

非常态下商业银行业务连续性（BCM）风险管控及应对策略

梁力军 副教授

一、培训背景

5 业务连续性管理（Business Continuity Management，BCM）是一项综合性的管理活动，通过识别组织所面临的潜在风险，评估风险可能对组织造成的影响，建立一套组织、流程和资源相配合的体系，提升组织应对风险的能力，保障组织价值创造活动的持续进行，有效提升组织的品牌声誉和相关方利益。

10 2011年12月底，中国银监会曾发布《商业银行业务连续性监管指引》，指引中明确规定了商业银行应当将业务连续性管理纳入全面风险管理体系，建立与本机构战略目标相适应的业务连续性管理体系。2020年初，新冠肺炎在我国爆发。中国全民上下共同抗击此次疫
情。我国银行业也积极响应，陆续调整金融政策和服务策略以便为中小微企业、零售客户提供各类更为快捷、适当的金融支持和金融服务。在此背景下，各类商业银行更应构建起真正有效的应对危机事件的业务连续性管理体系，使业务管理和系统管理实现科学化、快捷化、
15 网络化，这是保证银行业务连续运行、可持续发展的重要依据。

随着商业银行业务和机构的不断扩张，银行系统及业务的信息化程度提升，而系统运行和业务经营、金融环境也日益复杂。商业银行在面连续性风险管控与应对、如何更加有效地进行
20 商业银行全面风险管理，从而保证国家金融安全稳定发展，是我国金融监管部门和银行经营管理者共同关心的重大课题。

二、培训方案

20

Vuca – volatility（易变性），uncertainty（不确定性），complexity（复杂性），ambiguity（模糊性）

本培训设计为一天（6小时）。

第一天：业务连续性风险“规范标准篇”+“管控流程篇”

25 通过业务连续性风险事件视频素材与态势分析，引出实施金融业业务连续性风险管理的思考。

讲解和剖析国内外金融业业务连续性风险管理的行业规范与标准，并提出适合于参训机构、具可操作性的业务连续性风险管理规范与标准。

从战略层面和三道防线层面讲解国内外金融业业务连续性风险管理实施的流程，并提出适合于参训机构的、具可操作性的业务连续性风险管控流程。

第二天：业务连续性风险“工具实践篇”+“策略实施篇”

5 以银行信息系统和金融数据、银行业务的“生命周期”为主线，讲解不同阶段对应的业务连续性风险管理工具与方法，并比较不同工具与方法的优劣。

讲解国内外金融监管机构的业务连续性风险监管规范、监管科技工具、监管要求与要素等。从监管要求视角，讲解商业银行应如何进行业务连续性风险管控策略与方案的设计（BCP）等。

三、培训要点

10 一是业务连续性风险管理规范标准。通过信息与资料梳理、视频素材分析，解析国际和国内金融业在业务连续性风险控制、风险评级、信息安全和网络安全、系统安全和数据安全、科技及业务项目管理、信息资产与基础设施、信息科技外包管理等方面的管理框架、行业标准和最佳实践，分析比较国际与国内金融业业务连续性风险管理方面的特点、趋势和可借鉴之处。

15 二是业务连续性风险管控实践。（1）从战略层面、战术层面和操作层面三个视角，分析国内外金融业信息科技治理结构的架构、信息科技管控流程的构建和信息科技系统管控的实施等；（2）从三道防线视角，即信息科技部门、业务连续性风险管理部门、信息科技审计（稽核）部门，分析国内外金融业如何进行业务连续性风险管控的有效协作、资源与信息共享、数据传递等；（3）从全面风险管控流程视角，分析国内外金融业如何实现对业务连续性风险的感知与识别、评估与计量、应对等。

20 三是业务连续性风险管控工具实践。以银行业务、金融数据和信息系统的“生命周期”为主线，从信息科技立项与需求分析、科技项目采购与招投标、项目开发、项目时间与质量管控、成本控制和资源管控、沟通管理、信息科技测试与运行等不同阶段讲解适用的各类业务连续性风险管控工具与方法；从业务连续性风险存在的不同载体——系统、设备、网络、数据
25 和人员等视角，讲解防范信息系统单项风险和综合风险的工具与方法。

四是业务连续性风险监管与对应实施策略。讲解国外金融业监管机构（巴塞尔委员会、COSO）、国内金融业监管机构（人民银行、银保监会、证监会）以及相关机构，实施业务连续性风险监管的具体标准和规范、实施要素和要点等，从而提出针对商业银行特点的业务连续性风险管理对应策略。

四、培训特点

一是以业务、系统与数据的“生命周期”为剖析主线，逻辑清晰。

本培训内容将针对公司治理、业务循环、系统循环和数据循环等不同阶段和环节，系统性、动态性的分析业务连续性风险管理的特征与规律。

5 二是将业务连续性风险管理的理论与实践相结合，理实结合。

本培训系统性的分析业务连续性风险及风险管理的规范、行业标准、方法与工具、金融监管的国际、国内前沿发展和最佳实践，并结合业务连续性风险管理案例信息、视频素材、数据资料进行剖析讲解。

