外部供应商控制义务

恢复规划

版本 14.0，最终版本 2024 年 10 月

1. 定义：

中断事件	供应商选择通过实施恢复和复原力计划和功能来进行缓解的事故影响（无论原因为何）的登记册。 网络事件、自然灾害或人为事件等干扰因素可能会中断实体的运营。
事故	是指可通过调用恢复计划将其作为日常操作的一部分进行管理的中断事件。
恢复计划	恢复计划是详细说明将服务还原到运行状态所需执行的步骤和操作的文档。这些文档可能称为“业务连续性计划”或类似名称。
恢复规划	用于恢复业务服务、业务流程和基本依赖关系的流程或规划。
恢复时间目标	是指从服务意外失败或中断到恢复运行之间的时间。
恢复点目标	恢复点目标 (RPO) 是指“恢复过程开始时数据可用性的目标状态”。它是衡量业务在恢复情形中可承受的最大数据丢失量的标准。
复原力类别	复原力类别是巴克莱使用的一种评级，用于根据重要性和影响将复原力要求应用于服务。复原力类别推动实现恢复时间目标 (RTO)、恢复点目标 (RPO) 和验证频率要求。
不可容忍的损害	从顾客/消费者/客户、金融市场或巴克莱的安全性和稳健性角度来看，服务中断达到无法容忍的程度。
资源依赖关系	提供业务服务所需的依赖资源（技术、第三方服务、劳动力）。

2. 复原力关键性矩阵：

供应商的服务被分配至特定的复原力类别 (0-4)，这些类别反映了巴克莱根据服务中断可能对巴克莱造成的影响而要求供应商达到的恢复目标。较高的复原力类别（即较小的数字）将需要与巴克莱服务的重要性相称的较高复原力和恢复能力标准。供应商应确保，其服务符合巴克莱为合同服务规定的适用复原力类别的复原力关键性矩阵中规定的恢复要求。复原力关键性矩阵根据复原力类别指定适用的控制措施。有关控制要求的详细信息，请参见第 3 节（*控制*）。

风险影响评估	超高影响	高影响	中等影响	低影响	影响不大
复原力类别	0	1	2	3	4
RTO 目标	最长 1 小时	最长 4 小时	最长 12 小时	最长 24 小时	无计划恢复
RPO 目标	最长 5 分钟	最长 15 分钟	最长 30 分钟	最长 24 小时	无计划恢复

技术测试频率	复原力类别 0	复原力类别 1	复原力类别 2	复原力类别 3	复原力类别 4
系统恢复计划验证	至少每年两次	至少每年两次	至少每 12 个月一次	至少每 24 个月一次	无计划恢复
数据恢复计划验证	在类生产环境中对计划进行年度验证	通过桌面演练进行年度验证	至少每 12 个月一次	可选	无计划恢复
平台和应用程序重建计划验证	通过桌面演练进行年度验证	通过桌面演练进行年度验证	可选	可选	无计划恢复

供应商控制适用性	复原力类别 0	复原力类别 1	复原力类别 2	复原力类别 3	复原力类别 4
1. 包含在恢复规划中的资源依赖关系映射要求	✓	✓	✓	✓	O
2. 恢复规划中的中断事件要求	✓	✓	✓	✓	O
3. 业务恢复规划和验证要求	✓	✓	✓	✓	O
4. 综合测试要求	✓	✓	O	O	O
5. 系统恢复计划和验证要求	✓	✓	✓	✓	O
6. 数据恢复计划和验证要求	✓	✓	O	O	O
7. 数据中心多样性和云服务提供商要求	✓	✓	✓	✓	O
8. 平台和应用程序重建计划要求	✓	✓	O	O	O

✓ = 必需	O = 可选

如果在**审查期间发现任何问题，或在控制测试期间未能满足要求，供应商必须即时通知巴克莱（通常在** 10 天内）并在**约定日期之前补救问题。**

3. 控制：

供应商必须采用结构化的复原力方法（业务连续性和灾难恢复），并由《政策和标准》文档提供支持，该文档按照适用的行业最佳实践和监管要求管理运营和技术复原力要求。结构化的复原力方法必须由高级管理层监督，并每年对其有效性进行审查和评估。

控制标题	控制描述	为什么这很重要
1. 包含在恢复规划中的资源依赖关系映射要求	供应商必须定义并记录对向巴克莱提供服务至关重要的资源依赖关系。必须每 12 个月（或在发生重大变更时）维护并审查一次这些依赖关系。 需要考虑的资源依赖关系包括： ▪ 技术和数据（内部和分包商提供）。 ▪ 重要分包商（可能对巴克莱所用服务的性能和提供产生重大影响）。 ▪ 劳动力（人员流失；不考虑工作区域恢复策略或在家工作能力）。	供应商需要了解并记录其向巴克莱提供服务的资源依赖关系。资源依赖关系必须构成供应商业务恢复计划的一部分，以确保考虑这些依赖关系，从而减轻事故的影响，防止无法向巴克莱银行提供服务。
2. 恢复规划中的中断事件要求	供应商必须定义恢复规划范围内的中断事件，以及确保服务可在商定的服务级别和相应的恢复时间目标范围内交付所需的规划级别。供应商必须确保中断事件始终反映当前风险/威胁形势，对其严重性和合理性进行评估，并得到行业和情报洞察的支持。 供应商至少必须在其计划范围内包括以下中断事件。 ▪ 多个地点的建筑物损失，对向巴克莱交付服务有影响。（建筑物和相关基础设施不可用）。 ▪ 数据丢失情景，包括数据损毁、网络事件以及对向巴克莱交付服务的潜在影响。 ▪ 劳动力资源损失，对交付商定的服务水平有影响（即大流行病事件、地缘政治事件、国家基础设施严重故障等）。 ▪ 技术服务损失（即数据中心或云服务提供商区域的损失）。 ▪ 重要分包商（服务或用品）损失。	巴克莱具有商业（和风险驱动）要求，以避免和/或能够及时从重大中断事件中恢复，**即具有适当的复原力。巴克莱必须得到供应商的保证，并且必须能够向其利益相关者保证：如果发生中断，其服务能够尽可能减少中断的影响（无论是客户、财务和/或声誉影响）。**

