




重新定义 运营韧性

新形势刊物系列

2021年6月

kpmg.com/cn

“慧博资讯”专业的投资研究大数据分享平台

点击进入  <http://www.hibor.com.cn>

新系列刊物

欧洲、中东与非洲(EMA)金融服务监管洞察中心(RIC)欣然推出全新领先思维系列《**金融服务业：新形势下的监管**》的第七份刊物。

随着政府和商界将注意力焦点逐步从应对新型冠状病毒肺炎(COVID-19) 疫情转到恢复能力及新形势下的复苏, 预计金融服务监管机构也将进入调整和支持的新阶段。

本刊将探讨有关运营韧性的监管视角将如何发展?监管环境如何因COVID-19 而产生变化以及目前金融服务机构可执行哪些工作以增强它们在复苏期及以后的运营韧性?我们还分析了新兴监管方案的异同点, 以及它们对未来的运营韧性监管议程而言意味着什么。

请关注本系列的最后一份刊物, 聚焦针对零售行为问题而不断变化的监管方式。



Financial services: regulating the new reality
(“金融服务业：新形势下的监管”)



Remote governance and controls
(“远程治理和控制”)



Delivering sustainable finance
(“实现可持续金融”)



Ensuring stable capital markets
(“确保资本市场稳定”)



Financial resilience in banking: a balancing act
(“银行业财务韧性：权衡之道”)



Accelerating digital finance
(“加速数字金融”)



目录

引言	04
01. 向更全面的案发展	06
02. 关注第三方风险	10
03. 向更高级的数字化韧性迈进	14
04. 主题上的变化	17
05. 展望未来, 吸取教训	19

引言

运营韧性在过去数十年一直是监管焦点，但2008年金融危机发生后，其已让步于关于财务韧性的新规则及框架的开发。但在过去数年，运营韧性已上升到监管议程的首要位置，而当前的COVID-19更使其获得更大关注。

监管机构十分清楚，金融机构乃至其客户在困难时期面对的业务中断风险显著加剧。技术引导的业务转型、引人关注的业务中断事件以及对金融体系的相互关联性的承认使机构运营及运作方式受到更多关注。

随着新形势的到来，金融监管机构认为银行与保险机构的运营韧性与财务韧性同等重要，运营韧性也是财务韧性的主要驱动因素；并且，恢复能力不足不但可能影响金融机构个体及更广泛的金融稳定性，还会导致重大客户损害。对信托业务而言，运营韧性不足或对投资者回报及客户资产安全带来不利影响。

如今，监管机构的看法已发生切实改变。它们正以全新的方式看待金融机构的恢复能力：考虑的不仅是“如果”，还包括“何时”。它们希望金融机构不仅思考业务中断发生时需面对的情况，还应准备相关的应对方案。虽然金融机构已一直被要求管理好自身的运营风险、为意外事件做好准备并制定业务延续及灾难恢复计划，但在新形势下，运营韧性涵盖更广。

一直以来，全球监管机构对恢复能力的关注重点是网络及ICT¹安全。

这些方面目前仍是关键领域，尤其是在COVID-19疫情的压力下，技术加快应用以及外部不良因素愈加复杂。金融机构必须考虑多个并发中断事件的可能性以及新威胁及缺陷点的出现。

气候变化带来的极端事件，包括洪水、山火到非预期的暴风雪，均会对实体运营带来冲击。地缘政治事件或对运营模型带来影响。譬如，因某些辖区的运营许可的丧失。因创新或经济状况改变而不断变化的业务模式或会导致人才短缺。

监管机构已意识到采用一个范围更广—包含员工、流程、科技及信息等同等重要的组成部分—的运营韧性方案的必要性。客户影响受到长期关注，治理和问责也是焦点所在。

拟定法规强调了识别严重但具一定合理性的个性化情境以及执行压力测试以揭露运营模式弱点的重要性。

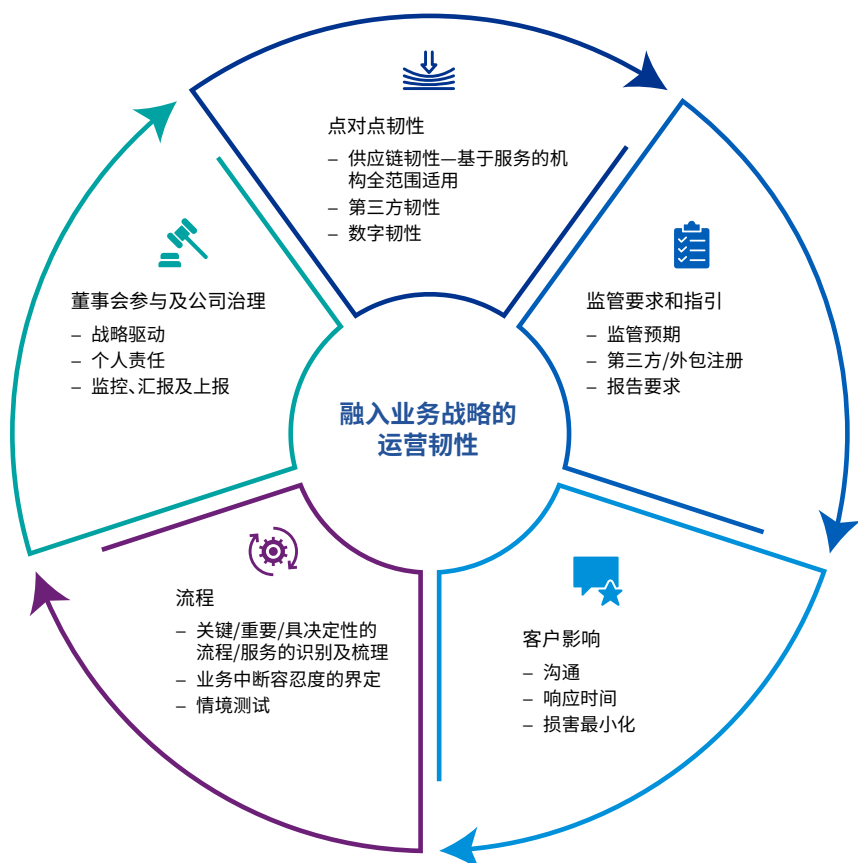
“金融实体以及作为一个整体的金融体系的运营韧性...与它们的财务韧性同等重要。”