三是提出业务连续性风险管理的实施体系与建议，具指导性。

10 本培训基于风险管理三道防线、“业务-数据-系统”生命周期，系统性提出金融机构实施业务连续性风险管理的实施体系与建议方案，具有可操作性、指导性。

五、培训收益

本培训通过系统讲解金融业（包括人民银行、银保监部门、商业银行、证券业及保险业等）业务连续性风险管理体系与框架、信息管理科技风险特征与分布、业务连续性风险的生命周期追踪、业务连续性风险管理具体技术及方法、业务连续性风险治理、业务连续性风险监管等方面的最新发展和最佳实践，提出适合于参训机构实施业务连续性风险管理的实施方案和体系建议，有效提升参训机构的业务连续性风险管理能力。工具、营销策略，全面提升商业银行零售金融的营销能力。

15

六、授课对象

20 各类商业银行、互联网公司、类金融企业等机构的信息技术部、电子银行部、网络金融部、风控合规部、集中运营部、零售业务部和公司业务部等部门的管理者、技术人员和业务人员等。

七、授课形式

课件讲授：制作培训课件，并以课件作为授课主线。

25 视频解析：通过播放业务连续性风险管理的相关视频，引发并组织参训人员对业务连续性管理进行思考和讨论。

案例分析：通过对中外商业银行的业务连续性管理真实案例，进行解读和剖析，引发参训人员思考。

情景设置与实战演练：通过预设金融场景或引入真实场景，组织参训人员进行业务连续性风险管理思维培训，并设计出相应的敏捷银行服务方案。

八、培训内容

5 (一) 基础认知篇

1. 视频与案例素材剖析

- 国外*业务连续性风险事件视频与案例剖析
- 国内*业务连续性风险事件视频与案例剖析

2. 业务连续性管理内涵及发展

- 10 ■ 业务连续性管理的起源与内涵（BCM）
- 业务连续性风险内涵、种类与全域风险视图
- 国内外业务连续性风险管理专业惯例
- 突发事件及应急对银行业务连续性的影响

15 (二) 规范标准篇

1. 业务连续性国际实践规范标准

- BS 25999（2002；2005）
- ISO 17799（2005）
- 信息安全管理：ISO27001
- 20 ■ 业务连续性管理：ISO22301
- ISACA: COBIT5
- IT 服务管理：ISO20000 和 ITIL V3
- DRI:业务连续性管理

2. 业务连续性国际实践规范标准

- 25 ■ 人民银行
- ✓ 《银行业信息系统灾难恢复管理规范》
- ✓ 《银行集中式数据中心规范》
- ✓ 《网上银行系统信息安全通用规范》
- ✓ 《金融行业信息系统信息安全等级保护》

- 银保监会
- ✓ 《商业银行业务连续性风险管理指引》
- ✓ 《银行业金融机构信息科技外包风险监管指引》
- ✓ 《商业银行业务连续性监管指引》
- 5 ✓ 《银行业重要信息系统突发事件应急管理规范（试行）》
- ✓ 《商业银行数据中心监管指引》
- ✓ 《银行业金融机构重要信息系统投产及变更管理办法》
- 其他相关规范
- ✓ 网络安全法
- 10 ✓ 国家网信办、公安部、国家保密局、国家密码管理局
- ✓ 关键基础设施风险评估
- ✓ 网络安全等级保护
- ✓ 《中华人民共和国突发事件应对法》
- ✓ GBT20988—2007《信息系统灾难恢复规范》□

15

(三) BCM 风险管控流程篇

- 1. 当前 **BCM** 存在的主要问题 □
- 2. **BCM** 风险管控战略/战术/操作
 - BCM 治理架构的构建与实施
 - 20 ■ BCM 管控流程的构建与实施
 - BCM 管控系统的构建与实施
- 3. **BCM** 风险管理三道防线
 - 信息科技部门职责与协作
 - 风险管理部門职责与协作
 - 25 ■ 信息科技审计部门职责与协作
- 4. **BCM** 风险管控流程及系统
 - 业务连续性风险感知与识别
 - 业务连续性风险评估
 - 业务连续性风险计量

- 业务连续性风险监测
- 风险情境恢复与业务恢复（6R 模型）
- 业务连续性风险管理系统构建

5. **BCM** 风险管控国内外实践

- 5 ■ 国外商业银行 BCM 风险管控实践
- 国内商业银行 BCM 风险管控实践

(四) 工具实践篇

1. 业务-数据-系统(**BDS**)生命周期

- 10 ■ 银行业务及产品生命周期管理
- 金融数据生命周期管理
- 信息系统/项目生命周期管理
- 全生命周期管理模式与工具

2. 各阶段 **BCM** 风险管控工具与方法

15

- BDS 需求与设计阶段/案例解析
- BDS 项目立项阶段/案例解析
- BDS 开发与测试阶段/案例解析
- BDS 运行与维护阶段/案例解析

20

- BDS 外包阶段/案例解析
- BDS 业务连续性管理/案例解析

3. 单项与综合 **BCM** 风险管控工具

- 系统与设备安全方面/案例解析
- 网络安全方面/案例解析
- 25 ■ 数据安全方面/案例解析
- 人员与操作风险方面/案例解析

(五) 策略实施篇

1. 国内外 **BCM** 监管实施情况.

- 巴塞尔委员会、COSO 监管情况

- 人民银行、银保监会等监管情况

5 **2. 国内外 BCM 审计实施情况**

- 国外信息科技审计实施及案例

- 国内信息科技审计实施及案例

3. BCM 风险管控策略实施建议

- 公司治理与全面风险管理视角建议

10 ■ 经营策略与业务模式建议

- 金融科技创新与应用建议

- 管理数据及业务数据管理建议

- BCP 计划编制与实施步骤建议