商业银行信息科技风险管理指引

第一章　总　　则

第一条　为加强商业银行信息科技风险管理，根据《中华人民共和国银行业监督管理法》、《中华人民共和国商业银行法》、《中华人民共和国外资银行管理条例》，以及国家信息安全相关要求和有关法律法规，制定本指引。

第二条　本指引适用于在中华人民共和国境内依法设立的法人商业银行。

政策性银行、农村合作银行、城市信用社、农村信用社、村镇银行、贷款公司、金融资产管理公司、信托公司、财务公司、金融租赁公司、汽车金融公司、货币经纪公司等其他银行业金融机构参照执行。

第三条　本指引所称信息科技是指计算机、通信、微电子和软件工程等现代信息技术，在商业银行业务交易处理、经营管理和内部控制等方面的应用，并包括进行信息科技治理，建立完整的管理组织架构，制订完善的管理制度和流程。

第四条 本指引所称信息科技风险，是指信息科技在商业银行运用过程中，由于自然因素、人为因素、技术漏洞和管理缺陷产生的操作、法律和声誉等风险。

第五条 信息科技风险管理的目标是通过建立有效的机制，实现对商业银行信息科技风险的识别、计量、监测和控制，促进商业银行安全、持续、稳健运行，推动业务创新，提高信息技术使用水平，增强核心竞争力和可持续发展能力。

第二章 信息科技治理

第六条 商业银行法定代表人是本机构信息科技风险管理的第一责任人，负责组织本指引的贯彻落实。

第七条 商业银行的董事会应履行以下信息科技管理职责：

（一） 遵守并贯彻执行国家有关信息科技管理的法律、法规和技术标准，落实中国银行业监督管理委员会（以下简称银监会）相关监管要求。

（二） 审查批准信息科技战略，确保其与银行的总体业务战略和重大策略相一致。评估信息科技及其风险管理工作的总体效果和效率。

（三） 掌握主要的信息科技风险，确定可接受的风险级别，确保相关风险能够被识别、计量、监测和控制。

（四） 规范职业道德行为和廉洁标准，增强内部文化建设，提高全体人员对信息科技风险管理重要性的认识。

（五） 设立一个由来自高级管理层、信息科技部门和主要业务部门的代表组成的专门信息科技管理委员会，负责监督各项职责的落实，定期向董事会和高级管理层汇报信息科技战略规划的执行、信息科技预算和实际支出、信息科技的整体状况。

（六） 在建立良好的公司治理的基础上进行信息科技治理，形成分工合理、职责明确、相互制衡、报告关系清晰的信息科技治理组织结构。加强信息科技专业队伍的建设，建立人才激励机制。

（七） 确保内部审计部门进行独立有效的信息科技风险管理审计，对审计报告进行确认并落实整改。

（八） 每年审阅并向银监会及其派出机构报送信息科技风险管理的年度报告。

（九） 确保信息科技风险管理工作所需资金。

（十） 确保银行所有员工充分理解和遵守经其批准的信息科技风险管理制度和流程，并安排相关培训。

（十一） 确保本法人机构涉及客户信息、账务信息以及产品信息等的核心系统在中国境内独立运行，并保持最高的管理权限，符合银监会监管和实施现场检查的要求，防范跨境风险。

（十二） 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或突发事件，按相关预案快速响应。

（十三） 配合银监会及其派出机构做好信息科技风险监督检查工作，并按照监管意见进行整改。

（十四） 履行信息科技风险管理其他相关工作。

第八条 商业银行应设立首席信息官，直接向行长汇报，并参与决策。首席信息官的职责包括：

（一） 直接参与本银行与信息科技运用有关的业务发展决策。

（二） 确保信息科技战略，尤其是信息系统开发战略，符合本银行的总体业务战略和信息科技风险管理策略。

（三） 负责建立一个切实有效的信息科技部门，承担本银行的信息科技职责。确保其履行：信息科技预算和支出、信息科技策略、标准和流程、信息科技内部控制、专业化研发、信息科技项目发起和管理、信息系统和信息科技基础设施的运行、维护和升级、信息安全管理、灾难恢复计划、信息科技外包和信息系统退出等职责。

