

防患未然：金融机构业务连续性管理怎么做？

摘要

2020年初的新冠肺炎疫情，不仅对正常的经济生活进行了冲击，各类企业也开始思考针对重大自然灾害、疫情等突发事件的应对预案。作为经济的“血脉”，金融机构提前制定业务连续性计划，确保各类情况下业务能连续进行的重要性不言而喻。本文以境外监管机构对金融机构业务连续性管理要求为基础，解构金融机构业务连续性管理的具体内容、必要性和运用案例。

确保金融体系在重大突发事件之下仍能保持韧性是金融机构和金融监管机构共同的利益所在，这主要是由于以下原因：一是金融体系对经济活动的重要支撑作用。二是绝大多数金融体系里清算和结算服务的集中性。三是境内外金融机构的关联性日益紧密。四是各类非传统安全风险和突发事件的概率有所提升。五是金融体系稳定运转对保持公众信心的作用。随着金融体系的复杂性进一步上升，相应的操作风险也有所提升，因此保证金融体系具有一定韧性，确保业务连续性的难度也进一步增大。

2011年911事件之后，美国监管部门认为金融机构业务连续性的目标有以下几点：一是当面对大范围业务中断（Wide Scale Disruption）时，关键业务职能（Critical Operations）能够快速恢复并及时重新运作。二是当面对一个或以上重要运营地点无法进入或损失该运营地点的职员后，关键业务职能（Critical Operations）能够快速恢复并及时重新开始。三是通过持续和有效的测试，来确保金融机构内外部业务连续性安排是高置信度有效和合适的。

按照美国联邦金融机构检查委员会（Federal Financial Institutions Examination Council, FFIEC）2019年11月发布的《业务连续性管理手册》，金融机构业务连续性管理应主要包括以下内容：业务连续性管理框架，董事会、管理层责任及审计要求，业务冲击分析和风险评估，确定业务连续性策略，建立业务连续性计划，培训、演练与测试等部分，并形成动态的管理闭环，实时根据金融机构的业务特性进行更新和改进。

关键词：业务连续性管理，金融机构

宏观研究-金融监管研究

陈昊

兴业研究金融监管分析师

电话：021-22852646

邮箱：880220@cib.com.cn

鲁政委

兴业银行首席经济学家

华福证券首席经济学家



扫描下载兴业研究 APP

获取更多研究成果

目录

一、金融机构制定业务连续性计划的必要性.....	3
（一）金融机构业务连续的意义	3
（二）金融机构业务连续的目标	4
二、金融机构应该如何制定业务连续性计划.....	5
（一）业务连续性管理框架	5
（二）董事会、管理层责任以及审计要求	7
（三）业务冲击分析和风险评估	8
（四）确定业务连续性策略	11
（五）建立业务连续性计划	13
（六）培训、演练与测试	16
三、业务连续性计划具体运用案例.....	17
（一）2003 年美国和加拿大金融机构应对大停电事故	17
（二）2003 年 SARS 疫情对中国香港证券市场的影响	18

2020 年 1 月底以来,新型冠状病毒肺炎疫情对我国的日常生产生活造成了较大影响。不仅全国春节假期统一延长,部分地区还进一步延长了不得复工的日期。然而,正所谓“经济是肌体,金融是血脉”¹,“肌体”或许可以短暂休息、暂停运动,“血脉”的流动和运转却一刻也不能中断。因此,金融机构和金融基础设施自 2 月 3 日以后便开始恢复运转。本次疫情,不仅对正常的经济生活进行了冲击,各类企业也开始思考针对重大自然灾害、疫情等突发事件的应对预案。作为经济的“血脉”,金融体系面对各类突发事件不能终止关键金融服务,因而提前制定业务连续性计划,确保各类情况下金融机构业务能够连续进行成为了金融机构的“必修课”。本文将以前美国监管机构对金融机构业务连续性管理要求为基础,解构金融机构业务连续性管理的具体内容、必要性和运用案例。

一、金融机构制定业务连续性计划的必要性

(一) 金融机构业务连续的意义

根据国际清算银行(BIS)等监管组织的定义,对于金融机构而言,业务连续性(Business Continuity)指的是业务连续的、不中断的持续运营状态。按照美国联邦金融机构检查委员会(FFIEC)的定义,业务连续性管理(Business Continuity Management)指的是金融机构为保护员工、客户的利益以及产品服务不会中断而进行韧性、连续性、危机响应等相关举措的管理流程。