Fabio Panetta,
欧洲央行执行理事会成员

金融机构务必界定它们愿意承受的业务中断次数，并监控并评估自身是否超出此等容忍度。

1. Information and Communications Technology (信息与通信技术)

运营韧性 - 监管重点之一



运营韧性成为**投资和业务战略的主要驱动力**。金融机构必须清晰了解自身的点对点流程,包括重要的相互依存关系以及业务中断将如何影响这些关系。运营韧性的提升可增强监管机构、客户、员工及第三方等利益相关者之间的信任。

互联性是关键。二十一世纪的金融服务业具备比以往更高的相互关联性和科技驱动性。外包已受业界关注一段时间,但目前其规模是前所未有的,因金融机构寻求通过加大对第三方的依赖,降低停运成本和提升效率。监管机构意识到少数大型的国际性技术及基础设施供应商的统治地位,并寻求相应地更新并扩大要求。

随着越来越多非金融机构为金融机构提供必要服务,**监管边界正不断扩张**。目前,运营韧性意味着贯穿整条供应链的点对点韧性,这将带来不少

新挑战。第三方的韧性以及与其相关的风险已受到监管机构的密切关注。随着科技及数字化的持续发展,数字运营韧性的含义正变得更加广泛。

有关新冠疫情如何促进科技的快速应用及其对金融服务监管带来的影响,请见新形势系列刊物“**Accelerating digital finance**”(“加速数字金融”)。

机构应回答的问题

- 运营韧性如何支持我们的业务增长议程及客户战略?其如何提升业绩增长?
- 我们是否视运营韧性为业务重点和业务战略的重要组成部分?
- 董事会层面是否有效参与?机构内部职责是否划分明确?
- 我们是否从自身机构、对客户的潜在影响以及对更广泛的金融体系的潜在影响角度识别并记录我们的关键/重要/具决定性的业务服务?
- 我们是否具备点对点的服务透明度,包括第三方关系?
- 我们能否保证第三方关系的有效管理以及正在执行的合同支持弹性响应?我们正进行何种工作以提升此方面的确定性?当合同不符合要求时,我们可以/将会采取什么措施?
- 我们是否具备合理的资源以应对能力及技能风险?是否需要更多及/或专业资源?
- 我们是否建立与客户及其它关键利益相关方之间的稳健沟通战略?



01. 向更全面的方案发展

运营韧性的监管虽已发展数十年,但不同地理区域及市场板块的监管模式依然呈现碎片化。不同辖区的发展速度不同,但所有辖区均认为运营韧性是优先考虑事项。网络韧性框架已有效整合,但需持续监控和更新以应对复杂程度不断提升的威胁(见第3章)。随着运营韧性的定义变得更加广泛和复杂,监管机构正推出不同的方案,从现行运营风险要求的高层次原则到新运营韧性框架的提出。

英国监管机构在2019年12月推出面向银行、保险机构、大型资产管理人和金融市场基础设施的一揽子咨询文件²,被广泛视为在此方面起领头作用。相关咨询是基于2018年7月讨论稿提出的概念。巴塞尔银行监管委员会(BCBS)也旨在通过其运营韧性原则(于2021年3月修订)实施全面的方案。这两种方案将完全兼容,但BCBS原则提供的是一个通用框架,英国的则是更为具体的表述。

适用于银行的全球原则

BCBS的运营韧性原则³是基于现行运营风险原则以及有关公司治理、外包及业务延续性的指引。BCBS还更新了运营风险健全管理原则⁴,在银行实施方面提供更多指引。

这些原则的主要目标是银行应致力于通过维持“在业务中断中交付关键运营”的能力来实现运营韧性。在这些原则的指引下,银行应能识别威胁及潜在失效并保护自身免受损害,并应对及适应业务中断事件,以及从中恢复和吸取教训。

T关键运营的定义与金融稳定委员会(FSB)制定的“韧性及解决方案”中

使用的定义一致(见第4章)。当评估运营韧性时,银行应审视其整体的风险偏好、风险敞口和风险状况。银行应通过协调现有管理架构并使其与主要目标匹配以实现运营韧性。

运营韧性被视为是运营风险有效管理的结果。

BCBS希望银行可以通过现行风险架构纳入这些原则,同时计及整体风险偏好、风险敞口和风险状况。BCBS不建议银行针对韧性建立独立的架构。

BCBS原则不仅对银行业有用,亦适用于其它更广泛行业,并可能构成一项全球行动方案。证券委员会国际组织(IOSCO)仅关注网络及外包(见第2、3章)。国际保险监管官协会(IAIS)并未专门关注运营韧性,

² <https://www.fca.org.uk/news/press-releases/building-operational-resilience-impact-tolerances-important-business-services>

³ <https://www.bis.org/bcbs/publ/d516.pdf>

⁴ <https://www.bis.org/bcbs/publ/d515.pdf>

BCBS: 银行运营韧性的高层次原则



1. 治理 – 银行应利用现有治理架构建立、监督及实施一个有效的运营韧性方案,使它们能应对并适应业务中断事件并从中恢复及吸取教训,以减少业务中断对关键运营交付的影响。



2. 运营风险管理 – 银行应利用各自的运营风险管理职能,持续识别有关人员、流程和系统的外部及内部威胁及潜在失效,及时评估关键运营的弱点并按运营韧性方案管理由此而来的风险。



3. 业务延续性计划及测试 – 银行应制定业务延续性计划,并在各种极端但可能发生的情景下执行业务延续性演练以测试它们在业务中断事件中交付关键运营的能力。



4. 梳理相互关联性及依存关系 – 银行识别关键运营后,应梳理其按运营韧性方案交付关键运营所必需的外部与内部相互关联性及依存关系。



5. 第三方依赖性管理 – 为交付关键运营,银行应管理它们对相互关系的依赖性,包括但不限于第三方或集团内部实体的关系。



6. 事件管理 – 银行应根据自身的风险偏好及中断事件容忍度,制定并实施应对及恢复计划,以管理可能会中断关键运营交付的事件。银行应整合以往事件的经验,持续提升事件应对及恢复计划。



7. 信息和通讯技术 (ICT) 包括网络安全 – 银行应确保ICT (包括网络安全) 富有韧性,即应具备保护、侦测、应对及恢复程序,且这些程序应接受定期测试、具备合理的情景认知并可及时传达相关信息以协助风险管理和决策流程,从而全面支持和促进银行关键运营的交付。

虽然其在“系统性风险的全面架构”⁵中提及有限可持续性、危机应对及管理以及服务干扰。BCBS原则是高层次并具合理性,在缺乏其它指引的情况下,尽管有行业特定要求,非银行机构可利用这些原则指引并制定策略。