（四） 确保信息科技风险管理的有效性，并使有关管理措施落实到相关的每一个内设机构和分支机构。

（五） 组织专业培训，提高人才队伍的专业技能。

（六） 履行信息科技风险管理其他相关工作。

第九条 商业银行应对信息科技部门内部管理职责进行明确的界定；各岗位的人员应具有相应的专业知识和技能，重要岗位应制定详细完整的工作手册并适时更新。对相关人员应采取下列风险防范措施：

（一） 验证个人信息，包括核验有效身份证件、学历证明、工作经历和专业资格证书等信息。

（二） 审核信息科技员工的道德品行，确保其具备相应的职业操守。

（三） 确保员工了解、遵守信息科技策略、指导原则、信息保密、授权使用信息系统、信息科技管理制度和流程等要求，并同员工签订相关协议。

（四） 评估关键岗位信息科技员工流失带来的风险，做好安排候补员工和岗位接替计划等防范措施；在员工岗位发生变化后及时变更相关信息。

第十条 商业银行应设立或指派一个特定部门负责信息科技风险管理工作，并直接向首席信息官或首席风险官（风险管理委员会）报告工作。该部门应为信息科技突发事件应急响应小组的成员之一，负责协调制定有关信息科技风险管理策略，尤其是在涉及信息安全、业务连续性计划和合规性风险等方面，为业务部门和信息科技部门提供建议及相关合规性信息，实施持续信息科技风险评估，跟踪整改意见的落实，监控信息安全威胁和不合规事件的发生。

第十一条 商业银行应在内部审计部门设立专门的信息科技风险审计岗位，负责信息科技审计制度和流程的实施，制订和执行信息科技审计计划，对信息科技整个生命周期和重大事件等进行审计。

第十二条 商业银行应按照知识产权相关法律法规，制定本机构信息科技知识产权保护策略和制度，并使所有员工充分理解并遵照执行。确保购买和使用合法的软硬件产品，禁止侵权盗版；采取有效措施保护本机构自主知识产权。

第十三条 商业银行应依据有关法律法规的要求，规范和及时披露信息科技风险状况。

第三章 信息科技风险管理

第十四条 商业银行应制定符合银行总体业务规划的信息科技战略、信息科技运行计划和信息科技风险评估计划，确保配置足够人力、财力资源，维持稳定、安全的信息科技环境。

第十五条 商业银行应制定全面的信息科技风险管理策略，包括但不限于下述领域：

（一） 信息分级与保护。

（二） 信息系统开发、测试和维护。

（三） 信息科技运行和维护。

（四） 访问控制。

（五） 物理安全。

（六） 人员安全。

（七） 业务连续性计划与应急处置。

第十六条 商业银行应制定持续的风险识别和评估流程，确定信息科技中存在隐患的区域，评价风险对其业务的潜在影响，对风险进行排序，并确定风险防范措施及所需资源的优先级别（包括外包供应商、产品供应商和服务商）。