控制标题	控制描述	为什么这很重要
	必须每年对中断事件进行持续审查，以便为规划和测试提供信息，并证明中断事件是如何随着时间的推移而演变的。	
3. 业务恢复规划和验证要求	供应商必须为其定义的中断事件维持恢复计划，以支持其恢复目标。 恢复计划应记录详细的恢复步骤和供应商的应对措施，以便减轻对向巴克莱提供的服务的影响和/或延迟其不可用性。 计划中至少应涉及： ▪ 可能的解决方法。 ▪ 决策方案。 ▪ 沟通和业务优先级，以恢复/维持最低可行服务水平。 ▪ 依赖关系。 必须每 12 个月（或在发生重大变更时）测试并验证一次恢复计划，证明可以提供商定的服务水平，并且服务符合巴克莱规定的复原力类别要求。 如果任何计划未能达到商定的服务水平或适用的复原力类别要求，供应商必须即时通知巴克莱（通常在 10 天内）并提供详细的修复计划（包括将要采取的措施和相应的完成日期）。	企业应制定有文件记录的恢复计划，完成相关验证，以此向巴克莱保证，这些计划不仅能够按预期运作，还考虑了所有依赖因素，以证明其能够提供商定的服务水平且服务符合巴克莱规定的复原力要求。
4. 综合测试要求	为确保了解巴克莱与供应商服务在服务恢复方面的相互依存关系，供应商必须应巴克莱的要求，在双方商定的日期参与综合测试，以验证供应商和巴克莱的集体复原力/连续性。 巴克莱每 2 年不会提出一次以上的此请求，除非之前的综合测试已突显出重大不足或发生了导致服务中断的事故。	联合练习有助于确保制定适当的恢复规划方案，并采用有效的沟通策略，同时确保供应商和巴克莱采取协调一致的对策，管理业务中断并尽可能减少对巴克莱客户和更广泛的金融系统的影响。 巴克莱需要按照监管要求，与第三方服务提供商执行业务连续性测试。

控制标题	控制描述	为什么这很重要
5. 系统恢复计划和验证要求	供应商必须制定系统恢复计划，详细说明在中断后将系统恢复到运行状态所需的操作。必须对计划进行测试和验证，以（用证据）证明系统可以按照定义的巴克莱复原力类别的要求，在规定的恢复时间目标和恢复点目标内恢复。 对于采用主动/被动配置设计的系统，必须激活被动环境并将其用作 BAU 生产环境，持续时间足以证明能力和完全集成功能。（至少一周） 对于设计为主动/主动的服务，验证应证明在节点、实例或可用性区域（对于云托管服务）丢失时，系统能够继续运行（至少 60 分钟）。 验证频率要求由系统的复原力类别定义。请参阅复原力关键性矩阵。	如果系统恢复计划缺失或不足，则可能会导致巴克莱或其客户在发生事故后承受不可接受的技术服务损失。保持更新和实践复原力文档可确保恢复计划与业务需求保持一致。
6. 数据恢复计划和验证要求	供应商必须为向巴克莱交付服务所需的每个技术系统制定数据恢复计划。必须至少每 12 个月（或在发生重大变更时）审查一次计划的准确性，并且计划至少应考虑以下事项： ▪ 数据源和流（上游和下游） ▪ 备份和复制源 ▪ 恢复后的数据同步要求 供应商必须针对向巴克莱交付服务所需的每个技术系统，测试并验证数据恢复计划，并（用证据）证明恢复流程可以将数据恢复至预期运行状态和必要的恢复点目标。	数据丢失是巴克莱面临的最大威胁之一，这可能是恶意行为或系统故障造成的。为此情景制定计划至关重要，这有助于识别和了解数据源和依赖关系。
7. 数据中心多样性和云服务提供商要求	供应商必须确保向巴克莱交付服务所需的每个技术系统在数据中心之间具有复原力，并且数据中心之间的地理距离足够远，以降低多个数据中心同时受到单个事件影响的风险。 如果技术系统托管在云服务提供商处，则该系统应在不同的可用性区域中可用，以缓解 AZ 中断的影响。关键系统必须证明从云服务提供商区域故障恢复的能力。	技术系统应部署在多个数据中心，以防范数据中心中断。这扩展到云服务提供商托管的系统 - 以防出现区域故障。

控制标题	控制描述	为什么这很重要
8. 平台和应用程序重建计划要求	供应商必须为向巴克莱交付服务所需的每个技术系统维护平台和应用程序重建计划，并至少每 12 个月（或在发生重大变更时）进行一次审查、批准和测试。 这些计划适用于无法使用传统恢复/还原选项，而需要从“裸机”重建系统的情形。 计划应考虑： ▪ 操作系统/基础设施软件 ▪ 应用程序部署和配置 ▪ 安全控制/配置 ▪ 系统生态系统依赖关系和重新集成 ▪ 数据要求（数据恢复计划） ▪ 用于执行和调度恢复计划的工具依赖关系 ▪ 控制面恢复（例如，Active Directory） 至少必须通过桌面演练来验证计划的可行性。	技术服务和支持安排具有适当的恢复计划至关重要，以应对网络/数据完整性事件。