适用于所有机构的运营韧性架构

英国监管机构将运营韧性定义为:“机构、金融市场基础设施以及银行业作为一个整体以防止、适应和应对运营中断事件及从这些事件中恢复及吸取教训的能力”。2019年咨询文件就重要业务服务⁶以及外包及第三方风险管理⁷的影响容忍度提出期望。英国方案力求“优先考虑重要事项”

以及“推进必要的改革”。

主要要求包括:

- **治理:**运营韧性必须由董事会驱动,并为差异化的投资决策设立明确的、合理考量韧性的问责制度。责任承担方很可能是高管层及认证体系下的首席运营职能角色。
- **重要业务服务:**董事会及高管层应优先考虑“重要业务服务”的韧性 — 即那些若被中断将对英国金融业稳定性、机构安全及稳健性以及合理的投保人保护 (对保险机构而言) 构成风险的服务。对多数机构而言,这将意味着摒弃过去只关注单独系统和

资源的韧性的思考方法,转向关注向客户或投保人提供的服务。

- **影响容忍度:**机构必须界定各项重要业务服务可以承受的最大中断容忍水平,作为影响容忍度,并制定相关指标以监控和计量机构能否保持在容忍度之内。机构应阐明特定中断的最大限度,如它们在“严重但可能发生”的业务中断后能够恢复重要业务服务交付的时限。

⁵ <https://www.iaisweb.org/page/news/press-releases-prior-to-2014/file/87109/holistic-framework-for-systemic-risk>

⁶ <http://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/publication/2021/building-operational-resilience-impact-tolerances-for-important-business-services.pdf>

⁷ <https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/consultation-paper/2019/cp3019.pdf>

© 2021毕马威会计师事务所(特殊普通合伙) — 中国合伙制会计师事务所,毕马威企业咨询(中国)有限公司 — 中国有限责任公司及毕马威会计师事务所 — 香港合伙制事务所,均是与英国私营担保有限公司 — 毕马威国际有限公司相关联的独立成员所全球性组织中的成员。版权所有,不得转载。

- **梳理:** 机构为交付其最重要服务而调配的资源必须在技术、数据、人员、设施、供应商及关键从属流程等方面予以识别和记录。点对点供应链活动的韧性必须予以考量。
- **测试:** 机构应识别“严重但可能发生”的情景以测试自身在影响容忍度范围内作出响应及恢复的能力。
- **沟通:** 机构必须实施稳健的内部及外部沟通方案以管理极端中断事件过程中受到的影响,并重点确保所提供信息的及时性及准确性。
- **恢复:** 机构必须展示它们已采取果断、有效的措施以提升韧性,并已在机构文化中融入以恢复为中心的思维。
- **为建立韧性而投资:** 机构应对自身的运营韧性负责,并根据方案和投资对公共利益的影响对它们进行优先选择。

运营韧性再次被视为保持金融稳定性的结果以及关键因素。对支持良好的客户结果及有效管理行为风险而言,运营韧性也是关键。相关方案旨在应对运营韧性面对的风险,包括由于金融系统的相互关联性以及机构运营所在的复杂及快速变化的环境导致的风险。政策定稿⁸已于2021年3月发表,将于2022年3月31日生效,实施期长达三年。

工作进行中 — 美国及其它地区

2019年11月,在银行政策学会年度会议上,联邦储备委员会的大型机构监督协调委员会(LISCC)副主任John A. Beebe表示⁹,美联储尚未正式界定运营韧性的定义,亦未制定相关政策。但他提及银行在业务中断中

交付关键服务的能力以及人们熟悉的网络韧性概念,即识别、侦测及防御危机事件,并在事件发生时作出响应并恢复。

在此期间,相关工作已取得一定进展。美联储现已将运营韧性定义¹⁰为:“在任何危险导致的业务中断事件中交付运营(包括关键运营及核心业务线)的能力。机构必须具备有效的运营风险管理以及充足的财务及运营资源才能准备、适应和抵御业务中断并从中恢复。”

2020年10月,美联储、联邦存款保险公司以及货币监理署联合发表了一份名为“提升运营韧性的良好实务”(“Sound Practices to Strengthen Operational Resilience”)的文件¹¹。此文件针对合并资产总值超过2500亿元(或总资产及其他风险特征超过1000亿美元)的美国银行,并涵盖治理及运营风险管理、第三方风险、IT韧性、网络安全及情景开发等多个领域。文件并未修改现有条例或提出新规例,而是概述了从现有规例、指引、声明及通用行业标准中提炼的实务方式来提升运营韧性。该文件指出,此等实务方式“是基于有效的治理及风险管理方式、以及第三方风险和包含具恢复力的信息系统。”

2020年12月,欧洲央行提出了期望,即主要欧洲银行将需在整体运营韧性方面取得发展,而不仅是网络方面。欧洲央行希望确保相关要求与英美监管机构的要求相协调。

从澳大利亚审慎监管机构(“APRA”)的运营风险团队在1999年成立以来,运营韧性一直是其重点关注领域。APRA将运营韧性定义¹²为“实体抵抗冲击并从中恢复的能力”。其表示,冲击包括会威胁实体提供业务服务的能力的事件以及已中断实体业务服务提供的事件。在极端情况下,

这包括可能会损害实体持续生存能力的事件,如新冠疫情。

从1999年以来,APRA已发布有关外包、业务延续性管理(“BCM”)以及风险管理的审慎标准和有关疫情规划、数据风险管理及信息安全(网络)的指引,并发表了一份有关云计算的参考文件。

运营韧性小组于2020年成立,有关BCM、外包及风险管理的审慎标准及指引的修订与更新也预期于2021年推出。与此同时,进一步的运营韧性要求及/或指引也很可能同步发布。

2020年6月,新加坡金融管理局发表¹³了相关指引及公告以应对运营、科技及网络风险,但其发表的背景是针对疫情响应,而非新要求的制定。

8 <https://www.bankofengland.co.uk/prudential-regulation/publication/2018/building-the-uk-financial-sectors-operational-resilience-discussion-paper>

9 <https://bpi.com/wp-content/uploads/2020/01/112019-BPI-DEFINING-OPERATIONAL-RESILIENCE.pdf>

10 <https://www.federalreserve.gov/supervisionreg/topics/information-technology-guidance.htm>

11 <https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20201030a1>

12 <https://www.apra.gov.au/covid-19-a-real-world-test-of-operational-resilience>