第十七条 商业银行应依据信息科技风险管理策略和风险评估结果，实施全面的风险防范措施。防范措施应包括：

（一） 制定明确的信息科技风险管理制度、技术标准和操作规程等，定期进行更新和公示。

（二） 确定潜在风险区域，并对这些区域进行详细和独立的监控，实现风险最小化。建立适当的控制框架，以便于检查和平衡风险；定义每个业务级别的控制内容，包括：

1. 最高权限用户的审查。

2. 控制对数据和系统的物理和逻辑访问。

3. 访问授权以“必需知道”和“最小授权”为原则。

4. 审批和授权。

5. 验证和调节。

第十八条 商业银行应建立持续的信息科技风险计量和监测机制，其中应包括：

（一） 建立信息科技项目实施前及实施后的评价机制。

（二） 建立定期检查系统性能的程序和标准。

（三） 建立信息科技服务投诉和事故处理的报告机制。

（四） 建立内部审计、外部审计和监管发现问题的整改处理机制。

（五） 安排供应商和业务部门对服务水平协议的完成情况进行定期审查。

（六） 定期评估新技术发展可能造成的影响和已使用软件面临的新威胁。

（七） 定期进行运行环境下操作风险和管理控制的检查。

（八） 定期进行信息科技外包项目的风险状况评价。

第十九条 中资商业银行在境外设立的机构及境内的外资商业银行，应当遵守境内外监管机构关于信息科技风险管理的要求，并防范因监管差异所造成的风险。

第四章　信息安全

第二十条　商业银行信息科技部门负责建立和实施信息分类和保护体系，商业银行应使所有员工都了解信息安全的重要性，并组织提供必要的培训，让员工充分了解其职责范围内的信息保护流程。

第二十一条　商业银行信息科技部门应落实信息安全管理职能。该职能应包括建立信息安全计划和保持长效的管理机制，提高全体员工信息安全意识，就安全问题向其他部门提供建议，并定期向信息科技管理委员会提交本银行信息安全评估报告。信息安全管理机制应包括信息安全标准、策略、实施计划和持续维护计划。

信息安全策略应涉及以下领域：

（一） 安全制度管理。

（二） 信息安全组织管理。

（三） 资产管理。

（四） 人员安全管理。

（五） 物理与环境安全管理。

（六） 通信与运营管理。

（七） 访问控制管理。

（八） 系统开发与维护管理。

（九） 信息安全事故管理。

（十） 业务连续性管理。

（十一） 合规性管理。

第二十二条 商业银行应建立有效管理用户认证和访问控制的流程。用户对数据和系统的访问必须选择与信息访问级别相匹配的认证机制，并且确保其在信息系统内的活动只限于相关业务能合法开展所要求的最低限度。用户调动到新的工作岗位或离开商业银行时，应在系统中及时检查、更新或注销用户身份。

第二十三条 商业银行应确保设立物理安全保护区域，包括计算机中心或数据中心、存储机密信息或放置网络设备等重要信息科技设备的区域，明确相应的职责，采取必要的预防、检测和恢复控制措施。

第二十四条 商业银行应根据信息安全级别，将网络划分为不同的逻辑安全域（以下简称为域）。应该对下列安全因素进行评估，并根据安全级别定义和评估结果实施有效的安全控制，如对每个域和整个网络进行物理或逻辑分区、实现网络内容过滤、逻辑访问控制、传输加密、网络监控、记录活动日志等。