2006 年 8 月,巴塞尔银行监管委员会(Basel Committee on Banking Supervision)及国际证监会组织(IOSCO)等国际监管组织组成的联合论坛(Joint Forum)发表了《业务连续性的高级别原则》(High-Level Principles for Business Continuity,以下简称“《原则》”),首次在国际层面统一对金融机构业务连续性提出了要求。《原则》详细解释了金融机构和金融体系确保业务连续性的重要意义,指出业务连续性是金融行业参与者和金融监管机构一直以来的最高任务(Ongoing Priority)。《原则》认为,确保金融体系在重大突发事件之下仍能保持韧性是金融机构和金融监管机构共同的利益所在,这主要是有以下几个因素所导致的:

一是金融体系对经济活动的重要支撑作用。在当前的全球经济模式下,金融中介所提供的服务对于便利和促进经济稳定运行起到了重要的作用,包括支付结算服务、存贷款服务、有效的转账服务和募集资金等投融资服务。

¹ 2019 年 2 月 22 日,习近平主持中共中央政治局第十三次集体学习新闻稿,
http://www.gov.cn/xinwen/2019-02/23/content_5367953.htm

二是绝大多数金融体系里清算和结算服务的集中性。如若在突发事件中金融体系的清算和结算服务发生了中断，将可能导致金融体系的重要参与者无法完成资金转移、难以偿付其应偿资金，从而对金融体系产生重大的负面影响。

三是境内外金融机构的关联性日益紧密。随着资金和证券交易速度的加快，金融机构之间的相互关联性(Interdependencies)也进一步增强。关联性的增强，使得结算风险、信用风险、流动性风险在金融体系之中扩散的风险加大。因此，即使是单一金融机构业务中断，也有可能导致其他金融机构产生相应风险。更为严重的是，随着金融市场的全球化，单一司法辖区(Jurisdiction)的业务中断可能会导致全球金融市场的传染性影响。

四是各类非传统安全风险和突发事件的概率有所提升。随着恐怖袭击等非传统安全因素风险的上升，金融体系基础设施被作为袭击目标的可能性也在上升。与此同时，随着气候变化等因素的影响，各类突发事件频率的提升对于金融体系保持业务连续性也提出了挑战。

五是金融体系稳定运转对保持公众信心的作用。如果金融体系经常发生故障或长时间的中断，那么金融消费者对于金融体系乃至更广泛体系的信心也会下降。这将有可能导致境内外的金融市场参与者从该金融体系中撤出投资资金。

值得注意的是，随着金融体系的复杂性进一步上升，相应的操作风险也有所提升，因此保证金融体系具有一定韧性以确保业务连续性的难度也进一步增大。例如，随着科技的发展，金融体系对于电脑、自动化、信息系统的依赖程度越来越高，进而对于这些信息系统的第三方提供者物理基础设施(如电力、电信网络)的依赖也愈发严重。与此同时，随着普惠金融惠及面的进一步拓展相比于以往，金融体系关键金融服务业务连续性也面临着比以往更为严重的挑战。

(二) 金融机构业务连续的目标

随着时代的变迁，金融机构所要应对的可能造成业务中断的风险因素时刻在发生着变化。例如，恐怖袭击等非传统安全风险，使得此前单纯应对自然灾害等突发事件的业务连续性计划无法充分应对。由此，**金融机构业务连续性的目标也发生了相应的变化。**2001年911事件发生之后，美国金融监管机构与金融机构就金融机构业务连续性的管理进行了讨论，形成了《加强美国金融体系韧性的有效实践》(Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System, 以下简称“《有效实践》”)。《有效实践》

指出，根据 911 事件后金融市场参与者与金融监管机构的讨论，共同认为**金融市场业务连续性有三个最为重要的目标**：

一是当面对大范围业务中断（Wide Scale Disruption）时，关键业务职能（Critical Operations）能够快速恢复并及时重新开始。

二是当面对一个或更多重要运营地点无法进入或损失该运营地点的职员后，关键业务职能（Critical Operations）能够快速恢复并及时重新开始。

三是通过持续和有效的测试，来确保金融机构内外部业务连续性安排是高置信度有效和合适的。

联合论坛（2006）认为，**关键业务职能或服务（Critical Operation or Services）**指的是：如若某职能或服务的中断，会对其他金融行业参与者、金融监管机构或金融体系相关方业务持续运作（continued operation）产生实质性（material）影响，那么该职能或服务则应被认定为关键业务职能或服务。在不同机构和金融市场环境之下，关键业务职能或服务的范畴也可能有所差异。一般而言，数据中心（Data Center）是绝大多数金融机构中的关键业务职能。除此之外，关键服务往往还包括了大额支付、交易清算和结算以及交易对账等服务。

二、金融机构应该如何制定业务连续性计划

为了更好地了解发达国家监管机构是如何要求金融机构制定业务连续性计划，我们考察了美国联邦金融机构检查委员会（Federal Financial Institutions Examination Council, FFIEC）²最新发布的《业务连续性管理手册》（Business Continuity Management, 以下简称“《手册》”）³。虽然，FFIEC 发布《手册》的主要目的只是为金融监管部门检查各机构业务连续性管理时的重点进行指导，但是通过《手册》的检查重点，可以从侧面了解监管部门对金融机构业务连续性管理的关注点和期望所在。