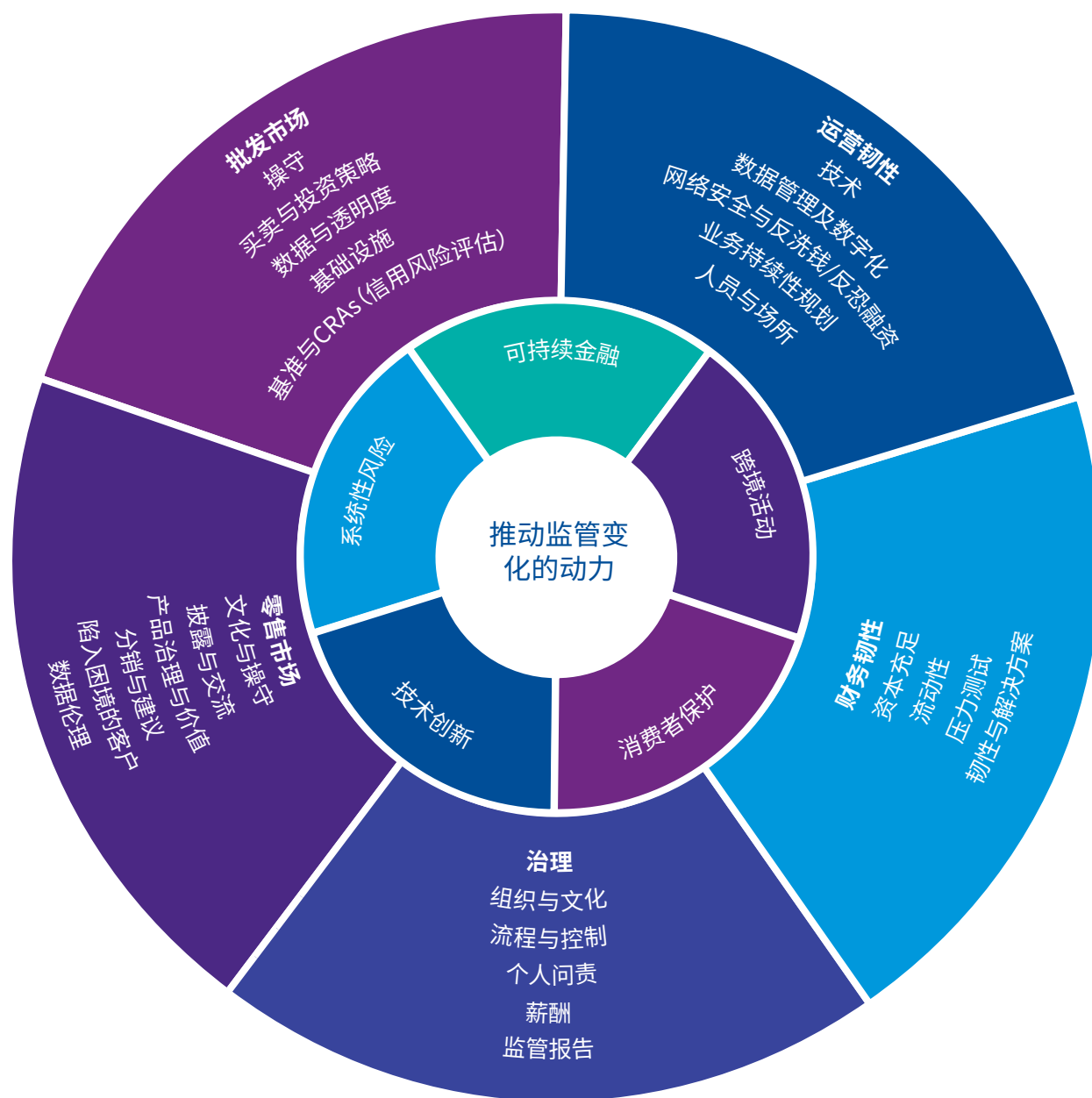
13 <https://www.mas.gov.sg/regulation/covid-19/ensuring-safe-distancing-and-operational-resilience-of-the-financial-sector>

2021年3月,其再发表一份关于“远程工作环境的风险管理及运营韧性”报告¹⁴以进一步阐述此主题。

该报告聚焦金融机构在运营、科技、信息安全、舞弊及员工不当行为等方面的潜在风险以及法律及监管风险。

对欧盟而言,稳健的ICT一直是业界焦点,金融实体的数字运营韧性现已成为重中之重(见第三章)。

新形势下的运营韧性



影响监管重点的五大动力。消费者保护和金融稳定是金融服务监管的堡垒,但疫情及因此而实施的封城措施暴露了更多问题。资本市场的波动使人们再度将目光转移到与计算机主导买卖策略及特定类型基金相关的系统性风险。此外,疫情还加快了科技应用及可持续金融需求的趋势,而跨境交易将面对新的挑战。这三大趋势目前是对监管重点有同样重要影响的动力。

14 <https://www.mas.gov.sg/-/media/MAS/News-and-Publications/Monographs-and-Information-Papers/Risk-Management-and-Operational-Resilience-in-a-Remote-Working-Environment.pdf>

02. 关注第三方风险

FSB在2020年11月指出，金融机构已在过去数十年依赖外包及其它第三方关系。但其也表示，在近年，机构与“一个广泛和多样化的第三方生态”进行互动的范围和性质已取得发展，尤其是在科技领域。金融板块近期对新冠疫情的响应突出了管理金融机构与第三方互动带来的风险的裨益以及挑战。疫情还可能加快了机构愈加依赖某些第三方技术的趋势。

金融服务机构为了获得外包提供的成本、效率及专业性方面的效益，已纷纷转用该类服务。多数金融机构并非基础设施专家，虽然它们已实施大量项目以简化或重组现有流程，但仍或多或少地受到旧有系统的掣肘。转型项目对大型机构而言成本高昂且繁复，而小型机构则根本缺乏内部的能力与资源以开发专属解决方案。

对它们而言，外包或会是一个具吸引力的选项，但第三方关系也带来不少挑战。监管机构关注的是：

- 供应商的集中度
- 合同条款，包括退出条款和规划
- 数据安全
- 访问权和监督，包括治理、系统及控制
- 第三方的韧性，包括BCP和灾后恢复
- 对与外包商的文化校准和融入性的合理考量
- 为客户输出的成果欠佳

适用于投资机构的外包原则

2020年5月，IOSCO就新的“外包原则”进行咨询¹⁵。这些新原则基于现有的2005及2009年原则，并进一步涵盖交易场所、自营市场参与者、信用评级机构和金融市场基础设施。IOSCO表示，“运营韧性是指受监管实体、服务供应商等其它机构以及作为一个整体的金融市场避免、应对运营中断、从中恢复及吸取经验的能力”。