（一） 域内应用程序和用户组的重要程度。

（二） 各种通讯渠道进入域的访问点。

（三） 域内配置的网络设备和应用程序使用的网络协议和端口。

（四） 性能要求或标准。

（五） 域的性质，如生产域或测试域、内部域或外部域。

（六） 不同域之间的连通性。

（七） 域的可信程度。

第二十五条 商业银行应通过以下措施，确保所有计算机操作系统和系统软件的安全：

（一） 制定每种类型操作系统的基本安全要求，确保所有系统满足基本安全要求。

（二） 明确定义包括终端用户、系统开发人员、系统测试人员、计算机操作人员、系统管理员和用户管理员等不同用户组的访问权限。

（三） 制定最高权限系统账户的审批、验证和监控流程，并确保最高权限用户的操作日志被记录和监察。

（四） 要求技术人员定期检查可用的安全补丁，并报告补丁管理状态。

（五） 在系统日志中记录不成功的登录、重要系统文件的访问、对用户账户的修改等有关重要事项，手动或自动监控系统出现的任何异常事件，定期汇报监控情况。

第二十六条 商业银行应通过以下措施，确保所有信息系统的安全：

（一） 明确定义终端用户和信息科技技术人员在信息系统安全中的角色和职责。

（二） 针对信息系统的重要性和敏感程度，采取有效的身份验证方法。

（三） 加强职责划分，对关键或敏感岗位进行双重控制。

（四） 在关键的接合点进行输入验证或输出核对。

（五） 采取安全的方式处理保密信息的输入和输出，防止信息泄露或被盗取、篡改。

（六） 确保系统按预先定义的方式处理例外情况，当系统被迫终止时向用户提供必要信息。

（七） 以书面或电子格式保存审计痕迹。

（八） 要求用户管理员监控和审查未成功的登录和用户账户的修改。

第二十七条 商业银行应制定相关策略和流程，管理所有生产系统的活动日志，以支持有效的审核、安全取证分析和预防欺诈。日志可以在软件的不同层次、不同的计算机和网络设备上完成，日志划分为两大类：

（一） 交易日志。交易日志由应用软件和数据库管理系统产生，内容包括用户登录尝试、数据修改、错误信息等。交易日志应按照国家会计准则要求予以保存。

（二） 系统日志。系统日志由操作系统、数据库管理系统、防火墙、入侵检测系统和路由器等生成，内容包括管理登录尝试、系统事件、网络事件、错误信息等。系统日志保存期限按系统的风险等级确定，但不能少于一年。

商业银行应保证交易日志和系统日志中包含足够的内容，以便完成有效的内部控制、解决系统故障和满足审计需要；应采取适当措施保证所有日志同步计时，并确保其完整性。在例外情况发生后应及时复查系统日志。交易日志或系统日志的复查频率和保存周期应由信息科技部门和有关业务部门共同决定，并报信息科技管理委员会批准。

第二十八条 商业银行应采取加密技术，防范涉密信息在传输、处理、存储过程中出现泄露或被篡改的风险，并建立密码设备管理制度，以确保：

（一） 使用符合国家要求的加密技术和加密设备。

（二） 管理、使用密码设备的员工经过专业培训和严格审查。

（三） 加密强度满足信息机密性的要求。

（四） 制定并落实有效的管理流程，尤其是密钥和证书生命周期管理。

第二十九条 商业银行应配备切实有效的系统，确保所有终端用户设备的安全，并定期对所有设备进行安全检查，包括台式个人计算机（PC）、便携式计算机、柜员终端、自动柜员

机（ATM）、存折打印机、读卡器、销售终端（POS）和个人数字助理（PDA）等。

第三十条 商业银行应制定相关制度和流程，严格管理客户信息的采集、处理、存贮、传输、分发、备份、恢复、清理和销毁。

第三十一条 商业银行应对所有员工进行必要的培训，使其充分掌握信息科技风险管理制度和流程，了解违反规定的后果，并对违反安全规定的行为采取零容忍政策。

第五章 信息系统开发、测试和维护

第三十二条 商业银行应有能力对信息系统进行需求分析、规划、采购、开发、测试、部署、维护、升级和报废，制定制度和流程，管理信息科技项目的优先排序、立项、审批和控制。项目实施部门应定期向信息科技管理委员会提交重大信息科技项目的进度报告，由其进行审核，进度报告应当包括计划的重大变更、关键人员或供应商的变更以及主要费用支出情况。应在信息系统投产后一定时期内，组织对系统的后评价，并根据评价结果及时对系统功能进行调整和优化。

第三十三条 商业银行应认识到信息科技项目相关的风险，包括潜在的各种操作风险、财务损失风险和因无效项目规划或不适当的项目管理控制产生的机会成本，并采取适当的项目管理方法，控制信息科技项目相关的风险。

第三十四条 商业银行应采取适当的系统开发方法，控制信息系统的生命周期。典型的系统生命周期包括系统分析、设计、开发或外购、测试、试运行、部署、维护和退出。所采用的系统开发方法应符合信息科技项目的规模、性质和复杂度。