（一）业务连续性管理框架

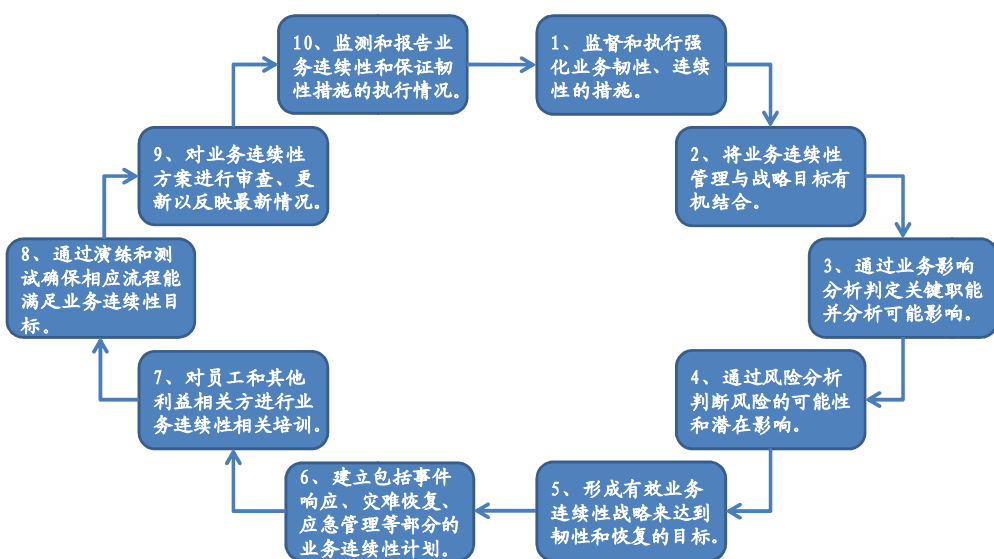
《手册》指出，金融机构的业务连续性管理流程应形成从设定目标、风险分析、构建业务连续性计划、培训与测试直至检测与更新的有机闭环。《手册》将业务连续性的管理分为了 10 个步骤，具体为：一是管理层对于金融机构整

² FFIEC 自 1979 年 3 月 10 日成立，其成员包括美联储理事会、金融消费者保护局（CFPB）、联邦存款保险公司（FDIC）、国家信用合作社管理局（NCUA）、货币监理署（OCC）以及地方监管机构。旨在为金融机构检查监管设定统一的标准。

³ 此前，FFIEC 从 20 世纪末即开始公布《手册》对金融机构业务连续性的监管要点进行明确，此后几乎每隔 5 年左右即会根据最新的情况更新《手册》内容，以便监管机构根据金融市场的发展调整监管重点。

体业务韧性、业务连续性和应急响应能力的监督和执行。**二是**将业务连续性管理的各个要素与机构战略目标等进行有机结合，使得业务连续性管理的目标、措施符合金融机构的特性和目标。**三是**通过业务影响分析（Business Impact Analysis）来确定关键业务职能（Critical Functions），分析与其他机构和企业的关联性，并评估影响。**四是**通过风险评估来识别确定风险、评估不同风险造成的业务中断的可能性和潜在影响。**五是**构建有效的业务连续性策略（Business Continuity Strategy）来确保业务韧性和恢复目标的实现。**六是在**前期分析和研判的基础上，基于业务连续性策略形成完备的业务连续性计划（Business Continuity Plan），其中包括事件响应（Incident Response）、灾害恢复（Disaster Recovery）以及危机管理（Crisis/Emergency Management）等组成部分。**七是**针对员工和其他利益相关方进行业务连续性的培训。**八是**通过演练和测试确保业务连续性相关流程能够有效支持此前建立的目标。**九是**对业务连续性策略、计划等进行整体的审查和更新，以此来反映最新的业务和市场情况。**十是**监测并同时向管理层汇报业务连续性管理的整体情况。

图表 1 业务连续性管理的总体框架流程



资料来源：FFIEC、兴业研究

通过上述的闭环动态过程，金融机构才能保证能持续确保其业务连续性管理有效且符合机构和金融市场的最新特征。根据金融机构的复杂程度和整体的规模，金融机构可以针对可能产生业务中断的不同风险制定单一或多项的具体业务连续性计划方案。