经修改的原则包含一组基本准则和七项原则。基本准则涵盖外包定义、重要性及关键性评估、关联实体上的应用、分包处理以及跨境外包等事项。七项原则涵盖以下领域：

- 选择和监控服务供应商中的尽职调查
- 与服务供应商订立的合同
- 信息安全、业务韧性、延续性和灾后恢复
- 保密事项
- 外包安排的集中度
- 对数据的获取、工作场所的进入和人员的接触以及相关检查权利
- 外包安排的终止

系统性风险视角

FSB的《关于外包及第三方关系的规范监督事宜》讨论稿¹⁶反映了许多机构正面对的问题和挑战。讨论稿探讨了与外包及第三方关系有关的规范监督事宜，尤其关注云和云服务供应商的集中度问题。

业界存在一个疑虑，即某些向金融机构提供的外包及第三方服务的集中可能会引致系统性风险。随着从某个第三方获取关键服务的金融机构的数量增加，这些风险将会增大。

当缺乏合理的缓释因素时，此类第三方的一个重大业务中断、停运或失效便可能会导致单点失效，

国际证监会组织 (IOSCO) 外包原则

原则一：受监管实体应执行适当的尽职调查流程以选择合适的服务供应商并持续监控其表现。

原则二：受监管实体应与各服务供应商签订有法律约束力的书面合同。这些合同的性质和内容应与外包任务对受监管实体业务的重要性或关键性相称。

原则三：受监管实体应采取合理措施以确保其与任何服务供应商建立相关程序与控制以保护受监管实体的专有及客户信息和软件，并确保服务供应商对受监管实体提供服务的延续性，包括灾后恢复计划以及对备用设施的定期测试。

原则四：受监管实体应采取合理措施以确保服务供应商保护好受监管实体及其客户的保密信息及数据，避免它们向第三方作出有意或无意的未经授权披露。

原则五：当受监管实体需依赖单独的服务供应商以交付重要或关键的外包任务，或当其知道某个服务供应商为包括其在内的多个受监管实体提供重要或关键的外包服务时，该受监管实体应了解其中风险并进行有效的风险管理。

原则六：受监管实体应采取合理措施以确保其监管者、审计师及自身能在发出请求后立即获取合同合规及/或监管监督方面的外包任务信息，包括在需要的情况下获得与外包任务相关的数据、访问相关IT系统、进入服务供应商工作场所及接触有关人员。

原则七：受监管实体应在其与服务供应商之间的合同中加入外包任务终止的有关书面条款，并确保已建立合理的退出策略。

并对金融稳定及/或多个金融机构的安全及稳健带来潜在负面影响。鉴于此依赖关系的跨境属性，FSB表示，监管机构和第三方可通过增加这方面的对话而获益。FSB表示，此讨论稿将促进业界对外包及第三方风险管理的现行监管方式的讨论。

¹⁵ <https://www.iosco.org/library/pubdocs/pdf/IOSCOPD654.pdf>

¹⁶ <https://www.fsb.org/2020/11/regulatory-and-supervisory-issues-relating-to-outsourcing-and-third-party-relationships-discussion-paper/>

FSB指出,金融机构、相关监管者以及清算机构访问、核查及获取第三方信息的契约性权利或难以商讨及行使,尤其是在一个多辖区背景下。在金融机构应对新冠疫情影响的背景下,分包商和供应链管理也是其中一个焦点。作为《金融科技行动方案》的一部分,欧盟委员会有意为外包协议制定标准合同条款。

欧洲方案成形

欧洲监管局(ESA)对外包指引采取了一个大体上协调的方案。

欧洲银行业管理局(EBA)于2019年2月发表了最终版的外包安排指引¹⁷,其中纳入了有关云外包的早前建议。重点是,外包并不会解除管理层的责任,管理层必须保留就外包业务活动进行决策的能力。

关键或重要职能的外包安排适用更严格的要求。机构必须对所有最新的外包安排做好记录,记录(如适用)必须在分支合并(sub-consolidated)

及合并层面进行,且在国家监管机构要求下应向其提供。方案提供了详尽的外包流程指引,从外包前分析到合同阶段的风险评估和尽职调查、访问、信息及核查权、终止权、外包职能监督以及退出策略。

2020年2月,欧洲保险和职业养老金管理局(EIOPA)发表了相同16个标题下的向云服务供应商¹⁸外包的指引最终版。这些指引同样要求详尽的风险评估、尽职调查和外包前分析。若关键或重要运营职能或活动需被外包,保险机构应在其自有风险及偿付能力评估(ORSA)中的风险状况中反映此信息。

在考虑相称原则的情况下,机构还应向监管机构提供书面说明。

保险机构需对云外包安排进行专门登记,包括近期终止的安排。合同要求需明确列明保险机构和云服务供应商各自的权利和义务。合同应包含可获取性(包括核查权)、服务可用性、完整性、保密性、数据隐私和

安全以及绩效监控等条款。就核查权而言,当与其他客户一起对同一服务供应商进行审计时或由多个客户委派一名第三方进行审计时,保险机构可考虑使用有云供应商提供的第三方认证或内部审计报告及/或合并审计。指引还提及终止权、外包职能监督以及退出策略。

¹⁷ https://eba.europa.eu/sites/default/documents/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA_revised_Guidelines_on_outsourcing_arrangements.pdf

¹⁸ https://www.eiopa.europa.eu/sites/default/files/publications/eiopa_guidelines/guidelines_on_outsourcing_to_cloud_service_providers_en.pdf



2020年6月，欧洲证券与市场监管局 (ESMA) 要求对云供应商进行全面审计，并于2020年12月发表了云服务供应商外包指引的最终版¹⁹，从2021年7月起实施。ESMA的九项指引与EBA及EIOPA的指引大致相同，同时考虑到欧盟委员会在2020年9月发布的数字运营韧性规范建议书（见第3章）。ESMA要求机构应为各项云外包服务实施具体策略，包括合理的治理安排和更严格的网络安全措施。外包前分析以及尽职调查应在委任供应商前执行。合同一般须包含有关访问及核查权及分包的具体条款。机构需在委任供应商前考虑退出策略（包括计划并测试机构如何迁移到另一家供应商；并不断更新外包登记信息，并在监管机构要求下向其提供。

虽然英国不再属于ESA的监管范围，但审慎监管局 (PRA) 在其有关外包及第三方风险管理的建议书²⁰及最终政策²¹中纳入许多ESA的指引。

但PRA的要求比ESA的更广泛和深入。譬如，ESA主要关注外包安排，而PRA探讨了所有重要的第三方安

排。PRA还要求机构在确定重大外包决定前作出通知，并就受压退出计划相关的退出及意外规划以及退出计划的情景测试制定了更进一步、更详尽的要求。PRA已计划进行后续咨询，并提出了有关在线门户的详细提案。所有机构将需通过此在线门户提交外包及第三方安排的信息。