第三十五条 商业银行应制定相关控制信息系统变更的制度和流程，确保系统的可靠性、完整性和可维护性，其中应包括以下要求：

（一） 生产系统与开发系统、测试系统有效隔离。

（二） 生产系统与开发系统、测试系统的管理职能相分离。

（三） 除得到管理层批准执行紧急修复任务外，禁止应用程序开发和维护人员进入生产系统，且所有的紧急修复活动都应立即进行记录和审核。

（四） 将完成开发和测试环境的程序或系统配置变更应用到生产系统时，应得到信息科技部门和业务部门的联合批准，并对变更进行及时记录和定期复查。

第三十六条 商业银行应制定并落实相关制度、标准和流程，确保信息系统开发、测试、维护过程中数据的完整性、保密性和可用性。

第三十七条 商业银行应建立并完善有效的问题管理流程，以确保全面地追踪、分析和解决信息系统问题，并对问题进行记录、分类和索引；如需供应商提供支持服务或技术援助，应向相关人员提供所需的合同和相关信息，并将过程记录在案；对完成紧急恢复起至关重要作用的任务和指令集，应有清晰的描述和说明，并通知相关人员。

第三十八条 商业银行应制定相关制度和流程，控制系统升级过程。当设备达到预期使用寿命或性能不能满足业务需求，基础软件（操作系统、数据库管理系统、中间件）或应用软件必须升级时，应及时进行系统升级，并将该类升级活动纳入信息科技项目，接受相关的管理和控制，包括用户验收测试。

第六章 信息科技运行

第三十九条 商业银行在选择数据中心的地理位置时，应充分考虑环境威胁（如是否接近自然灾害多发区、危险或有害设施、繁忙或主要公路），采取物理控制措施，监控对信息处理设备运行构成威胁的环境状况，并防止因意外断电或供电干扰影响数据中心的正常运行。

第四十条 商业银行应严格控制第三方人员（如服务供应商）进入安全区域，如确需进入应得到适当的批准，其活动也应受到监控；针对长期或临时聘用的技术人员和承包商，尤其是从事敏感性技术相关工作的人员，应制定严格的审查程序，包括身份验证和背景调查。

第四十一条 商业银行应将信息科技运行与系统开发和维护分离，确保信息科技部门内部的岗位制约；对数据中心的岗位和职责做出明确规定。

第四十二条 商业银行应按照有关法律法规要求保存交易记录，采取必要的程序和技术，确保存档数据的完整性，满足安全保存和可恢复要求。

第四十三条 商业银行应制定详尽的信息科技运行操作说明。如在信息科技运行手册中说明计算机操作人员的任务、工作日程、执行步骤，以及生产与开发环境中数据、软件的现场

及非现场备份流程和要求（即备份的频率、范围和保留周期）。

第四十四条 商业银行应建立事故管理及处置机制，及时响应信息系统运行事故，逐级向相关的信息科技管理人员报告事故的发生，并进行记录、分析和跟踪，直到完成彻底的处置和根本原因分析。商业银行应建立服务台，为用户提供相关技术问题的在线支持，并将问题提交给相关信息科技部门进行调查和解决。

第四十五条 商业银行应建立服务水平管理相关的制度和流程，对信息科技运行服务水平进行考核。

第四十六条 商业银行应建立连续监控信息系统性能的相关程序，及时、完整地报告例外情况；该程序应提供预警功能，在例外情况对系统性能造成影响前对其进行识别和修正。

第四十七条 商业银行应制定容量规划，以适应由于外部环境变化产生的业务发展和交易量增长。容量规划应涵盖生产系统、备份系统及相关设备。

第四十八条 商业银行应及时进行维护和适当的系统升级，以确保与技术相关服务的连续可用性，并完整保存记录（包括疑似和实际的故障、预防性和补救性维护记录），以确保有效维护设备和设施。

第四十九条 商业银行应制定有效的变更管理流程，以确保生产环境的完整性和可靠性。包括紧急变更在内的所有变更都应记入日志，由信息科技部门和业务部门共同审核签字，并事先进行备份,以便必要时可以恢复原来的系统版本和数据文件。紧急变更成功后,应通过正常的验收测试和变更管理流程,采用恰当的修正以取代紧急变更。