（二）董事会、管理层责任以及审计要求

在业务连续性管理框架中，董事会、管理层对其具有管理职责，内部或外部的审计组织也应该充分对业务连续性管理的有效性进行审核。

董事会和管理层对于机构整体对业务连续性管理具有监督和审查等职责，其重视程度和应对策略判断会对机构业务连续性管理的执行起到决定性作用。

《手册》指出，管理层需要从宏观角度评估业务连续性的潜在风险，并设定长期和短期的连续性目标，采取相关策略和计划来实现相应的业务连续性目标、增强业务的韧性，最后按照培训、测试和监测的反馈来更新业务连续性目标、计划等一系列内容。除此之外，管理层需要在设计批准新产品、新服务时充分考虑运营是否能保证相关业务连续性。

根据《手册》要求，**董事会（Board）的监督职责包括：一是布置业务连续性管理的总体责任和义务；二是针对业务连续性管理分配资源；三是将业务连续性管理总体要求与机构的业务策略和风险偏好结合统一；四是了解业务连续性潜在风险、可能采取的应对措施和政策；五是通过管理层的汇报、日常测试结果和审计结果来审查业务连续性管理执行情况；六是有效的对管理层的业务连续性管理进行质询等独立监督判断。**

管理层（Management）的监督管理职责包括：一是确定业务连续性管理各部门的角色、职责，以及相关方案；二是配置针对业务连续性管理的专职或兼职专业人员，并给予其充分的财务资源；三是确保相关人员了解其在业务连续性管理中的角色和责任；四是针对业务连续性的表现设立可以测度的目标，例如准备完成度、韧性目标等；五是设计和执行业务连续性执行战略；六是确保业务连续性管理中的演练、测试、培训等缓解足够全面，并与业务连续性管理策略相一致；七是解决在演练、测试、培训过程中暴露出来的超过公司风险承受能力的缺陷；八是设置业务连续性委员会（或协调人），并定期与其进行会议，讨论业务连续性管理相关策略、计划、演练、测试、培训等环节的修改；九是持续评估和更新业务连续性策略和计划，以期与公司最新的业务发展和市场环境相结合；十是与业务连续性管理的外部相关方（例如监管机构、第三方服务提供商等）定期进行协调。

《手册》要求，金融机构的董事会和管理层需要要求内部审计人员或聘请外部审计对业务连续性计划设计和执行的有效性进行审查。相关审计人员或单位应独立于此前的业务连续性管理框架。审计的频率和范围取决于机构的复杂程度、风险偏好和业务经营变化情况，比如大型、复杂的金融机构需要对于不同部门的业务连续性管理进行多个审计。《手册》指出，审计人员应在审计业务连续性管理时做好以下几方面内容：**一是评估业务冲击分析（Business Impact Analysis）和风险评估（Risk Assessment）的合理性、关键业务功能识别的准确**

性、不同事件的可能性以及对业务潜在冲击的严重程度；二是评估机构是否具有可靠、充足和有效率的管控来保证业务连续且具有韧性；三是将机构实际具有的风险水平和风险缓释措施与机构设定的风险偏好进行对比；四是检查测试计划是否取得了所希望的目标；五是监测业务连续性管理的测试，确保相关目标已经得到实现；六是评估业务连续性计划执行的有效性。

（三）业务冲击分析和风险评估

金融机构业务连续性管理的实际执行中，业务冲击分析（Business Impact Analysis）和风险评估（Risk Assessment）是业务连续性管理的基石。业务冲击分析（Business Impact Analysis）指的是对可能造成业务中断事件的识别，并对其潜在冲击的强度进行分析，包括关键业务职能的识别（Identification of Critical Business Functions）、相互依赖性分析（Interdependency Analysis）和中断的影响（Impact of Disruption）。风险评估（Risk Assessment）指的是识别金融机构业务操作、机构资产、员工和其他组织风险的过程，包括了风险的识别（Risk Identification）、可能性和影响分析（Likelihood and Impact）。

《手册》指出，管理层应当运用业务冲击分析和风险评估来有效识别和监测金融机构业务连续性的潜在风险。一旦管理层确认某个因素成为金融机构业务连续性的潜在风险，其可以选择四种应对方式：接受风险（Risk Acceptance）、风险缓释（Risk Mitigation）、风险转移（Risk Transference）或预防风险（Risk Avoidance）。在这其中，管理层的业务连续性管理应主要针对拟采取风险缓释和预防风险进行应对的领域。除此之外，风险转移的措施包括购买保险等，但是这并不意味着金融机构应该放松相关方面的风险管控。

业务冲击分析（Business Impact Analysis）可以大体分为三大部分：首先是关键业务职能（Critical Business Functions）的识别。关键业务职能可以通过多种方式来识别，包括业务流程（Work Flow）、访谈（Interview）、

预览已结束，完整报告链接和二维码如下：

https://www.yunbaogao.cn/report/index/report?reportId=1_6786

