银行业重要信息系统突发事件应急管理规范

（试行）

第一章　总　则

第一条 为规范银行业重要信息系统的突发事件应急管理，提高应对突发事件的综合管理水平和应急处置能力，有效防范银行业信息系统风险，根据《中华人民共和国银行业监督管理法》、《中华人民共和国突发事件应对法》以及相关法律法规，制定本规范。

第二条 在中华人民共和国境内设立的政策性银行、国有商业银行、股份制商业银行、邮政储蓄银行、城市商业银行、农村商业银行、农村合作银行、农村信用社、城市信用社，外商独资银行、中外合资银行和外国银行分行适用本规范。

第三条 银行业重要信息系统突发事件应对工作原则包括：

（一）健全机制。银行业金融机构应建立统一指挥、协调有序的应急管理机制，主动开展应急管理工作，定期演练和评价应急预案，持续改进本机构的应急预案和相关协调机制。

（二）明确职责。银行业金融机构应明确本机构各部门在应急管理工作中的职责，以保障银行业金融机构业务连续性为目标，以落实和完善应急预案为基础，全面加强信息系统应急管理

工作，并制定有效的问责制度。

（三）预防为主。银行业金融机构应建立和完善信息系统突发事件风险防范体系，对可能导致突发事件的风险进行有效地识别、分析和控制，并对风险指标动态、持续监测，减少重大突发事件发生的可能性。

（四）处置高效。银行业金融机构应加强应急处置队伍建设，提供充分的资源保障，确保突发事件发生时反应快速、报告及时、措施得力、操作准确，降低突发事件可能造成的损失。

第四条 以下术语适用于本规范：

（一）本规范所称重要信息系统是指银行业金融机构支撑关键业务，其信息安全和系统服务安全关系公民、法人和组织的权益或社会秩序和公共利益，甚至影响国家安全的信息系统。主要包括面向客户、涉及账务处理且时效性要求较高的业务处理类、渠道类和涉及客户风险管理等业务的管理类信息系统，支撑上述系统运行的前置机、客户端、机房、网络等基础设施也应作为重要信息系统的一部分。

（二）本规范所称业务服务时段是指银行业金融机构重要信息系统所承载业务对客户提供服务的时间。

（三）本规范所称突发事件是指银行业金融机构重要信息系统以及为之提供支持服务的电力、通讯等系统突然发生的，影响业务持续开展，需要采取应急处置措施应对的事件。

（四）本规范所称信息系统应急管理是指贯穿于整个信息系

统生命周期中，通过风险防范、应急响应、应急保障以确保信息系统能够满足业务发展战略对业务连续性要求的管理。

（五）本规范所称业务影响分析是指分析业务功能及其相关信息系统资源、评估特定信息系统突发事件对各种业务功能的影响的过程。

（六）本规范所称剩余风险是指采取了风险控制措施后仍不能被完全消除的信息系统风险。

第二章 组织机构及职责

第五条中国银行业监督管理委员会（以下简称“银监会”）信息科技监管部门是银行业信息系统应急处理日常管理机构，其应急管理职责是：

（一）监管、指导银行业金融机构信息系统应急管理工作；

（二）组织协调行业资源，指导银行业金融机构完成信息系统突发事件的应急处置；

（三）向上级部门报告银行业金融机构信息系统突发事件；

（四）通报、发布银行业信息系统应急处理情况；

（五）向银行业金融机构发布信息系统突发事件预警信息；

（六）督导、检查银行业金融机构信息系统应急演练；

（七）维护银行业应急管理组织机构通讯联络方式；

（八）维护完善本应急管理规范。

第六条 银监会派出机构结合本地实际情况设立相应的应急

管理组织机构，明确职责并监督、检查辖区内银行业金融机构做好应急预案，负责辖区内银行业信息系统突发事件应急管理工作。

第七条 银行业金融机构应综合考虑其业务和系统规模，建立应急管理组织机构，负责本机构信息系统突发事件应急管理工作。

（一）董事会和高级管理层应对本机构应急管理政策及其实施效果负有最终的责任。董事会和高级管理层应领导、监督本机构信息系统应急管理体系建设，制定落实应急管理的分级授权制度和问责制度，研究确定应急处置重大决策和指导意见，为应急管理工作配置充分的资源，定期听取风险状况分析、信息系统重大突发事件、现有应急管理政策重大修改等汇报，负责信息系统突发事件信息披露等。