有关第三方安排的要求正变得愈加繁重。治理、监管及记录方面的指引及规范或对小型机构带来挑战。由于特定外包或云战略的交付或在某些机构的能力范围之外，这些机构将需寻求外部指引。

机构的主要考量：

- 治理及记录
- 评估重要性和内在风险
- 签约前尽职调查
- 风险导向合同条款
- 安全及数据控制
- 持续风险评估
- 访问及核查权
- 管理分包商风险
- 退出计划及或有事项
- 与运营韧性项目的联系

19 https://www.esma.europa.eu/sites/default/files/library/esma50-157-2403_cloud_guidelines.pdf

20 <https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/consultation-paper/2019/cp3019.pdf>

21 <https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/consultation-paper/2021/march/ps721.pdf>

© 2021毕马威华振会计师事务所(特殊普通合伙) — 中国合伙制会计师事务所, 毕马威企业咨询(中国)有限公司 — 中国有限责任公司及毕马威会计师事务所 — 香港合伙制事务所, 均是与英国私营担保有限公司 — 毕马威国际有限公司相关联的独立成员所全球性组织中的成员。版权所有, 不得转载。



03. 向更高级的数字化韧性迈进

长期以来，网络韧性一直是韧性项目的支柱，并将继续在未来保持重要性。但在新形势下，业界关注正向更广泛的ICT风险环境扩展。同时，欧盟已提出了“数字化运营韧性”这一技术驱动型定义。

网络与ICT韧性 – 基本元素

作为确保金融行业的业务延续性的基础，网络韧性和ICT风险一直是业界的重点关注。在疫情发生前四年内，许多框架和指引已发表，这些框架和指引正被更新和扩展。

多数网络规范是不分行业的，如欧盟的2016年《网络及信息安全 (NIS) 指令》、全球性的国家标准和技术研究所 (NIST) 网络安全框架以及欧盟委员会的2020年欧盟网络安全战略。但更针对金融服务的条款已被制定。NIS将被扩展以涵盖更多行业并对“重要实体”提出更严格要求，其中包括金融服务及云和数据服务供应商。作为ICT监管审核及评估流程的一部分，欧盟银行亦需遵循特定要求。

2016年，支付及市场基础设施委员会 (CPMI) 以及IOSCO委员会联合发

布²²了金融市场基础设施的网络韧性指引。就以下主题列出了国际公认的指引：

- 董事会及高管层关注稳健网络治理的重要性
- 在遭受网络攻击后快速、安全地恢复业务运营的能力
- 利用质量良好的威胁情报及严格测试的需求
- 逐步建立网络风险认知，并持续评估和提升组织内各个层面的网络韧性
- 网络韧性作为整个生态体系的集体努力

2017年，FSB发表²³了《金融业网络安全规例和指引及监管实务汇总报告》以促进跨境合作。随后，《网络辞典》²⁴于2018年发布，包含约50个与金融业网络安全及网络韧性有关的

核心术语。

FSB于2020年10月发表的金融机构工具包²⁵包含了以下七个部分的49项有效网络事件应对及恢复实务：治理、计划与准备、分析、缓释、复原及恢复、协调和沟通以及提升。作为2021年工作计划的一部分，FSB还探讨了网络事件监管报告的趋同范围以及对FSB网络辞典进行修订的需要。

22 <https://www.iosco.org/library/pubdocs/pdf/IOSCOPD535.pdf>

23 <https://www.fsb.org/2017/10/summary-report-on-financial-sector-cybersecurity-regulations-guidance-and-supervisory-practices/>

24 <https://www.fsb.org/2018/11/cyber-lexicon/>

25 <https://www.fsb.org/2020/10/fsb-instrumental-guidance-for-financial-institutions-response-and-recovery-toolkit/>

© 2021毕马威华振会计师事务所(特殊普通合伙) — 中国合伙制会计师事务所，毕马威企业咨询(中国)有限公司 — 中国有限责任公司及毕马威会计师事务所 — 香港合伙制事务所，均是与英国私营担保有限公司 — 毕马威国际有限公司相关联的独立成员所全球性组织中的成员。版权所有，不得转载。

欧盟在2018年5月提出TIBER-EU框架(威胁基于情报道德的红队框架),由欧洲央行和欧盟国家银行联合制定,适用于作为核心金融基础设施的构成部分的(超)国家机构和实体。英国的大型受监管机构需接受CBEST渗透测试。此测试由英格兰银行创建,并获得道德安全测试员理事会(CREST)的支持。

在2018年末,欧洲央行发布²⁶了其对于金融市场基础设施的网络韧性监管期望;而美国证券交易委员会则于2020年1月发表²⁷了《网络安全及韧性观察》。

欧盟还出台了多项ICT风险指引。2017年5月,EBA发布²⁸了监管审核及评估流程下的《ICT风险评估最终指引》。2019年11月,ICT及安全风险管理最终指引出台²⁹。对保险机构而言,EIOPA关于ICT安全及治理的公开咨询³⁰在2020年3月结束。在国家层面,德国监管机构的“BAIT³¹”和荷兰中央银行的IT原则明确了当地监管预期,为机构提供了一个框架以执行IT风险管理的最低要求。

更广泛视角 – 通向DORA之路

欧盟委员会发布³²了一份针对金融业的涵盖广泛的数字运营韧性规范初稿(DORA)。此初稿是基于目前对运营韧性的监管预期,但重点关注机构从技术角度建造、保证及评估运营完整性的能力。DORA将建立一个全面的欧盟架构,包含适用于所有受监管金融机构的规则。其将:

— 通过以下手段,简化及提升现有金融法规并对不足之处提出新的要求:

- 更好地将机构的业务战略与ICT风险管理协调一致,从而提升ICT风险的全面管理,并确保机构能评估自身预防及

恢复措施的效力并识别ICT缺陷

- 根据机构规模、业务及风险状况,合理应用测试要求
- 加强机构监管并确保妥善监管第三方ICT
- 通过信息分享提升ICT风险意识和减低风险扩散,手段包括允许机构交换网络威胁信息和情报

— 通过以下手段,建立更连贯、一致的事件报告机制,以减少机构的行政负担和提升监管效率:

- 协调和简化ICT相关事件的报告
- 通过让监管者获取相关信息,提升它们对威胁及事件的了解。

前路或有挑战

DORA的宗旨是无可非议的,但各方还远未能就建议达成一致,方案在欧盟内部的执行也可能存在挑战。

目前,数个潜在问题已浮现,尤其是DORA需与其他指引及法规相互影响或共存。DORA将需要对多个现行金融服务法规进行修订,包括MiFID II、Solvency II、UCITS 和 AIFMD。

目前尚不明确这些相互影响及修订将如何执行,尤其是当现行指引已达成一致但尚未完全实施时。

此外,涉及的范围十分广泛。超过30类金融实体牵涉其中,而提供的相称性让步十分有限。ICT风险管理建议书(包括第三方风险管理)的执行将十分复杂。重大事件报告及执行流程需作进一步澄清。ESA将发布的详细规则及指引有望明确某些要点,但不大可能消除所有挑战。

“数字化运营韧性是指金融实体通过直接或间接地使用ICT第三方供应商服务,以确保为实现金融实体需利用的、支持金融服务的持续供应及其质量的网络及信息系统的安全所需的各项ICT相关能力,从而从技术角度建立、保证及评估其运营完整性的能力。”

26 https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf

27 https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf

28 [https://eba.europa.eu/sites/default/documents/files/documents/10180/1841624/ef88884a-2f04-18a1-8298-bb9c25b269a5/Final_Guidelines_on ICT_Risk_Assessment_under_SREP_\(EBA-17-05\).pdf](https://eba.europa.eu/sites/default/documents/files/documents/10180/1841624/ef88884a-2f04-18a1-8298-bb9c25b269a5/Final_Guidelines_on ICT_Risk_Assessment_under_SREP_(EBA-17-05).pdf)

29 https://eba.europa.eu/sites/default/documents/files/documents/10180/2522896/32a28233-12f5-49c8-9bb5-f8744ccb4e92/Final_Guidelines_on ICT_and_security_risk_management.pdf

30 https://www.eiopa.europa.eu/content/consultation-proposal-guidelines-information-and-communication-technology-ict-security-and_en

31 Bankaufsichtlichen Anforderungen and die IT

32 <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0595&from=EN>

多个ESA主席在2021年2月发出的联名信³³同意DORA的主要原则以及建立一个全面欧盟架构的需要。他们在信中也对增强欧盟内部及国际机构之间的协调和合作的呼声表示支持。但ESA提出了它们对在监督“关键第三方供应商”(CTTP)中承担的拟定角色的疑虑,尤其是在ESA的单个行业特定职权范围内监督跨行业CTTP存在的挑战。

它们还提及赋予它们的权利的错配

— 一旦ESA发布一项建议,相关主管机关将负责跟进和采取执法行动。此类行动包括要求受监管金融实体暂停CTPP服务或终止其与CTPP的合同。最后,它们表示需要充足的资源以履行新的职责以及提升执行上的合理性。

DORA在通过欧盟的立法流程时很可能会作出改变。最终版本有望在未来18至24个月发布。同时,金融实体和ICT服务供应商应留意即将发布的

运营韧性监管要求的重大变更,并开始评估这些变化将如何影响它们的ICT风险管理架构。

DORA的主要挑战



范围 – 实体类型多样、一体适用方案、有限相称性



执行 – 与现有指引相互影响,法规未明确;将直接应用于供应商



ICT 风险管理 – 具体要求可能影响灵活性和敏捷性;或会导致科技资产碎片化



第三方ICT风险 – 规定性要求将对小型机构和旧有系统构成挑战;重要供应商的定义不明确



分类及重大事件报告 – 报告要求需明确及一致;地方特定要求可能会阻碍事件管理;事件分类对国家监管机构构成负担



执法 – 执法权过大可能引起补偿问题或扰乱;不限制国家解释和应用



04. 主题上的变化

近期有关运营韧性的监管公告受到广泛关注。这些公告中大部分是关于术语的变化和潜在政策议程。这可能是监管声明中某些已被察觉的细微差异的基础。

全球统一的看法必然有助机构决策及规划的简化,尤其是对需遵循多个辖区机制的跨国机构而言;但我们可预期的是,不同监管机构以及不同地区或辖区的方案及分类法将有所差异。

措辞差异

不同文件中使用的措辞各不相同。BCBS使用“**关键运营**”(“**critical operations**”),而英国则是“**重要商业服务**”(“**important business services**”).“**关键运营**”是源于联合论坛的2006年业务延续性高层次原则,并借用“**韧性**与**解决方案**”中使用的术语。其包含FSB定义的“**关键职能**”(“**critical functions**”),并对定义进行扩充以涵盖“中断会对

银行的持续运营或其在金融体系中的角色产生重大影响的活动、流程、服务及相关辅助资产”。

在英国,“**商业服务**”是机构提供给外部终端用户或参与者的服务。

当商业服务的失效可导致消费者或市场参与者承受不可容忍的损害、使市场完整性受损或威胁到投保人的保障、机构安全及稳健或金融稳定时,此类商业服务可被视为“**重要**”。

在美国,FRB对“**关键运营**”和“**核心业务线**”(“**core business lines**”)作如下定义:第一个是指其失效或中断将对美国的金融稳定构成威胁的运营;第二个是指其失效会导致机构收入、利润或特许权价值严重流失的业务。

美国或欧盟的建议书中没有**影响容忍度**这个概念,而这是英国方案的基石。英国方案将影响容忍度定义为“在某项商业服务将发生业务中断的假设下,机构对业务中断的容忍度”。英国监管机构强调,影响容忍度不同于风险偏好指标。

但最重要的是,各方对运营韧性的定义大致相同 – BCBS强调“**从中断事件恢复的能力**”,而英国监管机构则要求机构“**应对并适应业务中断事件,并从中恢复并吸取经验。**”

相同目标, 不同视角

如第2章所述, 不同行业及地区的外包及第三方风险的监管要求已高度对应。在更广泛的运营韧性问题上, 监管机构及行业实体关注共同的目标, 如:

- 更强的问责及责任归属以及自上而下的管理
- 机构关键业务活动的明确定义
- 了解交付这些活动所需的主要依存关系
- 测试压力情景下的韧性
- 确定有意义的指标以量化韧性及评估对业务中断的容忍度
- 确保与客户、投保人或投资者进行及时、合理的沟通

BCBS代表着28个辖区和45个机构, 已提出多项高层次原则, 如治理、业务延续性及事件管理。其已明确表明, 运营韧性将要求管理和降低风险以确保关键运营的持续性。但国家机关需决定是否采取更具指令性的方案。

