外部供应商控制义务

恢复规划

版本 12.0，2022 年 10 月

1. 定义：

“危机”	是指需要超出正常 BAU 结构和/或资源范围的响应，并且需要进行人员干预以做出决策和进行协调的中断或声誉事件。
“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。
“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。
“生产转换”	生产转换是一个术语，是指将有故障的技术系统转移到备用环境 (DR) 并长时间运行生产功能。
“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。
“复原力类别”	复原力类别是一种评级，用于将复原力要求应用于服务。 其中包括 RTO、RPO、验证要求和频率。

2.复原力关键性矩阵：

巴克莱为供应商的服务分配了特定的复原力类别 (0-4)。 较高的复原力类别（即较小的数字）将需要与服务的重要性相称的较高复原力或恢复标准。供应商应确保其服务满足巴克莱为合同服务规定的适用恢复力类别对应的以下恢复时间目标 (RTO) 和恢复点目标 (RPO)：

		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
		复原力类型	连续	高复原力	有复原力	恢复	暂停/ 仅备份
中断事件	应用程序	RTO 目标 （非数据/网络事件）	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 （非数据/网络事件）	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

3.控制：

控制标题	控制描述	为什么这很重要
1.恢复规划中的中断事件要求	巴克莱应规定合同服务的复原力类别。 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。 中断事件规划应至少考虑以下因素： ▪ 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的损失，对所有技术服务有影响）。 ▪ 材料分包商（服务或用品）损失。 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。 供应商必须能够证明已考虑、测试并验证了各种严重因素。	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）。
2.包含在恢复规划中的依赖关系映射要求	供应商必须定义并记录对向巴克莱提供服务至关重要的依赖关系。必须每 12 个月维护并审查一次这些依赖关系。 需要考虑的依赖关系包括： ▪ 技术和数据（内部和分包商提供）。 ▪ 重大分包商（对向巴克莱提供服务至关重要的分包商）。 ▪ 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）。	服务提供商需要了解用于向巴克莱提供其服务的依赖关系。任何依赖关系都将构成业务恢复计划的一部分，确保考虑这些依赖关系，以减轻事故的影响并防止巴克莱无法获得服务。

控制标题	控制描述	为什么这很重要
3.恢复规划的验证要求	供应商必须为其商定的中断事件维护业务恢复计划。 业务恢复计划应记录详细的恢复步骤和供应商响应，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。 计划中至少应考虑： ▪ 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 ▪ 依赖关系 必须每 12 个月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，供应商必须立即通知巴克莱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）。	完成测试和验证，以便向巴克莱保证服务的设计和计划按预期进行，服务包括所有依赖关系，并证明可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	复原力类别为 0-1 的供应商应巴克莱的要求，在双方约定的日期，必须参与综合测试，以验证供应商和巴克莱的综合复原力/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。
5.系统恢复计划	供应商必须为向巴克莱交付服务所需的每个技术系统/服务制定系统恢复计划 (SRP)，以及相应的恢复时间目标 (RTO) 和恢复点目标 (RPO)。必须至少每 12 个月审查一次计划的准确性。	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	复原力类别为 0-1 的供应商，必须为向巴克莱交付服务所需的每个技术系统/服务制定数据恢复计划。必须至少每 12 个月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	数据丢失是我们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。

控制标题	控制描述	为什么这很重要
7.数据中心多样性	供应商必须确保向巴克莱交付服务所需的每个技术系统/服务在数据中心之间具有复原力，并且数据中心之间的距离足够远，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，则该服务应在不同的可用性区域中可用，以缓解 AZ 中断的影响。 复原力类别为 0-1 的服务应在云区域之间具有复原性。	数据中心应具有备用电源、网络链路等，并且之间的距离应足够远，以降低多个数据中心同时受到单个事件影响的风险。
8.系统恢复计划验证	供应商必须测试并验证系统恢复计划，证明技术系统/服务可以恢复，并且符合由复原力关键性矩阵定义的恢复时间目标和恢复点目标。 对于交付复原力类别为 0-1 的服务所需的每个技术系统/服务，如果为复原措施设计了主动/被动配置，则必须按照记录在案的系统恢复计划激活被动环境，并将其作为 BAU 生产环境使用，使用持续时间必须足够长，以证明能力和完全集成功能（生产转换）。 对于设计为主动/主动的服务，验证应证明在丢失一个主动环境（处理资源减少的情景）时，服务能够继续运行。 验证频率要求必须得到相关复原力类别的支持，即： - 复原力类别 0：每年必须通过 PCO 至少执行四次 SRP 验证。 - 复原力类别 1：每年必须通过 PCO 至少执行两次 SRP 和 PCO 验证。 - 复原力类别 2：每 12 个月必须至少执行一次 SRP 验证。 - 复原力类别 3：每 24 个月必须至少执行一次 SRP 验证。 如果任何测试未能达到适用复原力类别的最低恢复要求，供应商必须立即通知巴克莱，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）。	第三方提供的技术系统可能会影响巴克莱客户的行程。确保支持巴克莱业务运营的第三方拥有经过测试的充分复原力计划至关重要，同时监管机构也要求巴克莱在管理供应商时采用适当的治理措施。 生产转换 (PCO) 是用于验证采用主动-被动配置的系统的被动实例是否按预期运行并达到 BAU 操作所需的能力的一种方法。此外，PCO 还验证对上游或下游系统的任何依赖关系是否继续按预期运行。
9.数据恢复计划验证	复原力类别为 0-1 的供应商，必须针对向巴克莱交付服务所需的每个技术系统/服务，测试并验证数据恢复计划，并证明恢复流程可以将数据恢复至运行状态。应至少每 12 个月进行一次验证。 如果任何计划未能达到适用复原力类别的最低恢复要求，供应商必须立即通知巴克莱，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）。	数据是一个关键因素，可能会在许多方面受到不利影响。必须执行记录在案的数据还原、恢复或重新创建计划，确认数据准确且可行。

控制标题	控制描述	为什么这很重要
10.平台和应用程序重建计划	复原力类别为 0-1 的供应商，必须为向巴克莱交付服务所需的每个技术服务/系统维护平台和应用程序重建计划，并至少每 12 个月进行一次审查、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） • 用于执行恢复计划的工具依赖性 如果任何计划未能达到适用复原力类别的最低恢复要求，供应商必须立即通知巴克莱，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）。	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。