时间、单位、事实过程等）

3、违规条款

（二）×××××××××问题

1、略

2、略

3、略

处室负责人签名：　　签字日期：

检查组组长签名：　　签字日期：

主查员签名：　　签字日期：