英国已选择制定更详细的运营韧性框架, 包含为机构提供更具体的要求, 并为监管者的后续监控提供清晰预期。我们可在从2008年金融危机以来已广为人知的韧性失效事件以及源自多个源头的威胁升级的背景下审视此次框架制定。英国监管机构还重点关注消费者损害以及运营韧性失效导致行为问题的可能, 这或反映了英国的双重监管方案。按英国方案的交付也适用于按BCBS原则的交付。

在欧盟和美国, 有关运营韧性的探讨往往局限于风险职能内部。在某些情况下, 特定职责应归属风险部门, 如在EBA的ICT指引下。但对将运营韧性职责分配给首席运营职能而不是首席风险职能而言, 英国方案并未明确哪条防线应承担职责。相反, 在这个愈加数字化的世界, 目的应是增强

科技的角色并鼓励降低观点之间的相互孤立, 使机构能真正以服务为基础地看待它们最重要的活动。对第三方风险管理而言也是如此。其在过去一般被视为采购活动, 但目前它已成为许多金融服务机构持续运营的基础。

抓住要领

机构在制定运营韧性方案时必须注意定义的差异。与其说是为了展示分歧, 此类差异更可能反映了辖区之间如何制定法规及/或法规如何演进的差异。

过多关注语言及格式上的差异或意味着机构采取了一个过于合规导向的方案。

若机构仅关注某个立场是否比另一个立场更清晰或更优越, 那么, 其便没有抓住要领。不论监管机构各自的具体监管要求或定义是什么, 它们的真正目的是**使金融服务业更能抵御运营中断事件, 从而降低风险传导的范围、金融不稳定的可能和对终端客户带来的损害。**



05. 展望未来, 吸取教训

从监管角度而言, 新冠疫情并未改变事情的发展方向。若真有什么改变的话, 疫情加快了监管力量的推进, 这从欧盟的DORA和其它指引的发布可以看出。根据欧盟委员会的数据, 在新冠疫情开始时, 欧洲地区的金融应用使用量在一周之内增加³⁴了72%; 在疫情流行期间, 金融机构遭受的网络攻击增加了38%。这些数据显示了机构对稳健的运营韧性的明确、持续的需求。

BCBS原则和DORA包含了从新冠疫情中吸取的教训, 而英国的咨询方案则在疫情前已发布。但英国提出的所有概念均未在最终政策声明中削弱, 全球监管机构也继续宣传运营韧性的重要性。

机构正致力应对一系列执行挑战, 包括如何更好地:

- 通过建立一个更长期的可扩展、可持续的运营模型、建立真正的问责制和培育韧性文化, 以实现短期监管合规和战略韧性
- 在全球一致性与本地具体要求之间取得平衡 - 当运营韧性的各个方面并非同等适用于集团内的所有受监管实体时, 该怎样管理?
- 在狭义及广义的服务定义、完整性及颗粒度之间取得合理平衡
- 校准无法忍受的损害与影响容忍度 - 业界将需一段时间才能接受此类新概念
- 展望未来, 驾驭数字化韧性的潜力
- 监管机构已认识到监管碎片化的危险, 并尽可能进行合作。英格兰

银行正领导着FSB有关外包安排的工作, 并参与BCBS原则的制定。欧洲央行和PRA已承诺相互合作并与FRB协调以确保妥善配合的监管方案的实施。监管机构也面临挑战, 尤其是在新技能的需求下, 如何确保它们具备适合的专业人才以实现有效监管。

某些重大问题仍然存在, 譬如:

- 由于并非所有机构都采用相同的架构, 因此“良好”的标准是什么?
- 监管机构将如何使用它们收集的数据?
- 会最终实施资本占用及强制韧性压力测试吗?
- 此类测试会否导致表现欠佳者接受处罚? 潜在的声誉影响是什么?
- 监管范围可以或应该如何扩展以将其他实体纳入要求范围之内?

数年前, 所有讨论都是关于网络韧性。如今, 机构讨论的不仅是网络, 还

包括疫情及气候事件等业务中断因素影响下的韧性。业界需进行更多工作以确保整个系统具备必要的韧性以应对所有可能对金融体系构成风险的潜在威胁。监管者或能通过持续合作, 更好地识别全球标准及趋同需作进一步深化的领域。

监管要求很可能较为严格并范围广泛, 但根本而言, 其传达的信息是一致的 - 运营韧性对组织的成功及可持续性而言十分关键, 监管者已将其视为一项董事会议程。机构必须立即行动, 提升运营韧性以为未来做好准备。



本领先思维刊物系列将发布探讨其它“新形势”问题的最后一份报告, 请密切留意。

联系方式

Francisco Uriá Fernandez

EMA 金融服务、银行与资本市场主管合伙人

Karim Haji

英国金融服务主管合伙人

Michelle Adcock

EMA金融服务监管洞察中心

Philip Deeks

EMA 金融服务监管洞察中心

徐捷

金融业治理与风险咨询服务

主管合伙人

电话: +86 10 8508 5952

电邮: jessica.xu@kpmg.com

Andrew Husband

合伙人, Powered Resilience Leader

毕马威英国

James Lewis

EMA金融服务监管洞察中心联席主管

Kate Dawson

EMA金融服务监管洞察中心

Julie Patterson

EMA 金融服务监管洞察中心

李建维

金融业运营管理咨询服务

合伙人

电话: +86 21 2212 3676

电邮: frank.li@kpmg.com

home.kpmg/regulatorychallenges



本报告所载列的某些服务或全部服务,可能不允许提供给毕马威审计客户及其联营公司或关联实体。

所载资料仅供一般参考用,并非针对任何个人或团体的个别情况而提供。虽然本所已致力提供准确和及时的资料,但本所不能保证这些资料在阁下收取时或日后仍然准确。任何人士不应在没有详细考虑相关的情况及获取适当的专业意见下依据所载资料行事。

©2021毕马威华振会计师事务所(特殊普通合伙) — 中国合伙制会计师事务所,毕马威企业咨询(中国)有限公司 — 中国有限责任公司及毕马威会计师事务所 — 香港合伙制事务所,均是与英国私营担保有限公司 — 毕马威国际有限公司相关联的独立成员所全球性组织中的成员。版权所有,不得转载。

毕马威的名称和标识均为毕马威全球性组织中的独立成员所经许可后使用的商标。

本出版物经毕马威国际授权翻译,已获得原作者及成员所授权。

本刊物为毕马威国际发布的英文原文 Redefining operational resilience (“原文刊物”) 的中文译本。如本中文译本的字词含义与其原文刊物不一致,应以原文刊物为准。

CREATE | CRT004865 | 2021年6月

点击进入  <http://www.hibor.com.cn>

“慧博资讯”专业的投资研究大数据分享平台