（二）风险管理部门应制订应急管理政策和基本管理制度并报董事会和高级管理层审定，统一组织、协调、指导、检查本机构信息系统突发事件应急管理工作，建立应急处置的预授权制度，定期分析风险状况和总结信息系统突发事件应急管理工作，履行向董事会和高级管理层的报告职责，履行向银监会及其派出机构信息系统应急管理部门的报告职责等。

（三）信息科技管理部门和业务管理部门负责本机构信息系统突发事件应急管理工作的具体落实，制定信息系统突发事件预防措施、预警标准和应急策略，组织做好信息系统营运监测和维

护及实施信息系统突发事件应急处置，评估总结信息系统突发事件及应急处置过程中暴露的问题并整改，履行向风险管理部门的报告职责，定期组织信息系统应急演练，持续改进本机构信息系统应急预案等。各银行业金融机构的业务管理部门应针对信息系统突发事件建立相应的业务应急预案和操作流程，并进行持续改进和优化。

第八条 银行业金融机构应组建应急团队，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，实施专项应急处置工作。应急团队应包括但不限于应急领导小组、应急执行小组、支持保障小组。

（一）应急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，高级管理层人员任应急领导小组组长，各相关职能部门（包括但不限于风险管理部门、业务管理部门、信息科技管理部门和支持保障部门等）和一级分支机构的负责人为应急领导小组成员，其职责是：

1．负责信息系统突发事件的应急指挥、组织协调和过程控制；

2．明确新闻发布人，授权其在应急过程中统一对外信息发布口径；

3．宣布重大应急响应状态的降级或解除；

4．向董事会和高级管理层报告应急处置进展情况和总结报告。

（二）应急执行小组由业务管理部门、信息科技管理部门、运营部门等派员组成，对应急领导小组负责，其职责是：

1．实施信息系统突发事件的具体应急处置工作；

2．对信息系统突发事件业务影响情况进行分析和评估；

3．收集分析信息系统突发事件应急处置过程中的数据信息和日志；

4.向应急领导小组报告应急处置进展情况和事态发展情况。

（三）支持保障小组由人力资源部门、计划财务部门、法律事务部门、公共关系部门、安全保卫部门、后勤保障部门等派员组成，对应急领导小组负责，其职责是：

1．提供应急所需人力和物力等资源保障；

2．做好对受影响客户的解释和安抚工作；

3．做好秩序维护、安全保障、法律咨询和支援等工作；

4．建立与电力、通讯、公安和消防等相关外部机构的应急协调机制和应急联动机制；

5.其他为降低事件负面影响或损失提供的应急支持保障等。

第三章 突发事件分级

第九条 突发事件依照其影响范围及持续时间等因素分级。当突发事件同时满足多个级别的定级条件时，按最高级别确定突发事件等级。

（一）特别重大突发事件（I级）

1、银行业金融机构由于重要信息系统服务中断或重要数据损毁、丢失、泄露，造成经济秩序混乱或重大经济损失、影响金融稳定的，或对公众利益造成特别严重损害的突发事件；

2、由于重要信息系统服务异常，在业务服务时段导致银行业金融机构两个（含）以上省（自治区、直辖市）业务无法正常开展达 3 个小时（含）以上，或一个省（自治区、直辖市）业务无法正常开展达 6 个小时（含）以上的突发事件；