第七章 业务连续性管理

第五十条 商业银行应根据自身业务的性质、规模和复杂程度制定适当的业务连续性规划，以确保在出现无法预见的中断时，系统仍能持续运行并提供服务；定期对规划进行更新和演练，以保证其有效性。

第五十一条 商业银行应评估因意外事件导致其业务运行中断的可能性及其影响，包括评估可能由下述原因导致的破坏：

（一） 内外部资源的故障或缺失（如人员、系统或其他资产）。

（二） 信息丢失或受损。

（三） 外部事件（如战争、地震或台风等）。

第五十二条 商业银行应采取系统恢复和双机热备处理等措施降低业务中断的可能性，并通过应急安排和保险等方式降低影响。

第五十三条 商业银行应建立维持其运营连续性策略的文档，并制定对策略的充分性和有效性进行检查和沟通的计划。其中包括：

（一）规范的业务连续性计划,明确降低短期、中期和长期中断所造成影响的措施，包括但不限于：

1．资源需求（如人员、系统和其他资产）以及获取资源的方式。

2．运行恢复的优先顺序。

3．与内部各部门及外部相关各方（尤其是监管机构、客户和媒体等）的沟通安排。

（二）更新实施业务连续性计划的流程及相关联系信息。

（三）验证受中断影响的信息完整性的步骤。

（四）当商业银行的业务或风险状况发生变化时，对本条（一）到（三）进行审核并升级。

第五十四条 商业银行的业务连续性计划和年度应急演练结果应由信息科技风险管理部门或信息科技管理委员会确认。

第八章 外 包

第五十五条 商业银行不得将其信息科技管理责任外包，应合理谨慎监督外包职能的履行。

第五十六条 商业银行实施重要外包（如数据中心和信息科技基础设施等)应格外谨慎，在准备实施重要外包时应以书面材料正式报告银监会或其派出机构。

第五十七条 商业银行在签署外包协议或对外包协议进行重大变更前，应做好相关准备，其中包括：

（一） 分析外包是否适合商业银行的组织结构和报告路线、业务战略、总体风险控制，是否满足商业银行履行对外包服务商的监督义务。

（二） 考虑外包协议是否允许商业银行监测和控制与外包相关的操作风险。

（三） 充分审查、评估外包服务商的财务稳定性和专业经验，对外包服务商进行风险评估，考查其设施和能力是否足以承担相应的责任。

（四） 考虑外包协议变更前后实施的平稳过渡（包括终止合同可能发生的情况）。

（五） 关注可能存在的集中风险，如多家商业银行共用同一外包服务商带来的潜在业务连续性风险。

第五十八条 商业银行在与外包服务商合同谈判过程中，应考虑的因素包括但不限于：

（一） 对外包服务商的报告要求和谈判必要条件。

（二） 银行业监管机构和内部审计、外部审计能执行足够的监督。

（三） 通过界定信息所有权、签署保密协议和采取技术防护措施保护客户信息和其他信息。

（四） 担保和损失赔偿是否充足。

（五） 外包服务商遵守商业银行有关信息科技风险制度和流程的意愿及相关措施。

（六） 外包服务商提供的业务连续性保障水平，以及提供相关专属资源的承诺。

（七） 第三方供应商出现问题时，保证软件持续可用的相关措施。

（八） 变更外包协议的流程，以及商业银行或外包服务商选择变更或终止外包协议的条件，例如：

1. 商业银行或外包服务商的所有权或控制权发生变化。

2. 商业银行或外包服务商的业务经营发生重大变化。

3. 外包服务商提供的服务不充分，造成商业银行不能履行监督义务。

第五十九条 商业银行在实施双方关系管理，以及起草服务水平协议时，应考虑的因素包括但不限于：

（一） 提出定性和定量的绩效指标，评估外包服务商为商业银行及其相关客户提供服务的充分性。

（二） 通过服务水平报告、定期自我评估、内部或外部独立审计进行绩效考核。

（三） 针对绩效不达标的情况调整流程，采取整改措施。

第六十条 商业银行应加强信息科技相关外包管理工作，确保商业银行的客户资料等敏感信息的安全，包括但不限于采取以下措施：

