外部供应商控制义务

物理安全（技术控制）

版本 12.0，2022 年 10 月

控制标题	控制描述	为什么这很重要
1.访问控制 (TC 5.1)	在用于开展与巴克莱合同相关活动的所有场所，必须部署电子、机械或数字访问控制并加以管理。所有安全系统均应按照法律和法规要求进行安装、操作和维护。必须仅限授权人员对电子访问控制系统进行逻辑和管理访问，并且必须严格管理和控制对物理密钥和组合的访问。 必须维护凭据/密钥/组合持有人的审计记录，包括授予、修改和撤销访问权限。 必须有效管理所有访问凭据，以降低未经授权访问的风险。必须按照供应商的访问控制程序来管理访问凭据。 只有在收到适当的批准后才能签发访问凭据。 必须以适当的时间间隔重新认证所有进入受限区域的通道。 如果不再需要进入场所或受限区域，负责管理访问凭据的职能部门必须在收到相关业务部门或职能部门告知针对相关员工的要求发生变化后 24 小时内停用访问凭据（例如，角色或职责发生变化，或终止雇用）。 如果需要远程工作，其中供应商或其分包商将以物理或虚拟形式访问、存储或处理具有限制性质的巴克莱信息（包括个人数据或在“需要知道”的基础上向供应商提供的任何敏感信息），供应商必须先获得巴克莱对这些安排的批准，然后才能访问这些数据。	维持有效的访问控制系统和访问管理流程及程序，是保护场所免遭未经授权访问和确保资产安全所需的分层组合控制的重要组成部分。除非采取有效的访问控制措施，否则存在未经授权人员进入供应商场地或场地内受限区域的风险。 这可能会增加巴克莱资产丢失或损坏的风险，从而导致财务损失和相关的声誉损失和/或监管罚款或谴责等事件。
2.入侵检测系统和监控摄像头 (TC 5.2)	必须部署入侵检测系统 (IDS) 和监控摄像头，以阻止、检测、监控和识别不适当的访问或犯罪活动。部署的设备必须与通过每个地点的安全风险评估确定的当前物理安全威胁相符。所有摄像头系统和 IDS 必须按照当前行业标准（例如国际标准化组织 (ISO)、系统和组织控制 (SOC)、现行法律和法规要求以及当前制造商规格）进行安装、操作和维护。 必须制定相关程序，确保有效监控和管理 IDS 和监控摄像头警报。只有授权人员才能访问安全系统。	IDS 和监控摄像头系统是分层控制的一部分，用于保护场所免受未经授权的访问，并确保资产的安全。 除非这些系统得到有效安装、操作、监控和维护，否则存在未经授权访问网站和建筑物（内含巴克莱资产和数据）的风险，并且将无法及时检测到未经授权的访问。

3.数据中心、大厅和通信设施 (TC 5.3)	所有位于同一地点且独立的第三方数据中心、云提供商、数据大厅和通信设施（包括服务器机房和独立的通信机柜）都必须获得有效保护，以防止未经授权的访问以及巴克莱资产或数据被盗或损坏。所有数据中心都必须实施技术、物理和人工分层控制以及现场特定程序，以有效保护数据大厅和所有其他关键区域的边界、建筑物和完整性。 控制措施包括但不限于监控摄像头、入侵检测系统、访问控制和安全员。 如果设施位于共享位置，则必须在其离散隔离设施周围部署有效的安全措施。	为了保护数据中心、数据大厅和类似关键位置内的巴克莱资产或数据，避免因未经授权访问受限空间而导致其丢失、损坏或被盗的风险。

本标准必须与以下标准一起阅读，并且必须对其应用范围内确定的管理控制措施：

第三方服务提供商控制义务 (TPSPCO)，管理控制要求 - 信息、网络和物理安全、技术、恢复规划、数据隐私、数据管理、PCI DSS 和 EUDA。