3、业务服务时段以外，重要信息系统出现的故障或事件救治未果，可能产生（1）至（2）影响的突发事件。

（二）重大突发事件（II级）

1、银行业金融机构由于重要信息系统服务中断或重要数据损毁、丢失、泄露，对银行或客户利益造成严重损害的突发事件；

2、由于重要信息系统服务异常，在业务服务时段导致银行业金融机构两个（含）以上省（自治区、直辖市）业务无法正常开展达半个小时（含）以上，或一个省（自治区、直辖市）业务无法正常开展达 3 个小时（含）以上的突发事件；

3、业务服务时段以外，出现的重要信息系统故障或事件救治未果，可能产生（1）至（2）影响的突发事件。

（三）较大突发事件（III级）

1、银行业金融机构由于重要信息系统服务中断或重要数据损毁、丢失、泄露，对银行或客户利益造成较大损害的突发事件；

2、由于重要信息系统服务异常，在业务服务时段导致一个

省（自治区、直辖市）业务无法正常开展达半个小时（含）以上的突发事件；

3、业务服务时段以外，出现的重要信息系统故障或事件救治未果，可能产生（1）至（2）影响的突发事件。

第十条 重要信息系统突发事件发生后，银行业金融机构应依据影响范围和事件影响时间的变化，按照上述定义进行事件级别升级。

第四章 风险防范

第十一条 银行业金融机构应根据业务影响分析确定各项业务的信息系统恢复指标，主要包括：

（一）恢复时间目标（RTO）：业务功能恢复正常的时间要求；

（二）恢复点目标（RPO）：业务功能恢复时能够容忍的数据丢失量。

第十二条 银行业金融机构应根据信息系统恢复指标和系统间的依赖关系，确定各信息系统应急响应恢复优先顺序，并系统化地识别信息技术资源风险，包括基础设施类风险、主机和硬件设备类风险、系统类风险、应用类风险、网络类风险等以确保风险识别的全面性。

第十三条 银行业金融机构应制定全面的风险防范措施，并通过场景模拟、压力测试等手段验证风险防范措施的有效性。在

突发事件应急处置后，应评估已有风险防范措施的有效性并加以改进。

第十四条 银行业金融机构应依据风险防范措施对关键信息技术资源进行剩余风险评估，明确剩余风险的监测方法与预警条件，并将其纳入信息系统风险事件监测与预警体系中。

第十五条 银行业金融机构应对关键信息技术资源建立监测指标体系以及相关的日常监测与预警机制，对监测指标的异常波动及时预警，并定期测试与修订监测指标体系以确保其有效性。

第十六条 银行业金融机构应建立关键时点监测与预警机制，在重大业务活动、重大社会活动、信息系统重大变更等关键时点加强风险监控和预警，并及时向业务职能部门进行风险提示，多部门协同做好应急准备。

第十七条 银行业金融机构在系统上线、系统升级、网络改造、设备更新等关键信息技术资源发生重大变更及业务种类和交易量发生重大变化时，应重新识别、分析、控制风险，并更新剩余风险评估和风险事件监测与预警。

第十八条 银行业金融机构应与电力、通信等重要基础设施服务商，主机、网络、存储等重要设备服务商，系统集成服务商以及其他外包服务商签定服务水平协议，并对服务商的技术与产品政策、服务水平、服务能力发生变化所可能产生的影响及时进行风险评估和预警。

第五章 应急预案与演练

第十九条 银行业金融机构应根据恢复时间目标（RTO）和恢复点目标（RPO），结合风险控制策略，从基础设施、网络、信息系统等不同方面，分类制定本机构应急预案。

第二十条 银行业金融机构编制的信息系统应急预案应包括以下内容：

（一）明确有关各方的分工和责任；

（二）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；

（三）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、操作系统故障、系统漏洞、应用系统故障以及其他各类与信息系统相关的故障；

（四）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；

（五）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；

（六）明确应急相关人员的协调内容和沟通方式；

（七）明确系统重建步骤，确保信息系统恢复正常业务处理能力。

第二十一条 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其中，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（RTO）和恢复点目标（RPO）的要求。