（一） 实现本银行客户资料与外包服务商其他客户资料的有效隔离。

（二） 按照“必需知道”和“最小授权”原则对外包服务商相关人员授权。

（三） 要求外包服务商保证其相关人员遵守保密规定。

（四） 应将涉及本银行客户资料的外包作为重要外包，并告知相关客户。

（五） 严格控制外包服务商再次对外转包，采取足够措施确保商业银行相关信息的安全。

（六） 确保在中止外包协议时收回或销毁外包服务商保存的所有客户资料。

第六十一条 商业银行应建立恰当的应急措施，应对外包服务商在服务中可能出现的重大缺失。尤其需要考虑外包服务商的重大资源损失，重大财务损失和重要人员的变动，以及外包协议的意外终止。

第六十二条 商业银行所有信息科技外包合同应由信息科技风险管理部门、法律部门和信息科技管理委员会审核通过。商业银行应设立流程定期审阅和修订服务水平协议。

第九章 内部审计

第六十三条 商业银行内部审计部门应根据业务的性质、规模和复杂程度，对相关系统及其控制的适当性和有效性进行监测。内部审计部门应配备足够的资源和具有专业能力的信息科技审计人员，独立于本银行的日常活动，具有适当的授权访问本银行的记录。

第六十四条 商业银行内部信息科技审计的责任包括：

（一） 制定、实施和调整审计计划，检查和评估商业银行信息科技系统和内控机制的充分性和有效性。

（二） 按照第（一）款规定完成审计工作，在此基础上提出整改意见。

（三） 检查整改意见是否得到落实。

（四） 执行信息科技专项审计。信息科技专项审计，是指对信息科技安全事故进行的调查、分析和评估，或审计部门根据风险评估结果对认为必要的特殊事项进行的审计。

第六十五条 商业银行应根据业务性质、规模和复杂程度，信息科技应用情况，以及信息科技风险评估结果，决定信息科技内部审计范围和频率。但至少应每三年进行一次全面审计。

第六十六条 商业银行在进行大规模系统开发时，应要求信息科技风险管理部门和内部审计部门参与，保证系统开发符合本银行信息科技风险管理标准。

第十章 外部审计

第六十七条 商业银行可以在符合法律、法规和监管要求的情况下，委托具备相应资质的外部审计机构进行信息科技外部审计。

第六十八条 在委托审计过程中，商业银行应确保外部审计机构能够对本银行的硬件、软件、文档和数据进行检查，以

发现信息科技存在的风险，国家法律、法规及监管部门规章、规范性文件规定的重要商业、技术保密信息除外。

第六十九条 商业银行在实施外部审计前应与外部审计机构进行充分沟通，详细确定审计范围，不应故意隐瞒事实或阻挠审计检查。

第七十条 银监会及其派出机构必要时可指定具备相应资质的外部审计机构对商业银行执行信息科技审计或相关检查。外部审计机构根据银监会或其派出机构的委托或授权对商业银行进行审计时，应出示委托授权书，并依照委托授权书上规定的范围进行审计。

第七十一条 外部审计机构根据授权出具的审计报告，经银监会及其派出机构审阅批准后具有与银监会及其派出机构出具的检查报告同等的效力，被审计的商业银行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。

第七十二条 商业银行在委托外部审计机构进行外部审计时，应与其签订保密协议，并督促其严格遵守法律法规，保守本银行的商业秘密和信息科技风险信息，防止其擅自对本银行提供的任何文件进行修改、复制或带离现场。

第十一章　附　　则

第七十三条　未设董事会的商业银行，应当由其经营决策机构履行本指引中董事会的有关信息科技风险管理职责。

第七十四条　银监会依法对商业银行的信息科技风险管理实施监督检查。

第七十五条　本指引由银监会负责解释、修订。

第七十六条　本指引自颁布之日起施行，《银行业金融机构信息系统风险管理指引》（银监发〔2006〕63号）同时废止。