外部供应商控制义务

物理安全（技术控制）

版本 13.0，日期 2023 年 9 月

控制标题	控制描述	为什么这很重要
1.访问控制 (TC 5.1)	必须为所有安全区域定义访问控制规则，并通过正式批准的程序和明确定义的职责提供支持。 必须通过使用电子、机械或数字访问控制的适当入口控制和访问点保护安全区域。 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独特访问凭据。 必须以适当的时间间隔重新认证进入受限区域的所有访问凭据。 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）。	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. 安全边界、建筑物和空间 (TC 5.2)	必须定义和实施安全边界，以保护包含信息和其他相关资产的区域，使其与已确定和预期的风险和威胁环境相称。必须根据当前和预期的威胁级别，以基于风险的方式设计和实施针对办公室、房间、和设施的物理安全措施（包括访问控制系统、安全摄像头、入侵者检测系统和其他适当的技术控制措施），使其与所采取的业务流程以及信息和资产价值相称。 必须设计和实施在安全区域工作的安全流程。必须定义和适当执行针对纸张和可移动存储媒体的明确桌面规则以及针对信息处理设施的明确屏幕规则。	为了保护数据中心、数据大厅和供应商场所（包括供应商维护的位置和第三方）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。

	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。如果设施位于共享位置，则必须部署有效安全控制措施以实现离散隔离和监视。	
3.保护基础设施和资产免受物理威胁 (TC 5.3)	必须通过部署适合当前和预期威胁环境的安全摄像头、入侵者检测系统和/或其他分层安全控制措施，设计和实施针对基础设施和资产所面临物理威胁的保护。必须持续监控场所是否存在未经授权的物理访问。 设备必须安全放置并受到保护。必须保护承载电力、数据或支持信息服务的电缆，防止物理拦截、干扰或损坏。必须按照制造商的要求安装和维护安全设备和装置，并对其进行监控以确保信息的可用性、完整性和机密性。 保存在场外的巴克莱资产必须得到静态和动态保护。 必须以符合现行行业标准的方式，正确安装和维护设备，以确保信息的可用性、完整性和机密性。所有安全系统的安装和操作必须符合现行法律和法规要求。 如果存在交付和装载区域，则必须对其进行适当控制，并将其与运营设施隔离开来，以避免未经授权的访问和未经验证的交付的潜在威胁。	部署和操作与当前和预期威胁相称的物理安全控制措施，将限制或防止未经授权的访问、盗窃或故意损坏场所和资产的影响。

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。