第二十二条 银行业金融机构应定期对应急预案进行测试和演练，确保其有效性。

第二十三条 当信息系统发生系统上线、系统升级、网络改造、设备更新、配置参数调整等变更时应及时更新应急预案，并适时实施演练。

第二十四条 银行业金融机构应制定年度信息系统应急演练计划，明确演练的时间、内容、依据、目的、负责人和相关配合机构等要素。演练计划应涵盖对应急预案各环节的检验，验证应急预案的有效性、应急资源的完备性及应急人员的适应性。应急演练应做到全面演练和专项演练相结合，一般情况下，银行业金融机构每年至少应组织一次全机构范围内的应急演练。

第二十五条 银行业金融机构应严格按照应急演练计划实施应急演练，并注意如下事项：

（一）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；

（二）应急演练内容应全面完整，涵盖信息系统的各类应急

场景；

（三）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；

（四）应急演练应选择在非主要业务时段进行；

（五）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；

（六）定期对信息系统应急响应相关人员进行培训。

第二十六条 银行业金融机构应积极配合其他机构完成跨机构或跨行业应急演练。

第二十七条 银行业金融机构在应急演练的过程中，对可能存在较大风险的演练（如全机构范围的演练），应在实施演练前将应急演练计划向银监会及其派出机构报备。

第二十八条 应急演练结束后，银行业金融机构应组织编写应急演练情况总结报告，大型或重要的应急演练总结报告应提交董事会和高级管理层。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。

第二十九条 银行业金融机构应根据演练总结报告提出的改进措施进行整改，并及时修订相应的应急预案，银行业金融机构应组织审计部门对整改情况进行监督和检查。

第三十条 对于全机构范围的年度演练或跨机构和跨行业的演练，银行业金融机构应将演练总结报告上报银监会及其派出机

构。

第三十一条 银行业金融机构在应急演练的过程中，应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。

第六章 应急响应

第三十二条 银行业金融机构应按照本机构既定的应急预案，做好应急处置，快速有效处置突发事件。

第三十三条 银行业金融机构风险管理部门应在董事会和高级管理层授权下负责突发事件报告，并指定专人为报告责任人。当报告责任人确定或发生变更时应及时向银监会及其派出机构信息系统应急管理部门报备。

当多个重要信息系统同时受到影响时，按照受影响程度最高原则报告。

第三十四条全国性银行业金融机构总部向银监会信息系统应急管理部门报告；全国性银行业金融机构的一级分支机构、地方性银行业金融机构向当地银监会派出机构信息系统应急管理部门报告。

第三十五条 突发事件应急响应流程：

（一）应急执行小组应根据既定的应急预案，启动应急操作，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；

（二）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；

（三）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；

（四）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；

（五）银行业金融机构应在重要信息系统突发事件发生后60 分钟之内将突发事件相关情况上报银监会及其派出机构信息系统应急管理部门，并在事件发生后 12 小时内提交正式书面报告；

（六）对造成经济秩序混乱或重大经济损失、影响金融稳定的，或对银行、客户、公众的利益造成损害的突发事件，银行业金融机构要立即上报；

（七）银行业金融机构应将应急处置重大进展情况及时上报银监会及其派出机构，直至应急结束。I 级突发事件发生后，银行业金融机构应每 2 小时将应急处置进展情况上报，直至应急结束。

第三十六条 上报银监会及其派出机构的书面报告内容应包括突发事件时间、地点、现象、影响的业务范围、原因分析、后果的初步判断、已采取的措施、后续拟采取方案的建议、事件报告单位、联系人及联系方式、其他与本突发事件有关的内容，并

在报告中重点明确需要银监会协调的事项。

第三十七条 银监会及其派出机构信息系统应急管理部门根据银行业金融机构应急协调需求，组织协调国家信息化管理、信息安全管理、治安管理、电力管理等跨部门资源，统筹安排处置工作。

第三十八条 应急处置中所有相关的信息和处理过程应进行严格记录，外部供应商的处理过程应有专门记录文件，如果涉及到保险理赔，中间过程和场景可用摄像设备进行记录。所有过程资料应由专人存档保管。

