# 监管快讯

监管洞察

2020年8月

## 有关运营韧性和运营风险的拟定原则

*巴塞尔委员会的拟定建议旨在强化银行抵御重大运营故障或大范围运营干扰事件的能力。*

### 要点

- 新型冠状病毒肺炎疫情（简称“新冠疫情”）加剧了运营风险（特别是银行对科技与第三方服务供应商的依赖），并增加了经济与业务的不确定性。
- 针对运营韧性，巴塞尔委员会提出7项拟定原则，旨在帮助银行强化其对于疫情、网络安全事件、技术故障或自然灾难等运营风险事件的抵御、适应和恢复能力。
- 巴塞尔委员会同时发布了运营风险原则的拟定更新（简称“PMSOR”），其中包括有关变革管理的更新以及信息与通信技术的新原则。

巴塞尔银行监管委员会（简称“巴塞尔委员会”）发布了两份咨询文件，就拟定的《运营韧性原则》（*Principles for Operational Resilience*）及《运营风险的稳健管理原则》的更新（*Principles for the Sound Management of Operational Risk*，简称PMSOR）公开征求意见。巴塞尔委员会认为运营韧性建立在有效管理运营风险的基础之上，因此一并起草了这两份文件。此外，这两份文件均借鉴参考了现行指引和当前实践（包括有关企业治理、业务连续性以及外包的原则性指引），目的是建立一个“连贯的框架”。征求意见的截止日期为2020年11月6日。

### 运营韧性原则

巴塞尔委员会把运营韧性界定为“干扰关键运营的能力”。新冠疫情的影响已表明，尽管资本和流动性要求提高了银行抵御金融冲击的能力，但为了加强银行抵御可能造成运营故障或大范围干扰金融市场的运营风险事件的能力（抵御能力指应对、适应运营风险事件并从中恢复和汲取经验的能力），仍有大量工作待完成。此类事件包括疫情、网络安全事件、技术故障或自然灾难。巴塞尔委员会拟定了加强银行运营韧性的基于原则的方法，涵盖以下7个领域，并着重指出了每项原则的关键特征。

*1.治理*

- 董事会负责核准银行的运营风险预期，考虑银行的风险偏好、风险承受能力以及风险状况。

在制定银行对干扰关键运营事件的风险承受水平时，董事会应充分考虑各种“严重但可能发生”的场景。

*2. 运营风险管理*

- 运营风险管理职能应与相关职能（根据定义，相关职能包括三道防线在内的职能，由业务部门管理层、独立的运营风险管理职能及独立的鉴证部门组成）合作协调业务连续性规划工作、第三方依赖性管理、灾难恢复与应对管理以及与其他风险管理框架相关的事项（视情形而定）。
- 控制及程序应足以及时识别内外部的威胁以及员工、流程、系统中存在的薄弱环节。

*3. 业务连续性规划及测试*

- 银行应制定实施业务连续性计划，并根据各种“严重但可能发生”并可能干扰关键运营的场景进行定期演练。
- 业务连续性计划应包括影响分析、恢复策略、测试方案、培训及沟通计划。
- 业务连续性计划应提供灾难恢复框架的实施指引，为管理和应对权限中断和更替界定角色和职责。
- 业务连续性计划应载明决策流程，界定触发银行实施计划的因素。

*4. 绘制互连和相互依赖关系*

- 相关职能应记录内外部的相互关联和相互依赖关系，包括员工、技术、流程、信息以及参与实现关键运营的部门。
- 相关方法和颗粒度应足以识别薄弱环节，并支撑测试结果维持在风险承受水平内。

*5.第三方依赖性管理*

- 在与第三方签订协议前，银行应核实第三方机构是否拥有与银行同等的运营韧性条件，以保障银行的关键运营。
- 协议应采用书面形式，内容包括如何在正常情况下以及在发生干扰事件的情况下保持运营韧性。
- 业务连续性计划应考虑第三方退出策略，并评估第三方在发生故障或服务中断的情况下的适当性及其他可行的替代方案。

*6. 事件管理*

- 银行应制定事件响应和恢复计划以应对干扰运营的事件，并定期检视、测试和更新这一计划（包括根据直接和间接汲取的经验教训进行更新）。
- 事件管理计划的范围应覆盖事件的整个周期，包括基于预设的标准实施严重性分类；界定触发业务连续性、灾难恢复和危机管理程序的阈值；实施沟通计划向内外部进行汇报，总结相关经验教训。

*7. 弹性信息与通信技术（包括网络安全）*

- 银行应明文制定信息与通信技术政策（包括网络安全政策），规定治理和监督工作、风险管理责任与问责、信息安全、定期测试和监测以及事件响应、业务连续性和灾难恢复计划。
- 银行亦应确认其对关键信息资产和基础设施的依赖，根据关键信息资产对关键运营（包括保护数据完整性和保密性）的重要性，安排网络安全工作的优先顺序。
- 制定大规模远程访问方案，快速部署实体资产，或大幅提升带宽以支持远程用户连接及客户数据保护，有助于处理以下问题：
  - 风险缓解策略
  - 界定有关管理远程资产、用户和应用程序开发的流程

– 定期更新，维护安全防御机制

## 运营风险的稳健管理原则

根据2014年对60家银行机构的检视，巴塞尔委员会认为银行在部分领域需要额外的指引以实施相关原则。巴塞尔委员会此次拟订的PMSOR更新即旨在应对这些领域，包括：1) 运营风险识别及评估；2) 变革管理； 3) 运营风险偏好和承受能力；及 4) 披露。当时，巴塞尔委员会还认为有必要制定一项特定的信息与通信技术风险管理原则。

目前拟定的更新包括：

— 使PMSOR与《巴塞尔协议III》运营风险框架保持一致
— 更新与变革管理相关的指引
— 包含有关信息与通信技术风险管理的新指引
— 有助于提升文件的清晰度。

*根据初稿，关于信息与通信技术的第10条新原则（“信息与通信技术”）内容如下：*

> *银行应根据其风险偏好和风险承受能力实施稳健的信息与通信技术治理，并确保信息与通信技术充分支持、促进银行的业务运营。银行应针对信息与通信技术实施适当的风险识别保护监测、响应和恢复计划，定期对此类计划进行测试，在其中纳入态势感知培训，并及时向用户传达相关信息。*

## 巴塞尔银行监管委员会

巴塞尔委员会是银行审慎监管的国际准则制定机构，为银行业的监管提供合作平台，使命是加强全球银行的监管和监督，改善银行业的实践，提升金融稳定性。

巴塞尔委员会有45个成员，包括来自28个司法管辖区的中央银行和银行监督机构。巴塞尔委员会不拥有任何超越国家的权限，其决策亦不具有法律效力。更确切而言，巴塞尔委员会的成员承诺共同为巴塞尔委员会准则和稳健实务的制定贡献力量，并在各自的司法管辖区实施并采用此等准则。

**Amy Matsuo**
**主管和美国负责人**
监管洞察
**电话：**919-664-7302
**电邮：**amatsuo@kpmg.com

作者：
**Amy Matsuo，**主管和监管洞察业务美国负责人

**Karen Staines，**监管洞察业务总监

kpmg.com/cn/socialmedia

如需获取毕马威中国各办公室信息，请扫描二维码或登陆我们的网站：
https://home.kpmg.com/cn/en/home/about/offices.html