第三十九条 应急处置过程中出现异常或应急预案、决策方案失效，银行业金融机构应急领导小组要立即上报银监会及其派出机构信息系统应急管理部门。

第四十条 重要信息系统突发事件发生后，银行业金融机构应将相关信息及时通报给受影响的外部机构及重要客户，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，以获得应急响应支持。

第四十一条 重要信息系统突发事件发生后，根据突发事件的严重程度，银行业金融机构应急领导小组应及时向新闻媒体发布相关信息，严格按照行业、机构的相关规定和要求对外发布信息，机构内其它部门或者个人不得随意接受新闻媒体采访或对外发表个人看法。

第四十二条 重要信息系统恢复正常服务即为应急结束。

第四十三条 银行业金融机构在应急结束后，应针对应急工作进行评估和总结，并报银监会及其派出机构信息系统应急管理部门。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。

（一）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；

（二）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；

（三）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，并提出改进措施、计划及相关建议。

第七章 应急保障

第四十四条 银行业金融机构应建立长效的人员保障机制，确保人员能够胜任应急处置工作。在人员保障方面应达到以下要求：

（一）确保应急处置人员具备应急工作必要的技术资质，并定期组织人员培训以满足应急处置的要求，并通过应急演练，保证应急处置人员的熟练度；

（二）确保主、备岗机制的落实；

（三）确保主、备岗人员定期进行互换；

（四）避免一人兼过多的岗位。

第四十五条 银行业金融机构应建立有效的物质保障机制，

确保在应急响应过程中不会因物质缺乏而导致应急处置中断或延长应急处置时间。在物质保障方面应达到以下要求：

（一）应储备一定数量应急设备或物资，并确保物资供应渠道畅通；

（二）应建立应急响应专项资金预算管理与审批制度，确保应急响应过程中及时进行应急物资采购。

第四十六条 银行业金融机构应建立有效的技术保障机制，确保在应急响应过程中不会因技术能力缺乏而导致应急处置中断或延长应急处置时间。在技术保障方面应达到以下要求：

（一）建立应急事件预警平台，确保及时发现应急事件，并及时通知有关人员启动应急响应；

（二）明确相关厂商的技术支持服务水平，确保应急处置过程中相关厂商能够提供及时有效的技术支持。

第四十七条 银行业金融机构应采取必要的通讯保障措施，确保应急响应通讯及时有效。在通讯保障方面应达到以下要求：

（一）实时更新各级应急管理机构联络人和联络方式；

（二）建立多种通讯渠道，避免单点通讯风险，并明确各通讯渠道使用的优先顺序。

第八章 持续改进

第四十八条 银行业金融机构应每年开展一次对突发事件风险防范措施的全面评估和审计活动，包括评估风险识别、分析和

控制措施的有效性、应急预案的完备性、应急演练的全面性和及时性等，检验防范措施的有效性，并及时发现新的风险，改进风险控制措施，进一步完善应急预案，形成风险防范措施的持续改进。

第四十九条 银行业金融机构应每年开展一次对应急响应工作的全面评估和审计活动。评估范围包括应急响应的有效性、投入资源的充分性、突发事件报告的及时性等，确保应急响应持续有效。

第五十条 银行业金融机构应对应急管理的策略、机制、方法、流程等不断完善，对应急管理过程中发现的问题适时整改。

第五十一条 银行业金融机构应将应急管理纳入到机构全面风险管理体系中，建立应急管理的长效机制，保证应急管理工作的持续性和有效性。

第九章 附则

第五十二条 本规范由银监会负责解释和修订。银行业金融机构可依据本规范制定具体的信息系统应急管理实施细则。

第五十三条在中华人民共和国境内设立的金融资产管理公司、信托投资公司、企业集团财务公司、金融租赁公司、汽车金融公司及银监会批准设立的其他金融机构，参照本规范执行。

第五十四条本规范自公布之日起执行。